

EVALUACIÓN PRUEBA DE HABILIDADES PRACTICAS CCNA

DAVID ALBERTO PÉREZ MEJIA

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS Y TECNOLOGÍAS
INGENIERÍA DE SISTEMAS
BOGOTÁ
2021**

EVALUACIÓN PRUEBA DE HABILIDADES PRACTICAS CCNA

DAVID ALBERTO PÉREZ MEJIA

Diplomado de profundización cisco

Director

JUAN CARLOS VESGA FERREIRA

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS Y TECNOLOGÍAS
INGENIERÍA DE SISTEMAS
BOGOTA
2021**

Dedicatoria

Este trabajo está dedicado en primer lugar a Dios, a mis padres y a toda mi familia quienes me han brindado todo su apoyo para el logro de mis metas.

AGRADECIMIENTOS

Doy gracias a Dios por estar en mi camino siempre, a mis padres quienes han estado desde mi inicio de mi carrera apoyándome en todos los procesos de mi educación, a mi familia porque siempre en momentos difíciles me dieron ánimos de culminar con mi profesión.

CONTENIDO

	Pág.
GLOSARIO	8
RESUMEN.....	10
1. INTRODUCCIÓN.....	11
2. OBJETIVOS	12
2.1 OBJETIVO GENERAL.....	12
2.2 OBJETIVOS ESPECÍFICOS	12
3. ESCENARIO UNO	13
4. ESCENARIO 2	42
CONCLUSIONES.....	84
BIBLIOGRAFÍA.....	86

LISTA DE TABLAS

	Pág.
Tabla 1. Eliminar Configuración Inicial	14
Tabla 2. Direccionamiento IP Servidor	15
Tabla 3. Configuración en Router 1	16
Tabla 4. Configuración en Router 2	17
Tabla 5. Configuración en Router 3	19
Tabla 6. Configuración en Switch 1	21
Tabla 7. Configuración en Switch 3	21
Tabla 8. Verificar Conectividad	22
Tabla 9. Configuración de VLAN en Switch 1	24
Tabla 10. Configuración de Vlan en Switch 3.....	25
Tabla 11. Configuración de subinterfaces en Router 1	27
Tabla 12. Verificar Segunda Conectividad	28
Tabla 13. Configuración Protocolo RIP en Router 1.....	30
Tabla 14. Configuración Protocolo RIP en Router 2.....	31
Tabla 15. Configuración protocolo RIP en Router 3.....	32
Tabla 16. Verificación Protocolo RIP.....	32
Tabla 17. Creación Pool DHCP en Router 1	34
Tabla 18. Configuración NAT en Router 2	35
Tabla 19. Verificación protocolo DHCP y NAT	36
Tabla 20. Verificar NAT.....	39
Tabla 21. Sumarización Medellín 1	57
Tabla 22. Sumarización IP Bogotá 1.....	57
Tabla 23. Tabla de interfaces de router	65

LISTA DE ILUSTRACIONES

	Pág.
Ilustración 1 Topología Escenario Uno	13
Ilustración 2. Verificar conectividad1.....	23
Ilustración 3. Verificar conectividad3.....	29
Ilustración 4. Verificación Protocolo RIP	33
Ilustración 5. Verificación Protocolo DHCP	37
Ilustración 6. Verificar Interfaz.....	41
Ilustración 7. Topología planteada escenario 2.....	42
Ilustración 8. Tabla de router Medellín 1	58
Ilustración 9. Tabla de router Medellín 3.....	59
Ilustración 10. Tabla de router ISP.....	60
Ilustración 11. Tabla de router Bogotá 1	60
Ilustración 12. Tabla de router Bogotá 2	61
Ilustración 13. Tabla de router Bogotá 3	61
Ilustración 14. Redes redundantes en Bogotá 2	63
Ilustración 15. Rutas estáticas ISP	64
Ilustración 16. Protocolos de Bogotá 2.....	67
Ilustración 17. Protocolos de Medellín 1	68
Ilustración 18. Protocolos de Medellín 2	68
Ilustración 19. Protocolos de Medellín 3	69
Ilustración 20. Base de datos RIP Bogotá.....	70
Ilustración 21. Base de datos Rip Medellín 1	70
Ilustración 22. Conectividad de Medellín a ISP	73
Ilustración 23. Conectividad de ISP a Medellín 1 y 2	74
Ilustración 24. Conectividad de router Bogotá 1 a ISP	75
Ilustración 25. Conectividad de ISP a Bogotá 1 y 2.....	76
Ilustración 26. Conectividad de Medellín 2 a router Bogotá 1	77
Ilustración 27. Prueba de ping a Bogotá 1	79
Ilustración 28. DHCP en PC Medellín 1	80
Ilustración 29. DHCP en Medellín 2	81
Ilustración 30. DHCP Bogotá 1	82
Ilustración 31. DHCP Bogotá 2	83

GLOSARIO

ENRUTAMIENTO: es el proceso de reenviar paquetes entre redes, siempre buscando la mejor ruta (la más corta). Para encontrar esa ruta más óptima, se debe tener en cuenta la tabla de enrutamiento y algunos otros parámetros como la métrica, la distancia administrativa, el ancho de banda.

LAN: puede hacer referencia a: Red de área local (por sus siglas en inglés Local Área Network), interconexión de varios ordenadores y periféricos.

NETWORKING: El networking es una práctica común en el mundo empresarial y emprendedor. Es una palabra que ya se utiliza de forma cotidiana en el ámbito profesional y que hace referencia a eventos, tanto de tipo formal como informal, en los que puedes construir una red de contactos que te ayuden a generar oportunidades tanto de negocio como laborales.

PUERTA DE ENLACE: es el dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos, y también posibilita compartir recursos entre dos o más computadoras.

ROUTER también conocido como enrutador o rúter es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un encaminador (mediante puentes de red o un switch), y que por tanto tienen prefijos de red distintos.

TOPOLOGÍA DE RED: se define como el mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red,

sea en el plano físico o lógico. El concepto de red puede definirse como «conjunto de nodos interconectados». Un nodo es el punto en el que una curva se intercepta a sí misma. Lo que un nodo es concretamente depende del tipo de red en cuestión.

VLAN: acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física

RESUMEN

El objetivo de este trabajo es crear de manera razonable la información obtenida a través del Curso CISCO inside and out (Diseño y ejecución de arreglos LAN/WAN incorporados), centrandó al alumno en habilidades que permitan a la administración de las organizaciones ofrecer respuesta para las dos situaciones donde se trabaja cada una con su geografía particular y la configuración del engranaje según la tabla de tendencia para cada una de ellas, para su avance se utiliza la utilización de la programación CISCO PACKET TRACERT. La situación uno cubre la convención de dirección RIPv2, reasignación de curso, epítome PPP, verificación PAT y CHAP, administraciones DHCP y ejecución NAT. La situación dos lleva a cabo la dirección de OSPFv2, el deterioro de DNS, la configuración de NAT, las administraciones de DHCP, la convención 802.1Q y las VLAN.

PALABRAS CLAVE: Enrutamiento, Lan, Router, Topología de red

1. INTRODUCCIÓN

El trabajo prueba de habilidades de evaluación de Cisco pretende extender, planificar y ejecutar arreglos incorporados LAN/WAN donde se dará la respuesta para dos situaciones que son imperativas para probar las habilidades procuradas en el avance del equivalente, la situación uno aplica la convención de dirección RIP adaptación 2, verificación de encarnación PPP, uso de NAT, PAT, diseños de administración DHCP, registros de control de acceso ACL. Estos se ejecutan en los interruptores para construir la seguridad de la red, ya que utilizan enfoques de paquetes de entrada y salida para el hardware explícito asociado a la organización.

La situación dos juega el uso de la convención de dirección OSPFv2, los arreglos VLANS, los puertos de tronco, la ejemplificación, la seguridad del interruptor, la aplicación de la convención 802.1Q, la ejecución de DHCP - NAT para IPv4 y el uso de VLANS de curso estático.

El trabajo tiene como objetivo la creación de habilidades de análisis, el desarrollo de las topologías de la organización a través de la programación de recreación en Cisco Packet Tracer que permite hacer diseños esenciales en los diversos gadgets para establecer la disponibilidad en la organización. Las dos situaciones permitirán investigar y ofrecer respuesta a los distintos problemas de direccionamiento erróneo de IP mediante órdenes de disponibilidad.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Llevar a cabo las habilidades y la información adquirida, a través de la utilización de las diversas ideas viables en la mejora de las situaciones propuestas, para introducir las habilidades de las competencias en el avance de este curso de reconocimiento.

2.2 OBJETIVOS ESPECÍFICOS

Distinguir los distintos componentes que son importantes para el desarrollo de las topologías de red planteadas en la presente acción.

Aplicar los distintos diseños, según las convenciones demostradas para cada situación, permitiendo la disponibilidad de los componentes utilizados en cada topología.

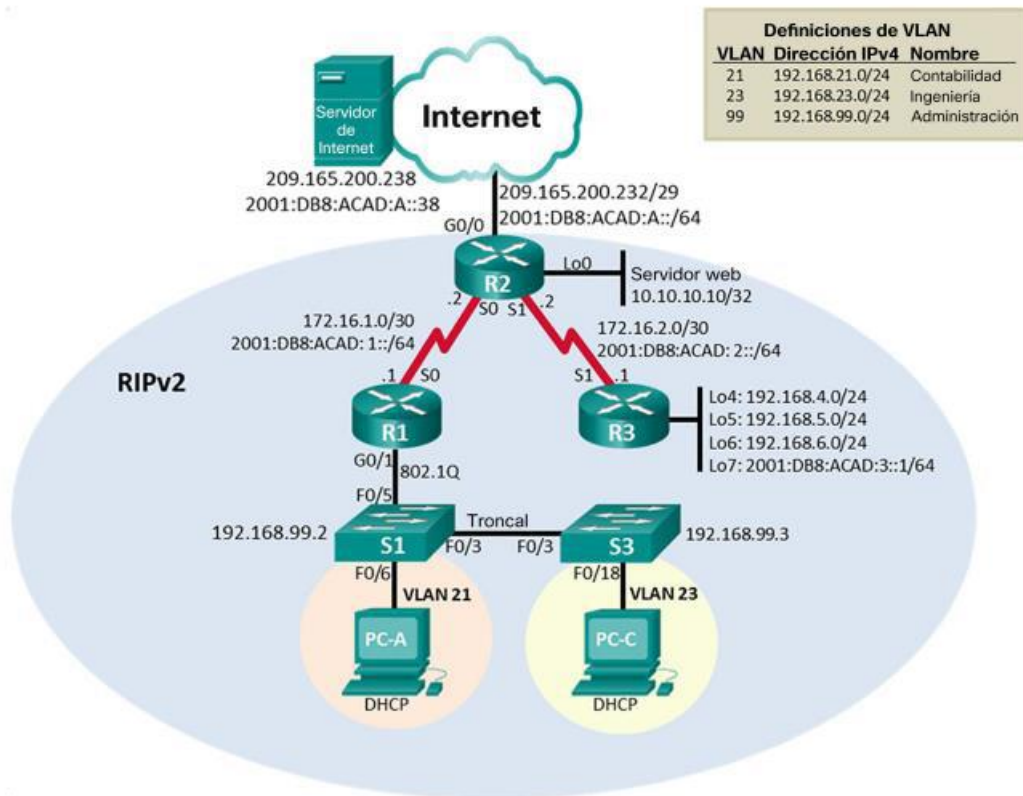
Aprobar la red en cada una de las situaciones, para aprobar la pertinencia de cada configuración, para transmitir un elemento útil.

3. ESCENARIO UNO

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.

Ilustración 1 Topología Escenario Uno

Topología



Nota: recuperado de packet tracer 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.

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

El objetivo de la presente parte es el de eliminar el registro de configuración inicial de todos los dispositivos a utilizar en el desarrollo de la presente práctica.

Configuración realizada

Tabla 1. Eliminar Configuración Inicial

Dispositivo	Comandos Utilizados
Router 1	R1>Enable R1#erase startup-config R1# reload
Router 2	R2>Enable R2#erase startup-config R2# reload
Router 3	R3>Enable R3#erase startup-config R3# Reload
Switch 1	S1>Enable S1#erase startup-config S1#delete Vlan.dat S1# reload S1# show flash
Switch 3	S3>Enable S3#erase startup-config S3#delete Vlan.dat S3#reload S3#show flash

PARTE 2: CONFIGURAR LOS PARÁMETROS BÁSICOS DE LOS DISPOSITIVOS

Paso 1: Configurar la computadora de Internet

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

Tabla 2. Direccionamiento IP Servidor

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

En el presente paso se realiza la configuración del servidor WEB, se asigna el direccionamiento IPV4 e IPV6 que tendrá en la presente actividad.

Paso 2: Configurar R1

En el presente paso se realiza la configuración básica del Router 1, se configuran los parámetros básicos tales como nombre del host, contraseña telnet, líneas vty, encriptación de contraseñas, mensaje de advertencia, se deshabilita la búsqueda DNS, esta configuración inicial permite ajustar de una manera practica y segura los diferentes elementos que se utilizan en la topología.

Se realiza la descripción de la interfaz serial 0/0/0, asignación de dirección IPV4 e IPV6, se habilita el direccionamiento IPV6, se habilita la interfaz como DCE y se

habilita el puerto utilizado por la interfaz, configuración realizada con el fin de garantizar la conectividad de la red.

Configuración realizada

Tabla 3. Configuración en Router 1

Dispositivo	Comandos Utilizados
Router 1	<pre> R1>Enable R1#configure terminal R1(config)#No ip domail-lookup R1(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)#Exit R1(config)#Service password- encryption R1(config)#Banner motd #SE PROHIBE EL ACCESO NO AUTORIZADO# R1(config)#Interface serial S0/0/0 R1(config-if)#Description CONECTADO A 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 shutdown R1(config-if)#exit R1(config)#Ipv6 unicast-routing R1(config)#Ip route 0.0.0.0 0.0.0.0 S0/0/0 R1(config)#Ipv6 route ::0/0 S0/0/0 </pre>

Paso 3: Configurar R2

En el presente paso se realiza la configuración básica del Router 2, se configuran los parámetros básicos tales como nombre del host, contraseña telnet, líneas vty, encriptación de contraseñas, mensaje de advertencia, se deshabilita la búsqueda DNS, parámetros básicos que permiten describir de manera detallada cada elemento.

Se realiza la descripción de las interfaz serial 0/0/0, asignación de dirección IPV4 e IPV6, se habilita el direccionamiento IPV6 y se habilita el puerto utilizado por la interfaz, descripción interfaz serial 0/0/1, asignación dirección IPV4 e IPV6, se habilita la interfaz como DCE, se habilita el puerto utilizado por la interfaz, para finalizar se habilita el router como servidor HTTP, se habilita interfaz gigabit ethernet como simulador de internet, se establece dirección IPV4 a dirección loopback 0 como servidor web simulado y se establecen rutas predeterminadas IPV4 e IPV6.

Configuración realizada

Tabla 4. Configuración en Router 2

Dispositivo	Comandos Utilizados
Router 2	R2>Enable R2#configure terminal R2(config)#No ip domail-lookup R2(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)#Exit R2(config)#Service password-

	<pre> encryption R2(config)#Ip http server R2(config)#Banner motd #SE PROHIBE EL ACCESO NO AUTORIZADO# R2(config)#Interface serial S0/0/0 R2(config-if)#Description CONECTADO A R1 R2(config-if)#Ip address 177.17.1.2 255.255.255.252 R2(config-if)#Ipv6 address 2001:db8: ACAD:1::2/64 R2(config-if)#No shutdown R2(config-if)#exit R2(config)#Ipv6 unicast-routing R2(config)#Interface serial S0/0/1 R2(config-if)#Description CONECTADO A R3 R2(config-if)#Ip address 177.17.2.2 255.255.255.252 R2(config-if)#Ipv6 address 2001:db8:ACAD:2::2/64 R2(config-if)#Clock rate 128000 R2(config-if)#No shutdown R2(config-if)#exit R2(config)#Ipv6 unicast-routing R2(config)#Ip route 0.0.0.0 0.0.0.0 S0/0/0 R2(config)#Ipv6 route ::0/0 S0/0/0 R2(config)#Interface g0/0 R2(config-if)#Description Simulador de internet R2(config-if)#Ip address 209.165.200.232 255.255.255.248 R2(config-if)#Ipv6 address 2001:DB8:ACAD:A::1/64 R2(config-if)#No shutdown R2(config-if)#exit R2(config)#Interface loopback 0 R2(config-if)#Ip address 10.10.10.10 255.255.255.255 R2(config-if)#Description Simulación servidor web R2(config-if)#exit </pre>
--	---

	R2(config)#ip route 0.0.0.0 0.0.0.0 G0/0 R2(config)#ipv6 route ::0/0 G0/0
--	--

Paso 4: Configurar R3

En el presente paso se realiza la configuración básica del Router 3, se configuran los parámetros básicos tales como nombre del host, contraseña telnet, líneas vty, encriptación de contraseñas, mensaje de advertencia, se deshabilita la búsqueda DNS, parámetros básicos que permiten describir de manera detallada cada elemento.

Se realiza la descripción de la interfaz serial 0/0/1, asignación de dirección IPV4 e IPV6, se habilita el direccionamiento IPV6 y se habilita el puerto utilizado por la interfaz, se habilitan interfaces loopback de la 4 a la 7, se establecen las descripciones y direcciones IPV4, utilizadas como servidores web simulados, para finalizar se asigna una ruta IPV4 e IPV6 predeterminada para la interfaz gigabit ethernet.

Configuración realizada

Tabla 5. Configuración en Router 3

Dispositivo	Comandos Utilizados
Router 3	R3>enable R3#confgiure terminal R3(config)#No ip domail-lookup R3(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

	<pre> R3(config-line)#Exit R3(config)#Service password- encryption R3(config)#Banner motd #SE PROHIBE EL ACCESO NO AUTORIZADO# R3(config)#Interface serial S0/0/1 R3(config-if)#Description CONECTADO A R2 R3(config-if)#Ip address 177.17.1.2 255.255.255.252 R3(config-if)#Ipv6 address 2001:db8:ACAD:2::1/64 R3(config-if)#No shutdown R3(config-if)#Interface loopback 4 R3(config-if)#Ip address 192.168.4.1 255.255.255.0 R3(config-if)#Interface loopback 5 R3(config-if)#Ip address 192.168.5.1 255.255.255.0 R3(config-if)#Interface loopback 6 R3(config-if)#Ip address 192.168.6.1 255.255.255.0 R3(config-if)#Interface loopback 7 R3(config-if)#Ip address 2001:DB8:ACAD:3::1/64 R3(config-if)#exit R3(config)#Ipv6 unicast-routing R3(config)#Ip route 0.0.0.0 0.0.0.0 S0/0/1 R3(config)#Ipv6 route ::0/0 S0/0/1 </pre>
--	---

Paso 5: Configurar S1

En el presente paso se realiza la configuración básica del Switch 1, se configuran los parámetros básicos tales como nombre del host, contraseña telnet, líneas vty, encriptación de contraseñas, mensaje de advertencia, se deshabilita la búsqueda de servidor DNS.

Configuración realizada

Tabla 6. Configuración en Switch 1

Dispositivo	Comandos Utilizados
Switch 1	S1>enable S1#configure terminal S1(Config)#No ip domain-lookup S1(Config)#Hostname S# 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)#Exit S1(Config)#Service password-encryption S1(Config)#Banner motd #SE PROHIBE EL ACCESO NO AUTORIZADO#

Paso 6: Configurar el S3

En el presente paso se realiza la configuración básica del Switch 3, se configuran los parámetros básicos tales como nombre del host, contraseña telnet, líneas vty, encriptación de contraseñas, mensaje de advertencia, se deshabilita la búsqueda de servidor DNS.

Configuración Realizada

Tabla 7. Configuración en Switch 3

Dispositivo	Comandos Utilizados
Switch 3	S3>enable S3#configure terminal S3(Config)#No ip domain-lookup S3(Config)#Hostname S#

	<pre> 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)#Exit S3(Config)#Service password- encryption S3(Config)#Banner motd #SE PROHIBE EL ACCESO NO AUTORIZADO# </pre>
--	---

Paso 7: Verificar la conectividad de la red

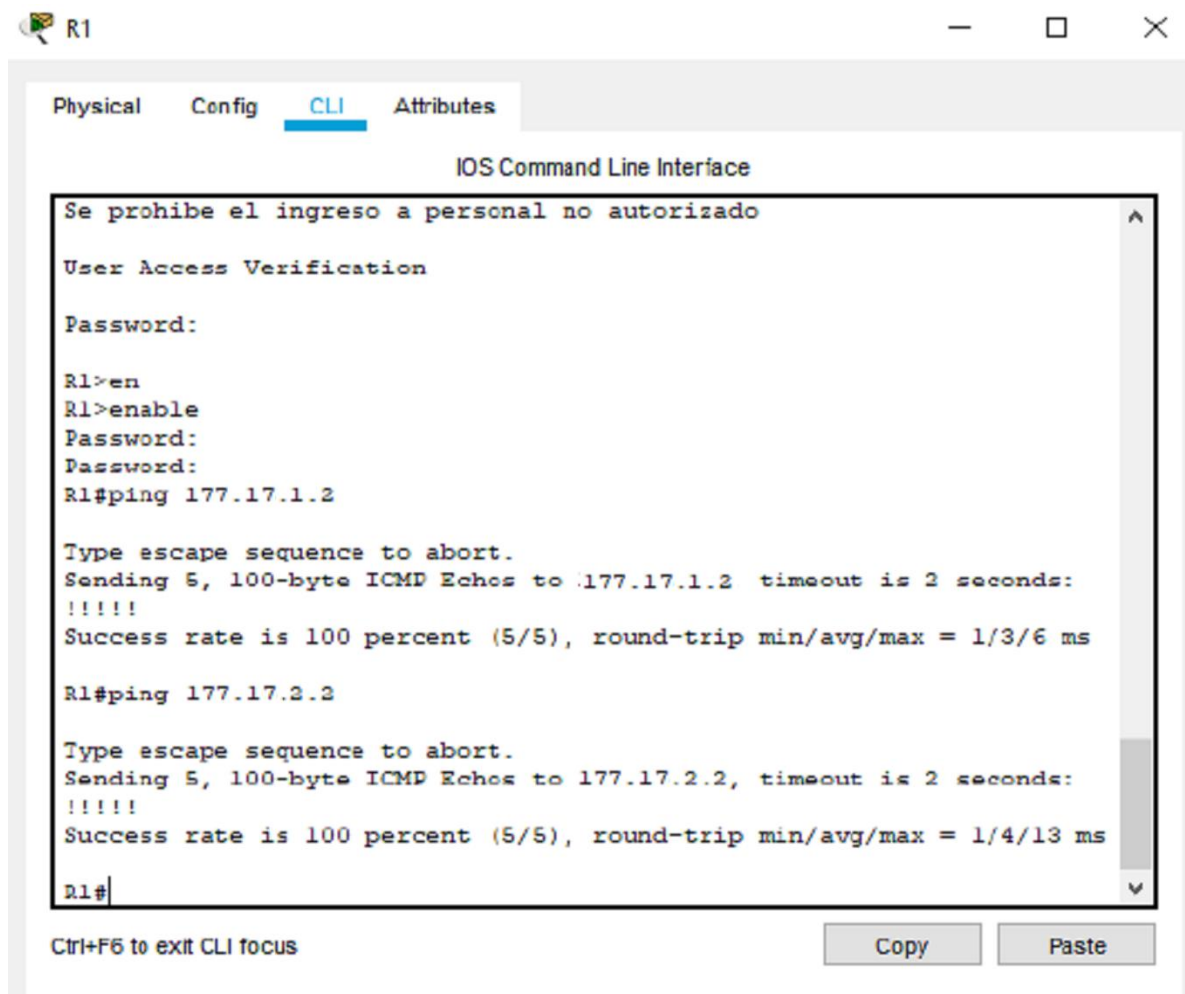
Utilice el comando ping para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 8. Verificar Conectividad

Desde	A	Dirección IP	Resultado de Ping
R1	R2, S0/0/0	177.171.1.2 2001:DB8:ACAD:1::2	Satisfactorio
R2	R3, S0/0/1	177.171.1.2 2001:DB8:ACAD:2::1	Satisfactorio
PC de Internet	Gateway predeterminado	209.165.200.225 2001:DB8:ACAD:A::	Satisfactorio

En el presente paso se verifica la conectividad que debe existir entre R1 y R2, de igual manera del PC de internet al Gateway predeterminado.

Ilustración 2. Verificar conectividad1.



The screenshot shows a network device window titled 'R1' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal output shows a security warning: 'Se prohíbe el ingreso a personal no autorizado' and 'User Access Verification'. The user enters 'en' to enter enable mode, followed by 'enable' and a password. Then, the user enters 'ping 177.17.1.2', which results in a success rate of 100 percent (5/5) with a round-trip time of 1/3/6 ms. The user then enters 'ping 177.17.2.2', also resulting in a success rate of 100 percent (5/5) with a round-trip time of 1/4/13 ms. The terminal ends with 'R1#' and a cursor. Below the terminal window, there is a 'Ctrl+F6 to exit CLI focus' message and 'Copy' and 'Paste' buttons.

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

Paso 1: Configurar S1

En el presente paso se realiza la creación de la base de datos de VLAN a utilizar, se crean y se nombran y crean las VLAN indicadas en el desarrollo del presente escenario, VLAN 22 contabilidad, VLAN 26 ingeniería, VLAN 92 administración, se realiza la asignación de las direcciones IP según la topología, se habilita como enlace troncal las interfaces F0/3 y F0/5 como VLAN nativas, se configuran los

demás puertos como acceso, se asigna la interfaz F0/6 como puerto de acceso de la VLAN 21 y se apagan los puertos que no se utilizaran en el Switch.

Configuración Realizada

Tabla 9. Configuración de VLAN en Switch 1

Dispositivo	Comandos Utilizados
Switch 1	<pre> S1(config)#Vlan 22 S1(config-vlan)#Name CONTABILIDAD S1(config-vlan)#Vlan 26 S1(config-vlan)#Name INGENIERIA S1(config-vlan)#Vlan 92 S1(config-vlan)#Name ADMINISTRATIVA S1(config-vlan)#Exit S1(config)#interface vlan99 S1(config-if)#Ip address 192.168.92.2 255.255.255.0 S1(config-if)#Ip default-gateway 192.168.92.1 S1(config-if)#Interface f0/3 S1(config-if)#Switchport mode trunk S1(config-if)#Swichport native vlan1 S1(config-if)#Interface f0/5 S1(config-if)#Swichpoirt mode trunk S1(config-if)#Swichport native vlan1 S1(config-if)#Exit S1(config)#Interface range fa0/1-2, fa0/4,fa0/6-24 S1(config-if-range)#Switchport mode Access S1(config-if-range)#Exit S1(config)#Interface fa0/6 S1(config-if)#Switchport mode Access vlan22 S1(config-if)#Interface range fa0/1-2, fa0/4, fa0/7-24 S1(config-if-range)#Shutdown </pre>

Paso 2: Configurar el S3

En el presente paso se realiza la creación de la base de datos de VLAN a utilizar, se crean y se nombran y crean las VLAN indicadas en el desarrollo del presente escenario, VLAN 22 contabilidad, VLAN 26 ingeniería, VLAN 92 administración, se realiza la asignación de las direcciones IP según la topología, se asigna como enlace troncal el puerto F0/3 para la VLAN 1 Nativa, se configuran los puertos restantes como acceso, se asigna el puerto F0/18 a la VLAN 22, por último se apagan los puertos sin utilizar.

Comandos Utilizados

Tabla 10. Configuración de Vlan en Switch 3

Dispositivo	Comandos Utilizados
Switch 3	S3>Enable S3#Configure terminal S3(config)#Vlan 22 S3(config-vlan)#Name CONTABILIDAD S3(config-vlan)#Vlan 26 S3(config-vlan)#Name INGENIERIA S3(config-vlan)#Vlan 92 S3(config-vlan)#Name ADMINISTRATIVA S3(config-vlan)#Exit S3(config)#interface vlan 92 S3(config-if)#Ip address 192.168.92.3 255.255.255.0 S3(config-if)#Ip default-gateway

	<pre> 192.168.92.1 S3(config-if)#Interface f0/3 S3(config-if)#Switchport mode trunk S3(config-if)#Swichport native vlan1 S3(config-if)#Interface f0/5 S3(config-if)#Swichpoirt mode trunk S3(config-if)#Swichport native vlan1 S3(config-if)#Exit S3(config)#Interface range fa0/1-2, fa0/4-24 S3(config-if-range)#Switchport mode Access S3(config-if-range)#Exit S3(config)#Interface fa0/18 S3(config-if)#Switichport mode Access vlan 26 S3(config-if)#Interface range fa0/1-2, fa0/4-17, fa0/19-24 S3(config-if-range)#Shutdown </pre>
--	---

Paso 3: Configurar R1

En el presente paso se realiza la configuración de las subinterfaces del puerto gigabit ethernet 0/1, se asignan las vlan a las diferentes subinterfaces creadas con el número de VLAN correspondiente Subinterfaz 802.1Q.22 Vlan de contabilidad se le asigna la dirección IP disponible, Subinterfaz 802.1Q.26 Vlan de ingeniería se le asigna la dirección IP disponible, Subinterfaz 802.1Q.92 Vlan de administración se le asigna la dirección IP disponible, se activa la interfaz Gigabit ethernet 0/1.

Configuración realizada

Tabla 11. Configuración de subinterfaces en Router 1

Dispositivo	Comandos Utilizados
Router 1	R1>Enable R1#Configure terminal R1(config)#Interface fa0/0.22 R1(config-subif)#Description LAN DE CONTABILIDAD R1(config-subif)#Encapsulation dot1Q 22 R1(config-subif)#Ip address 192.168.22.1 255.255.255.0 R1(config-subif)#Interface fa0/0.26 R1(config-subif)#Description LAN DE INGENIERIA R1(config-subif)#Encapsulation dot1Q 26 R1(config-subif)#Ip address 192.168.26.1 255.255.255.0 R1(config-subif)#Interface fa0/0.99 R1(config-subif)#Description LAN DE ADMINISTRACIÓN R1(config-subif)#Encapsulation dot1Q 92 R1(config-subif)#Ip address 192.168.92.1 255.255.25 R1(config-subif)#Exit R1(config)#Interface g0/0

	R1(config-if)#No shutdown
--	---------------------------

Paso 4: Verificar la conectividad de la red

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

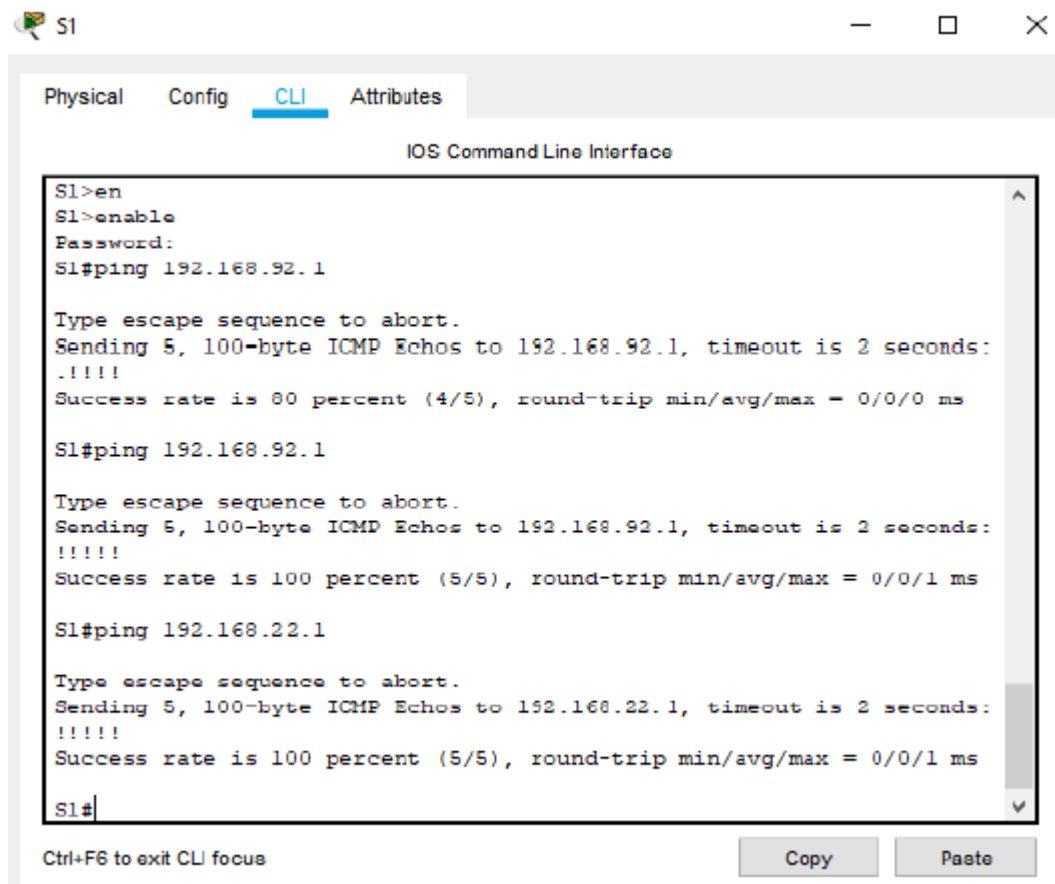
Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 12. Verificar Segunda Conectividad

Desde	A	Dirección IP	Resultado de Ping
S1	R1, dirección VLAN 99	192.168.92.1	Satisfactorio
S3	R1, dirección VLAN 99	192.168.92.1	Satisfactorio
S1	R1, dirección VLAN 21	192.168.22.1	Satisfactorio
S3	R1, dirección VLAN 23	192.168.26.1	Satisfactorio

En el presente paso se verifica la conectividad desde los Switch 1 y 3 a las direcciones ip de las subinterfaces del Router 1, se puede observar que existe conectividad en todas las subinterfaces, donde se evidencia la creación adecuada de las VLAN utilizadas en el desarrollo del presente ejercicio.

Ilustración 3. Verificar conectividad3



```
S1
Physical Config CLI Attributes
IOS Command Line Interface
S1>en
S1>enable
Password:
S1#ping 192.168.92.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.92.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

S1#ping 192.168.92.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.92.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

S1#ping 192.168.22.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.22.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

S1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Parte 4: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

En el presente paso se realiza la configuración del protocolo de enrutamiento RIP versión 2, se anuncian las redes directamente conectadas, se establecen todas las interfaces utilizadas para las redes LAN, se establecen las interfaces como pasivas, se desactiva la sumarización automática, ya en este momento la aplicación del protocolo de enrutamiento es fundamental para la conectividad de los elementos empleados en el ejercicio, se realiza la aplicación del protocolo dinámico RIPv2, se configura en cada uno de los router a vincular.

Configuración realizada

Tabla 13. Configuración Protocolo RIP en Router 1

Dispositivo	Comandos Utilizados
Router 1	R1>enable R1#Configure terminal R1(config)#Router rip R1(config-router)#Versión 2 R1(config-router)#do show ip route connected R1(config-router)#network 177.17.1.0 R1(config-router)#network 192.168.22.0 R1(config-router)#network 192.168.26.0 R1(config-router)#network 192.168.92.0 R1(config-router)#passive-interface g0/0.22 R1(config-router)#passive-interface g0/0.26 R1(config-router)#passive-interface g0/0.92 R1(config-router)#no auto-summary

Paso 2: Configurar RIPv2 en el R2

En el presente paso se realiza la configuración del protocolo de enrutamiento RIP versión 2, se anuncian las redes directamente conectadas a excepción de la red Gigabit Ethernet 0/0, se establecen todas las interfaces utilizadas para las redes LAN, se establecen las interfases como pasivas, se desactiva la sumarización automática, ya en este momento la aplicación del protocolo de enrutamiento es fundamental para la conectividad de los elementos empleados en el ejercicio.

Configuración realizada

Tabla 14. Configuración Protocolo RIP en Router 2

Dispositivo	Comandos Utilizados
Router 2	R2>enable R2#Configure terminal R2(config)#Router rip R2(config-router)#Versión 2 R2(config-router)#do show ip route connected R2(config-router)#network 10.10.10.10 R2(config-router)#network 177.17.1.0 R2(config-router)#network 177.17.26.0 R2(config-router)#passive-interface loopback 0 R2(config-router)#no auto-summary

Paso 3: Configurar RIPv2 en el R3

En el presente paso se realiza la configuración del protocolo de enrutamiento RIP versión 2, se anuncian las redes directamente conectadas a excepción de la red Gigabit Ethernet 0/0, se establecen todas las interfaces utilizadas para las redes LAN, se establecen las interfases como pasivas, se desactiva la sumarización automática, ya en este momento la aplicación del protocolo de enrutamiento es fundamental para la conectividad de los elementos empleados en el ejercicio.

Configuración realizada

Tabla 15. Configuración protocolo RIP en Router 3

Dispositivo	Comandos Utilizados
Router 3	<pre> R3>enable R3#Configure terminal R3(config)#Router rip R3(config-router)#Versión 2 R3(config-router)#do show ip route connected R3(config-router)#network 177.17.26.0 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)#end R3#show ip protocols R3#show ip route R3#show run section rip </pre>

Paso 4: Verificar la información de RIP

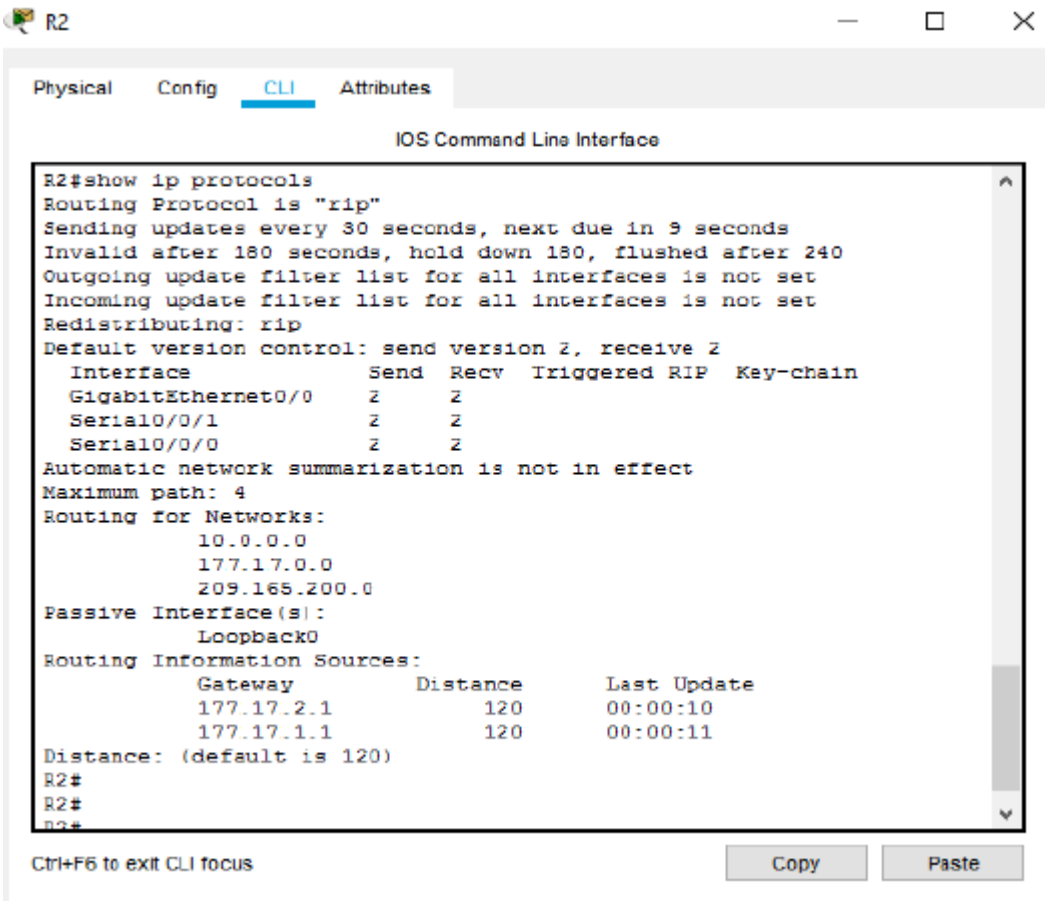
Verifique que RIP esté funcionando como se espera. Introduzca el comando de CLI adecuado para obtener la siguiente información:

Tabla 16. Verificación Protocolo 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?	Show ip protocols
¿Qué comando muestra solo las rutas RIP?	Show ip route rip
¿Qué comando muestra la sección de	Show run section rip – no funciona en

En este paso se verifica la implementación del protocolo RIP, se observan las ID de los router, las redes e interfases pasivas configuradas en el dispositivo, se observan las rutas RIP y la configuración de ejecución, en el presente paso se observa la correcta implementación del protocolo.

Ilustración 4. Verificación Protocolo RIP



Parte 5: Implementar DHCP y NAT para IPv4

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

En el presente paso se reservan las 20 primeras direcciones IP del segmento de direcciones asignadas para las VLAN 21 y 23, posteriormente en cada una de estas se realiza la creación del pool de DHCP para cada una de las VLAN.

Configuración realizada

Tabla 17. Creación Pool DHCP en Router 1

Dispositivo	Comandos Utilizados
Router 1	R1>enable R1#Configure terminal R1(config)#Ip dhcp exclude-address 192.168.21.1 192.168.22.20 R1(config)#Ip dhcp exclude-address 192.168.23.1 192.168.26.20 R1(config)#Ip dhcp pool ACCT R1(dhcp-config)#Network 192.168.22.0 255.255.255.0 R1(dhcp-config)#Dns-server 10.10.10.10 R1(dhcp-config)#Domain-name ccna- aa.com R1(dhcp-config)#Defalut router 1192.168.22.1 R1(dhcp-config)#Ip dhcp pool ENGNR R1(dhcp-config)#Network 192.168.26.0 255.255.255.0 R1(dhcp-config)#Dns-server 10.10.10.10 R1(dhcp-config)#Domain-name ccna- aa.com R1(dhcp-config)#Defalut router 1192.168.26.1

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

En el presente paso se realiza la configuración de NAT estática y dinámica en el router 2, en primera instancia se realiza la creación de una base de datos local, se procede habilitar el servicio del servidor HTTP, se configura el servidor de tal manera que pueda utilizar los datos locales para su autenticación, posteriormente se crea la NAT estática en el servidor web, se asignan las interfaces interna y externa a la NAT, se realiza la configuración de NAT dinámica en un ACL privada, se define el pool de direcciones IP utilizables y para finalizar se define la traducción de NAT dinámica.

Configuración realizada

Tabla 18. Configuración NAT en Router 2

Dispositivo	Comandos Utilizados
Router 2	R2>enable R2#Configure terminal R2(config)#Username Webuser privilege 15 secret cisco12345 R2(config)#Ip http server R2(config)#Ip http authentication local R2(config)#ip nat inside source static 10.10.10.10 209.165.200.234 R2(config)#Interface loopback 0 R2(config-if)#Ip nat inside R2(config-if)#Interface g0/0 R2(config-if)#Ip nat outside R2(config-if)#Exit R2(config)#Access-list 1 permit 192.168.22.0 0.0.0.255 R2(config)#Access-list 1 permit 192.168.26.0 0.0.0.255 R2(config)#Ip nat pool INTERNET 209.165.200.235 209.165.200.237 R2(config)#Netmask 255.255.255.248 R2(config)#Ip nat inside source list 1

	pool INTERNET
--	---------------

<

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.

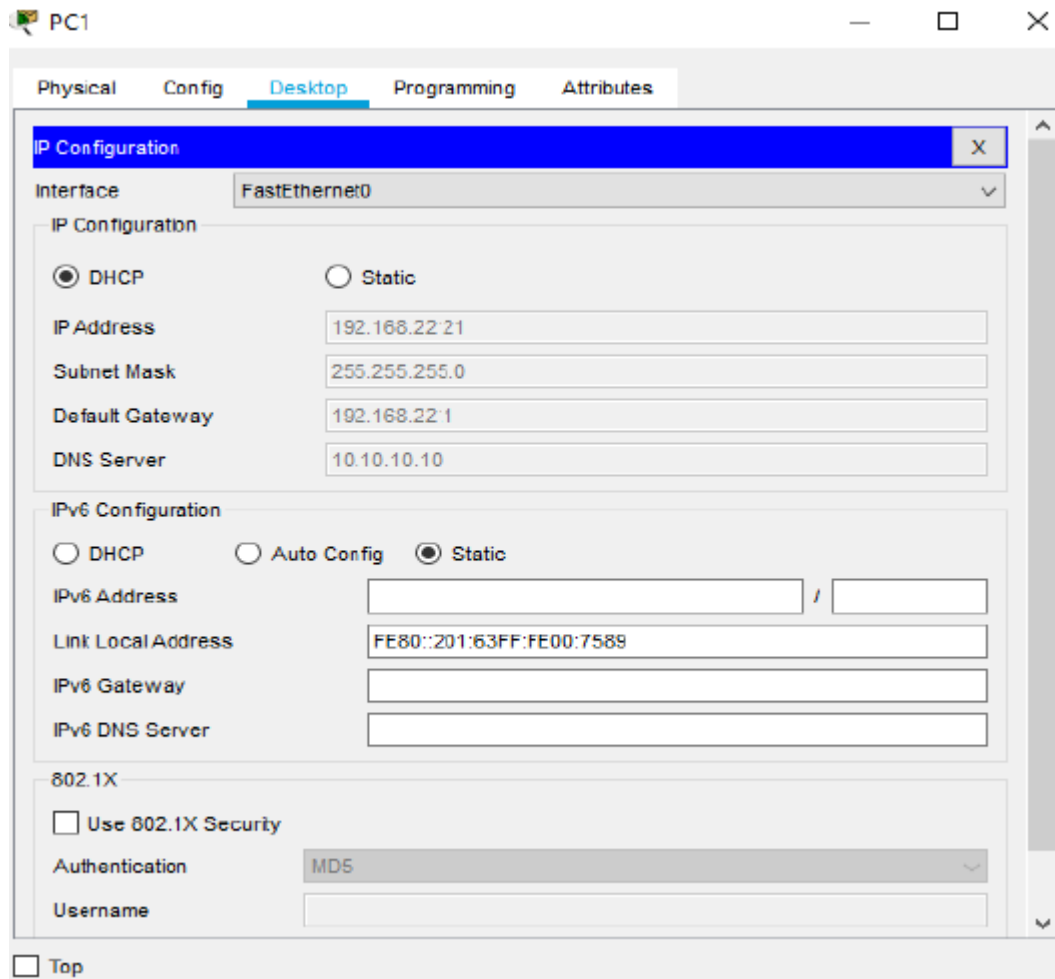
Tabla 19. Verificación protocolo DHCP y NAT

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Direccionamiento automático
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Direccionamiento automático
Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Respuesta satisfactoria
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.234) Iniciar sesión con el nombre de usuario webuser y la contraseña cisco12345	No soportado por packet tracer

Se verifica la información IP del servidor DHCP en cada uno de los hosts, se verifica la respuesta de cada uno de estos, se verifica el servicio WEB ingresando a la dirección global del servidor WEB.

En el presente paso se puede observar como el router inicia su función como servidor DHCP, se puede comprobar en los equipos de cómputo, teniendo en cuenta que cada uno de estos obtiene su dirección IP de manera automática, como se puede evidenciar en la siguiente ilustración.

Ilustración 5. Verificación Protocolo DHCP



Parte 6: Configurar NTP

En el presente paso se ajusta la fecha y hora en el router 2, se procede a establecer a este como router maestro NTP, se configura al router 1 como cliente NTP, se configuran las actualizaciones de calendarios periódicos con hora NTP en router 1, por último, se verifica la configuración NTP en R1.

Configuración realizada

Dispositivo	Comandos Utilizados
Router 1	R2(config)#Clock set 10:00:00 march 20 2021 R2(config)#Ntp master 5
Router 2	R1(config)#Ntp server 177.17.1.2 ntp update-calendar R1(config)#Exit R1#Show ntp associations

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

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

En el presente paso, se realiza la configuración de las listas de control de acceso, se nombra una ACL que solo establezca una conexión telnet entre R1 y R2, se aplica la ACL con nombre para las líneas VTY, por último, se verifica su funcionamiento.

Configuración realizada

Dispositivo	Comandos Utilizados
Router 1	R1(config)#Telenet 177.17.1.2
Router 2	R2(config)#Ip Access-list standard ADMIN-MGT R2(config-std-nacl)#Permit host 177.17.1.1 R2(config-std-nacl)#Line vty 0 15

	R2(config-line)#Access-list ADMIN-MGT in R2(config-line)#Transport input telnet
--	--

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

Tabla 20. Verificar NAT.

Descripción del Comando	Entrada del Estudiante
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Show access-lists
Restablecer los contadores de una lista de acceso	Clear Access-list
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	Show ip interface #Nombre interfaz#
¿Con qué comando se muestran las traducciones NAT?	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. Show ip nat trans
¿Qué comando se utiliza para eliminar	No ip nat inside source list #Nombre

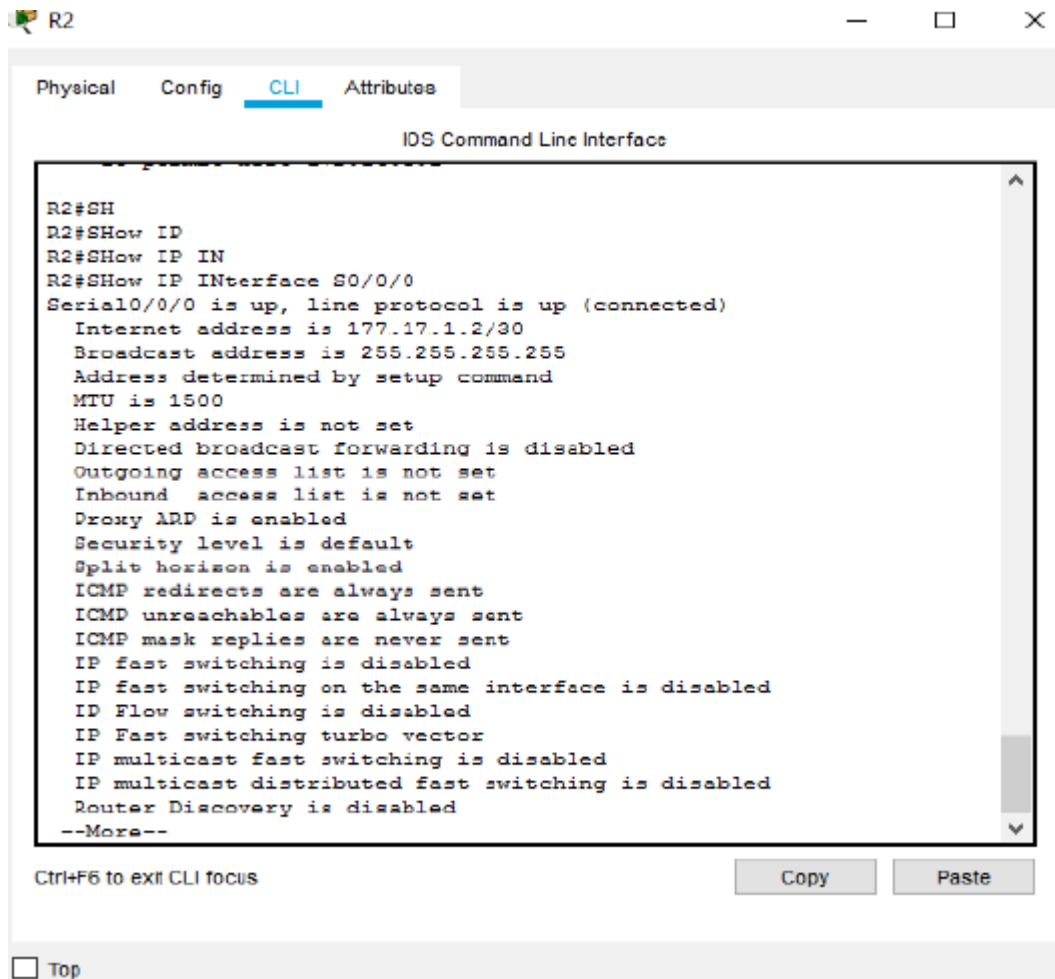
las traducciones de NAT dinámicas?	lista#
------------------------------------	--------

En el presente paso, se verifican las coincidencias recibidas por la ACL desde la última vez que se restableció, se realiza el restablecimiento de la ACL, en seguida se verifica la ACL aplicada a una interfaz junto a su dirección IP, de igual manera se verifican las traducciones NAT y para finalizar se procede a practicar el cómo se eliminan las direcciones NAT dinámicas.

Configuración realizada

Dispositivo	Comandos Utilizados
Router 2	R2#Show Access-list R2(config)#Clear Access-list R2(config)#exit R2#Show ip interface S0/0/0 R2#Show ip nat trans R2#Configure terminal R2(config)#No ip nat inside source list #

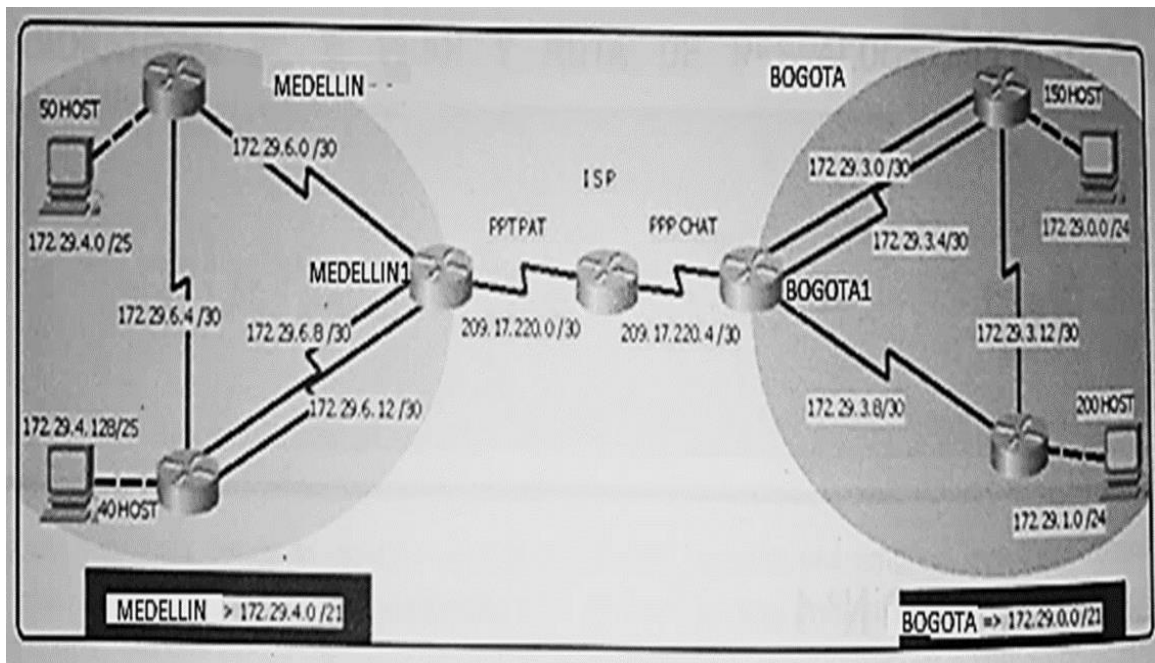
Ilustración 6. Verificar Interfaz



4. ESCENARIO 2

Escenario: 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.

Ilustración 7. Topología planteada escenario 2



Direccionamiento IP escenario 1

EQUIPO	CONEXIÓN	DIRECCION IP
Router ISP s0/1/1	Bogotá 1	209.17.220.4
Router ISP s0/1/0	Medellin1	209.17.220.0
Bogotá 1 s0/0/1	Bogota2	172.29.3.8
Bogotá 1 s0/1/0	Bogota3	172.29.3.0
Bogotá 1 s0/0/1	Bogota3	179.29.3.4
Bogotá 1 s0/0/1	ISP	209.17.220.4
Bogotá 2 s0/0/0	Bogota3	172.29.3.12
Bogotá 2 s0/0/1	Bogotá 1	172.29.3.8
Bogotá 3 s0/0/0	Bogotá 1	179.29.3.4
Bogotá 3 s0/1/0	Bogotá 1	172.29.3.0
Medellín 1 s0/0/0	Medellín 3	172.29.6.8/30
Medellín 1 s0/0/1	Medellin2	172.29.6.0/30
Medellín 1 s0/1/1	Medellin3	192.29.6.12/30
Medellín 1 s0/1/0	ISP	209.17.220.0/30
Medellín 2 s0/0/0	Medellin1	172.29.6.0/30
Medellín 2 s0/0/1	Medellin3	172.29.6.4/30
Medellín 3 s0/0/0	medellin1	172.29.6.8/30
Medellín 3 s0/0/1	Medellin2	172.29.6.4/30
Medellín 3 s0/1/1	Medellin1	192.29.6.12/30

Paso 1. Se realiza la topología de la red con la conexión de los seriales y los diferentes equipos, luego se reinician los dispositivos con el comando `erase startup-config` y `reload` para proceder con la configuración.

```
Router>enable
```

```
Router#erase startup-config
```

Router#reload

Paso 2. Configuración básica en cada uno de los equipos de la red como es el nombre, claves de acceso, encriptación de contraseñas y mensaje de acceso no autorizado

Configuración del R1 Medellín 1

Router>enable

Router#configure terminal

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

Router(config)#hostname Medellin1

Medellin1(config)#enable secret class

Medellin1(config)#no ip domain-lookup

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 #Solo personas autorizadas#

Configuración del R2 Medellín 2

Router>enable

Router#configure terminal

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

Router(config)#hostname Medellin2

Medellin2(config)#no ip domain-lookup

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 #Solo personas autorizadas#
Configuración de R3 Medellín 3
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Medellin3
Medellin3(config)#no ip domain-lookup
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-encryption
Medellin3(config)#banner motd #Solo personas autorizadas#
Configuración de R4 Bogotá 1
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Bogota1
Bogota1(config)#no ip domain-lookup
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 #Solo personas autorizadas#
Configuración de R4 Bogotá 2
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Bogota2
Bogota2(config)#no ip domain-lookup
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 #Solo personas autorizadas#
Configuración de Router Bogota 3
Router(config)#hostname Bogota3
Bogota3(config)#no ip domain-lookup
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 #Solo personas autorizadas#
Configuración de ISP
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#no ip domain-lookup
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 #Solo personas autorizadas#
```

Paso 3. Configuración del direccionamiento IP y la activación de interfaces de la topología para realizar las respectivas conexiones.

Configuración de Medellín 2 y sus conexiones

```
Medellin1>enable
```

```
Password:
```

```
Medellin1#configure terminal
```

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

```
Medellin1(config)#interf s0/0/0
```

```
Medellin1(config-if)#ip address 172.29.6.9 255.255.255.252
```

```
Medellin1(config-if)#clock rate 128000
```

```
Medellin1(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
```

```
Medellin1(config-if)#interf s0/0/1.
```

```
Medellin1(config-if)#ip address 172.29.6.1 255.255.255.252
```

```
Medellin1(config-if)#clock rate 128000
```

```
Medellin1(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
```

```
Medellin1(config-if)#int s0/0/1
```

```
Medellin1(config-if)#interface s0/1/1
```

```
Medellin1(config-if)#ip address 172.29.6.13 255.255.255.252
```

```
Medellin1(config-if)#clock rate 128000
```

```
Medellin1(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
```

```
Medellin1(config-if)#interface s0/1/0
```

```
Medellin1(config-if)#description conectio ta ISP
```

```
Medellin1(config-if)#ip address 209.17.220.1 255.255.255.252
```

```
Medellin1(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
```

```
Medellin1(config-if)#
```

Configuración de Medellín 2 y sus conexiones

```
Medellin2>enable
```

```
Password:
```

```
Medellin2#configure terminal
```

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

```
Medellin2(config)#interface s0/0/0
```

```
Medellin2(config-if)#description conectio to Medellin1
```



```

Medellin2(config-if)#ip address 172.29.6.2 255.255.255.252
Medellin2(config-if)#clock rate 128000
Medellin2(config-if)#no shutdown
Medellin2(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
Medellin2(config-if)#interface s0/0/1
Medellin2(config-if)#description conexion con Medellin3
Medellin2(config-if)#ip address 172.29.6.5 255.255.255.252
Medellin2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Medellin2(config-if)#exit
Medellin2(config)#int g0/0
Medellin2(config-if)#description conection con PC-Medellind2
Medellin2(config-if)#ip address 172.29.4.1 255.255.255.128
Medellin2(config-if)#no shtdown
Medellin2(config-if)#no shutdown
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)#
Activación de seriales y conexiones de Medellín 3
Medellin3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellin3(config)#interface s0/0/0
Medellin3(config-if)#ip address 172.29.6.10 255.255.255.252
Medellin3(config-if)#no shutdown
Medellin3(config-if)#

```

```
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
Medellin3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
Medellin3(config-if)#description conection to Medellin1
Medellin3(config-if)#interface serial0/0/1
Medellin3(config-if)#description conection con Medellin2
Medellin3(config-if)#ip address 172.29.6.6 255.255.255.252
Medellin3(config-if)#no shutdown
Medellin3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
Medellin3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state
to up
Medellin3(config-if)#interface s0/1/0
Medellin3(config-if)#description conection con Medellin1
ip address 172.29.6.14 255.255.255.252
Medellin3(config-if)#no shutdown
Medellin3(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
Medellin3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state
to up
Medellin3(config-if)#exit
Medellin3(config)#interface g0/0
Medellin3(config-if)#description Conection con PC-Medellin3
Medellin3(config-if)#ip address 172.29.4.129 255.255.255.128
Medellin3(config-if)#no shutdown
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)#
Activación de seriales y conexiones de Bogotá 1
Bogota1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota1(config)#interface s0/0/1
Bogota1(config-if)#description conection to Bogota
Bogota1(config-if)#ip address 172.29.3.9 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Bogota1(config-if)#interface s0/1/0
Bogota1(config-if)#description conection to Bogota3
Bogota1(config-if)#ip address 172.29.3.1 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
Bogota1(config-if)#interface serial 0/1/1
Bogota1(config-if)#description conection to Bogota 3
Bogota1(config-if)#ip address 172.29.3.5 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
Bogota1(config-if)#interface s0/0/0
Bogota1(config-if)#description conection to ISP
Bogota1(config-if)#ip address 209.17.220.5 255.255.255.252
Medellin2(config-if)#clock rate 128000
Bogota1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
```

```
Bogota1(config-if)#
Activación de seriales y direccionamiento en Bogotá 2
Bogota2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota2(config)#interface s0/0/0
Bogota2(config-if)#description Conection to Bogota3
Bogota2(config-if)#ip address 172.29.3.13 255.255.255.252
Bogota1(config-if)#clock rate 128000
Bogota2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Bogota2(config-if)#interface s0/0/1
Bogota2(config-if)#description Conection to Bogota1
Bogota2(config-if)#ip address 172.29.3.10 255.255.255.252
Bogota2(config-if)#no shutdown
Bogota2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
Bogota2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state
to up
Bogota2(config-if)#exit
Bogota2(config)#interface g0/0
Bogota2(config-if)#description conection Bogota2-PC
Bogota2(config-if)#ip address 172.29.1.1 255.255.255.0
Bogota2(config-if)#no shutdown
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)#
Activación de seriales y direccionamiento Bogotá 3
```

```
Bogota3>enable
Password:
Bogota3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota3(config)#interface s0/0/0
Bogota3(config-if)#description Conection to Bogota1
Bogota3(config-if)#ip address 172.29.3.14 255.255.255.252
Bogota3(config-if)#no shutdown
Bogota3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
Bogota3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
Bogota3(config-if)#interface s0/0/1
Bogota3(config-if)#description Conection to Bogota1
Bogota3(config-if)#ip address 172.29.3.6 255.255.255.252
Bogota3(config-if)#no shutdown
Bogota3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
Bogota3(config-if)#
Bogota3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota3(config)#int s0/1/0
Bogota3(config-if)#ip address 172.29.3.2 255.255.255.252
Bogota3(config-if)#no shutdown
Bogota3(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state
to up
Bogota3(config-if)#exit
```

```

Bogota3(config)#interface g0/0
Bogota3(config-if)#description Conection to PC-Bogota3
Bogota3(config-if)#ip address 172.29.0.1 255.255.255.0
Bogota3(config-if)#no shutdown
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)#
Activación de seriales en ISP
ISP>enable
Password:
ISP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#interface s0/1/1
ISP(config-if)#description Conection to Bogota1
ISP(config-if)# 209.17.220.6 255.255.255.252
ISP(config-if)#no shutdown
ISP(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to up
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state
to up
ISP(config-if)#interface s0/1/0
ISP(config-if)#description Conection to Medellin1
ISP(config-if)#ip address 209.17.220.2 255.255.255.252
ISP(config-if)#no shutdown
ISP(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
ISP(config-if)#

```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

ISP(config-if)#

PARTE 1: CONFIGURACIÓN DEL ENRUTAMIENTO

a. Configuración del enrutamiento de la red usando el protocolo RIP versión 2, con la declaración de la red principal y la desactivación de la sumarización automática.

Paso 1. Se declara RIP versión 2 en cada uno de los router, la red principal y por último se desactiva la sumarización automática.

Medellin 1

Medellin1(config)#router rip

Medellin1(config-router)#version 2

Medellin1(config-router)#network 172.29.0.0

Medellin1(config-router)#no auto-summary

RIP Medellin 2

Medellin2(config)#router rip

Medellin2(config-router)#version 2

Medellin2(config-router)#network 172.29.0.0

Medellin2(config-router)#no auto-summary

RIP Medellin 3

Medellin3(config)#router rip

Medellin3(config-router)#version 2

Medellin3(config-router)#network 172.29.0.0

Medellin3(config-router)#no auto-summary

RIP Bogota 1

Bogota1(config)#router rip

Bogota1(config-router)#version 2

Bogota1(config-router)#network 172.29.0.0

Bogota1(config-router)#no auto-summary

RIP Bogota 2

Bogota2(config)#router rip

```
Bogota2(config-router)#version 2
Bogota2(config-router)#network 172.29.0.0
Bogota2(config-router)#no auto-summary
RIP Bogota 3
Bogota3(config)#router rip
Bogota3(config-router)#version 2
Bogota3(config-router)#network 172.29.0.0
Bogota3(config-router)#no auto-summary
```

b. 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 RIP.

Paso 1. Se Configura la ruta por defecto de Medellín 1 y Bogotá 1, por último se termina con el comando de redistribución.

Configuración Medellín 1

```
Medellin1#configure terminal
```

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

```
Medellin1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.2
```

```
Medellin1(config-router)#redistribute static
```

Configuración Bogotá 1

```
Bogota1#confi terminal
```

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

```
Bogota1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.6
```

```
Bogota1 (config-router)#redistribute static
```

c. El router ISP debe 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.

Paso 1. Se sumarizan las Redes Medellín 1 y Bogotá 1 sumando todas sus redes internas a /22, para ello realizamos el cálculo de conversión a binario y sumamos.

```
Suma Medellín 172.29.4.0/22 255.255.252.0
```


Tabla 21. Sumarizacion Medellín 1

Conversión de binario a decimal				Dirección IP
10101100	11101	110	100	172.29.6.4/30
10101100	11101	110	0	172.29.6.0/30
10101100	11101	110	1000	172.29.6.8/30
10101100	11101	110	1100	172.29.6.12/30
10101100	11101	100	0	172.29.4.0/25
10101100	11101	100	10000000	172.29.4.128/25
10101100	11101	100	0	Sumarización
172	29	4	0	IP Sumarizada

Tabla 22. Sumarizacion IP Bogotá 1

Suma Bogotá: 172.29.0.0 255/22255.252.0

Conversión de hexadecimal a binario				Dirección IP
10101100	11101	11	1100	172.29.3.12/30
10101100	11101	11	0	172.29.3.0/30
10101100	11101	11	1000	172.29.3.8/30
10101100	11101	11	100	172.29.3.4/30
10101100	11101	0	0	172.29.0.0/25
10101100	11101	1	0	172.29.1.0/25
10101100	11101	0	0	Sumarización
172	29	0	0	IP Sumarizada

Paso 2. Se configura las rutas estáticas en ISP

ISP>enable

Password:

ISP#configure terminal

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

ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.1

ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.5

PARTE 2: TABLA DE ENRUTAMIENTO

Paso 1. Ejecución del comando show ip route para visualizar la tabla de enrutamiento de Medellín 2 la cual se describe teniendo en cuenta la Figura 3 y las demás figuras de los demás router que se presentan más adelante.

Descripción de Medellín 1 vista en la Figura 3

L: Describe aquellas redes Locales

172.29.6.1/32 conectada al s0/0/1, 172.29.6.9/32 conectada al s0/0/0,

172.29.6.13/32 conectada al s0/1/1

C: Aquellas redes que se encuentran conectadas

172.29.6.0/30 conectada al s0/0/1, 172.29.6.8/30 conectada a s0/0/0,

172.29.6.12/30 conectada a s0/1/1, 209.17.220.0/30 conectada a s0/1/0

209.17.220.1/32 conectada a s0/1/0, 209.17.220.1/32 conectada a s0/1/0

S: Es la red estática: 0.0.0.0/1[0] vía 209.17.220.2

R: son asignadas por ISP y tienen diferentes caminos para llegar a él, se tiene el ejemplo en la Figura 3 R 172.29.6.4/30 los caminos por los seriales 0/0/1 y s0/1/1

Ilustración 8. Tabla de router Medellín 1

```
Medellin1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.17.220.2 to network 0.0.0.0

     172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R       172.29.4.0/25 [120/1] via 172.29.6.2, 00:00:12, Serial0/0/1
R       172.29.4.128/25 [120/1] via 172.29.6.10, 00:00:09, Serial0/0/0
         [120/1] via 172.29.6.14, 00:00:09, Serial0/1/1
C       172.29.6.0/30 is directly connected, Serial0/0/1
L       172.29.6.1/32 is directly connected, Serial0/0/1
R       172.29.6.4/30 [120/1] via 172.29.6.2, 00:00:12, Serial0/0/1
         [120/1] via 172.29.6.14, 00:00:09, Serial0/1/1
C       172.29.6.8/30 is directly connected, Serial0/0/0
L       172.29.6.9/32 is directly connected, Serial0/0/0
C       172.29.6.12/30 is directly connected, Serial0/1/1
L       172.29.6.13/32 is directly connected, Serial0/1/1
     209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/1/0
C       209.17.220.1/32 is directly connected, Serial0/1/0
C       209.17.220.2/32 is directly connected, Serial0/1/0
S*     0.0.0.0/0 [1/0] via 209.17.220.2
```

Paso 2. se analiza en todos los router la tabla de enrutamiento teniendo en cuenta la información detallada del Paso 1 descrito anteriormente.

```

Medellin 2
Physical Config CLI Attributes
IOS Command Line Interface
Password:
Password:
Medellin2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
        area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is 172.29.6.1 to network 0.0.0.0

    172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
C       172.29.4.0/25 is directly connected, GigabitEthernet0/0
L       172.29.4.1/32 is directly connected, GigabitEthernet0/0
R       172.29.4.128/25 [120/1] via 172.29.6.6, 00:00:20, Serial0/0/1
C       172.29.6.0/30 is directly connected, Serial0/0/0
L       172.29.6.2/32 is directly connected, Serial0/0/0
C       172.29.6.4/30 is directly connected, Serial0/0/1
L       172.29.6.5/32 is directly connected, Serial0/0/1
R       172.29.6.8/30 [120/1] via 172.29.6.1, 00:00:01, Serial0/0/0
        [120/1] via 172.29.6.6, 00:00:20, Serial0/0/1
R       172.29.6.12/30 [120/1] via 172.29.6.1, 00:00:01, Serial0/0/0
        [120/1] via 172.29.6.6, 00:00:20, Serial0/0/1
R*      0.0.0.0/0 [120/1] via 172.29.6.1, 00:00:01, Serial0/0/0
  
```

Ctrl+F6 to exit CLI focus

Copy Paste

Ilustración 9. Tabla de router Medellín 3

```

Medellin 3
Physical Config CLI Attributes
IOS Command Line Interface
Medellin3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
        inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is 172.29.6.9 to network 0.0.0.0

    172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
R       172.29.4.0/25 [120/1] via 172.29.6.5, 00:00:06, Serial0/0/1
C       172.29.4.128/25 is directly connected, GigabitEthernet0/0
L       172.29.4.129/32 is directly connected, GigabitEthernet0/0
R       172.29.6.0/30 [120/1] via 172.29.6.5, 00:00:06, Serial0/0/1
        [120/1] via 172.29.6.9, 00:00:22, Serial0/0/0
C       172.29.6.4/30 is directly connected, Serial0/0/1
L       172.29.6.6/32 is directly connected, Serial0/0/1
C       172.29.6.8/30 is directly connected, Serial0/0/0
L       172.29.6.10/32 is directly connected, Serial0/0/0
C       172.29.6.12/30 is directly connected, Serial0/1/0
L       172.29.6.14/32 is directly connected, Serial0/1/0
R*      0.0.0.0/0 [120/1] via 172.29.6.9, 00:00:22, Serial0/0/0
  
```

Ctrl+F6 to exit CLI focus

Copy Paste

Ilustración 10. Tabla de router ISP

```

ISP#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.17.220.0 to network 0.0.0.0

   172.29.0.0/16 is variably subnetted, 4 subnets, 2 masks
S       172.29.0.0/22 [1/0] via 209.17.220.5
S       172.29.0.0/24 [1/0] via 209.17.220.6
S       172.29.4.0/22 [1/0] via 209.17.220.1
S       172.29.4.0/24 [1/0] via 209.17.220.2
   209.17.220.0/24 is variably subnetted, 5 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/1/0
L       209.17.220.2/32 is directly connected, Serial0/1/0
C       209.17.220.4/30 is directly connected, Serial0/1/1
C       209.17.220.5/32 is directly connected, Serial0/1/1
L       209.17.220.6/32 is directly connected, Serial0/1/1
S*     0.0.0.0/0 [1/0] via 209.17.220.0
    
```

Ctrl+F6 to exit CLI focus

Copy Paste

Ilustración 11. Tabla de router Bogotá 1

```

Bogota1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.17.220.6 to network 0.0.0.0

   172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R       172.29.0.0/24 [120/1] via 172.29.3.6, 00:00:19, Serial0/1/1
R       172.29.1.0/24 [120/2] via 172.29.3.6, 00:00:19, Serial0/1/1
C       172.29.3.0/30 is directly connected, Serial0/1/0
L       172.29.3.1/32 is directly connected, Serial0/1/0
C       172.29.3.4/30 is directly connected, Serial0/1/1
L       172.29.3.5/32 is directly connected, Serial0/1/1
C       172.29.3.8/30 is directly connected, Serial0/0/1
L       172.29.3.9/32 is directly connected, Serial0/0/1
R       172.29.3.12/30 [120/1] via 172.29.3.6, 00:00:19, Serial0/1/1
   209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.17.220.4/30 is directly connected, Serial0/0/0
L       209.17.220.5/32 is directly connected, Serial0/0/0
S*     0.0.0.0/0 [1/0] via 209.17.220.6
           [1/0] via 209.17.220.5
    
```

Ctrl+F6 to exit CLI focus

Copy Paste

Ilustración 12. Tabla de router Bogotá 2

```

Bogota2#enable
Password:
Bogota2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

      172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R       172.29.0.0/24 [120/1] via 172.29.3.14, 00:00:20, Serial0/0/0
C       172.29.1.0/24 is directly connected, GigabitEthernet0/0
L       172.29.1.1/32 is directly connected, GigabitEthernet0/0
R       172.29.3.0/30 [120/1] via 172.29.3.9, 00:00:23, Serial0/0/1
        [120/1] via 172.29.3.14, 00:00:20, Serial0/0/0
R       172.29.3.4/30 [120/1] via 172.29.3.9, 00:00:23, Serial0/0/1
        [120/1] via 172.29.3.14, 00:00:20, Serial0/0/0
C       172.29.3.8/30 is directly connected, Serial0/0/1
L       172.29.3.10/32 is directly connected, Serial0/0/1
C       172.29.3.12/30 is directly connected, Serial0/0/0
L       172.29.3.13/32 is directly connected, Serial0/0/0

Bogota2#
    
```

Ilustración 13. Tabla de router Bogotá 3

```

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.29.3.5 to network 0.0.0.0

      172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
C       172.29.0.0/24 is directly connected, GigabitEthernet0/0
L       172.29.0.1/32 is directly connected, GigabitEthernet0/0
R       172.29.1.0/24 [120/1] via 172.29.3.13, 00:00:14, Serial0/0/0
C       172.29.3.0/30 is directly connected, Serial0/1/0
L       172.29.3.2/32 is directly connected, Serial0/1/0
C       172.29.3.4/30 is directly connected, Serial0/0/1
L       172.29.3.6/32 is directly connected, Serial0/0/1
R       172.29.3.8/30 [120/1] via 172.29.3.5, 00:00:10, Serial0/0/1
        [120/1] via 172.29.3.13, 00:00:14, Serial0/0/0
        [120/1] via 172.29.3.1, 00:00:10, Serial0/1/0
C       172.29.3.12/30 is directly connected, Serial0/0/0
L       172.29.3.14/32 is directly connected, Serial0/0/0
R*    0.0.0.0/0 [120/1] via 172.29.3.5, 00:00:10, Serial0/0/1
        [120/1] via 172.29.3.1, 00:00:10, Serial0/1/0

Bogota3#
    
```

b. Verificar el balanceo de carga que presentan los routers

El balanceo se observa en cada una de las figuras que fueron aplicadas anteriormente con el comando show ip route

En la Ilustración 13. Tabla de router Bogotá 3 el balanceo se observa debido a que tiene diferentes rutas, por ejemplo, las IP que tienen vías por diferentes seriales no poseen equilibrio de carga por lo tanto existe balanceo.

c. Obsérvese en los routers Bogotá1 y Medellín1 tienen cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.

En la tabla de enrutamiento de Medellín 1 y Bogotá 1 en la ejecución del comando show ip route se observa varias semejanzas debido a que utiliza una ruta estática que conecta a las redes internas como el router Bogotá 1 que tiene a Bogotá 2 y 3 como redes internas y Medellín 1 que tiene a Medellín 2 y 3 como redes internas

Ruta Medellin1: 0.0.0.0/0[1/0] vía 209.17.22.2

Ruta Bogota1: 0.0.0.0/0 [1/0] vía 209.17.220.6

d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante RIP.

El router Bogotá 2 posee varias redes que se obtiene con RIP lo cual significa que puede haber comunicación con otras redes, para analizar entramos a la tabla de router con el comando show ip router el cual se generó anteriormente.

R* 0.0.0.0/0 [120/1] vía 172.29.3.9, 00:00:15, Serial0/0/1

172.29.3.4/30 [120/1] vía 172.29.3.9, 00:00:15, Serial0/0/1

Redes por medio de RIP Medellín 2

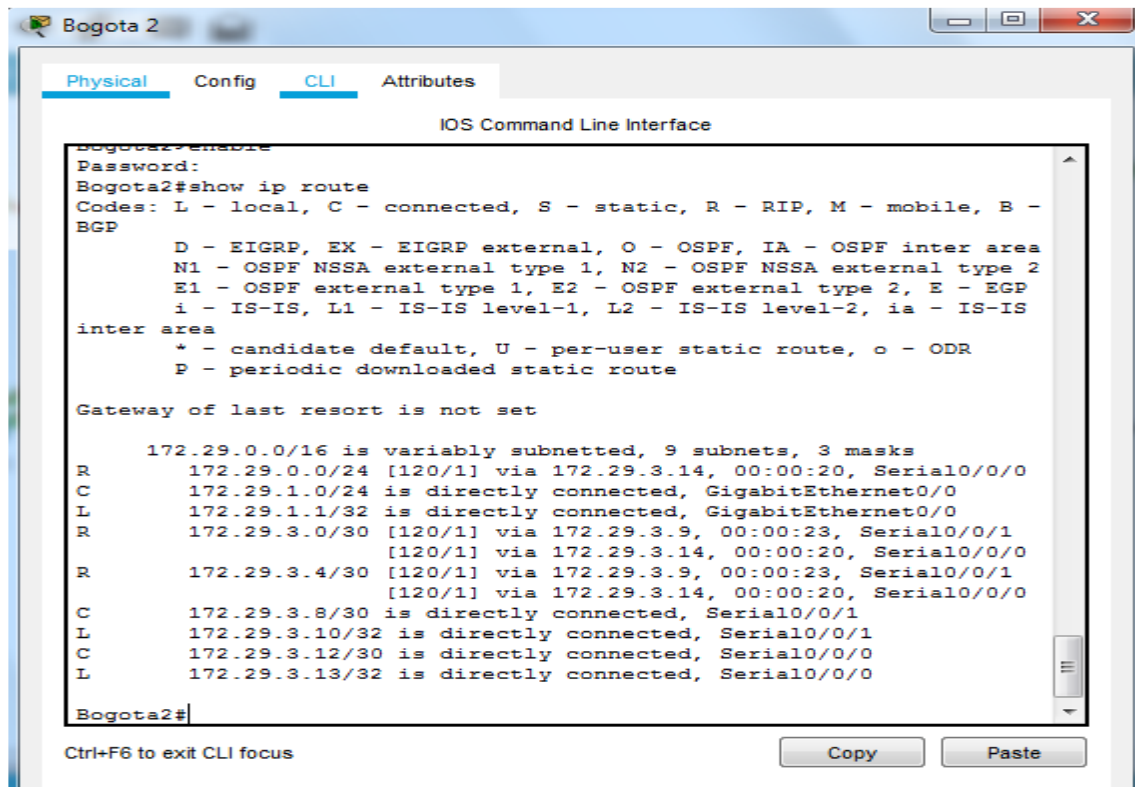
R 172.29.4.0/25 [120/1] vía 172.29.6.2, 00:00:25, Serial0/0/1

R 172.29.4.128/25 [120/1] vía 172.29.6.10, 00:00:07,

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

Se verifica las redes redundantes con la letra R las cuales conectan varias redes

Ilustración 14. Redes redundantes en Bogotá 2



Se indican las redes redundantes que conecta a un puerto dos veces descritas con letras R y que tienen comunicación por diferentes seriales.

f. El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

Ilustración 15. Rutas estáticas ISP

```
ISP
Physical Config CLI Attributes
IOS Command Line Interface
%SYS-S-CONFIG_1: Configured from console by console

ISP#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.17.220.0 to network 0.0.0.0

      209.17.220.0/24 is variably subnetted, 4 subnets, 2 masks
C       209.17.220.0/30 is directly connected, Serial0/1/0
L       209.17.220.2/32 is directly connected, Serial0/1/0
C       209.17.220.4/30 is directly connected, Serial0/1/1
L       209.17.220.6/32 is directly connected, Serial0/1/1
S*    0.0.0.0/0 [1/0] via 209.17.220.0

ISP#
```

Vemos que en la ilustración 12. Tabla de router ISP presenta su ruta estática y a las cuales conectan y se describen con la letra C. las rutas utilizan diferente dirección con sus seriales y una vía 209.17.220.0.

Rutas estáticas
209.17.220.0/30
209.17.220.4

PARTE 3: DESHABILITAR LA PROPAGACIÓN DEL PROTOCOLO RIP.

a. Para no propagar las publicaciones por interfaces que no lo requieran se debe deshabilitar la propagación del protocolo RIP, en la siguiente tabla se indican las interfaces de cada router que no necesitan desactivación.

Tabla 23. Tabla de interfaces de router

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

Desactivación de la propagación en Bogotá 2

```
Bogota2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogota2(config)#router rip
Bogota2(config-router)#version 2
Bogota2(config-router)#passive-interface s0/1/0
Bogota2(config-router)#passive-interface s0/1/1
```

Desactivación de la propagación en Bogotá 3

Bogota3#configure terminal

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

Bogota3(config)#router rip

Bogota3(config-router)#version 2

Bogota3(config-router)#passive-interface s0/1/1

Bogota3(config-router)#

Desactivación de la propagación en Medellín 2

Medellin2#configure terminal

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

Medellin2(config)#router rip

Medellin2(config-router)#version 2

Medellin2(config-router)#passive-interface s0/1/0

Medellin2(config-router)#passive-interface s0/1/1

Medellin2(config-router)#

Desactivación de la propagación en Medellín 3

Medellin3#configure terminal

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

Medellin3(config)#router rip

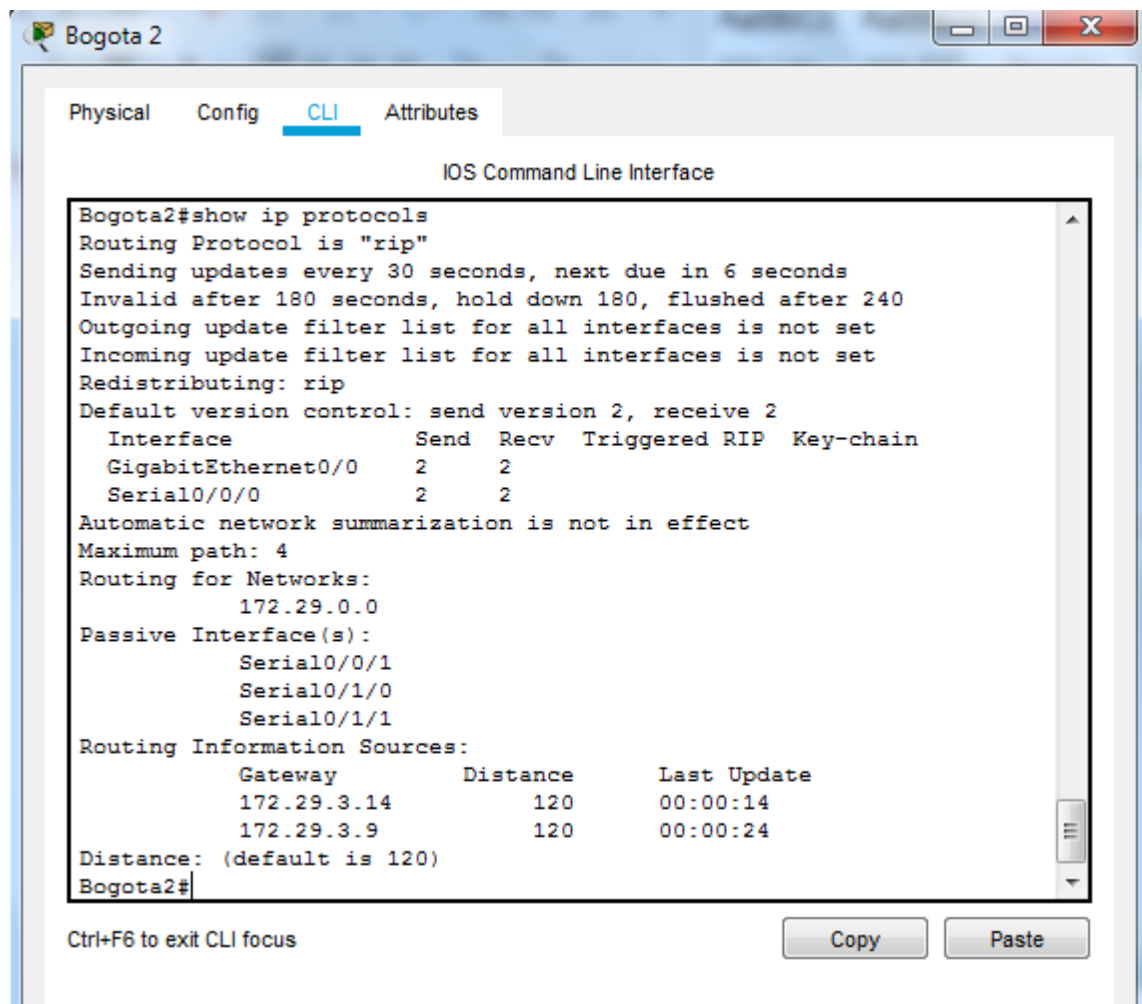
Medellin3(config-router)#version 2

Medellin3(config-router)#passive-interface s0/1/1

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

Ejecución del comando show ip protocols para analizar que las interfaces pasivas son los puertos seriales 0/0/1, 0/1/0 y 0/1/1, la versión del RIP es versión 2, también observamos unas direcciones por Gateway como es la 172.22.3.14 y la 172.29.3.9 y la distancia es de 120.

Ilustración 16. Protocolos de Bogotá 2



```
Bogota2#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 6 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
GigabitEthernet0/0   2     2
Serial0/0/0          2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
  172.29.0.0
Passive Interface(s):
  Serial0/0/1
  Serial0/1/0
  Serial0/1/1
Routing Information Sources:
  Gateway           Distance    Last Update
  172.29.3.14       120        00:00:14
  172.29.3.9        120        00:00:24
Distance: (default is 120)
Bogota2#
```

Las mismas verificaciones se realiza para Bogotá 3, Medellín 2 y Medellín 3

Ilustración 17. Protocolos de Medellín 1

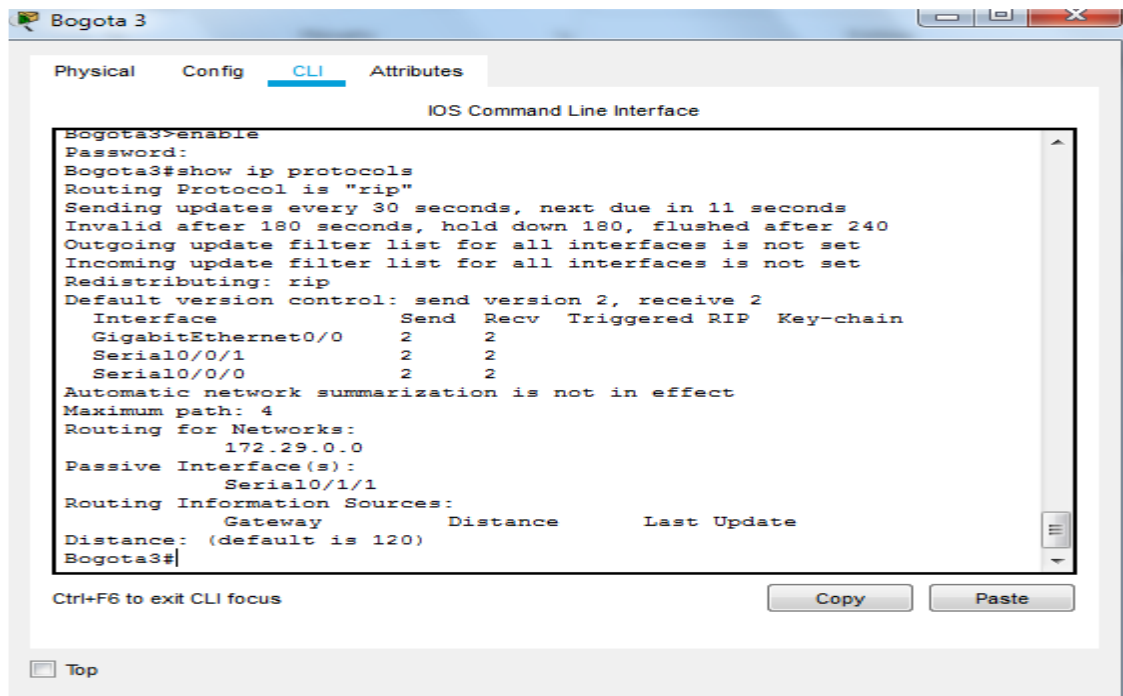


Ilustración 18. Protocolos de Medellín 2

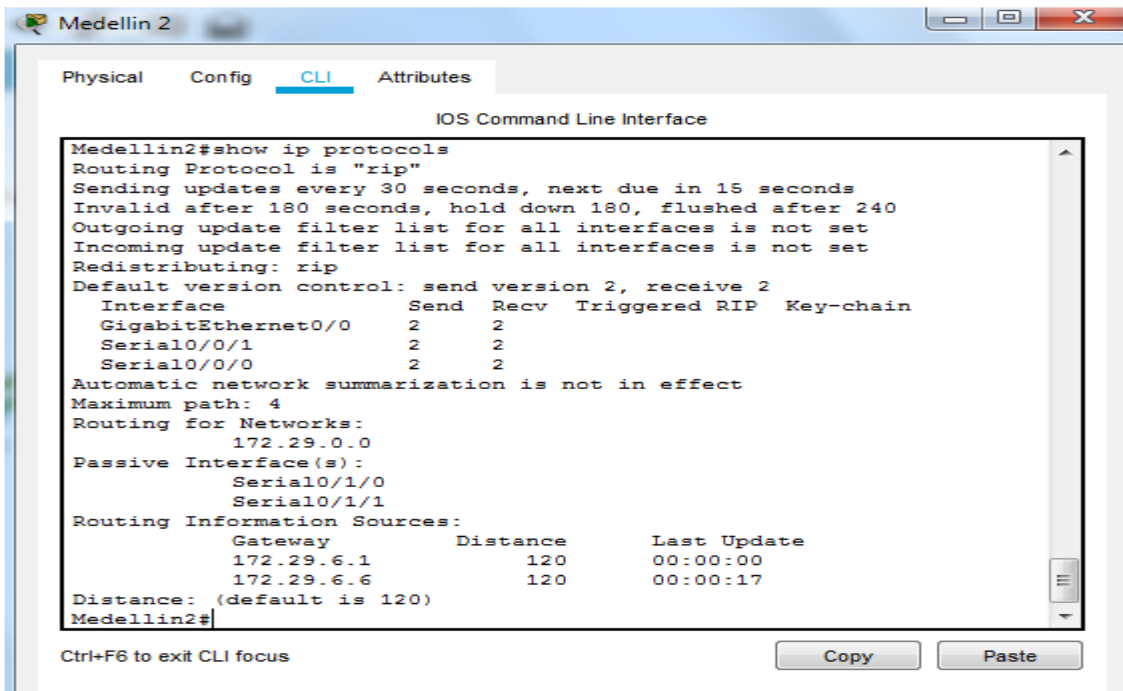
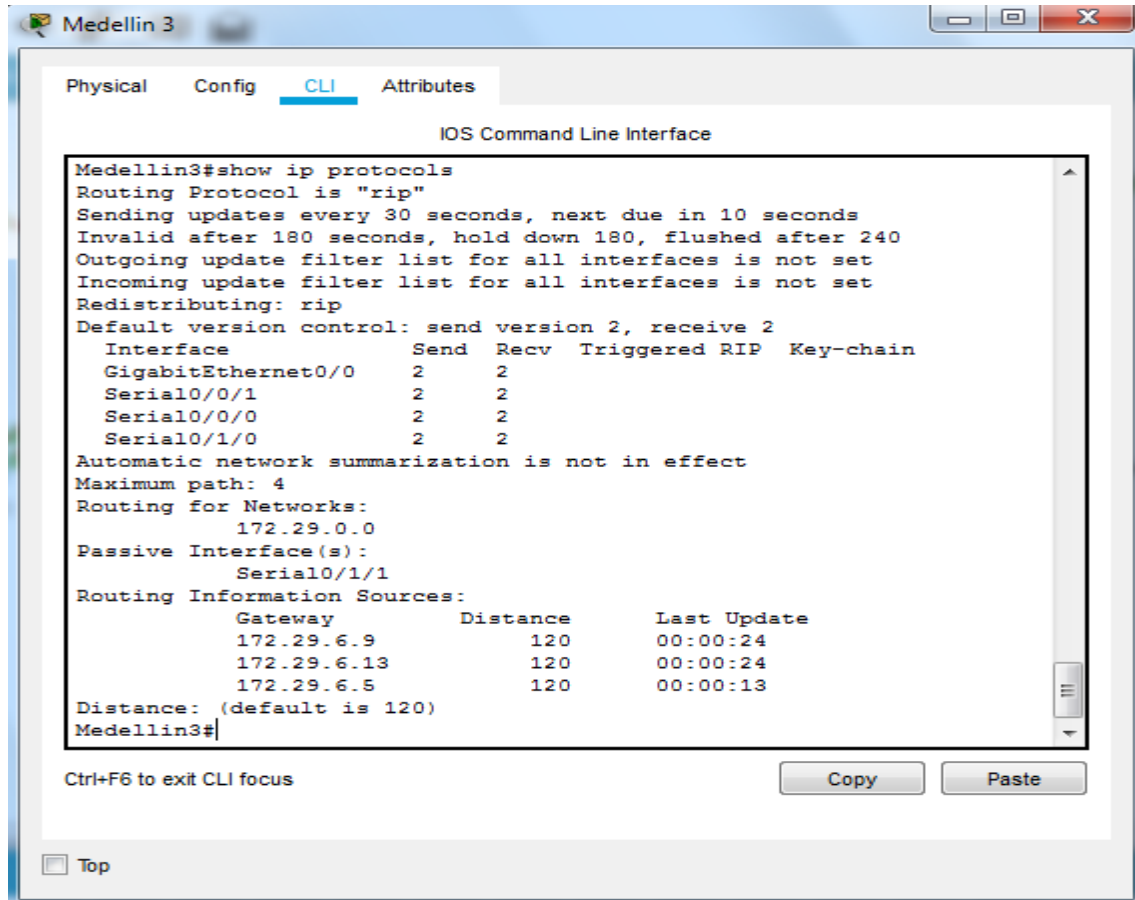


Ilustración 19. Protocolos de Medellín 3

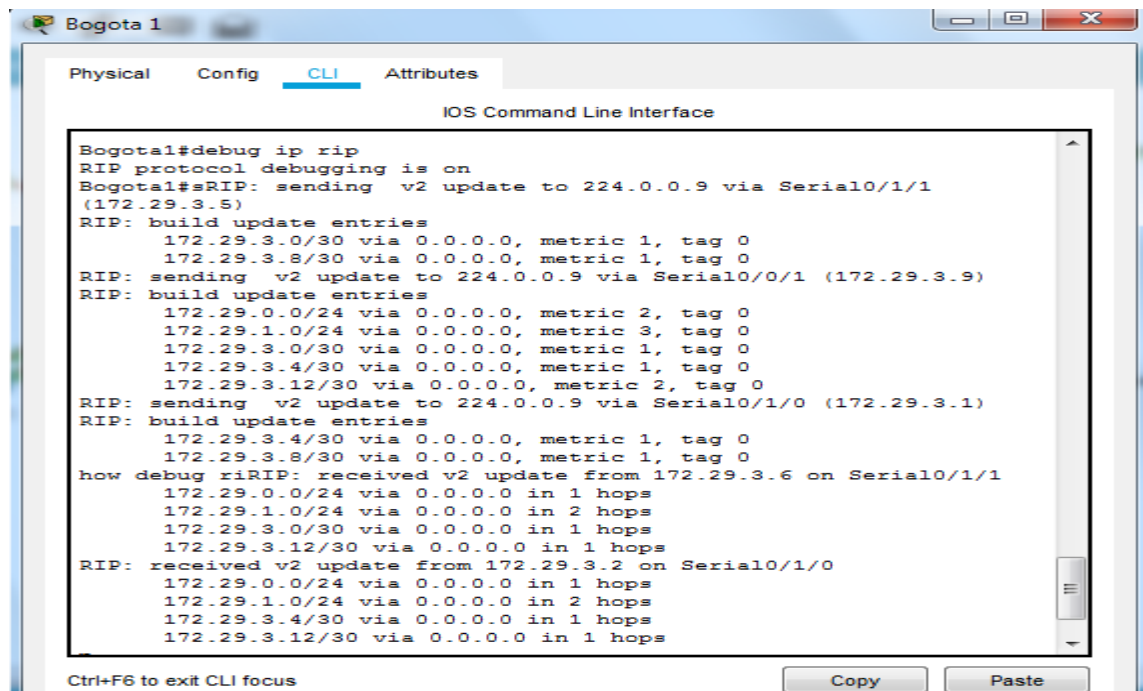


b. Verificar y documentar la base de datos de RIP de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

El comando `debug ip rip` permite mostrar de manera detallada las transacciones de enrutamiento en tiempo real.

Se realiza en Bogotá1 y se detalla los diferentes recorridos de IP a los que se interconecta.

Ilustración 20. Base de datos RIP Bogotá

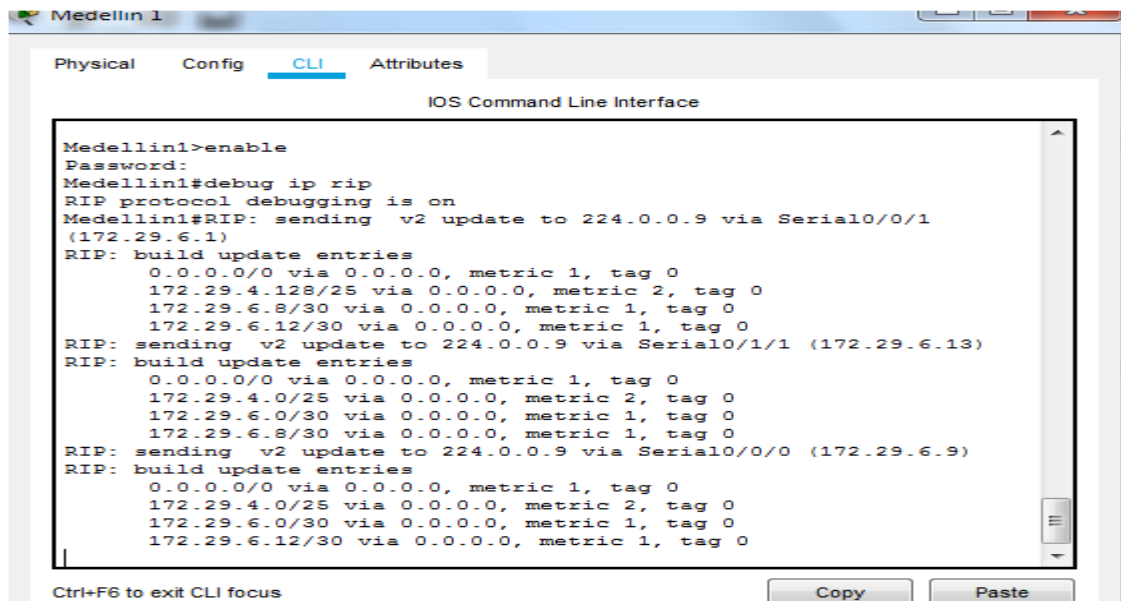


The screenshot shows a CLI window titled "Bogota 1" with tabs for Physical, Config, CLI, and Attributes. The CLI interface displays the following output:

```
Bogota1#debug ip rip
RIP protocol debugging is on
Bogota1#RIP: sending v2 update to 224.0.0.9 via Serial0/1/1
(172.29.3.5)
RIP: build update entries
  172.29.3.0/30 via 0.0.0.0, metric 1, tag 0
  172.29.3.8/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/1 (172.29.3.9)
RIP: build update entries
  172.29.0.0/24 via 0.0.0.0, metric 2, tag 0
  172.29.1.0/24 via 0.0.0.0, metric 3, tag 0
  172.29.3.0/30 via 0.0.0.0, metric 1, tag 0
  172.29.3.4/30 via 0.0.0.0, metric 1, tag 0
  172.29.3.12/30 via 0.0.0.0, metric 2, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/1/0 (172.29.3.1)
RIP: build update entries
  172.29.3.4/30 via 0.0.0.0, metric 1, tag 0
  172.29.3.8/30 via 0.0.0.0, metric 1, tag 0
how debug riRIP: received v2 update from 172.29.3.6 on Serial0/1/1
  172.29.0.0/24 via 0.0.0.0 in 1 hops
  172.29.1.0/24 via 0.0.0.0 in 2 hops
  172.29.3.0/30 via 0.0.0.0 in 1 hops
  172.29.3.12/30 via 0.0.0.0 in 1 hops
RIP: received v2 update from 172.29.3.2 on Serial0/1/0
  172.29.0.0/24 via 0.0.0.0 in 1 hops
  172.29.1.0/24 via 0.0.0.0 in 2 hops
  172.29.3.4/30 via 0.0.0.0 in 1 hops
  172.29.3.12/30 via 0.0.0.0 in 1 hops
```

At the bottom of the window, there is a prompt "Ctrl+F6 to exit CLI focus" and two buttons labeled "Copy" and "Paste".

Ilustración 21. Base de datos Rip Medellín 1



The screenshot shows a CLI window titled "Medellin 1" with tabs for Physical, Config, CLI, and Attributes. The CLI interface displays the following output:

```
Medellin1>enable
Password:
Medellin1#debug ip rip
RIP protocol debugging is on
Medellin1#RIP: sending v2 update to 224.0.0.9 via Serial0/0/1
(172.29.6.1)
RIP: build update entries
  0.0.0.0/0 via 0.0.0.0, metric 1, tag 0
  172.29.4.128/25 via 0.0.0.0, metric 2, tag 0
  172.29.6.8/30 via 0.0.0.0, metric 1, tag 0
  172.29.6.12/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/1/1 (172.29.6.13)
RIP: build update entries
  0.0.0.0/0 via 0.0.0.0, metric 1, tag 0
  172.29.4.0/25 via 0.0.0.0, metric 2, tag 0
  172.29.6.0/30 via 0.0.0.0, metric 1, tag 0
  172.29.6.8/30 via 0.0.0.0, metric 1, tag 0
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (172.29.6.9)
RIP: build update entries
  0.0.0.0/0 via 0.0.0.0, metric 1, tag 0
  172.29.4.0/25 via 0.0.0.0, metric 2, tag 0
  172.29.6.0/30 via 0.0.0.0, metric 1, tag 0
  172.29.6.12/30 via 0.0.0.0, metric 1, tag 0
```

At the bottom of the window, there is a prompt "Ctrl+F6 to exit CLI focus" and two buttons labeled "Copy" and "Paste".

En la ilustración 21 Medellín 1 se ejecuta y se analiza lo siguiente:

Evidencia de todas las interfaces con las cuales existe comunicación, la información se describe así

La versión de RIP La cual es V2

Entrada de la información: IP 172.29.6.2 por medio de serial 0/0/1

Las demás redes que encuentra por la vía en este caso: 172.29.4.0/25, 172.29.4.128/25 y 172.29.6.4/30

PARTE 5: CONFIGURAR ENCAPSULAMIENTO Y AUTENTICACIÓN PPP

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

La configuración se realiza en donde el router solicita autenticación solo en uno de ellos o en los dos.

Pasos 1. Configuración de Medellín 1 con la encapsulación PPP

```
Medellin1>enable
```

```
Password:
```

```
Medellin1#configure terminal
```

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

```
Medellin1(config)#interface s0/1/0
```

```
Medellin1(config-if)#encapsu?
```

```
encapsulation
```

```
Medellin1(config-if)#encapsulation ppp
```

```
Medellin1(config-if)#
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to down
```

```
Medellin1(config-if)#no shutdown
```

Paso 2. Configuración en ISP con la encapsulación

```
ISP#configure terminal
```

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

```
ISP(config)#interface s0/1/0
```

```
ISP(config-if)#encapsulation ppp
```

```
ISP(config-if)#
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
```

```
ISP(config-if)#no shutdown
```

Paso 3. Se ingresa a la interface de Medellin1 que se conecta con el ISP que tiene el serial S0/1/0 para configurar el encapsulamiento PPP, este proceso se realiza en el ISP lo cual ambas interfaces deben estar activas.

```
Medellin1(config-if)#username class
```

```
Medellin1(config-if)#username class password 1991
```

```
Medellin1(config)#interface s0/1/0
```

```
Medellin1(config-if)#ppp authentication pap
```

```
Medellin1(config-if)#
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to down
```

```
Medellin1(config-if)#
```

Paso 4. En Medellín1 se crean un usuario y la contraseña del mismo y se activa en la interface con el ISP, la autenticación de PPP como PAP, luego se realiza la autenticación con un ping.


```
ISP(config)#int s0/1/0
```

```
ISP(config-if)#ppp pap sent-username class password 1991
```

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

Se realiza de la misma manera, pero inversamente de ISP creando autenticación y en Medellín autenticándose.

```
ISP(config)#username class1 password 1611
```

```
ISP(config)#int s0/1/0
```

```
ISP(config-if)#ppp authentication pap
```

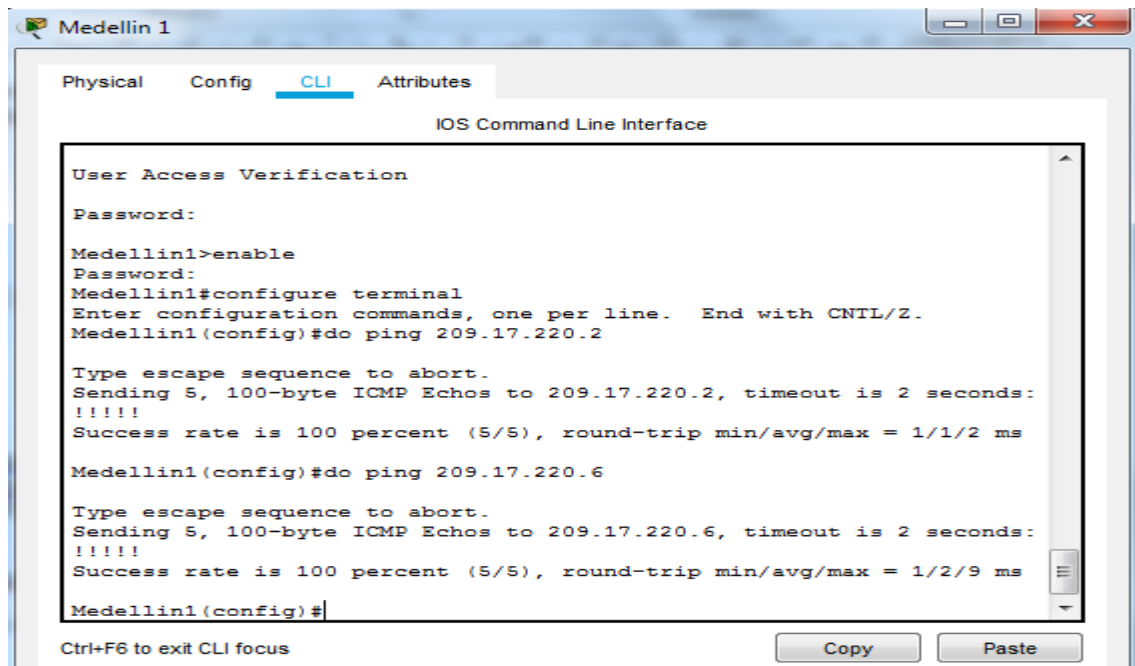
```
ISP(config-if)#
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

```
Medellin1(config-if)#ppp pap sent-username class1 password 1611
```

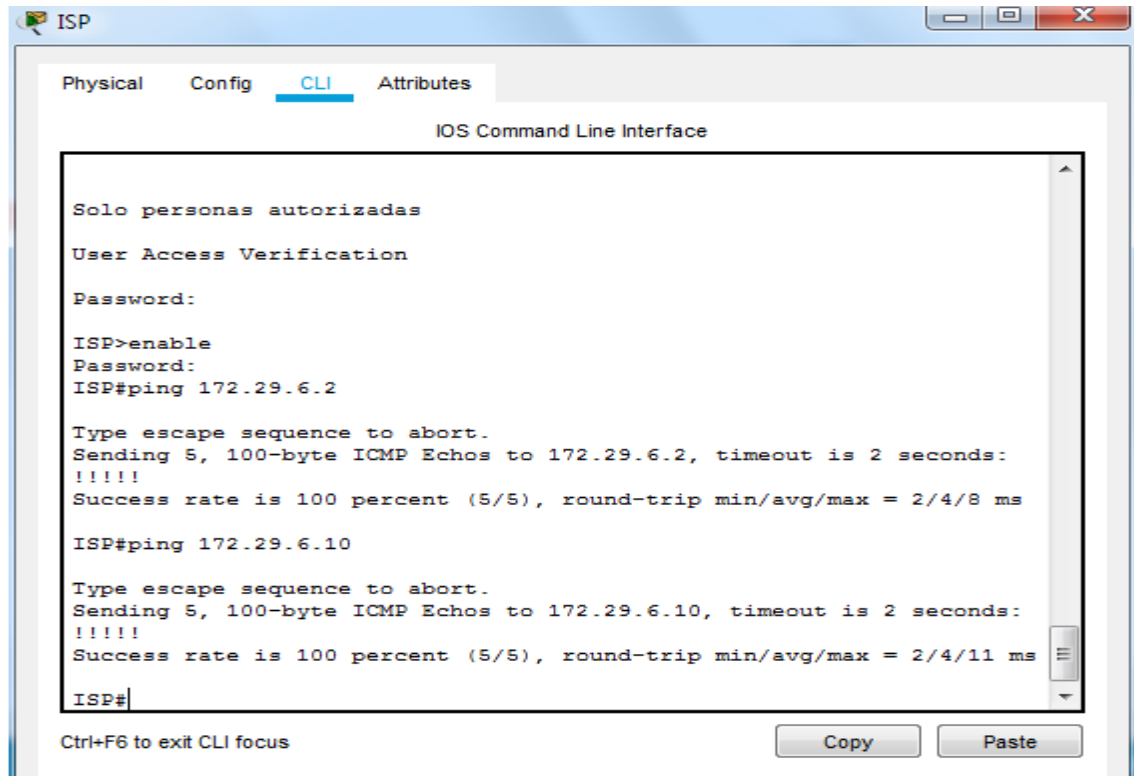
Paso 5. Para probar realizamos ping de Medellín 1 a ISP

Ilustración 22. Conectividad de Medellín a ISP



Ping desde ISP a Medellín 2 y 3

Ilustración 23. Conectividad de ISP a Medellín 1 y 2



b. El enlace Bogotá1 con ISP se debe configurar con autenticación CHAP.

Paso 1. Se configura el ISP creando un usuario y contraseña para la autenticación y agregamos la autenticación de CHAP en ISP

```
ISP(config)#username Bogota1 password bogota1
```

```
ISP(config)#int s0/1/1
```

```
ISP(config-if)#encapsulation ppp
```

```
ISP(config-if)#
```

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

```
ISP(config-if)#ppp authentication chap
```

```
ISP(config-if)#
```

Se ingresa el comando y se verifica la conectividad con ping de router Bogotá 1 a ISP

```
Bogota1>enable
```

```
Password:
```

```
Bogota1#configure terminal
```

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

```
Bogota1(config)#username ISP password bogota1
```

```
Bogota1(config)#interface s0/0/0
```

```
Bogota1(config-if)#encapsulation ppp
```

```
Bogota1(config-if)#ppp authentication chap
```

```
Bogota1(config-if)#exit
```

```
Bogota1(config)#
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
```

```
Bogota1(config)#
```

Verificamos la conectividad con ping del router Bogotá 1 a ISP

Ilustración 24. Conectividad de router Bogotá 1 a ISP

```
Bogota1
Physical Config CLI Attributes
IOS Command Line Interface
Bogota1(config)#username ISP password bogota1
Bogota1(config)#interface s0/0/0
Bogota1(config-if)#encapsulation ppp
Bogota1(config-if)#ppp authentication chap
Bogota1(config-if)#
Bogota1(config-if)#exit
Bogota1(config)#do ping 209.17.220.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

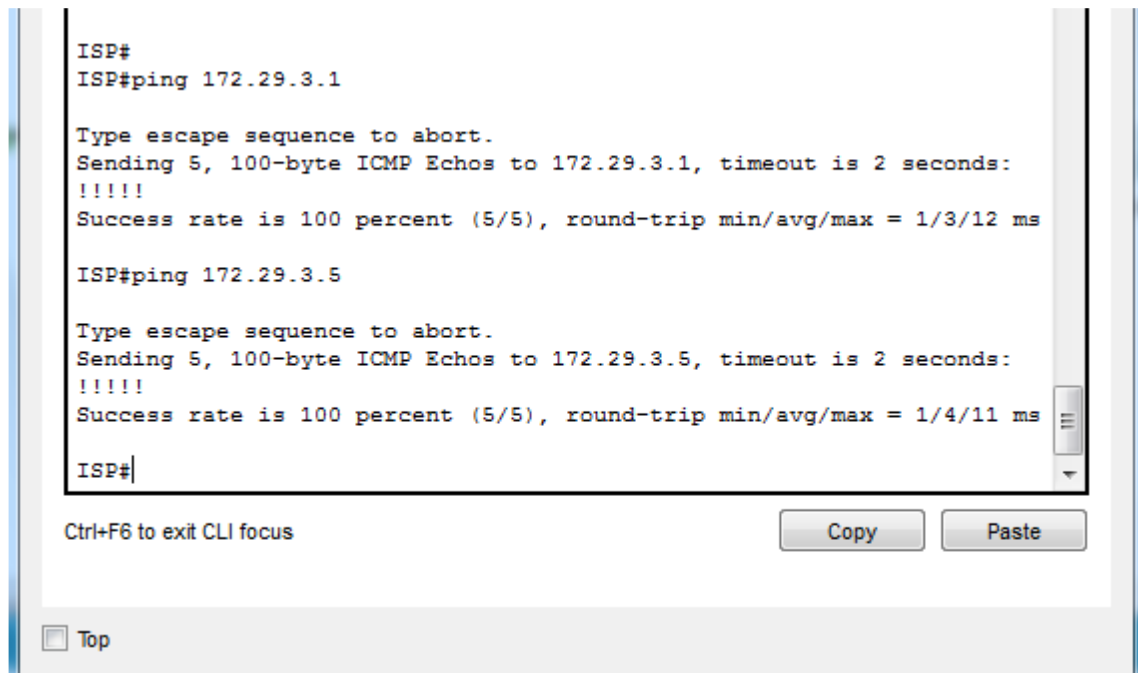
Bogota1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up

Bogota1(config)#do ping 209.17.220.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.6, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/14 ms

Bogota1(config)#
```

Conectividad de router ISP a direcciones de Bogotá 1 y 2

Ilustración 25. Conectividad de ISP a Bogotá 1 y 2



```
ISP#
ISP#ping 172.29.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/12 ms

ISP#ping 172.29.3.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/11 ms

ISP#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

PARTE 6: CONFIGURACIÓN DE PAT.

a. cuando se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.

b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.

configuracion access-list

Medellin1#configure term

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

```
Medellin1(config)#access-list 1 permit 172.29.0.0 0.0.0.255
```

Se crea la lista de acceso global a la red interna

```
Medellin1(config)#ip nat inside source list 1 interface s0/1/0 overload
```

Se determina cual es la ruta de salida y además se declara la lista de acceso global, al agregar el comando overload se indica NAT con sobrecarga es decir PAT

```
Medellin1(config)#inter s0/0/0
```

```
Medellin1(config-if)#ip nat inside
```

```
Medellin1(config-if)#interface s0/0/1
```

```
Medellin1(config-if)#ip nat inside
```

```
Medellin1(config-if)#nterface s0/1/0
```

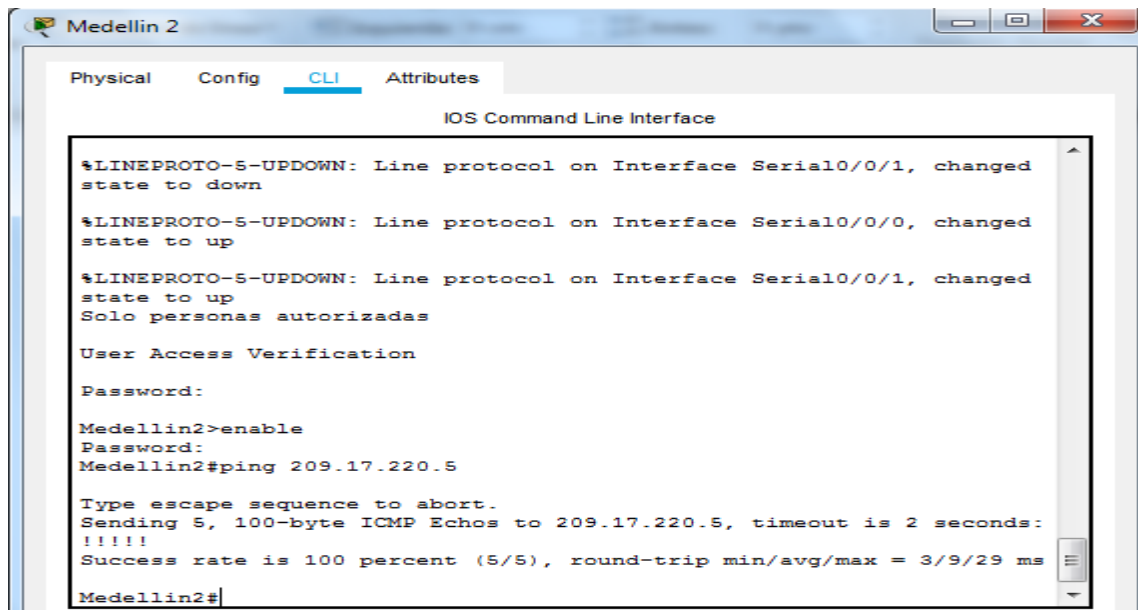
Interface de entrada

```
Medellin1(config-if)#interface s0/1/0
```

```
Medellin1(config-if)#ip nat outside
```

```
Medellin1(config-if)#
```

Ilustración 26. Conectividad de Medellín 2 a router Bogotá 1



c. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, como diferente puerto.

```
Bogota1>enable
```

```
Password:
```

```
Bogota1#configure terminal
```

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

```
Bogota1(config)#access-list 1 permit 172.29.0.0 0.0.0.255
```

```
Bogota1(config)#ip nat inside source list 1 interface s0/0/0 overload
```

```
Bogota1(config)#inter s0/0/1
```

```
Bogota1(config-if)#ip nat inside
```

```
Bogota1(config-if)#interface s0/1/0
```

```
Bogota1(config-if)#ip nat inside
```

```
Bogota1(config-if)#inter s0/1/1
```

```
Bogota1(config-if)#ip nat inside
```

```
Bogota1(config-if)#exit
```

```
Bogota1(config)#
```

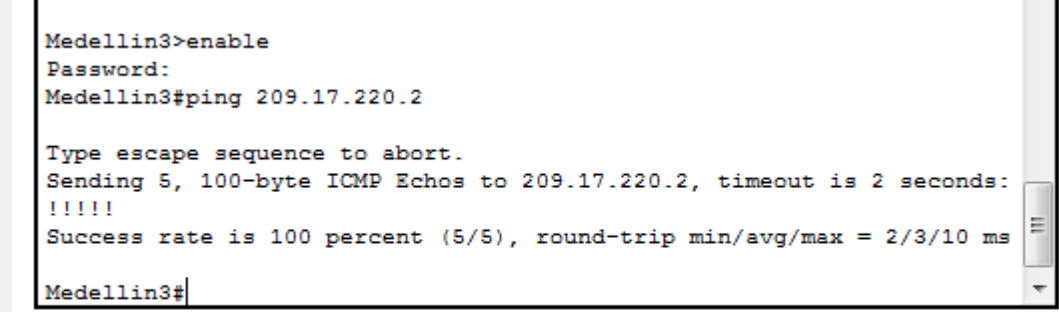
```
Bogota1(config)#interface s0/0/0
```

```
Bogota1(config-if)#ip nat outside
```

```
Bogota1(config-if)#
```

Conectividad de router Medellin3 a router Bogotá 1

Ilustración 27. Prueba de ping a Bogotá 1



```
Medellin3>enable
Password:
Medellin3#ping 209.17.220.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/10 ms
Medellin3#
```

Ctrl+F6 to exit CLI focus

Copy Paste

PARTE 7: CONFIGURACIÓN DEL SERVICIO DHCP

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

```
Medellin2>enable
```

```
Password:
```

```
Medellin2#configure terminal
```

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

```
Medellin2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.20
```

```
Medellin2(config)#ip dhcp pool Pool_Medellin2
```

```
Medellin2(dhcp-config)#network 172.29.4.0 255.255.255.128
```

```
Medellin2(dhcp-config)#dns-server 209.17.220.1
```

```
Medellin2(dhcp-config)#default-router 172.29.4.1
```

```
Medellin2(dhcp-config)#ip dhcp excluded-address 172.29.4.129 172.29.4.149
```

```
Medellin2(config)#ip dhcp pool Pool_Medellin3
```

```
Medellin2(dhcp-config)#network 172.29.4.128 255.255.255.128
```

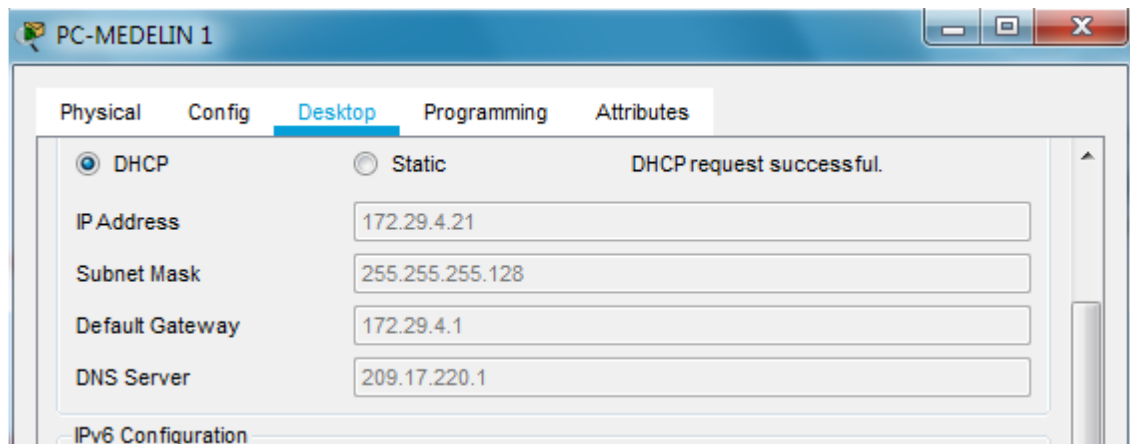
```
Medellin2(dhcp-config)#dns-server 209.17.220.1
```

```
Medellin2(dhcp-config)#default-router 172.29.4.129
```

Medellin2(dhcp-config)#

Se comprueba mediante la dirección IP de la PC activando DHCP lo cual se observa que se activa en la red para Medellín 1

Ilustración 28. DHCP en PC Medellín 1



b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.

Se habilita el acceso a la red de la otra PC de Medellín 3

```
Medellin3>enable
```

```
Password:
```

```
Password:
```

```
Medellin3#configure terminal
```

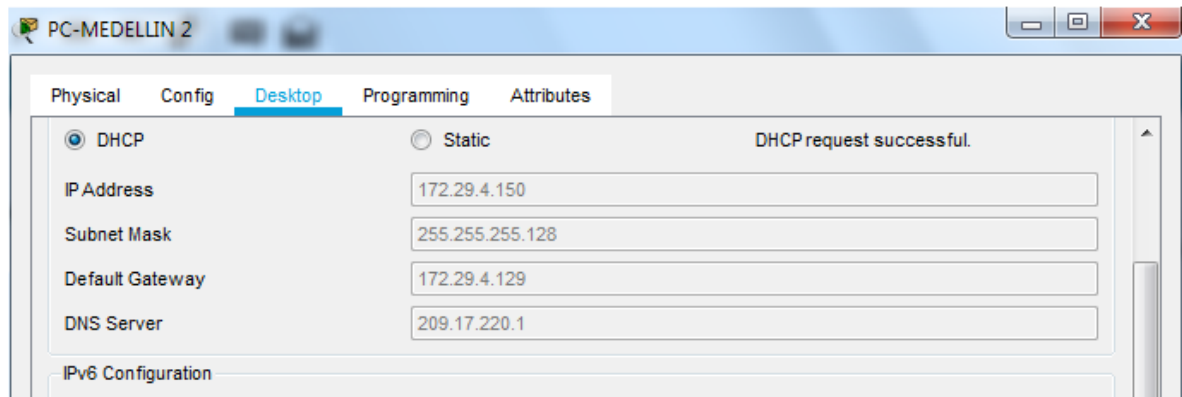
```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Medellin3(config)#interface g0/0
```

```
Medellin3(config-if)#ip helper-address 172.29.6.5
```

```
Medellin3(config-if)#
```


Ilustración 29. DHCP en Medellín 2



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

Paso 1. El proceso de configuración se realiza determinando las redes así:

```
Bogota2>enable
```

Password:

```
Bogota2#configure terminal
```

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

```
Bogota2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.20
```

```
Bogota2(config)#ip dhcp pool Pool_Bogota2
```

```
Bogota2(dhcp-config)#ip dhcp pool Pool_Bogota2
```

```
Bogota2(dhcp-config)#network 172.29.1.0 255.255.255.0
```

```
Bogota2(dhcp-config)#dns-server 209.17.220.1
```

```
Bogota2(dhcp-config)#default-router 172.29.1.1
```

```
Bogota2(dhcp-config)#exit
```

Paso 2. Se realiza el mismo procedimiento para el servicio a la Red Bogotá3

```
Bogota2#configure terminal
```

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

```
Bogota3(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.20
```

```
Bogota3(config)#ip dhcp pool Pool_Bogota2
```

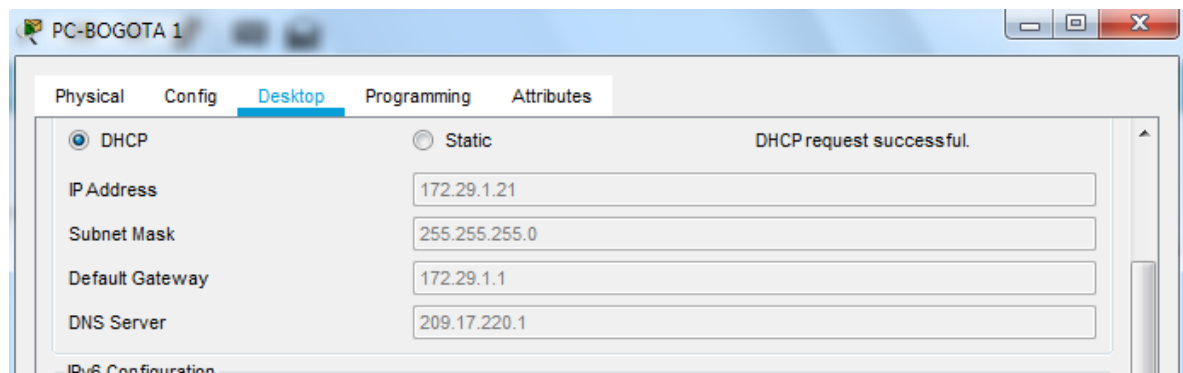
```
Bogota3(dhcp-config)#ip dhcp pool Pool_Bogota2
```

```

Bogota3(dhcp-config)#network 172.29.1.0 255.255.255.0
Bogota3(dhcp-config)#dns-server 209.17.220.1
Bogota3(dhcp-config)#default-router 172.29.1.1
Bogota3(dhcp-config)#exit
Bogota3(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.20
Bogota3(config)#ip dhcp pool Pool_Bogota3
Bogota3(dhcp-config)#network 172.29.0.0 255.255.255.0
Bogota3(dhcp-config)#network 172.29.0.0 255.255.255.0
Bogota3(dhcp-config)#dns-server 209.17.220.1
Bogota3(dhcp-config)#default-router 172.29.0.1
Bogota3(dhcp-config)#

```

Ilustración 30. DHCP Bogotá 1



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

Se habilita DHCP

Bogotá1.

Bogota1#configure terminal

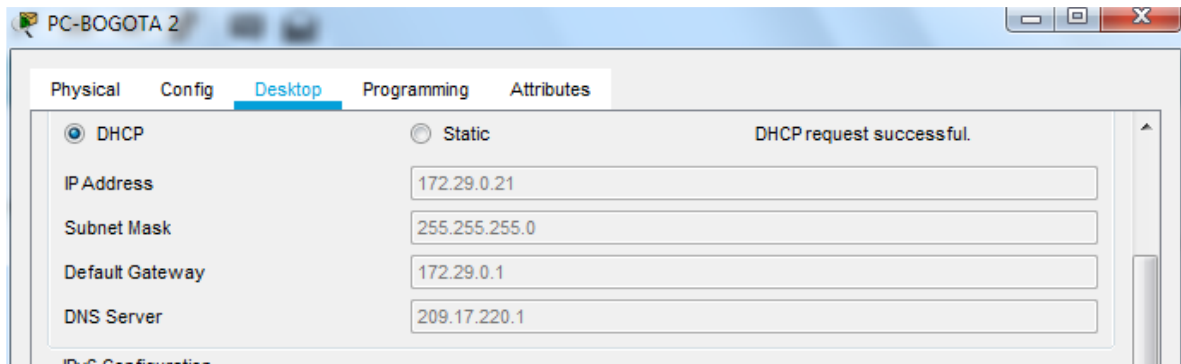
Enter configuration commands, one per line. End with CNTL/Z.

Bogota1(config)#interface g0/0

Bogota1(config-if)#ip helper-address 172.29.3.13

Bogota1(config-if)#

Ilustración 31. DHCP Bogotá 2



CONCLUSIONES

Este trabajo permitió introducir las diversas habilidades obtenidas a lo largo del avance del curso, la utilización de las habilidades en el objetivo de las cuestiones de diseño genuino en una organización empresarial, aplicado constantemente a la mejora de la correspondencia empresarial.

En las diversas circunstancias introducidas anteriormente, se obtuvo información para establecer una organización decente, se aplicaron varios límites para dar seguridad y calidad en las administraciones de la organización. Las órdenes de diseño son fundamentales para la configuración de cada equipo donde se ejecutan arreglos esenciales, por ejemplo, el acceso y el direccionamiento IP para lograr la disponibilidad a través del cableado.

Se obtuvo información sobre la convención RIPv2 que permite la correspondencia en varias LANs a través de un curso estático que conecta y percibe redes situadas a diferentes distancias, el proveedor de acceso a la red ISP se dispuso con la ejemplificación PPP que permite conectarse a través de las convenciones de validación PAT y CHAP, ambas tienen la capacidad de mencionar el acceso del cliente y la clave secreta a lo largo de estas líneas satisfaciendo una seguridad superior en la disponibilidad. Otro enfoque para prevenir las correspondencias a una organización es el diseño a través de NAT, una convención que organiza las organizaciones a las que permite el acceso.

Se perciben los medios para organizar DHCP que nos da una dirección IP programada con IP guardada, los diseños ospfv2 que permiten la dirección y la correspondencia con organizaciones lejanas para construir la asociación en una organización WAN, lo que es más hay información sobre las organizaciones que se organizan a través de VLANS que mantienen lejos de un impacto de la caída de la información y los puertos troncales o troncos permiten la admisión para impartir a los PC y salir a Internet.

Las órdenes de acceso distintivas se conocen a través de registros de acceso, por ejemplo, ACL donde se permite o limita la disponibilidad de cualquier host en una organización particular. Las órdenes de confirmación de disponibilidad como ping, traceroute y órdenes de detalle son clave para cuidar los problemas introducidos en las organizaciones.

En definitiva, estas habilidades permiten conocer la dirección de las organizaciones, el uso de convenciones, registros de acceso, VLAN los ejecutivos, y así sucesivamente, que permite diseñar de una manera segura a una organización en particular.

La configuración fundamental aplicada a cada uno de los componentes, permite un campo viable de participación, considerando que es el arreglo base para aplicar en el desarrollo de otra organización de correspondencias.

Los distintos tipos de arreglos realizados en los componentes, se aclimatan a las necesidades reconocidas, se aplican las convenciones y se realizan las distintas organizaciones que permiten la correspondencia por distintos métodos, permitiendo en consecuencia una organización total y cambiada exhaustivamente.

Los arreglos se hacen por la mejora del diseño fundamental de cada componente, vlan se hacen y se diseña en las subinterfaces de los interruptores, de la web y http se reactiva, dhcp se diseña en un ámbito asignado de direcciones ip, la forma de convención de desgarrado 2 se aplica, NAT estática y dinámica se diseña en función de las percepciones del registro, una organización cambió de acuerdo con las necesidades del negocio se organiza. A la luz de lo anterior, la prueba de información viable se termina de cumplir.

Se aplica la configuración de la adaptación de la convención OSPF como una convención de dirección dinámica, se ve su estrategia de engendramiento e interconexión para difundir las organizaciones que no están directamente asociadas, se sugiere la utilización de la convención para las organizaciones.

BIBLIOGRAFÍA

CISCO. (2021). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#2>

CISCO. (2021). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#3>

CISCO. (2021). Acceso a la red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#4>

CISCO. (2021). Ethernet. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#5>

CISCO. (2021). Capa de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#6>

CISCO. (2021). Direccionamiento IP. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#7>

CISCO. (2021). División de redes IP en subredes. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#8>

CISCO. (2021). Capa de transporte. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#9>

CISCO. (2021). Capa de aplicación. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#10>

CISCO. (2021). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: <https://static-course-assets.s3.amazonaws.com/ITN6/es/index.html#11>

CISCO. (2021). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#1>

CISCO. (2021). Routing Estático. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE6/es/index.html#2>

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