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

HEINER MADERA DUARTE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
INGENIERIA DE SISTEMAS
CCAV COROZAL
MAGANGUÉ, BOLÍVAR
2020

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

HEINER MADERA DUARTE

ASESOR
NILSON ALBEIRO FERREIRA MANZANARES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍAS
INGENIERIA DE SISTEMAS
CCAV COROZAL
MAGANGUÉ, BOLÍVAR
2020

**CONTENIDO**

Pág.

RESUMEN ....8

ABSTRACT ....9

GLOSARIO....10

INTRODUCCIÓN ....12

OBJETIVOS ....13

1. DESARROLLO ESCENARIO 1....14
1.1 Parte 1: Inicializar dispositivos....15
1.1.1 Paso 1: Inicializar y volver a cargar los routers y los switches. ....15
1.2 Parte 2: Configurar los parámetros básicos de los dispositivos ....16
1.2.1 Paso 1: Configurar la computadora de Internet....16
1.2.2 Paso 2: Configurar R1....17
1.2.3 Paso 3: Configurar R2....19
1.2.4 Paso 4: Configurar R3....23
1.2.5 Paso 5: Configurar S1....26
1.2.6 Paso 6: Configurar el S3 ....27
1.2.7 Paso 7: Verificar la conectividad de la red....28
1.3 Parte 3: Configurar la seguridad del switch, las VLAN y el routing entre VLAN ....29
1.3.1 Paso 1: Configurar S1....29
1.3.2 Paso 2: Configurar el S3 ....31
1.3.4 Paso 4: Verificar la conectividad de la red....33
1.4 Parte 4: Configurar el protocolo de routing dinámico RIPv2 ....35
1.4.1 Paso1: Configurar RIPv2 en el R1 ....35
1.4.2 Paso 2: Configurar RIPv2 en el R2 ....36
1.4.1 Paso 3: Configurar RIPv2 en el R3....36
1.5 Parte 5: Implementar DHCP y NAT para IPv4 ....40
1.5.1 Paso 1: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23 ..... 40
1.5.2 Paso 2: Configurar la NAT estática y dinámica en el R2....41
1.5.3 Paso 3: Verificar el protocolo DHCP y la NAT estática....42
1.6 Parte 6: Configurar NTP ....44
1.7 Parte 7: Configurar y verificar las listas de control de acceso (ACL)....45
1.7.1 Restringir el acceso a las líneas VTY en el R2....45

2 DESARROLLO ESCENARIO 2....51

2.1 Parte 1: Configuración del enrutamiento....52
2.2 Parte 2: Tabla de Enrutamiento....54
2.3 Parte 3: Deshabilitar la propagación del protocolo OSPF....58
2.4 Parte 4: Verificación del protocolo OSPF....59
2.5 Parte 5: Configurar encapsulamiento y autenticación PPP....63
2.6 Parte 6: Configuración de PAT....65
2.7 Parte 7: Configuración del servicio DHCP....68

CONCLUSIONES....70

BIBLIOGRAFÍA....71

## LISTA DE TABLAS

Tabla 1. Inicializar y volver a cargar los routers y los switches. ..... 15
Tabla 2. Configuración de direcciones en la computadora de Internet ..... 16
Tabla 3. Subnnetting de la red 209.165.200.232 ..... 16
Tabla 4.Tabla de direccionamiento del escenario 1 ..... 17
Tabla 5. Configurar R1 ..... 18
Tabla 6.Configurar R2 ..... 21
Tabla 7. Configurar R3 ..... 25
Tabla 8. Configurar S1 ..... 27
Tabla 9. Configurar el S3 ..... 27
Tabla 10. Verificar la conectividad de la red ..... 28
Tabla 11. Configurar VLAN en S1, enlace troncal y puertos de éste ..... 30
Tabla 12. Configurar VLANS en S3, enlace troncal y puertos de éste ..... 31
Tabla 13. Configurar subinterfaces en R1 y activar G0/1 ..... 33
Tabla 14. Verificar la conectividad de la red ..... 34
Tabla 15. Configurar RIPv2 en el R1 y desactivar la sumarización automatica ..... 35
Tabla 16. Configurar RIPv2 en el R2 y desactivar el resumen automática ..... 36
Tabla 17.Configurar RIPv2 en el R3 y descativar la sumarización automática ..... 37
Tabla 18. Verificar la información de RIP a través de comandos ..... 38
Tabla 19. Implementar DHCP y NAT para IPv4 ..... 40
Tabla 20. Verificar el protocolo DHCP y la NAT estática ..... 43
Tabla 21. Configurar NTP ..... 45
Tabla 22. Configurar y verificar las listas de control de acceso (ACL) ..... 46
Tabla 23. Introducir commandos show access-list, clear access-list counters, R2#show ip interface, show ip nat translations y clear ip nat translation * ..... 48

## LISTA DE GRAFICAS

Figura 1. Escenario de red 1 .....14
Figura 2.Verificación de tabla de enrutamiento IPV4 en R1 .....18
Figura 3. Tabla de enrutamiento IPV6 en R1.....19
Figura 4. Verificación de tabla de enrutamiento IPV4 en R2 .....22
Figura 5.Tabla de enrutamiento IPV6 en R2 .....22
Figura 6.Verificación tabla de enrutamiento IPV4 en R3 .....25
Figura 7.Tabla de enrutamiento IPV6 en R3 .....26
Figura 8. Verificación de conectividad Servidor de Internet, R1 y R2 .....29
Figura 9. Verificación de VLAN configuradas en S1 y S2.....32
Figura 10. Verificación de asignación de VLAN en S1 (21 a F0/6) y S3 (23 A F0/18) ....32
Figura 11. Comprobación de conexiones S3 a R1 y S1 a R1.....34
Figura 12. Verificación del comando show ip protocols en R1, R2 y R3.....38
Figura 13. Verificación del comando show ip route rip R1, R2 y R3 .....39
Figura 14. Verificación del protocolo RIPv2 a través del comando show run R1, R2 y R3. .....39
Figura 15. Verificación servidor DHCP en PC-A y PC-C .....43
Figura 16. Verificación Ping PC-A y PC-C.....44
Figura 17. Verificación del funcionamiento de Telnet en R2.....46
Figura 18. Verificar Interfaz y la dirección ACL a que se aplica.....48
Figura 19. Verificación del comando show ip nat translations. .....49
Figura 20. Verificación de conexión entre PC-A y PC-C al servidor web desde el Command Prompt .....49
Figura 21. Verificación de conexión entre PC-A y PC-C al servidor web desde el navegador. .....50
Figura 22. Verificación de la ruta de destino de PC-A y PC-C hasta el servidor de internet a través del comando tracert .....50
Figura 23. Escenario de red 2 .....51
Figura 24. Tablas de enrutamiento BOGOTA1.....55
Figura 25. Tablas de enrutamiento BOGOTA2 y BOGOTA3.....56
Figura 26. Tablas de enrutamiento MEDELLIN1 .....56
Figura 27. Tabla de enrutamiento MEDELLIN2 y MEDELLIN3 .....57
Figura 28. Tabla de enrutamiento ISP. .....57
Figura 29. Verificación de conectividad de extremo a extremo entre los Routers de Bogotá y Medellín.....58
Figura 30. Verificación del protocolo OSPF en BOGOTA1.....59
Figura 31. Verificación del protocolo OSPF en BOGOTA2 y BOGOTA3.....59

Figura 32. Verificación del protocolo OSPF en MEDELLIN1 .....60
Figura 33. Verificación del protocolo OSPF en MEDELLIN2 y MEDELLIN3.....60
Figura 34. Base de datos de OSPF de BOGOTA1.....61
Figura 35. Base de datos de OSPF BOGOTA2 y BOGOTA3.....61
Figura 36. Base de datos de OSPF MEDELLIN1 .....62
Figura 37. Base de datos de OSPF MEDELLIN2 y MEDELLIN3.....62
Figura 38. Verificación PAP entre ISP y MEDELLIN1 .....63
Figura 39. Verificación CHAP entre ISP y BOGOTA1 .....64
Figura 40. Ping de extremo a extremo (MEDELLIN3 a BOGOTA3). .....65
Figura 41. Ping de extremo a extremo (No funciona). .....66
Figura 42. Ping a ISP, Medellin1 y Bogota1 (Funciona), desde los computadores ubicadas en las LAN de Medellín y Bogotá .....67
Figura 43.Verificación de la ruta de destino de PC0 y PC2 hasta el otro extremo a través del comando tracert .....67
Figura 44. Verificación dhcp MEDELLIN2 y MEDELLIN3 .....68
Figura 45. Verificación del servicio dhcp BOGOTA2 y BOGOTA3 .....69

## RESUMEN

En el presente trabajo se evalúa el grado de desarrollo de competencias y habilidades relacionadas con el montaje, configuración y seguridad de redes LAN y WAM a través de la solución de dos estudios de caso bajo el uso de tecnología CISCO desarrollados en la herramienta de simulación Packet Tracer. Los escenarios de red propuestos ponen a prueba el análisis y la interpretación de diversos problemas relacionados con la implementación eficaz y escalable de infraestructuras de red.



**Palabras claves:** seguridad, configuración, red, escalabilidad, Internet, enrutamiento, CISCO, VLAN, LAN, WAN.

## ABSTRACT

This work evaluates the degree of development of competencies and skills related to the assembly, configuration and security of LAN and WAM networks is evaluated through the solution of two case studies developed in the simulation tool Packet Tracer using CISCO technology. The proposed network scenarios test the analysis and interpretation of various problems related to the efficient and scalable implementation of network infrastructures.



Keywords: security, configuration, network, scalability, Internet, routing, CISCO, VLAN, LAN, WAN

## GLOSARIO

**CISCO SYSTEMS:** Es una compañía multinacional dedicada al diseño, fabricación y venta de productos y servicios de red basados en el Protocolo de Internet relacionados con la industria de las tecnologías de la información y las comunicaciones. La compañía fue fundada por Sandra Lerner y Leonard Bosack el 10 de diciembre de 1984 y tiene su sede en San José, California.

**Protocolo:** Descripción formal de formatos de mensaje y de reglas que dos computadoras deben seguir para intercambiar dichos mensajes. Un protocolo puede describir detalles de bajo nivel de las interfaces máquina a máquina o intercambios de alto nivel entre programas de asignación de recursos.

**Red**: Sistema de comunicación de datos que conecta entre sí sistemas informáticos situados en lugares más o menos próximos. Puede estar compuesta por diferentes combinaciones de diversos tipos de redes. En inglés se le conoce como Network. El internet está compuesto de miles de redes, por lo tanto al internet también se le conoce como "la red".

**LAN** (Local Area Network). Red de área local. Red de computadoras personales ubicadas dentro de un área geográfica limitada que se compone de servidores, estaciones de trabajo, sistemas operativos de redes y un enlace encargado de distribuir las comunicaciones.

**WAN,** Siglas del inglés Wide Area Network (Red de área Amplia). Es una red de computadoras conectadas entre sí. Usando líneas terrestres o satélites para interconectar redes LAN en un área geográfica extensa que puede ser hasta de miles de kilómetros.

**VLAN,** Siglas de virtual LAN (red de área local virtual)- Es un método que permite crear redes lógicas independientes compartiendo dispositivos físicos de red, ofreciendo una subdivisión por grupos garantizando la comunicación y envío de los datos en la red como si se tratará de redes aisladas.

**Switches o conmutadores:** Son dispositivos que permiten la interconexión en redes de área local, recibiendo paquetes de datos y direccionándolos al destinatario correcto. Al hacer posible que la información y los recursos sean compartidos, los switches le ayudan a ahorrar dinero e incrementar la productividad.

**Routers o enrutadores**: Son dispositivos que conectan múltiples redes entre sí o con Internet. Analizan los datos y los envían por la mejor ruta. Protegen la información de las amenazas de seguridad e incluso deciden qué equipos de cómputo tienen prioridad sobre otros.

**Red escalable:** es aquella que tiene la capacidad de reaccionar y adaptarse fácilmente al crecimiento de su negocio, de los usuarios y de las cargas de trabajo, protegiendo su inversión y asegurando la continuidad de la operación.

**Red segura** es aquella que cuenta con las políticas y prácticas necesarias para prevenir y supervisar el acceso no autorizado, así como el uso indebido, en la información de su empresa y sus recursos. Actualmente, las amenazas a la seguridad son cada vez mayores y pueden poner en riesgo tanto la integridad como la continuidad de su negocio.

# INTRODUCCIÓN

En las últimas décadas los sistemas de comunicación han tenido un enorme desarrollo que se ve reflejado en la gran cantidad de información que circula a través de ellos. Este intercambio de información es posible gracias a medios físicos y lógicos interconectados entre sí que trabajan conjuntamente en la recuperación, almacenamiento y procesamiento de los datos que fluyen a través de redes LAN o WAN. Un claro ejemplo de todo lo mencionado anteriormente es Internet, el cual constituye una red global descentralizada dotada de una gran cantidad de servicios (chat, correo electrónico, foros, ftp, video conferencia, etc.) situados en equipos remotos.

En el presente trabajo se pretende aplicar los conocimientos adquiridos a través de los diferentes módulos Cisco CCNA vistos a lo largo del curso profundización, para lo cual se propone la implementación de dos escenarios diferentes que pondrán a prueba las habilidades relacionadas con el montaje, inicialización, configuración y seguridad de los diversos equipos que integraran cada una de estas topologías de red mediante la utilización de una herramienta de simulación de red (Packet Tracer o GNS3).

El producto final de este trabajo debe contener la documentación del código de configuración aplicado en cada una de las soluciones implementadas, la verificación exitosa de las conexiones por medio de imágenes, las conclusiones finales y referencias bibliográficas utilizadas para el desarrollo del trabajo. Adicionalmente se deberán adjuntar los archivos de simulación en Packet Tracer o GNS3 asociados a la actividad que permitan evidenciar el cumplimiento de los objetivos propuestos durante la actividad.

# OBJETIVOS

## OBJETIVO GENERAL

Implementar la solución de dos estudios de caso bajo el uso de tecnología cisco aplicando los conocimientos y las habilidades adquiridas durante el curso de profundización.

## OBJETIVOS ESPECIFICOS

Documentar el paso a paso de cada una de las configuraciones realizadas a los dispositivos que integran los escenarios de red propuestos.

Evidenciar la conectividad de los dispositivos que integran cada una de escenarios de red propuestos, mediante el uso de los comandos ping, traceroute, show ip route, entre otros.

Utilizar una herramienta de simulación de red para realizar el montaje y configuración de los escenarios de red propuestos.

## 1. DESARROLLO ESCENARIO 1

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.

### Topología

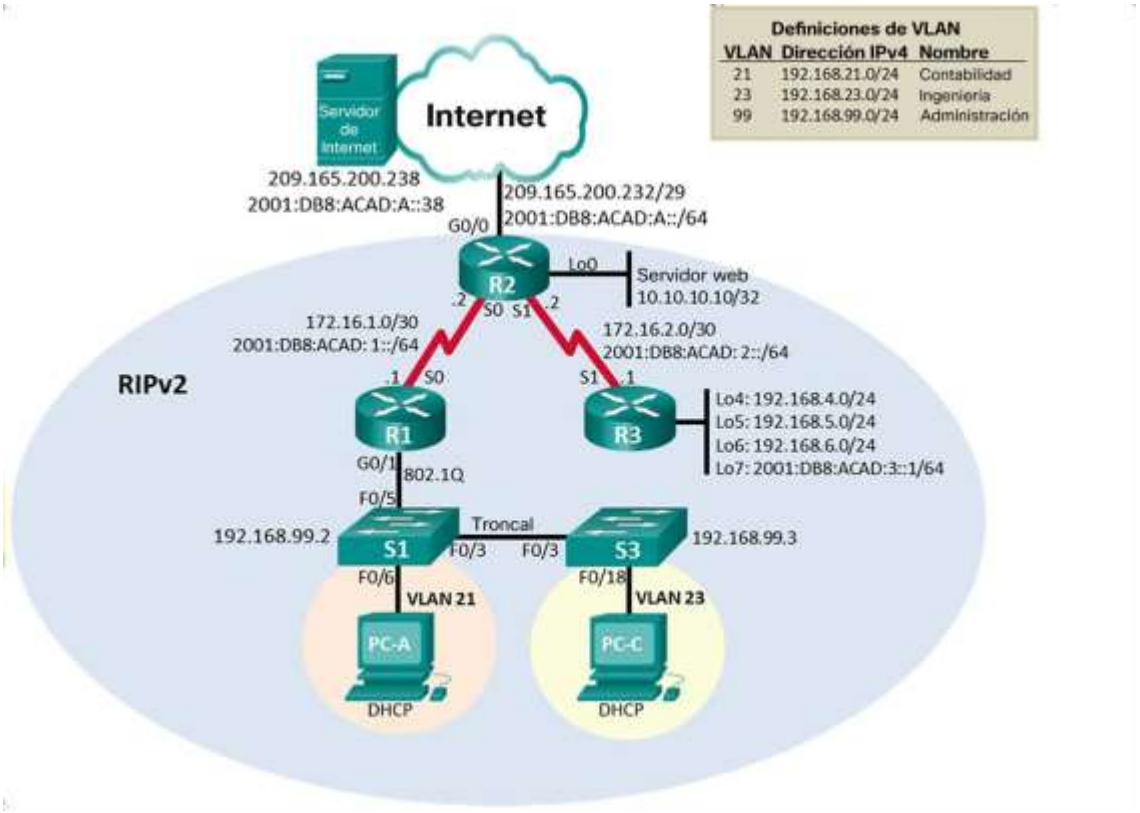


*Figura 1. Escenario de red 1*

## 1.1 Parte 1: Inicializar dispositivos

### 1.1.1 Paso 1: Inicializar y volver a cargar los routers y los switches.

| Tarea | Comando de IOS |
|---|---|
| Eliminar el archivo startup-config de todos los routers | **Router>en**<br>**Router#erase startup-config**<br>Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]<br>[OK]<br>Erase of nvram: complete<br>%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram |
| Volver a cargar todos los routers | **Router#reload**<br>Proceed with reload? [confirm] |
| Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior | **Switch>en**<br>**Switch#erase startup-config**<br>Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]<br>[OK]<br>Erase of nvram: complete<br>%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram<br>**Switch#delete vlan.dat**<br>Delete filename [vlan.dat]?<br>Delete flash:/vlan.dat? [confirm]<br>%Error deleting flash:/vlan.dat (No such file or directory) |
| Volver a cargar ambos switches | **Switch#reload**<br>Proceed with reload? [confirm] |
| Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches | **Switch>show flash**<br>Directory of flash:/<br>1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin<br>64016384 bytes total (59601463 bytes free)<br>Switch> |

*Tabla 1. Inicializar y volver a cargar los routers y los switches.*

## 1.2 Parte 2: Configurar los parámetros básicos de los dispositivos

### 1.2.1 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):

| Elemento o tarea de configuración | Especificación |
|---|---|
| Dirección IPv4 | 209.165.200.238/29 |
| Máscara de subred para IPv4 | 255.255.255.248 |
| Gateway predeterminado | 209.165.200.233 |
| Dirección IPv6/subred | 2001:DB8:ACAD:A::38/64 |
| Gateway predeterminado IPv6 | 2001:DB8:ACAD:A::1 |

*Tabla 2. Configuración de direcciones en la computadora de Internet.*

**Clase c**

| | | |
|---|---|---|
| Network: | 209.165.200.232/29 | 11010001.10100101.11001000.11101**.000** |
| HostMin: | 209.165.200.233 | 11010001.10100101.11001000.11101 **001** |
| HostMax: | 209.165.200.238 | 11010001.10100101.11001000.11101 **110** |
| Broadcast: | 209.165.200.239 | 11010001.10100101.11001000.11101 111 |
| Hosts: | 6 | |

*Tabla 3. Subnnetting de la red 209.165.200.232.*

**Tabla de direccionamiento**

| Dispositivo | Interfaz | Dirección IP | Máscara de subred IPV4 |
|---|---|---|---|
| R1 | G0/1.21 | LAN de Contabilidad 192.168.21.1 | 255.255.255.0 |
| | G0/1.23 | LAN de Ingeniería 192.168.23.1 | 255.255.255.0 |
| | G0/1.99 | LAN de Administración 192.168.99.1 | 255.255.255.0 |

| | | | |
|---|---|---|---|
| | S0/0/0 (DCE) | 172.16.1.1<br>2001:db8:ACAD:1::1/64 | 255.255.255.252 |
| R2 | G0/0 | 209.165.200.233<br>2001:DB8:ACAD:A::1/64 | 255.255.255.248 |
| | Lo 0 | 10.10.10.10 | 255.255.255.255 |
| | S0/0/0 | 172.16.1.2<br>2001:DB8:ACAD:1::2/64 | 255.255.255.252 |
| | S0/0/1 (DCE) | 172.16.2.2<br>2001:DB8:ACAD:2::2/64 | 255.255.255.252 |
| R3 | S0/0/1 | 172.16.2.1<br>2001:DB8:ACAD:2::1/64 | 255.255.255.252 |
| | Lo4 | 192.168.4. | 255.255.255.0 |
| | Lo5 | 192.168.5.1 | 255.255.255.0 |
| | Lo6 | 192.168.6.1 | 255.255.255.0 |
| | Lo7 | 2001:DB8:ACAD:3::1/64 | |
| PC-A | NIC | Dirección dinamica | 255.255.255.0 |
| Internet PC | NIC | 209.165.200.238 | 255.255.255.248 |
| PC-C | NIC | Dirección dinamica | 255.255.255.0 |
| Web Server | Fa0 | 10.10.10.10 | 255.255.255.0 |

*Tabla 4.Tabla de direccionamiento del escenario 1.*

### 1.2.2 Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | **Router(config)#no ip domain-lookup** |
| Nombre del router | **Router(config)#hostname R1** |
| Contraseña de exec privilegiado cifrada | **R1(config)#enable secret class** |
| Contraseña de acceso a la consola | **R1(config)#line console 0**<br>**R1(config-line)#password cisco**<br>**R1(config-line)#login** |
| Contraseña de acceso Telnet | **R1(config-line)#line vty 0 15**<br>**R1(config-line)#password cisco**<br>**R1(config-line)#login** |
| Cifrar las contraseñas de texto no cifrado | **R1(config-line)#service password-encryption** |

| | |
|---|---|
| Mensaje MOTD | **R1(config)#banner motd #Se prohibe el acceso no autorizado.#** |
| Interfaz S0/0/0 | **R1(config)#int s0/0/0**<br>**R1(config-if)#description Connection R2**<br>**R1(config-if)#ip address 172.16.1.1 255.255.255.252**<br>**R1(config-if)#ipv6 address 2001:db8:ACAD:1::1/64**<br>**R1(config-if)#clock rate 128000**<br>**R1(config-if)#no shutdown**<br><br>%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down |
| Rutas predeterminadas | **R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0**<br>%Default route without gateway, if not a point-to-point interface, may impact performance<br>R1(config)#ipv6 unicast-routing<br>**R1(config)#ipv6 route ::/0 s0/0/0** |

*Tabla 5. Configurar R1.*

### Verificación de tabla de enrutamiento en R1

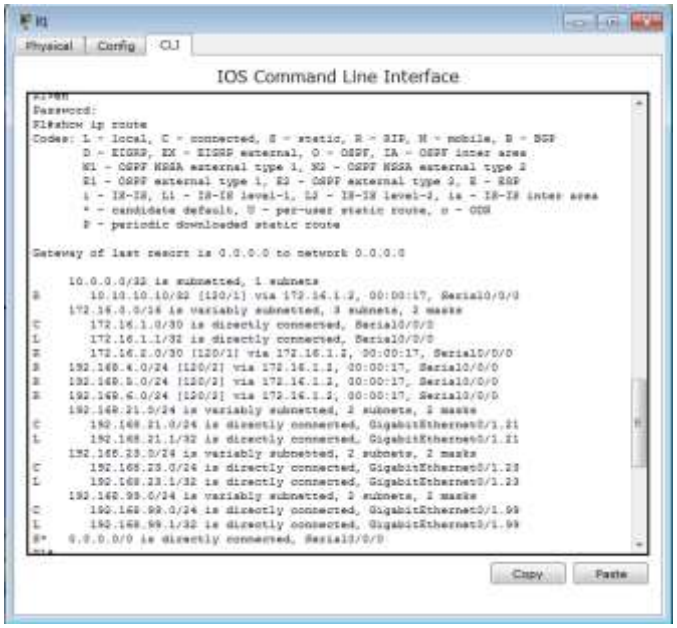


*Figura 2.Verificación de tabla de enrutamiento IPV4 en R1 .*

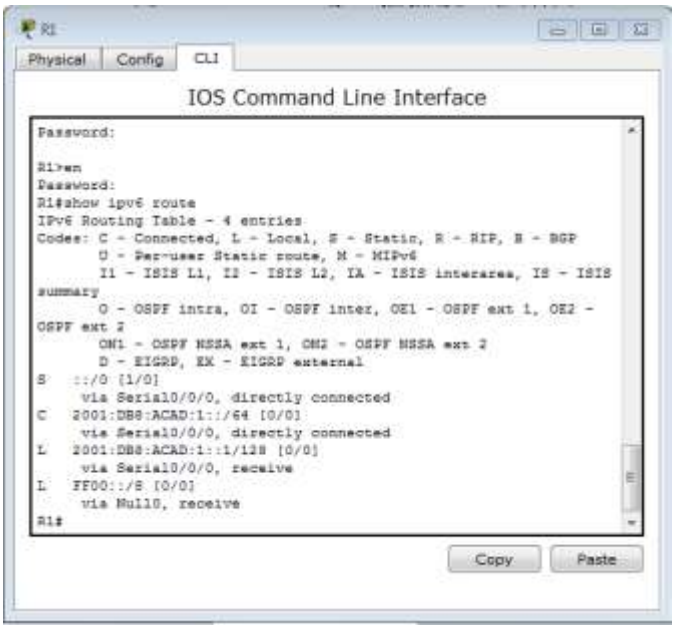


*Figura 3. Tabla de enrutamiento IPV6 en R1.*

**Análisis de resultados R1:** En la tabla de enrutamiento se pueden evidenciar que todas las rutas están configuradas correctamente incluyendo la ruta predeterminada.

### 1.2.3 Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | **Router>en**<br>**Router#config t**<br>Enter configuration commands, one per line. End with CNTL/Z.<br>**Router(config)#no ip domain-lookup** |
| Nombre del router | **Router(config)#hostname R2** |
| Contraseña de exec privilegiado cifrada | **R2(config)#enable secret class** |
| Contraseña de acceso a la consola | **R2(config)#line console 0**<br>**R2(config-line)#password cisco**<br>**R2(config-line)#login** |

| | |
|---|---|
| Contraseña de acceso Telnet | **R2(config-line)#line vty 0 15**<br>**R2(config-line)#password cisco**<br>**R2(config-line)#login** |
| Cifrar las contraseñas de texto no cifrado | **R2(config-line)#service password-encryption** |
| Habilitar el servidor HTTP | **R2(config)#ip http server**% Invalid input detected at '^' marker.<br>- Packet tracer no soporta el comando |
| Mensaje MOTD | **R2(config)#banner motd #Se prohibe el acceso no autorizado.#** |
| Interfaz S0/0/0 | **R2(config)#int s0/0/0**<br>**R2(config-if)#description Connection to R1**<br>**R2(config-if)#ip address 172.16.1.2 255.255.255.252**<br>**R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64**<br>**R2(config-if)#no shutdown** |
| Interfaz S0/0/1 | **R2(config-if)#int s0/0/1**<br>**R2(config-if)#description Connection to R3**<br>**R2(config-if)#ip address 172.16.2.2 255.255.255.252**<br>**R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64**<br>**R2(config-if)#clock rate 128000**<br>**R2(config-if)#no shutdown**<br>%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down |

| | |
|---|---|
| Interfaz G0/0 (simulación de Internet) | **R2(config-if)#int g0/0**<br>**R2(config-if)#description Connection to Internet**<br>**R2(config-if)#ip address 209.165.200.233 255.255.255.248**<br>**R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64**<br>**R2(config-if)#no shutdown**<br><br>R2(config-if)#<br>%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up<br><br>%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up |
| Interfaz loopback 0 (servidor web simulado) | **R2(config-if)#int loopback 0**<br>R2(config-if)#<br>%LINK-5-CHANGED: Interface Loopback0, changed state to up<br>%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up<br>**R2(config-if)#description servidor web simulado**<br>**R2(config-if)#ip address 10.10.10.10 255.255.255.255**<br>**R2(config-if)#no shutdown** |
| Ruta predeterminada | **R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0**<br>%Default route without gateway, if not a point-to-point interface, may impact performance<br>R2(config)#ipv6 unicast-routing<br>**R2(config)#ipv6 route ::/0 g0/0** |

*Tabla 6.Configurar R2.*

**Verificación de tabla de enrutamiento R2**

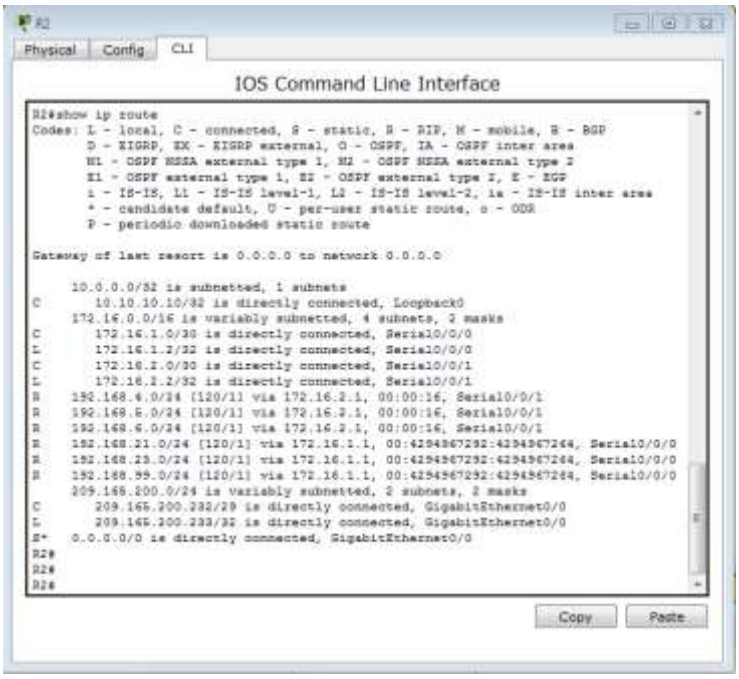


*Figura 4. Verificación de tabla de enrutamiento IPV4 en R2*

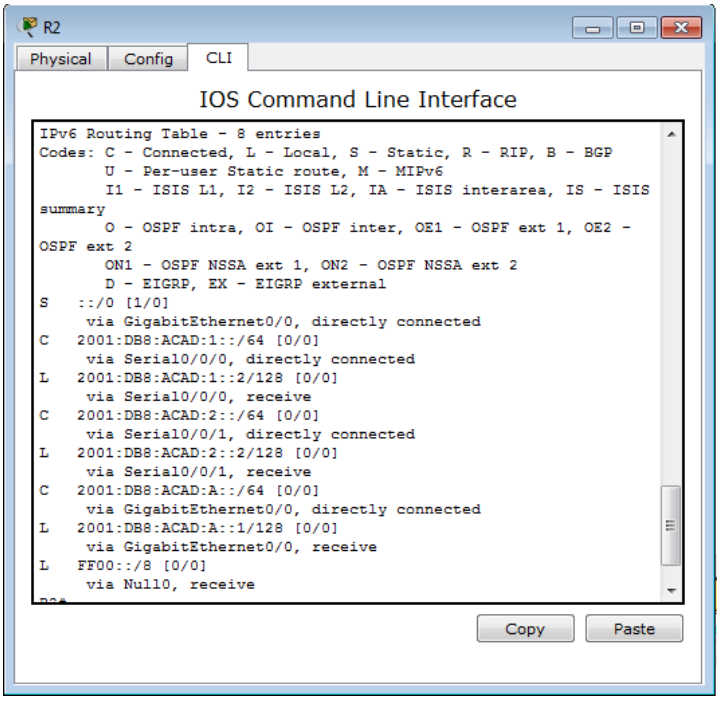


*Figura 5.Tabla de enrutamiento IPV6 en R2..*

**Análisis de resultados R2:** En la tabla de enrutamiento se pueden evidenciar que todas las rutas están configuradas correctamente incluyendo la ruta predeterminada.

### 1.2.4 Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | **Router(config)#no ip domain-lookup** |
| Nombre del router | **Router(config)#hostname R3** |
| Contraseña de exec privilegiado cifrada | **R3(config)#enable secret class** |
| Contraseña de acceso a la consola | **R3(config)#line console 0**<br>**R3(config-line)#password cisco**<br>**R3(config-line)#login** |
| Contraseña de acceso Telnet | **R3(config-line)#line vty 0 15**<br>**R3(config-line)#password cisco**<br>**R3(config-line)#login** |
| Cifrar las contraseñas de texto no cifrado | **R3(config-line)#service password-encryption** |
| Mensaje MOTD | **R3(config)#banner motd #Se prohibe el acceso no autorizado.#** |
| Interfaz S0/0/1 | **R3(config)#int s0/0/1**<br>**R3(config-if)#Description Connection to R2**<br>**R3(config-if)#ip address 172.16.2.1 255.255.255.252**<br>**R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64**<br>**R3(config-if)#no shutdown**<br><br>**R3(config-if)#**<br>%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up<br><br>%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up |

| | |
|---|---|
| Interfaz loopback 4 | **R3(config-if)#int loopback 4**<br>%LINK-5-CHANGED: Interface Loopback4, changed state to up<br><br>%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up<br>**R3(config-if)#ip address 192.168.4.1 255.255.255.0** |
| Interfaz loopback 5 | **R3(config-if)#int loopback 5**<br>R3(config-if)#<br>%LINK-5-CHANGED: Interface Loopback5, changed state to up<br><br>%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up<br><br>**R3(config-if)#ip address 192.168.5.1 255.255.255.0** |
| Interfaz loopback 6 | **R3(config-if)#int loopback 6**<br><br>**R3(config-if)#**<br>%LINK-5-CHANGED: Interface Loopback6, changed state to up<br><br>%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up<br><br>**R3(config-if)#ip address 192.168.6.1 255.255.255.0** |
| Interfaz loopback 7 | **R3(config-if)#int loopback 7**<br>R3(config-if)#<br>%LINK-5-CHANGED: Interface Loopback7, changed state to up<br>%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up<br>**R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64** |

| | |
|---|---|
| Rutas predeterminadas | **R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64**<br>**R3(config-if)#EXIT**<br>**R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1**<br>%Default route without gateway, if not a point-to-point interface, may impact performance<br>**R3(config)**#ipv6 unicast-routing<br>**R3(config)#ipv6 route ::/0 s0/0/1** |

*Tabla 7. Configurar R3.*

## Verificación de tabla de enrutamiento R3

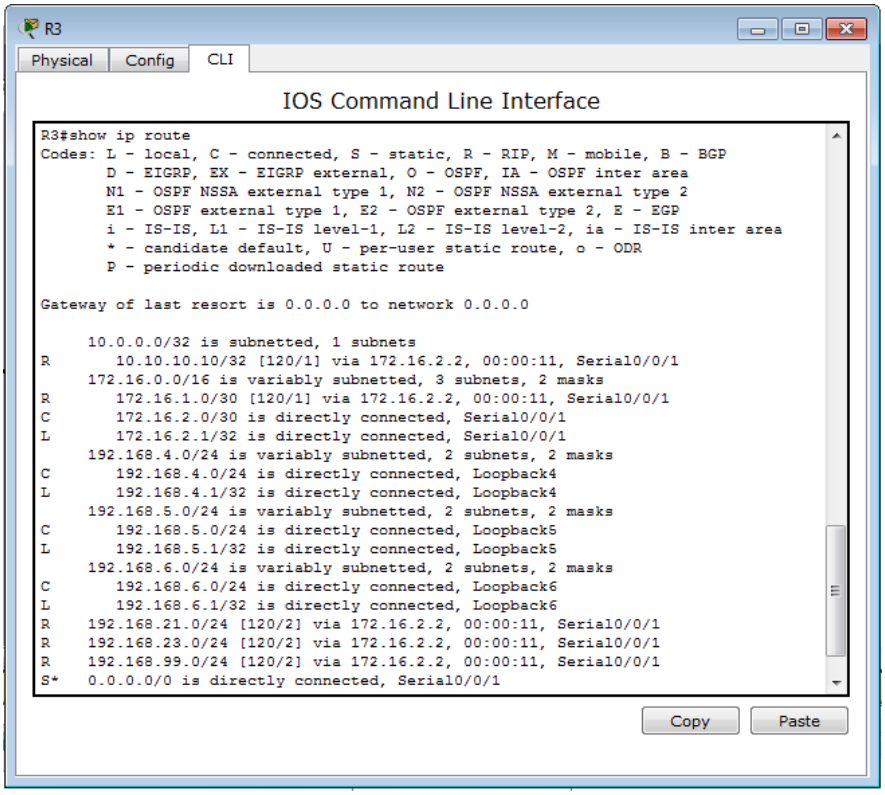


*Figura 6.Verificación tabla de enrutamiento IPV4 en R3.*

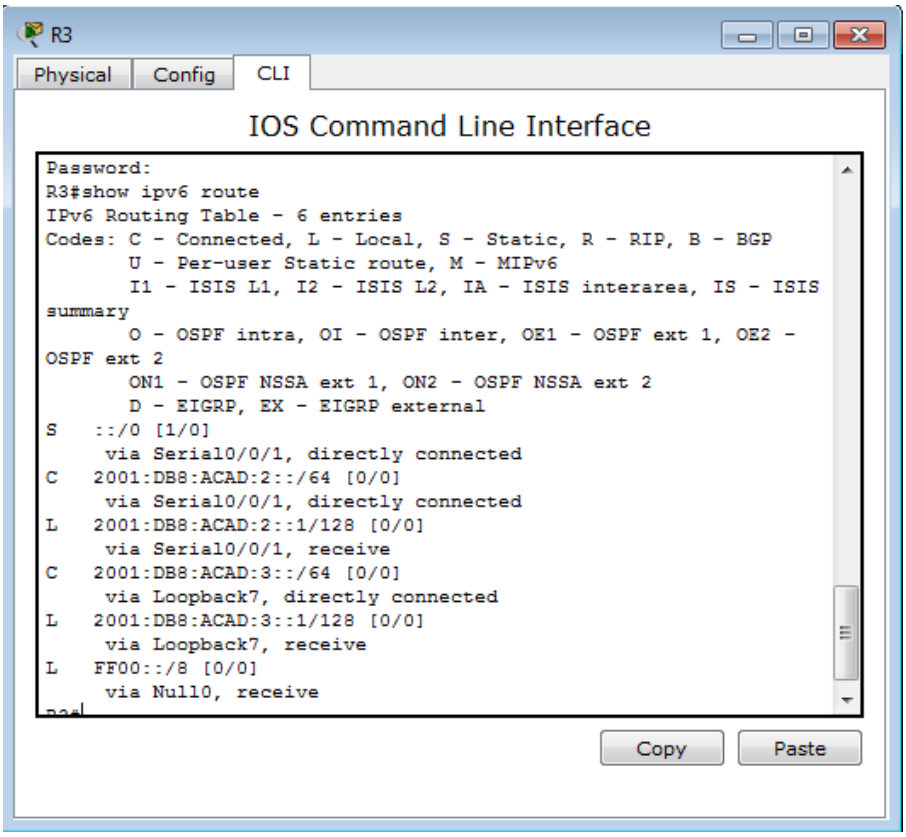


*Figura 7.Tabla de enrutamiento IPV6 en R3.*

**Análisis de resultados R3:** En la tabla de enrutamiento se pueden evidenciar que todas las rutas están configuradas correctamente incluyendo la ruta predeterminada que permite la salida a internet.

### 1.2.5 Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | Switch>en<br>Switch#config t<br>Enter configuration commands, one per line.<br>End with CNTL/Z.<br>**Switch(config)#no ip domain-lookup** |
| Nombre del switch | **Switch(config)#hostname S1** |

| | |
|---|---|
| Contraseña de exec privilegiado cifrada | **S1(config)#enable secret class** |
| Contraseña de acceso a la consola | **S1(config)#line console 0**<br>**S1(config-line)#password cisco**<br>**S1(config-line)#login** |
| Contraseña de acceso Telnet | **S1(config-line)#line vty 0 15**<br>**S1(config-line)#password cisco**<br>**S1(config-line)#login** |
| Cifrar las contraseñas de texto no cifrado | **S1(config-line)#service password-encryption** |
| Mensaje MOTD | **S1(config)#banner motd #Se prohibe el acceso no autorizado.#** |

*Tabla 8. Configurar S1*

### 1.2.6 Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | **Switch(config)#no ip domain-lookup** |
| Nombre del switch | **Switch(config)#hostname S3** |
| Contraseña de exec privilegiado cifrada | **S3(config)#enable secret class** |
| Contraseña de acceso a la consola | **S3(config)#line console 0**<br>**S3(config-line)#password cisco**<br>**S3(config-line)#login** |
| Contraseña de acceso Telnet | **S3(config-line)#line vty 0 15**<br>**S3(config-line)#password cisco**<br>**S3(config-line)#login** |
| Cifrar las contraseñas de texto no cifrado | **S3(config-line)#service password-encryption** |
| Mensaje MOTD | **S3(config-line)# banner motd #Se prohibe el acceso no autorizado.#** |

*Tabla 9. Configurar el S3.*

### 1.2.7 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:

| Desde | A | Dirección IP | Resultados de ping |
|---|---|---|---|
| R1 | R2, S0/0/0 | 172.16.1.2 | Success rate is 100 percent (5/5), round-trip min/avg/max = 5/20/77 ms |
| R2 | R3, S0/0/1 | 172.16.2.2 | Success rate is 100 percent (5/5), round-trip min/avg/max = 10/12/15 ms |
| PC de Internet | Gateway predeterminado | 209.165.200.233 | Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 11ms, Average = 2ms |

*Tabla 10. Verificar la conectividad de la red*

**Verificación mediante ping**

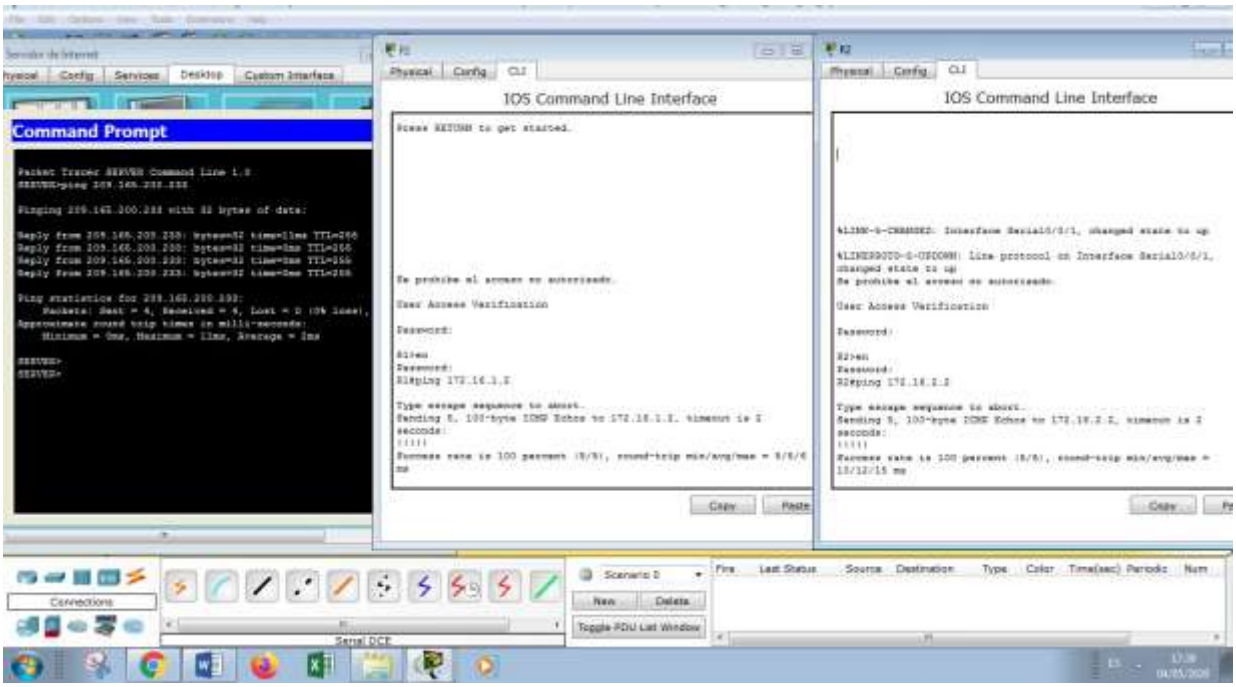


*Figura 8. Verificación de conectividad Servidor de Internet, R1 y R2*

**Análisis de resultados R2:** En la imagen se pueden evidenciar que todas las conexiones son satisfactorias.

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

### 1.3.1 Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear la base de datos de VLAN | **S1(config)#vlan 21**<br>**S1(config-vlan)#name Contabilidad**<br>**S1(config-vlan)#vlan 23**<br>**S1(config-vlan)#name Ingenieria**<br>**S1(config-vlan)#vlan 99**<br>**S1(config-vlan)#name Administración** |

| | |
|---|---|
| Asignar la dirección IP de administración. | **S1(config)#int vlan 99**<br>S1(config-if)#<br>%LINK-5-CHANGED: Interface Vlan99, changed state to up<br>**S1(config-if)#ip address 192.168.99.2 255.255.255.0**<br>S1(config-if)#no shutdown |
| Asignar el gateway predeterminado | **S1(config)#ip default-gateway 192.168.99.1** |
| Forzar el enlace troncal en la interfaz F0/3 | **S1(config)#int f0/3**<br>**S1(config-if)#switchport mode trunk**<br>**S1(config-if)#**<br>%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down<br>%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up<br>%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up<br>**S1(config-if)#switchport trunk native vlan 1** |
| Forzar el enlace troncal en la interfaz F0/5 | **S1(config)#int f0/5**<br>**S1(config-if)#switchport mode trunk**<br>**S1(config-if)#switchport trunk native vlan 1** |
| Configurar el resto de los puertos como puertos de acceso | **S1(config)#int range f0/1-2, f0/4, f0/6-24, g0/1-2**<br>**S1(config-if-range)#switchport mode access** |
| Asignar F0/6 a la VLAN 21 | **S1(config-if-range)#int f0/6**<br>**S1(config-if)#switchport access vlan 21** |
| Apagar todos los puertos sin usar | **S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2**<br>**S1(config-if-range)#shutdown** |

*Tabla 11. Configurar VLAN en S1, enlace troncal y puertos de éste.*

### 1.3.2 Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear la base de datos de VLAN | **S3(config)#vlan 21**<br>**S3(config-vlan)#name Contabilidad**<br>**S3(config-vlan)#vlan 23**<br>**S3(config-vlan)#name Ingenieria**<br>**S3(config-vlan)#vlan 99**<br>**S3(config-vlan)#name Administracion** |
| Asignar la dirección IP de administración | **S3(config)#int vlan 99**<br>S3(config-if)#<br>%LINK-5-CHANGED: Interface Vlan99, changed state to up<br>%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up<br>**S3(config-if)#ip address 192.168.99.3 255.255.255.0**<br>**S3(config-if)#no shutdown** |
| Asignar el gateway predeterminado. | **S3(config)#ip default-gateway 192.168.99.1** |
| Forzar el enlace troncal en la interfaz F0/3 | **S3(config)#int f0/3**<br>**S3(config-if)#switchport mode trunk**<br>**S3(config-if)#switchport trunk native vlan 1** |
| Configurar el resto de los puertos como puertos de acceso | **S3(config)#int range f0/1-2, f0/4-24, g0/1-2**<br>**S3(config-if-range)#switchport mode access** |
| Asignar F0/18 a la VLAN 23 | **S3(config-if-range)#int f0/18**<br>**S3(config-if)#switchport access vlan 23** |
| Apagar todos los puertos sin usar | **S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2**<br>**S3(config-if-range)#shutdown** |

*Tabla 12. Configurar VLANS en S3, enlace troncal y puertos de éste.*

## Verificación de VLAN configuradas

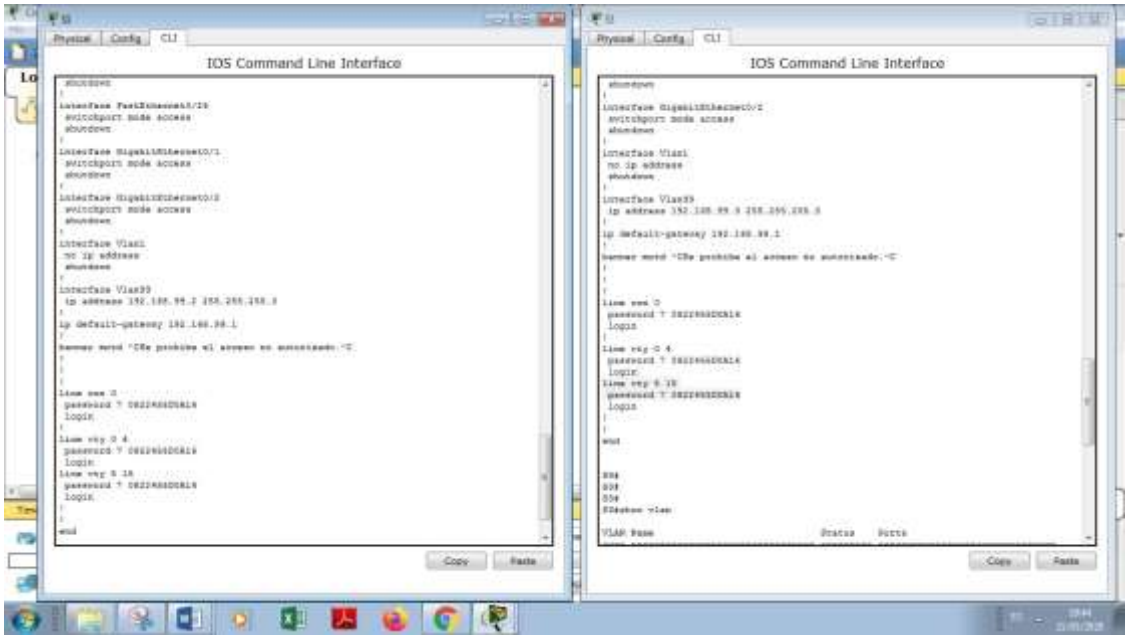


*Figura 9. Verificación de VLAN configuradas en S1 y S2*

## Verificación de asignación de vlan en S1(21 a F0/6) y S2(23 a F0/18)

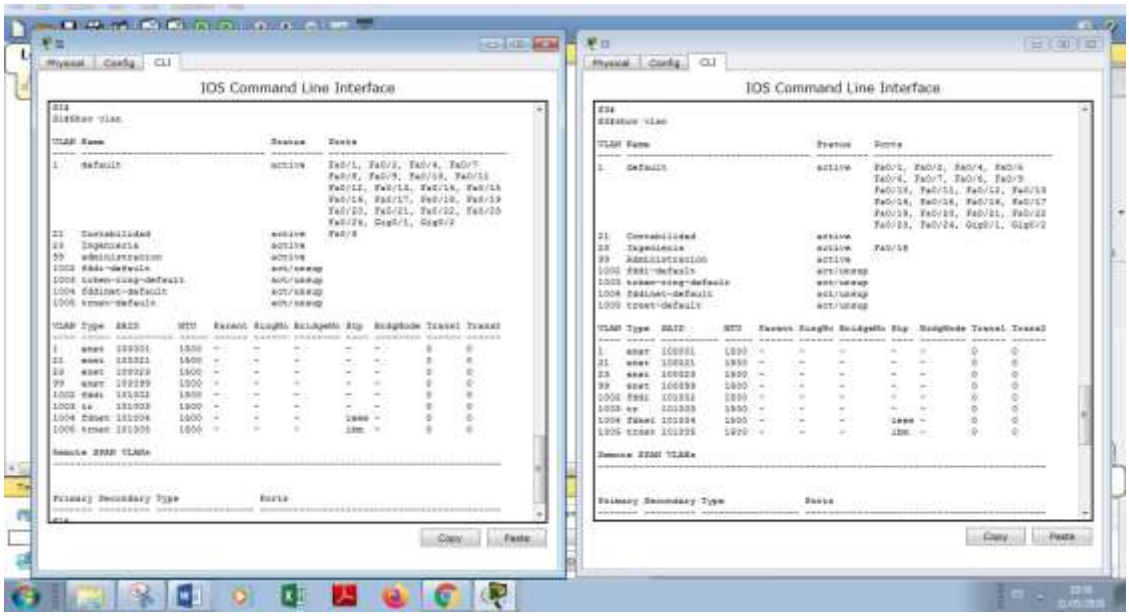


*Figura 10. Verificación de asignación de VLAN en S1 (21 a F0/6) y S3 (23 A F0/18)*

### 1.3.3 Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar la subinterfaz 802.1Q .21 en G0/1 | **R1#config t**<br>Enter configuration commands, one per line. End with CNTL/Z.<br>**R1(config)#int g0/1.21**<br>**R1(config-subif)#description LAN de Contabilidad**<br>**R1(config-subif)#encapsulation dot1q 21**<br>**R1(config-subif)#ip address 192.168.21.1 255.255.255.0** |
| Configurar la subinterfaz 802.1Q .23 en G0/1 | **R1(config-subif)#int g0/1.23**<br>**R1(config-subif)#description LAN de Ingenieria**<br>**R1(config-subif)#encapsulation dot1q 23**<br>**R1(config-subif)#ip address 192.168.23.1 255.255.255.0** |
| Configurar la subinterfaz 802.1Q .99 en G0/1 | **R1(config-subif)#int g0/1.99**<br>**R1(config-subif)#description LAN de Administracion**<br>**R1(config-subif)#encapsulation dot1q 99**<br>**R1(config-subif)#ip address 192.168.99.1 255.255.255.0** |
| Activar la interfaz G0/1 | **R1(config-subif)#int g0/1**<br>**R1(config-if)#no shutdown** |

*Tabla 13. Configurar subinterfaces en R1 y activar G0/1.*

### 1.3.4 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:

| Desde | A | Dirección IP | Resultados de ping |
|---|---|---|---|
| S1 | R1, dirección VLAN 99 | 192.168.99.1 | Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms |
| S3 | R1, dirección VLAN 99 | 192.168.99.1 | Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms |
| S1 | R1, dirección VLAN 21 | 192.168.21.1 | Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms |
| S3 | R1, dirección VLAN 23 | 192.168.23.1 | Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms |

*Tabla 14. Verificar la conectividad de la red*

## Comprobación de conexiones S3 a R1 y S1 a R1

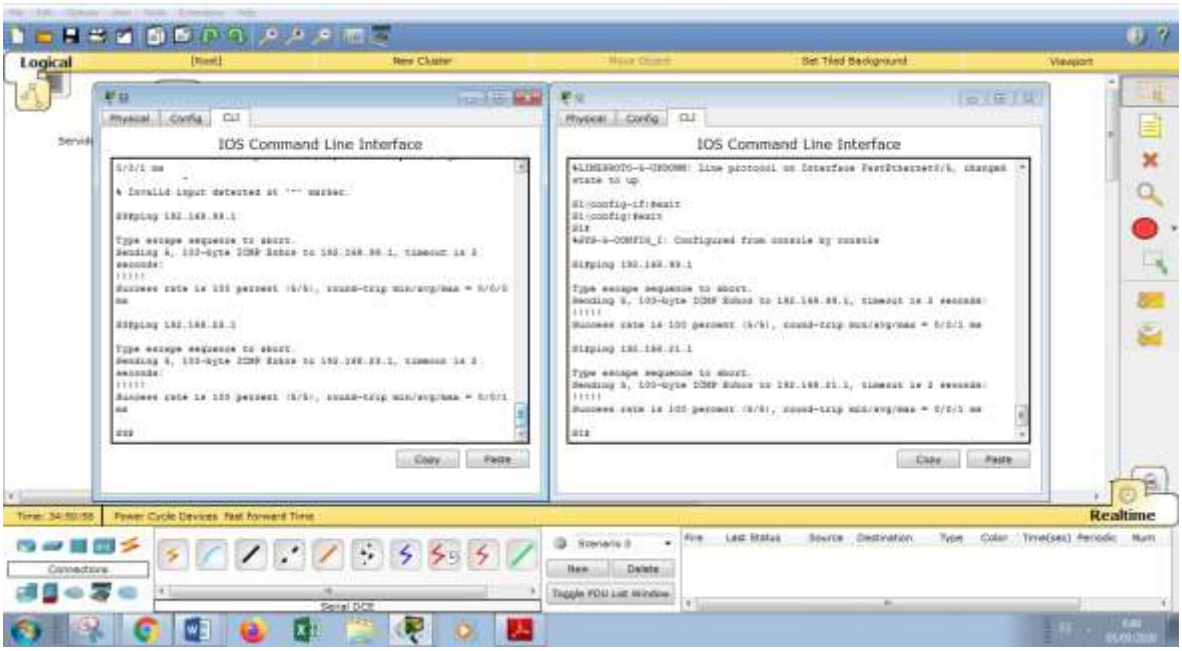


*Figura 11. Comprobación de conexiones S3 a R1 y S1 a R1*

## 1.4 Parte 4: Configurar el protocolo de routing dinámico RIPv2

### 1.4.1 Paso1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar RIP versión 2 | R1#config t<br>Enter configuration commands, one per line. End with CNTL/Z.<br>**R1(config)#router rip**<br>**R1(config-router)#version 2** |
| Anunciar las redes conectadas directamente | **R1(config-router)#do show ip route connected**<br>C 172.16.1.0/30 is directly connected, Serial0/0/0<br>C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21<br>C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23<br>C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99<br>**R1(config-router)#network 172.16.1.0**<br>**R1(config-router)#network 192.168.21.0**<br>**R1(config-router)#network 192.168.23.0**<br>**R1(config-router)#network 192.168.99.0** |
| Establecer todas las interfaces LAN como pasivas | **R1(config-router)#passive-interface g0/1.21**<br>**R1(config-router)#passive-interface g0/1.23**<br>**R1(config-router)#passive-interface g0/1.99** |
| Desactive la sumarización automática | **R1(config-router)#no auto-summary** |

*Tabla 15. Configurar RIPv2 en el R1 y desactivar la sumarización automatica*

### 1.4.2 Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar RIP versión 2 | **R2(config)#router rip**<br>**R2(config-router)#version 2** |
| Anunciar las redes conectadas directamente | **R2(config-router)#do show ip route connected**<br>C 10.10.10.10/32 is directly connected, Loopback0<br>C 172.16.1.0/30 is directly connected, Serial0/0/0<br>C 172.16.2.0/30 is directly connected, Serial0/0/1<br>C 209.165.200.232/29 is directly connected, GigabitEthernet0/0<br>**R2(config-router)#network 10.10.10.10**<br>**R2(config-router)#network 172.16.1.0**<br>**R2(config-router)#network 172.16.2.0** |
| Establecer la interfaz LAN (loopback) como pasiva | **R2(config-router)#passive-interface loopback 0** |
| Desactive la sumarización automática. | **R2(config-router)#no auto-summary** |

*Tabla 16. Configurar RIPv2 en el R2 y desactivar el resumen automática.*

### 1.4.1 Paso 3: Configurar RIPv2 en el R3

La configuración del R3 incluye las siguientes tareas:

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar RIP versión 2 | **R3(config)#router rip**<br>**R3(config-router)#version 2** |
| Anunciar redes IPv4 conectadas directamente | **R3(config-router)#do show ip route connected**<br>C 172.16.2.0/30 is directly connected, Serial0/0/1<br>C 192.168.4.0/24 is directly connected, Loopback4<br>C 192.168.5.0/24 is directly connected, Loopback5<br>C 192.168.6.0/24 is directly connected, Loopback6<br>**R3(config-router)#network 172.16.2.0**<br>**R3(config-router)#network 192.168.4.0**<br>**R3(config-router)#network 192.168.5.0**<br>**R3(config-router)#network 192.168.6.0** |
| Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas | **R3(config-router)#passive-interface loopback 4**<br>**R3(config-router)#passive-interface loopback 5**<br>**R3(config-router)#passive-interface loopback 6** |
| Desactive la sumarización automática. | **R3(config-router)#no auto-summary** |

*Tabla 17.Configurar RIPv2 en el R3 y descativar la sumarización automática*

### 1.4.2 Parte 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:

| 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? | **R1#show ip protocols** |
| ¿Qué comando muestra solo las rutas RIP? | **R2#show ip route rip** |
| ¿Qué comando muestra la sección de RIP de la configuración en ejecución? | **R1#show running-config \| section router rip**<br>% Invalid input detected at '^' marker.<br>Comando no soportado por PACKET TRACER, se debe usar<br>Usar **show run** |

*Tabla 18. Verificar la información de RIP a través de comandos.*

**Verificación del comando show ip protocols en R1, R2 y R3**

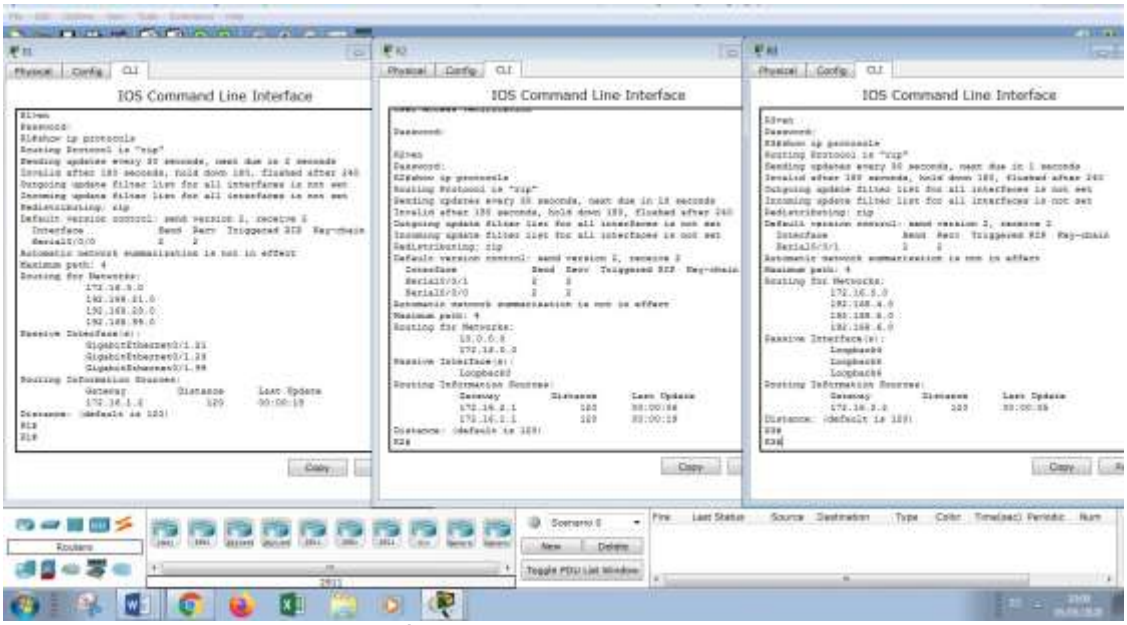


*Figura 12. Verificación del comando show ip protocols en R1, R2 y R3.*

## Verificación del comando show ip route rip R1, R2 y R3

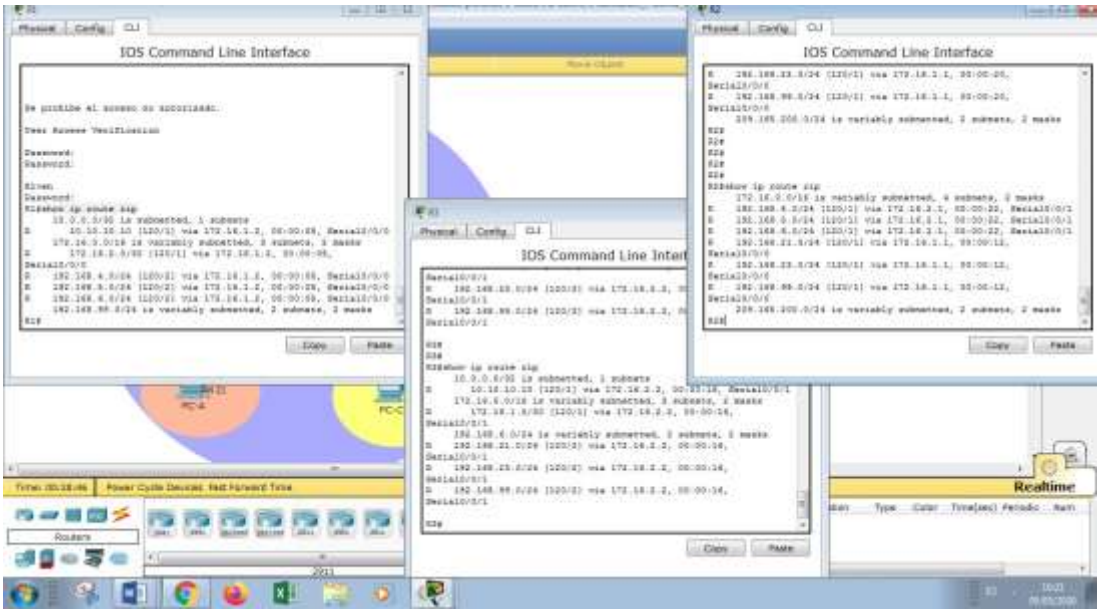


*Figura 13. Verificación del comando show ip route rip R1, R2 y R3*

## Verificación del protocolo RIPv2 a través del comando show run R1, R2 y R3

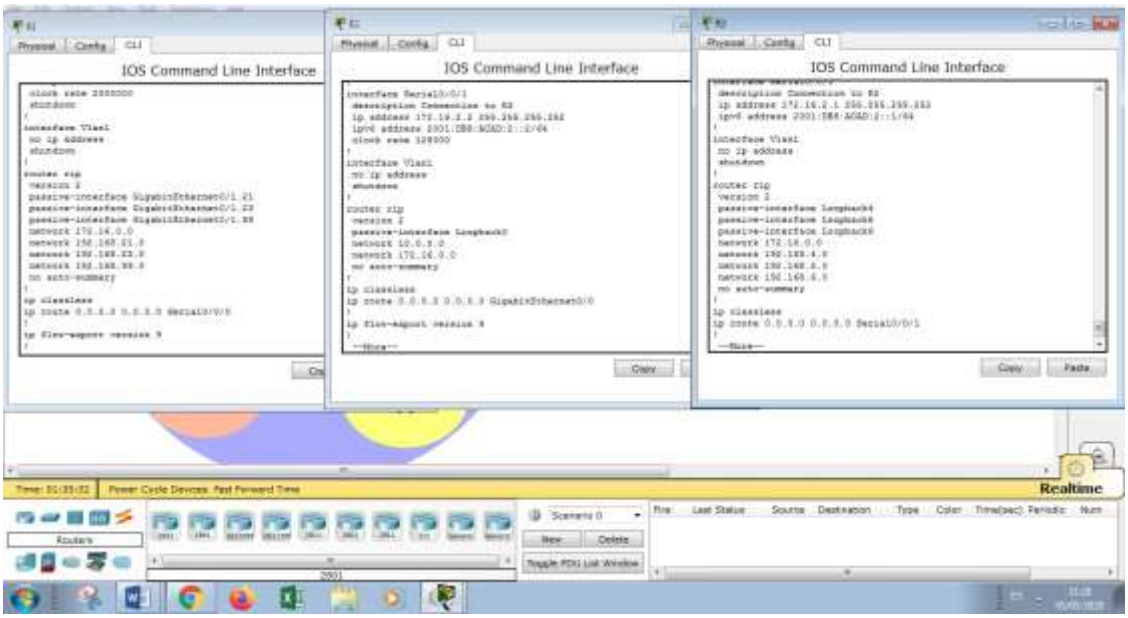


*Figura 14. Verificación del protocolo RIPv2 a través del comando show run R1, R2 y R3.*

## 1.5 Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

| Elemento o tarea de configuración | Especificación |
|---|---|
| Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas | **R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20** |
| Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas | **R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20** |
| Crear un pool de DHCP para la VLAN 21. | **R1(config)#ip dhcp pool ACCT**<br>**R1(dhcp-config)#network 192.168.21.0 255.255.255.0**<br>**R1(dhcp-config)#default-router 192.168.21.1**<br>**R1(dhcp-config)#dns-server 10.10.10.10**<br>**R1(dhcp-config)#domain-name ccna-sa.com**<br>**^**<br>% Invalid input detected at '^' marker.<br>**Nota:** El comando **domain-name** no está soportado por Packet Tracer 6.3. |
| Crear un pool de DHCP para la VLAN 23 | **R1(dhcp-config)#ip dhcp pool ENGNR**<br>**R1(dhcp-config)#network 192.168.23.0 255.255.255.0**<br>**R1(dhcp-config)#dns-server 10.10.10.10**<br>**R1(dhcp-config)#domain-name ccna-sa.com**<br>**^**<br>% Invalid input detected at '^' marker.<br>**Nota:** El comando **domain-name** no está soportado por Packet Tracer 6.3. |

*Tabla 19. Implementar DHCP y NAT para IPv4.*

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

La configuración del R2 incluye las siguientes tareas:

| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear una base de datos local con una cuenta de usuario | **R2(config)#username webuser privilege 15 secret cisco12345** |
| Habilitar el servicio del servidor HTTP | **R2(config)#ip http server**<br>^<br>% Invalid input detected at '^' marker.<br>**Nota. ip http server** no es soportado por Packet Tracer. |
| Configurar el servidor HTTP para utilizar la base de datos local para la autenticación | **R2(config)#ip http authentication local**<br>^<br>% Invalid input detected at '^' marker.<br>**Nota. ip http authentication local** no es soportado por Packet Tracer 6.3 |
| Crear una NAT estática al servidor web. | **R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237**<br>Dirección global interna: **209.165.200.237** |
| Asignar la interfaz interna y externa para la NAT estática | **R2(config)#int g0/0**<br>**R2(config-if)#ip nat outside**<br>**R2(config-if)#int s0/0/0**<br>**R2(config-if)#ip nat inside**<br>**R2(config-if)#int s0/0/1**<br>**R2(config-if)#ip nat inside** |
| Configurar la NAT dinámica dentro de una ACL privada | **R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255**<br>**R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255**<br>**R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255**<br>Lista de acceso: 1<br>Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1<br>Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 |

| | |
|---|---|
| Defina el pool de direcciones IP públicas utilizables. | **R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248**<br>Nombre del conjunto: **INTERNET**<br>El conjunto de direcciones incluye:<br>**209.165.200.233** – **209.165.200.236** |
| Definir la traducción de NAT dinámica | **R2(config)#ip nat inside source list 1 pool INTERNET** |

**Análisis de resultados: Los comandos** ip http server y **ip http authentication local** no son soportados por Packet Tracer por lo que no se puede utilizar un navegador web simulado en la computadora de Internet para acceder al servidor web (209.165.200.237) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345.** Crear una NAT estática al servidor web se usó la dirección global interna: **209.165.200.237** que estaba desocupada, recordemos que el rango de direcciones en esta red va desde la **209.165.200.233** ocupada por la G0/0 **hasta la 209.165.200.238** ocupada por el servidor de internet.

### 1.5.3 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.

| Prueba | Resultados |
|---|---|
| Verificar que la PC-A haya adquirido información de IP del servidor de DHCP | Satisfactorio |
| Verificar que la PC-C haya adquirido información de IP del servidor de DHCP | Satisfactorio |
| Verificar que la PC-A pueda hacer ping a la PC-C | Satisfactorio |

| | |
|---|---|
| Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.2237) Iniciar sesión con el nombre de usuario **webuser** y la contraseña **cisco12345** | Packet tracer no soporta este procedimiento, ya que el comando ip http server en R2 tampoco es soportado por este este software |

*Tabla 20. Verificar el protocolo DHCP y la NAT estática.*

## Verificación servidor DHCP en PC-A y PC-C

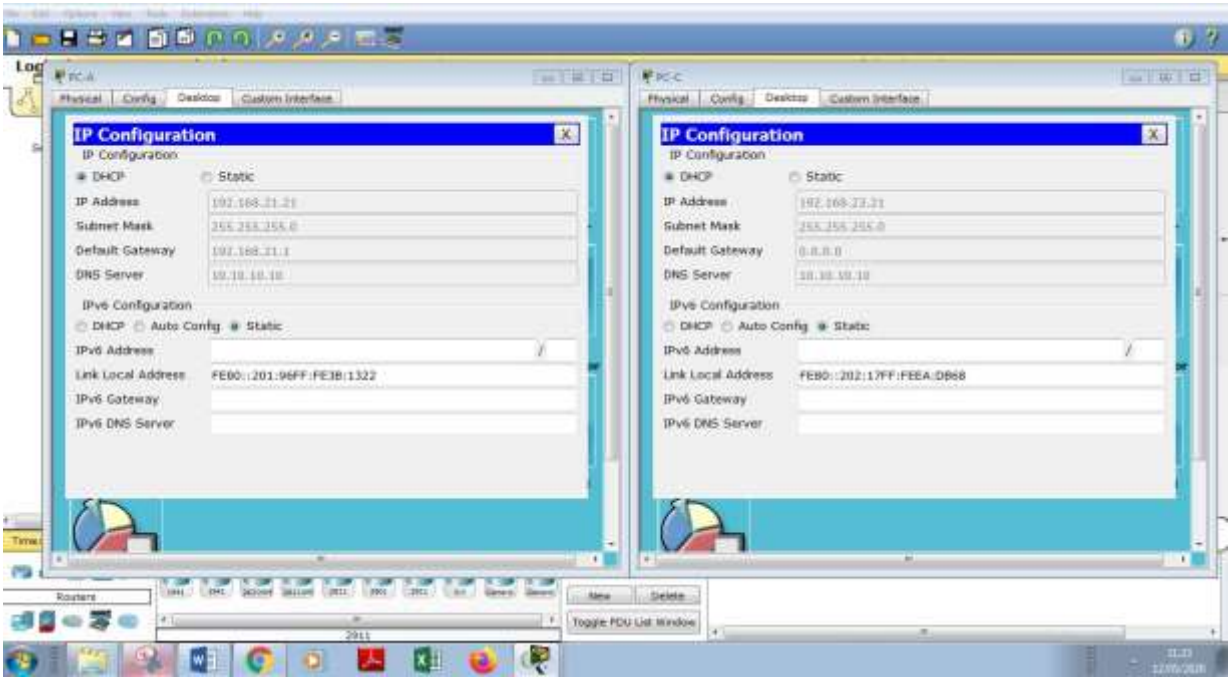


*Figura 15. Verificación servidor DHCP en PC-A y PC-C*

## Verificación Ping PC-A y PC-C

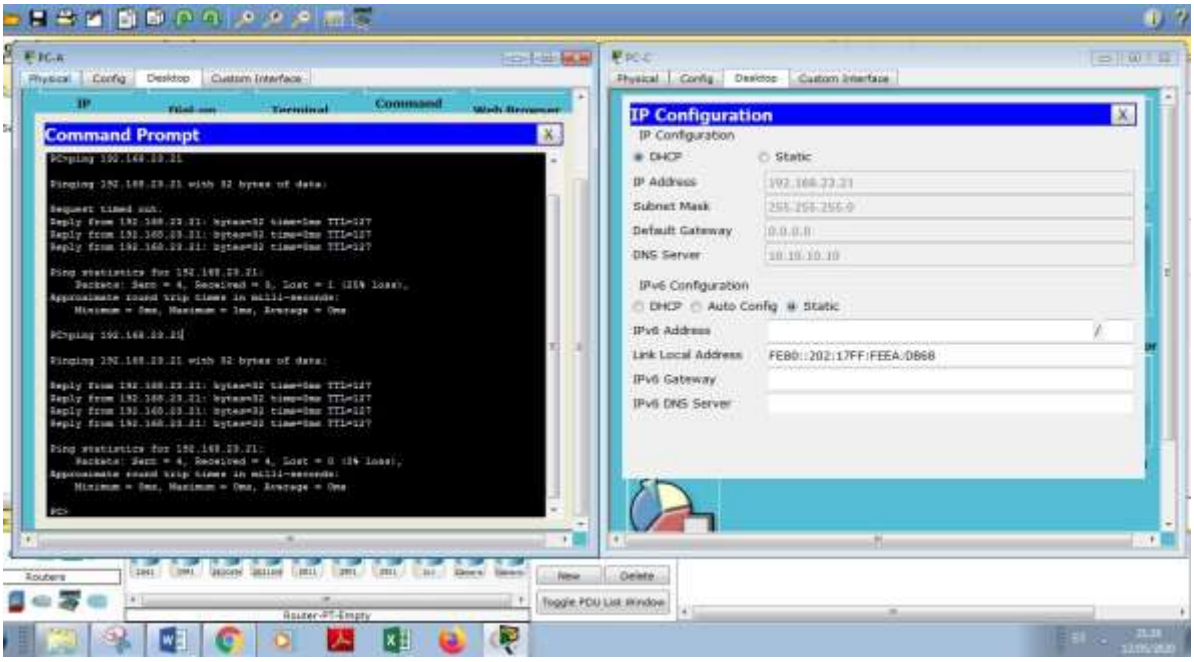


*Figura 16. Verificación Ping PC-A y PC-C*

## 1.6 Parte 6: Configurar NTP

| Elemento o tarea de configuración | Especificación |
|---|---|
| Ajuste la fecha y hora en R2. | **R2#clock set 14:25:00 may 05 2020** |
| Configure R2 como un maestro NTP. | **R2(config)#ntp master 5**<br>^<br>% Invalid input detected at '^' marker.<br>Nota. Packet Tracer 6.3 no soporta el comando **ntp master 5.** |
| Configurar R1 como un cliente NTP. | **R1(config)#ntp server 172.16.1.2** |

| | |
|---|---|
| Configure R1 para actualizaciones de calendario periódicas con hora NTP. | **R1(config)#ntp update-calendar** |
| Verifique la configuración de NTP en R1. | **R1#show ntp associations**<br>^<br>% Invalid input detected at '^' marker<br>**NOTA**. El commando **show ntp associations** no es soportado por packet Tracer. |

*Tabla 21. Configurar NTP.*

**Análisis:** Los comandos **show ntp associations y ntp master 5** no funcionan para Packet Tracer 6.3, pero para versiones más recientes si funciona.

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

### 1.7.1 Restringir el acceso a las líneas VTY en el R2

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2 | Nombre de la ACL:<br>**ADMIN-MGT**<br>**R2(config)#ip access-list standard ADMIN-MGT**<br>**R2(config-std-nacl)#permit host 172.16.1.1** |
| Aplicar la ACL con nombre a las líneas VTY | **R2(config)#line vty 0 15**<br>**R2(config-line)#access-class ADMIN-MGT in** |
| Permitir acceso por Telnet a las líneas de VTY | **R2(config-line)#transport input telnet** |

| | |
|---|---|
| Verificar que la ACL funcione como se espera | Satisfactorio<br>**R1>en**<br>**Password:**<br>**R1#telnet 172.16.1.2**<br>Trying 172.16.1.2<br>...OpenSe prohibe el acceso no autorizado.<br><br>User Access Verification<br>Password:<br>R2> |

*Tabla 22. Configurar y verificar las listas de control de acceso (ACL)*

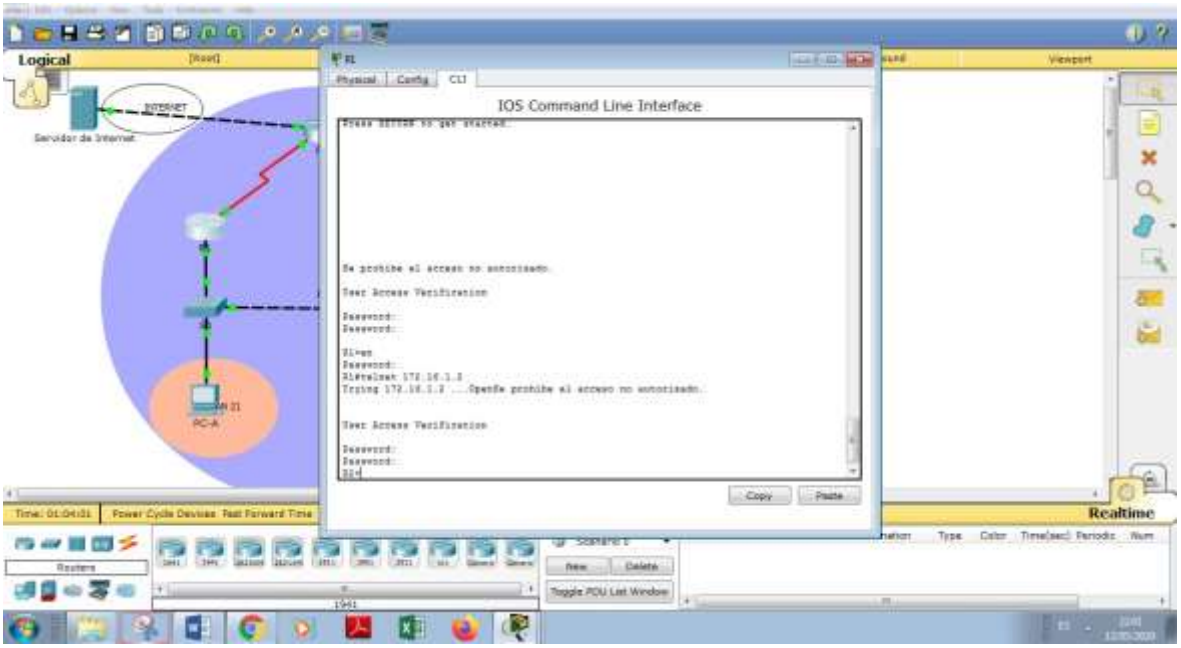


*Figura 17. Verificación del funcionamiento de Telnet en R2.*

**Introducir el comando de CLI adecuado que se necesita para mostrar lo siguiente**

| Descripción del comando | Entrada del estudiante (comando) |
|---|---|
| Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció | **R2#show access-list**<br>Standard IP access list 1<br>10 permit 192.168.21.0 0.0.0.255<br>20 permit 192.168.23.0 0.0.0.255<br>30 permit 192.168.4.0 0.0.3.255<br>Standard IP access list ADMIN-MGT<br>10 permit host 172.16.1.1 (2 match(es))<br>**R2#show ip access-list**<br>Standard IP access list 1<br>10 permit 192.168.21.0 0.0.0.255<br>20 permit 192.168.23.0 0.0.0.255<br>30 permit 192.168.4.0 0.0.3.255<br>Standard IP access list ADMIN-MGT<br>10 permit host 172.16.1.1 (2 match(es)) |
| Restablecer los contadores de una lista de acceso | **R2#clear access-list counters**<br>R2#show ip access-list<br>Standard IP access list 1<br>10 permit 192.168.21.0 0.0.0.255<br>20 permit 192.168.23.0 0.0.0.255<br>30 permit 192.168.4.0 0.0.3.255<br>Standard IP access list ADMIN-MGT<br>10 permit host 172.16.1.1 |
| ¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica? | **R2#show ip interface** |

| | |
|---|---|
| ¿Con qué comando se muestran las traducciones NAT? | **R2#show ip nat translations**<br>Pro Inside global Inside local Outside local Outside global<br>--- 209.165.200.237 10.10.10.10 --- ---<br>tcp 209.165.200.234:1025192.168.23.2:1025 209.165.200.238:80 209.165.200.238:80<br>**Nota:** Las traducciones para la PC-A y la PC-C se agregaron a la tabla cuando la computadora de Internet intentó hacer ping a esos equipos en el paso 2. Si hace ping a la computadora de Internet desde la PC-A o la PC-C, no se agregarán las traducciones a la tabla debido al modo de simulación de Internet en la red. |
| ¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas? | **R2#clear ip nat translation ***<br>R2#show ip nat translations<br>Pro Inside global Inside local Outside local Outside global<br>--- 209.165.200.237 10.10.10.10 --- --- |

*Tabla 23. Introducir commandos show access-list, clear access-list counters, R2#show ip interface, show ip nat translations y clear ip nat translation **

## Interfaz y la dirección ACL en que se aplica

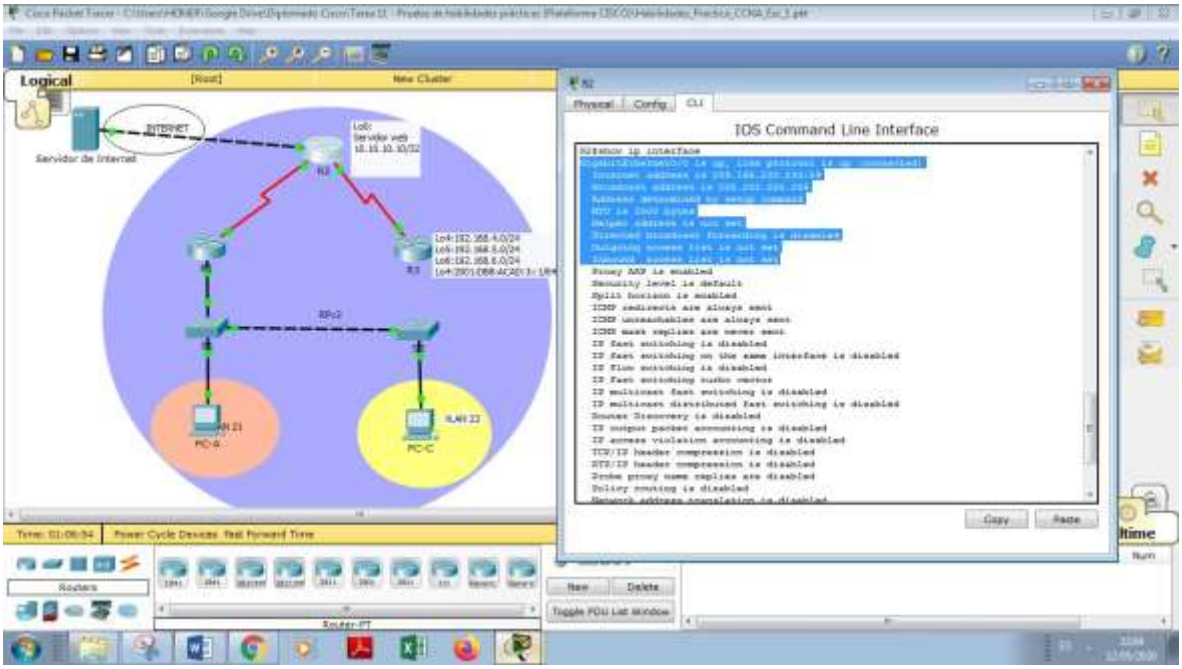


*Figura 18. Verificar Interfaz y la dirección ACL a que se aplica*

## Verificación del comando show ip nat translations

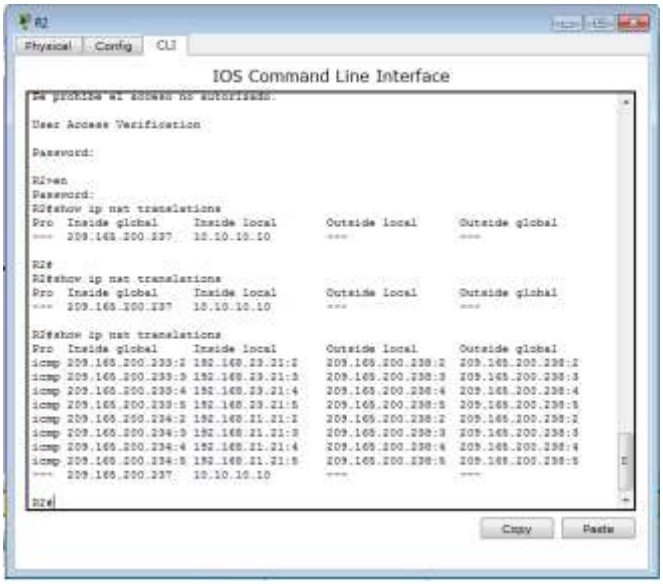


*Figura 19. Verificación del comando show ip nat translations.*

## Verificación de conexión entre PC-A y PC-C al servidor web

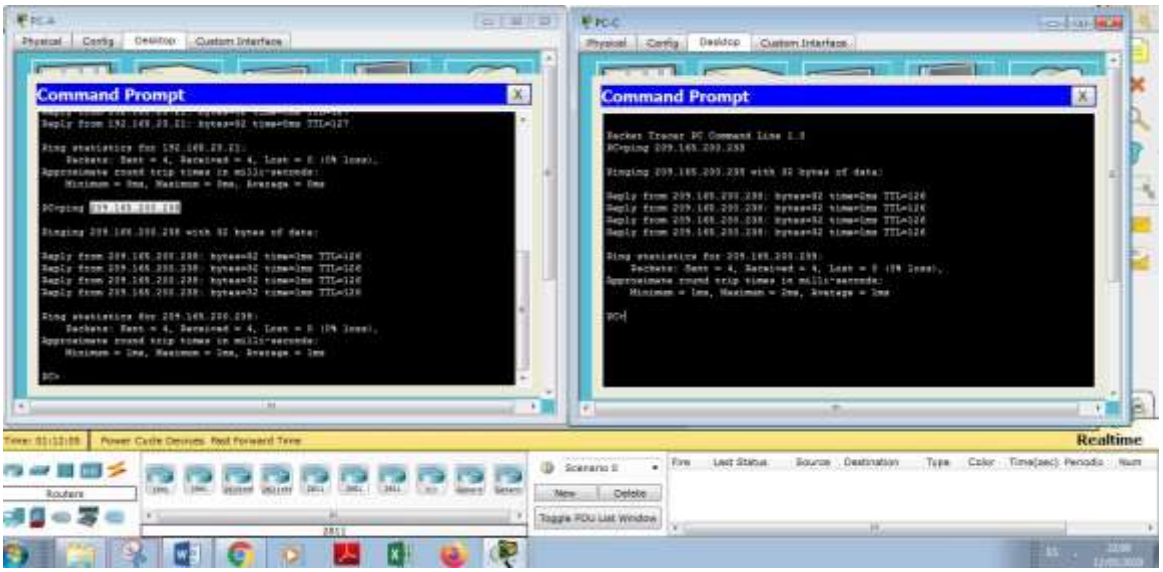


*Figura 20. Verificación de conexión entre PC-A y PC-C al servidor web desde el Command Prompt*

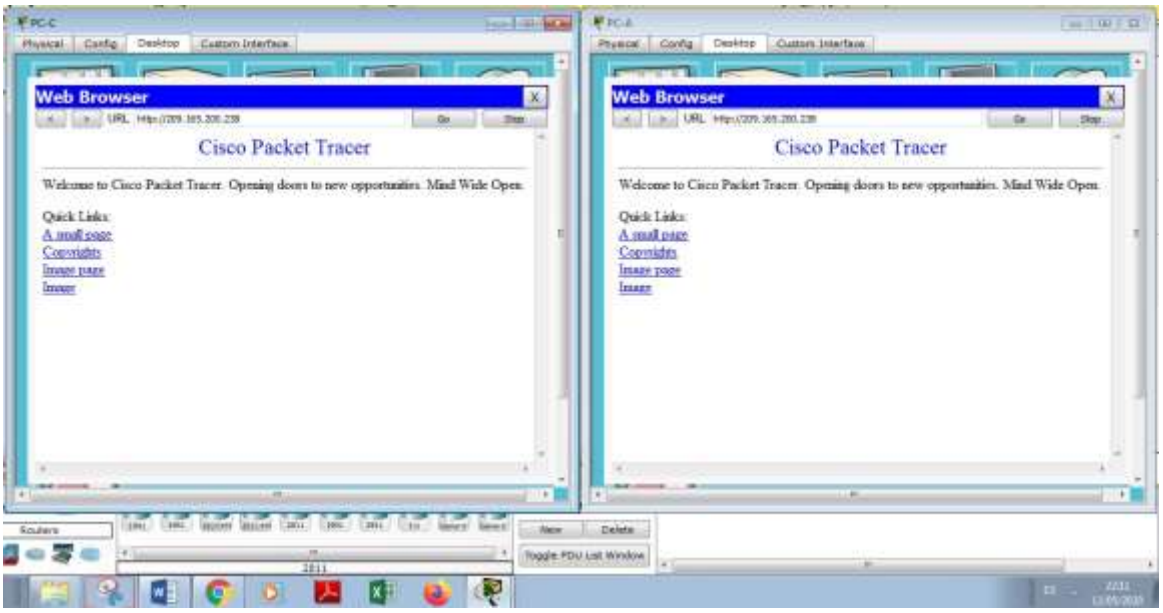


*Figura 21. Verificación de conexión entre PC-A y PC-C al servidor web desde el navegador.*

.

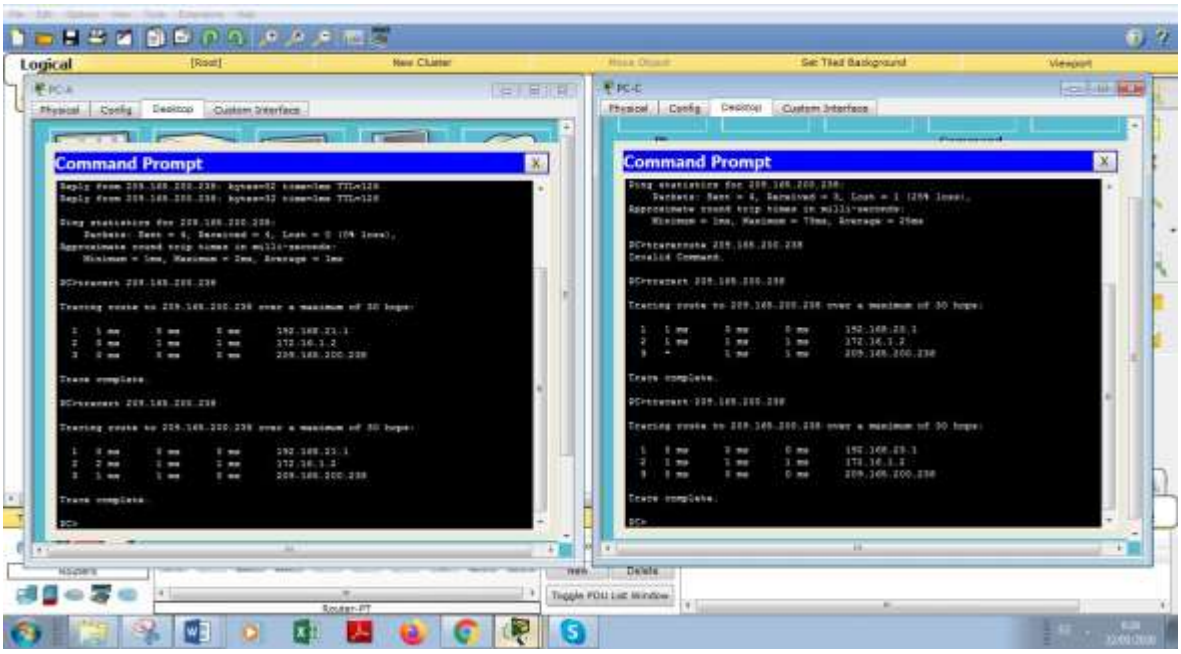


*Figura 22. Verificación de la ruta de destino de PC-A y PC-C hasta el servidor de internet a través del comando tracert.*

# 2 DESARROLLO ESCENARIO 2

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

**Topología de red**

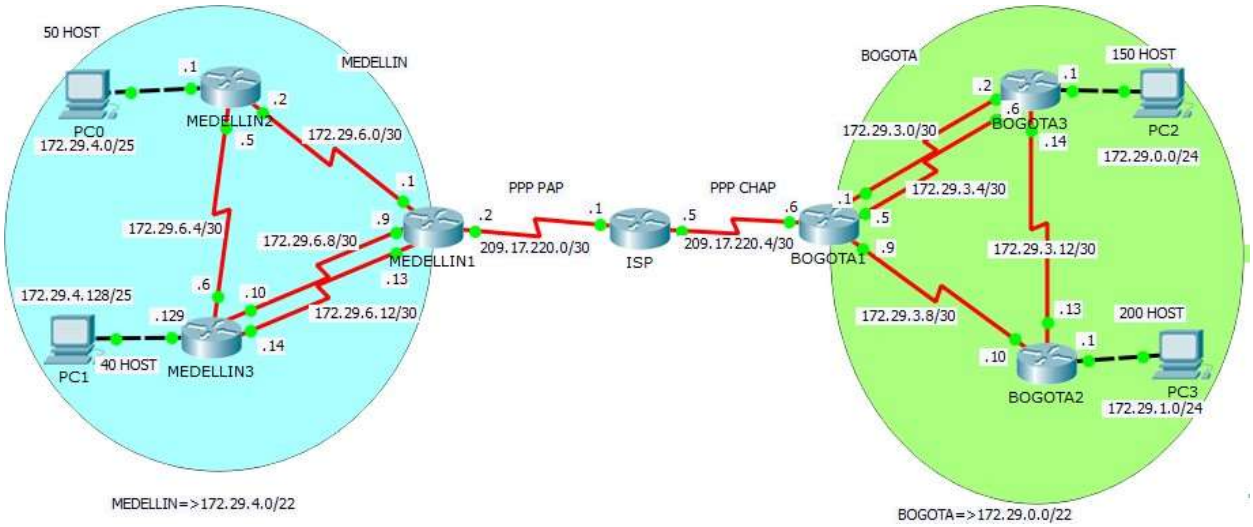


*Figura 23. Escenario de red 2*

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

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.
Debe configurar PPP en los enlaces hacia el ISP, con autenticación.
Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

**Desarrollo**

Como trabajo inicial se debe realizar lo siguiente.

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

**Rutinas de diagnotico aplicadas a todos los routers**

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #Acceso no autorizado-Heiner MADERA duarte#
line console 0
password cisco
login
line vty 0 15
password cisco
login
```

- Realizar la conexión fisica de los equipos con base en la topología de red

Configurar la topología de red, de acuerdo con las siguientes especificaciones.

**2.1 Parte 1: Configuración del enrutamiento**

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

**Configuracion OSPF versión 2 en BOGOTA1**

```
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#router-id 1.1.1.1
BOGOTA1(config-router)#passive-interface s0/0/0
BOGOTA1(config-router)#network 172.29.3.0 0.0.0.255 area 0
```

**Configuracion OSPF versión 2 en BOGOTA2**

```
BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#router-id 2.2.2.2
BOGOTA2(config-router)#passive-interface g0/0
BOGOTA2(config-router)#network 172.29.0.0 0.0.255.255 area 0
```

**Configuracion OSPF versión 2 en BOGOTA3**

```
BOGOTA3(config)#no router ospf 1
BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#router-id 3.3.3.3
BOGOTA3(config-router)#passive-interface g0/0
BOGOTA3(config-router)#network 172.29.0.0 0.0.255.255 area 0
```

**Configuracion OSPF versión 2 en MEDELLIN1**

```
MEDELLIN1(config)#router ospf 2
MEDELLIN1(config-router)#router-id 1.1.1.1
MEDELLIN1(config-router)#passive-interface s0/0/0
MEDELLIN1(config-router)#network 172.29.6.0 0.0.0.255 area 1
```

**Configuracion OSPF versión 2 en MEDELLIN2**

```
MEDELLIN2(config)#router ospf 2
MEDELLIN2(config-router)#router-id 2.2.2.2
MEDELLIN2(config-router)#passive-interface g0/0
MEDELLIN2(config-router)#network 172.29.0.0 0.0.255.255 area 1
```

**Configuracion OSPF versión 2 en MEDELLIN3**

```
MEDELLIN3(config)#router ospf 2
MEDELLIN3(config-router)#router-id 3.3.3.3
MEDELLIN3(config-router)#passive-interface g0/0
MEDELLIN3(config-router)#network 172.29.0.0 0.0.255.255 area 1
```

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

**Configuración ruta por defecto hacia el ISP y redistribución dentro de las publicaciones**

**Medellín1**

```
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
MEDELLIN1(config)#router ospf 2
MEDELLIN1(config-router)#default-information originate
```

**Bogota1**

```
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#default-information originate
```

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

```
ISP>en
ISP#config t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6
```

**2.2 Parte 2: Tabla de Enrutamiento.**

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

**b. Verificar el balanceo de carga que presentan los routers.**

**RTA/**Corresponde a los enrutadores que tienen varias trayectorias para llegar a otra red o subred como por ejemplo MEDELLIN3 tiene tres rutas para llegar a MEDELLIN2 y dos rutas para llegar a internet.

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

**RTA**/Estos dos routers estan configurados para el acceso a internet. Ellos Tambien estan configurados para redistribuir la ruta estática por defecto a lo routers que tengan adayacencia con cada uno de ellos.

**d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante OSPF. RTA/** Son las rutas que están representadas por la letra o al principio de la tabla de cada uno de los routers.

**e. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto. RTA/En la topología se pueden ver rutas que permiten la comunicación a traves de varios caminos. Ejemplo. Medellin3 a Medellin1 o Bogotá1 a Bogota2.**

**Tablas de enrutamiento Bogota**

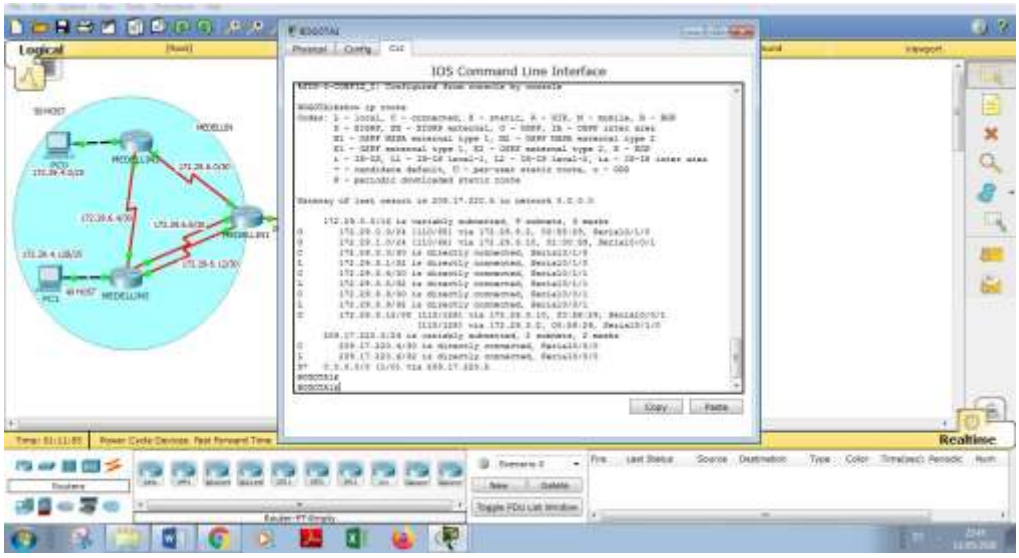


*Figura 24. Tablas de enrutamiento BOGOTA1.*

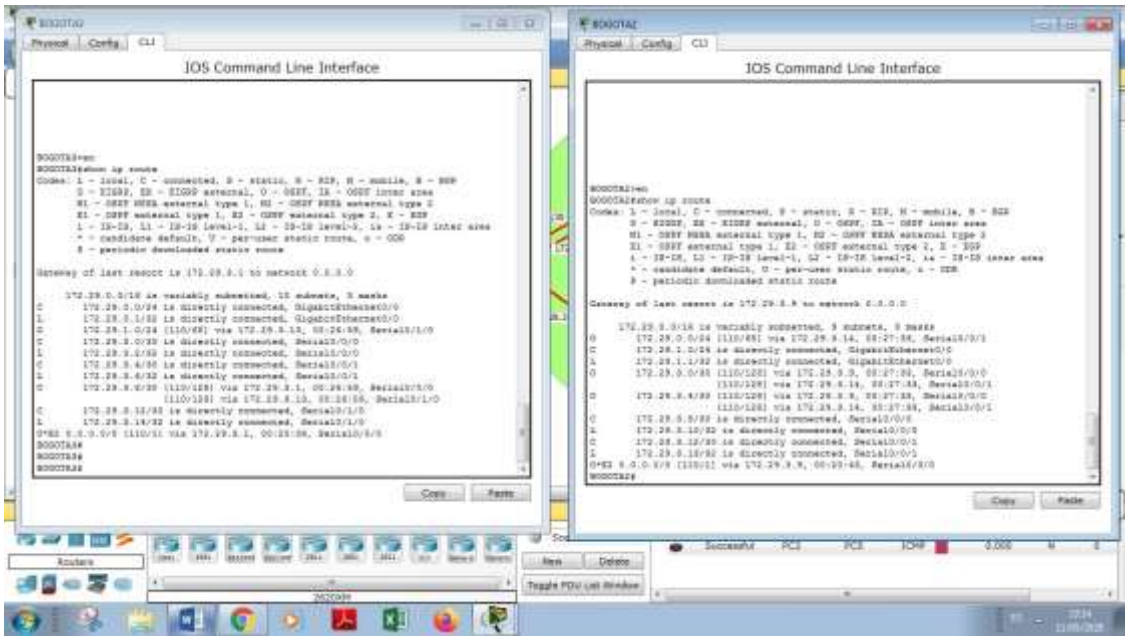


*Figura 25. Tablas de enrutamiento BOGOTA2 y BOGOTA3.*

## Tablas de enrutamiento Medellin

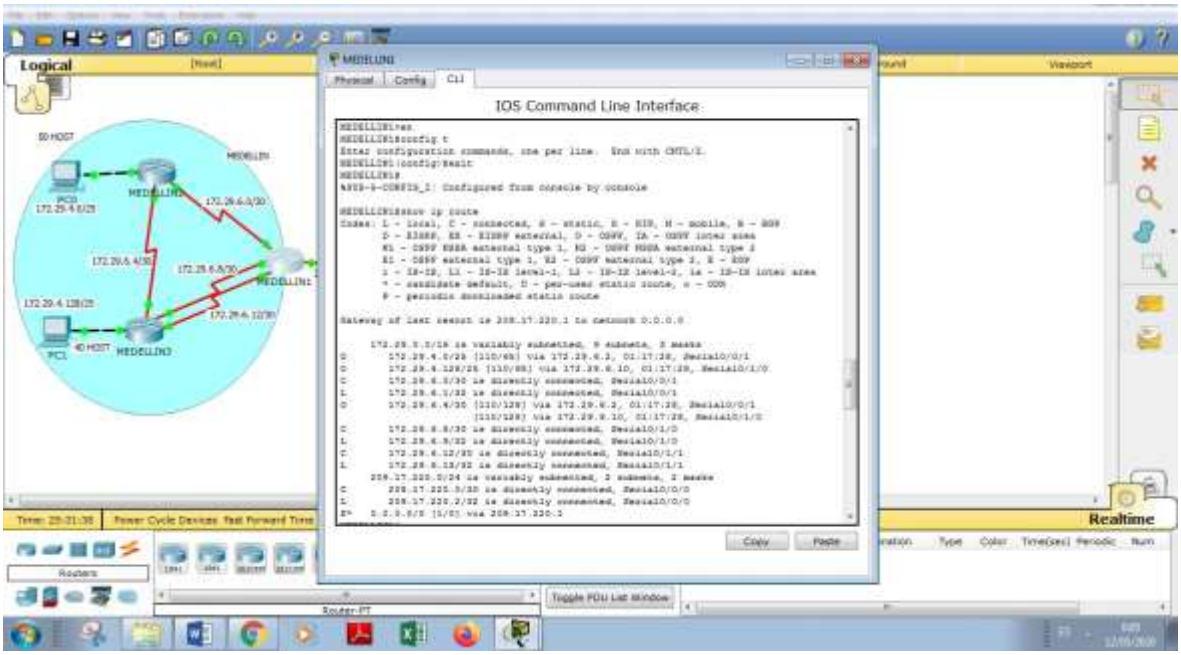


*Figura 26. Tablas de enrutamiento MEDELLIN1.*

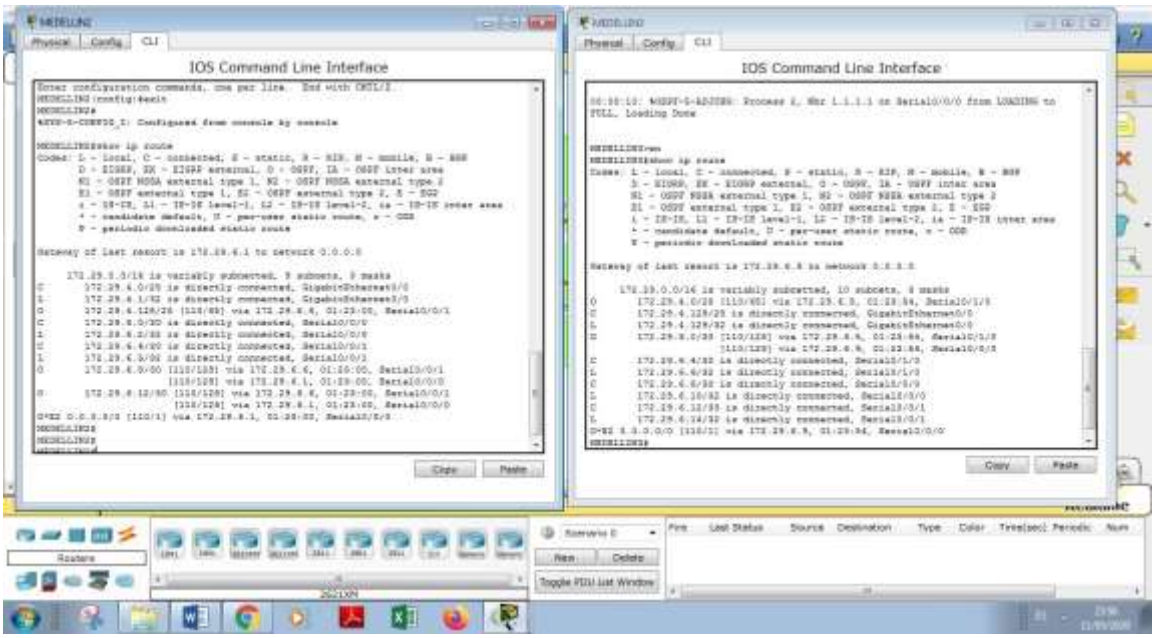


*Figura 27. Tabla de enrutamiento MEDELLIN2 y MEDELLIN3.*

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

### Tabla de enrutamiento ISP

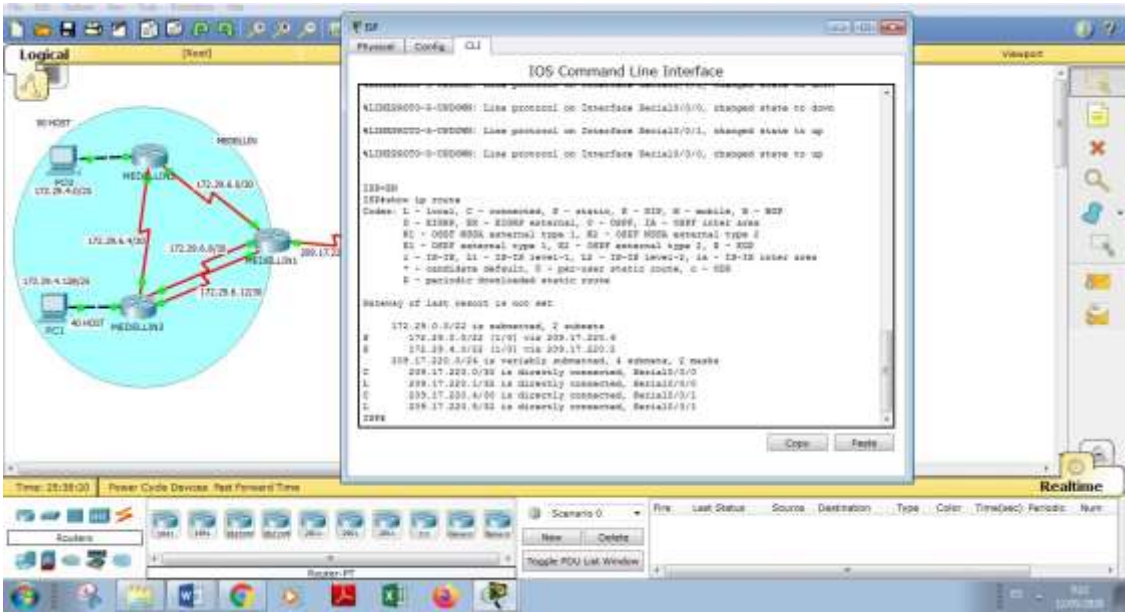


*Figura 28. Tabla de enrutamiento ISP.*

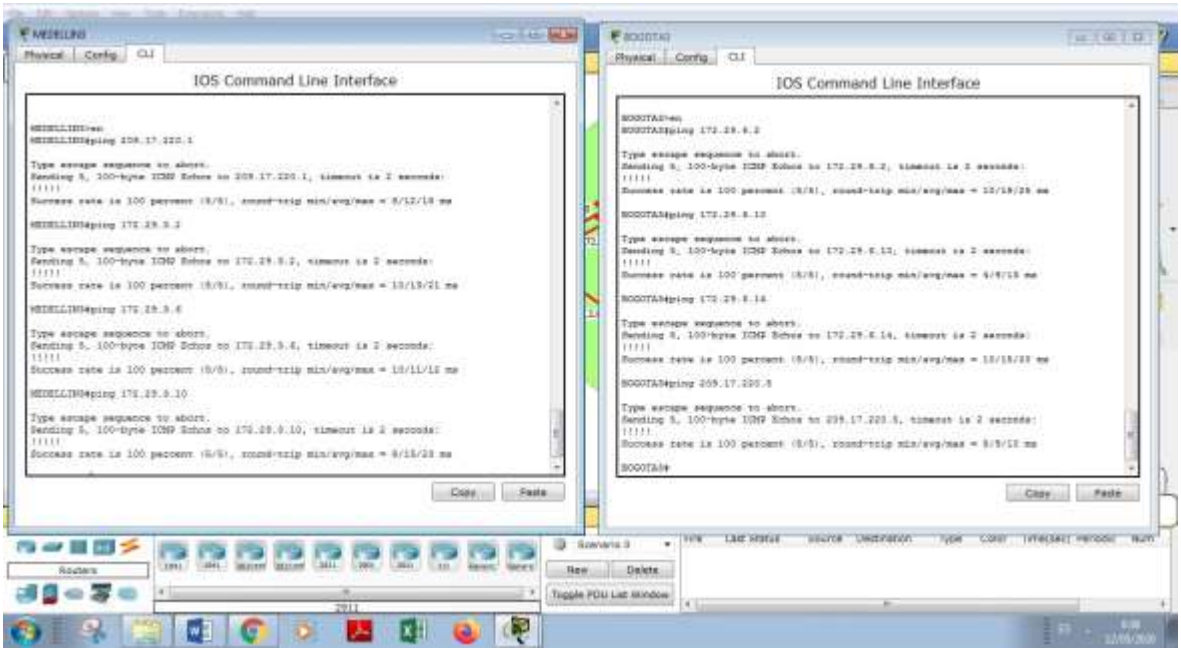


*Figura 29. Verificación de conectividad de extremo a extremo entre los Routers de Bogotá y Medellín.*

### 2.3 Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

Esta operación fue realizada en la parte 1 utilizando el comando passive-interface [ NUMERO INTERFAZ]

| 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 |

## 2.4 Parte 4: Verificación del protocolo OSPF.

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

### Bogotá

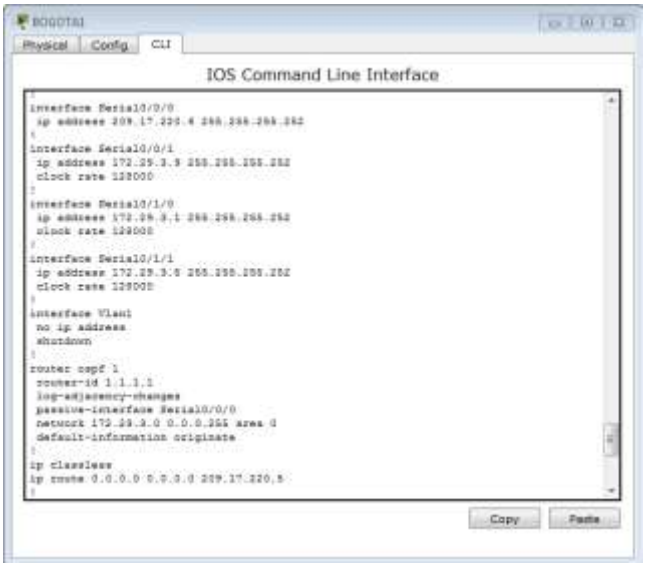


*Figura 30. Verificación del protocolo OSPF en BOGOTA1.*

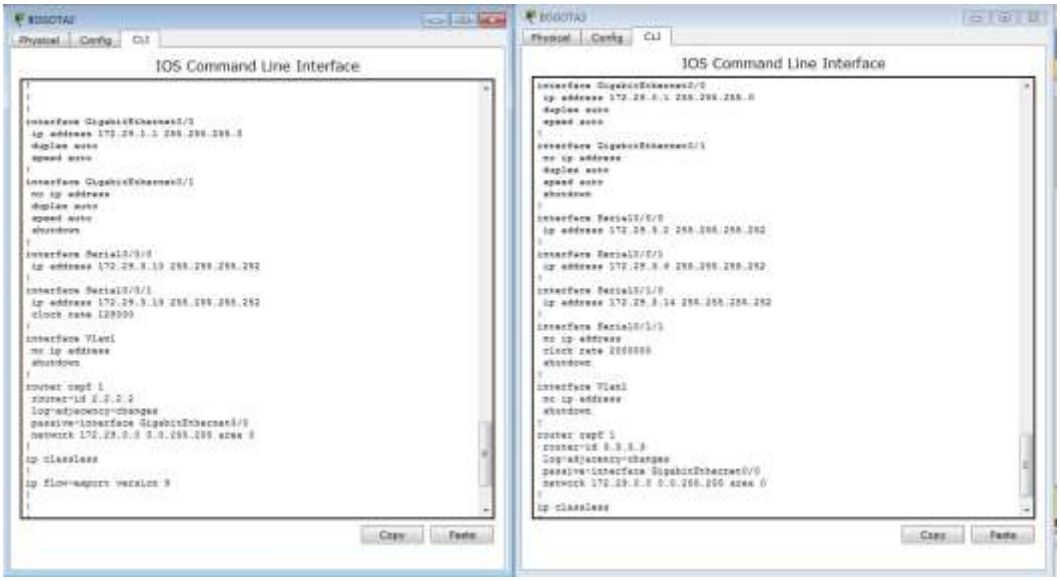


*Figura 31. Verificación del protocolo OSPF en BOGOTA2 y BOGOTA3.*

## Medellín

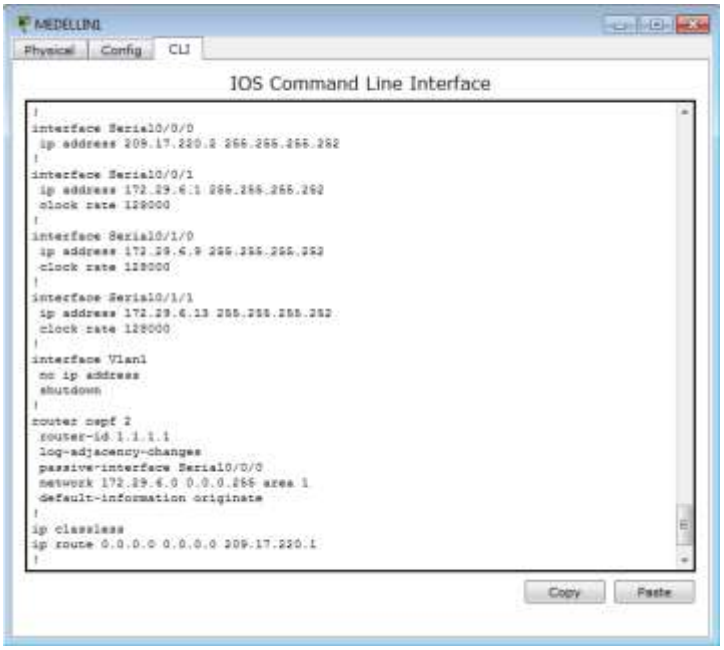


*Figura 32. Verificación del protocolo OSPF en MEDELLIN1.*

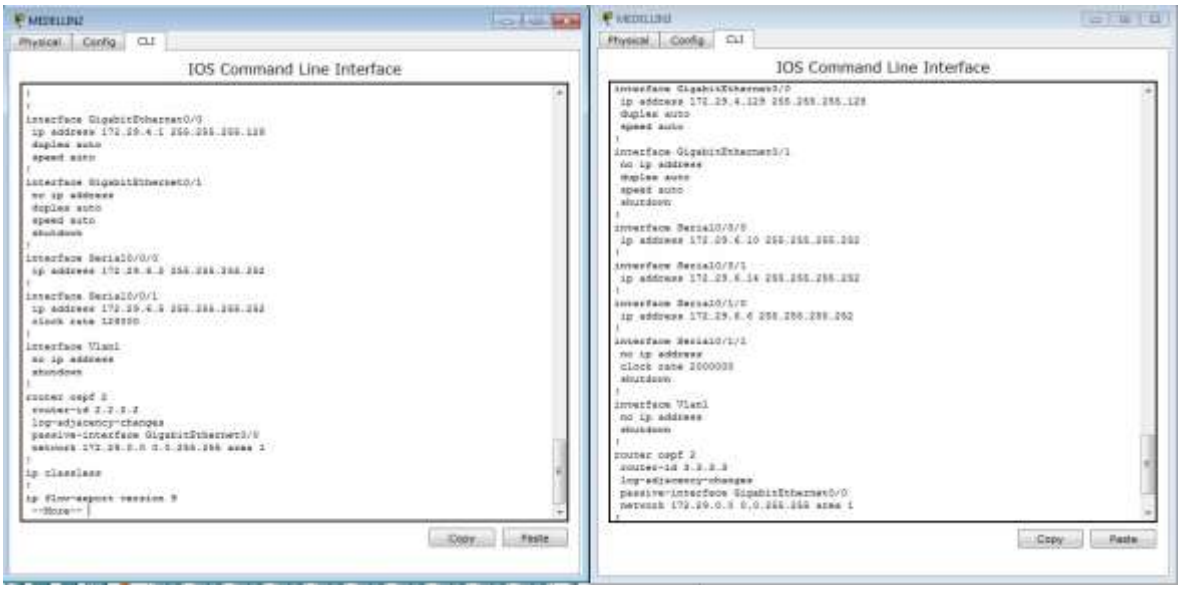


*Figura 33. Verificación del protocolo OSPF en MEDELLIN2 y MEDELLIN3.*

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

## Bogotá

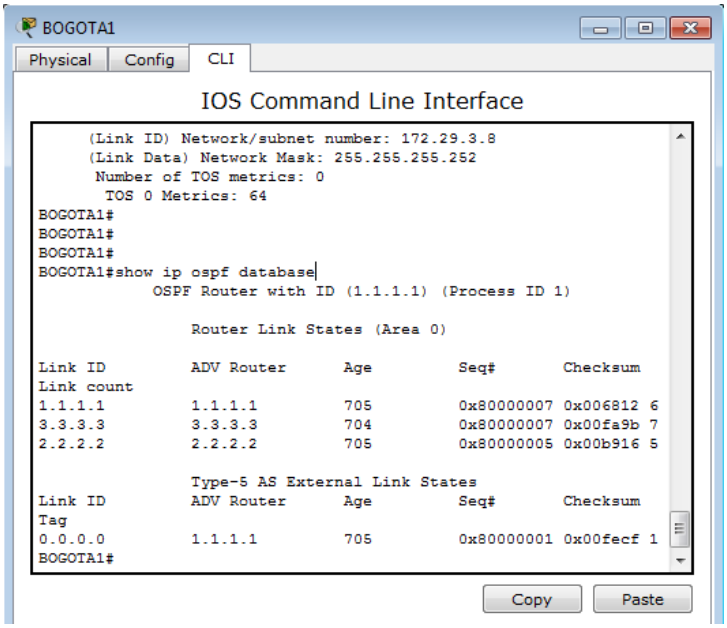


*Figura 34. Base de datos de OSPF de BOGOTA1*

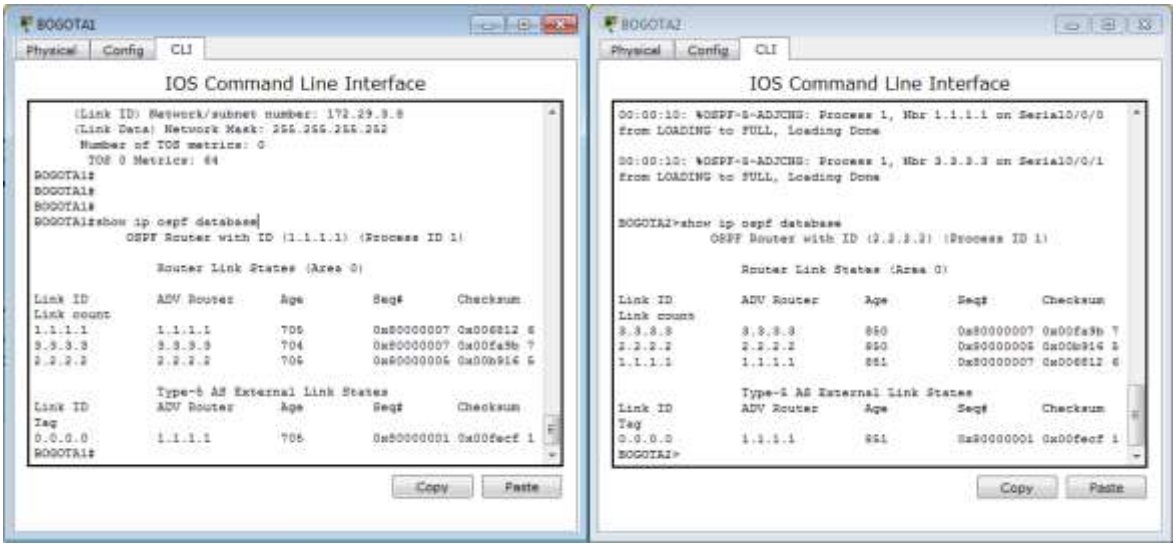


*Figura 35. Base de datos de OSPF BOGOTA2 y BOGOTA3*

## Medellín

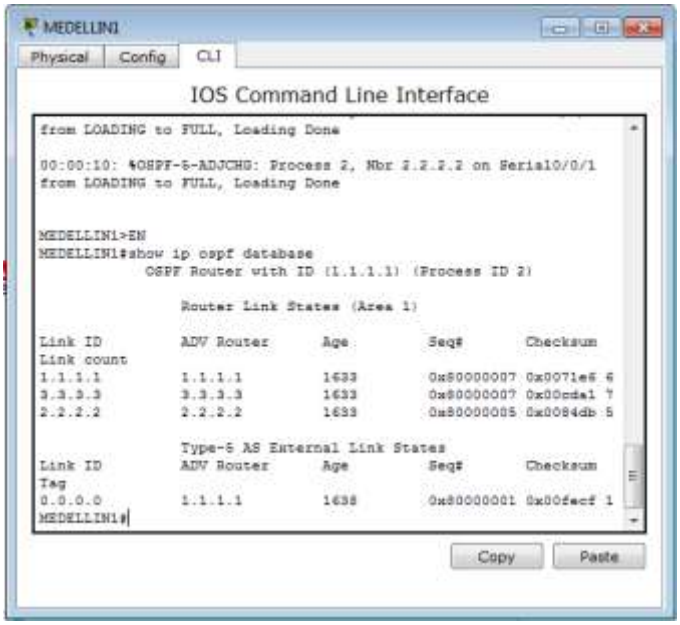


*Figura 36. Base de datos de OSPF MEDELLIN1.*

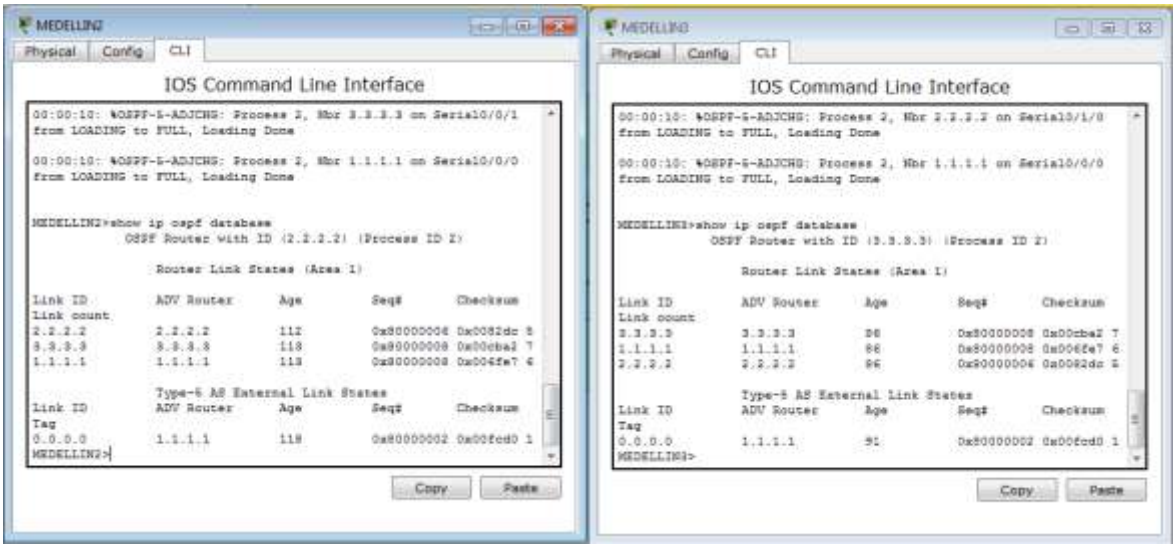


*Figura 37. Base de datos de OSPF MEDELLIN2 y MEDELLIN3.*

**2.5 Parte 5: Configurar encapsulamiento y autenticación PPP.**

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

**Configuración PAP en el ISP**

ISP(config)#username MEDELLIN1 password cisco
ISP(config)#int s0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password cisco

**Configuración PAP en MEDELLIN1**

MEDELLIN1(config)#username ISP password cisco
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#encapsulation ppp
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)#ppp pap sent-username MEDELLIN1 password cisco

**Verificación pap entre ISP y MEDELLIN1**

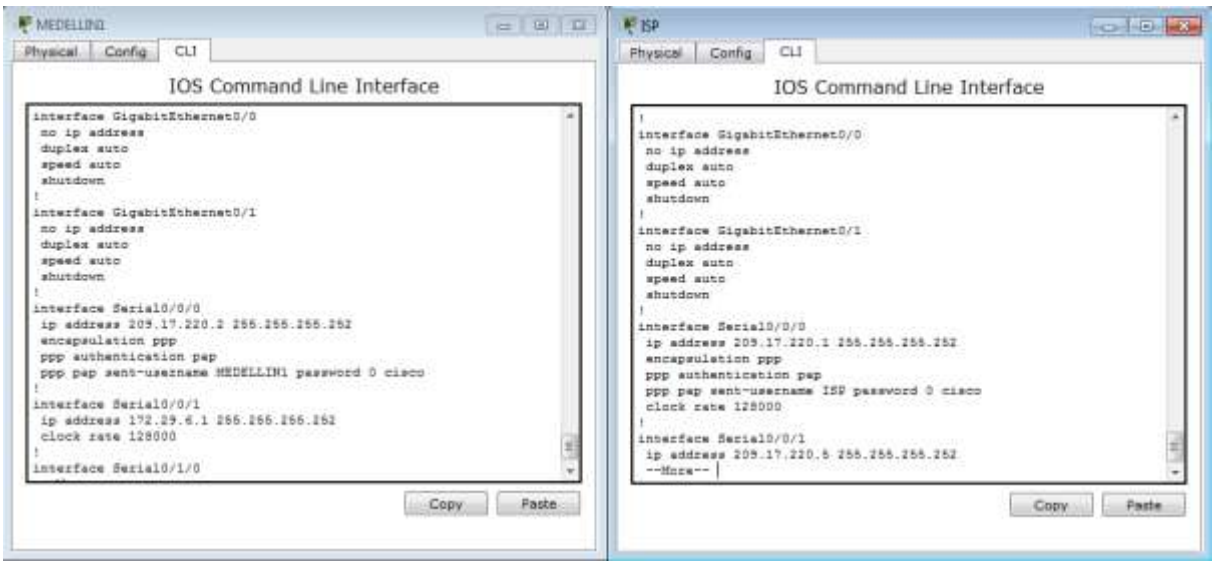


*Figura 38. Verificación PAP entre ISP y MEDELLIN1.*

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

**Configuración CHAP ISP**

ISP(config)#username BOGOTA1 password cisco
ISP(config)#int s0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#
ISP(config-if)#ppp authentication chap
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up

**Configuración CHAP BOGOTA1**

BOGOTA1>en
BOGOTA1#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA1(config)#username ISP password cisco
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#encapsulation ppp
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
BOGOTA1(config-if)#ppp authentication chap

**Nota:** Se debe guardar la configuración y reiniciar los routers ISP, MEDELLIN1 Y BOGOTA1

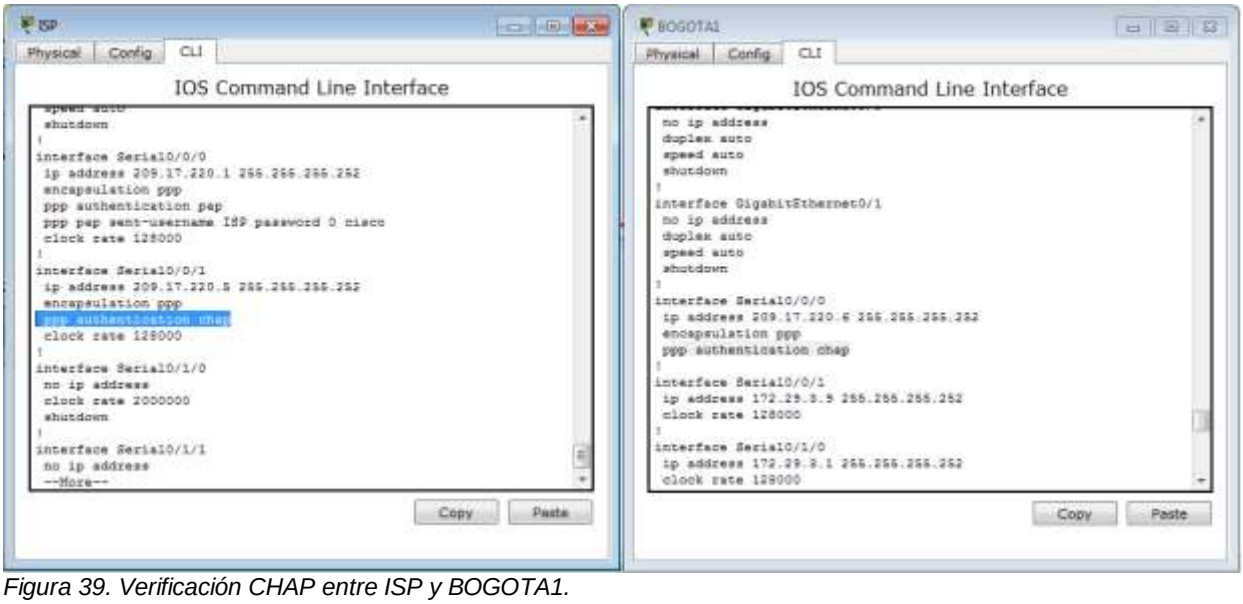


*Figura 39. Verificación CHAP entre ISP y BOGOTA1.*

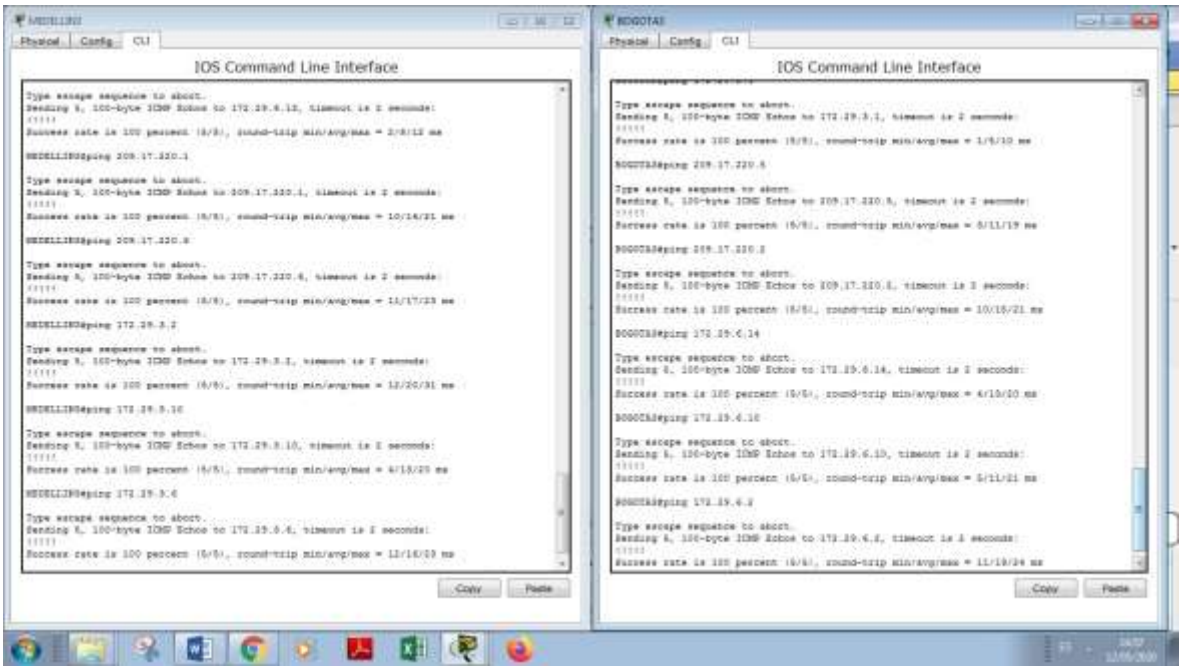


*Figura 40. Ping de extremo a extremo (MEDELLIN3 a BOGOTA3).*

## 2.6 Parte 6: Configuración de PAT.

a. **En la topología, si 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**.

```
MEDELLIN1(config)#ip nat inside source list 1 interface s0/0/0 overload
MEDELLIN1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#int s0/0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#int s0/1/0
MEDELLIN1(config-if)#ip nat inside
```

MEDELLIN1(config-if)#int s0/1/1
MEDELLIN1(config-if)#ip nat inside

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, cómo diferente puerto**.

BOGOTA1(config)#ip nat inside source list 1 interface s0/0/0 overload
BOGOTA1(config)#access-list 1 permit 172.29.0.0 0.0.3.255
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#int s0/0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int s0/1/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int s0/1/1
BOGOTA1(config-if)#ip nat inside

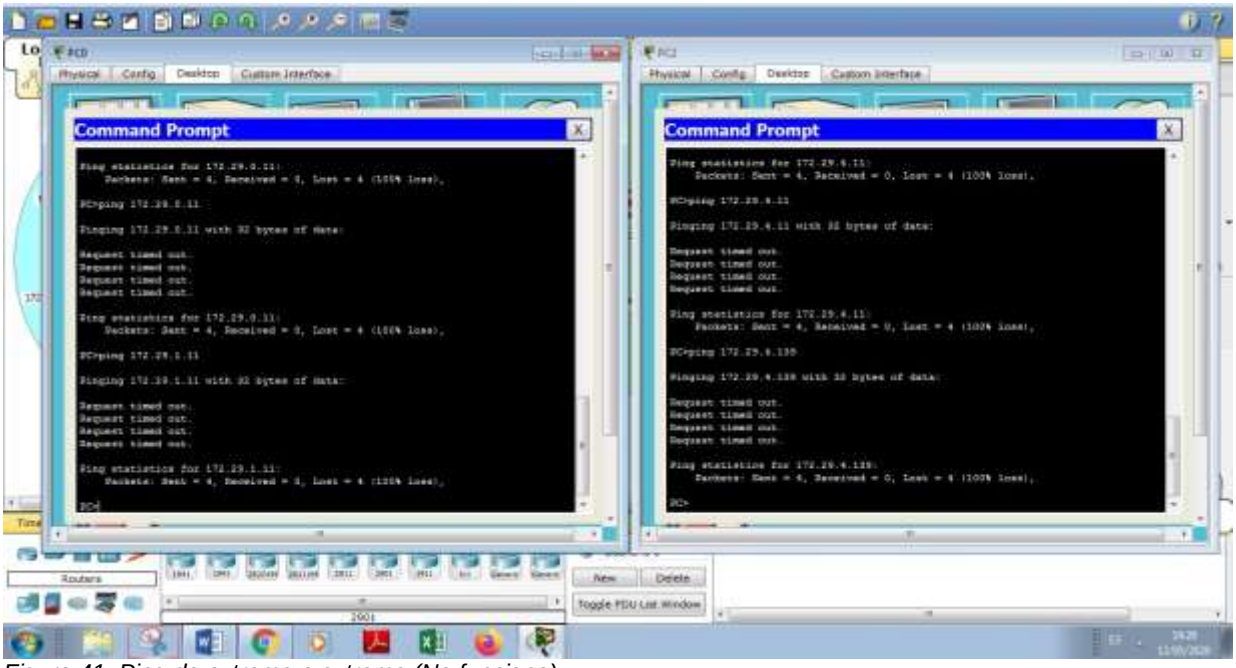

*Figura 41. Ping de extremo a extremo (No funciona)..*

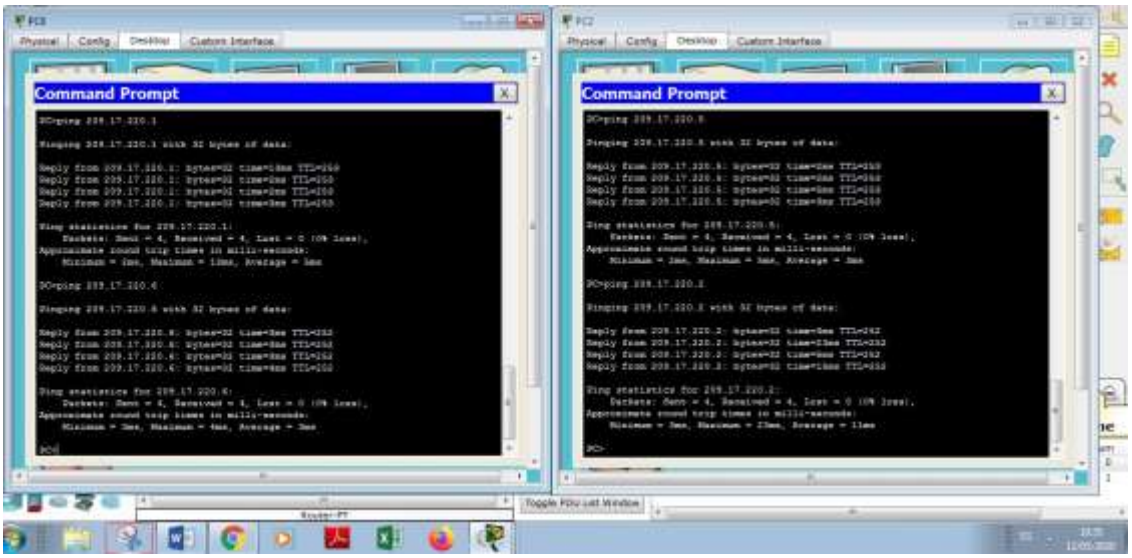


*Figura 42. Ping a ISP, Medellin1 y Bogota1 (Funciona), desde los computadores ubicadas en las LAN de Medellín y Bogotá.*

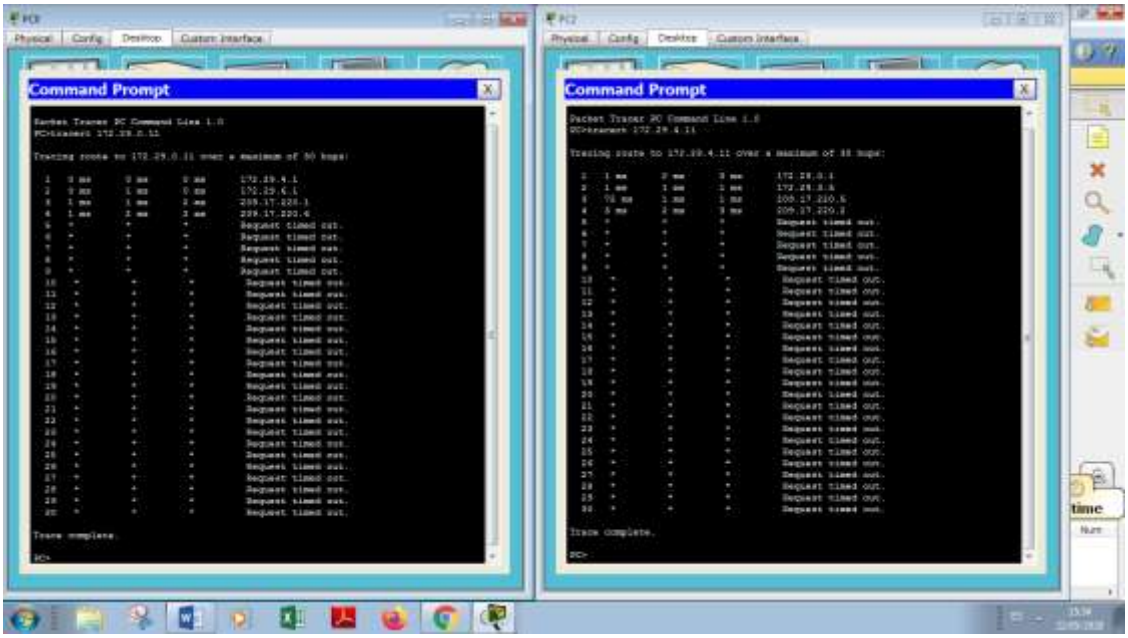


*Figura 43.Verificación de la ruta de destino de PC0 y PC2 hasta el otro extremo a través del comando tracert.*

**Resultados:** Vemos que según el comando tracert la conectividad se pierde cuando sobrepasa el router de borde de la ciudad contraria a donde está el computador. Por ejemplo, el PCO ubicado en una de las LAN de Medellín puede hacer ping solo hasta la dirección 209.17.220.6 que corresponde al router BOGOTA1, esto se debe a las restricciones que se hicieron.

### 2.7 Parte 7: Configuración del servicio DHCP.

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

```
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.10
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.138
MEDELLIN2(config)#ip dhcp pool MED2
MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.1
MEDELLIN2(dhcp-config)#dns-server 2.2.2.2
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#ip dhcp pool MED3
MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.129
MEDELLIN2(dhcp-config)#dns-server 2.2.2.2
```

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

```
MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5
```

### Verificación DHCP MEDELLIN2 y MEDELLIN3

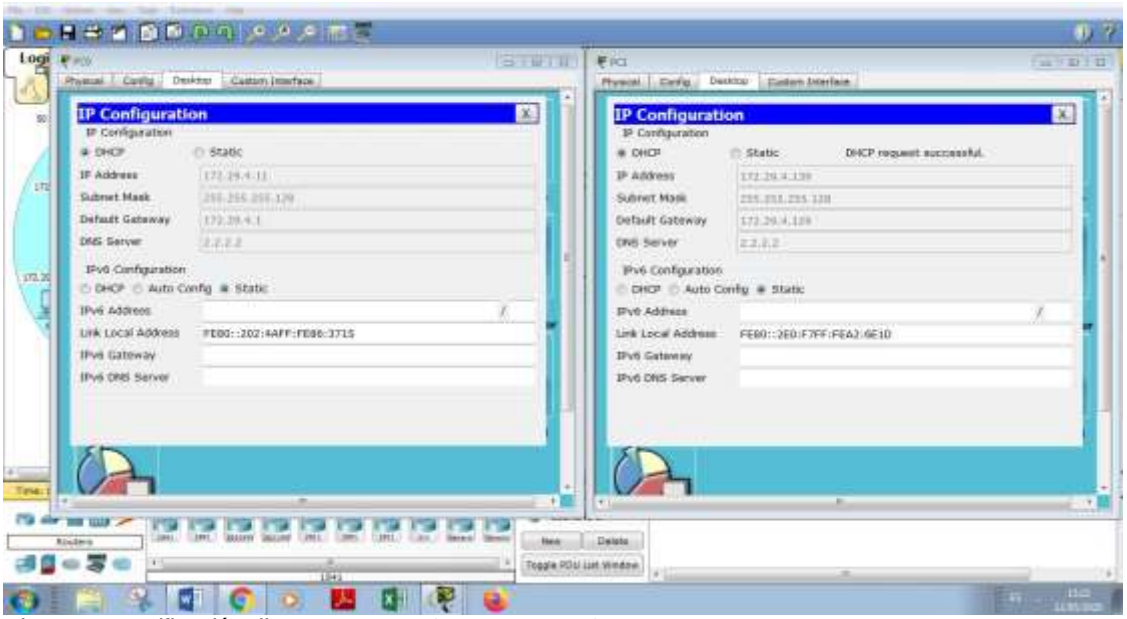


*Figura 44. Verificación dhcp MEDELLIN2 y MEDELLIN3.*

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

**Router BOGOTA2**

```
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.10
BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.10
BOGOTA2(config)#ip dhcp pool BOG2
BOGOTA2(dhcp-config)#network 172.29.1.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.1.1
BOGOTA2(dhcp-config)#dns-server 2.2.2.2
BOGOTA2(dhcp-config)#exit
BOGOTA2(config)#ip dhcp pool BOG3
BOGOTA2(dhcp-config)#network 172.29.0.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.0.1
BOGOTA2(dhcp-config)#dns-server 2.2.2.2
```

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

**Router BOGOTA3**

```
BOGOTA3(config)#int g0/0
BOGOTA3(config-if)#ip helper-address 172.29.3.13
```

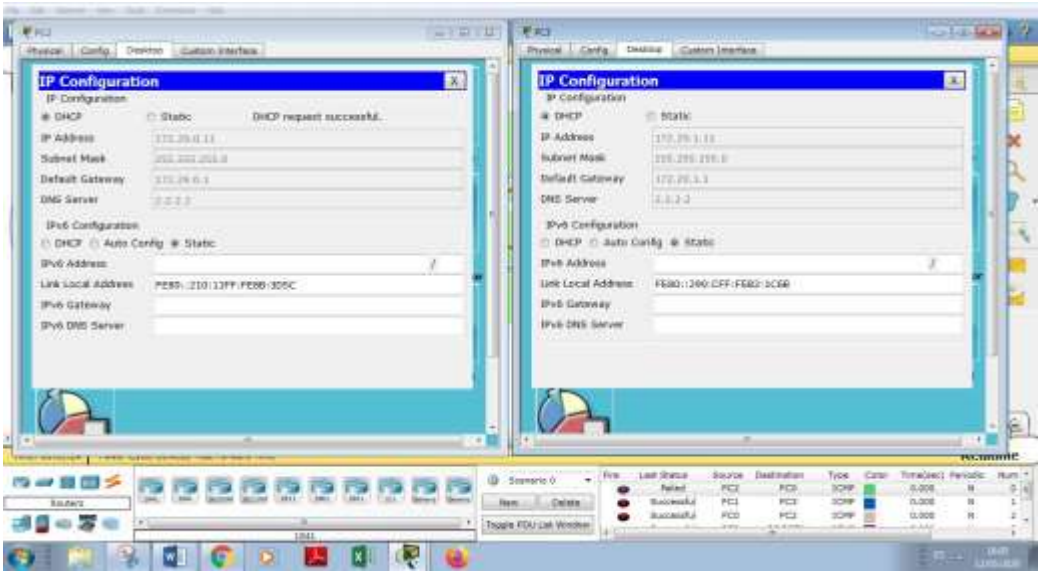


*Figura 45. Verificación del servicio dhcp BOGOTA2 y BOGOTA3*

## CONCLUSIONES

Se presentaron algunos problemas de comunicación entre los dispositivos de los extremos del escenario 2 cuando se configuró la autenticación PAP y CHAP. Estos problemas fueron solucionados guardando la configuración y reiniciando los routers ISP, MEDELLIN1 y BOGOTA1.

PAT y NAT se utilizan para solucionar el problema del agotamiento de direcciones ipv4, básicamente lo que hacen es traducir la dirección de un host que no es globalmente única a un espacio de direcciones global que se pueda conectar a Internet.

La diferencia entre PAT (NAT con sobrecarga) y NAT radica en que la primera usa una dirección global interna para muchas direcciones locales de la intranet a través del uso de diferentes puertos, en cambio la segunda asigna direcciones IP públicas a direcciones IP privadas en una relación de uno a uno. PAT es muy utilizada en las conexiones internet de los hogares debido al menor costo de inversión en la compra de direcciones IP únicas.

NAT para IPV6 se constituye en un mecanismo que contribuye en la transición que debe hacerse de IPV4 a IPV6.

OSPFv2 y RIPv2 son protocolos que facilitan el enrutamiento de manera dinámica disminuyendo la sobrecarga administrativa. El primero es muy utilizado en la actualidad debido a su rápida convergencia.

OSPFv2 a diferencia de RIP2 no realiza sumarización automática en los routers de borde.

En OSPFv2, el router que está conectado a internet es utilizado para propagar la ruta predeterminada a los otros routers vinculados mediante este protocolo, para esta configuración se utiliza el comando default-information originate en el router de borde. En el caso del escenario 2 corresponden los routers encargados de propagar esta ruta son MEDELLIN1(a MEDELLIN2 y MEDELLIN3) y BOGOTA1(a BOGOTA2 Y BOGOTA3).

## BIBLIOGRAFÍA


CISCO. Conceptos sobre tecnología de redes {En línea}. {21 mayo de 2020} disponible en: (https://www.cisco.com/c/dam/global/es_mx/solutions/small-business/pdfs/smb-redes-mx.pdf)

CISCO. Cisco.com Worldwide {En línea}. {21 mayo de 2020} disponible en: (https://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_network_assistant/version5_0/quick/guide/Spanish/gsg_esp/cnapref.html)

Cruz Domínguez José Martín, Mora Cárdenas Gloria Evila], Beatriz Sauza Avila, Pérez Castañeda Suly Sendy, Cruz Ramírez Dorie. Seguridad en redes LAN implementando VLAN {En línea}. {21 mayo de 2020} disponible en: (https://repository.uaeh.edu.mx/revistas/index.php/sahagun/article/download/2355/2357?inline=1)

JOSKOWICZ, José. (2008). Redes de datos. *Montevideo, Uruguay, Universidad de la Republica, Instituto de Ingeniería Eléctrica, Facultad de Ingeniería* {En línea}. {21 mayo de 2020} disponible en: (https://www.researchgate.net/profile/Jose_Joskowicz/publication/266907714_REDES_DE_DATOS/links/544e350a0cf26dda088e75f1/REDES-DE-DATOS.pdf)

MARION, Luis. [mariontechacademy]. (2013, Noviembre 11). CS071 21.04 OSPF - Ruta Acceso a Internet en Packet Tracer [Archivo de video].Disponible en: (https://www.youtube.com/watch?v=vQROsYyB89Q&t=4838s)

REVISTA FORBES. Cisco Systems (CSCO). {En línea}. {21 mayo de 2020} disponible en: (https://www.forbes.com/companies/cisco-systems/#286d57fc7029)

SOLUTECSA. Glosario de Internet e informática. {En línea}. {21 mayo de 2020} disponible en: (https://www.internetglosario.com/450/Protocolo.html)

VELTE, Toby. J., VELTE, Anthony. (2008). *Manual de CISCO* (No. 004.6 V4). McGraw-Hill Interamericana {En línea}. {21 mayo de 2020} disponible en: (https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=equipos+cisco&btnG=)

ZÚÑIGA LÓPEZ, Vicente. (2005). Redes de Transmisión de datos {En línea}. {21 mayo de 2020} disponible en: (http://dgsa.uaeh.edu.mx:8080/bibliotecadigital/handle/231104/144)