EVALUACIÓN- PRUEBA DE HABILIDADES PRACTICAS CCNA

DIPLOMADO DE PROFUNDIZACIÓN

DIANA MEDINA RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
INGENIERIA DE SISTEMAS
DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN/WAN)
NEIVA
2019

EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

DIANA MEDINA RODRIGUEZ

Trabajo de Diplomado para optar el título de Ingeniero de Sistemas

Director y tutor Diplomado profundización Ing. Juan Carlos Vesga

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
INGENIERIA DE SISTEMAS
DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN/WAN)
NEIVA
2019

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Neiva, 13 de Julio 2019

DEDICATORIA

Dedico este trabajo a mi familia, al motor de mi hogar; Héctor Fabio Cañón y a mis hijos, por supuesto a mi madre y mi gordo querido que ya no nos acompaña, mis hermanos Y mi abuela que siempre me lleva en sus oraciones. A todos por el apoyo incondicional que me brindaron para nunca desfallecer y llegar a la meta.

AGRADECIMIENTOS

Agradezco primeramente al Dios de la gloria, que me bendice cada día y a tantas y a cada una de las personas que de una u otra manera me ayudaron en el andar de este camino. Al señor Jaime Camacho por haberme brindado su apoyo en parte de mi carrera. Dios los bendiga.

Tabla de contenido

LISTADO DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

Con este trabajo se pretende mostrar lo que hemos aprendido durante estos meses, manejado la herramienta Packet Traicer, haciendo simulaciones, configurando dispositivos, topologías de red, simulaciones de conectividad etc.

Se realizarán prácticas sobre equipos reales, con el simulador de Cisco Networking Academy y con Packet Tracer; el cual tiene como objetivo la adquisición y la Formalización de habilidades para el mejor acceso a los equipos y realizar una configuración básica de los distintos aspectos físicos (hardware) y lógicos (software).

Palabras claves: Redes, protocolo, packet Tracer, simulación y conexión.

1 OBJETIVOS

1.1 OBJETIVO GENERAL

Realizar y dar solución a los dos escenarios propuestos como prueba de habilidades del Diplomado de profundización en Cisco, poniendo en la práctica todos los conceptos estudiados en todos los fundamentos importantes como lo son el ruteo y conmutación de las redes que existen en un conocimiento general y global.

1.2 OBJETIVOS ESPECIFICOS

Aplicar las diferentes configuraciones aprendidas en el diplomado para direcciones IP, RIP, encapsulamiento OSFP, DCHP, ACL, NAT, VLANs según lo indicado. Diseñar un esquema de direccionamiento según los requerimientos de los escenarios 1 y 2. Describir el paso a paso de cada uno de los procedimientos realizados en la solución de los escenarios propuestos para esta actividad final. Finalmente revisar y verificar la conectividad de las configuraciones mediante los comandos ping, tracert, show ip route, y show ip protocols, en los dos escenarios propuestos para esta práctica final del Diplomado.

2 DESARROLLO DE LOS ESCENARIOS

2.1 ESCENARIO 1

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

2.1.1 Topología de red

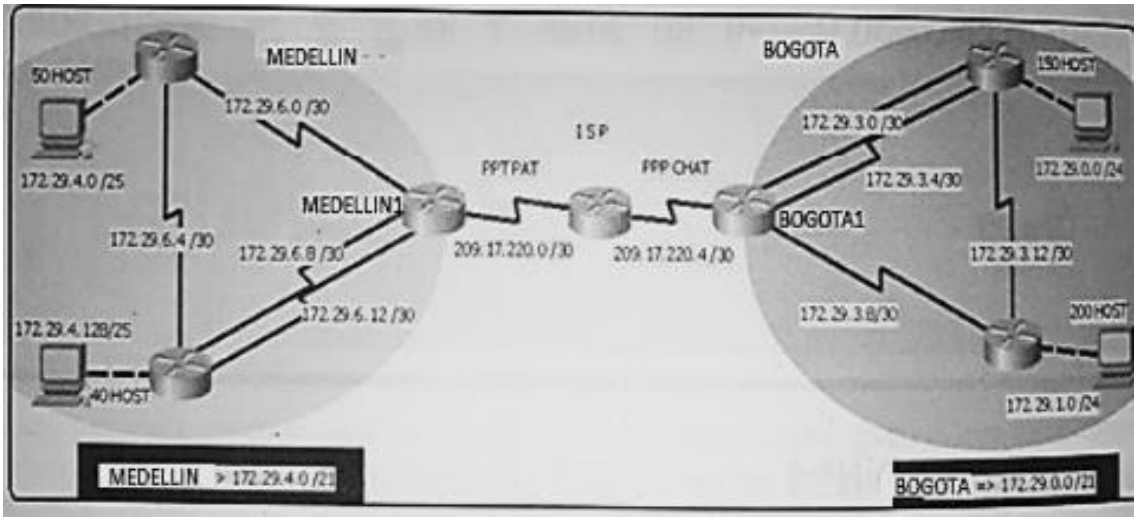


FIGURA 1 TOPOLOGIA DE RED

Este escenario plantea el uso de RIP como protocolo de enrutamiento, considerando que se tendrán rutas por defecto redistribuidas; así mismo, 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.

2.1.2 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.).
• Realizar la conexión física de los equipos con base en la topología de red.

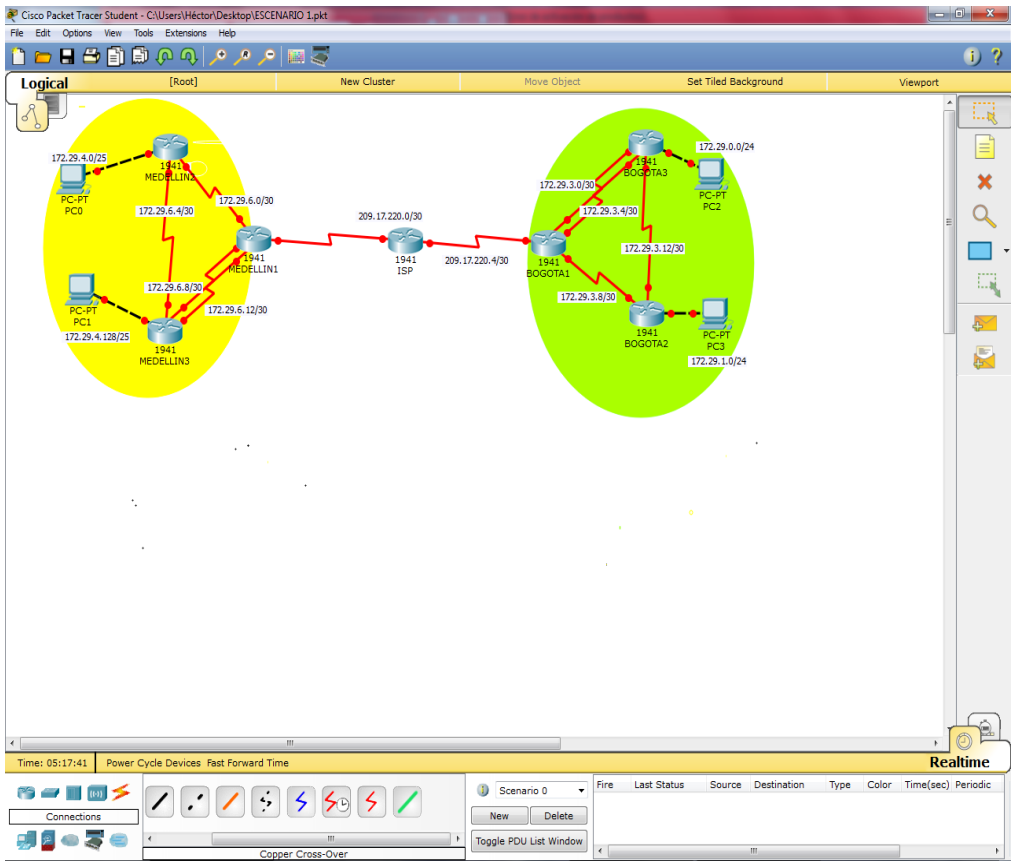


Figura 2 conexión física de la red

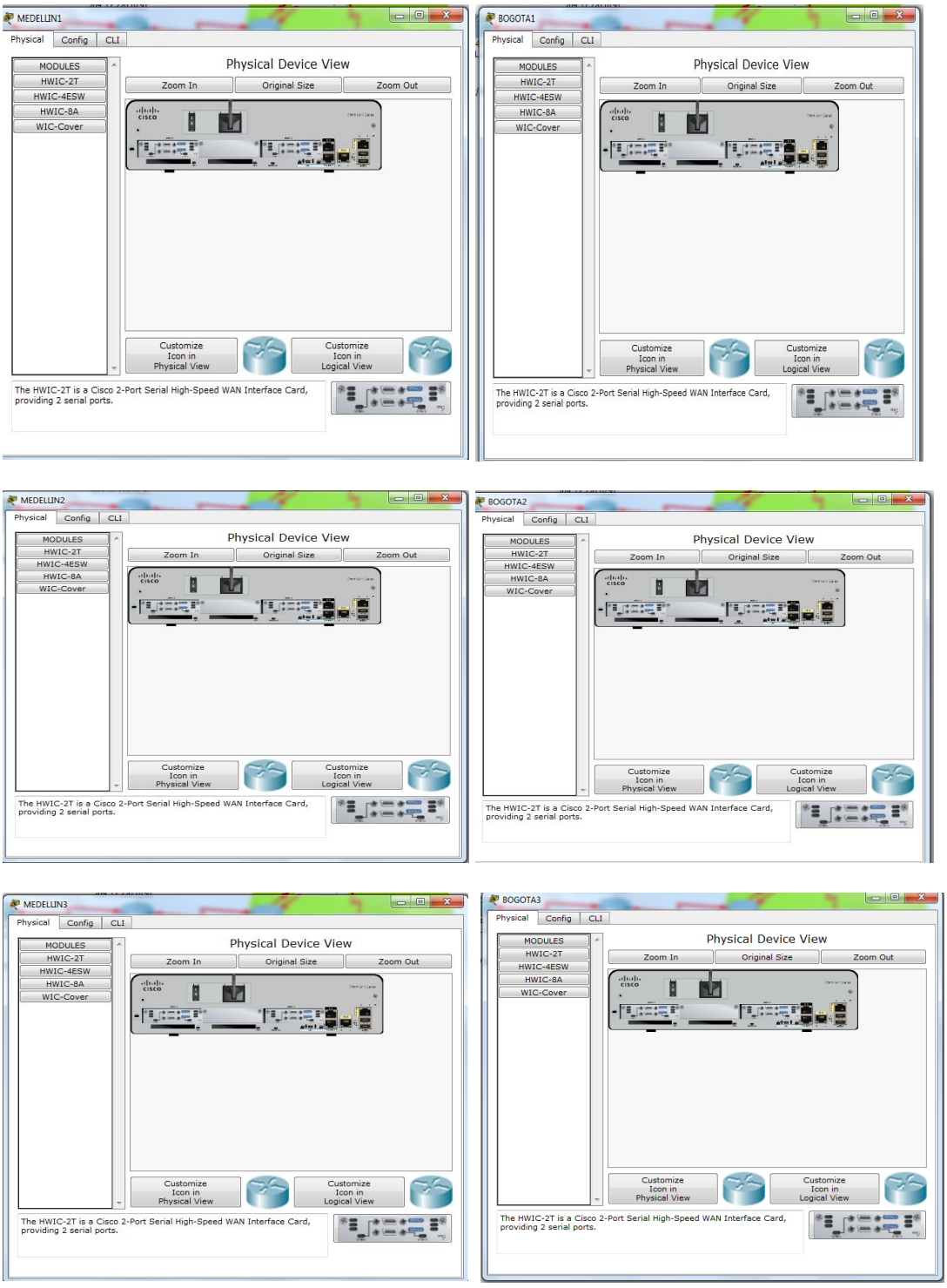


Figura 3.configurar topología de red, de acuerdo con las siguientes especificaciones.

2.1.3 Configuración ISP

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#no ip domain-lookup
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#line vty 0 15
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#enable secret class
ISP(config)#service password-encryption
ISP(config)#banner motd $Prohibido el acceso a personal no autorizado $
ISP(config)#
```

2.1.4 configuración MEDELLIN 1

```
Router>ENABLE
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN1
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 15
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#exit
MEDELLIN1(config)#enable secret class
MEDELLIN1(config)#service password-encryption
MEDELLIN1(config)#banner motd $Prohibido el acceso a personas no autorizadas $
MEDELLIN1(config)#
```

2.15 Configuración MEDELLIN2

```
Router>ENABLE
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN2
MEDELLIN2(config)#line console 0
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#line vty 0 15
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#exit
MEDELLIN2(config)#enable secret class
MEDELLIN2(config)#service password-encryption
MEDELLIN2(config)#banner motd $Prohibido el acceso a personas no autorizadas $
MEDELLIN2(config)#
```

2.1.6 configuración MEDELLIN3

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN3
MEDELLIN3(config)#no ip domain-lookup
MEDELLIN3(config)#line console 0
MEDELLIN3(config-line)#password cisco
MEDELLIN3(config-line)#login
MEDELLIN3(config-line)#line vty 0 15
MEDELLIN3(config-line)#password cisco
MEDELLIN3(config-line)#login
MEDELLIN3(config-line)#exit
MEDELLIN3(config)#enable secret class
MEDELLIN3(config)#service password-encryption
MEDELLIN3(config)#banner motd $Prohibido el acceso a personas no autorizadas $
MEDELLIN3(config)#
```

2.1.7 Configuración BOGOTA1

```
Router>ENABLE
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA1
BOGOTA1(config)#no ip domain-lookup
BOGOTA1(config)#line console 0
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#line vty 0 15
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#enable secret class
BOGOTA1(config)#service password-encryption
BOGOTA1(config)#banner motd $Prohibido el acceso a personas no autorizadas $
BOGOTA1(config)#
```

2.1.8 Configuración BOGOTA2

```
Router>ENABLE
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA2
BOGOTA2(config)#no ip domain-lookup
BOGOTA2(config)#line console 0
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#line vty 0 15
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#enable secret class
BOGOTA2(config)#service password-encryption
BOGOTA2(config)#banner motd $Prohibido el acceso a personas no autorizadas $
BOGOTA2(config)#
```

2.1.9 configuración BOGOTA3

```
Router(config)#hostname BOGOTA3
BOGOTA3(config)#no ip domain-lookup
BOGOTA3(config)#line console 0
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
BOGOTA3(config-line)#line vty 0 15
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
BOGOTA3(config-line)#enable secret class
BOGOTA3(config)#service password-encryption
BOGOTA3(config)#banner motd $Prohibido el acceso a personas no autorizadas $
BOGOTA3(config)#
```

2.1.10 Direccionamiento IP ISP

```
ISP>enable
Password:
Password:
Password:
ISP#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#int s0/0/0
ISP(config-if)#description conexion MEDELLIN1
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
ISP(config-if)#int s0/0/1
ISP(config-if)#description conexion con BOGOTA1
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
    ISP(config-if)#
```

2.1.11 Direccionamiento IP MEDELLIN1

```
MEDELLIN1>enable
Password:
Password:
Password:
MEDELLIN1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#description conexion hacia MEDELLIN2
MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
This command applies only to DCE interfaces
MEDELLIN1(config-if)#no sh

MEDELLIN1(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

MEDELLIN1(config-if)#int s0/0/1
MEDELLIN1(config-if)#description conexion 1 hacia MEDELLIN3
MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
MEDELLIN1(config-if)#description conexion 2 hacia MEDELLIN3
MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no sh
MEDELLIN1(config-if)#int s0/1/1
MEDELLIN1(config-if)#description conexion hacia IPS
MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252
MEDELLIN1(config-if)#clokc rate 128000
^
% Invalid input detected at '^' marker.
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
MEDELLIN1(config-if)#
```

2.1.12 Direccionamiento IP MEDELLIN2

Prohibido el acceso a personas no autorizadas

User Access Verification
Password:
MEDELLIN2>enable
Password:
MEDELLIN2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN2(config)#int s0/0/0
MEDELLIN2(config-if)#description conexion con MEDELLIN1
MEDELLIN2(config-if)#ip address 179.29.6.2 25.25.255.252
Bad mask 0x1919FFFC for address 179.29.6.2
MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252
MEDELLIN2(config-if)#clock rate 128000
This command applies only to DCE interfaces
MEDELLIN2(config-if)#no sh

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)#int 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)#clock rate 128000
MEDELLIN2(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
MEDELLIN2(config-if)#int f0/0
%Invalid interface type and number
MEDELLIN2(config)#int f0/0/0
%Invalid interface type and number
MEDELLIN2(config)#description conexiones con hosts
^
% Invalid input detected at '^' marker.
MEDELLIN2(config)#int s0/0/0
MEDELLIN2(config-if)#description conexion con hosts
MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128
MEDELLIN2(config-if)#no sh
MEDELLIN2(config-if)#
MEDELLIN2(config-if)#

2.1.13 Direccionamiento IP MEDELLIN3

```
MEDELLIN3>enable
Password:
Password:
MEDELLIN3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN3(config)#int s0/0/0
MEDELLIN3(config-if)#description conexion2 hacia MEDELLIN1
MEDELLIN3(config-if)#ip address 179.29.6.14 255.255.255.252
MEDELLIN3(config-if)#clock rate 12800
Unknown clock rate
MEDELLIN3(config-if)#clock rate 128000
This command applies only to DCE interfaces
MEDELLIN3(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
MEDELLIN3(config-if)#int s0/0/1
MEDELLIN3(config-if)#description conexion 1 hacia MEDELLIN1
MEDELLIN3(config-if)#ip address 172.29.6.10 255.255.255.252
MEDELLIN3(config-if)#clock rate 128000
This command applies only to DCE interfaces
MEDELLIN3(config-if)#no sh

MEDELLIN3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

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

MEDELLIN3(config-if)#int s0/1/0
MEDELLIN3(config-if)#description conexion hacia MEDELLIN2
MEDELLIN3(config-if)#ip address 172.29.6.6 255.255.255.252
MEDELLIN3(config-if)#clock rate 128000
This command applies only to DCE interfaces
MEDELLIN3(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
MEDELLIN3(config-if)#

MEDELLIN3(config-if)#in f0/0
%Invalid interface type and number
MEDELLIN3(config)#description conexion hacia hosts
^
```

% Invalid input detected at '^' marker.
MEDELLIN3(config)#ip address 172.29.4.129 255.255.255.128
^
% Invalid input detected at '^' marker.
MEDELLIN3(config)#no sh
^
% Invalid input detected at '^' marker.
MEDELLIN3(config)#

2.1.14 Direccionamiento IP BOGOTA 1

Prohibido el acceso a personas no autorizadas

User Access Verification

Password:

BOGOTA1>enable
Password:
BOGOTA1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#description conexion con ISP
BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
This command applies only to DCE interfaces
BOGOTA1(config-if)#no sh

BOGOTA1(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

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

BOGOTA1(config-if)#int s0/0/1
BOGOTA1(config-if)#description conexion con BOGOTA-2
BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
BOGOTA1(config-if)#int s0/1/0

BOGOTA1(config-if)#description conexion1 con BOGOTA2
BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
BOGOTA1(config-if)#int s0/1/1
BOGOTA1(config-if)#description conexion2 con BOGOTA2
BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
BOGOTA1(config-if)#

2.1.15 Direccionamiento IP BOGOTA 2

Prohibido el acceso a personas no autorizadas

User Access Verification

Password:
BOGOTA2>enable
Password:
BOGOTA2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA2(config)#int s0/0/0
BOGOTA2(config-if)#description conexion con BOGOTA1
BOGOTA2(config-if)#ip address 172.29.3.10 255.255.255.252
BOGOTA2(config-if)#clock rate 128000
This command applies only to DCE interfaces
BOGOTA2(config-if)#no sh
BOGOTA2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

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

BOGOTA2(config)#int s0/0/0
BOGOTA2(config-if)#description conexion con host
BOGOTA2(config-if)#ip address 172.29.1.1 255.255.255.0
BOGOTA2(config-if)#no sh
BOGOTA2(config-if)#

2.1.16 Direccionamiento IP BOGOTA 3

Prohibido el acceso a personas no autorizadas

User Access Verification

Password:

BOGOTA3>enable
Password:
BOGOTA3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA3(config)#int s0/0/0
BOGOTA3(config-if)#description conexion2 hacia BOGOTA1
BOGOTA3(config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA3(config-if)#clock rate 128000
This command applies only to DCE interfaces
BOGOTA3(config-if)#no sh

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)#int s0/0/1
BOGOTA3(config-if)#description conexion1 hacia BOGOTA1
BOGOTA3(config-if)#ip address 172.29.3.6 255.255.255.252
BOGOTA3(config-if)#clock rate 128000
This command applies only to DCE interfaces
BOGOTA3(config-if)#no sh

BOGOTA3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

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

BOGOTA3(config-if)#int s0/1/0
BOGOTA3(config-if)#description conexion hacia BOGOTA2
BOGOTA3(config-if)#ip address 172.29.3.14 255.255.255.252
BOGOTA3(config-if)#clock rate 128000
This command applies only to DCE interfaces
BOGOTA3(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
BOGOTA3(config-if)#
BOGOTA3(config-if)#int f0/0
%Invalid interface type and number
BOGOTA3(config)#int s0/0
%Invalid interface type and number
BOGOTA3(config)#int s0/0/0
BOGOTA3(config-if)#description conexion hacia hosts
BOGOTA3(config-if)#ip address 172.29.0.1 255.255.255.0
BOGOTA3(config-if)#no sh
BOGOTA3(config-if)#

2.1.17 Parte 1: Configuration del enrutamiento

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

2.1.18 Enrutamiento en Router ISP, ip route antes de rip en router ISP

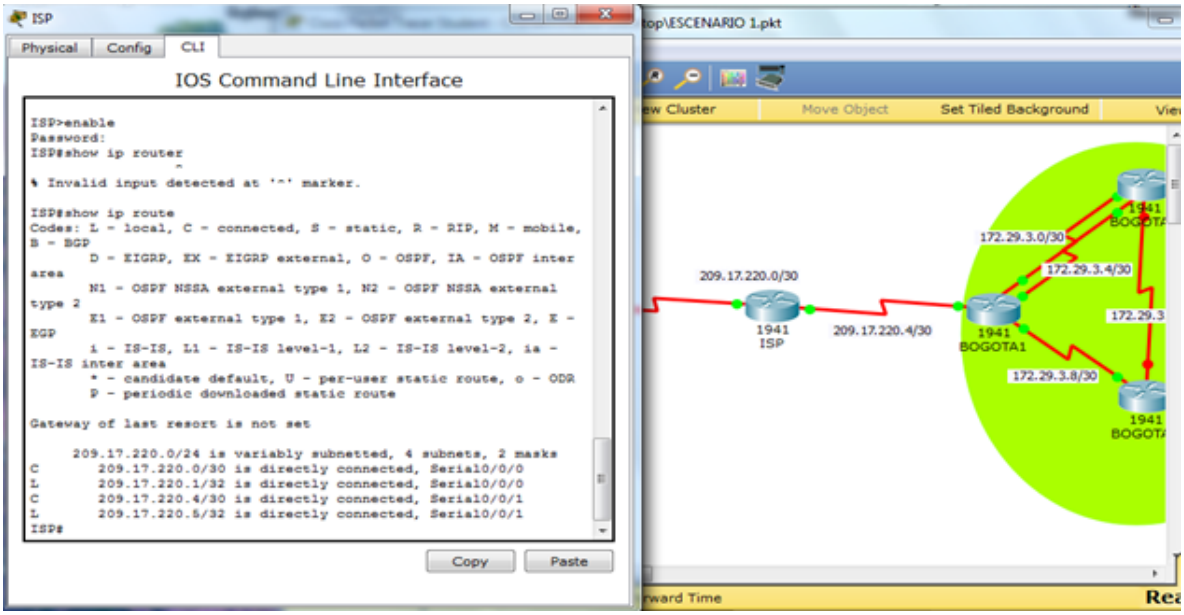


Figura 4 ip route ISP

Codigo de configuración router rip

```
ISP#conf t
Enter configuration commands, one per line. End with CNTL/Z
ISP(config)#route rip
ISP(config-router)#version 2
ISP(config-router)#network 209.17.220.0
ISP(config-router)#network 209.17.220.4
ISP(config-router)#no auto-summary
ISP(config-router)#
```

2.1.19 Show ip route antes de rip en router ISP

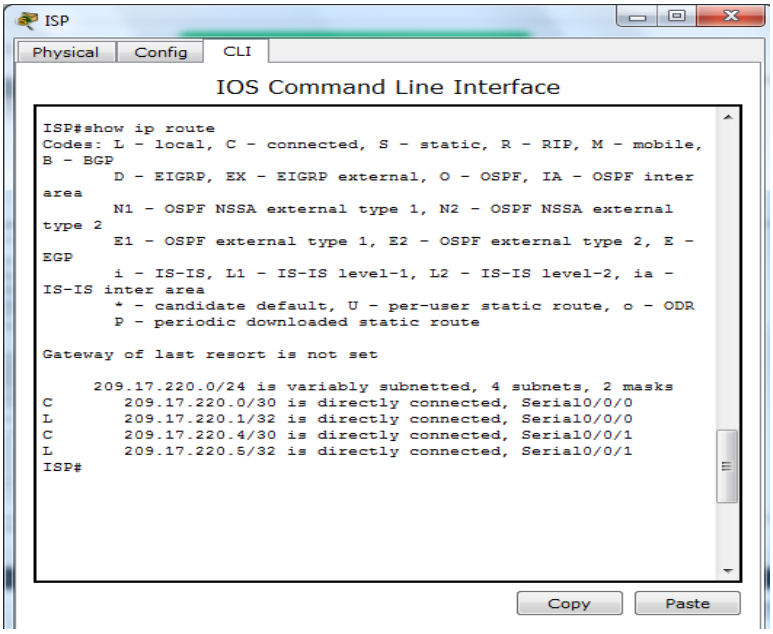


Figura 5 show ip route antes de rip en router ISP

2.1.20 Enrutamiento en router y verificación ip route antes rip en MEDELLIN1

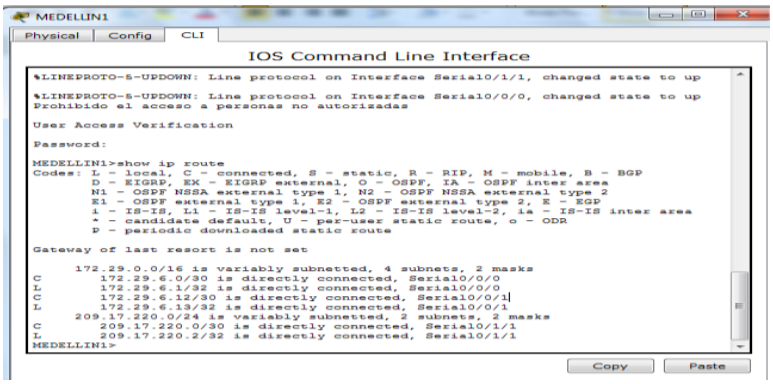


Figura 6 ip route antes rip en MEDELLIN-1

Código configuración de route rip

MEDELLIN-1>en

Password:

MEDELLIN-1#conf t

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

MEDELLIN-1(config)#route rip

MEDELLIN-1(config-router)#version 2

MEDELLIN-1(config-router)#network 172.29.6.0

MEDELLIN-1(config-router)#network 172.29.6.8

MEDELLIN-1(config-router)#network 172.29.6.12

MEDELLIN-1(config-router)#network 209.17.220.0

MEDELLIN-1(config-router)#no auto-summary

MEDELLIN-1(config-router)#exit

2.1.21 Show ip después de rip en router MEDELLIN1

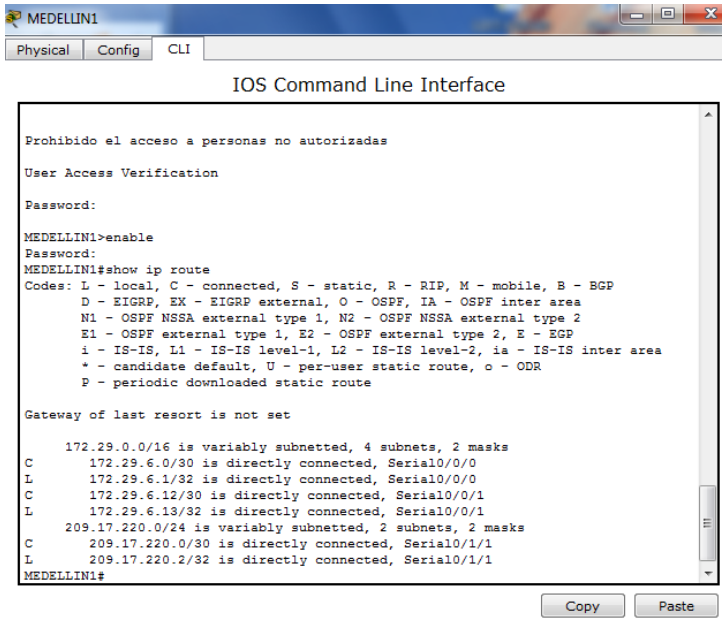


Figura 7 Show ip route despues de rip en router MEDELLIN-1

2.1.22 Enrutamiento en router y verificación ip route antes rip en MEDELLIN2

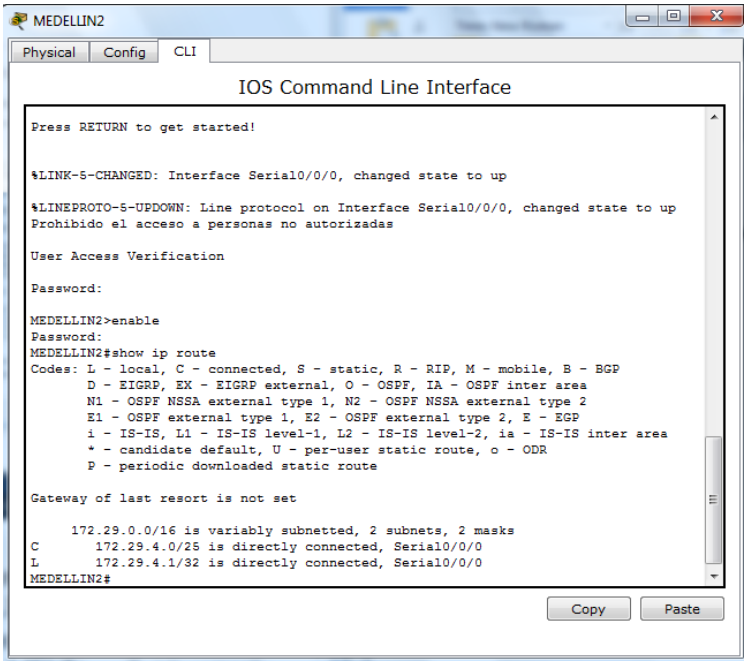


Figura 8 ip route antes rip en MEDELLIN-2

Código route rip

MEDELLIN-2#conf t

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

MEDELLIN-2(config)#route rip

MEDELLIN-2(config-router)#version 2

MEDELLIN-2(config-router)#network 172.29.6.0

MEDELLIN-2(config-router)#network 172.29.6.4

MEDELLIN-2(config-router)#no auto-summary

MEDELLIN-2(config-router)#exit

2.1.23 Show ip route despues de rip en router MEDELLIN2

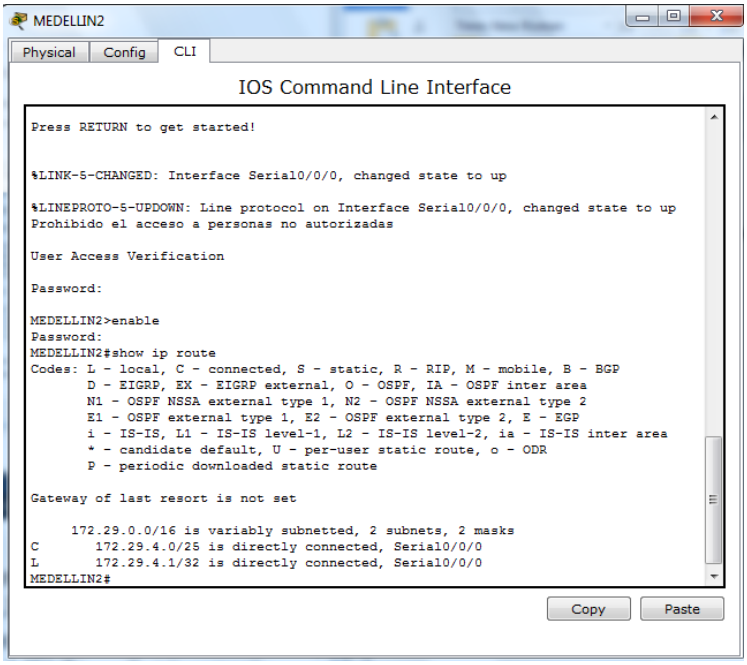


Figura 9 **Show ip route despues de rip en router MEDELLIN2**

2.1.24 Enrutamiento en router y verificación ip route antes rip en MEDELLIN3

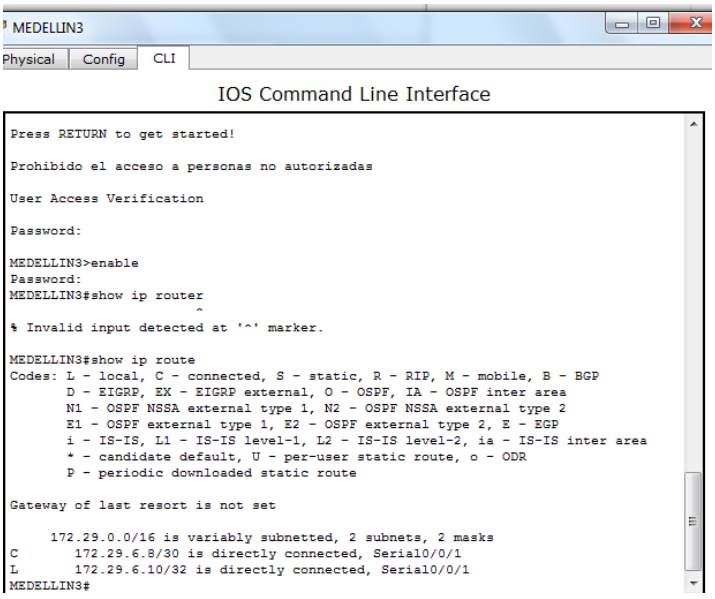


Figura 10 Enrutamiento en router y verificación ip route antes rip en MEDELLIN3

Código route rip

MEDELLIN-3#conf t

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

MEDELLIN-3(config)#route rip

MEDELLIN-3(config-router)#version 2

MEDELLIN-3(config-router)#network 172.29.6.4

MEDELLIN-3(config-router)#network 172.29.6.8

MEDELLIN-3(config-router)#network 172.29.6.12

MEDELLIN-3(config-router)#no auto-summary

MEDELLIN-3(config-router)#exit

2.1.25 Show ip route despues de rip en router MEDELLIN3

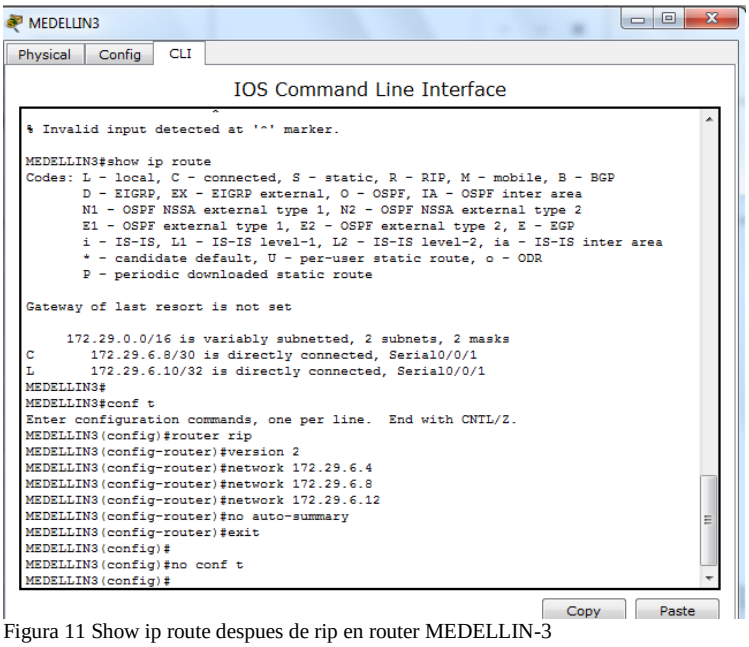


Figura 11 Show ip route despues de rip en router MEDELLIN-3

2.1.26 Enrutamiento en router y verificación ip route antes rip en BOGOTA1

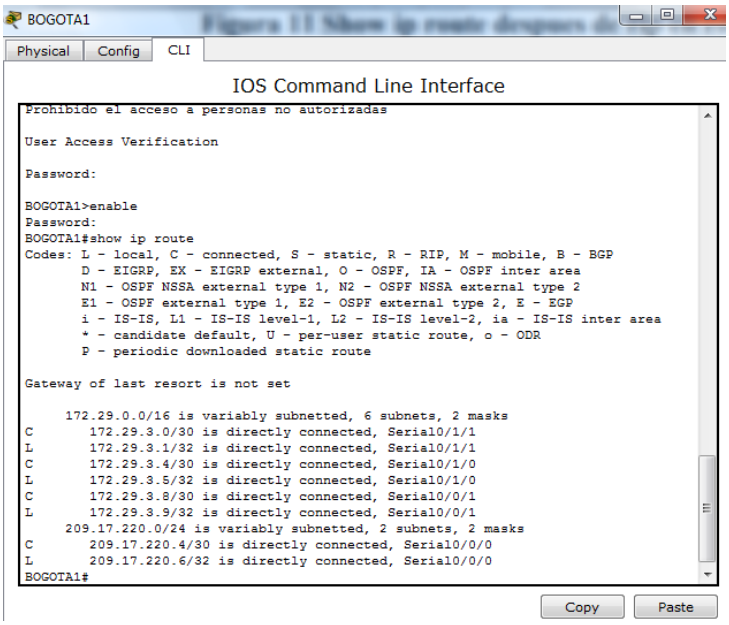


Figura 12 Figura 12 ip route antes rip en BOGOTA-1

Código route rip

BOGOTA-1#conf t

32

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

BOGOTA-1(config)#route rip

BOGOTA-1(config-router)#version 2

BOGOTA-1(config-router)#network 209.17.220.6

BOGOTA-1(config-router)#network 172.29.3.9

BOGOTA-1(config-router)#network 172.29.3.5

BOGOTA-1(config-router)#network 172.29.3.1

BOGOTA-1(config-router)#no auto-summary

BOGOTA-1(config-router)#exit

2.1.27 Show ip route despues de rip en router BOGOTA1

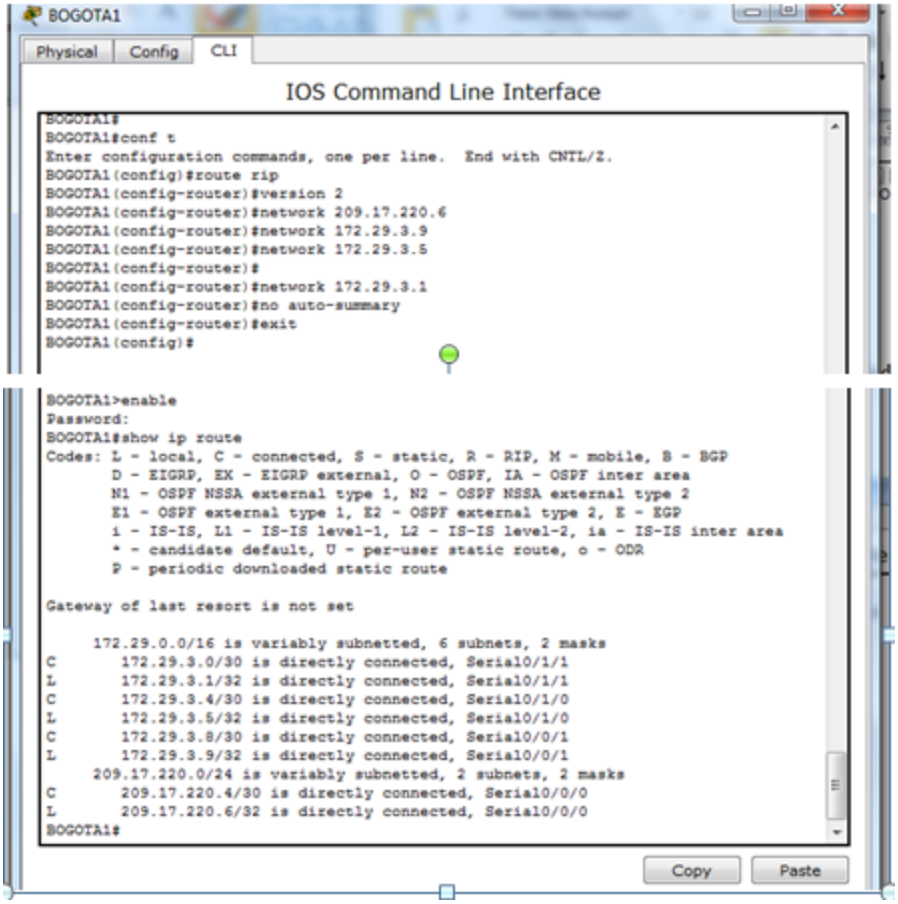


Figura 13 Show ip route despues de rip en router BOGOTA1

2.1.28 Enrutamiento en router y verificación ip route antes rip en BOGOTA2

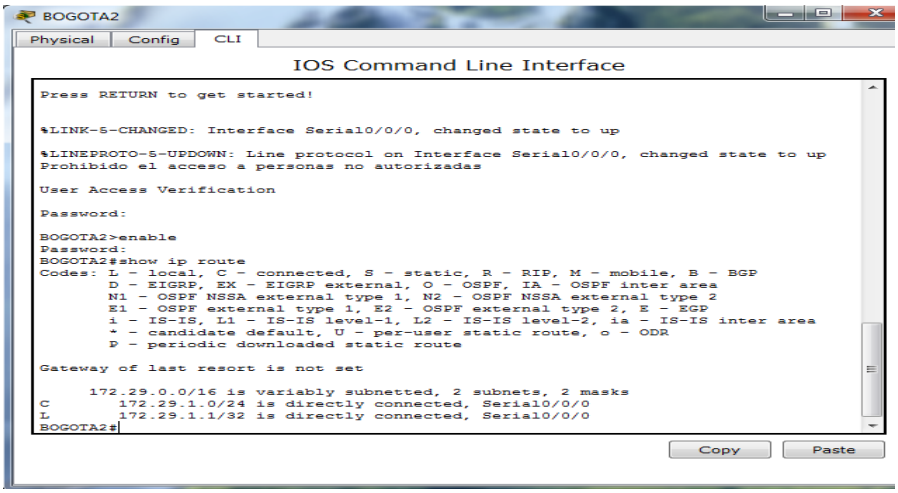


Figura 14 ip route antes rip en BOGOTA-2

Código ip route rip

BOGOTA-2#conf t

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

BOGOTA-2(config)#route rip

BOGOTA-2(config-router)#version 2

BOGOTA-2(config-router)#network 172.29.3.8

BOGOTA-2(config-router)#network 172.29.3.12

BOGOTA-2(config-router)#no auto-summary

BOGOTA-2(config-router)#exit

2.1.29 Show ip route despues de rip en router BOGOTA2

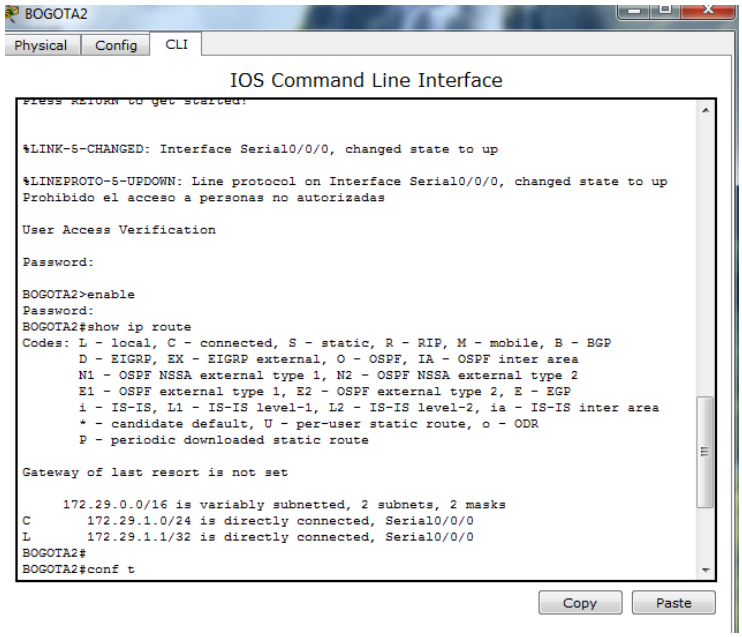


Figura 15 Show ip route despues de rip en router BOGOTA2

2.1.30 Enrutamiento en router y verificación ip route antes rip en BOGOTA3

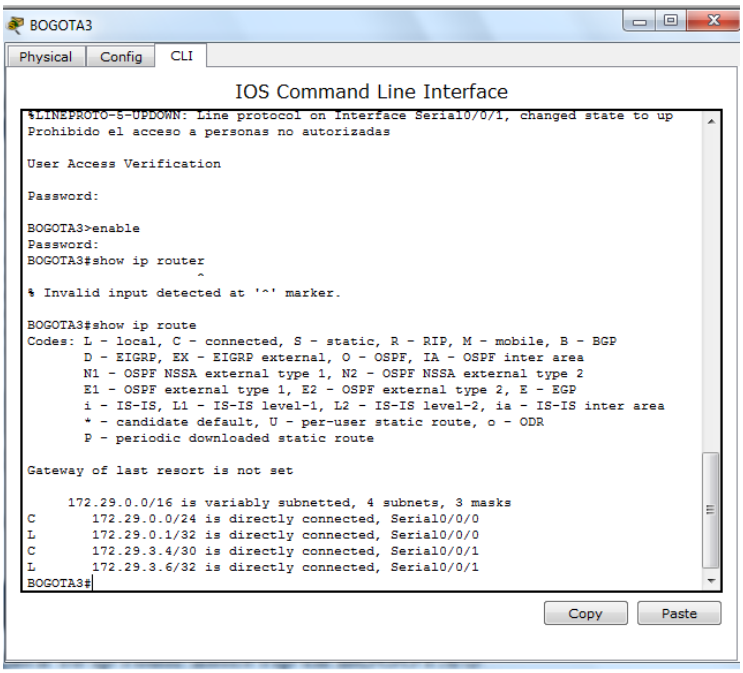


Figura 16 ip route antes rip en BOGOTA3

Codigo route rip

BOGOTA-3#conf t

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

BOGOTA-3(config)#route rip

BOGOTA-3(config-router)#version 2

BOGOTA-3(config-router)#network 172.29.3.0

BOGOTA-3(config-router)#network 172.29.3.4

BOGOTA-3(config-router)#network 172.29.3.12

BOGOTA-3(config-router)#no auto-summary

BOGOTA-3(config-router)#exit

2.1.31 Show ip route despues de rip en router BOGOTA3

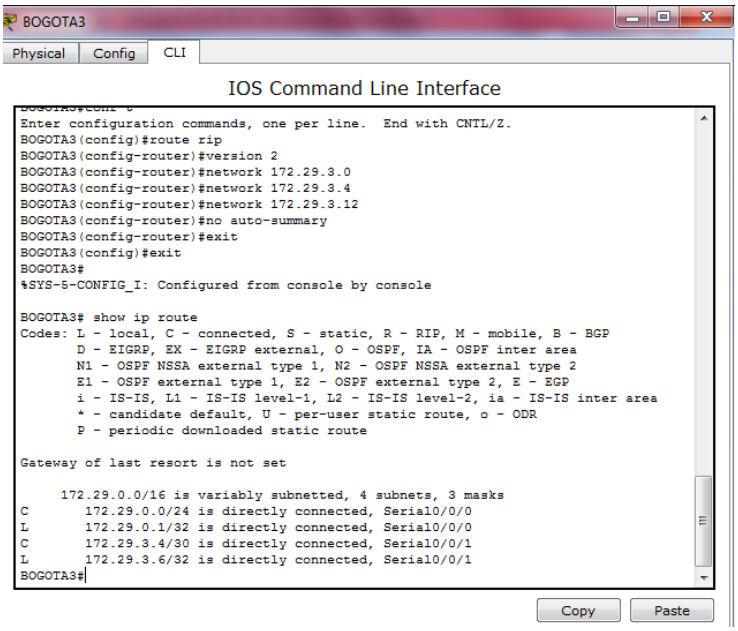


Figura 17 Show ip route despues de rip en router BOGOTA3

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 RIP.

MEDELLIN-1

MEDELLIN-1(config)#ip route 0.0.0.0 0.0.0.0 s0/1/1

MEDELLIN-1(config)#route rip

MEDELLIN-1(config-router)#version 2

MEDELLIN-1(config-router)#default-information originate

MEDELLIN-1(config-router)#

BOGOTA-1

BOGOTA-1 (config)#ip route 0.0.0.0 0.0.0.0 s0/0/0

BOGOTA-1 (config)#route rip

BOGOTA-1 (config-router)#version 2

BOGOTA-1 (config-router)#default-information originate

BOGOTA-1 (config-router)#

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.

2.1.32 sumarizacion de cada red

La red Medellin con dir ip 172.29.4.0

La red Bogota con direccion ip 172.29.0.0

DIRECCIONAMIENTO BINARIO	DIRECCIONAMIENTO IP			
Red Medellin	172.29	0.0.0.0.0.1.0.0	0.0.0.0.0.0.0.0	172.29.4.0/25
	172.29	0.0.0.0.0.1.0.0	1.0.0.0.0.0.0.0	172.29.4.128/25
	172.29	0.0.0.0.0.1.1.0	0.0.0.0.0.1.0.0	172.29.6.4/30
	172.29	0.0.0.0.0.1.1.0	0.0.0.0.1.0.0.0	172.29.6.8/30
	172.29	0.0.0.0.0.1.1.0	0.0.0.0.1.1.0.0	172.29.6.12/30
	172.29	0.0.0.0.0.1.1.0	0.0.0.0.0.0.0.0	172.29.6.0/30
	172.29	0.0.0.0.0.1.0.0	0.0.0.0.0.0.0.0	172.29.4.0/22
Red Bogota	172.29	0.0.0.0.0.0.0.0	0.0.0.0.0.0.0.0	172.29.0.0/24
	172.29	0.0.0.0.0.0.0.1	0.0.0.0.0.0.0.0	172.29.1.0/24
	172.29	0.0.0.0.0.0.1.1	0.0.0.0.0.1.0.0	172.29.3.4/30
	172.29	0.0.0.0.0.0.1.1	0.0.0.0.1.0.0.0	172.29.3.8/30
	172.29	0.0.0.0.0.0.1.1	0.0.0.0.1.1.0.0	172.29.3.12/30
	172.29	0.0.0.0.0.0.1.1	0.0.0.0.0.0.0.0	172.29.3.0/30
	172.29	0.0.0.0.0.0.0.0	0.0.0.0.0.0.0.0	172.29.0.0/22

Tabla 1 de sumarización de cada red

User Access Verification

Password:

ISP>en

Password:

ISP#conf t

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

ISP(config)#ip route 172.29.4.0 255.255.252.0 s0/0/0

ISP(config)#ip route 172.29.0.0 255.255.252.0 s0/0/1

ISP(config)#

2.1.33 Tabla de Enrutamiento.

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

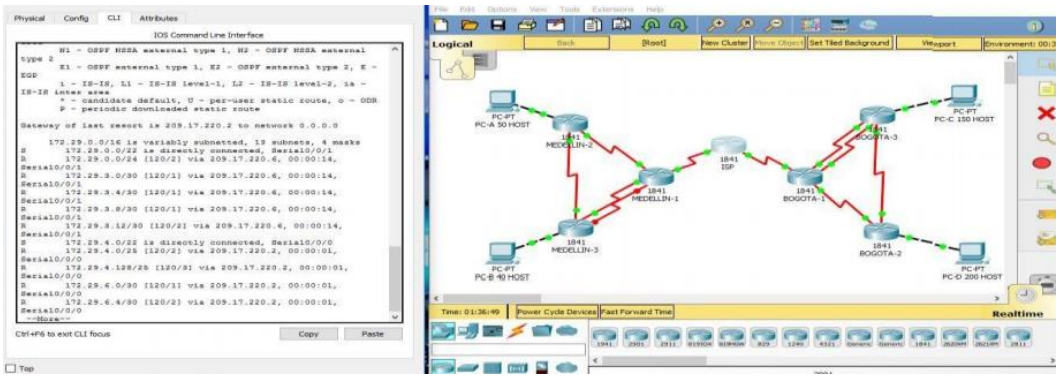


Figura 18 Verificar la tabla de enrutamiento

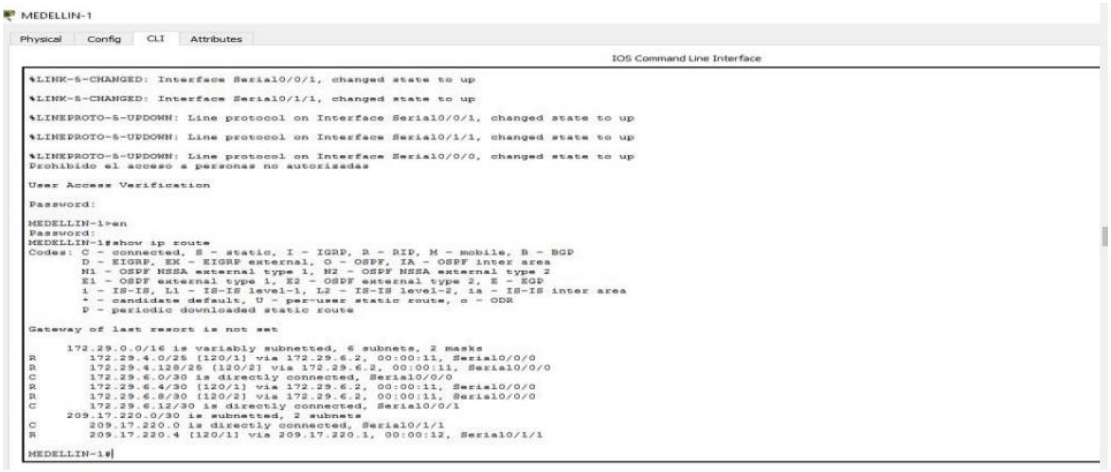


Figura 19 Enrutamiento medellin1

Figura 20 Enrutamiento medellin2

Figura 21 Enrutamiento medellin3

Figura 22 Enrutamiento Bogota1

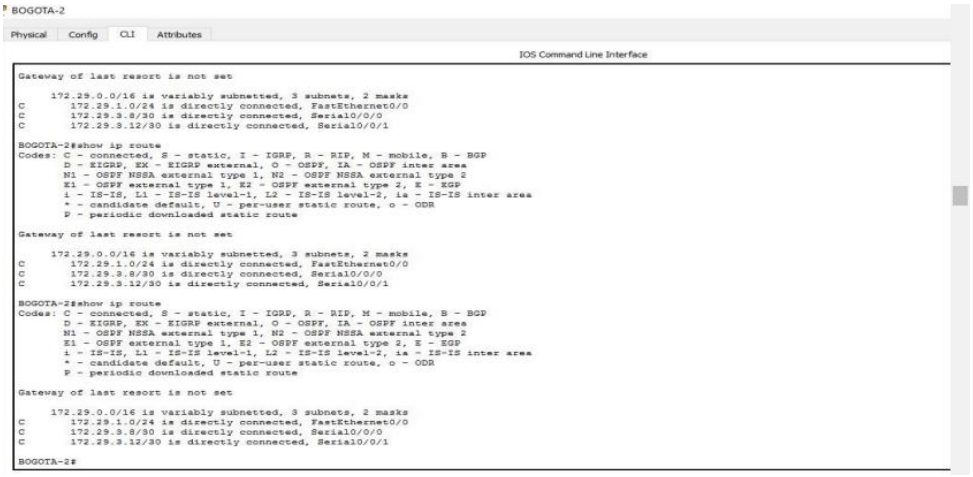


Figura 23 Enrutamiento Bogota2

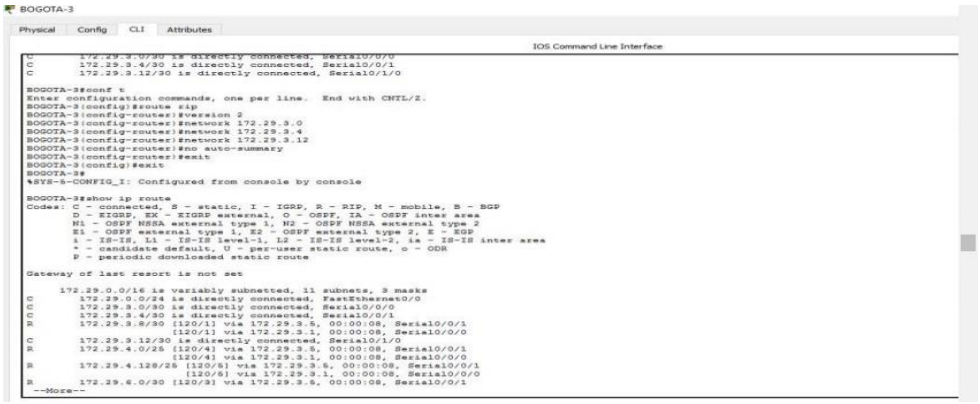


Figura 24 Enrutamiento Bogota3

2.1.34 Verificar el balanceo de carga que presentan los routers.

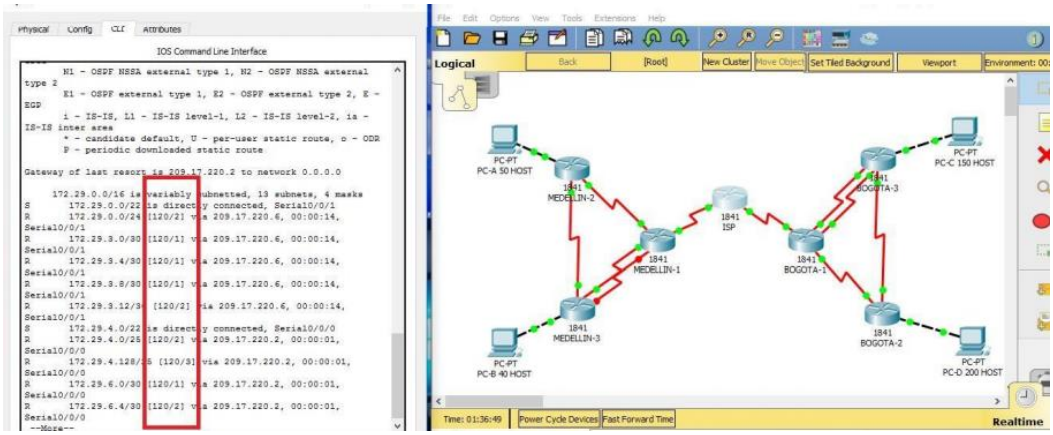


Figura 25 balanceo de carga que presentan los routers

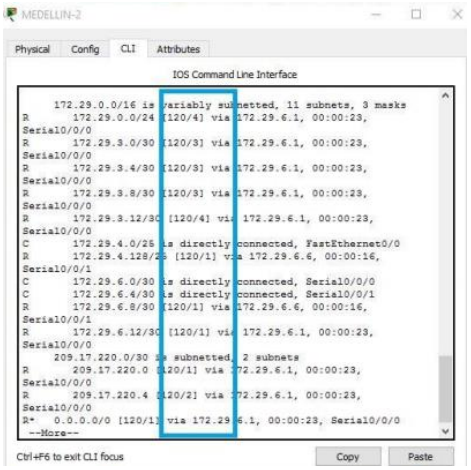


Figura 26 carga que presentan router Medellin

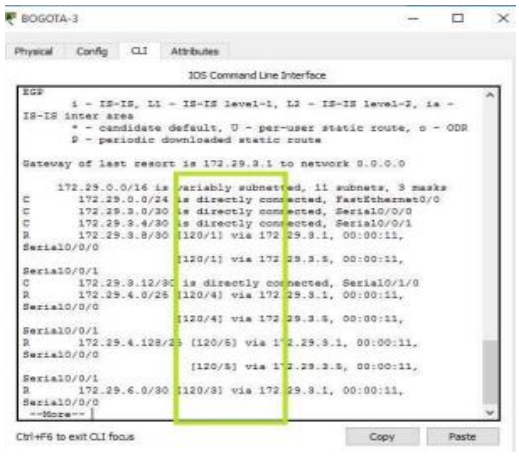


Figura 27 carga que presentan los routers Bogota

b. 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.

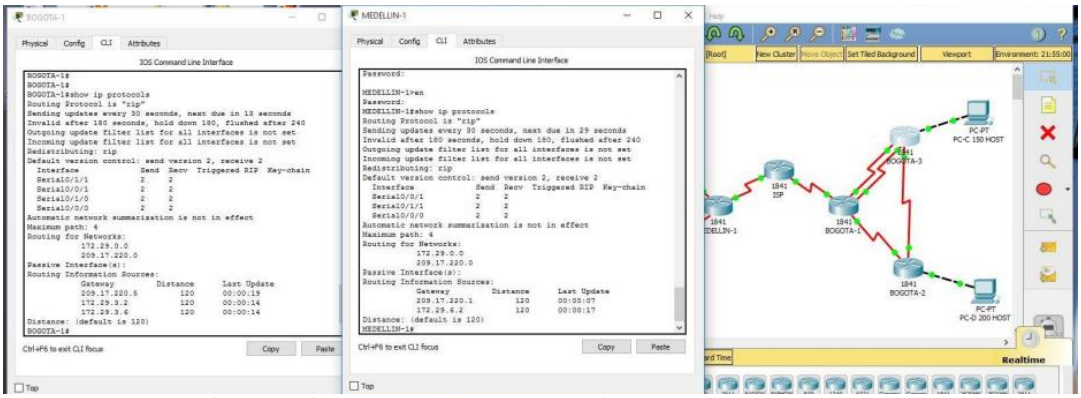


Figura 28 routers Bogotá1 y Medellín1 cierta similitud por su ubicación

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

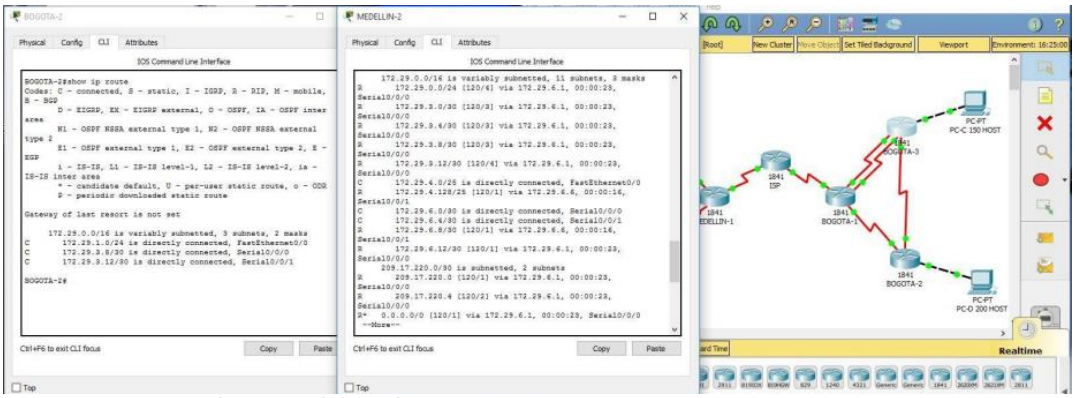


Figura 29 routers Medellín2 y Bogotá2 también presentan redes conectadas directamente

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

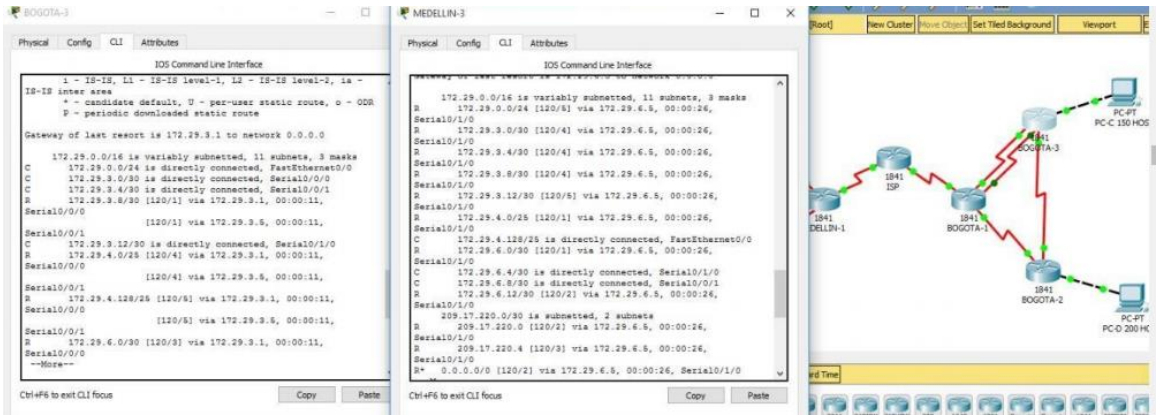


Figura 30 rutas redundantes

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

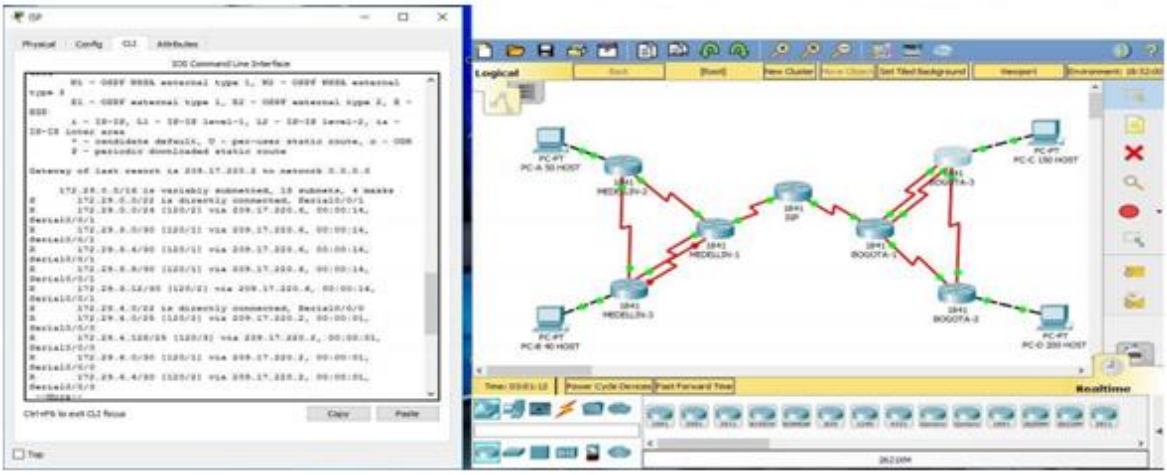


Figura 31 router ISP indica sus rutas estáticas adicionales a las directamente conectadas.

2.1.35 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.

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 requiere

Tabla 2 interfaces de cada router que no necesitan desactivación.

2.1.36 Parte 4 Verificación del protocolo RIP.

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.

Router ISP

Prohibido el acceso a personal no autorizado

User Access Verification

Password:

Password:

ISP>en

Password:

ISP#conf t

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

ISP(config)#route rip

ISP(config-router)#passive-interface f0/0

ISP(config-router)#passive-interface f0/1

ISP(config-router)#

Router MEDELLIN1

Prohibido el acceso a personas no autorizadas

User Access Verification

Password:

MEDELLIN-1>en

Password:

MEDELLIN-1#conf t

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

MEDELLIN-1(config)#route rip

MEDELLIN-1(config-router)#passive-interface f0/0

MEDELLIN-1(config-router)#passive-interface f0/1

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

MEDELLIN-1(config-router)#

Router MEDELLIN2

Prohibido el acceso a personas no autorizadas

User Access Verification

Password:

Password:

MEDELLIN-2>en

Password:

MEDELLIN-2#conf t

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

MEDELLIN-2(config)#route rip

MEDELLIN-2(config-router)#passive-interface f0/0

MEDELLIN-2(config-router)#passive-interface f0/1

MEDELLIN-2(config-router)#

Router MEDELLIN-3

Prohibido el acceso a personas no autorizadas

User Access Verification

Password:

MEDELLIN-3>en

Password:

MEDELLIN-3#conf t

45

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

MEDELLIN-3(config)#route rip

MEDELLIN-3(config-router)#passive-interface f0/0

MEDELLIN-3(config-router)#passive-interface f0/1

MEDELLIN-3(config-router)#

Router BOGOTA1

Prohibido el acceso a personas no autorizadas

User Access Verification

Password:

BOGOTA-1>en

Password:

BOGOTA-1#conf t

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

BOGOTA-1(config)#route rip

BOGOTA-1(config-router)#passive-interface f0/0

BOGOTA-1(config-router)#passive-interface f0/1

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

BOGOTA-1(config-router)#

Router BOGOTA-2

Prohibido el acceso a personas no autorizadas

User Access Verification

Password:

BOGOTA-2>en

Password:

BOGOTA-2#conf t

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

BOGOTA-2(config)#route rip

BOGOTA-2(config-router)#passive-interface f0/0

BOGOTA-2(config-router)#passive-interface f0/1

BOGOTA-2(config-router)#

Router BOGOTA-3

Prohibido el acceso a personas no autorizadas

User Access Verification

Password:

Password:

BOGOTA-3>en

Password:

BOGOTA-3#conf t

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

BOGOTA-3(config)#route rip

BOGOTA-3(config-router)#passive-interface f0/0

BOGOTA-3(config-router)#passive-interface f0/1

BOGOTA-3(config-router)#

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.

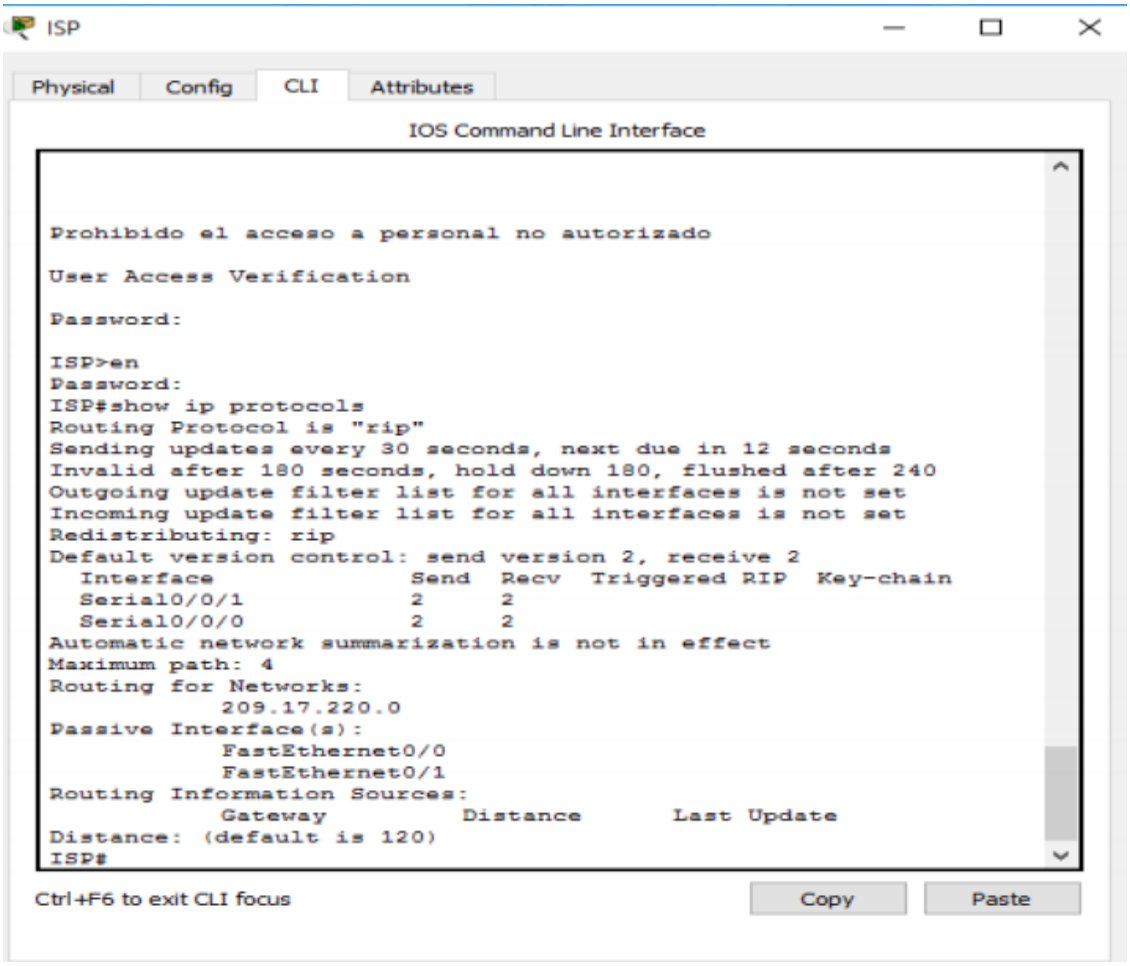


Figura 32 router ISP

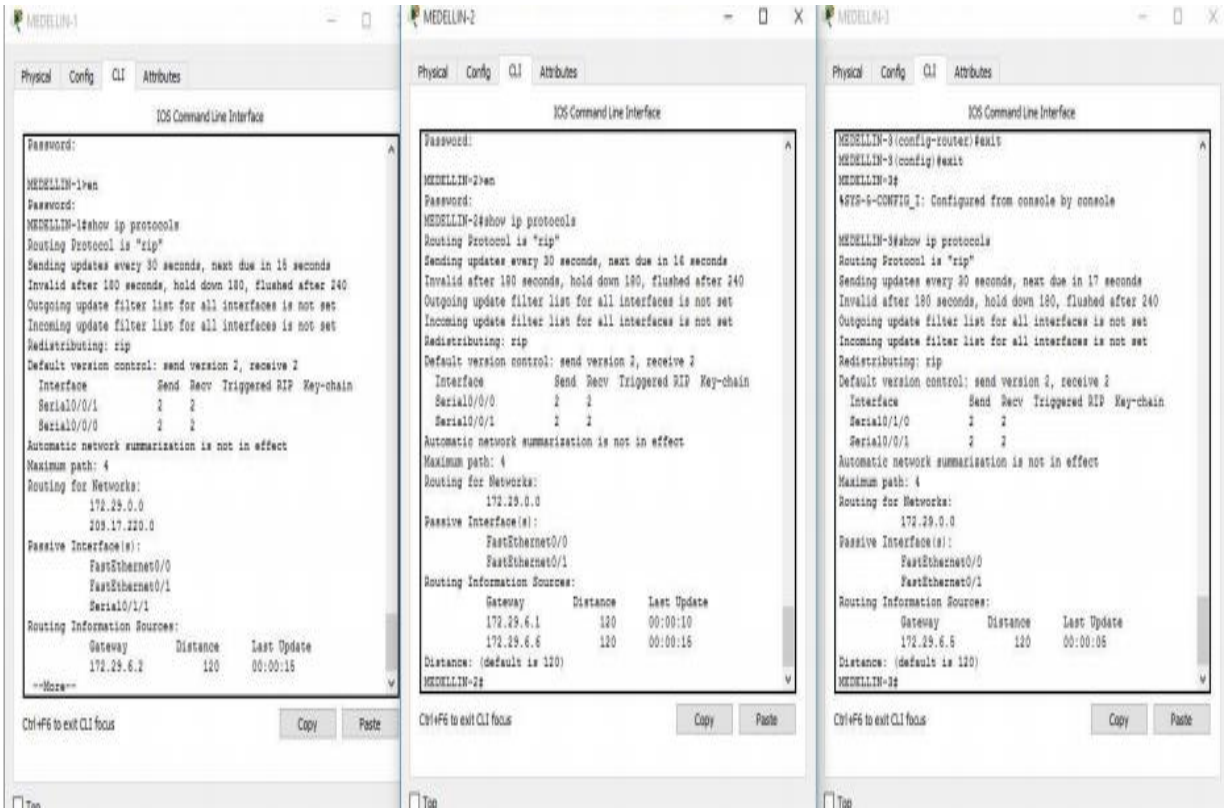


Figura 33 routers Medellin

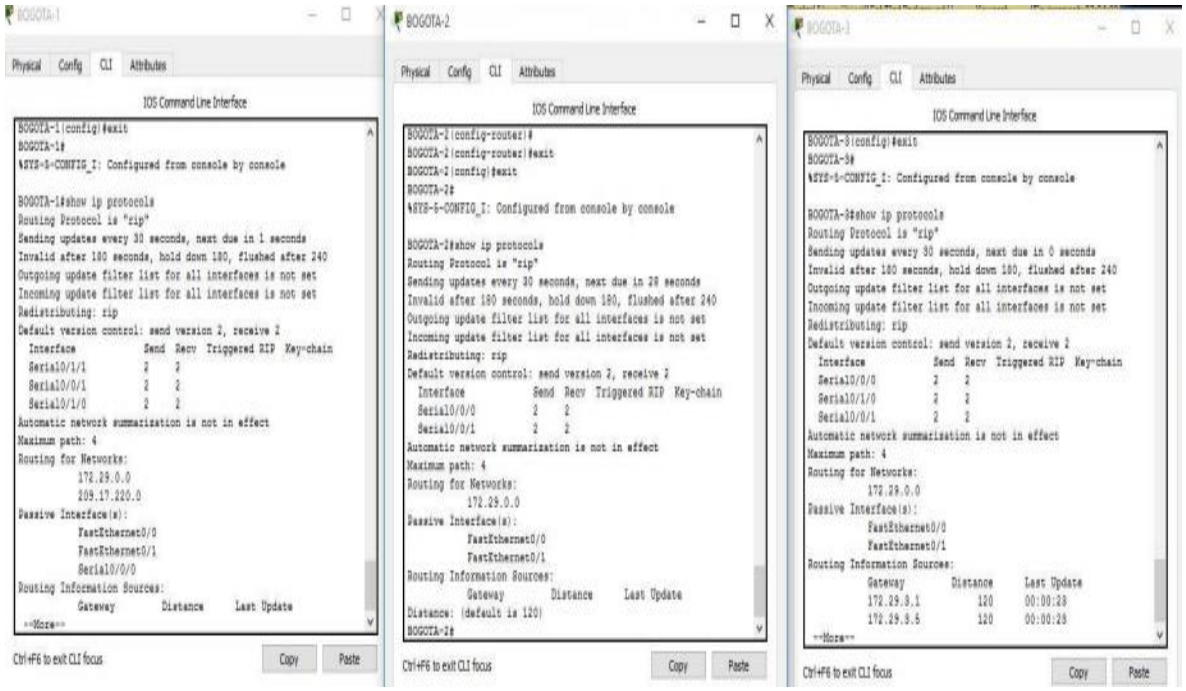


Figura 34 routers Bogota

2.1.37 Parte 5 Configurar encapsulamiento y autenticación PPP.

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

MEDELLIN-1#conf t

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

MEDELLIN-1(config)#username DIANA password UNAD

MEDELLIN-1(config)#INT S0/1/1

MEDELLIN-1(config-if)#encapsulation ppp

MEDELLIN-1(config-if)#ppp authentication pap

MEDELLIN-1(config-if)#ppp pap sent-username DIANA password UNAD

PPP: Warning: You have chosen a username/password combination that

is valid for CHAP. This is a potential security hole.

MEDELLIN-1(config-if)#

ISP>en

Password:

ISP#conf t

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

ISP(config)#username DIANA password UNAD

ISP(config)#int s0/0/0

ISP(config-if)#encapsulation ppp

ISP(config-if)#ppp pap sent-username DIANA password UNAD

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

BOGOTA-1>en

Password:

BOGOTA-1#conf t

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

BOGOTA-1(config)#username ISP password UNAD

BOGOTA-1(config)#int s0/0/0

BOGOTA-1(config-if)#encapsulation ppp

BOGOTA-1(config-if)#

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

BOGOTA-1(config-if)#ppp authentication chap

ISP(config-if)#

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

49

ISP(config-if)#username BOGOTA1 password UNAD

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 Serial0/0/0, changed state to up

ISP(config-if)#username BOGOTA-1 password UNAD

ISP(config)#int s0/0/1

ISP(config-if)#encapsulation ppp

ISP(config-if)#

ISP(config-if)#ppp authentication chap

ISP(config-if)#

2.1.38 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.

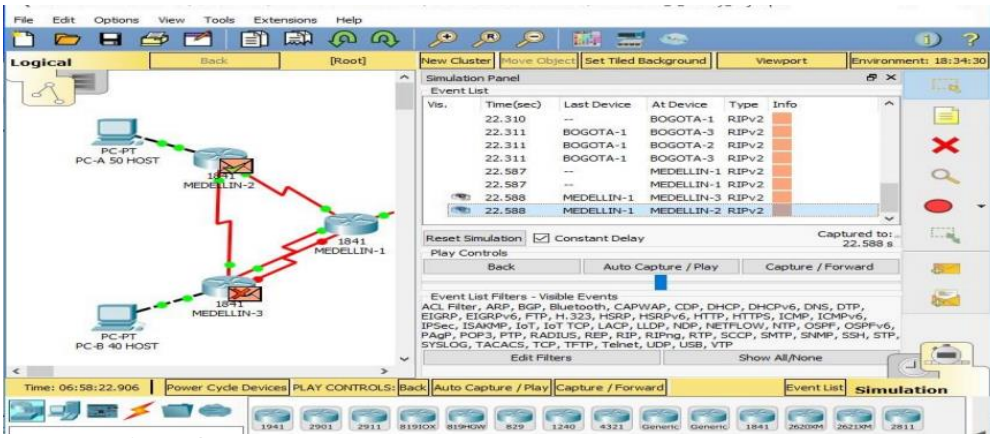


Figura 35 Configuración de PAT

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.

Prohibido el acceso a personas no autorizadas

User Access Verification

Password:

MEDELLIN-1>en

Password:

MEDELLIN-1#conf t

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

MEDELLIN-1(config)#access-list 1 permit 172.29.4.0 0.0.3.255

MEDELLIN-1(config)#ip nat inside source list 1 interface serial0/1/1 overload

MEDELLIN-1(config)#interface s0/1/1

MEDELLIN-1(config-if)#ip nat outside

MEDELLIN-1(config-if)#interface s0/0/0

MEDELLIN-1(config-if)#ip nat inside

MEDELLIN-1(config-if)#interface s0/0/1

MEDELLIN-1(config-if)#ip nat inside

MEDELLIN-1(config-if)#interface s0/1/0

MEDELLIN-1(config-if)#ip nat inside

MEDELLIN-1(config-if)#

2.1.39 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.

User Access Verification

Password:

MEDELLIN-2>en

Password:

MEDELLIN-2#conf t

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

MEDELLIN-2(config)#ip dhcp excluded-address 172.29.4.0 172.29.4.6

MEDELLIN-2(config)#ip dhcp excluded-address 172.29.4.128 172.29.4.133

MEDELLIN-2(config)#ip dhcp pool MEDELLIN-3

MEDELLIN-2(dhcp-config)#network 172.29.4.128 255.255.255.128

MEDELLIN-2(dhcp-config)#default-router 172.29.4.129

MEDELLIN-2(dhcp-config)#dns-server 1.1.1.1

MEDELLIN-2(dhcp-config)#ip dhcp pool MEDELLIN-2

MEDELLIN-2(dhcp-config)#network 172.29.4.0 255.255.255.128

MEDELLIN-2(dhcp-config)#default-router 172.29.4.1

MEDELLIN-2(dhcp-config)#dns-server 1.1.1.1

MEDELLIN-2(dhcp-config)#

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

User Access Verification

Password:

MEDELLIN-3>en

Password:

MEDELLIN-3#conf t

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

MEDELLIN-3(config)#int f0/0

MEDELLIN-3(config-if)#ip helper-address 172.29.6.5

MEDELLIN-3(config-if)#

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

Prohibido el acceso a personas no autorizadas

User Access Verification

Password:

BOGOTA-2>en

Password:

BOGOTA-2#conf t

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

BOGOTA-2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.6

BOGOTA-2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.6

BOGOTA-2(config)#ip dhcp pool BOGOTA-3

BOGOTA-2(dhcp-config)#neywork 172.29.0.0 255.255.255.0

BOGOTA-2(dhcp-config)#network 172.29.0.0 255.255.255.0

BOGOTA-2(dhcp-config)#default-router 172.29.0.1

BOGOTA-2(dhcp-config)#dns-server 1.1.1.1

BOGOTA-2(dhcp-config)#ip dhcp pool BOGOTA-2

BOGOTA-2(dhcp-config)#network 172.29.1.0 255.255.255.0

BOGOTA-2(dhcp-config)#default-router 172.29.1.1

BOGOTA-2(dhcp-config)#dns-server 1.1.1.1

BOGOTA-2(dhcp-config)#

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

Prohibido el acceso a personas no autorizadas

User Access Verification

Password:

BOGOTA-3>en

Password:

BOGOTA-3#conf t

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

BOGOTA-3(config)#int f0/0

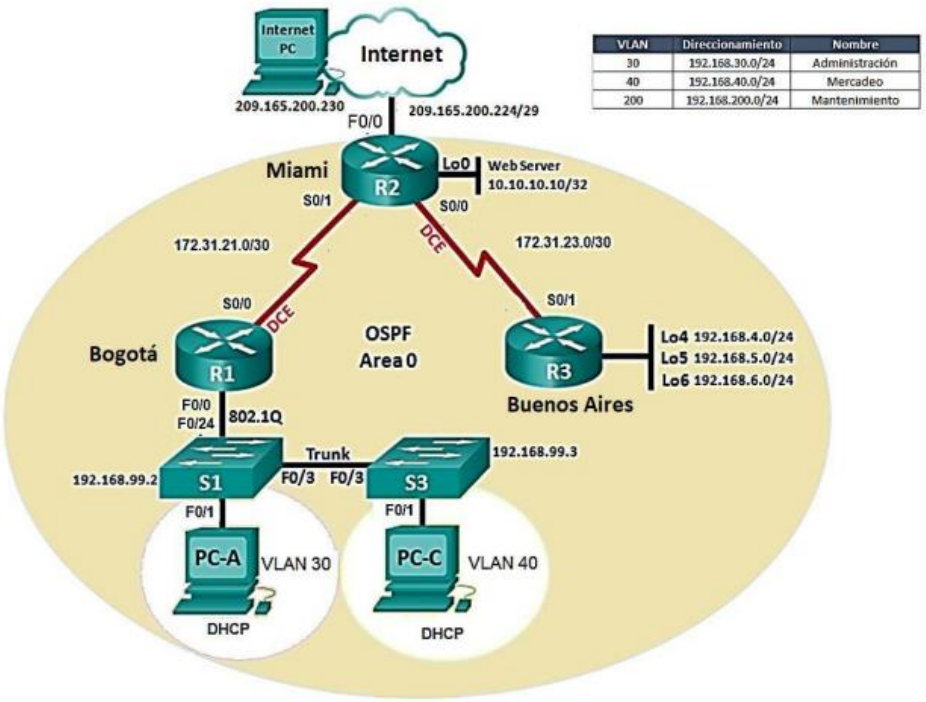
BOGOTA-3(config-if)#ip helper-address 172.29.3.13

BOGOTA-3(config-if)#

2.2 ESCENARIO 2

Escenario: Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Miami, Bogotá y Buenos Aires, 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.

2.2.1 TOPOLOGIA DE LA RED



VLAN	Direccionamiento	Nombre
30	192.168.30.0/24	Administración
40	192.168.40.0/24	Mercadeo
200	192.168.200.0/24	Mantenimiento

Figura 36 TOPOLOGIA DE LA RED

Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario

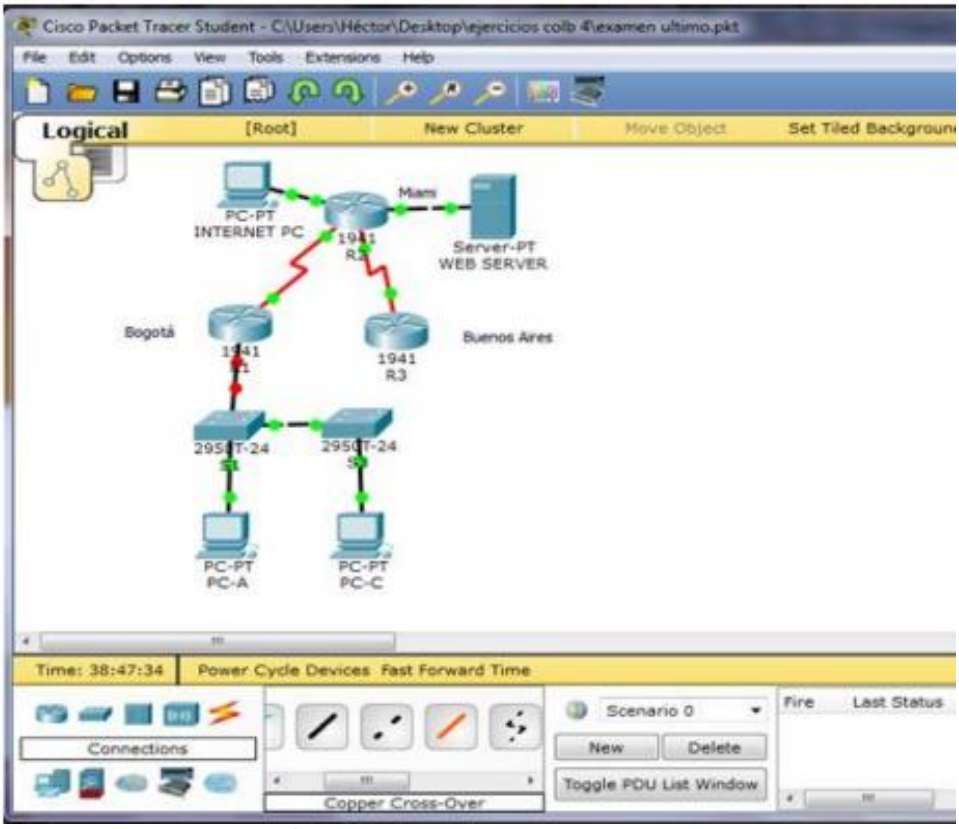


Figura 37 IP acorde con la topología de red para cada uno de los dispositivos

2.2.2 Tablas de direccionamiento

DISPOSITIVO	INTERFAZ	DIRECCIÓN	MASCARA
BOGOTA R 1	S0/0/0	172.31.21.1	255.255.255.252
	F0/0.30	192.168.30.1	255.255.255.252
	F0/0.40	192.168.40.1	255.255.255.252
	F0/0.200	192.168.200.1	255.255.255.252
MIAMI R2	S0/0/0	172.31.23.1	255.255.255.252
	S0/0/1	172.31.21.2	255.255.255.252
	F0/0	209.165.200.225	255.255.255.248
	F0/1	10.10.10.1	255.255.255.0
BUENOS AIRES R3	S0/0/1	172.31.23.2	255.255.255.252
	Lo4	192.168.4.1	255.255.255.0
	Lo5	192.168.5.1	255.255.255.0
	Lo6	192.168.6.1	255.255.255.0

S1	Fa 0/1	VLAN 30	
	Fa 0/3	TRONCAL	
	Fa 0/24	TRONCAL	
S3	Fa 0/1	VLAN40	
	Fa 0/3	TRONCAL	
PC-A	Fa 0	DHCP	
PC-C	Fa 0	DHCP	
WEB SERVER	Fa 0	10.10.10.10	255.255.255.0
PC INTERNET	Fa 0	209.165.200.230	255.255.255.248

Tabla VLANs

VLAN	**EQUIPO**	**DIRECCIONAMIENTO**		**NOMBRE**
VLAN 30	PC-A	192.168.30.0	255.255.255.0	ADMINISTRACIÓN
VLAN 40	PC-C	192.168.40.0	255.255.255.128	MERCADEO
VLAN400		192.168.200.0	255.255.255.192	MANTENIMIENTO

Tabla 3 direccionamiento

2.2.3 Configuración parámetros y direccionamiento ip, routers y switches

2 2.2.4 Configuración S1

Switch>en

Switch#conf t

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

Switch(config)#hostname S1

S1(config)#enable secret class

S1(config)#line vty 0 5

S1(config-line)#password cisco

S1(config-line)#login

S1(config-line)#line console 0

S1(config-line)#password cisco

S1(config-line)#login

S1(config-line)#line console 0

S1(config-line)#login

S1(config-line)#service password-encryption
S1(config)#banner motd $Prohibido el acceso a personas no autorizadas$
S1(config)#exit
S1#
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#

2.2.5 Configuración S3

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line vty 0 5
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#service password-encryption
S3(config)#banner motd $Prohibido el acceso a personas no autorizadas$
S3(config)#exit
S3#
S3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S3#

2.2.6 Configuración R1 BOGOTA

Router>en

Router#conf t

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

Router(config)#hostname Bogota

Bogota(config)#enable secret claas

Bogota(config)#line vty 0 5

Bogota(config-line)#password cisco

Bogota(config-line)#login

Bogota(config-line)#line console0

Bogota(config-line)#password cisco

Bogota(config-line)#login

Bogota(config-line)#service password-encryption

Bogota(config)#banner motd $prohibido el acceso a personal no autorizado$

Bogota(config)#exit

Bogota#

S1>en

Password:

S1#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...[OK]

2.2.7 Configuración R2 MIAMI

Router>en

Router#conf t

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

Router(config)#hostname MIAMI

MIAMI(config)#enable secret class

MIAMI(config)#line vty 0 5

MIAMI(config-line)#password cisco

MIAMI(config-line)#login
MIAMI(config-line)#line console 0
MIAMI(config-line)#password cisco
MIAMI(config-line)#login
MIAMI(config-line)#service password-encryption
MIAMI(config)#banner motd $Prohibido el acceso a personal no autorizado$
MIAMI(config)#exit
MIAMI#
MIAMI#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

2.2.8 Configuración R3 BUENOS AIRES

Router(config)#hostname BUENOSAIRES
BUENOSAIRES(config)#enable secret class
BUENOSAIRES(config)#line vty 0 5
BUENOSAIRES(config-line)#password cisco
BUENOSAIRES(config-line)#login
BUENOSAIRES(config-line)#line console 0
BUENOSAIRES(config-line)#password cisco
BUENOSAIRES(config-line)#login
BUENOSAIRES(config-line)#service password-encryption
BUENOSAIRES(config)#banner motd $Prohibido el acceso a personas no autorizadas$
BUENOSAIRES(config)#exit
BUENOSAIRES#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

2.2.9 Configuración de VLANs en Switches

2.2.10 Configuración S1

Prohibido el acceso a personas no autorizadas
User Access Verification
Password:
S1>en
Password:
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 30
S1(config-vlan)#name ADMINISTRACION
S1(config-vlan)#vlan 40
S1(config-vlan)#name Mercadeo
S1(config-vlan)#vlan 200
S1(config-vlan)#name MANTENIMIENTO
S1(config-vlan)#exit
S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
S1(config)#int f0/24
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#no sh
S1(config-if)#interface range fa0/2,fa0/4-23,g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#exit
S1(config)#int f0/1

S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1(config-if)#interface range fa0/2,fa0/4-23,g0/1-2
S1(config-if-range)#exit
S1(config)#int vlan 200
S1(config-if)#
S1(config-if)#ip address 192.168.200.2 255.255.255.252
S1(config-if)#ip default-gateway 192.168.200.1
S1(config)#exit
S1#
S1#copy running-config startup-config

2.2.11 Configuración S3

User Access Verification
Password:
S3>en
Password:
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 30
S3(config-vlan)#name ADMINISTRACION
S3(config-vlan)#vlan 40
S3(config-vlan)#name MERCADEO
S3(config-vlan)#vlan 200
S3(config-vlan)#name ADMINISTRACION
VLAN #30 and #200 have an identical name: ADMINISTRACION
S3(config-vlan)#name MANTENIMIENTO
S3(config-vlan)#exit
S3(config)#int vlan 200
S3(config-if)#

S3(config-if)#ip address 192.168.200.3 255.255.255.252
Bad mask /30 for address 192.168.200.3
S3(config-if)#ip default-gateway 192.168.200.1
S3(config)#int f0/3
S3(config-if)#switchport trunk
% Incomplete command.
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#int range f0/2,f0/4-24,g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#int f0/1
S3(config-if)#switchport mode access
S3(config-if)#int range f0/2,f0/4-24,g0/1-2
S3(config-if-range)#sh
S3(config-if-range)#exit
S3(config)#exit
S3#
S3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

2.2.12 Configuración interfaces en routers

2.2.13 R1 BOGOTA

Bogota>en
Password:
Password:
Bogota#conf t
Enter configuration commands, one per line. End with CNTL/Z.

Bogota(config)#int s0/0/0
Bogota(config-if)#description conexion con MIAMI
Bogota(config-if)#ip address 172.31.21.1 255.255.255.252
Bogota(config-if)#clock
% Incomplete command.
Bogota(config-if)#clock rate 128000
This command applies only to DCE interfaces
Bogota(config-if)#no sh
Bogota(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/0
Bogota(config)#

2.2.14 R2 MIAMI

Prohibido el acceso a personal no autorizado
User Access Verification
Password:
MIAMI>en
Password:
MIAMI#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MIAMI(config)#int s0/0/0
MIAMI(config-if)#ip address 172.31.23.1 255.255.255.252
MIAMI(config-if)#clock rate 128000
This command applies only to DCE interfaces
MIAMI(config-if)#no sh
MIAMI(config-if)#int s0/0/1
MIAMI(config-if)#ip address 172.31.21.1 255.255.255.252
MIAMI(config-if)#clock rate 128000
MIAMI(config-if)#no sh
MIAMI(config-if)#
MIAMI(config-if)#int.

MIAMI(config-if)#int fa0/0
MIAMI(config-if)#ip address 209.165.200.225 255.255.255.248
MIAMI(config-if)#no sh
MIAMI(config-if)#
MIAMI(config-if)#ip route 0.0.0.0 0.0.0.0 f0/0
MIAMI(config)#int fa0/1
MIAMI(config-if)#ip address 10.10.10.1 255.255.255.0
MIAMI(config-if)#no sh
MIAMI(config-if)#

2.2.15 R3 BUENOS AIRES

Prohibido el acceso a personas no autorizadas
User Access Verification
Password:
BUENOSAIRES>en
Password:
BUENOSAIRES#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUENOSAIRES(config)#int s0/0/1
BUENOSAIRES(config-if)#ip address 172.31.23.2 255.255.255.252
BUENOSAIRES(config-if)#no sh
BUENOSAIRES(config-if)#
BUENOSAIRES(config-if)#ip route
BUENOSAIRES(config-if)#ip route 0.0.0.0 0.0.0.0 s0/0/1
BUENOSAIRES(config)#int lo4
BUENOSAIRES(config-if)#
BUENOSAIRES(config-if)#ip address 192.168.4.1 255.255.255.0
BUENOSAIRES(config-if)#int lo5
BUENOSAIRES(config-if)#
BUENOSAIRES(config-if)#ip address 192.168.5.1 255.255.255.0
BUENOSAIRES(config-if)#int lo6

BUENOSAIRES(config-if)#

BUENOSAIRES(config-if)#ip address 192.168.6.1 255.255.255.0

BUENOSAIRES(config-if)

2.2.16 Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

OSPFv2 area 0

Configuration Item or Task	**Specification**
Router ID R1	1.1.1.1
Router ID R2	5.5.5.5
Router ID R3	8.8.8.8
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales	256 Kb/s
Ajustar el costo en la métrica de s0/0a	9500

Tabla 4 enrutamiento OSPF v2

2.2.17 Configuracion en BOGOTA

prohibido el acceso a personal no autorizado

User Access Verification

Password:

Bogota>en

Password:

Bogota#conf t

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

Bogota(config)#router ospf 1

Bogota(config-router)#router-id 1.1.1.1

Bogota(config-router)#network 172.31.21.0 0.0.0.3 area 0

Bogota(config-router)#network 172.168.30.0 0.0.0.255 area 0

Bogota(config-router)#network 172.168.40.0 0.0.0.255 area 0

Bogota(config-router)#network 172.168.200.0 0.0.0.255 area 0

Bogota(config-router)#passive-interface f0/0.30

%Invalid interface type and number
Bogota(config-router)#passive-interface f0/0.40
%Invalid interface type and number
Bogota(config-router)#passive-interface f0/0.200
%Invalid interface type and number
Bogota(config-router)#passive-interface f0/0-30
Bogota(config-router)#passive-interface f0/0
Bogota(config-router)#int s0/0/0
Bogota(config-if)#bandwidth 256
Bogota(config-if)#exit
Bogota(config)#int s0/0/0
Bogota(config-if)#ip ospf cost 9500
Bogota(config-if)#

2.2.18 Configuracion en MIAMI

Password:
MIAMI>en
Password:
MIAMI#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MIAMI(config)#router ospf 1
MIAMI(config-router)#router-id 5.5.5.5
MIAMI(config-router)#network 172.31.21.0 0.0.0.3 area 0
MIAMI(config-router)#
MIAMI(config-router)#network 172.31.23.0 0.0.0.3 area 0
MIAMI(config-router)#network 10.10.10.0 0.0.0.255 area 0
MIAMI(config-router)#passive-interface f0/1
MIAMI(config-router)#exit
MIAMI(config)#int s0/0/0
MIAMI(config-if)#bandwidth 256

MIAMI(config-if)#int s0/0/1
MIAMI(config-if)#bandwidth 256
MIAMI(config-if)#int s0/0/0
MIAMI(config-if)#ip ospf cost 9500
MIAMI(config-if)#

2.2.19 Configuración BUENOS AIRES

Prohibido el acceso a personas no autorizadas
User Access Verification
Password:
BUENOSAIRES>en
Password:
BUENOSAIRES#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUENOSAIRES(config)#router ospf 1
BUENOSAIRES(config-router)#router-id 8.8.8.8
BUENOSAIRES(config-router)#exit
BUENOSAIRES(config)#network 172.31.23.0 0.0.0.3 area
^
% Invalid input detected at '^' marker.
BUENOSAIRES(config)#network 172.31.23.0 0.0.0.3 area 0
^
2.2.18 Configuracion en MIAMI
User Access Verification
% Invalid input detected at '^' marker.
BUENOSAIRES(config)#network 172.31.23.0 0.0.0.3 area 0
BUENOSAIRES(config)#172.31.23.0 0.0.0.3 area 0
Invalid input detected at '^' marker.
BUENOSAIRES(config)#router-id 8.8.8.8
Invalid input detected at '^' marker.

BUENOSAIRES(config)#route ospf 1

BUENOSAIRES(config-router)#router-id 8.8.8.8

BUENOSAIRES(config-router)#network 172.31.23.0 0.0.0.3 area 0

BUENOSAIRES(config-router)#network 172.31.23.0 0.0.0.3 area

04:16:50: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0/1 from LOADING to FULL,

Load

BUENOSAIRES(config-router)#network 192.168.4.0 0.0.3.255 area 0

BUENOSAIRES(config-router)#passive-interface lo4

BUENOSAIRES(config-router)#passive-interface lo5

BUENOSAIRES(config-router)#passive-interface lo6

BUENOSAIRES(config-router)#exit

BUENOSAIRES(config)#int s0/0/1

BUENOSAIRES(config-if)#bandwidth 256

BUENOSAIRES(config-if)#ip ospf cost 9500

BUENOSAIRES(config-if)#

2.2.20 Verificar informacion de OSPF

• Visualizar tablas de enrutamiento y routers conectados por OSPFv2

• Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface

• Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks,

and passive interfaces configuradas en cada router

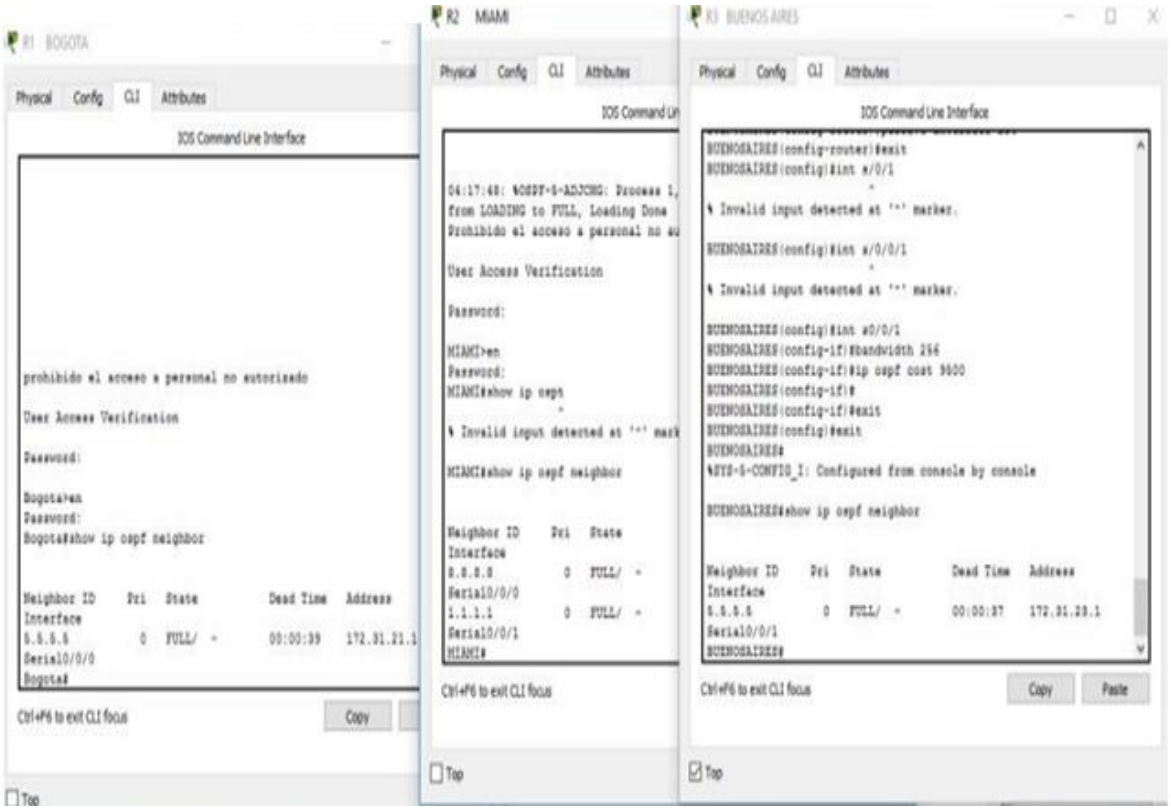


Figura 38 informacion de OSPF

Figura 39 informacion de ospf

2.2.21 Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, InterVLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.

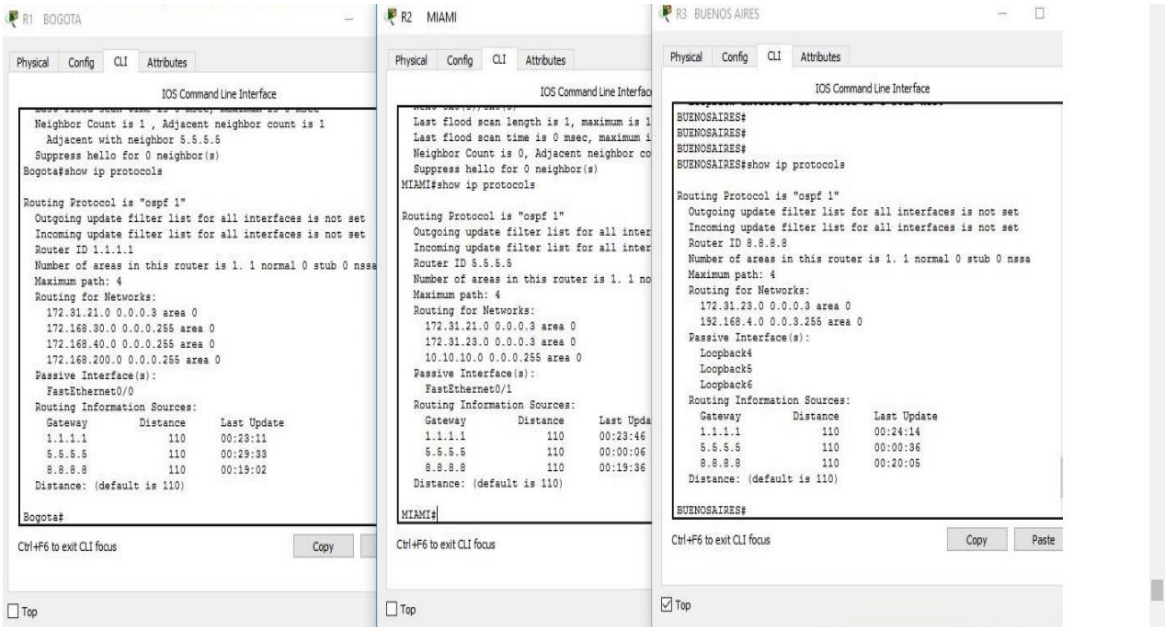


Figura 40 VLAN Routing y Seguridad en los Switches

2.2.22 En el Switch 3 deshabilitar DNS lookup

Prohibido el acceso a personas no autorizadas

User Access Verification

Password:

S3>en

Password:

S3#conf t

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

S3(config)#no ip domain lookup

S3(config)#

2.2.23 Asignar direcciones IP a los Switches acorde a los lineamientos.

```
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int vlan200
S1(config-if)#ip address 192.168.200.2 255.255.255.0
S1(config-if)#no sh
S1(config-if)#
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#no ip domain lookup
S3(config)#int vlan200
S3(config-if)#ip address 192.168.200.3 255.255.255.0
S3(config-if)#no sh
```

2.2.24 Desactivar todas las interfaces que no sean utilizadas en el esquema de red.

```
S1(config)#int range fa0/2,fa0/4-23
S1(config-if-range)#sh
S1(config-if-range)#
S3(config)#int range f0/2,f0/4-24
S3(config-if-range)#
```

2.2.25 Implement DHCP and NAT for IPv4

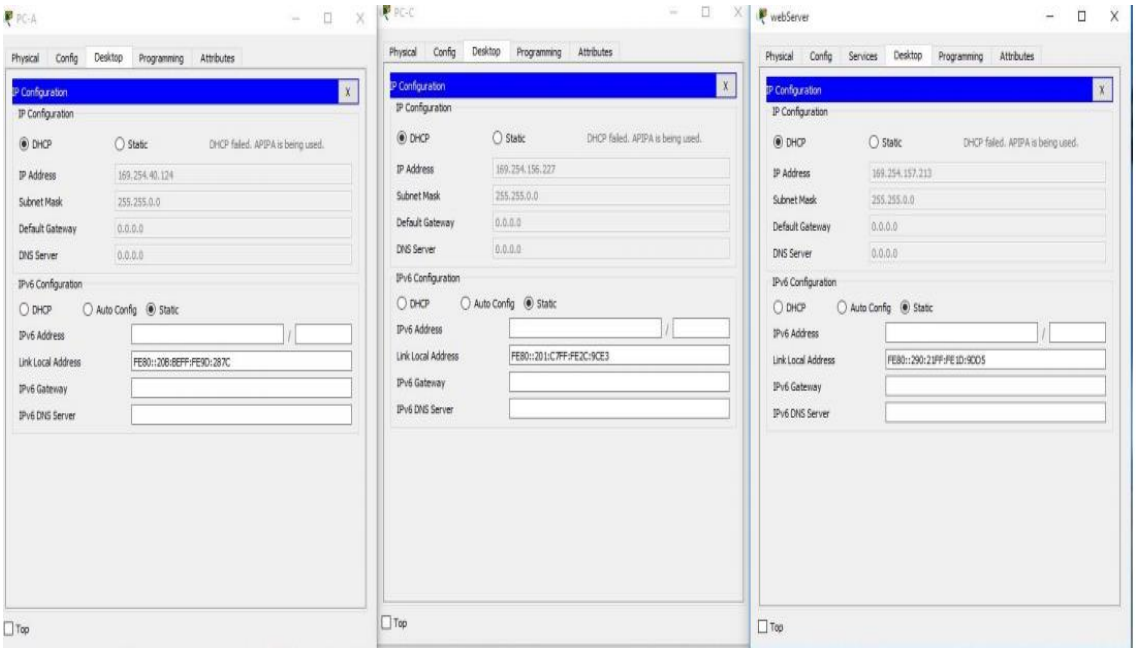


Figura 41 DHCP and NAT for IPv4

2.2.26 Configurar R1 como servidor DHCP para las VLANs 30 y 40.

Bogota>en

Password:

Bogota#conf t

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

Bogota(config)#ip dhcp pool ADMINISTRACION

Bogota(dhcp-config)#dns-server 10.10.10.11

Bogota(dhcp-config)#default-router 192.168.30.1

Bogota(dhcp-config)#network 192.168.30.0 255.255.255.0

Bogota(dhcp-config)#ip domain-name ccna-unad.com

Bogota(config)#

Bogota#conf t

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

Bogota(config)#ip dhcp pool ADMINISTRACION

Bogota(dhcp-config)#dns-server 10.10.10.11

Bogota(dhcp-config)#default-router 192.168.30.1

Bogota(dhcp-config)#network 192.168.30.0 255.255.255.0

Bogota(dhcp-config)#ip domain-name ccna-unad.com

Bogota(config)#ip dhcp pool MERCADEO

Bogota(dhcp-config)#dns-server 10.10.10.11

Bogota(dhcp-config)#default-router 192.168.40.1

Bogota(dhcp-config)#network 192.168.40.0 255.255.255.0

Bogota(dhcp-config)#ip domain-name ccna-unad-comBogota(config)#

2.2.27 Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

Configurar DHCP pool para VLAN 30	Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway
Configurar DHCP pool para VLAN 40	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway

Tabla 5 configuraciones estáticas

Bogota>en

Password:

Bogota#conf t

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

Bogota(config)#ip dhcp pool ADMINISTRACION

Bogota(dhcp-config)#dns-server 10.10.10.11

Bogota(dhcp-config)#default-router 192.168.30.1

Bogota(dhcp-config)#network 192.168.30.0 255.255.255.0

Bogota(dhcp-config)#ip domain-name ccna-unad.com

Bogota(config)#

Bogota#conf t

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

Bogota(config)#ip dhcp pool ADMINISTRACION

Bogota(dhcp-config)#dns-server 10.10.10.11

Bogota(dhcp-config)#default-router 192.168.30.1

Bogota(dhcp-config)#network 192.168.30.0 255.255.255.0

Bogota(dhcp-config)#ip domain-name ccna-unad.com

Bogota(config)#ip dhcp pool MERCADEO

Bogota(dhcp-config)#dns-server 10.10.10.11

Bogota(dhcp-config)#default-router 192.168.40.1

Bogota(dhcp-config)#network 192.168.40.0 255.255.255.0

Bogota(dhcp-config)#ip domain-name ccna-unad-com

Bogota(config)#

2.2.28 Configurar NAT en R2 para permitir que los hosts puedan salir a internet

MIAMI#conf t

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

MIAMI(config)#ip nat inside source static 10.10.10.10 209.166.200.229

MIAMI(config)#int f0/0

MIAMI(config-if)#ip nat outside

MIAMI(config-if)#int f0/1

MIAMI(config-if)#ip nat inside

MIAMI(config-if)

2.2.29 Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

restringir o permitir tráfico desde R1 o R3 hacia R2.

MIAMI(config)#access-list 1 permit 192.168.30.0 0.0.0.255

MIAMI(config)#access-list 1 permit 192.168.40.0 0.0.0.255

MIAMI(config)#access-list 1 permit 192.168.4.0 0.0.3.255

MIAMI(config)#

2.2.30 Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

MIAMI(config)#access-list 101 permit tcp any host 209.165.200.229

MIAMI(config)#access-list 101 permit icmp any any echo-reply

MIAMI(config)#

2.2.31 Verificar procesos de comunicación y re direccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

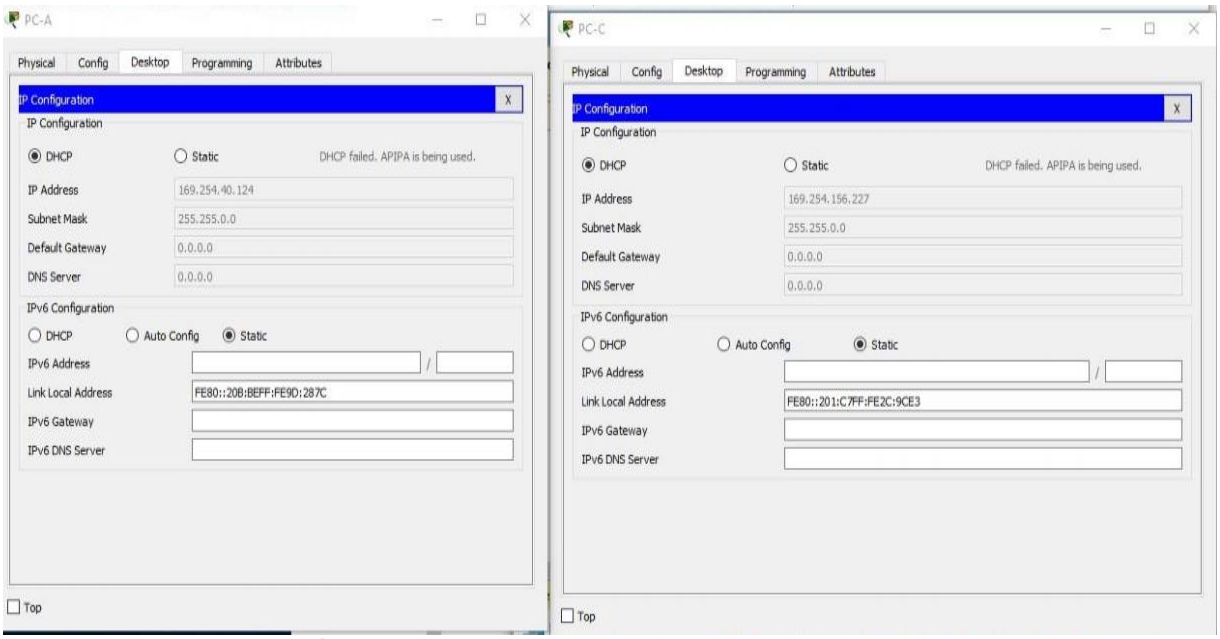


Figura 42 procesos de comunicación

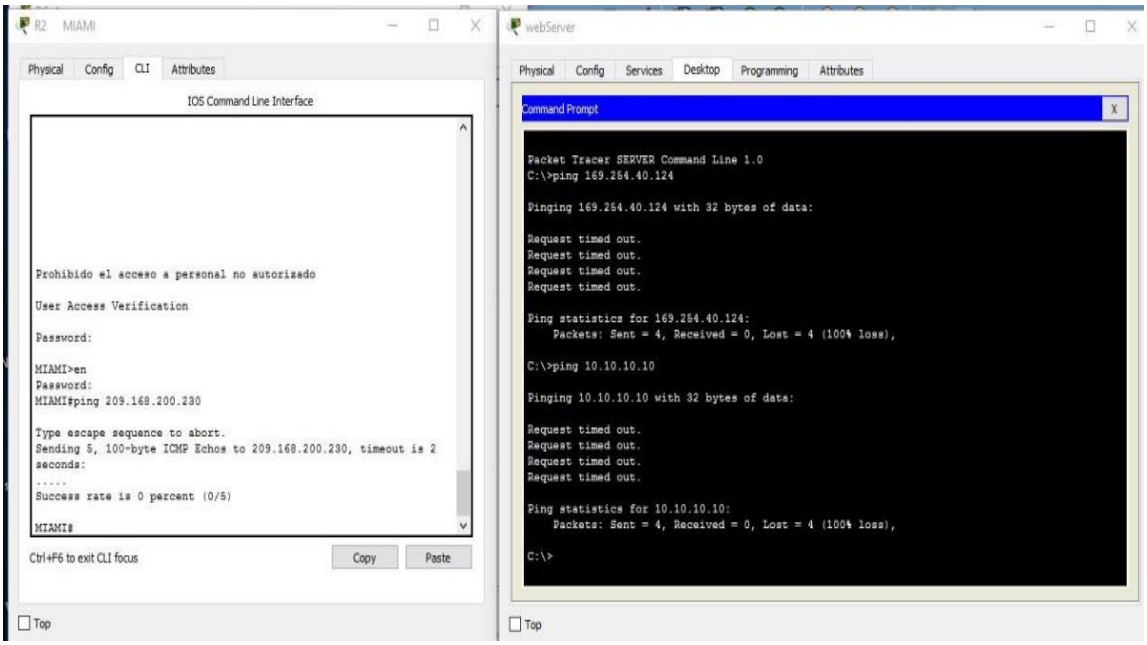


Figura 43 direccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

3. CONCLUSIONES

Mediante el presente proyecto se pretende mostrar el conocimiento adquirido durante el diplomado de Cisco CCNA sobre diseño e implementación de soluciones integradas lan / wan lo cual se ha hecho mucho énfasis en la herramienta Packet Tracer con la cual se realizarán simulaciones, así como también topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales.

En este trabajo se crean topologías físicas y análisis de las diferentes redes, una vez completada la configuración física y lógica de la red, también se puede hacer simulaciones de conectividad: pings, etc., todo ello desde las mismas consolas incluidas.

En el trascurso de todas las actividades en la plataforma cisco, se logró realizar de manera gradual los procedimientos básicos para configuración de una red básica como compleja, donde se logra identificar, analizar y configurar dispositivos de red según las necesidades requeridas, durante todo el desarrollo de la asignatura se logra comprender la importancia que debe tener todo equipo de red a la hora de asignar las direcciones IP, hasta implementar protocolos de seguridad en las diferentes capaz y otros apartados más permitiendo una red confiable y robusta.

Durante todo el aprendizaje como estudiante de carrera profesional en sistemas, el Curso de CISCO ha aportado a mis conocimientos en gran medida, gracias a eso mi perfil se vuelve más competente en el ámbito laboral y personal, gracias a que el conocimiento adquirido me abre más puertas de trabajo para alcanzar mis objetivos y metas.

4. REFERENCIAS BIBLIOGRAFICA

-Ángel Calvo, A. C. (2015, 11 mayo). RIP Cisco, aprende a configurar este Protocolo fácilmente. Recuperado 5 junio, 2019, de https://aplicacionesysistemas.com/rip-cisco-version2-de-manera-facil-ysencilla/

- Byspel, B. (2017, 14 junio). Configurar servidor DHCP en Packet Tracer. Recuperado 5 junio, 2019, de https://byspel.com/configurar-servidor-dhcpen-cisco-packet-tracer/

- Colaboradores de Wikipedia. (2019b, 30 abril). Máscara de red - Wikipedia, la enciclopedia libre. Recuperado 5 junio, 2019, de https://es.wikipedia.org/wiki/M%C3%A1scara_de_red

-Eugenio Duarte, E. D. (2016, 13 abril). Cisco CCNA – Cómo Configurar DHCP En Cisco Router. Recuperado 5 junio, 2019, de http://blog.capacityacademy.com/2014/01/09/cisco-ccna-como-configurardhcp-en-cisco-router/

- Rosbarbosa, R. B. (2017, 25 septiembre). IP Helper y Relay Agent – Manteniendo un servidor DHCP en otra red.. Recuperado 5 junio, 2019, de https://www.seaccna.com/ip-helper-relay-agent/

- Temática: Listas de control de acceso CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

- Temática: OSPF de una sola área CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

- Victor E. Martinez G, V. E. M. (2015, 22 abril). Configuración de RIPv2 (protocolo dinámico). Recuperado 5 junio, 2019, de http://theosnews.com/2013/02/configuracion-de-ripv2-protocolo-dinamico/