**PRUEBA DE HABILIDADES PRÁCTICAS CCNA**

**OSCAR CASTELLANOS**

**ACTIVIDAD EVALUATIVA DEL DIPLOMADO DE PROFUNDIZACIÓN CCNA**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD**
**ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI**
**DIPLOMADO DE PROFUNDIZACIÓN CISCO**
**CUNDINAMARCA**
**2019**

**TABLA DE CONTENIDO**

# 1    INDICE DE FIGURAS

## 2 RESUMEN

El término LAN (Red de área local) alude a una red -a veces llamada subred- instalada en una misma sala, oficina o edificio. Los nodos o puntos finales de una LAN se conectan a una topología de red compartida utilizando un protocolo determinado. Con la autorización adecuada, se puede acceder a los dispositivos de la LAN, esto es, estaciones de trabajo, impresoras, etc., desde cualquier otro dispositivo de la misma. Las aplicaciones software desarrolladas para las LAN (mensajería electrónica, procesamiento de texto, hojas electrónicas, etc.) también permiten ser compartidas por los usuarios.

Una red de área ancha o WAN (Red de área amplia) es una colección de LAN interconectadas. Las WAN pueden extenderse a ciudades, estados, países o continentes. Las redes que comprenden una WAN utilizan enrutadores para dirigir sus paquetes al destino apropiado. Los encaminadores son dispositivos hardware que enlazan diferentes redes para proporcionar el camino más eficiente para la transmisión de datos. Estos encaminadores están conectados por líneas de datos de alta velocidad, generalmente, líneas telefónicas de larga distancia, de manera que los datos se envían junto a las transmisiones telefónicas regulares.

Las redes LAN cubren una distancia geográfica relativamente pequeña y tienen altas velocidades de transmisión. Las WAN cubren grandes distancias geográficas, e ilimitadas en algún momento, y operan a velocidades de transmisión más bajas. Las LAN requieren un único proveedor de servicios Internet, o ISP (por sus siglas en inglés), como tu compañía telefónica o de cable, para proporcionar el punto de acceso o conexión. Las WAN por otra parte se basan en las infraestructuras de comunicación múltiples para llevar las señales a grandes distancias, a menudo saltando de una infraestructura a otra.

# 3   ABSTRACT

The term LAN (Local Area Network) refers to a network - sometimes called a subnet - installed in the same room, office or building. The nodes or endpoints of a LAN connect to a shared network topology using a specific protocol. With the proper authorization, you can access the devices on the LAN, that is, workstations, printers, etc., from any other device on it. Software applications developed for LANs (electronic messaging, word processing, electronic sheets, etc.) also allow them to be shared by users.

A wide area network or WAN (Wide Area Network) is a collection of interconnected LANs. WANs can be extended to cities, states, countries or continents. Networks that comprise WAN use routers to direct their packets to the appropriate destination. Routers are hardware devices that link different networks to provide the most efficient path for data transmission. These routers are connected by high-speed data lines, usually long-distance telephone lines, so that the data is sent alongside regular telephone transmissions.

LAN networks cover a relatively small geographical distance and have high transmission speeds. WANs cover large geographical distances, and unlimited at some time, and operate at lower transmission speeds. LANs require a single Internet service provider, or ISP, such as your telephone or cable company, to provide the access point or connection. WANs on the other hand rely on multiple communication infrastructures to carry signals over long distances, often jumping from one infrastructure to another.

# 4 INTRODUCCION

En el presente documento se desarrolló una prueba de habilidades practicas la cual consiste en el análisis de dos escenarios propuestos, donde se realizó una descripción detallada para cada escenario y la implementación de su topología física, las configuraciones de cada uno de los dispositivos y la verificación de la conectividad de cada uno de ellos se realizó por medio de la simulación haciendo uso del software Packet Tracer, el cual es un programa de simulación de redes que permite a los estudiantes experimentar con el comportamiento de la red y resolver dudas respecto a las mismas.

El fin de este trabajo es obtener la certificación CCNA Routing and Switching (Cisco Certified Network Associate Routing & Switching) está orientada a las habilidades prácticas en el diagnóstico y solución de problemas específicos de redes y, actualmente, es de las más importantes y respetadas por las empresas del mercado de las TI.

Además de demostrar las capacidades para configurar, operar y solucionar problemas de redes conmutadas y enrutadas, esta certificación ayuda a aquellos que la poseen a impulsar sus carreras profesionales, permitiéndoles optar a mejores puestos de trabajo especializados en la gestión de redes TI y, como consecuencia, obtener mayores salarios.

# 5   OBJETIVOS

## 5.1   GENERAL

Realizar las tareas asignadas en cada uno de los dos (2) escenarios propuestos

## 5.2   ESPECIFICOS

- Identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado.
- Lograr realizar un registro de la configuración de cada uno de los dispositivos
- Describir detalladamente el paso a paso de cada una de las etapas realizadas durante el desarrollo de esta actividad
- Presentar un informe el cual debe cumplir con las normas **ICONTEC 1486**

## 6   ESCENARIO 1

Una empresa posee sucursales distribuidas en las ciudades de Bogotá,  Medellín y Cali 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**

Los requerimientos solicitados son los siguientes:

Parte 1: Para el direccionamiento IP debe definirse una dirección de acuerdo con el número de hosts requeridos.

Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

Parte 3: La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.

Parte 4: Implementar la seguridad en la red, se debe restringir el acceso y comunicación entre hosts de acuerdo con los requerimientos del administrador de red.

Parte 5: Comprobación total de los dispositivos y su funcionamiento en la red.

Parte 6: Configuración final.
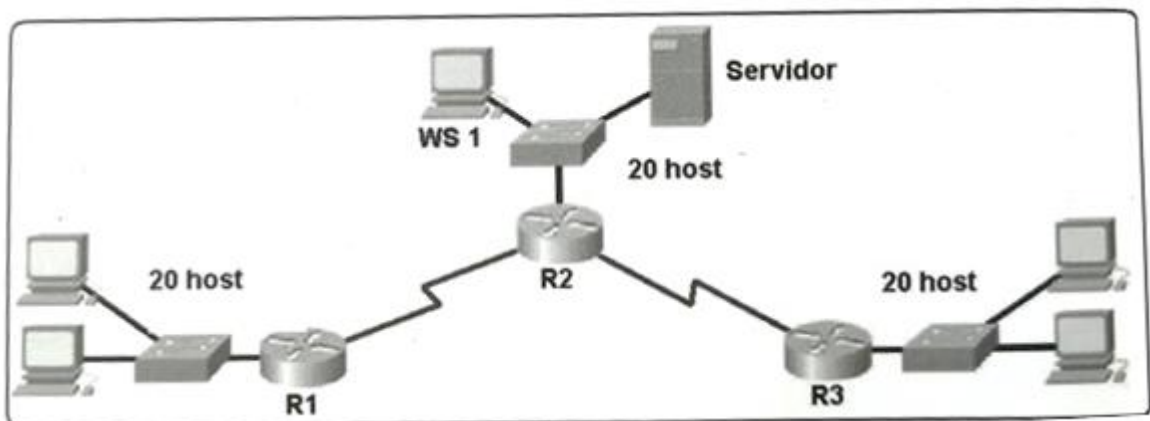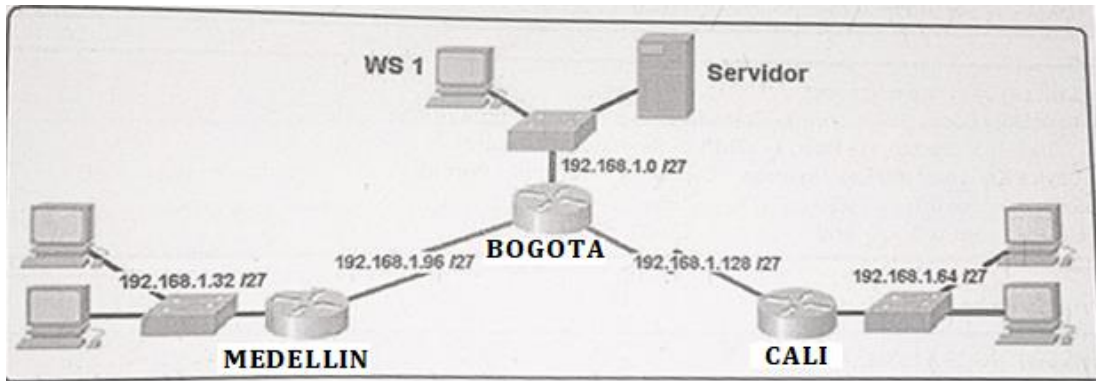
*Figura 1. Topología de red escenario 1*

**Desarrollo**
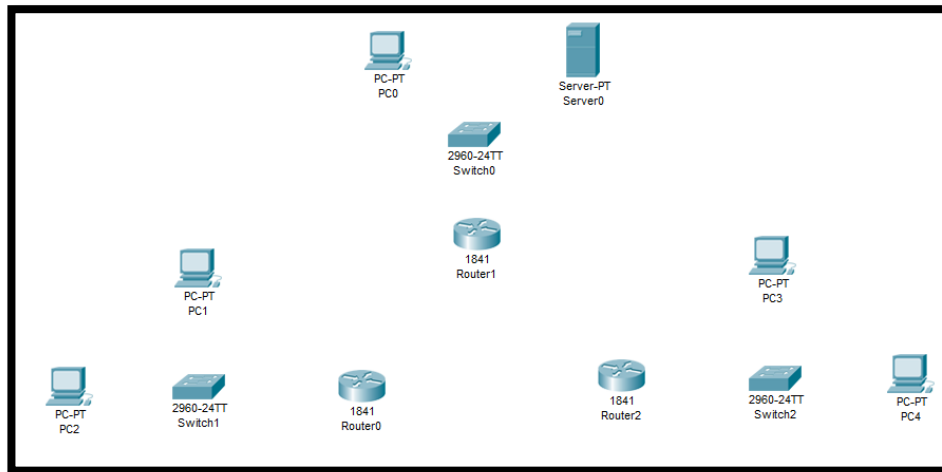


*Figura 2. Elementos a utilizar*

Para poder instalar el módulo WIC-1T que es el que nos permite la comunidad WAN entre routers, debemos apagarlo e insertar el modulo en los SLOT 0 y 1.
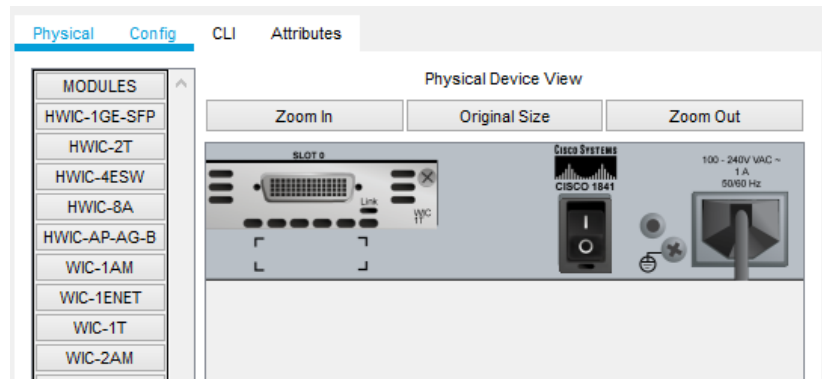


*Figura 3. Inserción módulo WIC-1T*

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

### ROUTER BOGOTA

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA
BOGOTA(config)#no ip domain-lookup
BOGOTA(config)#enable secret class
BOGOTA(config)#line console 0
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#line vty 0 4
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#service password-encryption
BOGOTA(config)#banner motd 'Los infractores se procesaran en la medida en que lo permita la ley'
BOGOTA(config)#exit
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console

### ROUTER MEDELLIN

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN
MEDELLIN(config)#no ip domain-lookup
MEDELLIN(config)#enable secret class
MEDELLIN(config)#line console 0
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#line vty 0 4
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
MEDELLIN(config)#service password-encryption
MEDELLIN(config)#banner motd 'Los infractores se procesaran en la medida en que lo permita la ley'
MEDELLIN(config)#exit
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console

**ROUTER CALI**

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CALI
CALI(config)#no ip domain-lookup
CALI(config)#enable secret class
CALI(config)#line console 0
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#line vty 0 4
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#exit
CALI(config)#service password-encryption
CALI(config)#banner motd 'Los infractores se procesaran en la medida en que lo permita la ley'
CALI(config)#exit
CALI#
%SYS-5-CONFIG_I: Configured from console by console

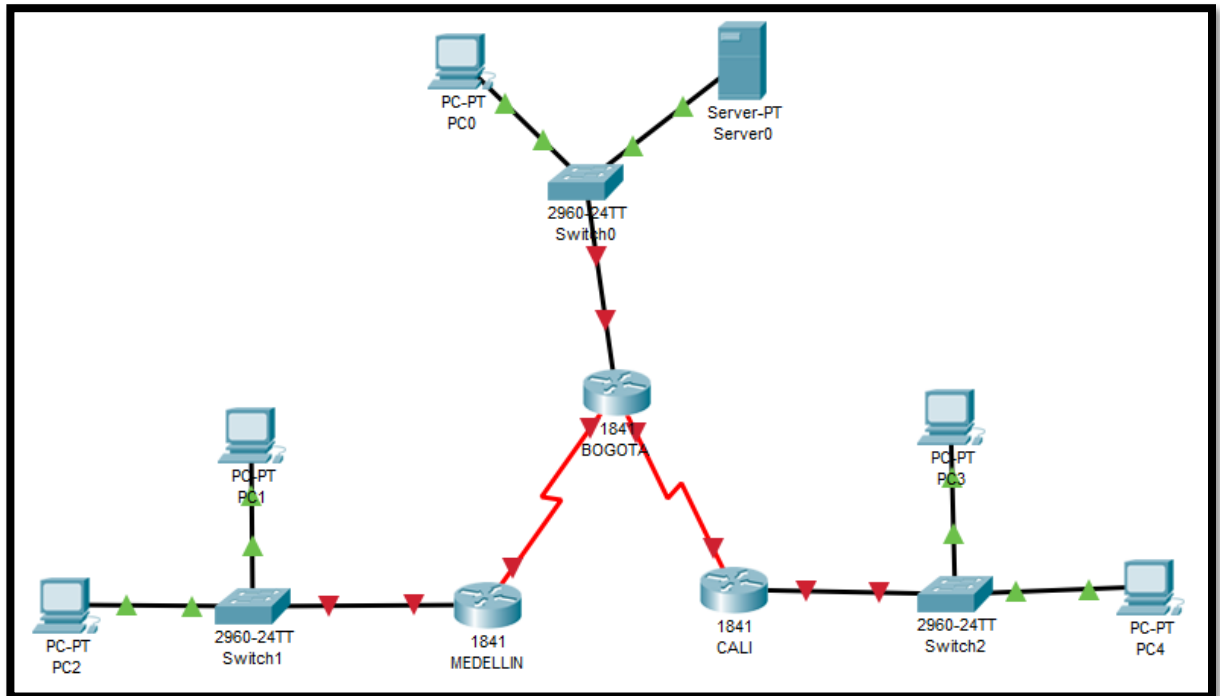- Realizar la conexión fisica de los equipos con base en la topología de red



*Figura 4. Conexión física*

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

### 6.1 Parte 1: Asignación de direcciones IP

a. Se debe dividir (subnetear) la red creando una segmentación en ocho partes, para permitir creciemiento futuro de la red corporativa.

| BOGOTA | | RESERVA | |
|---|---|---|---|
| IP Inicial | 192.168.1.1 | IP inicial | 192.168.1.97 |
| Mask | 27 | Mask | 27 |
| | 255.255.255.224 | | 255.255.255.224 |
| GW | 192.168.1.1 | GW | 192.168.1.97 |
| LAN | 192.168.1.2 al 192.168.1.30 | LAN | 192.168.1.98 al 192.168.1.126 |

| MEDELLIN | | RESERVA | |
|---|---|---|---|
| IP Inicial | 192.168.1.33 | IP inicial | 192.168.1.129 |
| Mask | 27 | Mask | 27 |
| | 255.255.255.224 | | 255.255.255.224 |
| GW | 192.168.1.33 | GW | 192.168.1.129 |
| LAN | 192.168.1.34 al 192.168.1.62 | LAN | 192.168.1.130 al 192.168.1.158 |

| CALI | | RESERVA | |
|---|---|---|---|
| IP Inicial | 192.168.1.65 | IP inicial | 192.168.1.161 |
| Mask | 27 | Mask | 27 |
| | 255.255.255.224 | | 255.255.255.224 |
| GW | 192.168.1.65 | GW | 192.168.1.161 |
| LAN | 192.168.1.66 - 192.168.1.94 | LAN | 192.168.1.162 - 192.168.1.190 |

b. Asignar una dirección IP a la red.

**IP asignada a la red: 192.168.1.100**

### 6.2 Parte 2: Configuración Básica.

a. Completar la siguiente tabla con la configuración básica de los routers, teniendo en cuenta las subredes diseñadas.

| | R1 | R2 | R3 |
|---|---|---|---|
| Nombre de Host | **MEDELLIN** | **BOGOTA** | **CALI** |
| Dirección de Ip en interfaz Serial 0/0 | 192.168.1.99 | 192.168.1.98 | 192.168.1.131 |
| Dirección de Ip en interfaz Serial 0/1 | | 192.168.1.130 | |
| Dirección de Ip en interfaz FA 0/0 | 192.168.1.33 | 192.168.1.1 | 192.168.1.65 |
| Protocolo de enrutamiento | **Eigrp** | **Eigrp** | **Eigrp** |
| Sistema Autónomo | 200 | 200 | 200 |
| Afirmaciones de red | 192.168.1.0 | 192.168.1.0 | 192.168.1.0 |

| | R1 | R2 | R3 |
|---|---|---|---|
| Nombre de Host | **MEDELLIN** | **BOGOTA** | **CALI** |
| Dirección de Ip en interfaz Serial 0/0 | 192.168.1.99 | 192.168.1.98 | 192.168.1.131 |
| Dirección de Ip en interfaz Serial 0/1 | 192.168.1.97 | 192.168.1.130 | 192.168.1.129 |
| Dirección de Ip en interfaz FA 0/0 | 192.168.1.33 | 192.168.1.1 | 192.168.1.65 |
| Protocolo de enrutamiento | **Eigrp** | **Eigrp** | **Eigrp** |
| Sistema Autónomo | 200 | 200 | 200 |
| Afirmaciones de red | 192.168.1.0 | 192.168.1.0 | 192.168.1.0 |

**MEDELLIN**



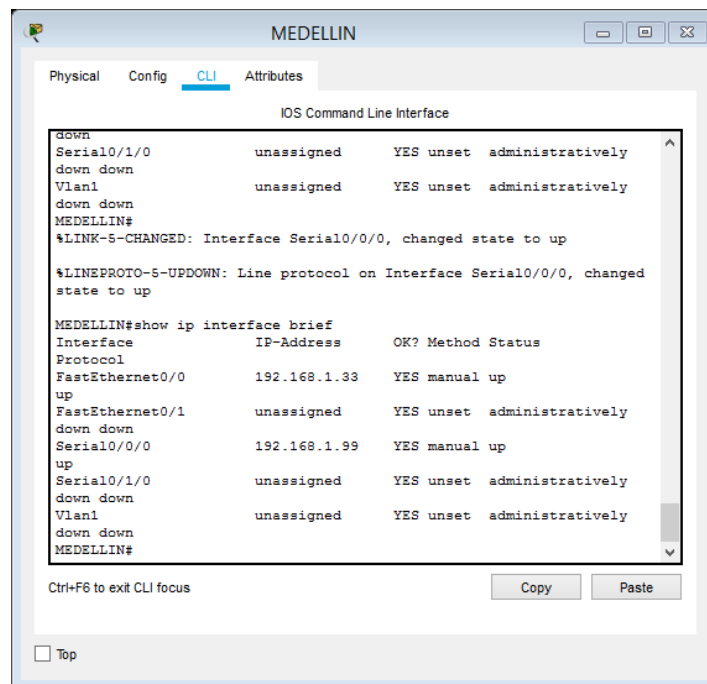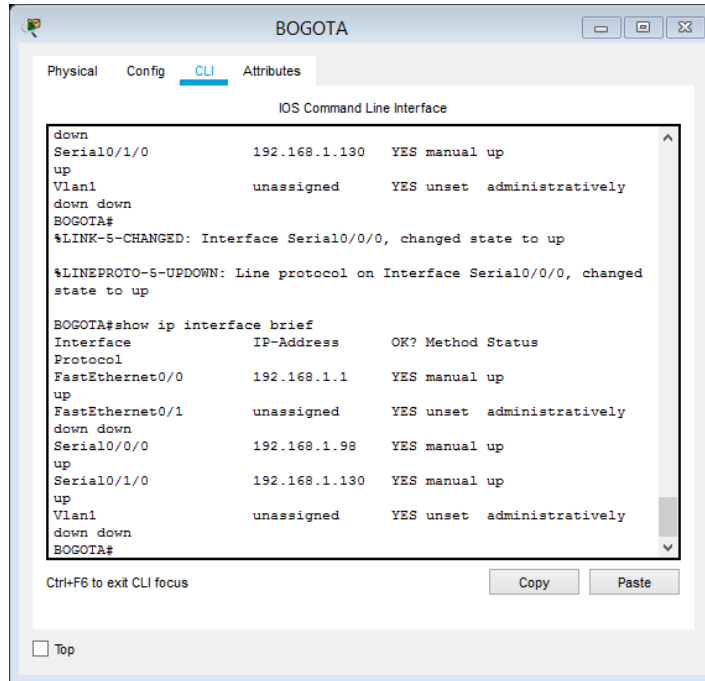*Figura 5. Configuración básica Router Medellín*

14

**BOGOTA**



*Figura 6. Configuración básica Router Bogotá*

**CALI**
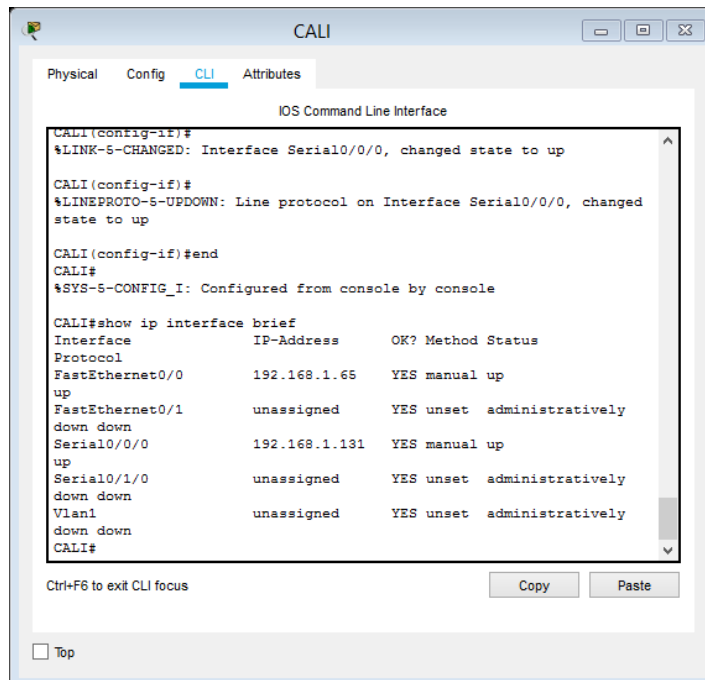


*Figura 7. Configuración básica Router Cali*

b. Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.
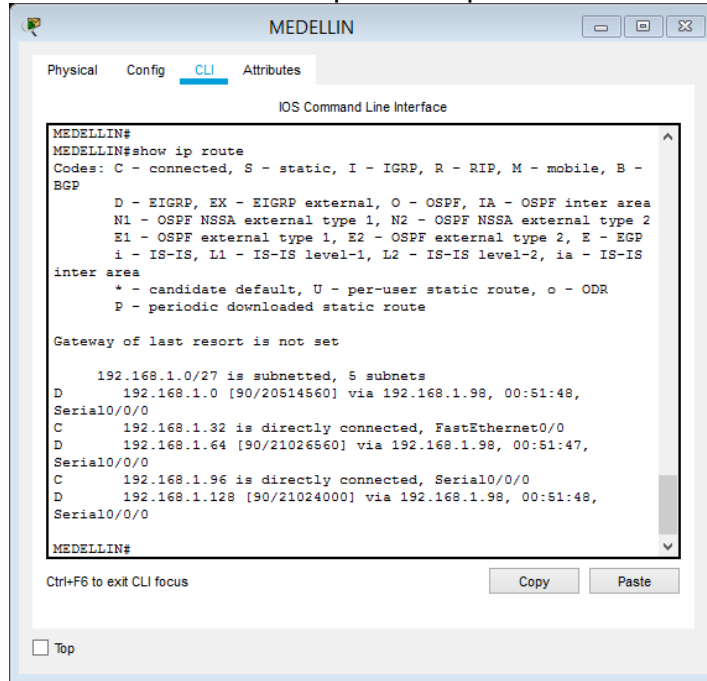


*Figura 8. Enrutamiento Router Medellín*
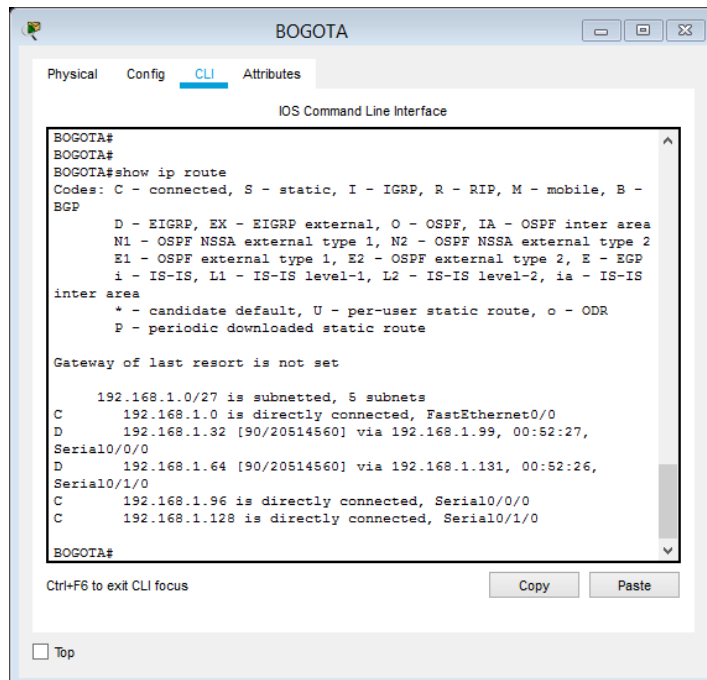


*Figura 9. Enrutamiento Router Bogotá*
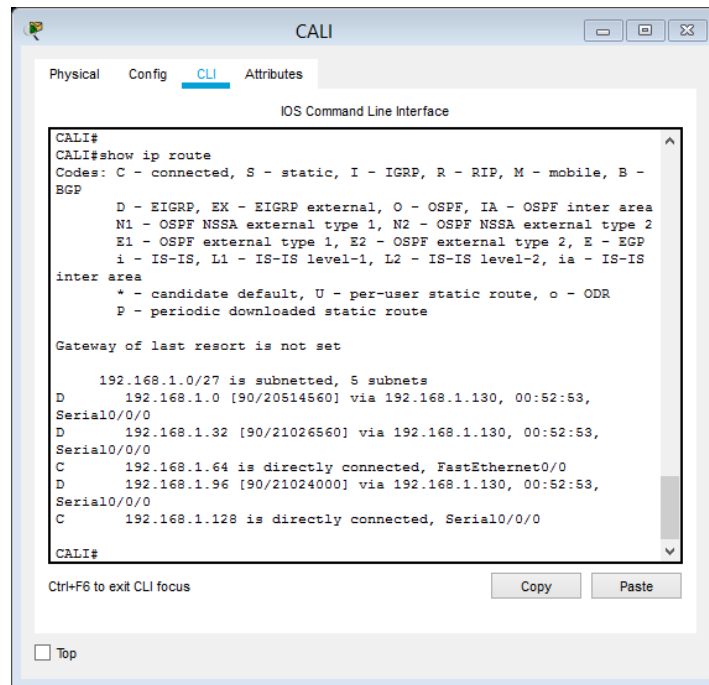
**Figura 10. Enrutamiento Router Cali**

c. Verificar el balanceo de carga que presentan los routers.

   Para esto hacemos uso del comando **show ip eigrp topology**

   BOGOTA#show ip eigrp topology
   IP-EIGRP Topology Table for AS 200/ID(192.168.1.130)

   Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
   r - Reply status

   P 192.168.1.0/27, 1 successors, FD is 28160
   via Connected, FastEthernet0/0
   P 192.168.1.32/27, 1 successors, FD is 20514560
   via 192.168.1.99 (20514560/28160), Serial0/0/0
   P 192.168.1.64/27, 1 successors, FD is 20514560
   via 192.168.1.131 (20514560/28160), Serial0/1/0
   P 192.168.1.96/27, 1 successors, FD is 20512000
   via Connected, Serial0/0/0
   P 192.168.1.128/27, 1 successors, FD is 20512000
   via Connected, Serial0/1/0
   BOGOTA#
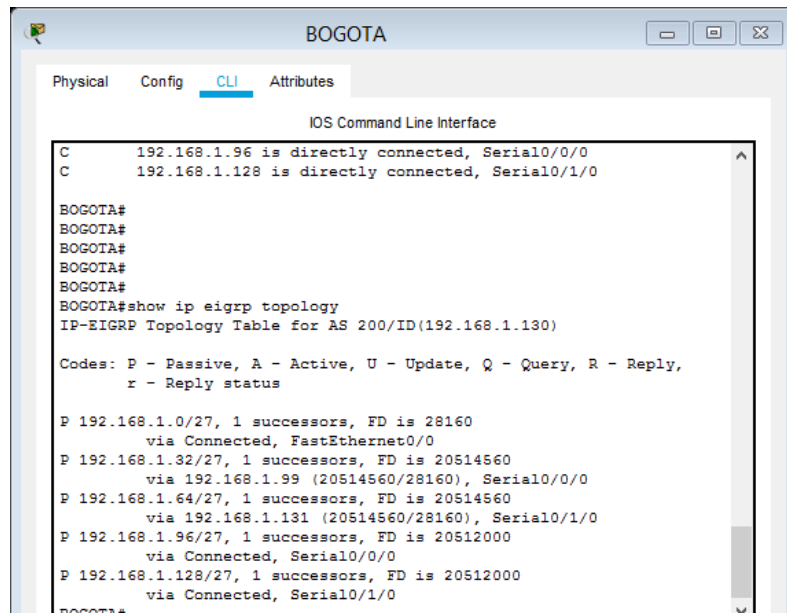
*Figura 11. Balanceo de carga*

d. Realizar un diagnóstico de vecinos uando el comando cdp.

BOGOTA#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

| Device ID | Local Intrfce | Holdtme | Capability | Platform | Port ID |
|-----------|---------------|---------|------------|----------|---------|
| Switch | Fas 0/0 | 134 | S | 2960 | Gig 0/1 |
| MEDELLIN | Ser 0/0/0 | 134 | R | C1841 | Ser 0/0/0 |
| CALI | Ser 0/1/0 | 142 | R | C1841 | Ser 0/0/0 |
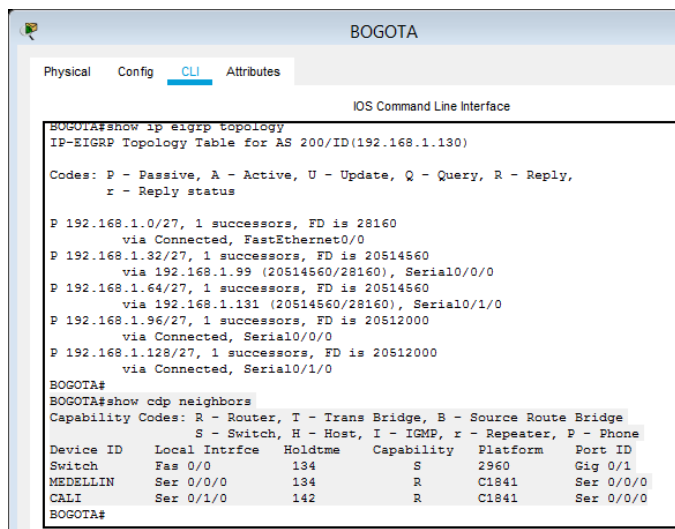


*Figura 12. Dianóstico de vecinos*

e. Realizar una prueba de conectividad en cada tramo de la ruta usando Ping.
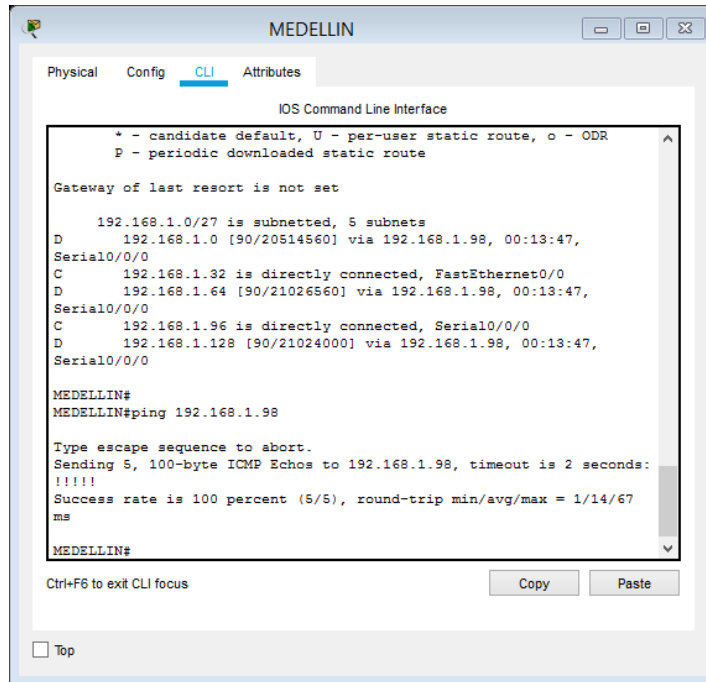


*Figura 13. Ping Router MEDELLIN A Router BOGOTA*
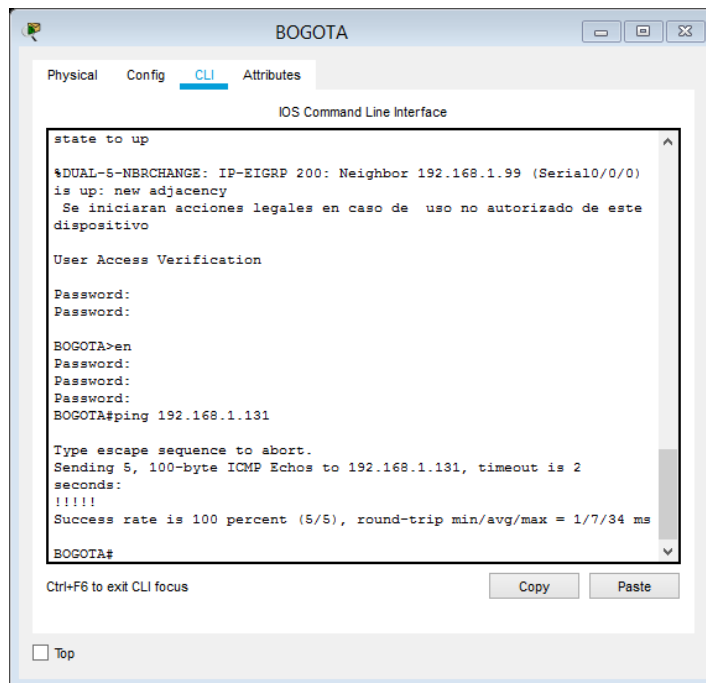


*Figura 14. Ping Router BOGOTA a Router CALI*
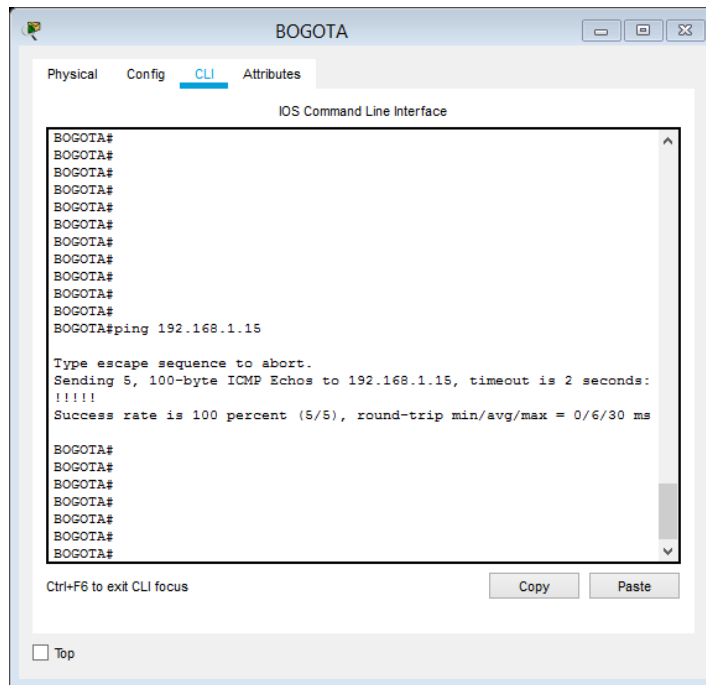
*Figura 15. Ping Router BOGOTA a PC-0*
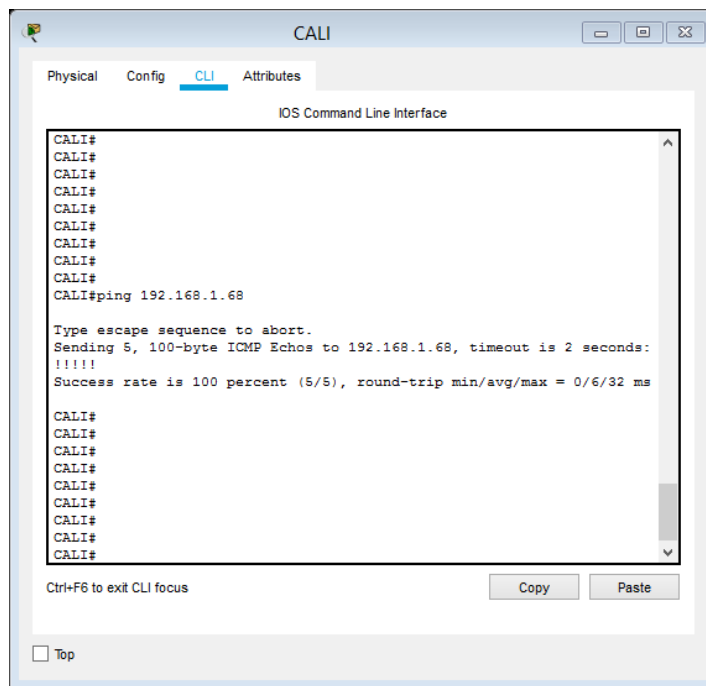


*Figura 16. Ping Router CALI a PC-3*
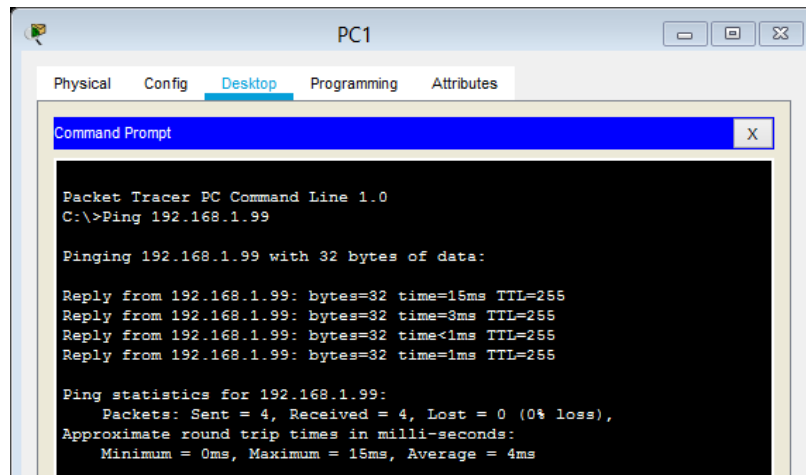
*Figura 17. Ping PC-1 Router MEDELLIN*

### 6.3 Parte 3: Configuración de Enrutamiento.

a. Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.

BOGOTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#router eigrp 200
BOGOTA(config-router)#network 192.168.1.0
BOGOTA(config-router)#do wr
Building configuration...
[OK]

MEDELLIN#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#router eigrp 200
MEDELLIN(config-router)#network 192.168.1.0
MEDELLIN(config-router)#do wr
Building configuration...
[OK]

CALI#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#router eigrp 200
CALI(config-router)#network 192.168.1.0
CALI(config-router)#do wr
Building configuration...
[OK]

b. Verificar si existe vecindad con los routers configurados con EIGRP.



```
MEDELLIN#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address         Interface       Hold Uptime    SRTT   RTO    Q    Seq
                                    (sec)          (ms)        Cnt  Num
0   192.168.1.98    Se0/0/0         12   00:29:44  40     1000   0    8
```

```
BOGOTA#
BOGOTA#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address         Interface       Hold Uptime    SRTT   RTO    Q    Seq
                                    (sec)          (ms)        Cnt  Num
0   192.168.1.131   Se0/1/0         10   00:28:33  40     1000   0    7
1   192.168.1.99    Se0/0/0         12   00:28:29  40     1000   0    7

BOGOTA#
```

```
CALI#
CALI#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address         Interface       Hold Uptime    SRTT   RTO    Q    Seq
                                    (sec)          (ms)        Cnt  Num
0   192.168.1.130   Se0/0/0         11   00:30:28  40     1000   0    7

CALI#
```

*Figura 18. Verificación de vecindad de Routers*

c. Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas.
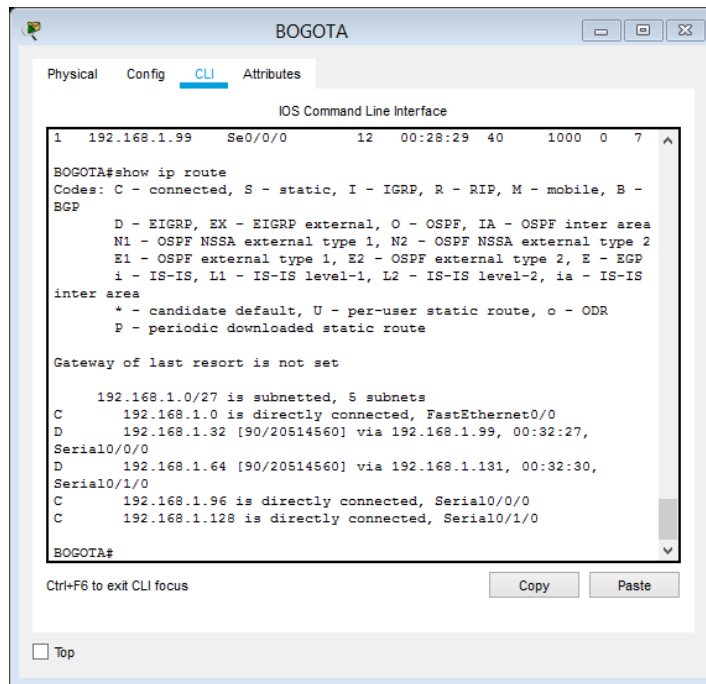


*Figura 19. Comprobacion enrutamiento Router Bogotá*
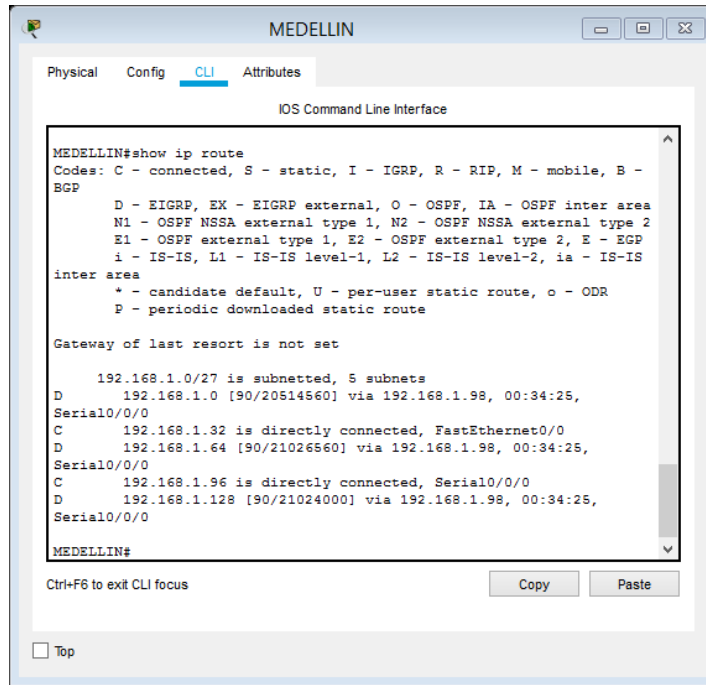
**Figura 20. Comprobacion enrutamiento Router Medellín**
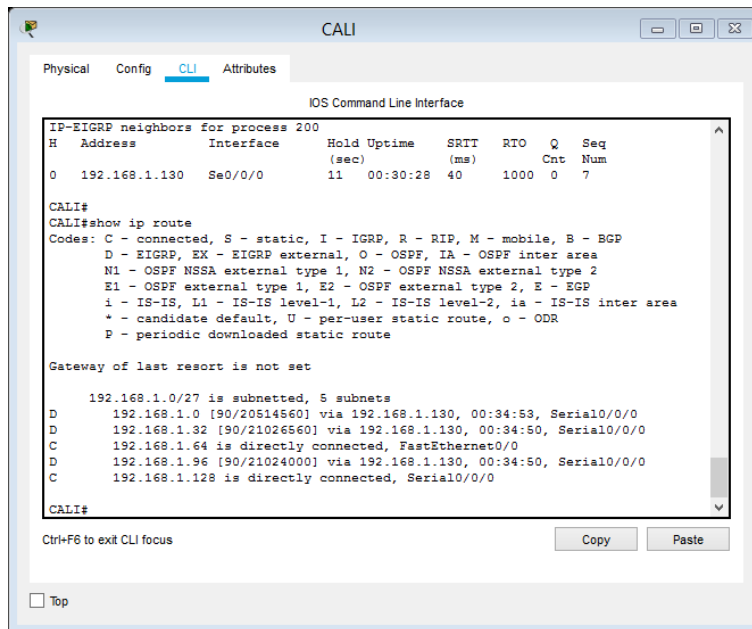


**Figura 21. Comprobacion enrutamiento Router Cali**

d. Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí. Realizar esta prueba desde un host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor.
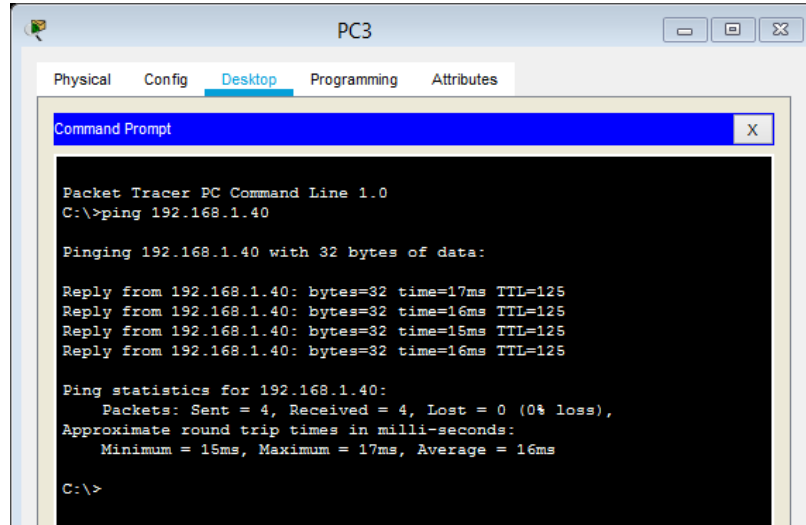


*Figura 22. Ping PC-3 CALI a PC-1 MEDELLIN*
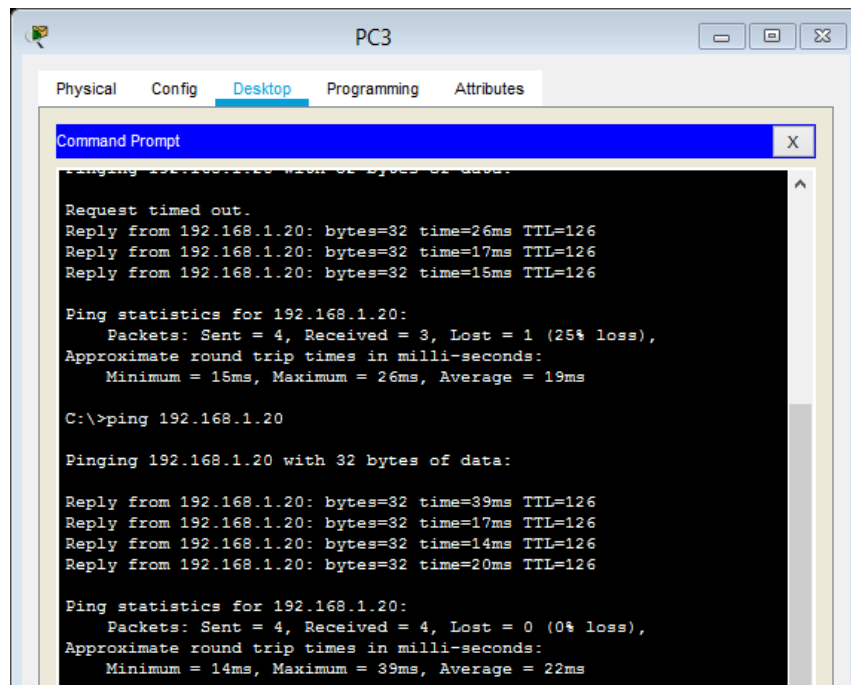


*Figura 23. Ping PC-3 CALI a Server-0*
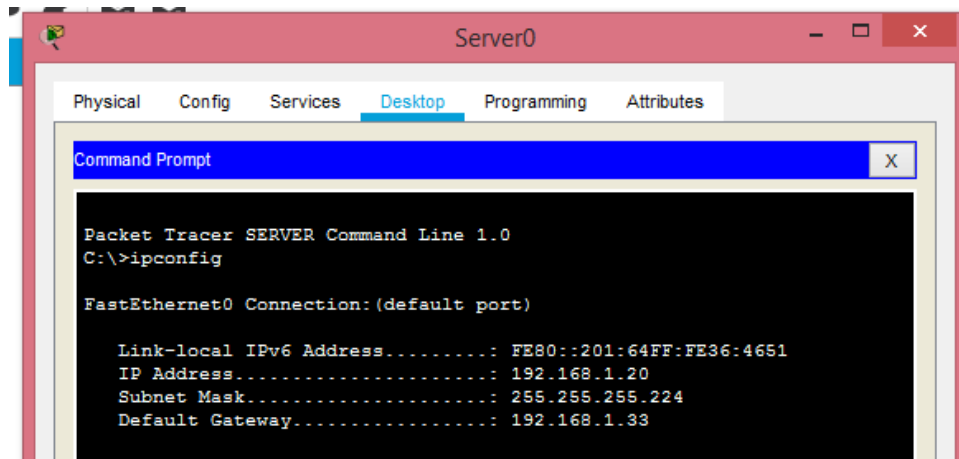
*Figura 24. IP asignada Server 0*

## 6.4 Parte 4: Configuración de las listas de Control de Acceso.

En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo. El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers. Las condiciones para crear las ACL son las siguientes:

- Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red.
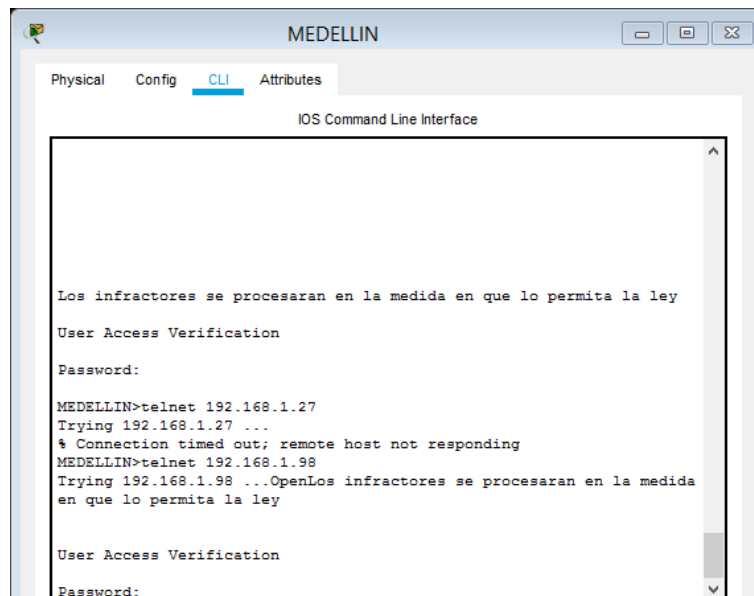


*Figura 25. Telnet router MEDELLIN a router BOGOTA*

25
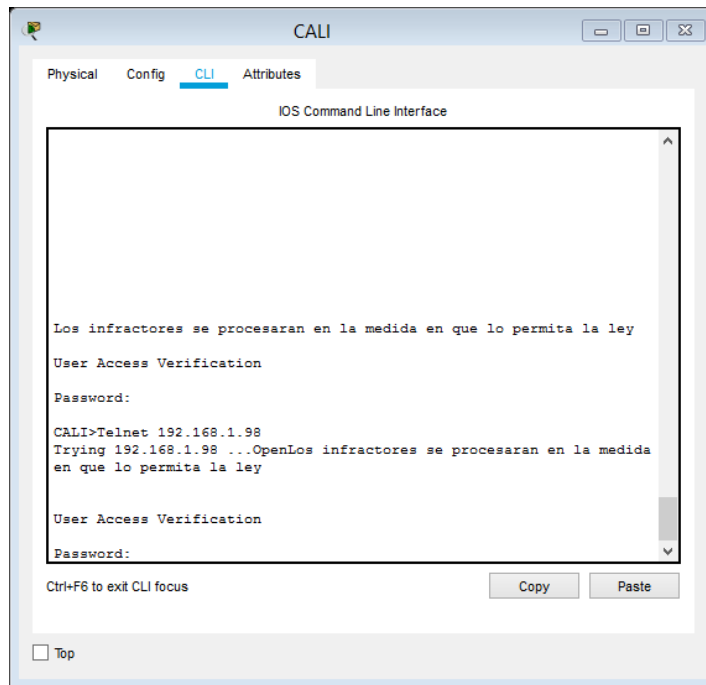
*Figura 26. Telnet router CALI a router BOGOTA*

- El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.
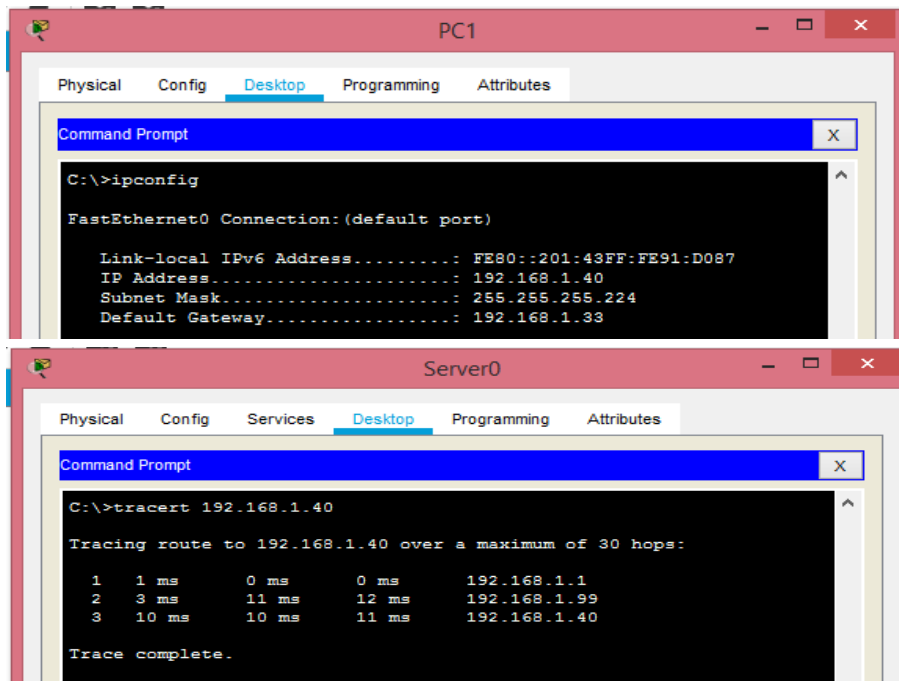


*Figura 27. Tracert de Server-0 a PC-1 MEDELLIN*
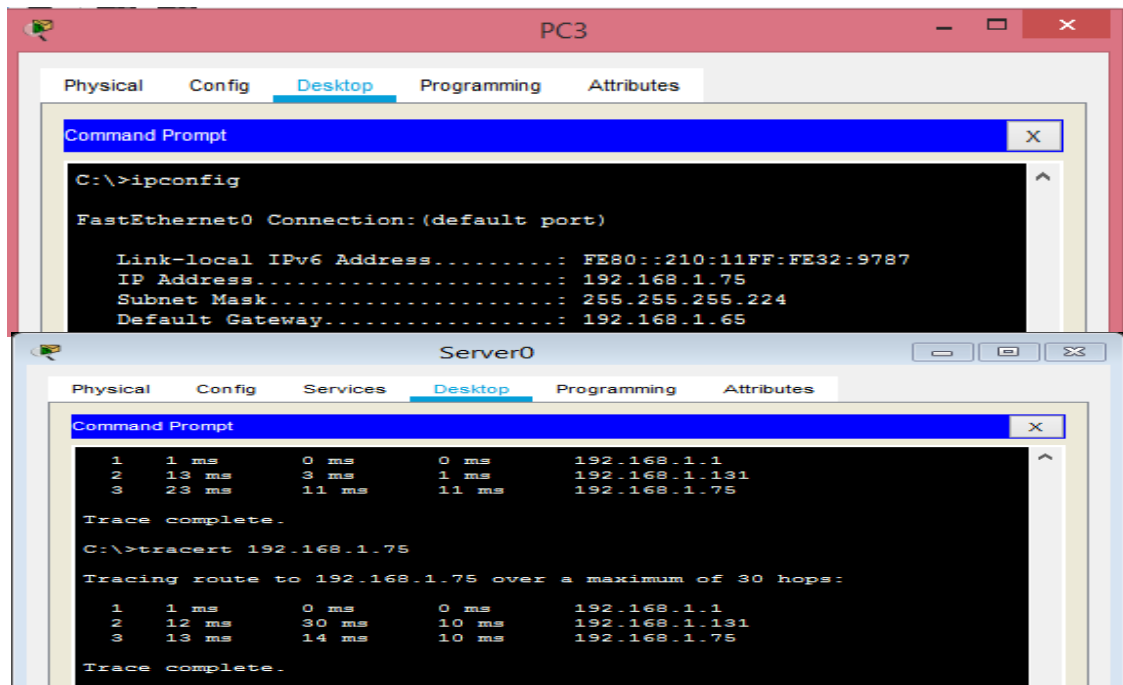
*Figura 28. Tracert de Server-0 a PC-3 CALI*

- Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor.

Compruebo el acceso de PC-1 MEDELLIN a PC-0 y Server-0 y se puede ver que está conectado, ahora procedo a hacer configuración de las listas de acceso en el router BOGOTA.
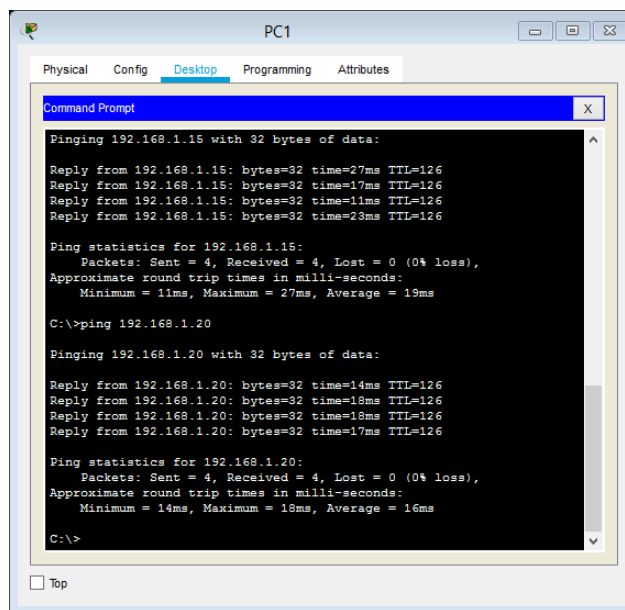


*Figura 29. Ping PC-1 MEDELLIN a PC-0 y Server-0*

Ahora ingresamos las listas de acceso
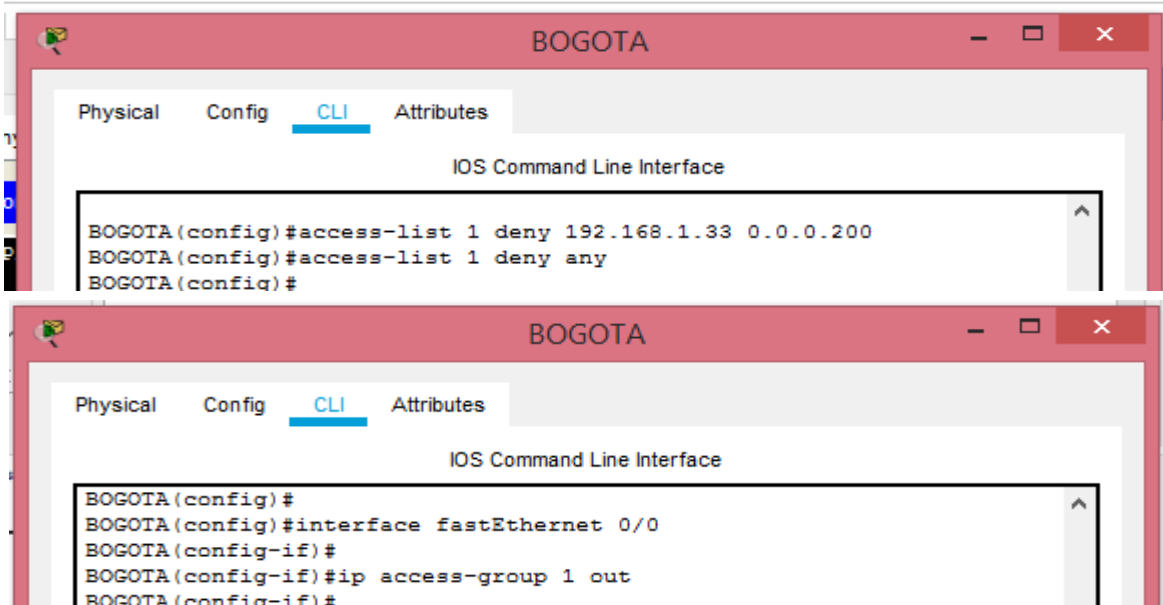


*Figura 30. Lista de acceso Router Bogotá*

## 6.5 Parte 5: Comprobación de la red instalada.

a. Se debe probar que la configuración de las listas de acceso fue exitosa.
Al hacer ping de nuevo debe denegar la conexión.
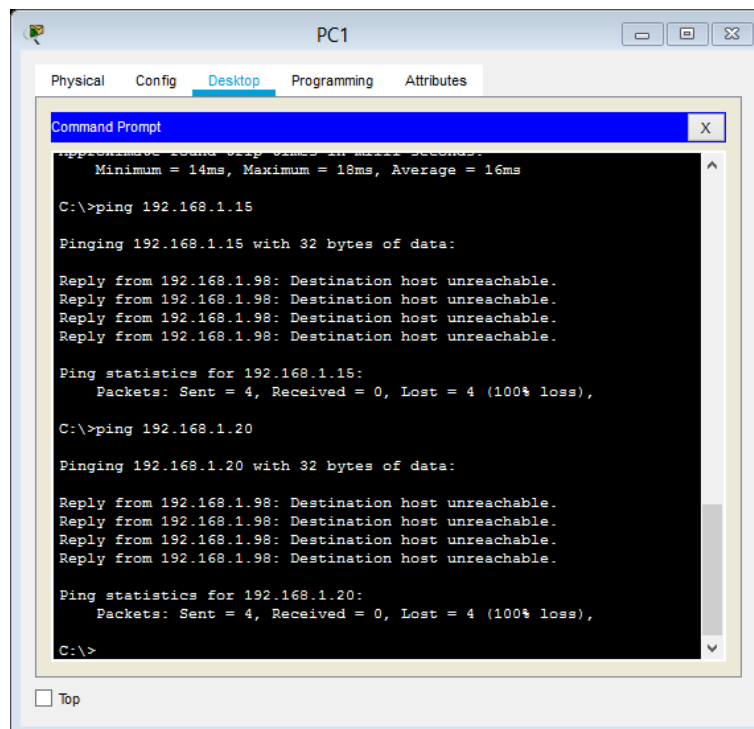


*Figura 31. Comprobación listas de acceso*

b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.

| | ORIGEN | DESTINO | RESULTADO |
|---|---|---|---|
| TELNET | Router MEDELLIN | Router CALI | |
| | WS_1 | Router BOGOTA | |
| | Servidor | Router CALI | |
| | Servidor | Router MEDELLIN | |
| TELNET | LAN del Router MEDELLIN | Router CALI | |
| | LAN del Router CALI | Router CALI | |
| | LAN del Router MEDELLIN | Router MEDELLIN | |
| | LAN del Router CALI | Router MEDELLIN | |
| PING | LAN del Router CALI | WS_1 | |
| | LAN del Router MEDELLIN | WS_1 | |
| | LAN del Router MEDELLIN | LAN del Router CALI | |
| PING | LAN del Router CALI | Servidor | |
| | LAN del Router MEDELLIN | Servidor | |
| | Servidor | LAN del Router MEDELLIN | |
| | Servidor | LAN del Router CALI | |
| | Router CALI | LAN del Router MEDELLIN | |
| | Router MEDELLIN | LAN del Router CALI | |

| | ORIGEN | DESTINO | RESULTADO |
|---|---|---|---|
| TELNET | Router MEDELLIN | Router CALI | ABIERTO |
| | WS_1 | Router BOGOTA | ABIERTO |
| | Servidor | Router CALI | ABIERTO |
| | Servidor | Router MEDELLIN | ABIERTO |
| TELNET | LAN del Router MEDELLIN | Router CALI | CERRADO |
| | LAN del Router CALI | Router CALI | ABIERTO |
| | LAN del Router MEDELLIN | Router MEDELLIN | ABIERTO |
| | LAN del Router CALI | Router MEDELLIN | CERRADO |
| PING | LAN del Router CALI | WS_1 | HOST INALCANZABLE |
| | LAN del Router MEDELLIN | WS_1 | HOST INALCANZABLE |
| | LAN del Router MEDELLIN | LAN del Router CALI | HOST INALCANZABLE |
| PING | LAN del Router CALI | Servidor | HOST INALCANZABLE |
| | LAN del Router MEDELLIN | Servidor | HOST INALCANZABLE |
| | Servidor | LAN del Router MEDELLIN | 100% 5/5 |
| | Servidor | LAN del Router CALI | 100% 5/5 |
| | Router CALI | LAN del Router MEDELLIN | 100% 5/5 |
| | Router MEDELLIN | LAN del Router CALI | 100% 5/5 |

# 7    ESCENARIO 2

Una empresa tiene la conexión a internet en una red Ethernet, lo cual deben adaptarlo para facilitar que sus routers y las redes que incluyen puedan, por esa vía, conectarse a internet, pero empleando las direcciones de la red LAN original.
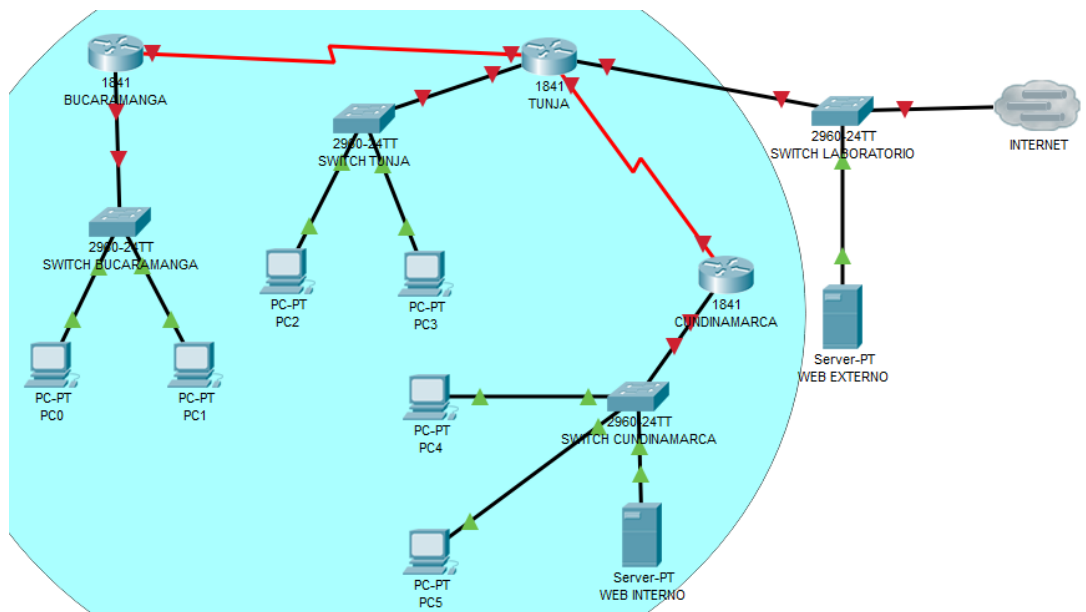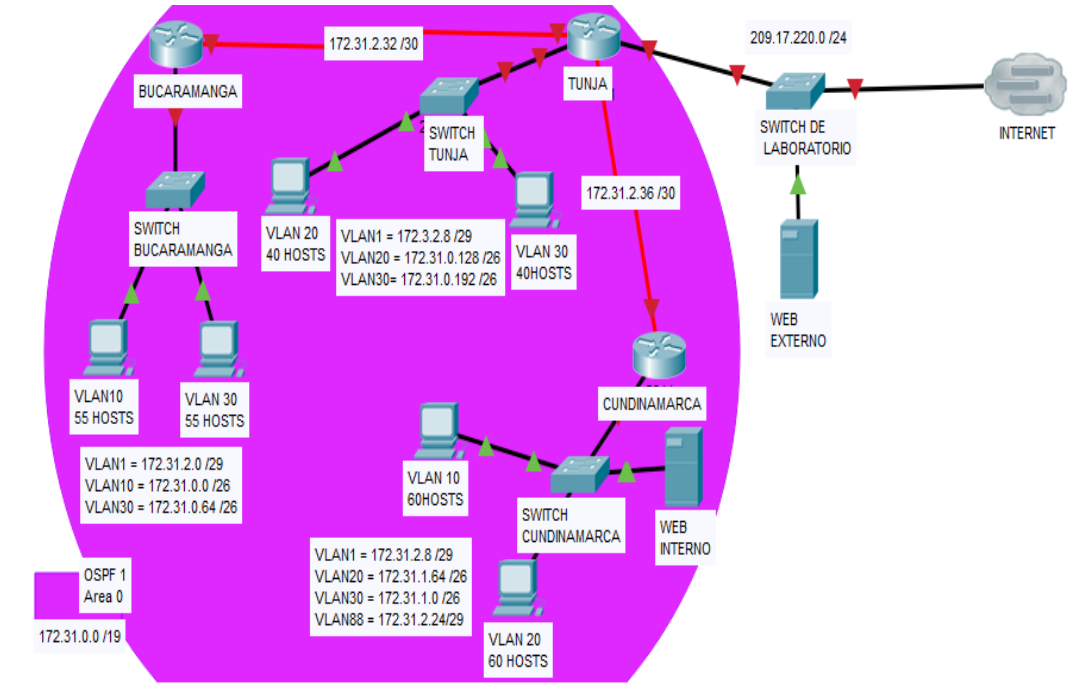


*Figura 32. Topología de red escenario 2*

### 7.1 Desarrollo

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:

#### 7.1.1 Configuración básica.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BUCARAMANGA
BUCARAMANGA(config)#no ip domain-lookup
BUCARAMANGA(config)#enable secret class
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#password cisco
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#line vty 0 4
BUCARAMANGA(config-line)#password cisco
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#banner motd 'Los infractores se procesaran en la medida en
que lo permita la ley'
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#interface s
BUCARAMANGA(config)#interface serial 0/1/0
BUCARAMANGA(config-if)#ip ad
BUCARAMANGA(config-if)#ip address 172.31.2.33 255.255.255.252
BUCARAMANGA(config-if)#no shutdown
BUCARAMANGA(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
BUCARAMANGA(config-if)#do wr
Building configuration...
[OK]
BUCARAMANGA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
BUCARAMANGA(config)#interface FaSTEthernet 0/0
BUCARAMANGA(config-if)#ip address 172.31.0.10 255.255.255.192
BUCARAMANGA(config-if)#no shutdown
BUCARAMANGA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname TUNJA
TUNJA(config)#no ip domain-lookup
TUNJA(config)#enable secret class
TUNJA(config)#line console 0
TUNJA(config-line)#password cisco
TUNJA(config-line)#login
TUNJA(config-line)#line vty 0 4
TUNJA(config-line)#password cisco
TUNJA(config-line)#login
TUNJA(config-line)#exit
TUNJA(config)#banner motd 'Los infractores se procesarán en la medida en que lo permita la ley'
TUNJA(config)#exit
TUNJA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#interface fastEthernet 0/0
TUNJA(config-if)#ip address 209.17.220.5 255.255.255.0
TUNJA(config-if)#no shutdown
TUNJA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
TUNJA(config)#interface serial0/0/0
TUNJA(config-if)#ip address 172.31.2.34 255.255.255.252
TUNJA(config-if)#no shutdown
%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
TUNJA(config)#interface serial 0/1/0
TUNJA(config-if)#ip address 172.31.2.37 255.255.255.252
TUNJA(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
TUNJA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#interface fastEthernet 0/0
TUNJA(config-if)#ip address 209.17.220.5 255.255.255.0
TUNJA(config-if)#no shutdown
TUNJA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
TUNJA(config-if)#exit
TUNJA(config)#interface fastEthernet 0/1
TUNJA(config-if)#ip address 172.31.0.130 255.255.255.192
TUNJA(config-if)#no shutdown
TUNJA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CUNDINAMARCA
CUNDINAMARCA(config)#no ip domain-lookup
CUNDINAMARCA(config)#enable secret class
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#password cisco
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#line vty 0 4
CUNDINAMARCA(config-line)#password cisco
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#exit
CUNDINAMARCA(config)#banner motd 'Los infractores se procesaran en la medida en que lo permita la ley'
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
CUNDINAMARCA#configure t
CUNDINAMARCA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#interface fas
CUNDINAMARCA(config)#interface fastEthernet 0/0
CUNDINAMARCA(config-if)#ip address 172.31.0.5 255.255.255.192
CUNDINAMARCA(config-if)#no shut
CUNDINAMARCA(config-if)#no shutdown
CUNDINAMARCA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

### 7.1.2 Autenticación local con AAA.

BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#username Admin1 secret ozkr636
BUCARAMANGA(config)#aaa authentication login default group tacacs+ local
BUCARAMANGA(config)#tacacs-server host 192.168.2.2
BUCARAMANGA(config)#tacacs-server key tacacspa55
BUCARAMANGA(config)#exit

TUNJA(config)#aaa new-model
TUNJA(config)#username Admin1 secret ozkr636
TUNJA(config)#aaa authentication login default group tacacs+ local
TUNJA(config)#tacacs-server host 192.168.2.2
TUNJA(config)#tacacs-server key tacacspa55
TUNJA(config)#exit

CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#username Admin1 secret ozkr636
CUNDINAMARCA(config)#aaa authentication login default group tacacs+ local
CUNDINAMARCA(config)#tacacs-server host 192.168.2.2
CUNDINAMARCA(config)#tacacs-server key tacacspa55
CUNDINAMARCA(config)#exit
Dd

### 7.1.3 Cifrado de contraseñas.

BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#service password-encryption
BUCARAMANGA(config)#end
BUCARAMANGA#show running-config
%SYS-5-CONFIG_I: Configured from console by console



*Figura 33.  Cifrado contraseñas Router Bucaramanga*

TUNJA#conf t

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

TUNJA(config)#service password-encryption

TUNJA(config)#end

TUNJA#show running-config

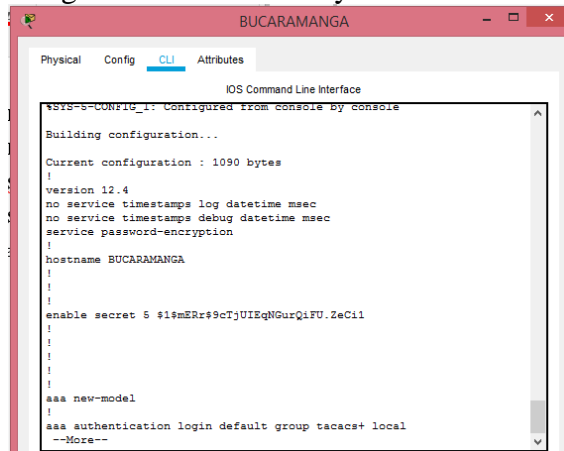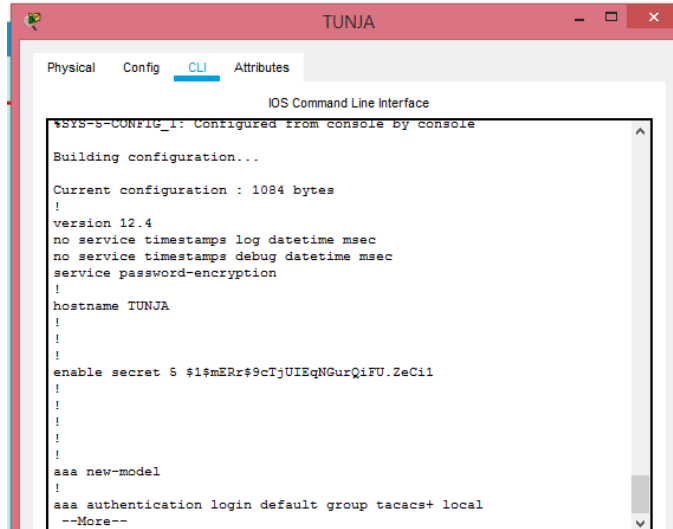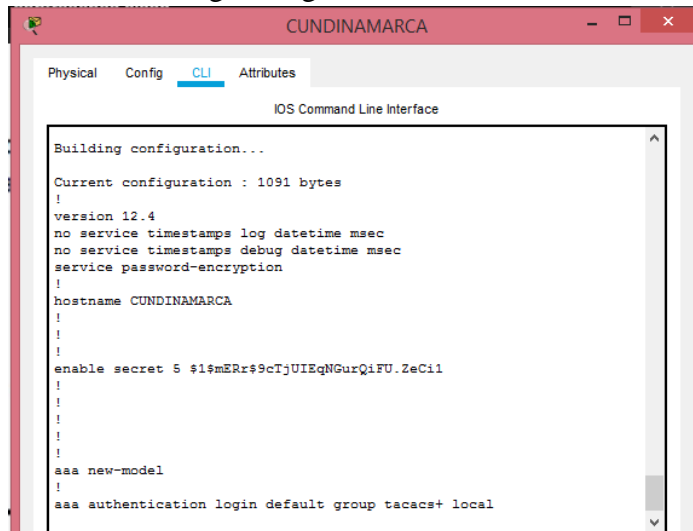%SYS-5-CONFIG_I: Configured from console by console



*Figura 34. Cifrado contraseñas Router Tunja*

CUNDINAMARCA#conf t

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

CUNDINAMARCA(config)#service password-encryption

CUNDINAMARCA(config)#end

CUNDINAMARCA#show running-config



*Figura 35. Cifrado contraseñas Router Cundinamarca*

2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y
   Cundinamarca

BUCARAMANGA>en
Password:
Password:
BUCARAMANGA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
BUCARAMANGA(config)#ip dhcp pool red_buc
BUCARAMANGA(dhcp-config)#net
BUCARAMANGA(dhcp-config)#network 172.31.0.0 255.255.255.192
BUCARAMANGA(dhcp-config)#defa
BUCARAMANGA(dhcp-config)#default-router 172.31.0.1
BUCARAMANGA(dhcp-config)#
BUCARAMANGA(dhcp-config)#dn
BUCARAMANGA(dhcp-config)#dns-server 8.8.8.8
BUCARAMANGA(dhcp-config)#
BUCARAMANGA(dhcp-config)#exit
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console

BUCARAMANGA#sh
BUCARAMANGA#show ip dhcp pool

Pool redBuc :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 16382
 Leased addresses               : 0
 Excluded addresses             : 0
 Pending event                  : none
 1 subnet is currently in the pool
 Current index      IP address range               Leased/Excluded/Total
 172.31.0.1         172.31.0.1    - 172.31.63.254    0   / 0   / 16382
Pool red_buc :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 62
 Leased addresses               : 1
 Excluded addresses             : 0

Pending event              : none
1 subnet is currently in the pool
Current index       IP address range                  Leased/Excluded/Total
172.31.0.1          172.31.0.1      - 172.31.0.62       1    / 0     / 62
BUCARAMANGA#
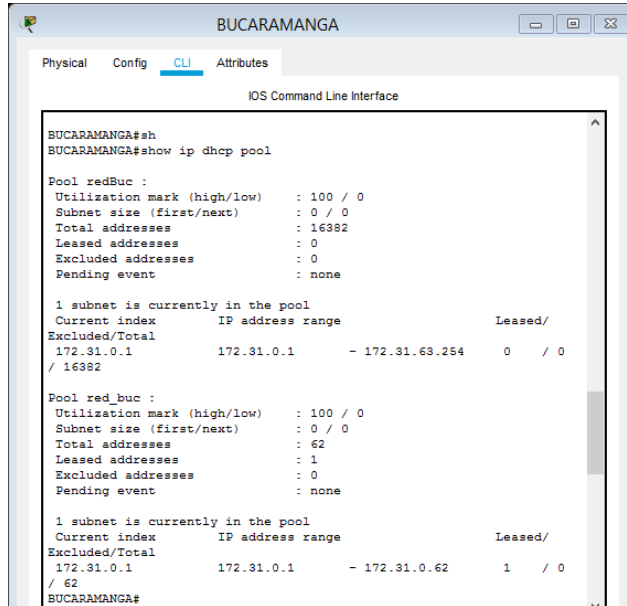


*Figura 36. DHCP Router Bucaramanga*
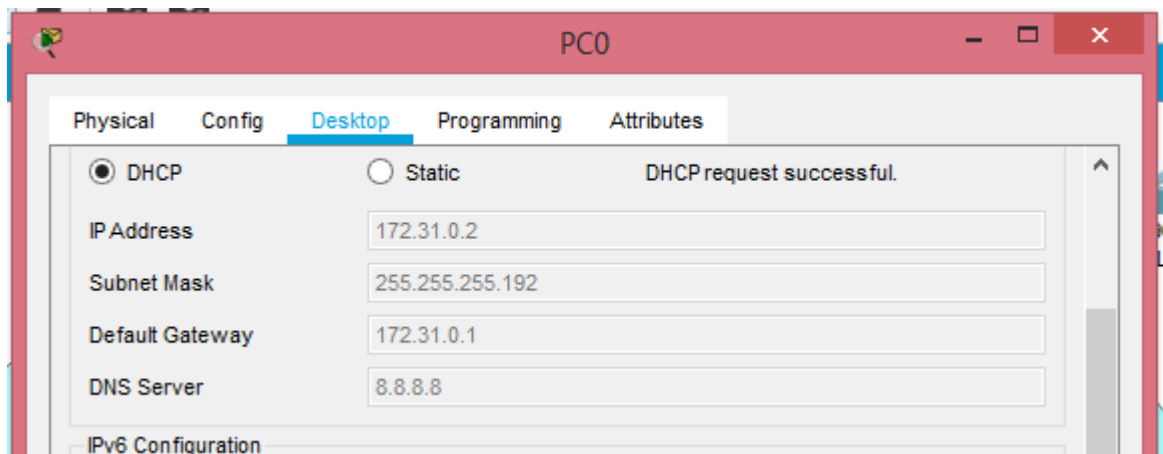


*Figura 37. Solicitud DHCP exitosa en PC-0*

CUNDINAMARCA>en
Password:
Password:
CUNDINAMARCA#conf t

Enter configuration commands, one per line.  End with CNTL/Z.
CUNDINAMARCA(config)#ip dhcp pool red_cun
CUNDINAMARCA(dhcp-config)#net
CUNDINAMARCA(dhcp-config)#network 172.31.0.0 255.255.255.192
CUNDINAMARCA(dhcp-config)#de
CUNDINAMARCA(dhcp-config)#default-router 172.31.0.1
CUNDINAMARCA(dhcp-config)#dns
CUNDINAMARCA(dhcp-config)#dns-server 8.8.8.8
CUNDINAMARCA(dhcp-config)#exit
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
CUNDINAMARCA#show
% Incomplete command.
CUNDINAMARCA#show ip dhcp pool
Pool red_cun :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 62
 Leased addresses               : 0
 Excluded addresses             : 0
 Pending event                  : none
1 subnet is currently in the pool
Current index       IP address range              Leased/Excluded/Total
172.31.0.1          172.31.0.1       - 172.31.0.62       0    / 0     / 62
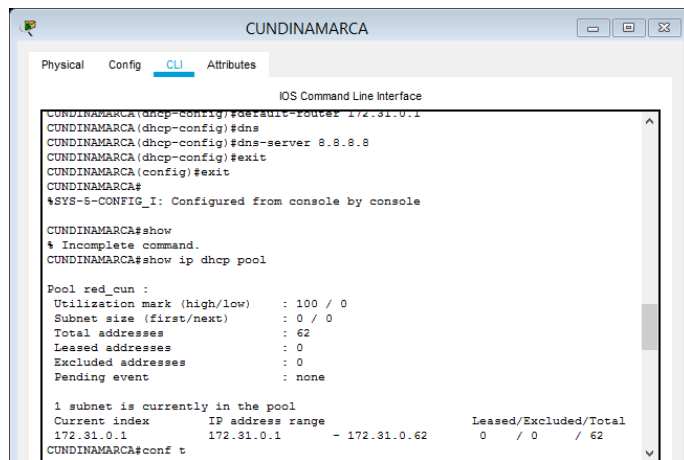


*Figura 38. DHCP Router Cundinamarca*
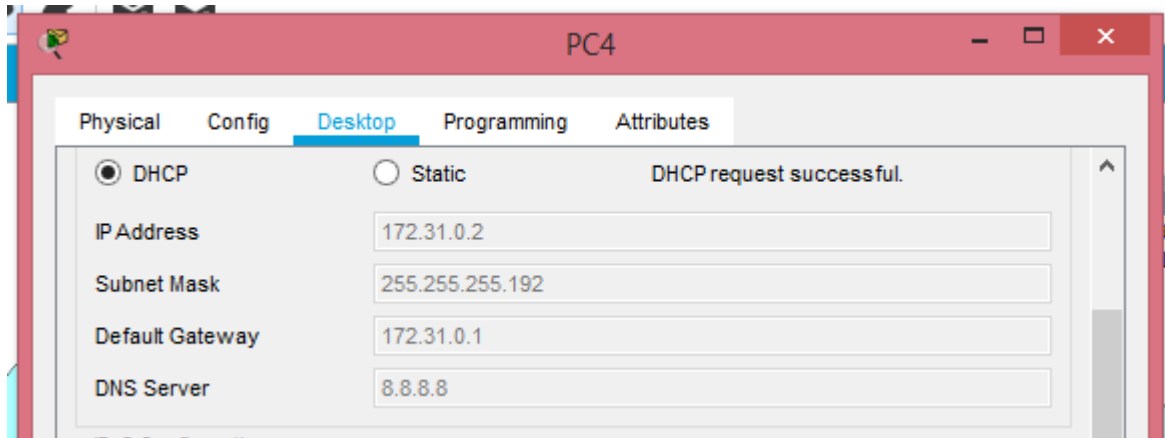
*Figura 39. Solicitud DHCP exitosa PC-4*

3. El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).

Username: Admin1
Password:
TUNJA>en
Password:
Password:
TUNJA#en
TUNJA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
TUNJA(config)#access-list 1 permit 172.31.0.0 255.255.192.0
TUNJA(config)#ip nat inside source list 1 interface serial 0/0/0 overload
TUNJA(config)#interface fastEthernet 0/0
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#interface serial 0/0/0
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#exit

Username: Admin1
Password:
CUNDINAMARCA>en
Password:
Password:
CUNDINAMARCA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#access-list 1 permit 172.31.1.0 0.0.0.192
CUNDINAMARCA(config)#ip nat inside source list 1 interface fa 0/0 overload

CUNDINAMARCA(config)#interfac fastEthernet 0/0
CUNDINAMARCA(config-if)#ip nat inside
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#interface serial 0/1/0
CUNDINAMARCA(config-if)#ip nat outside
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#exit

### 7.2  Listas de control de acceso:

- Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.

Username: admin1
Password:
CUNDINAMARCA>en
Password:
Password:
CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#access-list 111 deny icmp host 172.31.1.68 host 172.31.2.37
CUNDINAMARCA(config)#interface serial 0/1/0
CUNDINAMARCA(config-if)#ip access-group 111 out
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console

Username: admin1
Password:
TUNJA>en
Password:
Password:
TUNJA#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#interface serial 0/1/0
TUNJA(config-if)#ip access-group 111 in
TUNJA(config-if)#exit
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console

- Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.

CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#access-list 112 permit icmp host 172.31.2.12 host 172.31.2.37
CUNDINAMARCA(config)#interface serial 0/1/0
CUNDINAMARCA(config-if)#ip access-group 112 out
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#exit
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#interface serial 0/1/0
TUNJA(config-if)#ip access-group 112 in
TUNJA(config-if)#exit
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console

Se deben denegar las conexiones:
**Entre vlan 10 a vlan 20**
CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#access-list 113 deny icmp host 172.31.2.12 host 172.31.1.68
CUNDINAMARCA(config)#interface serial 0/1/0
CUNDINAMARCA(config-if)#ip access-group 113 in
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
00:47:14: %OSPF-5-ADJCHG: Process 1, Nbr 2.3.4.5 on Serial0/1/0 from FULL to DOWN, Neighbor Down: Dead timer expired
00:47:14: %OSPF-5-ADJCHG: Process 1, Nbr 2.3.4.5 on Serial0/1/0 from FULL to DOWN, Neighbor Down: Interface down or detached

**Entre vlan 10 a vlan 30**
CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#access-list 114 deny icmp host 172.31.2.12 host 172.31.1.2
CUNDINAMARCA(config)#interface serial 0/1/0
CUNDINAMARCA(config-if)#ip access-group 114 in
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console

- Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.

TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#access-list 115 permit icmp host 172.31.1.0 host 209.17.220.10
TUNJA(config)#interface fastethernet 0/0
TUNJA(config-if)#ip access-group 115 out
TUNJA(config-if)#exit
TUNJA(config)#interface fastEthernet 0/1
TUNJA(config-if)#ip access-group 115 in
TUNJA(config-if)#exit
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console

- Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.

**Vlan 20 Tunja a vlan 20 Cund.**
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#access-list 116 permit icmp host 172.31.0.130 host 172.31.1.68
TUNJA(config)#interface fastEthernet 0/1
TUNJA(config-if)#ip access-group 116 in
TUNJA(config-if)#exit
TUNJA(config)#interface serial 0/1/0
TUNJA(config-if)#ip access-group 116 out
TUNJA(config-if)#exit
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console

CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#interface serial 0/1/0
CUNDINAMARCA(config-if)#ip access-group 116 in
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#
00:28:28: %OSPF-5-ADJCHG: Process 1, Nbr 2.3.4.5 on Serial0/1/0 from LOADING to FULL, Loading Done

**Vlan 20 Tunja a vlan 10 Buc.**

TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#access-list 117 permit icmp host 172.31.0.130 host 172.31.0.2
TUNJA(config)#interface fastEthernet 0/1
TUNJA(config-if)#ip access-group 117 in
TUNJA(config-if)#exit
TUNJA(config)#interface serial 0/0/0
TUNJA(config-if)#ip access-group 117 out
TUNJA(config-if)#exit
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console

BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#interface serial 0/1/0
BUCARAMANGA(config-if)#ip access-group 117 in
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#interface fastEthernet 0/0
BUCARAMANGA(config-if)#ip access-group 117 out
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
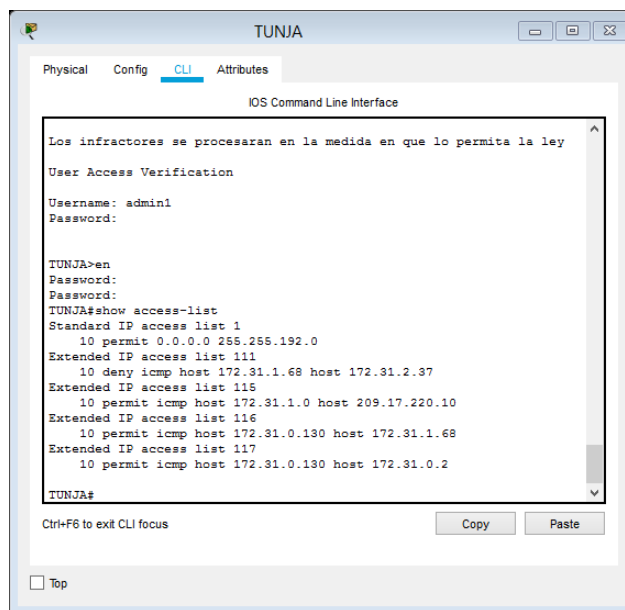


*Figura 40. Access-list Tunja*
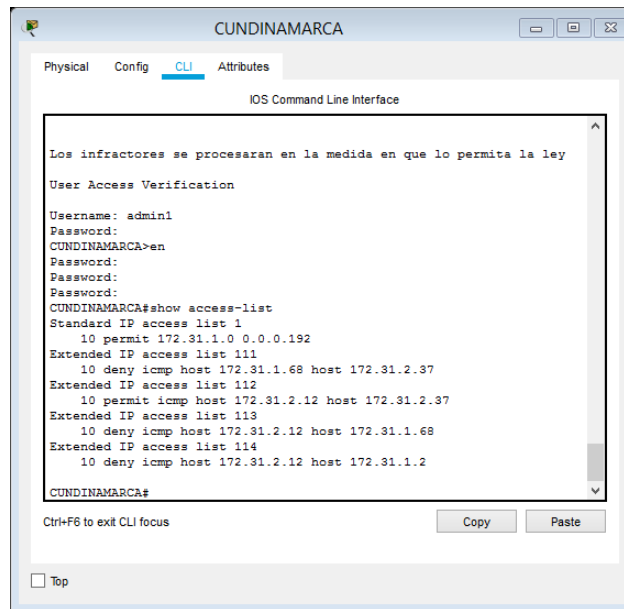
*Figura 41. Access-list Cundinamarca*

## 7.3 Aspectos a tener en cuenta

- Habilitar VLAN en cada switch y permitir su enrutamiento.

### 7.3.1 Switch Bucaramanga

Switch_Buc#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch_Buc(config)#vlan 1
Switch_Buc(config-vlan)#name vlan_1
Switch_Buc(config-vlan)#exit
Switch_Buc(config)#int vlan 1
Switch_Buc(config-if)#ip address 172.31.2.2 255.255.255.248
Switch_Buc(config-if)#no shutdown
Switch_Buc(config-if)#do wr
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch_Buc#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch_Buc(config)#hostname Switch_Buc
Switch_Buc(config)#vlan 10
Switch_Buc(config-vlan)#name Vlan_10
Switch_Buc(config-vlan)#exit
Switch_Buc(config)#int Vlan 10
Switch_Buc(config-if)#ip address 172.31.0.2 255.255.255.192
Switch_Buc(config-if)#

%LINK-5-CHANGED: Interface Vlan10, changed state to up


witch_Buc#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch_Buc(config)#vlan 30
Switch_Buc(config-vlan)#name Vlan_30
Switch_Buc(config-vlan)#exit
Switch_Buc(config)#int vlan 30
Switch_Buc(config-if)#ip address 172.31.0.65 255.255.255.192
Switch_Buc(config-if)#no shutdown
Switch_Buc(config-if)#do wr
Building configuration...
[OK]
Switch_Buc(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

### 7.3.2  Switch Tunja

Switch>en
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Switch_Tun
Switch_Tun(config)#vlan 1
Switch_Tun(config-vlan)#name Vlan_1
Switch_Tun(config-vlan)#exit
Switch_Tun(config)#int vlan 1
Switch_Tun(config-if)#ip address 172.31.2.10 255.255.255.248
Switch_Tun(config-if)#no shutdown
Switch_Tun(config-if)#do wr
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch_Tun#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch_Tun(config)#vlan 20
Switch_Tun(config-vlan)#name Vlan_20
Switch_Tun(config-vlan)#exit
Switch_Tun(config)#int vlan 20
Switch_Tun(config-if)#ip address 172.31.0.130 255.255.255.192
Switch_Tun(config-if)#no shutdown
Switch_Tun(config-if)#do wr
%LINK-5-CHANGED: Interface Vlan20, changed state to up

Switch_Tun#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Switch_Tun(config)#vlan 30
Switch_Tun(config-vlan)#name Vlan_30
Switch_Tun(config-vlan)#exit
Switch_Tun(config)#int vlan 30
Switch_Tun(config-if)#ip address 172.31.0.194 255.255.255.192
Switch_Tun(config-if)#no shutdown
Switch_Tun(config-if)#do wr
%LINK-5-CHANGED: Interface Vlan30, changed state to up


### 7.3.3  Switch Cundinamarca

Switch>en
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Switch_Cun
Switch_Cun(config)#vlan 1
Switch_Cun(config-vlan)#name Vlan_1
Switch_Cun(config-vlan)#exit
Switch_Cun(config)#int vlan 1
Switch_Cun(config-if)#ip address 172.31.2.12 255.255.255.248
Switch_Cun(config-if)#no shutdown
Switch_Cun(config-if)#do wr
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch_Cun#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch_Cun(config)#vlan 20
Switch_Cun(config-vlan)#name Vlan_20
Switch_Cun(config-vlan)#exit
Switch_Cun(config)#int vlan 20
Switch_Cun(config-if)#ip address 172.31.1.68 255.255.255.192
Switch_Cun(config-if)#no shutdown
Switch_Cun(config-if)#do wr
%LINK-5-CHANGED: Interface Vlan20, changed state to up

Switch_Cun#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch_Cun(config)#vlan 30
Switch_Cun(config-vlan)#name Vlan_30
Switch_Cun(config-vlan)#exit
Switch_Cun(config)#int vlan 30
Switch_Cun(config-if)#ip address 172.31.1.2 255.255.255.192
Switch_Cun(config-if)#no shutdown

Switch_Cun(config-if)#do wr
%LINK-5-CHANGED: Interface Vlan30, changed state to up

Switch_Cun#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch_Cun(config)#vlan 88
Switch_Cun(config-vlan)#name Vlan_88
Switch_Cun(config-vlan)#exit
Switch_Cun(config)#int vlan 88
Switch_Cun(config-if)#ip address 172.31.2.26 255.255.255.248
Switch_Cun(config-if)#no shutdown
Switch_Cun(config-if)#do wr
%LINK-5-CHANGED: Interface Vlan88, changed state to up


## 7.4 Enrutamiento OSPF con autenticación en cada router.

CUNDINAMARCA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#router ospf 1
CUNDINAMARCA(config-router)#router-id 1.2.3.4
CUNDINAMARCA(config-router)#network 172.31.0.0 0.0.31.255 area 0
CUNDINAMARCA(config-router)#exit
CUNDINAMARCA(config)#exit
CUNDINAMARCA#Reload or use "clear ip ospf process" command, for this to take effect

TUNJA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#router ospf 1
TUNJA(config-router)#router-id 2.3.4.5
TUNJA(config-router)#network 172.31.0.0 0.0.31.255 area 0
TUNJA(config-router)#exit
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
03:23:26: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.38 on Serial0/1/0 from
LOADING to FULL, Loading Done


BUCARAMANGA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#router ospf 1
BUCARAMANGA(config-router)#router-id 3.4.5.6
BUCARAMANGA(config-router)#network 172.31.0.0 0.0.31.255 area 0

BUCARAMANGA(config-router)#exit
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
03:25:00: %OSPF-5-ADJCHG: Process 1, Nbr 2.3.4.5 on Serial0/1/0 from LOADING to
FULL, Loading Done

# 8  CONCLUSIONES

Considero que con la realización de este trabajo obtuve conocimientos claros acerca de las direcciones IP y cual su funcionamiento, lo cual me puede ayudar a decidir qué tipo o clase de direccionamiento IP debo utilizar de acuerdo a ciertas necesidades ya sea en el hogar, empresa pública o privada.

De esta práctica puedo concluir que, existen protocolos sencillos y fáciles de implementar, los cuales ayudan a establecer de manera estática las direcciones ip de las diferentes interfaces de los distintos dispositivos que conforman una red; haciendo énfasis en el router, donde se pueden usar protocolos para enrutar y comunicar a diferentes redes, tanto LAN como WAN. Pues este proceso de asignar direcciones es complejo de aplicar en redes de gran tamaño.

Además, se pudo observar que la transmisión de los datos, al utilizar enrutamiento estático es más confiable, este protocolo ayuda a que la confiabilidad en la red sea muy segura. Al implementar una ruta de respaldo o ruta sucesora, va a permitir que, si por algún motivo la conexión de los dispositivos es defectuosa, desconectada o violada en su acceso, la comunicación en la red se va a seguir transmitiendo por medio de esta ruta sucesora, sin que los datos sufran algunos cambios y llevándolos a sus destinos establecidos.

Finalmente, en cuanto al protocolo EIGRP se puede decir que es un protocolo sencillo que ayuda a muchos procesos dentro de la implementación de una red, ayuda a saber cuándo se presentaron daños, permite conocer dispositivos que son vecinos o están conectados adyacentemente, enruta de manera ordenada las direcciones de las interfaces.

# 9    REFERENCIAS BIBLIOGRAFICAS

*CISCO. (2014*, 01*). Asignación de direcciones IP. Fundamentos de Networking.* Obtenido 12, 2019, de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

*CISCO. (2014*, 01*). SubNetting. Fundamentos de Networking. Obtenido 12, 2019, de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1*

CISCO SYSTEM. (2017, 01). Capítulo 6. Enrutamiento estático. Obtenido 12, 2019, de https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#6.0.1.1

CISCO SYSTEM. (2017, 01). Capítulo 7. Routing Dinámico. Obtenido 12, 2019, de https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#7.0.1.1

CISCO SYSTEM. (2017, 01). Capítulo 6. Enrutamiento estático. Obtenido 12, 2019, de https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#6.0.1.1

CISCO SYSTEM. (2017, 01). Capítulo 7. Routing Dinámico Obtenido 12, 2019, de https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#7.0.1.1

UNAD (2014). Principios de Enrutamiento [OVA]. Obtenido 12, 2019, de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

CISCO SYSTEM. (2017, 01). Capítulo 3. VLAN. Obtenido 12, 2019, de https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#3.0.1.1

CISCO SYSTEM. (2017, 01). Capítulo 8. OSPF de área única. Obtenido 12, 2019, de https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#8.0.1.1

Pérez, S. (2017, 01). DISPOSITIVOS Y PROTOCOLOS DE REDES LAN Y WAN. CERECON. Obtenido 12, 2019, de http://www.cerecon.frm.utn.edu.ar/archives/Libro-Dispositivos-y-protocolos-de-Redes-LAN-y-WAN.pdf