TITULO DELTRABAJO
Evaluación de habilidades practicas CCNA

John Erikc Alexander Obando Ramírez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA (ECBTI)
PROGRAMA DE INGENIERIA DE SISTEMAS
PALMIRA
2019

EVALUACIOIN DE HABILIDADES PRACTICAS CCNA

John Erikc Alexander Obando Ramírez

DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

JOSE IGNACIO CARDONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA (ECBTI)
PROGRAMA DE INGENIERIA DE SISTEMAS
PALMIRA
2019

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Ciudad y Fecha (día, mes, año) (Fecha de entrega)

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE GRÁFICAS

Pág.

RESUMEN

En el presente trabajo desarrollado muestra 2 escenarios

Escenario 1 es una empresa donde posee sucursales distribuidas en la ciudad de Bogotá, Medellín y Cali donde se debe crear una red el cual se debe de configurar e intercambiar entre sí, donde se requiere direccionamiento IP de acuerdo al numero de host asignar parámetros básicos a cada router y swicht que se encuentren en la red crear subredes para establecer la conexión total de todos los hosts que deben de comunicarse realizar implementación de seguridad en la red al igual restringir el acceso y comunicación entre los host de acuerdo al administrador de la red al igual que realizar el proceso de validación del funcionamiento de los dispositivos de red.

Escenario 2 es una empresa que cuenta con una conexión de internet en una red Ethernet en donde se debe adaptar para que sea más fácil que los routers y las redes puedan conectarse a internet, pero con la condición de emplear direcciones de red LAN original donde debemos realizar configuraciones de routers, configuración de DHCP que van a proporcionar direcciones a los hosts de Bucaramanga y Cundinamarca, configurando servidores web crear enrutamientos y listas de control de acceso mediante VLAN al igual que VLSM

PALABRAS CLAVE: Routers, Switch, VLAN, VLMS, Enrutamiento, Red, DHCP, Sucursales, Comunicación, Internet, Ethernet, LAN y Direcciones

ABSTRACT

In the present work developed shows 2 scenarios

Scenario 1 is a company where it has branches distributed in the city of Bogotá, Medellín and Cali where a network must be created which must be configured and exchanged with each other, where IP addressing is required according to the host number assign basic parameters to each router and swicht that are in the network create subnets to establish the total connection of all the hosts that must communicate perform security implementation in the network as well as restrict access and communication between the hosts according to the network administrator at as well as performing the process of validating the operation of the network devices.
Scenario 2 is a company that has an internet connection in an Ethernet network where it must be adapted to make it easier for routers and networks to connect to the internet, but with the condition of using original LAN network addresses where we must Perform router configurations, DHCP settings that will provide addresses to Bucaramanga and Cundinamarca hosts, configuring web servers create routing and access control lists via VLAN as well as VLSM

KEY WORDS: Routers, Switch, VLAN, VLMS, Routing, Network, DHCP, Branches, Communication, Internet, Ethernet, LAN and Addresses

1. INTRODUCCIÓN

El presente trabajo nos permite desarrollar 2 escenarios donde pondremos en practica todas las habilidades adquiridas en el transcurso de la enseñanza del diplomado Cisco donde ponemos en marcha los conocimientos en el desarrollo y diseño de redes por medio de la herramienta Packet Tracer.

Con el cual realizaremos configuraciones o parámetros básicas y de seguridad a router, switches para que así se puedan comunicar los equipos conectados a la red al igual que la comparación total de todos los dispositivos y su funcionamiento a cada unos de los escenarios planteados en la actividad donde se desarrolla en la modalidad práctica.

De manera que nosotros como estudiantes apliquemos los conocimientos en la solución de problemas LAN y WAN comenzando con los conocimientos básicos en cada uno de los elementos de una red como son los dispositivos tipos de redes cableado configuración y su óptimo funcionamiento.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Crear 2 escenarios aplicando todos los conocimientos adquiridos en el trascurso del DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN) creando las diversas soluciones a los problemas planteados a cada uno de los escenarios mediante Packet tracer

2.2 OBJETIVOS ESPECÍFICOS

- ✓ Analizar el problema
- ✓ Realizar el diseño de cada escenario
- ✓ Utilizar la herramienta de Packet tracer
- ✓ Realizar conexiones y configuraciones Básicas a routers y switches
- ✓ Realizar proceso de asignación de IP al host
- ✓ Realizar procesos de configuración de DHCP
- ✓ Comprobar conexiones por medio de ping y telnet
- ✓ Comprobar el funcionamiento de cada escenario

6 DESARROLLO DEL PROYECTO

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.

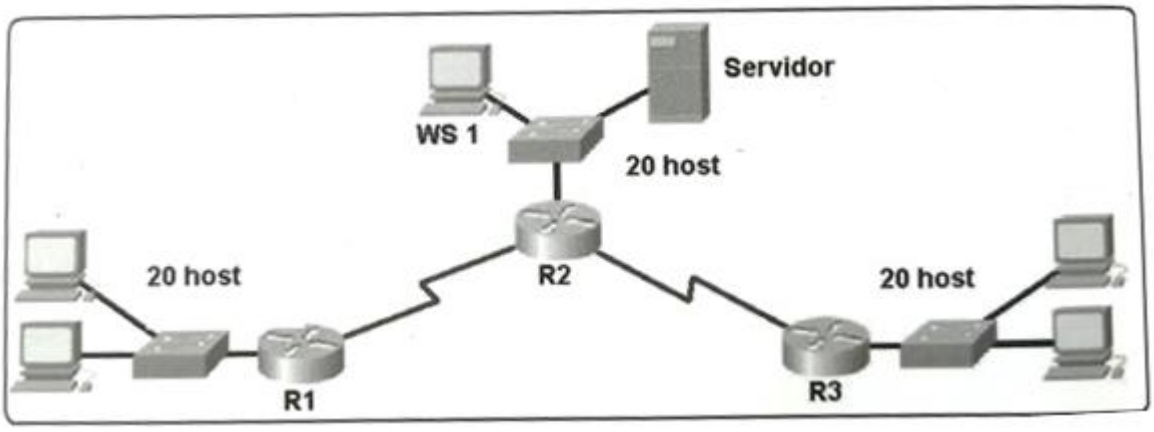

Figura 1: Escenario 1

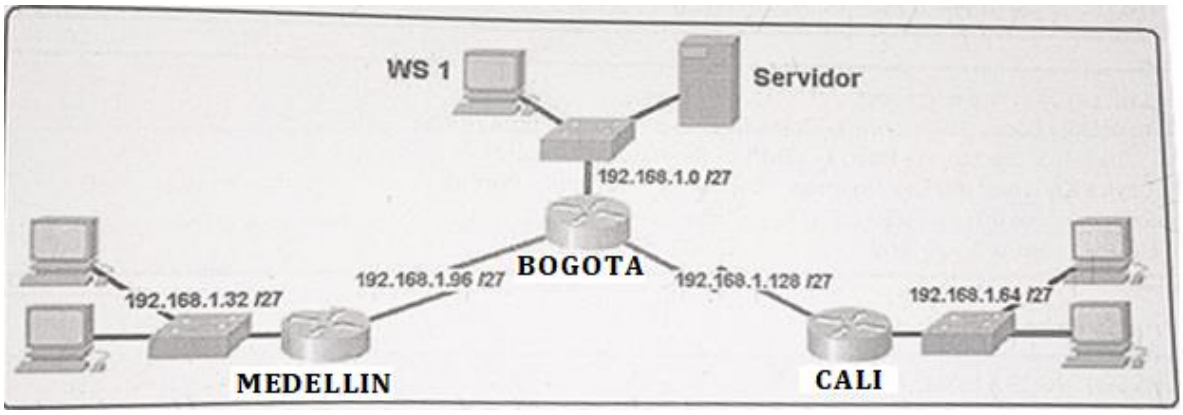

Figura 2: Topología de red

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).

  - **Router BOGOTA**

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA
BOGOTA(config)#enable secret class
BOGOTA(config)#banner motd #
Enter TEXT message. End with the character '#'.
Unauthorized access is strictly prohibited. #
BOGOTA(config)#line con 0
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#logging synchronous
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
```

- **Router MEDELLIN**

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN
MEDELLIN(config)#enable secret class
MEDELLIN(config)#banner motd #
Enter TEXT message. End with the character '#'.
Unauthorized access is strictly prohibited. #
MEDELLIN(config)#line con 0
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#logging synchronous
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
```

- **Router CALI**

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CALI
CALI(config)#enable secret class
CALI(config)#banner motd #
Enter TEXT message. End with the character '#'.
Unauthorized access is strictly prohibited. #
CALI(config)#line con 0
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#logging synchronous
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
```

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

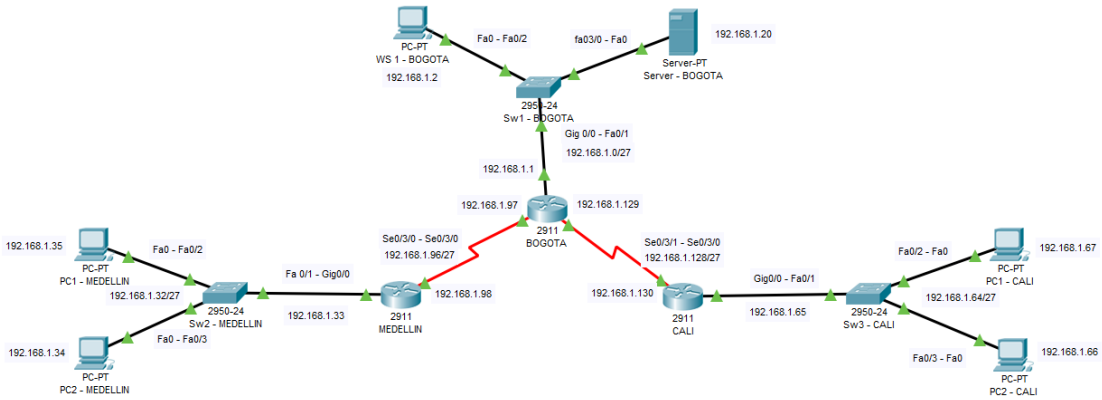

Figura 3 Conexión fisica de los equipos con base en la topología

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

Parte 1: Asignación de direcciones IP.

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

- **Dirección de red: 192.168.1.0/24**
  Mascara: 255.255.255.0
  Binario: 11111111.11111111.11111111.00000000

- **Segmentación:** Se requiere segmentar en 8 partes la red

  $2^3 = 8$
  Se encienden 3 bits que corresponde al numero usado para elevado en la formula anterior

  Binario: 11111111.11111111.11111111.111 00000
  Red Host

  Mascara: 255.255.255.224
  Dirección de Red: 192.168.1.0/27

- **Determinamos los saltos de red**

  $\frac{-256}{224}$ Los saltos serán de 32

- **Cantidad de Host por subred**

  $2^m - 2 = H$

  $2^5 - 2 = H$

  $2x2x2x2x2 = 32 - 2 = 30\ Host$

- **Definición Subredes**

SUBRED 1	SUBRED 5
Network: 192.168.1.0/27	**Network: 192.168.1.128/27**
HostMin: 192.168.1.1	**HostMin: 192.168.1.129**
HostMax:192.168.1.30	**HostMax:192.168.1.158**
Broadcast:192.168.1.31	**Broadcast:192.168.1.159**
SUBRED 2	SUBRED 6
Network: 192.168.1.32/27	**Network: 192.168.1.160/27**
HostMin: 192.168.1.33	**HostMin: 192.168.1.161**
HostMax:192.168.1.62	**HostMax:192.168.1.190**
Broadcast:192.168.1.63	**Broadcast:192.168.1.191**
SUBRED 3	SUBRED 7
Network: 192.168.1.64/27	**Network: 192.168.1.192/27**
HostMin: 192.168.1.65	**HostMin: 192.168.1.193**
HostMax:192.168.1.94	**HostMax:192.168.1.222**
Broadcast:192.168.1.95	**Broadcast:192.168.1.223**
SUBRED 4	SUBRED 8
Network: 192.168.1.96/27	**Network: 192.168.1.224/27**
HostMin: 192.168.1.97	**HostMin: 192.168.1.225**
HostMax:192.168.1.126	**HostMax:192.168.1.254**
Broadcast:192.168.1.127	**Broadcast:192.168.1.255**

Tabla 1. Definición Subredes

b. Asignar una dirección IP a la red.

BOGOTA – 20 HOSTS		
1	Dirección de red	192.168.1.0
2	Dirección IP Gateway	192.168.1.1
3	IP PC1	192.168.1.2
4	SW1	192.168.1.19
5	IP Servidor	192.168.1.20
6	Máscara de Subred	255.255.255.0

Tabla 2. Asignar dirección IP a la red BOGOTA-20 HOST

MEDELLIN – 20 HOSTS		
1	Dirección de red	192.168.1.32
2	Dirección IP Gateway	192.168.1.32
3	IP PC1	192.168.1.35
4	IP PC20	192.168.1.54
5	Mascara de Subred	255.255.255.0

Tabla 3. Asignar dirección IP a la red MEDELLIN – 20 HOST

CALI – 20 HOSTS		
1	Dirección de red	192.168.1.65
2	Dirección IP Gateway	192.168.1.64
3	IP PC1	192.168.1.66
4	IP PC20	192.168.1.86
5	Máscara de Subred	255.255.255.0

Tabla 4. Asignar dirección IP a la red CALI – 20 HOST

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	192.168.1.98	192.168.1.97	192.168.1.130
Dirección de Ip en interfaz Serial 0/1		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

Tabla 5. Configuración básica de routers

- **Configuración Básica Router BÓGOTA**

  - ✓ **IP ROUTER BOGOTA G0/0 – SWITCH**

    BOGOTA#en
    BOGOTA#config t
    Enter configuration commands, one per line. End with CNTL/Z.
    BOGOTA(config)#int g0/0
    BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224
    BOGOTA(config-if)#no shut
    BOGOTA(config-if)#
    %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
    %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
    BOGOTA(config-if)#exit

  - ✓ **IP ROUTER BOGOTA S0/3/0 – ROUTER MEDELLIN**

    BOGOTA>en
    BOGOTA#config t
    Enter configuration commands, one per line. End with CNTL/Z.
    BOGOTA(config)#int s0/3/0
    BOGOTA(config-if)#ip address 192.168.1.97 255.255.255.240

BOGOTA(config-if)#no shut

BOGOTA(config-if)#exit

- ✓ **IP ROUTER BOGOTA S0/3/1 – ROUTER CALI**

BOGOTA#en
BOGOTA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#int s0/3/1
BOGOTA(config-if)#ip address 192.168.1.129 255.255.255.240
BOGOTA(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
BOGOTA(config-if)#exit
BOGOTA(config)#exit
BOGOTA#

- ➢ **Configuración Básica Router MEDELLIN**

- ✓ **IP ROUTER MEDELLIN – G0/0 – SWITCH**

MEDELLIN#en
MEDELLIN#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#int g0/0
MEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.240
MEDELLIN(config-if)#no shut
MEDELLIN(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
MEDELLIN(config-if)#exit

- ✓ **IP ROUTER MEDELLIN S0/3/0 – ROUTER BOGOTA**

MEDELLIN#en
MEDELLIN#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#int s0/3/0
MEDELLIN(config-if)#ip address 192.168.1.98 255.255.255.240
MEDELLIN(config-if)#no shut
MEDELLIN(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
MEDELLIN(config-if)#exit
MEDELLIN(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

- ➢ **Configuración Básica Router CALI**

- ✓ **IP ROUTER CALI S0/3/0 – ROUTER BOGOTA**

CALI>en
CALI#config t
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#int s0/3/0
CALI(config-if)#ip address 192.168.1.130 255.255.255.240
CALI(config-if)#no shut
CALI(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
CALI(config-if)#exit
CALI(config)#

- ✓ **IP ROUTER CALI G0/0 – SWITCH**

CALI#en
CALI#config t
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#int g0/0
CALI(config-if)#ip address 192.168.1.65 255.255.255.240
CALI(config-if)#no shut

CALI(config-if)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

CALI(config-if)#exit

CALI(config)#

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.

show ip route

- **Router BOGOTA**

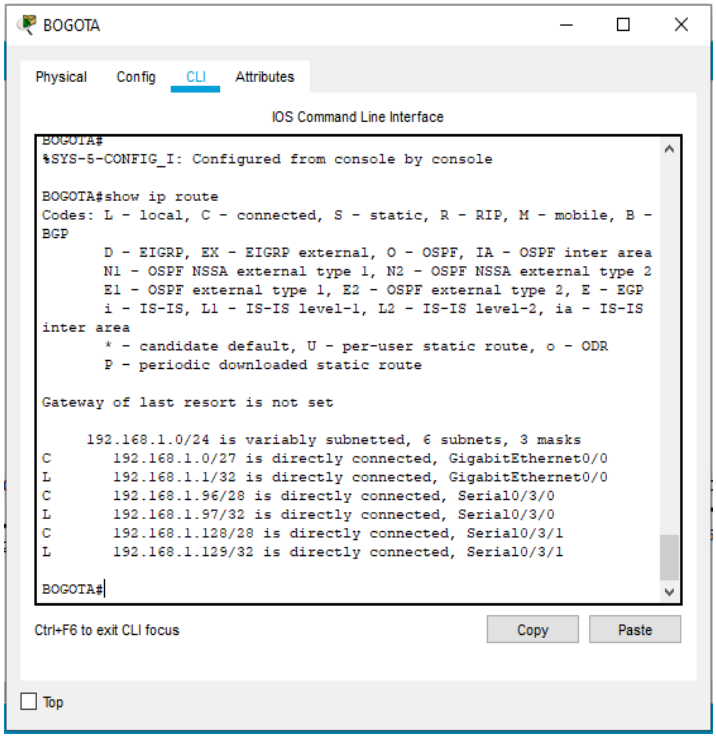

Figura 4: Show ip route Router BOGOTA

➢ Router MEDELLIN

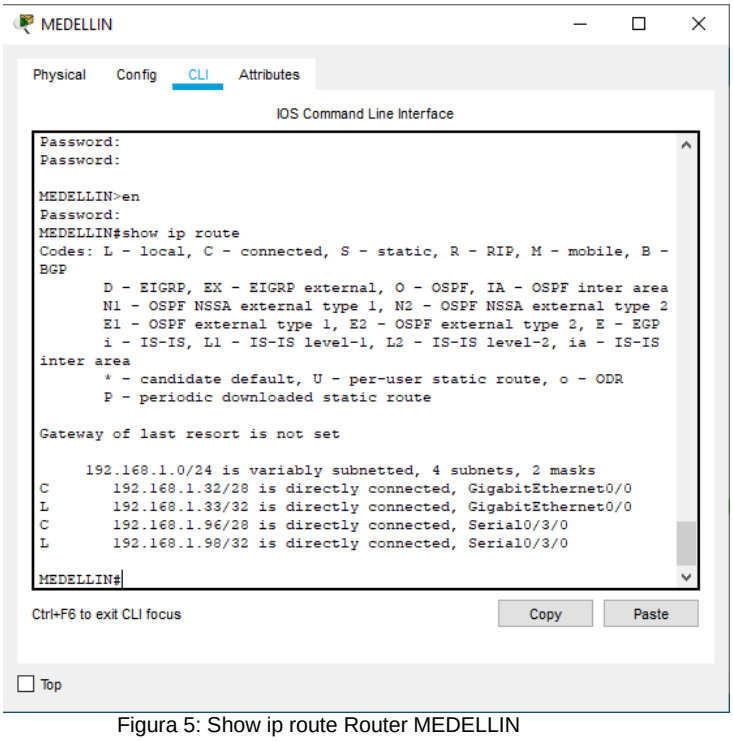

Figura 5: Show ip route Router MEDELLIN

➢ Router CALI

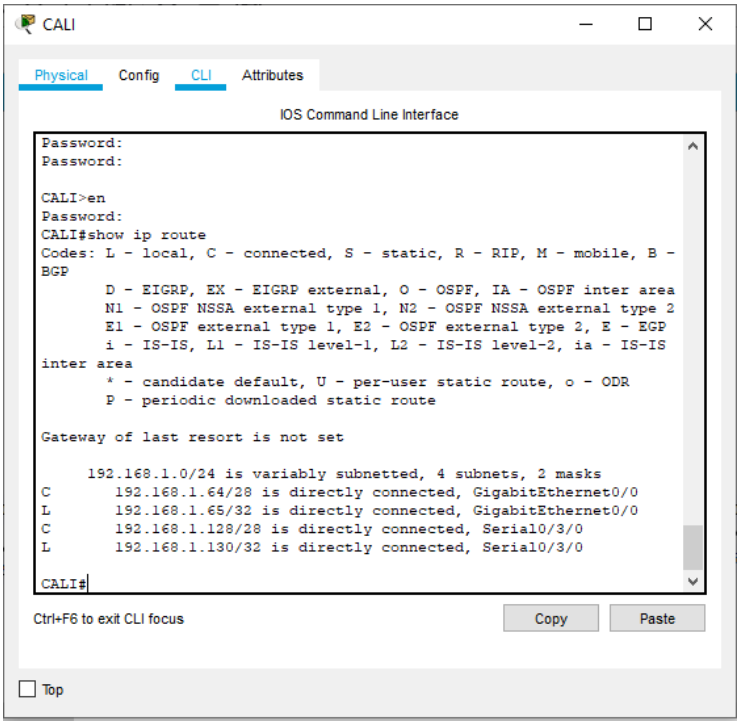

Figura 6: Show ip route Roter CALI

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

show ip route

- **Balanceo de carga BOGOTA**

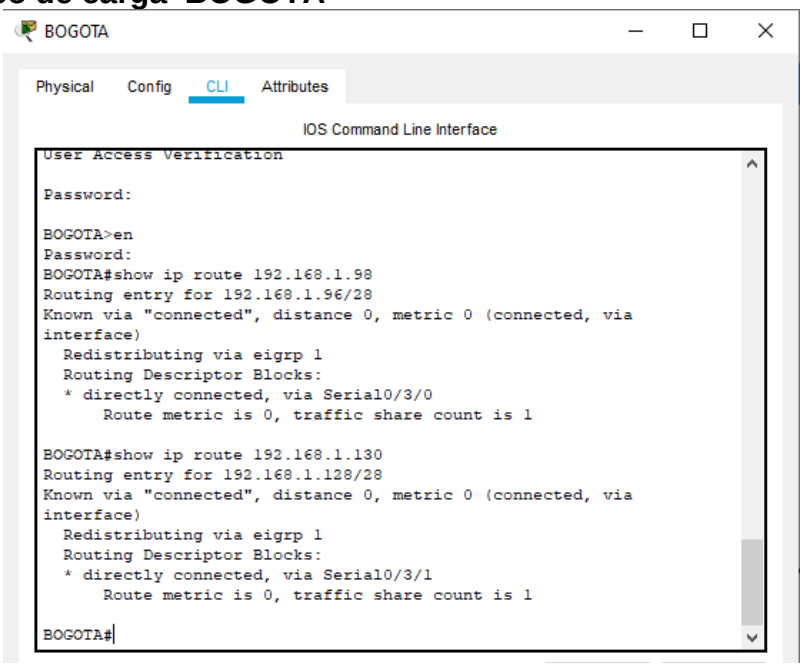

Figura 7: Balanceo de carga BOGOTA

- **Balanceo de carga Router MEDELLIN**

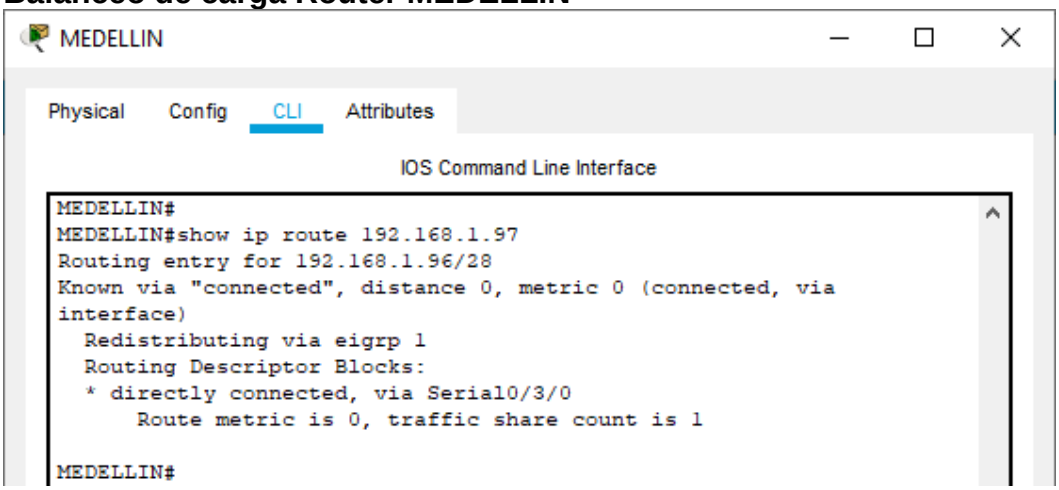

Figura 8: Balanceo de carga Router MEDELLIN

- **Balanceo de carga Router CALI**

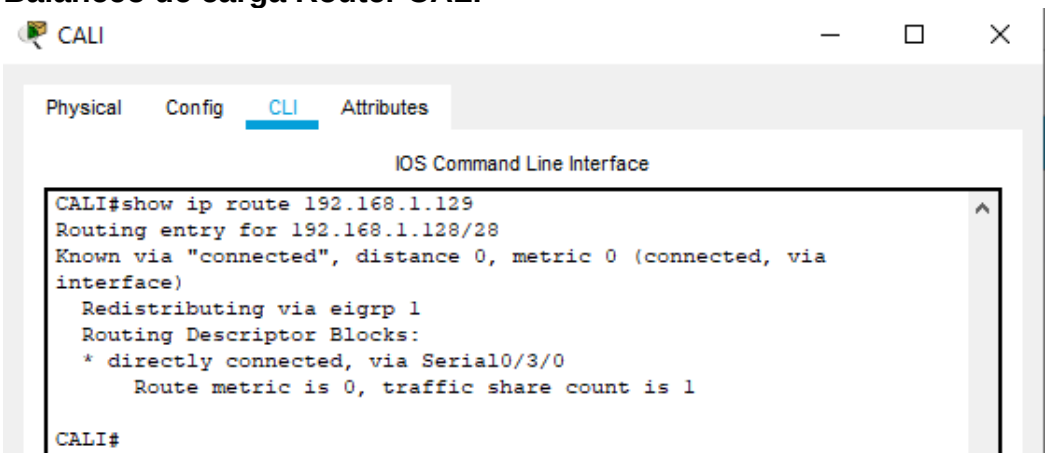

Figura 9: Balanceo de carga Router CALI

d. Realizar un diagnóstico de vecinos uzando el comando cdp.
show cdp neighbors

- **Diagnóstico de vecinos Router BOGOTA**

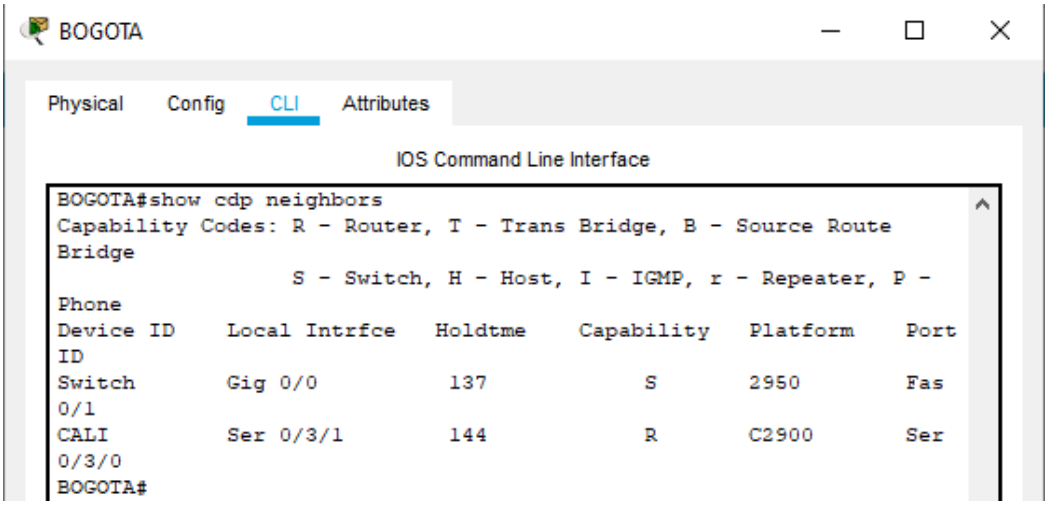

Figura 10: Diagnóstico de vecinos Router BOGOTA

➢ Diagnóstico de vecinos Router MEDELLIN

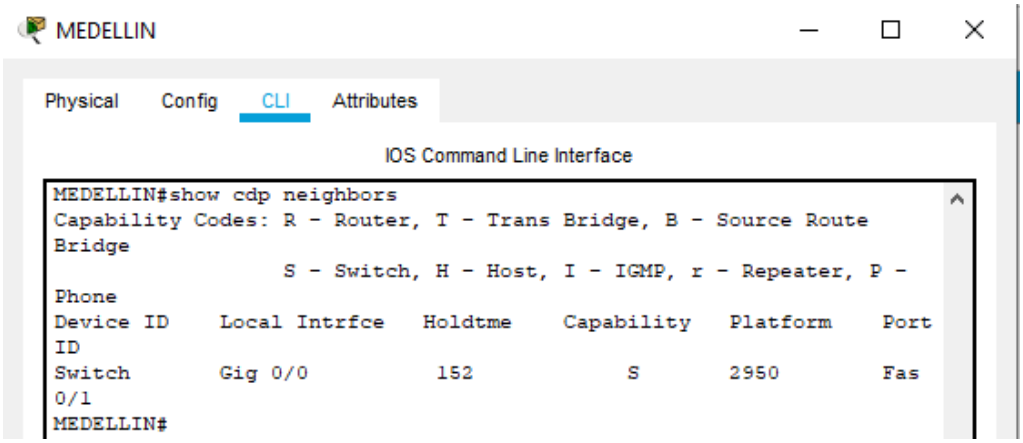

Figura 11: Diagnóstico de vecinos Router MEDELLIN

➢ Diagnóstico de vecinos Router CALI

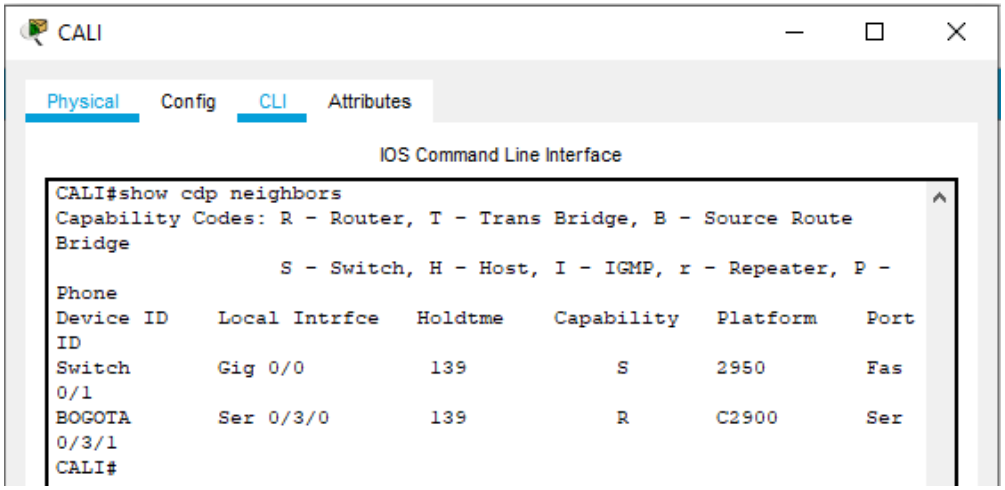

Figura 12: Diagnóstico de vecinos Router CALI

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

- **PING WS 1–BOGOTA A ROUTER BOGOTA**
- **PING WS 1-BOGOTA A ROUTER MEDELLIN**
- **PING WS 1-BOGOTA A ROUTER CALI**

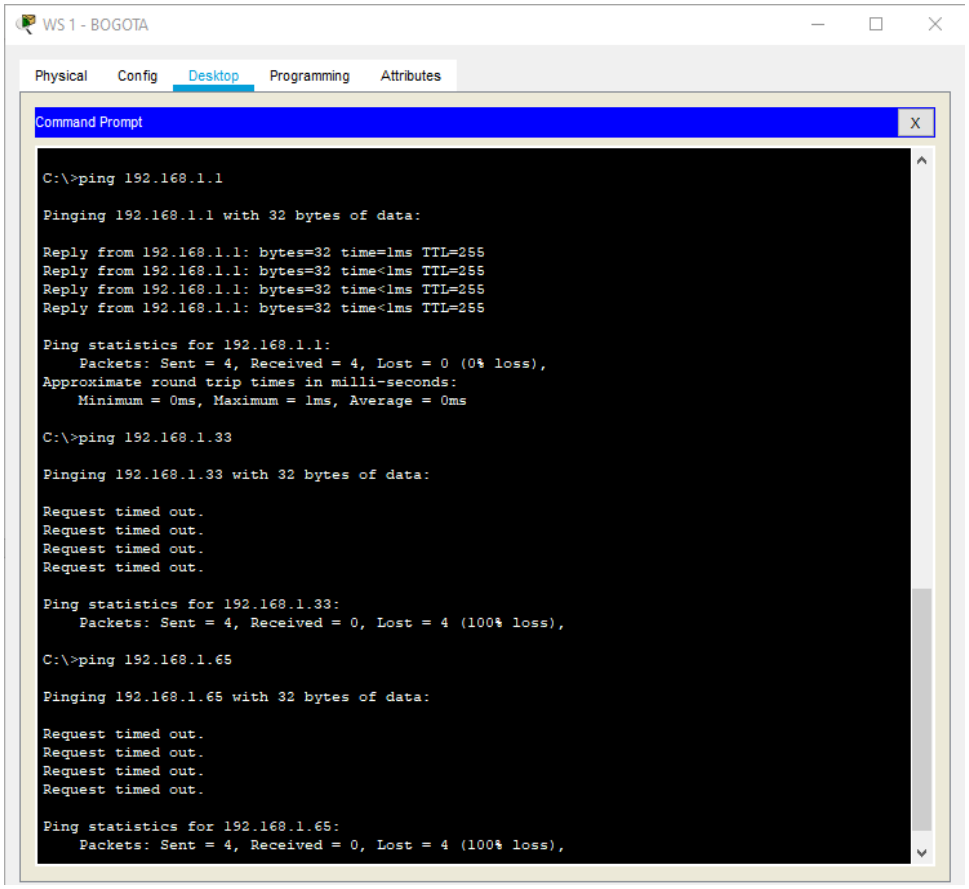

Figura 13: PING BOGOTA

- **PING PC1-MEDELLIN A ROUTER MEDELLIN**
- **PING PC1–MEDELLIN A ROUTER BOGOTA**

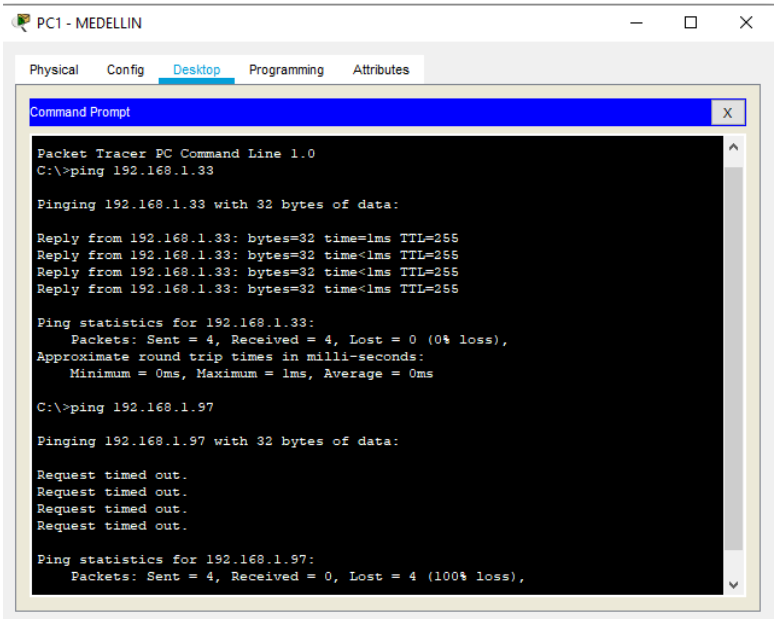

Figura 14: PING MEDELLIN

- **PING PC1-CALI A ROUTER CALI**
- **PING PC1-CALI A ROUTER BOGOTA**

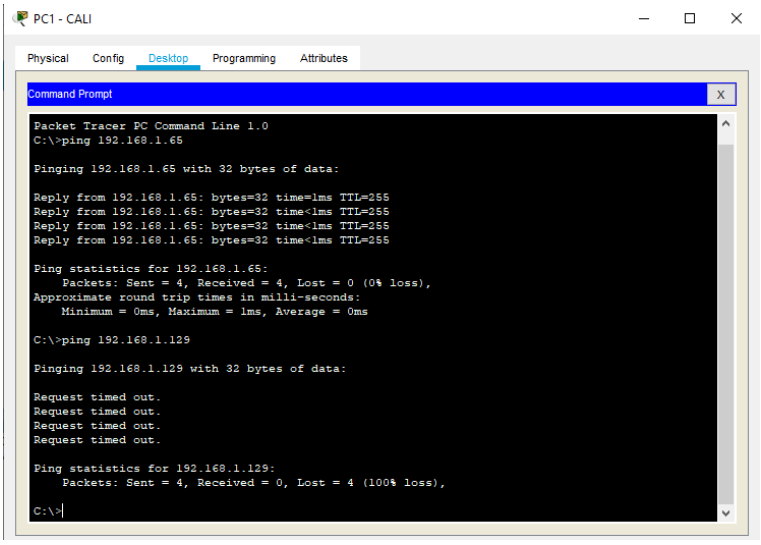

Figura 15: PING CUNDINAMARCA

Parte 3: Configuración de Enrutamiento.

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

- **EIGRP ROUTER BOGOTA**

```
Unauthorized access is strictly prohibited.
User Access Verification
Password:
BOGOTA>en
Password:
BOGOTA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#router eigrp 1
BOGOTA(config-router)#network 192.168.1.0 0.0.0.255
BOGOTA(config-router)#network 192.168.1.96 0.0.0.255
BOGOTA(config-router)#network 192.168.1.128 0.0.0.255
BOGOTA(config-router)#no auto-summary
BOGOTA(config-router)#exit
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.1.98 (Serial0/3/0)
is up: new adjacency
BOGOTA(config-router)#exit
BOGOTA(config)#
```

- **EIGRP ROUTER MEDELLIN**

```
Unauthorized access is strictly prohibited.
User Access Verification
Password:
MEDELLIN>en
Password:
MEDELLIN#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#router eigrp 1
MEDELLIN(config-router)#network 192.168.1.32 0.0.0.255
MEDELLIN(config-router)#network 192.168.1.96 0.0.0.255
MEDELLIN(config-router)#no auto-summary
MEDELLIN(config-router)#exit
MEDELLIN(config)#
```

- **EIGRP ROUTER CALI**

  Unauthorized access is strictly prohibited.
  User Access Verification
  Password:
  CALI>en
  Password:
  CALI#config t
  Enter configuration commands, one per line. End with CNTL/Z.
  CALI(config)#router eigrp 1
  CALI(config-router)#network 192.168.1.64 0.0.0.255
  CALI(config-router)#network 192.168.1.128 0.0.0.255
  CALI(config-router)#no auto-summary
  CALI(config-router)#exit
  %DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.1.129 (Serial0/3/0) is up: new adjacency
  CALI(config-router)#exit
  CALI(config)#

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

- **Vecindad Router BOGOTA**

  BOGOTA#show ip eigrp neighbors
  IP-EIGRP neighbors for process 1
  H Address Interface Hold Uptime SRTT RTO Q Seq
  (sec) (ms) Cnt Num
  0 192.168.1.130 Se0/3/1 10 02:03:54 40 1000 0 13
  1 192.168.1.98 Se0/3/0 14 01:59:04 40 1000 0 8
  BOGOTA#

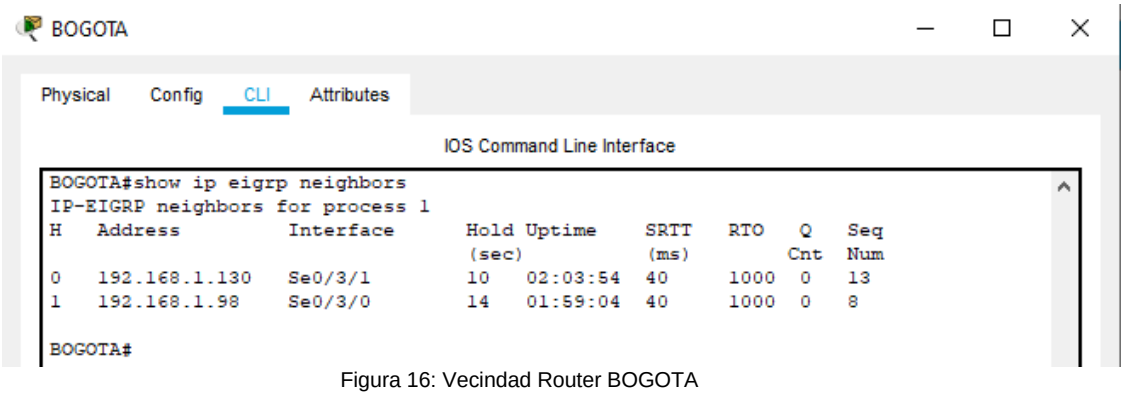

Figura 16: Vecindad Router BOGOTA

- **Vecindad Router MEDELLIN**

MEDELLIN#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.1.97 Se0/3/0 13 02:08:07 40 1000 0 13
MEDELLIN#

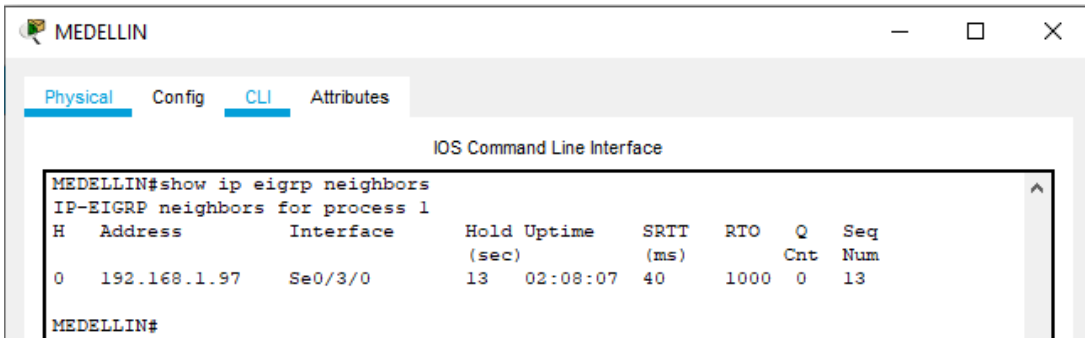

Figura 17: Vecindad Router MEDELLIN

- **Vecindad Router CALI**

CALI#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.1.129 Se0/3/0 10 02:02:56 40 1000 0 12
CALI#

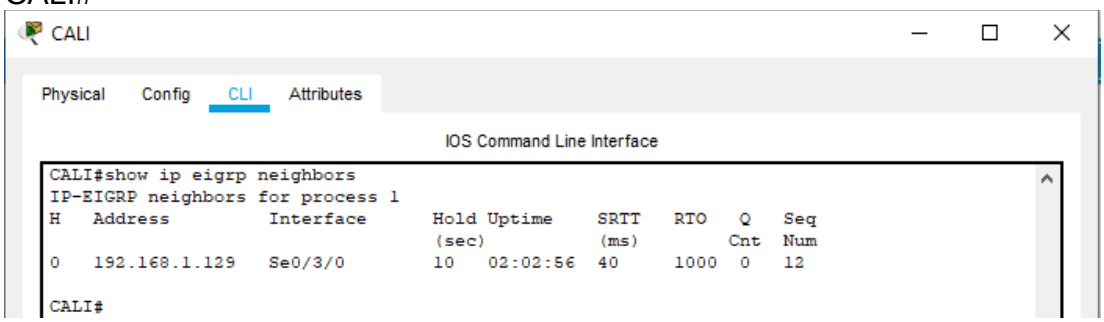

Figura 18: Vecindad Router CALI

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

- **Rutas establecidas del Router BOGOTA**

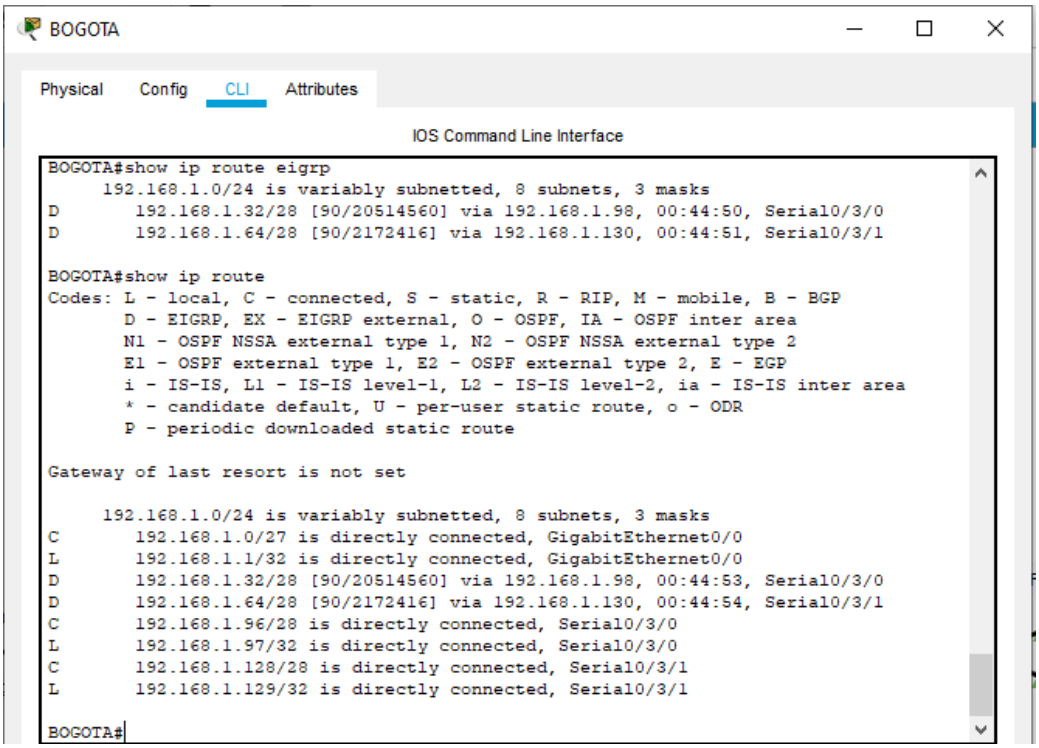

Figura 19: Rutas establecidas del Router BOGOTA

➢ Rutas establecidas del Router MEDELLIN

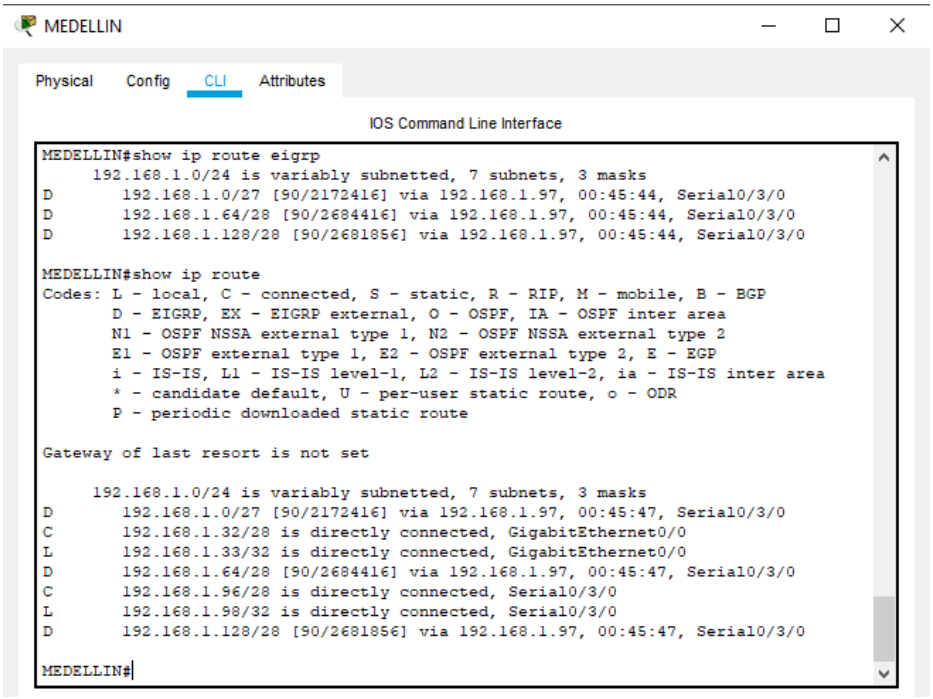

Figura 20: Rutas establecidas del Router MEDELLIN

➢ Rutas establecidas del Router CALI

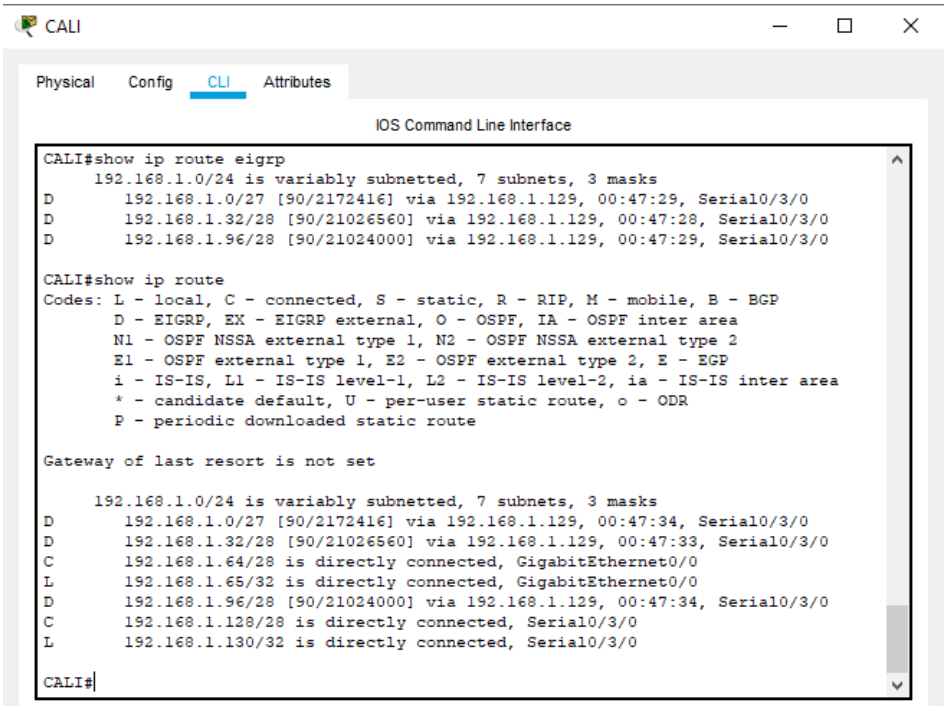

Figura 21: Rutas establecidas del Router CALI

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.

- **PC2 – CALI --> PC1 – MEDELLIN**
- **PC2 – CALI --> SERVER – BOGOTA**

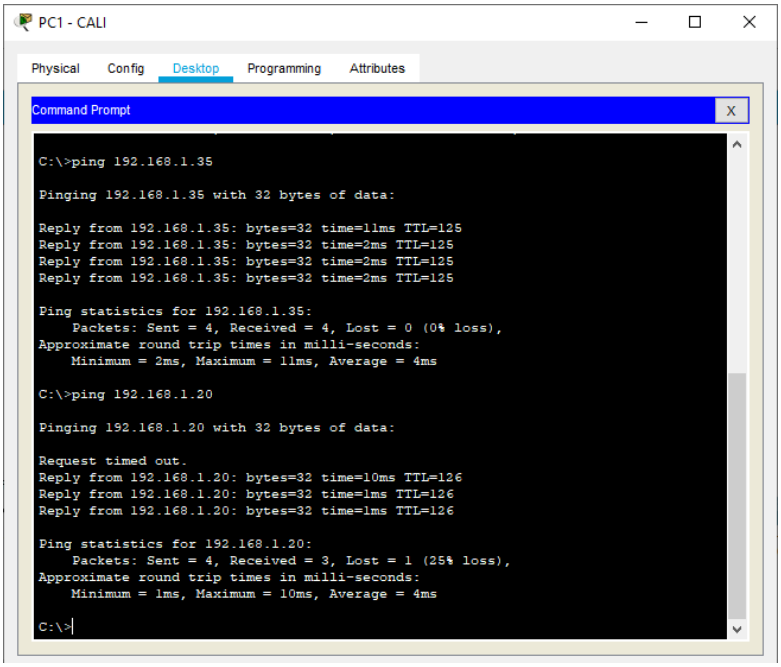

Figura 22: PING PC2-CALI →MEDELLIN→SERVIDOR BOGOTA

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:

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

- **Establecer conexiones Telnet del Router BOGOTA a MEDELLIN y CALI**

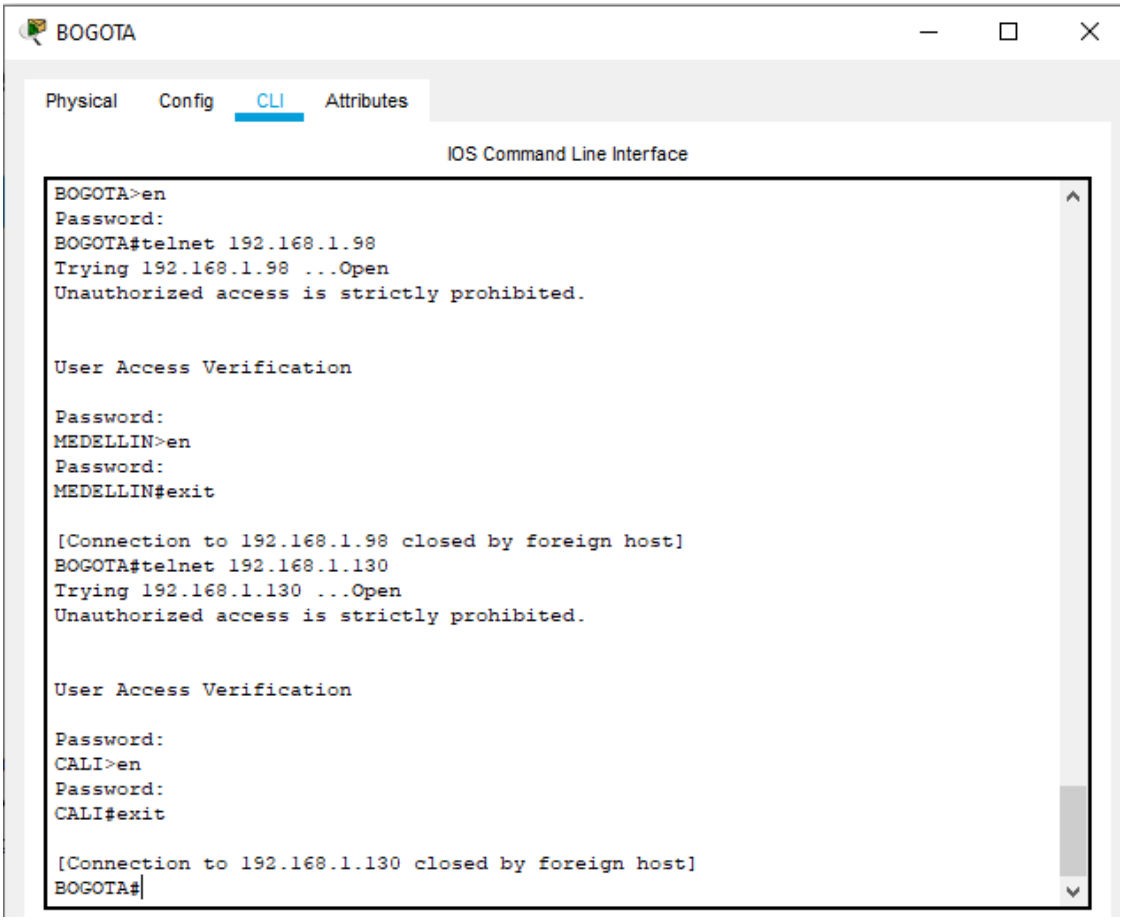

Figura 23: Router BOGOTA a MEDELLIN y CALI

- **Establecer conexiones Telnet del Router MEDELLIN a BOGOTA y CALI**

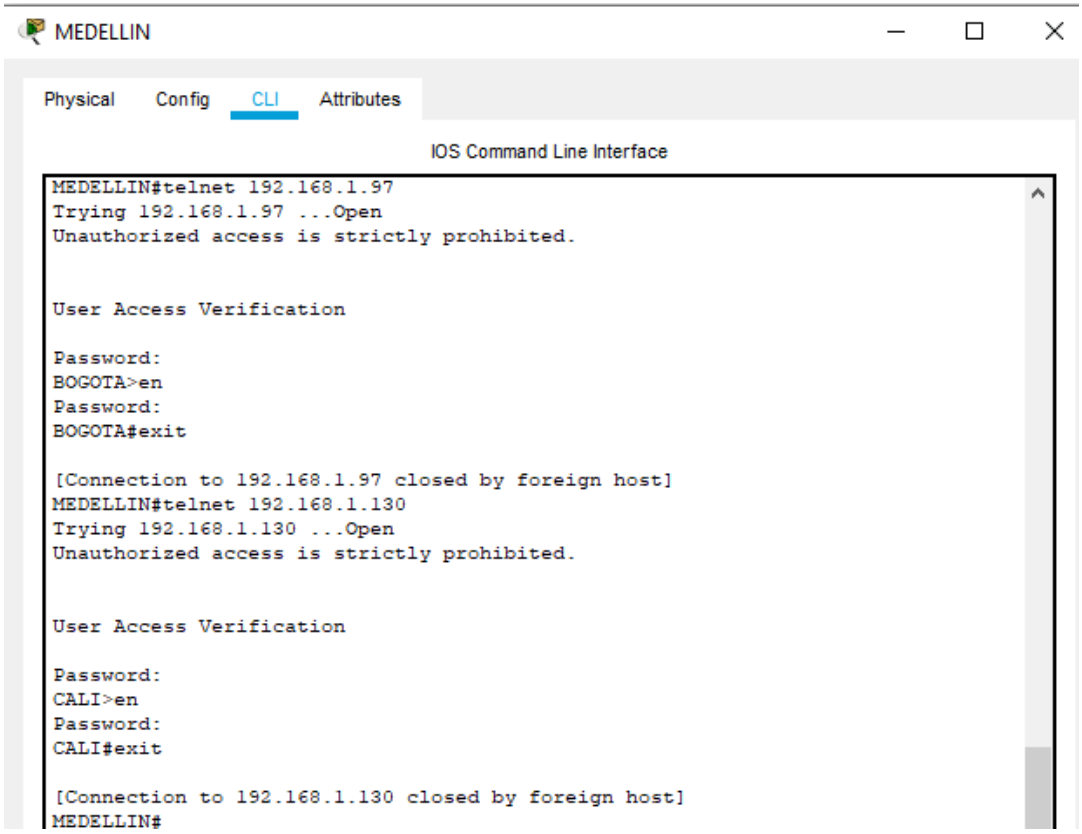

Figura 24: Telnet Router MEDELLIN a BOGOTA y CALI

- **Establecer conexiones Telnet del Router CALI a MEDELLIN y BOGOTA**

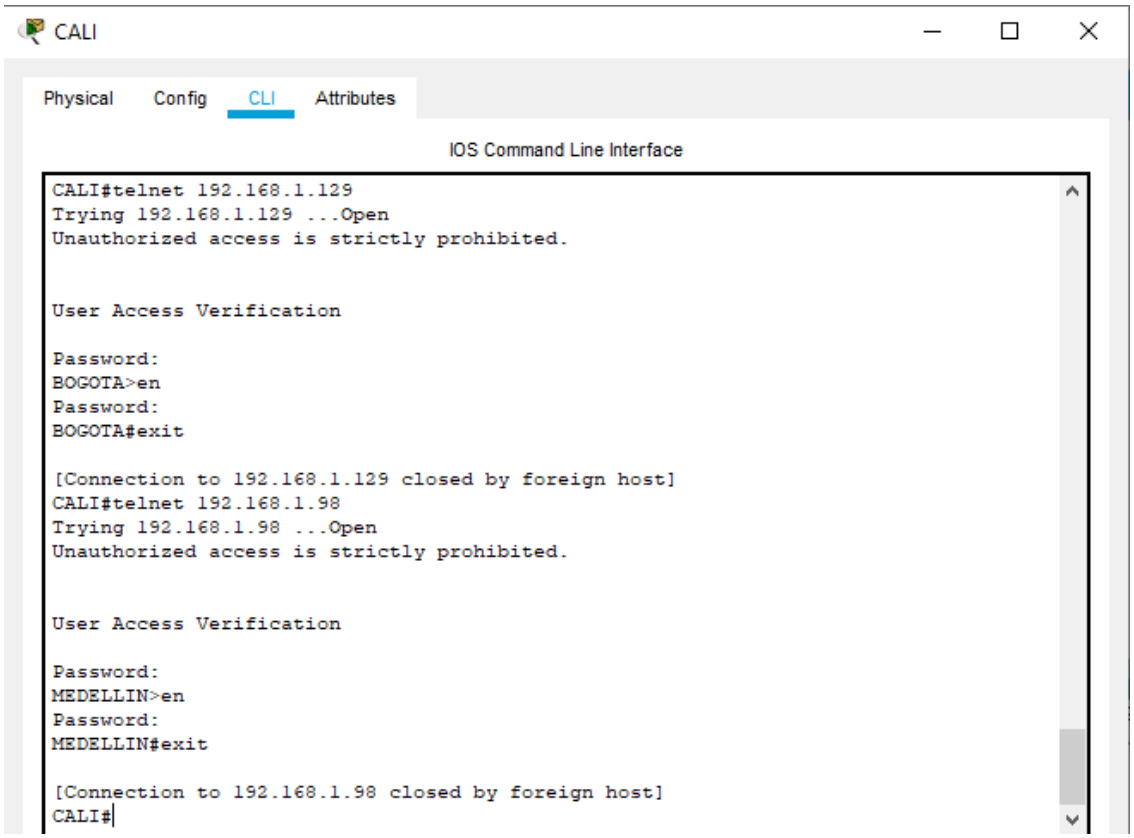

Figura 25: Telnet del Router CALI a MEDELLIN y BOGOTA

a. 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.

➢ Acceso del servidor BOGOTA a equipos CALI

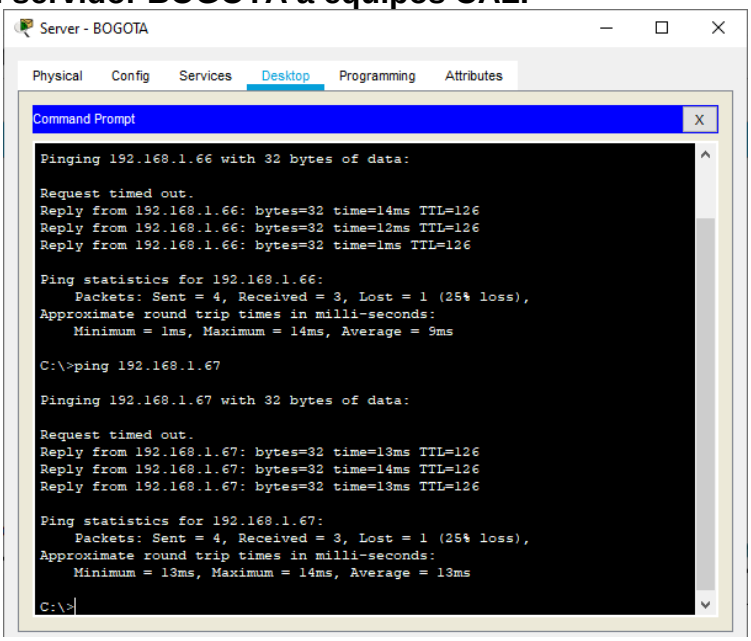

Figura 26: Acceso del servidor BOGOTA a equipos CALI

➢ Acceso del servidor BOGOTA a equipos MEDELLIN

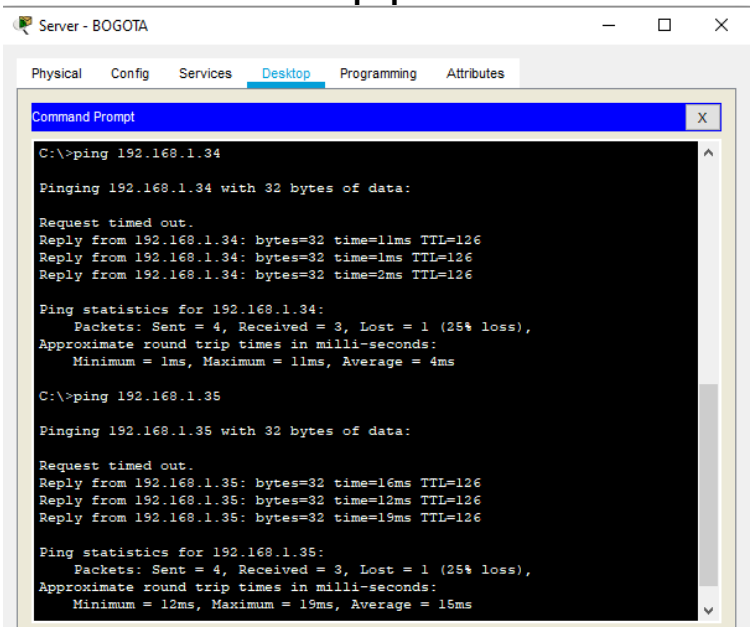

Figura 27: Acceso del servidor BOGOTA a equipos MEDELLIN

➢ Acceso del WS 1 BOGOTA a equipos CALI

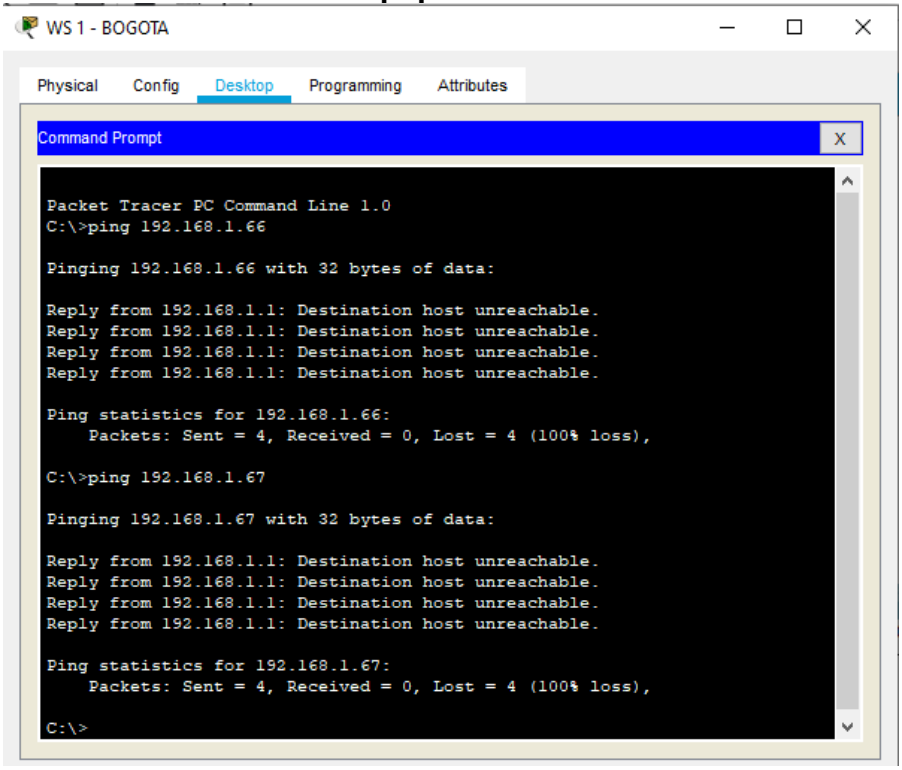

Figura 28: Acceso del WS 1 BOGOTA a equipos CALI

➢ Acceso del WS 1 BOGOTA a equipos MEDELLIN

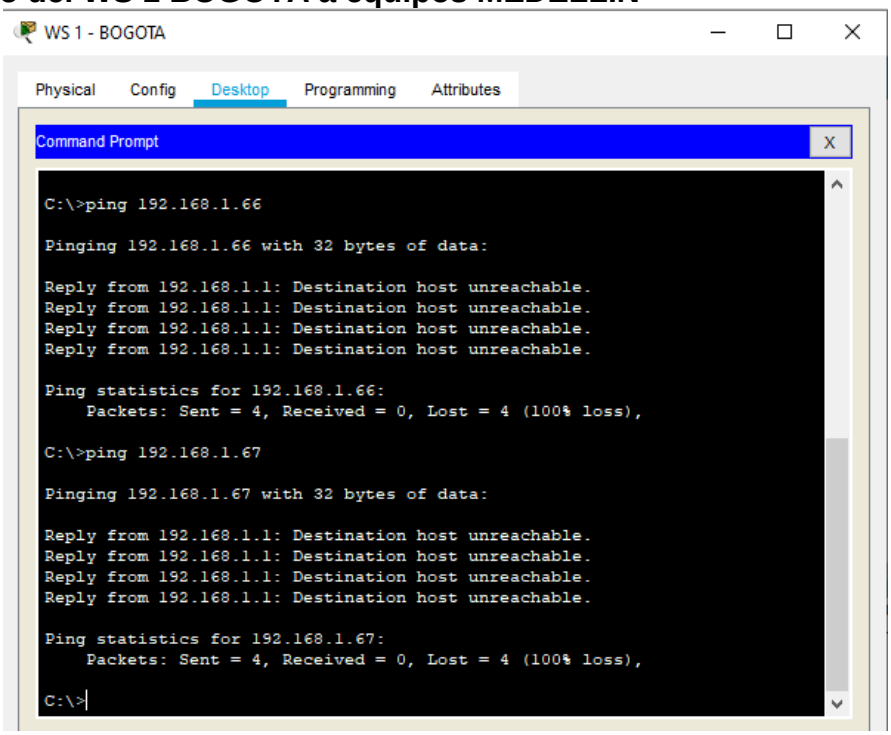

Figura 29: Acceso del WS 1 BOGOTA a equipos MEDELLIN

b. 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.

- **Configuración ACL Router BOGOTA**

```
Unauthorized access is strictly prohibited.
User Access Verification
Password:
BOGOTA>en
Password:
BOGOTA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 host
192.168.1.1
BOGOTA(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 host
192.168.1.98
BOGOTA(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 host
192.168.1.130
BOGOTA(config)#access-list 101 permit ip host 192.168.1.20 192.168.1.32
0.0.0.255
BOGOTA(config)#access-list 101 permit ip host 192.168.1.20 192.168.1.64
0.0.0.255
BOGOTA(config)#access-list 101 deny ip any any
BOGOTA(config)#int g0/0
BOGOTA(config-if)#ip access-group 101 in
BOGOTA(config-if)#exit
BOGOTA(config)#
```

- **Configuración ACL Router MEDELLIN**

```
Unauthorized access is strictly prohibited.
User Access Verification
Password:
MEDELLIN>en
Password:
MEDELLIN#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#access-list 100 permit ip 192.168.1.32 0.0.0.255 host
192.168.1.33
```

MEDELLIN(config)#access-list 100 permit ip 192.168.1.32 0.0.0.255 host 192.168.1.97
MEDELLIN(config)#access-list 100 permit ip 192.168.1.32 0.0.0.255 host 192.168.1.130
MEDELLIN(config)#access-list 100 permit ip 192.168.1.32 0.0.0.255 host 192.168.1.20
MEDELLIN(config)#access-list 100 deny ip any any
MEDELLIN(config)#int g0/0
MEDELLIN(config-if)#ip access-group 100 in
MEDELLIN(config-if)#exit
MEDELLIN(config)#

- **Configuración ACL Router CALI**

Unauthorized access is strictly prohibited.
User Access Verification
Password:
CALI>en
Password:
CALI#config t
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#access-list 102 permit ip 192.168.1.64 0.0.0.255 host 192.168.1.65
CALI(config)#access-list 102 permit ip 192.168.1.64 0.0.0.255 host 192.168.1.129
CALI(config)#access-list 102 permit ip 192.168.1.64 0.0.0.255 host 192.168.1.98
CALI(config)#access-list 102 permit ip 192.168.1.64 0.0.0.255 host 192.168.1.20
CALI(config)#access-list 102 deny ip any any
CALI(config)#int g0/0
CALI(config-if)#ip access-group 102 in
CALI(config-if)#exit
CALI(config)#

- **PING PC1 MEDELLIN –-> SERVER BOGOTA**
- **PING PC1 MEDELLIN –-> SW1 BOGOTA**

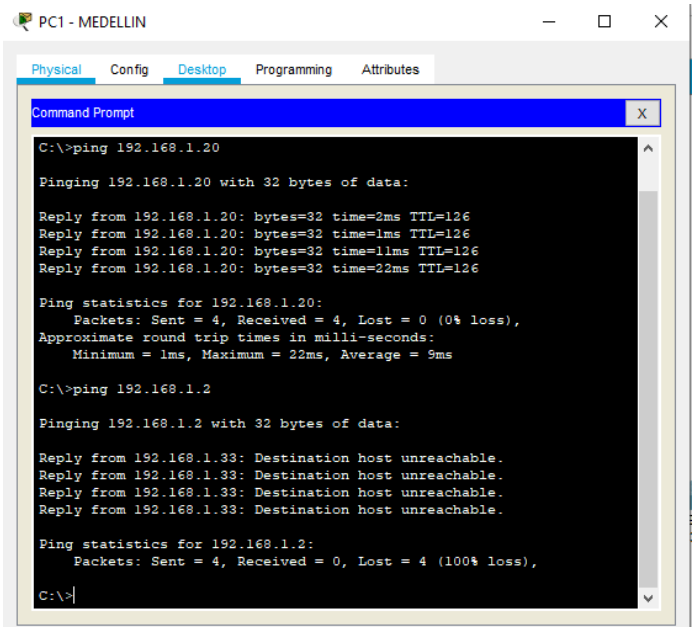

Figura 30: PING PC1 MEDELLIN →SERVIDOR, SW1 BOGOTA

- **PING PC1 CALI –-> SERVER BOGOTA**
- **PING PC1 CALI –-> PC2 MEDELLIN**

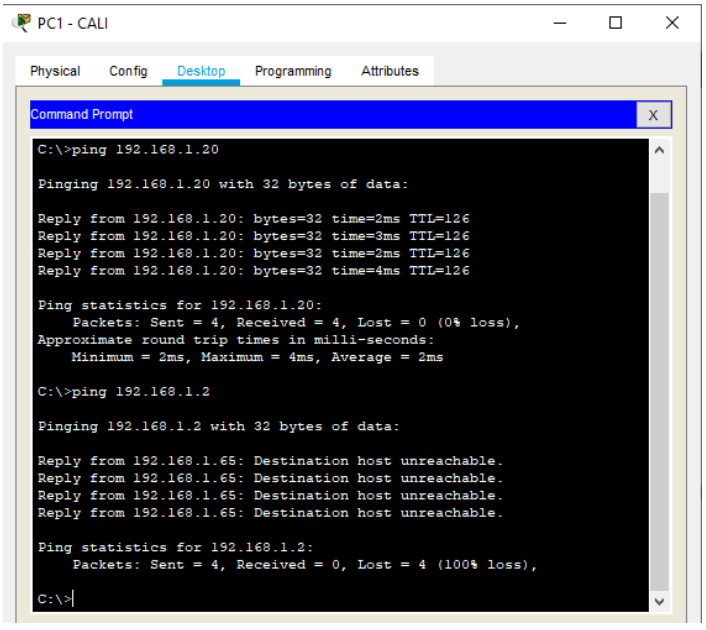

Figura 31: PING PC1 CALI → SERVIDOR BOGOTA → PC2 MEDELLIN

Parte 5: Comprobación de la red instalada.

a. Se debe probar que la configuración de las listas de acceso fue exitosa.
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	OK
	WS_1	Router BOGOTA	NULL
	Servidor	Router CALI	OK
	Servidor	Router MEDELLIN	OK
TELNET	LAN del Router MEDELLIN	Router CALI	OK
	LAN del Router CALI	Router CALI	OK
	LAN del Router MEDELLIN	Router MEDELLIN	OK
	LAN del Router CALI	Router MEDELLIN	OK
PING	LAN del Router CALI	WS_1	NULL
	LAN del Router MEDELLIN	WS_1	NULL
	LAN del Router MEDELLIN	LAN del Router CALI	OK
PING	LAN del Router CALI	Servidor	OK
	LAN del Router MEDELLIN	Servidor	OK
	Servidor	LAN del Router MEDELLIN	OK
	Servidor	LAN del Router CALI	OK
	Router CALI	LAN del Router MEDELLIN	OK
	Router MEDELLIN	LAN del Router CALI	OK

Tabla 6. Condiciones de prueba

- **TELNET**
  - ✓ **Router MEDELLIN → Router CALI**

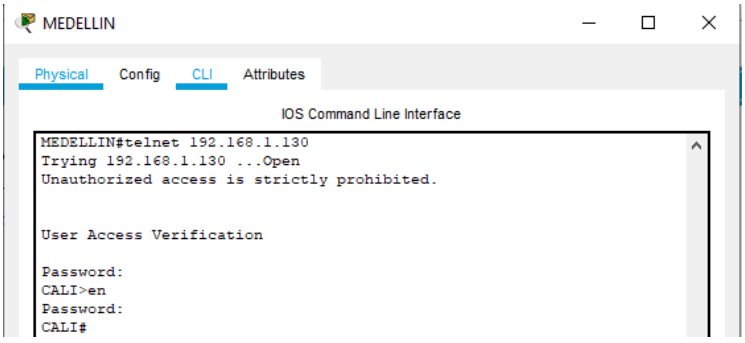

Figura 32: TELNET Router MEDELLIN → Router CALI

✓ WS_1 → Router BOGOTA

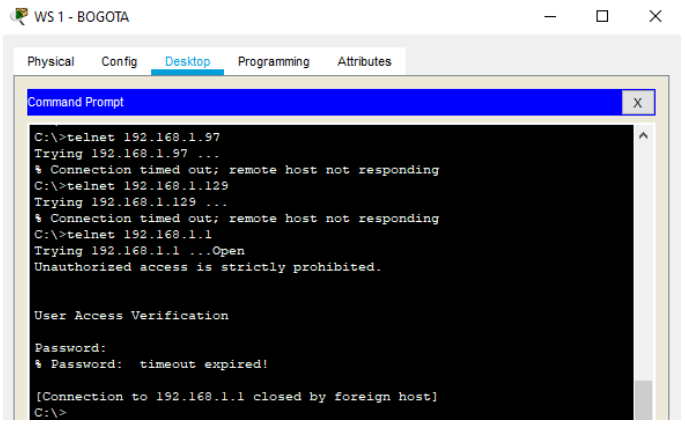

Figura 33: TELNET WS_1 → Router BOGOTA

✓ SERVIDOR → Router CALI

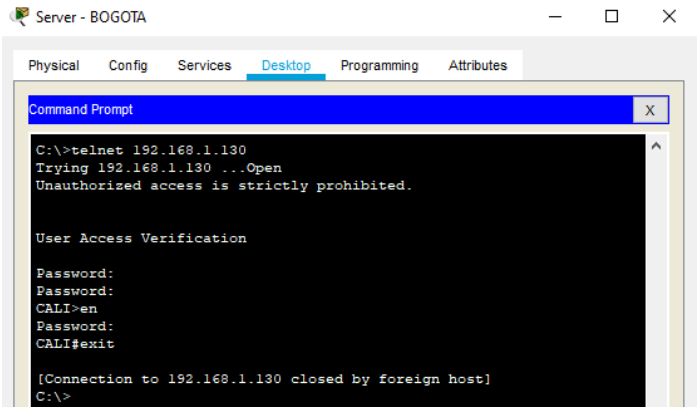

Figura 34: TELNET SERVIDOR → Router CALI

✓ SERVIDOR → Router MEDELLIN

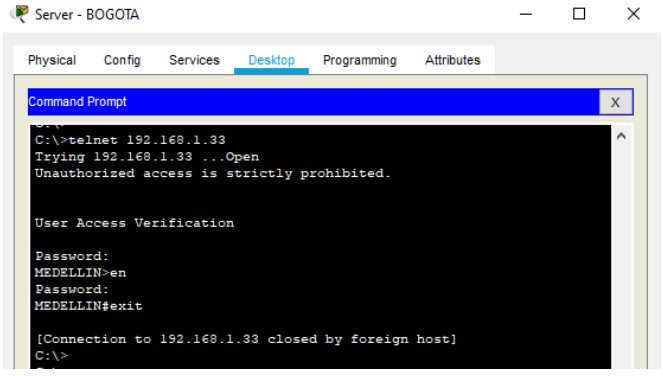

Figura 35: TELNET SERVIDOR → Router MEDELLIN

- **TELNET LAN**
  - ✓ **LAN del Router MEDELLIN → Router CALI**

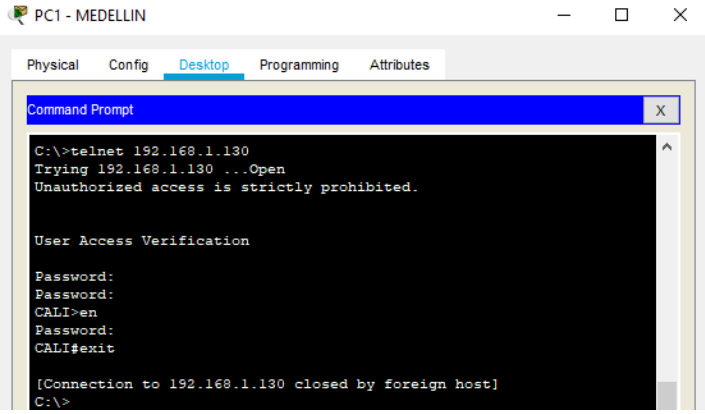

Figura 36: TELNET LAN del Router MEDELLIN → Router CALI

  - ✓ **LAN del Router CALI → Router CALI**

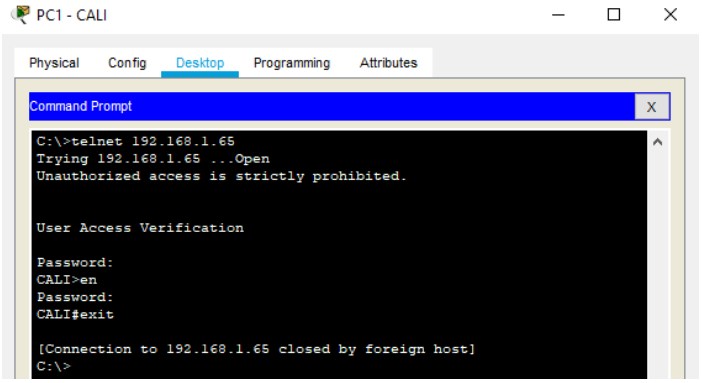

Figura 37: TELNET LAN del Router CALI → Router CALI

  - ✓ **LAN del Router MEDELLIN → Router MEDELLIN**

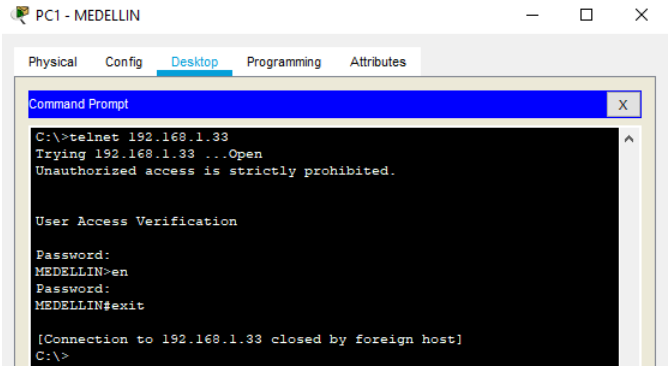

Figura 38: TELNET LAN del Router MEDELLIN → Router MEDELLIN

✓ **LAN del Router CALI → Router MEDELLIN**

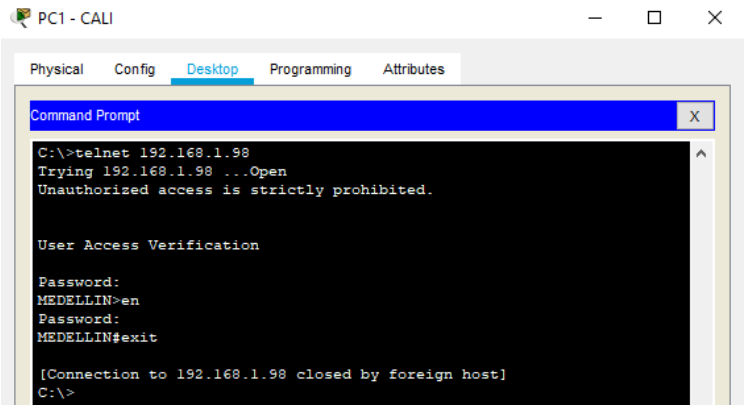

Figura 39: TELNET LAN del Router CALI → Router MEDELLIN

- **PING**

✓ **LAN del Router CALI → WS_1**

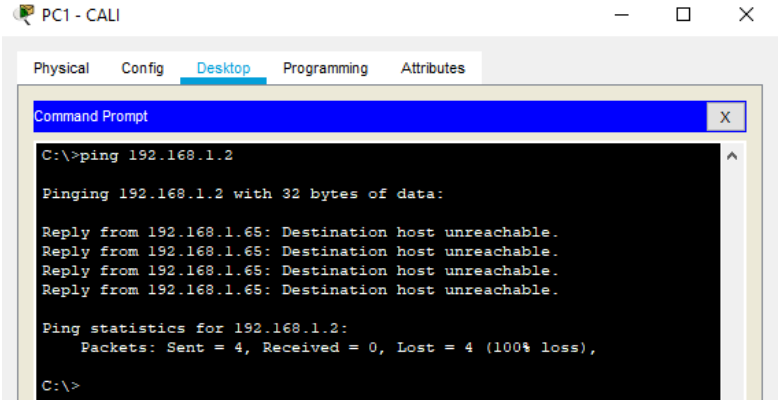

Figura 40: PING LAN del Router CALI → WS_1

✓ **LAN del Router MEDELLIN → WS_1**

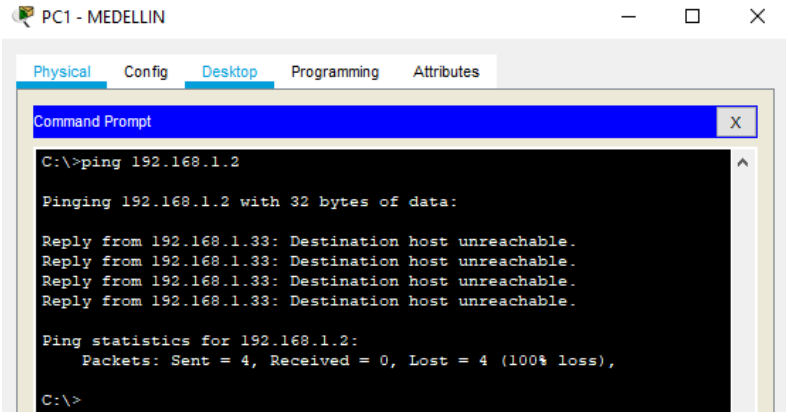

Figura 41: PING LAN del Router MEDELLIN → WS_1

✓ **LAN del Router MEDELLIN → LAN del Outer CALI**

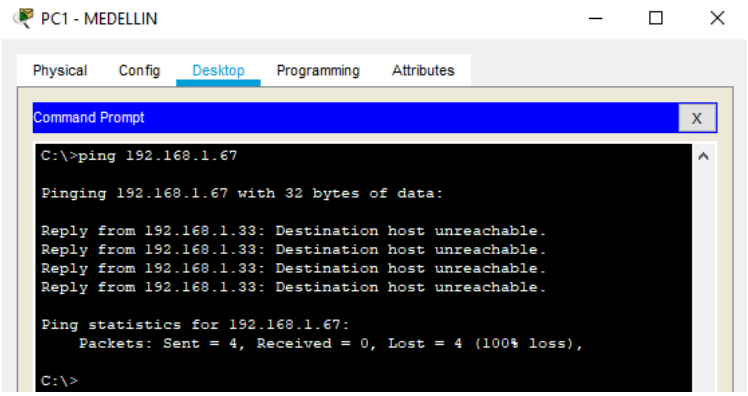

Figura 42: PING LAN del Router MEDELLIN → LAN del Outer CALI

- **PING**

✓ **LAN del Router CALI → SERVIDOR**

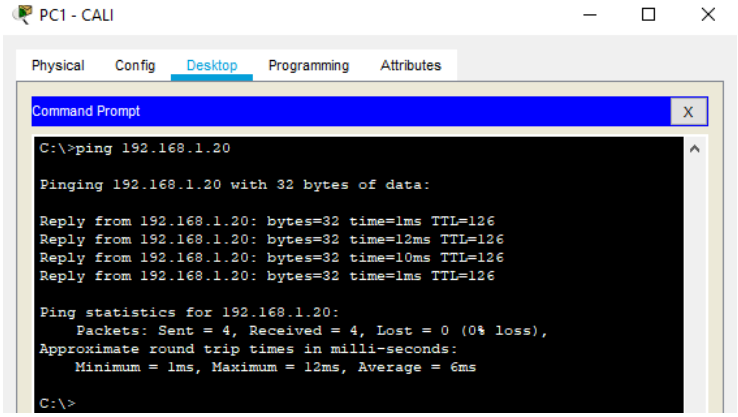

Figura 43: PING LAN del Router CALI → SERVIDOR

✓ **LAN del Router MEDELLIN → SERVIDOR**

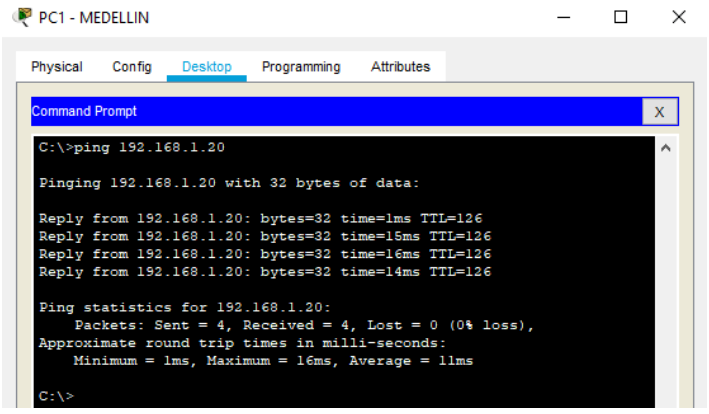

Figura 44: PING LAN del Router MEDELLIN → SERVIDOR

✓ SERVIDOR → LAN del Router MEDELLIN

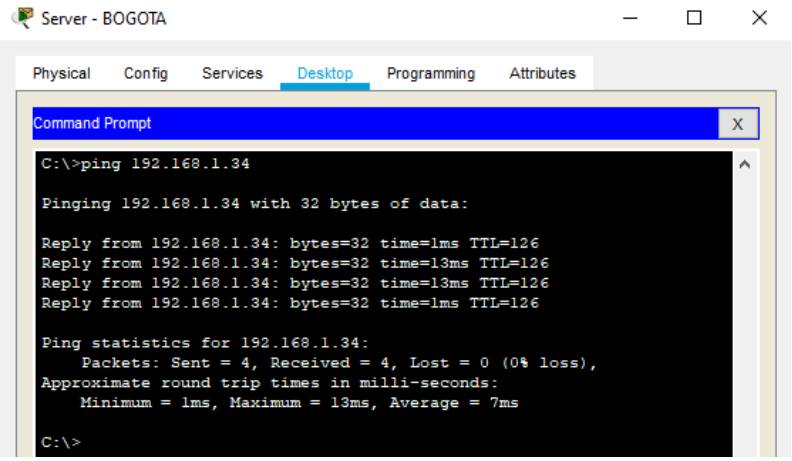

Figura 45: PING SERVIDOR → LAN del Router MEDELLIN

✓ SERVIDOR → LAN del Router CALI

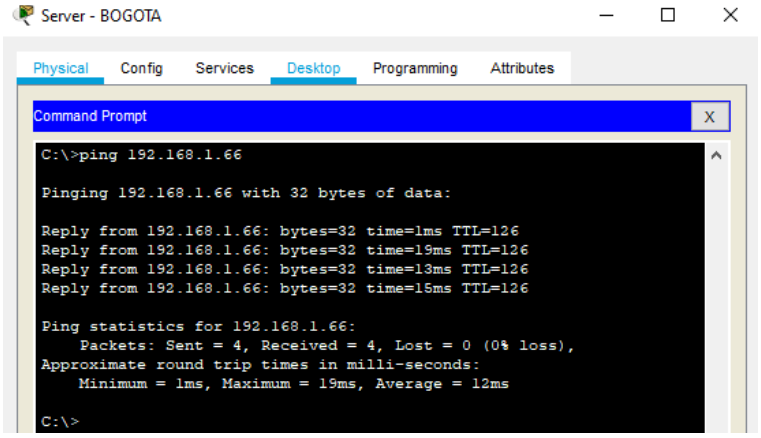

Figura 46: PING SERVIDOR → LAN del Router CALI

✓ Router CALI → LAN del Router MEDELLIN

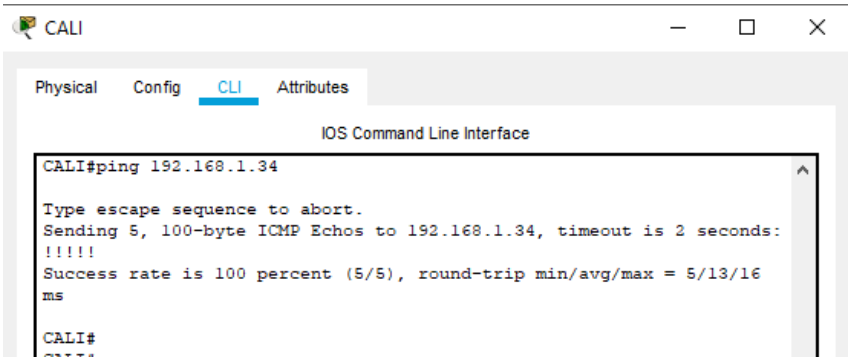

Figura 47: PING Router CALI → LAN del Router MEDELLIN

✓ **Router MEDELLIN → LAN del Router CALI**

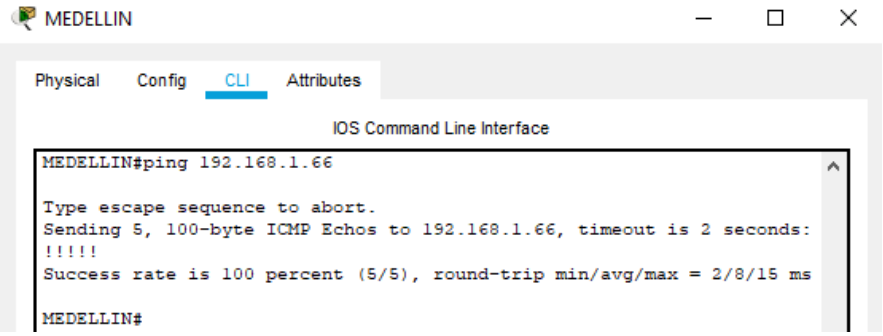

Figura 48: PING Router MEDELLIN → LAN del Router CALI

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 49: Escenario 2

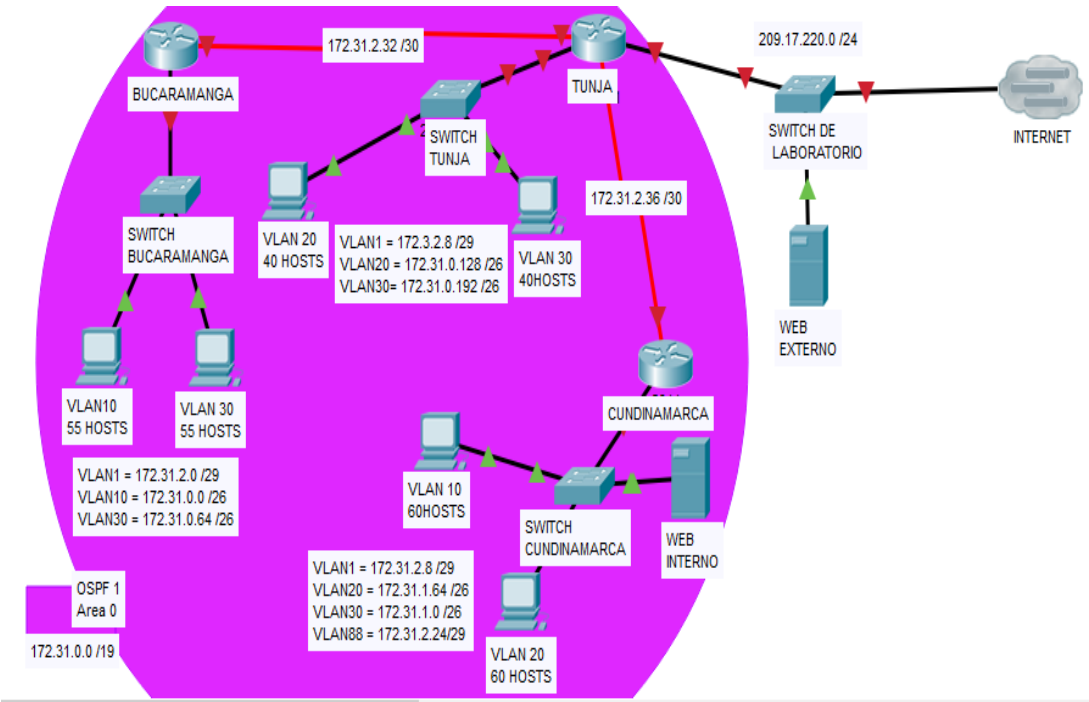

Figura 49: Escenario 2

Desarrollo

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:
   - Configuración básica.

     ✓ **TUNJA**

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname TUNJA
TUNJA(config)#enable secret class
TUNJA(config)#banner motd #
Enter TEXT message. End with the character '#'.
Unauthorized access is strictly prohibited. #
TUNJA(config)#line con 0
TUNJA(config-line)#password cisco
TUNJA(config-line)#login
TUNJA(config-line)#logging synchronous
TUNJA(config-line)#line vty 0 4
TUNJA(config-line)#password cisco
TUNJA(config-line)#login
TUNJA(config-line)#exit
TUNJA(config)#service password-encryption
TUNJA(config)# exit

TUNJA#

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

TUNJA#
```

     ✓ **BUCARAMANGA**

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BUCARAMANGA
BUCARAMANGA(config)#enable secret class
BUCARAMANGA(config)#banner motd #
Enter TEXT message. End with the character '#'.
Unauthorized access is strictly prohibited. #
BUCARAMANGA(config)#line con 0
BUCARAMANGA(config-line)#password cisco
```

```
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#logging synchronous
BUCARAMANGA(config-line)#line vty 0 4
BUCARAMANGA(config-line)#password cisco
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#service password-encryption
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#
```

- ✓ **CUNDINAMARCA**

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CUNDINAMARCA
CUNDINAMARCA(config)#enable secret class
CUNDINAMARCA(config)#banner motd #
Enter TEXT message. End with the character '#'.
Unauthorized access is strictly prohibited. #
CUNDINAMARCA(config)#line con 0
CUNDINAMARCA(config-line)#password cisco
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#logging synchronous
CUNDINAMARCA(config-line)#line vty 0 4
CUNDINAMARCA(config-line)#password cisco
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#exit
CUNDINAMARCA(config)#service password-encryption
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
CUNDINAMARCA#
```

- Autenticación local con AAA.

  - ✓ **TUNJA**

```
TUNJA#config t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#aaa new-model
TUNJA(config)#username cisco secret unad
```

TUNJA(config)#aaa authentication login default local
TUNJA(config)#aaa authentication login default enable
TUNJA(config)#enable secret cisco
TUNJA(config)#aaa authentication login console local
TUNJA(config)#line console 0
TUNJA(config-line)#login authentication console
TUNJA(config-line)#exit
TUNJA(config)#aaa authentication login vty local
TUNJA(config)#line vty 0 4
TUNJA(config-line)#password class
TUNJA(config-line)#login authentication vty
TUNJA(config-line)#end
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
TUNJA#

- ✓ **BUCARAMANGA**

BUCARAMANGA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#username cisco secret unad
BUCARAMANGA(config)#aaa authentication login default local
BUCARAMANGA(config)#aaa authentication login default enable
BUCARAMANGA(config)#enable secret cisco
BUCARAMANGA(config)#aaa authentication login console local
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#login authentication console
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#aaa authentication login vty local
BUCARAMANGA(config)#line vty 0 4
BUCARAMANGA(config-line)#password class
BUCARAMANGA(config-line)#login authentication vty
BUCARAMANGA(config-line)#end
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#

- ✓ **CUNDINAMARCA**

CUNDINAMARCA#config t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#username cisco secret unad

CUNDINAMARCA(config)#aaa authentication login default local
CUNDINAMARCA(config)#aaa authentication login default enable
CUNDINAMARCA(config)#enable secret cisco
CUNDINAMARCA(config)#aaa authentication login console local
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#login authentication console
CUNDINAMARCA(config-line)#exit
CUNDINAMARCA(config)#aaa authentication login vty local
CUNDINAMARCA(config)#line vty 0 4
CUNDINAMARCA(config-line)#password class
CUNDINAMARCA(config-line)#login authentication vty
CUNDINAMARCA(config-line)#end
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
CUNDINAMARCA#

- Cifrado de contraseñas.
  - ✓ Se realizo en la configuración Básica de cada router
- Un máximo de internos para acceder al router.
  - ✓ **TUNJA**

TUNJA#config t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#ip domain name DOMAIN.TUNJA
TUNJA(config)#crypto key generate rsa
The name for the keys will be: TUNJA.DOMAIN.TUNJA
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
TUNJA(config)#ip ssh authentication-retries 3
*mar. 1 4:59:16.734: %SSH-5-ENABLED: SSH 1.99 has been enabled
TUNJA(config)#ip ssh time-out 120
TUNJA(config)#line vty 0 15
TUNJA(config-line)#transport input ssh
TUNJA(config-line)#exit
TUNJA(config)#

- ✓ **BUCARAMANGA**

```
BUCARAMANGA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#ip domain name
DOMAIN.BUCARAMANGA
BUCARAMANGA(config)#crypto key generate rsa
The name for the keys will be:
BUCARAMANGA.DOMAIN.BUCARAMANGA
Choose the size of the key modulus in the range of 360 to 2048 for
your
General Purpose Keys. Choosing a key modulus greater than 512
may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
BUCARAMANGA(config)#ip ssh authentication-retries 3
*mar. 1 3:37:1.177: %SSH-5-ENABLED: SSH 1.99 has been
enabled
BUCARAMANGA(config)#ip ssh time-out 120
BUCARAMANGA(config)#line vty 0 15
BUCARAMANGA(config-line)#transport input ssh
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#
```

- ✓ **CUNDINAMARCA**

```
CUNDINAMARCA#config t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#ip domain name
DOMAIN.CUNDINAMARCA
CUNDINAMARCA(config)#crypto key generate rsa
The name for the keys will be:
CUNDINAMARCA.DOMAIN.CUNDINAMARCA
Choose the size of the key modulus in the range of 360 to 2048 for
your
General Purpose Keys. Choosing a key modulus greater than 512
may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
CUNDINAMARCA(config)#ip ssh authentication-retries 3
*mar. 1 5:3:0.188: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

```
CUNDINAMARCA(config)#ip ssh time-out 120
CUNDINAMARCA(config)#line vty 0 15
CUNDINAMARCA(config-line)#transport input ssh
CUNDINAMARCA(config-line)#exit
CUNDINAMARCA(config)#
```

- Máximo tiempo de acceso al detectar ataques.
  - ✓ **TUNJA**

```
TUNJA#config t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#banner motd #Acceso solo para personal
autorizado#
TUNJA(config)#login block-for 10 attempts 2 within 60
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
TUNJA#
```

  - ✓ **BUCARAMANGA**

```
BUCARAMANGA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#banner motd #Acceso solo para personal
autorizado#
BUCARAMANGA(config)#login block-for 10 attempts 2 within 60
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#
```

  - ✓ **CUNDINAMARCA**

```
CUNDINAMARCA#config t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#banner motd #Acceso solo para personal
autorizado#
CUNDINAMARCA(config)#login block-for 10 attempts 2 within 60
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
```

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

- Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.

❖ **ASIGNARCION DE IP A CADA INTERFAZ DEL ROUTER**

✓ **TUNJA**

TUNJA#config t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#int s0/0/0
TUNJA(config-if)#ip address 172.31.2.34 255.255.255.252
TUNJA(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
TUNJA(config-if)#exit
TUNJA(config)#int s0/0/1
TUNJA(config-if)#ip address 172.31.2.38 255.255.255.252
TUNJA(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
TUNJA(config-if)#exit
TUNJA(config)#int g0/0
TUNJA(config-if)#ip address 172.3.2.9 255.255.255.248
TUNJA(config-if)#no shut
TUNJA(config-if)#exit
TUNJA(config)#int g0/1
TUNJA(config-if)#ip address 209.17.220.1 255.255.255.0
TUNJA(config-if)#no shut
TUNJA(config-if)#exit
TUNJA(config)#copy running-config startup-config
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
TUNJA(config)#copy running-config startup-config
^
% Invalid input detected at '^' marker.
TUNJA(config)#exit
TUNJA#

%SYS-5-CONFIG_I: Configured from console by console
TUNJA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
TUNJA#

- ✓ **BUCARAMANGA**

BUCARAMANGA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#int s0/0/0
BUCARAMANGA(config-if)#ip address 172.31.2.33 255.255.255.252
BUCARAMANGA(config-if)#no shut
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#int g0/0
BUCARAMANGA(config-if)#ip address 172.31.2.1 255.255.255.248
BUCARAMANGA(config-if)#no shut
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#exit
BUCARAMANGA#copy running-config startup-config
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
BUCARAMANGA#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
BUCARAMANGA#

- ✓ **CUNDINAMARCA**

CUNDINAMARCA#config t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#int s0/0/1

CUNDINAMARCA(config-if)#ip address 172.31.2.37
255.255.255.252
CUNDINAMARCA(config-if)#no shut
CUNDINAMARCA(config-if)#int g0/0
CUNDINAMARCA(config-if)#ip address 172.31.2.9 255.255.255.248
CUNDINAMARCA(config-if)#no shut
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#exit
CUNDINAMARCA#copy running-config startup-config
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
%SYS-5-CONFIG_I: Configured from console by console
CUNDINAMARCA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CUNDINAMARCA#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up
CUNDINAMARCA#

- **Establezca un servidor TFTP**

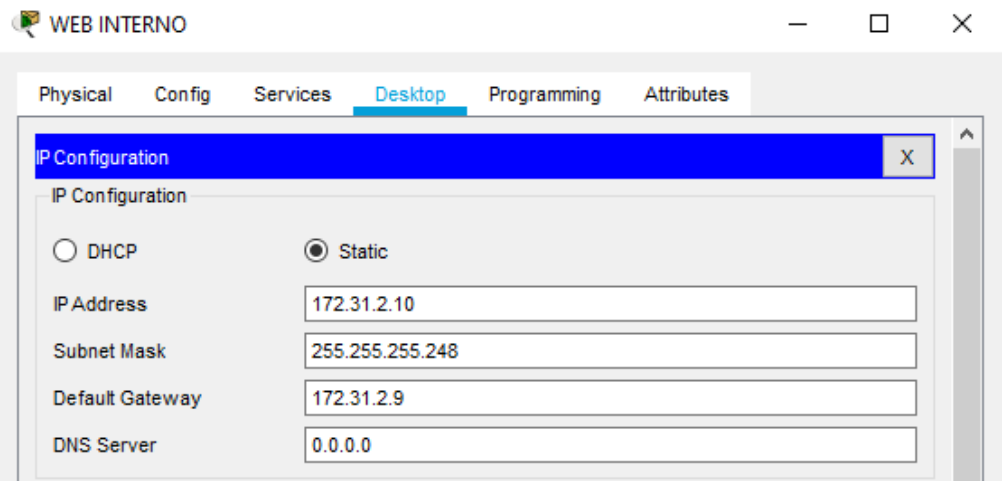

Figura 50: Establezca un servidor TFTP

- ✓ **Configuración Router CUNDINAMARCA**

```
CUNDINAMARCA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CUNDINAMARCA#copy startup-config tftp
Address or name of remote host []? 172.31.2.10
Destination filename [CUNDINAMARCA-confg]?
Writing startup-config....!!
[OK - 1535 bytes]
1535 bytes copied in 3 secs (511 bytes/sec)
CUNDINAMARCA#config t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#ip route 172.31.2.32 255.255.255.252
172.31.2.38
CUNDINAMARCA(config)#
```

- ✓ **Configuración Router TUNJA**

```
TUNJA#config t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#ip route 172.31.2.10 255.255.255.254 172.31.2.37
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
TUNJA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
TUNJA#copy startup-config tftp
Address or name of remote host []? 172.31.2.10
Destination filename [TUNJA-confg]?
Writing startup-config...!!
[OK - 1619 bytes]
1619 bytes copied in 0.002 secs (809500 bytes/sec)
TUNJA#
```

- ✓ **Configuración Router BUCARAMANGA**

```
BUCARAMANGA#config t
Enter configuration commands, one per line. End with CNTL/Z.
```

```
BUCARAMANGA(config)#ip route 172.31.2.36 255.255.255.254
172.31.2.34
BUCARAMANGA(config)#ip route 172.31.2.10 255.255.255.254
172.31.2.37
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
BUCARAMANGA#copy startup-config tftp
Address or name of remote host []? 172.31.2.10
Destination filename [BUCARAMANGA-confg]?
Writing startup-config...!!
[OK - 1646 bytes]
1646 bytes copied in 0.01 secs (164600 bytes/sec)
BUCARAMANGA#
```

- VERIFICACION DEL FUNCIONAMIENTO DE TFTP CON EL PROCESO REALIZADO

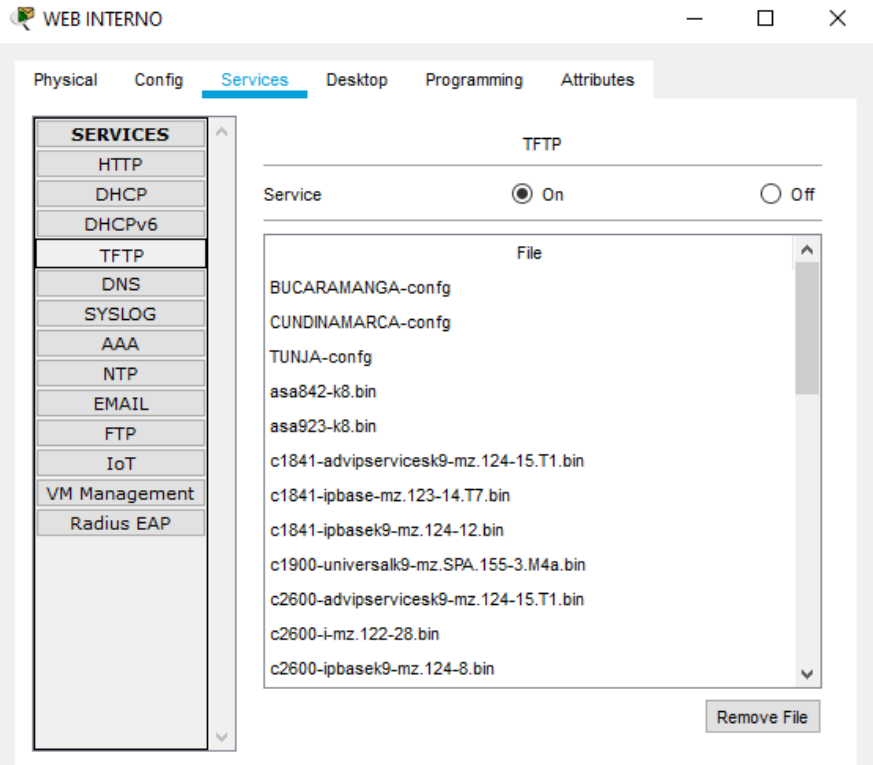

Figura 51: VERIFICACION DEL FUNCIONAMIENTO DE TFTP

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

.

- **Configuración de VLAN en swich**
  - ✓ **BUCARAMANGA**

```
SW_BUCARAMANGA#EN
SW_BUCARAMANGA#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW_BUCARAMANGA(config)#int f0/1
SW_BUCARAMANGA(config-if)#switchport mode trunk
SW_BUCARAMANGA(config-if)#exit
SW_BUCARAMANGA(config)#int f0/2
SW_BUCARAMANGA(config-if)#switchport mode access
SW_BUCARAMANGA(config-if)#switchport access vlan 10
SW_BUCARAMANGA(config-if)#exit
SW_BUCARAMANGA(config)#int f0/3
SW_BUCARAMANGA(config-if)#switchport mode access
SW_BUCARAMANGA(config-if)#switchport access vlan 30
SW_BUCARAMANGA(config-if)#END
SW_BUCARAMANGA#
```

  - ✓ **CUNDINAMARCA**

```
SW_CUNDINAMARCA#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW_CUNDINAMARCA(config)#int f0/1
SW_CUNDINAMARCA(config-if)#switchport mode trunk

SW_CUNDINAMARCA(config-if)#exit
SW_CUNDINAMARCA(config)#int f0/2
SW_CUNDINAMARCA(config-if)#switchport mode access
SW_CUNDINAMARCA(config-if)#switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
SW_CUNDINAMARCA(config-if)#exit
SW_CUNDINAMARCA(config)#int f0/3
SW_CUNDINAMARCA(config-if)#switchport mode access
SW_CUNDINAMARCA(config-if)#switchport access vlan 20
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

% Access VLAN does not exist. Creating vlan 20
SW_CUNDINAMARCA(config-if)#end
SW_CUNDINAMARCA#

- **Creación del HERPER ADDRESS EN LOS ROUTER**

  - ✓ **BUCARAMANGA**

```
BUCARAMANGA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#int g0/0
BUCARAMANGA(config-if)#ip helper-address 172.31.2.34
BUCARAMANGA(config-if)#int g0/0.10
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
BUCARAMANGA(config-subif)#int g0/0.30
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.34
BUCARAMANGA(config-subif)#exit
BUCARAMANGA(config)#int g0/0.10
BUCARAMANGA(config-subif)#encapsulation dot1q 10
BUCARAMANGA(config-subif)#ip address 172.31.0.1
255.255.255.248
BUCARAMANGA(config-subif)#int g0/0.30
BUCARAMANGA(config-subif)#encapsulation dot1q 30
BUCARAMANGA(config-subif)#ip address 172.31.0.65
255.255.255.248
%LINK-5-CHANGED: Interface GigabitEthernet0/0.10, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.10, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.30, changed state to up

BUCARAMANGA(config-subif)#ip address 172.31.0.65
255.255.255.248
BUCARAMANGA(config-subif)#exit
```

BUCARAMANGA(config)#

- ✓ **CUNDINAMARCA**

CUNDINAMARCA#config t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#int g0/0
CUNDINAMARCA(config-if)#ip helper-address 172.31.2.38
CUNDINAMARCA(config-if)#int g0/0.20
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.38
CUNDINAMARCA(config-subif)#int g0/0.30
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.38
CUNDINAMARCA(config-subif)#int g0/0.88
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.38
CUNDINAMARCA(config-subif)#exit
CUNDINAMARCA(config)#int g0/0.20
CUNDINAMARCA(config-subif)#encapsulation dot1q 20
CUNDINAMARCA(config-subif)#ip address 172.31.1.65
255.255.255.192
CUNDINAMARCA(config-subif)#int g0/0.30
CUNDINAMARCA(config-subif)#encapsulation dot1q 30
CUNDINAMARCA(config-subif)#ip address 172.31.1.1
255.255.255.192
CUNDINAMARCA(config-subif)#int g0/0.88
CUNDINAMARCA(config-subif)#encapsulation dot1q 88
CUNDINAMARCA(config-subif)#ip address 172.31.2.25
255.255.255.248
%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed state to up

%LINK-5-CHANGED: Interface GigabitEthernet0/0.88, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.88, changed state to up

CUNDINAMARCA(config-subif)#ip address 172.31.2.25
255.255.255.248
CUNDINAMARCA(config-subif)#end
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console

CUNDINAMARCA#

- **CREACION DEL DHCP**

  - ✓ **TUNJA**

    TUNJA#config t
    Enter configuration commands, one per line. End with CNTL/Z.
    TUNJA(config)#ip dhcp pool VLAN10
    TUNJA(dhcp-config)#network 172.31.0.0 255.255.255.248
    TUNJA(dhcp-config)#default-router 172.31.2.1
    TUNJA(dhcp-config)#exit
    TUNJA(config)#ip dhcp pool VLAN30
    TUNJA(dhcp-config)#network 172.31.0.64 255.255.255.248
    TUNJA(dhcp-config)#default-router 172.31.2.1
    TUNJA(dhcp-config)#exit
    TUNJA(config)#ip dhcp pool VLAN30_2
    TUNJA(dhcp-config)#network 172.31.1.0 255.255.255.192
    TUNJA(dhcp-config)#default-router 172.31.2.9
    TUNJA(dhcp-config)#exit
    TUNJA(config)#ip route 172.31.0.0 255.255.255.0 172.31.2.33
    TUNJA(config)#ip route 172.31.0.64 255.255.255.248 172.31.2.33
    TUNJA(config)#exit
    TUNJA#
    %SYS-5-CONFIG_I: Configured from console by console

    TUNJA#config t
    Enter configuration commands, one per line. End with CNTL/Z.
    TUNJA(config)#ip dhcp pool VLAN20
    TUNJA(dhcp-config)#network 172.31.1.64 255.255.255.192
    TUNJA(dhcp-config)#default-router 172.31.2.9
    TUNJA(dhcp-config)#exit
    TUNJA(config)#ip route 172.31.1.0 255.255.255.0 172.31.2.37
    TUNJA(config)#ip route 172.31.1.64 255.255.255.248 172.31.2.37
    TUNJA(config)#

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

- ✓ **Router TUNJA**

```
TUNJA#config t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#access-list 1 permit 172.31.2.0 0.0.0.255
TUNJA(config)#access-list 1 permit 172.31.0.0 0.0.0.255
TUNJA(config)#access-list 1 permit 172.31.0.64 0.0.0.255
TUNJA(config)#access-list 1 permit 172.31.0.128 0.0.0.255
TUNJA(config)#access-list 1 permit 172.31.0.192 0.0.0.255
TUNJA(config)#access-list 1 permit 172.31.1.64 0.0.0.255
TUNJA(config)#access-list 1 permit 172.31.1.0 0.0.0.255
TUNJA(config)#access-list 1 permit 172.31.2.9 0.0.0.255
TUNJA(config)#access-list 1 permit 172.3.2.9 0.0.0.255
TUNJA(config)#ip nat inside source list 1 int g0/1 overload
TUNJA(config)#
TUNJA(config)#int s0/0/0
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#int s0/0/1
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#int g0/1
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#exit
TUNJA(config)#router rip
TUNJA(config-router)#version 2
TUNJA(config-router)#network 172.31.2.0
TUNJA(config-router)#network 209.17.220.0
TUNJA(config-router)#exit
TUNJA(config)#
```

- ✓ **Router BUCARAMANGA**

```
BUCARAMANGA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#ip route 209.17.220.0 255.255.255.0
172.31.2.34
BUCARAMANGA(config)#ip route 172.31.1.0 255.255.255.192
172.31.2.37
BUCARAMANGA(config)#ip route 172.31.1.64 255.255.255.192
172.31.2.37
```

BUCARAMANGA(config)#

- ✓ **Router CUNDINAMARCA**

CUNDINAMARCA#config t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#ip route 209.17.220.0 255.255.255.0 172.31.2.38
CUNDINAMARCA(config)#ip route 172.31.0.64 255.255.255.192 172.31.2.33
CUNDINAMARCA(config)#ip route 172.31.0.0 255.255.255.192 172.31.2.33
CUNDINAMARCA(config)#

4. El enrutamiento deberá tener autenticación.

- ✓ **TUNJA**

TUNJA#config t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#router ospf 1
TUNJA(config-router)#network 172.31.2.32 0.0.0.255 area 1
TUNJA(config-router)#network 172.3.2.9 0.0.0.255 area 1
TUNJA(config-router)#network 172.31.2.26 0.0.0.255 area 1
TUNJA(config-router)#do wr
Building configuration...
[OK]
TUNJA(config-router)#

- ✓ BUCARAMANGA

BUCARAMANGA(config)#config t
BUCARAMANGA(config)#router ospf 1
BUCARAMANGA(config-router)#network 172.31.2.0 0.0.0.255 area 1
BUCARAMANGA(config-router)#network 172.31.2.32 0.0.0.255 area 1
BUCARAMANGA(config-router)#do wr
Building configuration...
[OK]
BUCARAMANGA(config-router)#exit
BUCARAMANGA(config)#

- ✓ CUNDINAMARCA

```
CUNDINAMARCA#config t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#router ospf 1
CUNDINAMARCA(config-router)#network 172.31.2.36 0.0.0.255
area 1
CUNDINAMARCA(config-router)#network 172.31.2.8 0.0.0.255 area
1
CUNDINAMARCA(config-router)#do wr
Building configuration...
[OK]
```

Aspectos a tener en cuenta

- Habilitar VLAN en cada switch y permitir su enrutamiento.
- Enrutamiento OSPF con autenticación en cada router.
- Servicio DHCP en el router Tunja, mediante el helper address, para los routers Bucaramanga y Cundinamarca.
- Configuración de NAT estático y de sobrecarga.
- Establecer una lista de control de acceso de acuerdo con los criterios señalados.
- Habilitar las opciones en puerto consola y terminal virtual

CONCLUSIONES

El aprendizaje desarrollado en el trabajo final del diplomado de Cisco no brinda muchos conocimientos respecto a las redes y telecomunicaciones donde nos prepara en el ámbito de que decisiones debemos de tomar al momento de diseñar y desarrollar una red como que configuraciones básicas y de seguridad debemos de tomar en los dispositivos que van hacer parte de la red

Al igual que en la realización de la practica nos fortaleció y en ella se demostró todo el conocimiento que se adquirió en el transcurso de diplomado de cisco como las diferentes configuraciones de NAT, PAT, DHCP, enrutamiento, ACL, OSPF entre otras que fueron necesarias en la realización del trabajo final.

BIBLIOGRAFÍA

Temática: Capa de Transporte

CISCO. (2014). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

Temática: Asignación de direcciones IP

CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

Temática: SubNetting

CISCO. (2014). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

Temática: Capa de Aplicación

CISCO. (2014). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

Temática: Soluciones de Red

CISCO. (2014). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

Temática: Conceptos de Routing

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

Temática: Enrutamiento entre VLANs

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

Temática: Enrutamiento Estático

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

Temática: Listas de control de acceso

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

Temática: DHCP

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1