

**PRUEBA DE HABILIDADES PRÁCTICAS CCNA**

**DANIEL SÁNCHEZ RESTREPO**

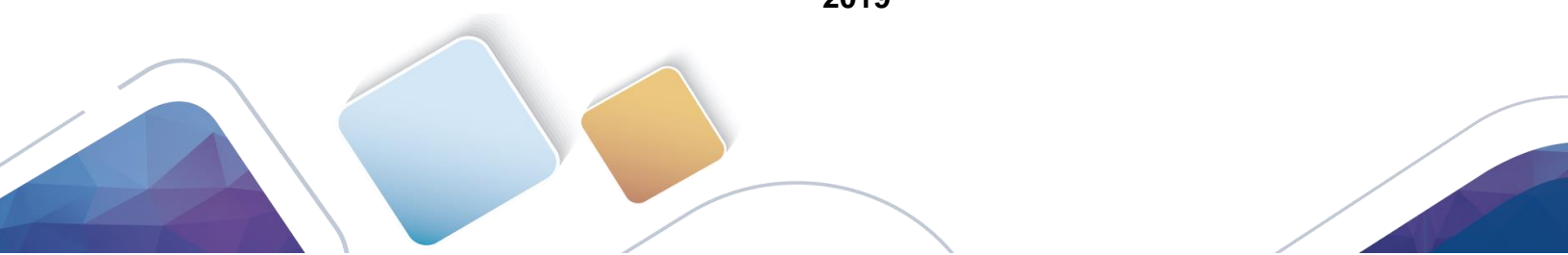
**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD**

**ECBTI**

**INGENIERÍA DE SISTEMAS**

**SANTA ROSA DE CABAL**

**2019**



## Tabla de Contenido

### Contenido

Tabla de Ilustraciones .....	3
Resumen .....	5
Abstract.....	6
Introducción.....	7
Objetivos .....	8
Desarrollo de los Escenarios .....	9
Escenario 1 .....	9
Escenario 2 .....	32
Conclusiones .....	48
Bibliografía .....	49



## Tabla de Ilustraciones

Ilustración 1: Topología escenario 1 .....	9
Ilustración 2: Topología escenario 1 .....	10
Ilustración 3: Topología escenario 1 sin configuración .....	11
Ilustración 4: Dirección ip PC-A y PC-B Medellín .....	13
Ilustración 5: Configuración General Router Medellín .....	13
Ilustración 6: Dirección IP WS1 y Servidor Bogotá.....	14
Ilustración 7: Configuración General Router Bogotá .....	14
Ilustración 8: Dirección IP PC-C y PC-D Cali.....	15
Ilustración 9: Configuración General Router Cali.....	15
Ilustración 10: Balanceo de Carga Router Bogotá .....	16
Ilustración 11: Balanceo de Carga Router Medellín .....	16
Ilustración 12: Balanceo de Carga Router Cali .....	17
Ilustración 13: Diagnóstico CDP .....	18
Ilustración 14: Conectividad tramo Medellín .....	18
Ilustración 15: Ping tramo Medellín.....	19
Ilustración 16: Conectividad tramo Bogotá .....	19
Ilustración 17: Ping tramo Bogotá .....	20
Ilustración 18: Conectividad tramo Cali .....	20
Ilustración 19: Ping tramo Cali .....	21
Ilustración 20: Protocolo EIGRP a todos los Routers .....	23
Ilustración 21: Vecindad entre Routers .....	24
Ilustración 22: Tablas de Enrutamiento .....	25
Ilustración 23: Conectividad Cali a Medellín.....	26
Ilustración 24: Conectividad Cali a Bogotá.....	26
Ilustración 25: Conexiones Telnet.....	27
Ilustración 26: Listas de Acceso Bogotá .....	28
Ilustración 27: Listas de Acceso Medellín .....	29
Ilustración 28: Ping entre Medellín y Cali .....	30
Ilustración 29: Topología Escenario 2 .....	32
Ilustración 30: Construcción Escenario 2.....	32
Ilustración 31: Configuración Básica Routers .....	34
Ilustración 32: Configuración AAA a todos los Routers .....	35
Ilustración 33: Cifrado de Contraseñas en los Routers.....	36
Ilustración 34: Máximo de Intentos para entrar a los Routers.....	37
Ilustración 35: Limitación al Detectar Ataques en los Routers.....	38
Ilustración 36: Archivos de seguridad de los Routers a TFTP .....	38
Ilustración 37: Configuración DHCP de los Routers .....	39



Ilustración 38: Configuración DHCP Switches.....	40
Ilustración 39: Asignación DHCP .....	41
Ilustración 40: Configuración NAT .....	41
Ilustración 41: Autenticación al enrutamiento de cada Router.....	42
Ilustración 42: Listas de Control de Acceso Cundinamarca .....	43
Ilustración 43: Listas de Control de Acceso Tunja.....	43
Ilustración 44: Listas de Control de Acceso Bucaramanga .....	44
Ilustración 45: IP's de VLAN distintas.....	44
Ilustración 46: No hay ping para otra VLAN.....	45
Ilustración 47: Acceso a los Router .....	45
Ilustración 48: Direccionamiento.....	46
Ilustración 49: Conexión de Toda la Red.....	47



## Resumen

A lo largo del Diplomado en redes Cisco se han visto temas que son de suma importancia para la carrera de ingeniería en Sistemas, desde la configuración básica de un router, computador, switch, etc. Hasta lo que implica la interconexión entre redes de una ciudad a otra, sean privadas o públicas.

Teniendo esto en cuenta, se presentan una serie de escenarios que ejemplifican con exactitud problemáticas o situaciones que se pueden presentar en espacios laborales y que deben solucionar con prontitud.



## Abstract

Throughout the Cisco's networks certification, we have seen topics that are of utmost importance for the Systems engineering career, from the basic configuration of a router, computer, switch, etc. Even what the interconnection between networks from one city to another implies, whether private or public.

Taking this into account, a series of scenarios are presented that accurately exemplify problems or situations that may arise in work spaces and that must be resolved promptly.



## Introducción

El presente documento contiene los objetivos de la prueba de habilidades para el diplomado en redes Cisco. Así mismo, contiene el desarrollo de los dos escenarios propuestos con sus respectivos lineamientos según la rúbrica de evaluación.

Se tratarán diversos temas que se vieron a lo largo del curso como la configuración básica de un router, conectividad a través del protocolo EIGRP, la configuración del DHCP en IPv4, entre otros. Se han adjuntado pantallazos de los resultados que cada proceso ha arrojado frente a las redes que se debieron crear desde cero, esto con el fin de poner pruebas gráficas del desarrollo de este.

El objetivo principal de este documento es el de documentar el último trabajo del curso, el cual refleja los conocimientos adquiridos a lo largo de esta jornada en la que se curso el diplomado en la academia Cisco.

La importancia de las temáticas vistas en el diplomado radica en todos los aspectos de la carrera de ingeniería en sistemas, se centra en la obtención de un diseño eficiente de una red telemática que pueda ser la solución a una problemática o problemáticas de una entidad, empresa, cliente determinado, etc.



## Objetivos

- Desarrollar los dos escenarios propuestos aplicando los conocimientos adquiridos durante el curso.
- Cumplir a cabalidad la rúbrica de evaluación para el último trabajo práctico del diplomado de redes CISCO.
- Apropiar los conceptos estudiados en la duración del curso.





## Desarrollo de los Escenarios

### 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.

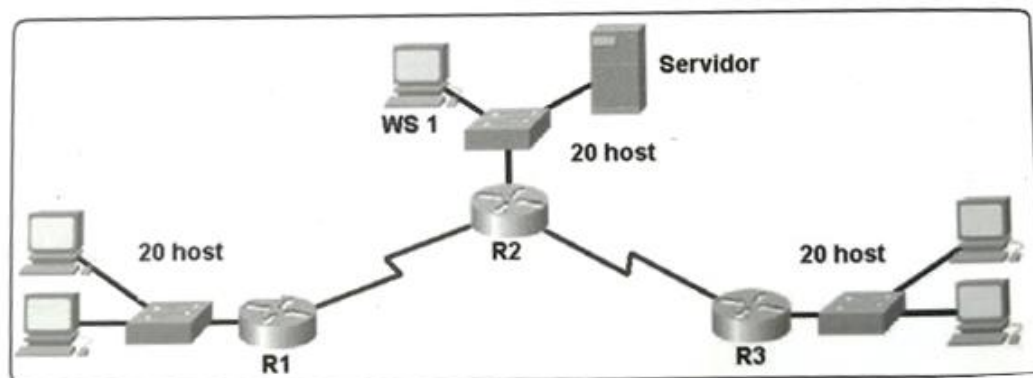


Ilustración 1: Topología escenario 1

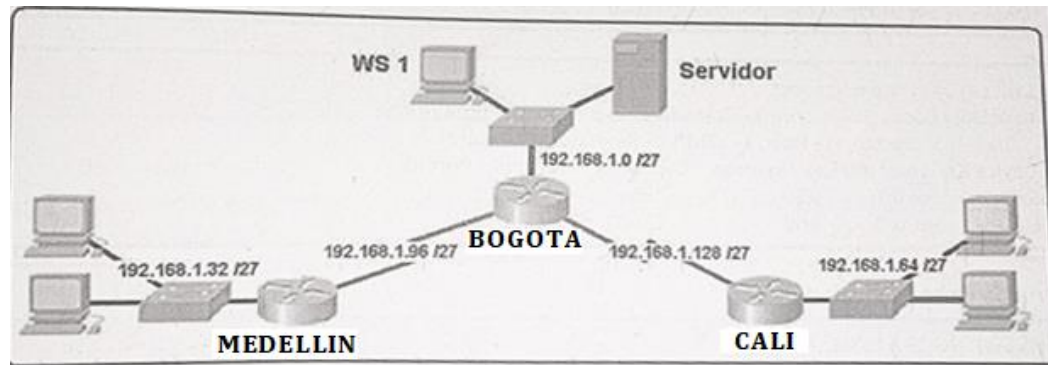


Ilustración 2: Topología escenario 1

## Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).
- Realizar la conexión física de los equipos con base en la topología de red

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



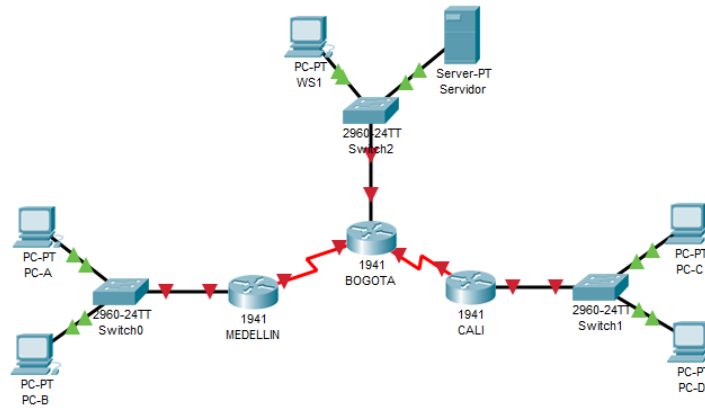


Ilustración 3: Topología escenario 1 sin configuración

**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.

La red se dividirá cada 32 direcciones para dejar 8 segmentos y permitir el crecimiento siendo de la siguiente forma:

**192.168.1.0 – 192.168.1.31**

**192.168.1.32 – 192.168.1.63**

**192.168.1.64 – 192.168.1.95**

**192.168.1.96 – 192.168.1.127**

**192.168.1.128 – 192.168.1.159**

**192.168.1.160 – 192.168.1.191**

**192.168.1.192 – 192.168.1.223**

**192.168.1.224 – 192.168.1.255**

b. Asignar una dirección IP a la red.

**192.168.1.0**

**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	<b>MEDELLIN</b>		<b>BOGOTA</b>		<b>CALI</b>	
Dirección de Ip en interfaz Serial 0/0	192.168.1.99		192.168.1.98			
Dirección de Ip en interfaz Serial 0/1			192.168.1.130		192.168.1.131	
Dirección de Ip en interfaz GigabitEthernet 0/0	192.168.1.33		192.168.1.224		192.168.1.65	
Protocolo de enrutamiento	<b>Eigrp</b>		<b>Eigrp</b>		<b>Eigrp</b>	
Sistema Autónomo	10		10		10	
Afirmaciones de red	192.168.1.0		192.168.1.0		192.168.1.0	
PC's	<b>PC-A</b>	<b>PC-B</b>	<b>WS1</b>	<b>SER</b>	<b>PC-C</b>	<b>PC-C</b>
Dirección ip	.35	.36	.225	.226	.66	.67

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.



## MEDELLIN

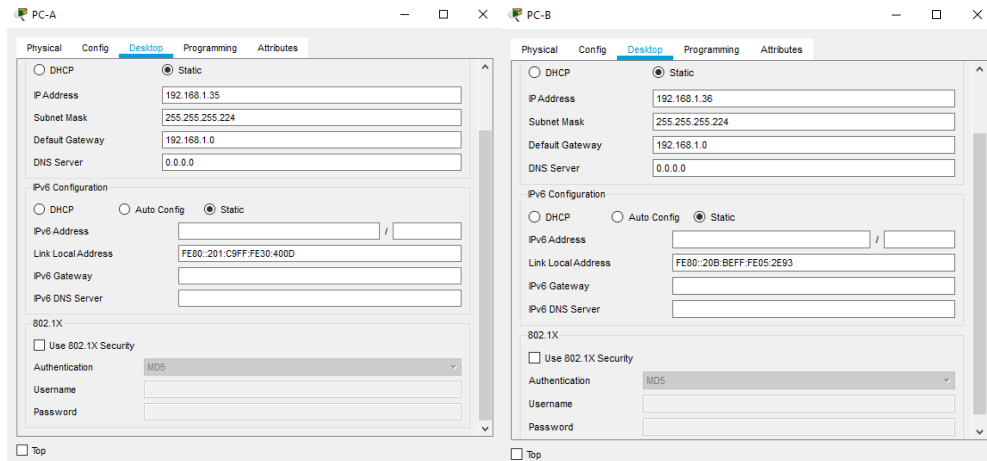


Ilustración 4: Dirección ip PC-A y PC-B Medellín

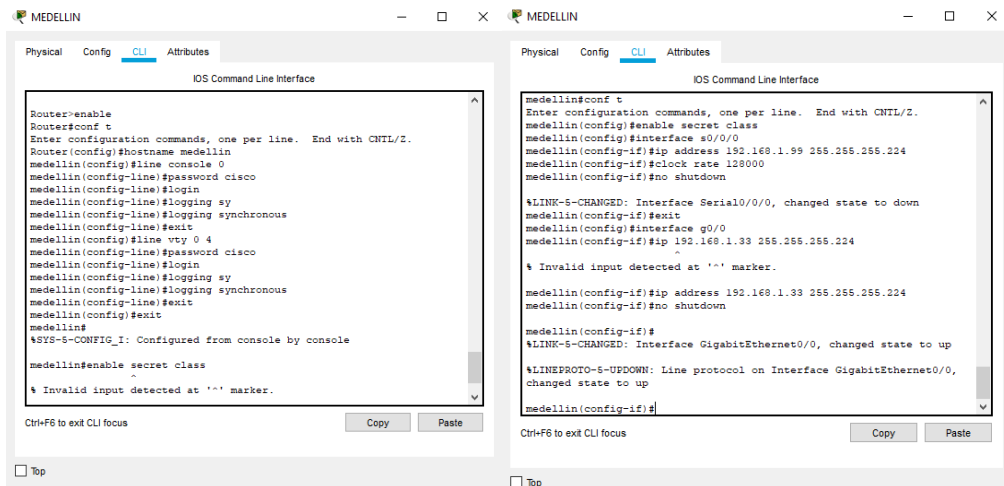


Ilustración 5: Configuración General Router Medellín

## BOGOTA

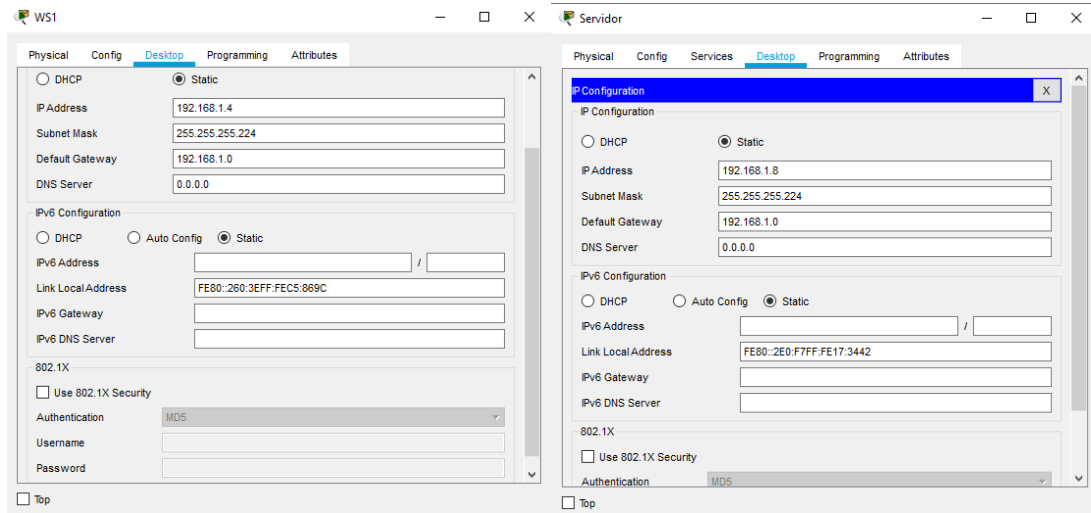


Ilustración 6: Dirección IP WS1 y Servidor Bogotá

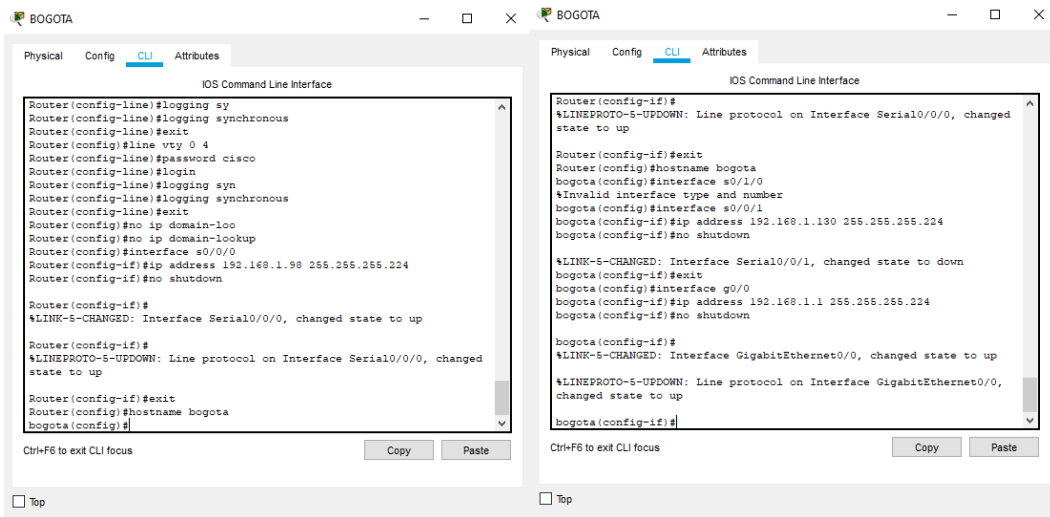


Ilustración 7: Configuración General Router Bogotá

## CALI

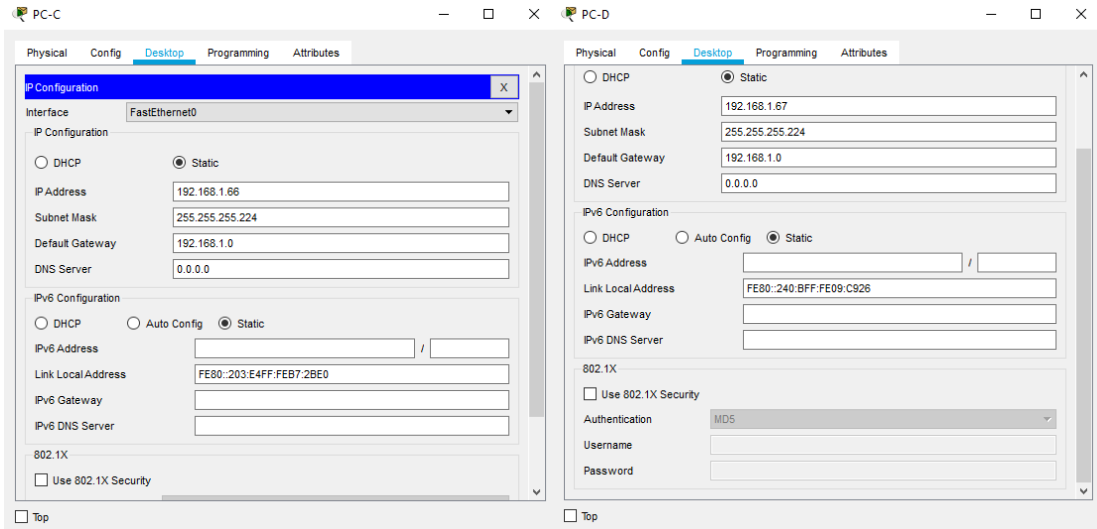


Ilustración 8: Dirección IP PC-C y PC-D Cali

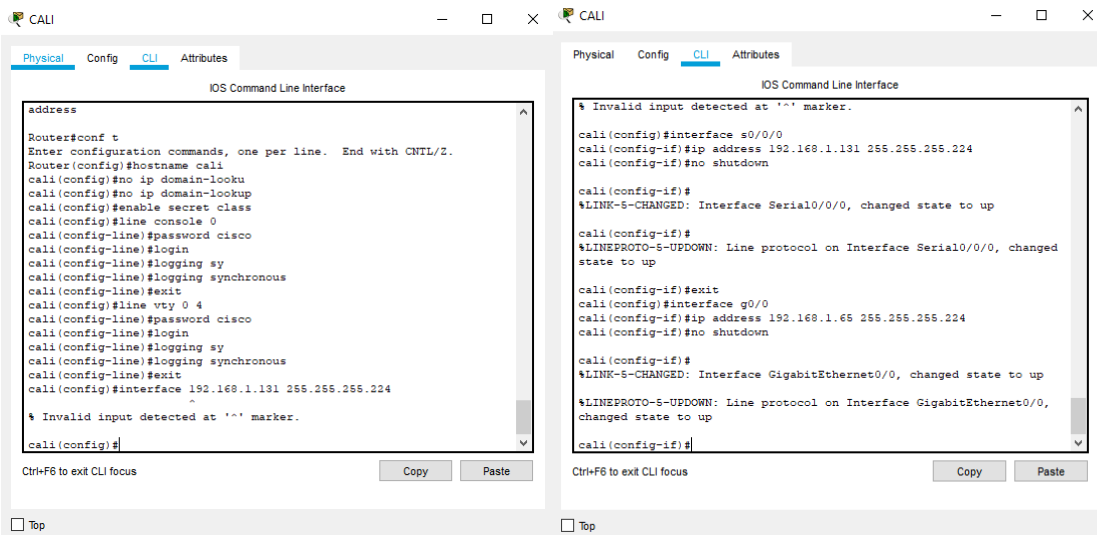


Ilustración 9: Configuración General Router Cali

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

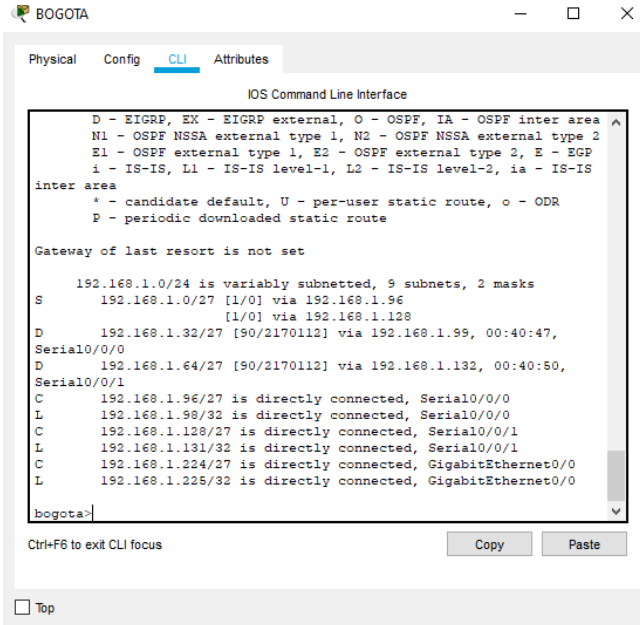


Ilustración 10: Balanceo de Carga Router Bogotá

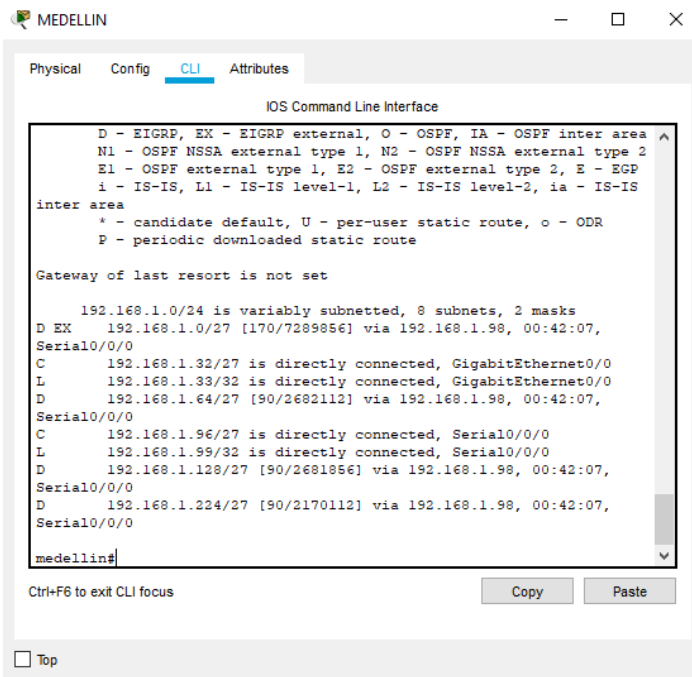


Ilustración 11: Balanceo de Carga Router Medellín





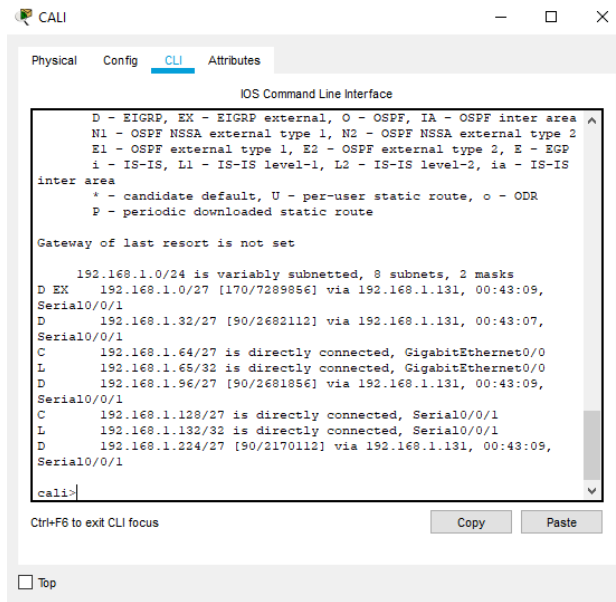


Ilustración 12: Balanceo de Carga Router Cali

- d. Realizar un diagnóstico de vecinos usando el comando cdp.

Se activa en todos los routers el cdp con el comando **router(config)#cdp run**



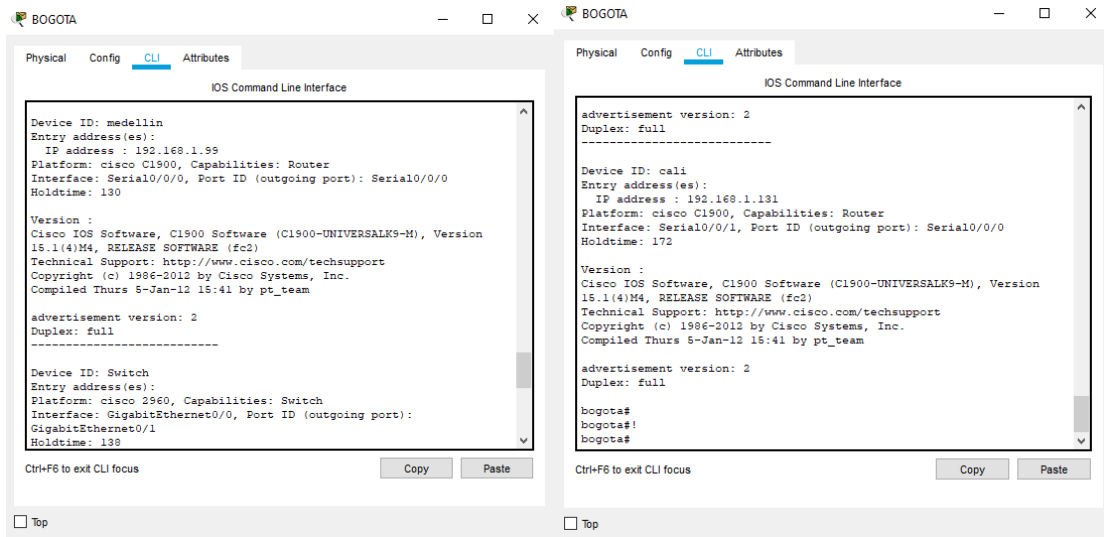


Ilustración 13: Diagnóstico CDP

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

## MEDELLIN

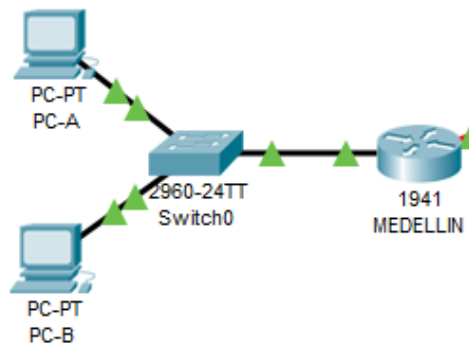


Ilustración 14: Conectividad tramo Medellín



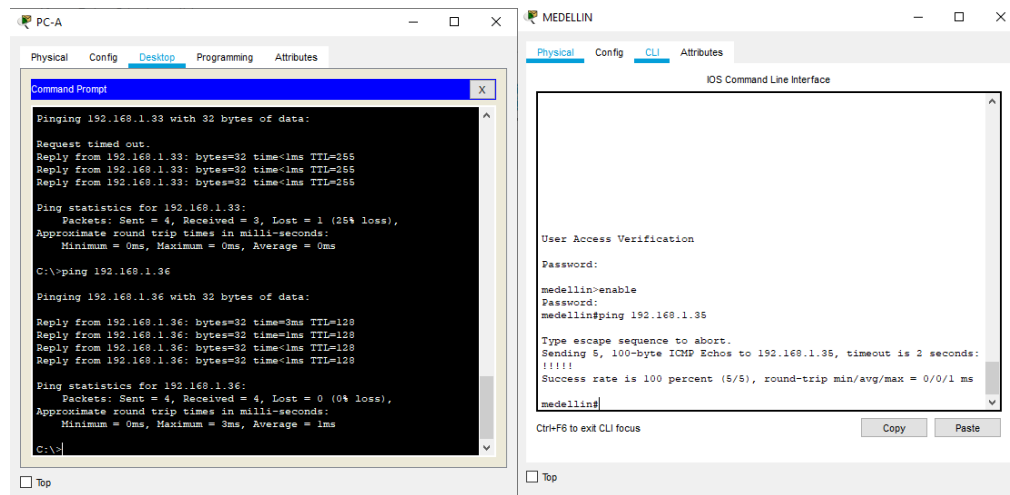


Ilustración 15: Ping tramo Medellín

## BOGOTA

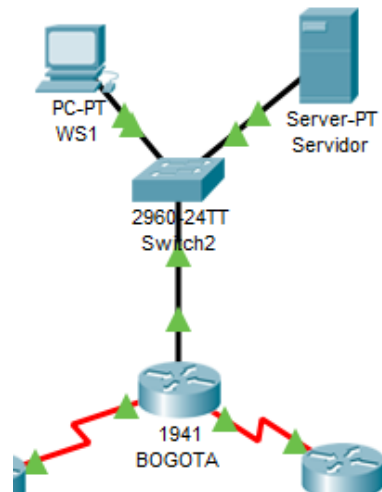


Ilustración 16: Conectividad tramo Bogotá



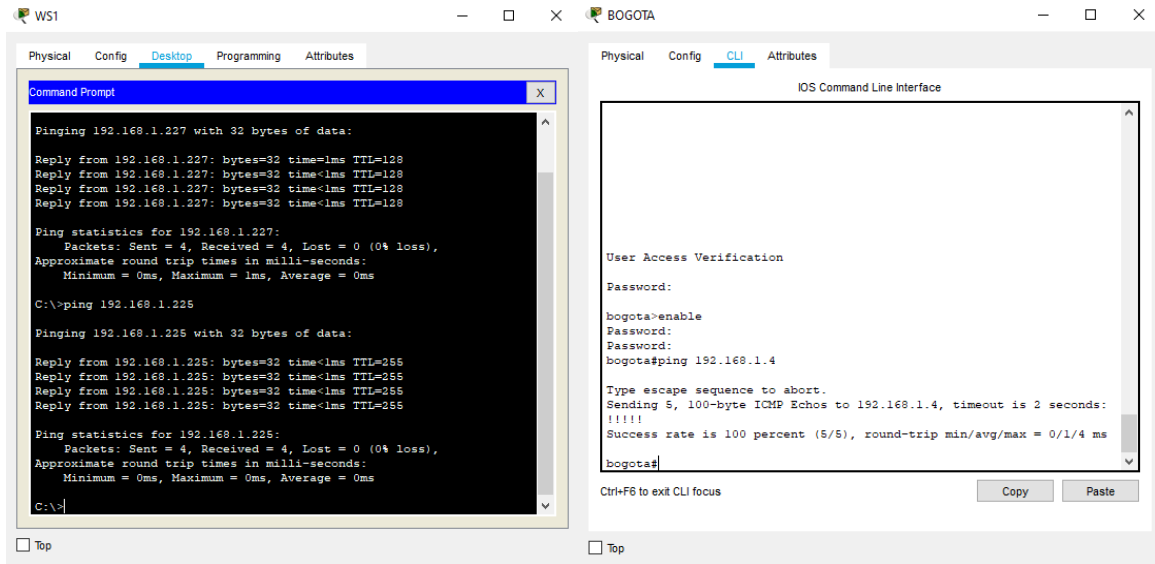


Ilustración 17: Ping tramo Bogotá

## CALI

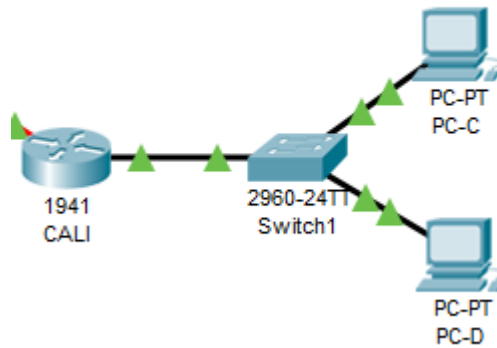


Ilustración 18: Conectividad tramo Cali



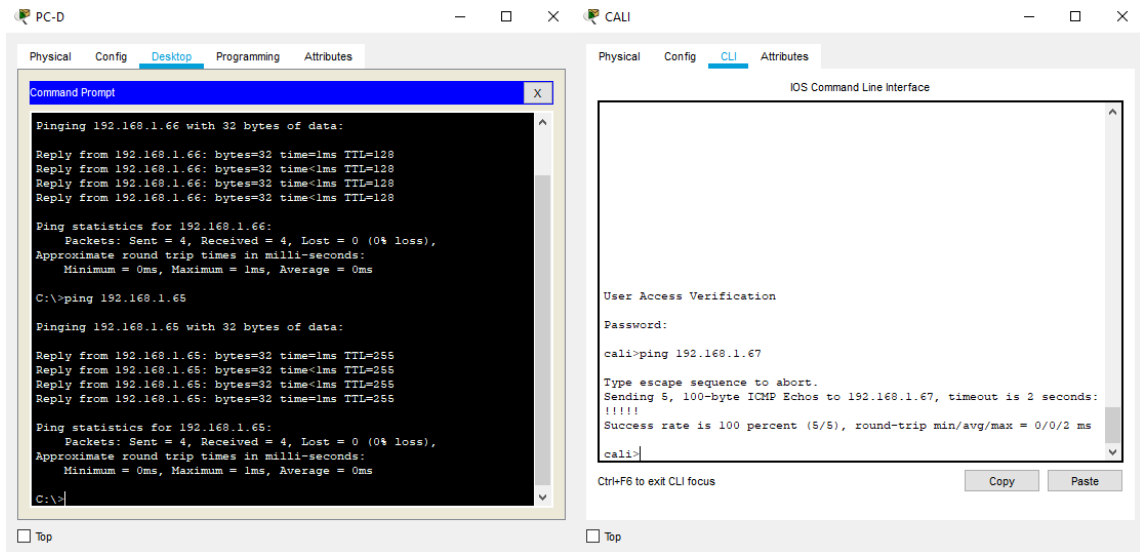


Ilustración 19: Ping tramo Cali

### Parte 3: Configuración de Enrutamiento.

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



```
Distance: internal 90 external 170
bogota#
bogota#conf t
Enter configuration commands, one per line. End with CNTL/Z.
bogota(config)#router eigrp 1
bogota(config-router)#network 192.168.1.128
bogota(config-router)#exit
bogota(config)#no router eigrp 1
bogota(config)#router eigrp 10
bogota(config-router)#network 192.168.1.0
bogota(config-router)#
%DUAL-S-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.1.99 (Serial0/0/0)
is up: new adjacency
%DUAL-S-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.1.132 (Serial0/0/1)
is up: new adjacency
bogota(config-router)#network 192.168.1.96
bogota(config-router)#network 192.168.1.32 0.0.0.31
bogota(config-router)#network 192.168.1.64 0.0.0.31
bogota(config-router)#network 192.168.1.128
bogota(config-router)#
```

```
medellin#
medellin#configure terminal
medellin#configure terminal
medellin#
medellin#conf t
Enter configuration commands, one per line. End with CNTL/Z.
medellin(config)#router eigrp 10
medellin(config-router)#network 192.168.1.96
medellin(config-router)#network 192.168.1.32 0.0.0.31
medellin(config-router)#no auto
medellin(config-router)#no auto-summary
medellin(config-router)#
%DUAL-S-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.1.98 (Serial0/0/0)
is up: new adjacency
medellin(config-router)#end
medellin#
medellin#show ip protocols
Routing Protocol is "eigrp 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
```

```
Routing Information Sources:
Gateway         Distance      Last Update
Distance: internal 90 external 170
cali#
cali#conf t
Enter configuration commands, one per line. End with CNTL/Z.
cali(config)#router eigrp 10
cali(config-router)#network 192.168.1.128
cali(config-router)#network 192.168.1.64 0.0.0.31
cali(config-router)#no au
cali(config-router)#no auto-summary
cali(config-router)#
%DUAL-S-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.1.131 (Serial0/0/1)
is up: new adjacency
cali(config-router)#
```

```
Press RETURN to get started!

User Access Verification

Password:
bogota#enable
Password:
bogota#conf t
Enter configuration commands, one per line. End with CNTL/Z.
bogota(config)#router rip
bogota(config-router)#network 192.168.1.96
bogota(config-router)#network 192.168.1.128
bogota(config-router)#192.164.1.0
^
% Invalid input detected at '^' marker.
bogota(config-router)#192.168.1.0
^
% Invalid input detected at '^' marker.
bogota(config-router)#network 192.168.1.0
bogota(config-router)#
```

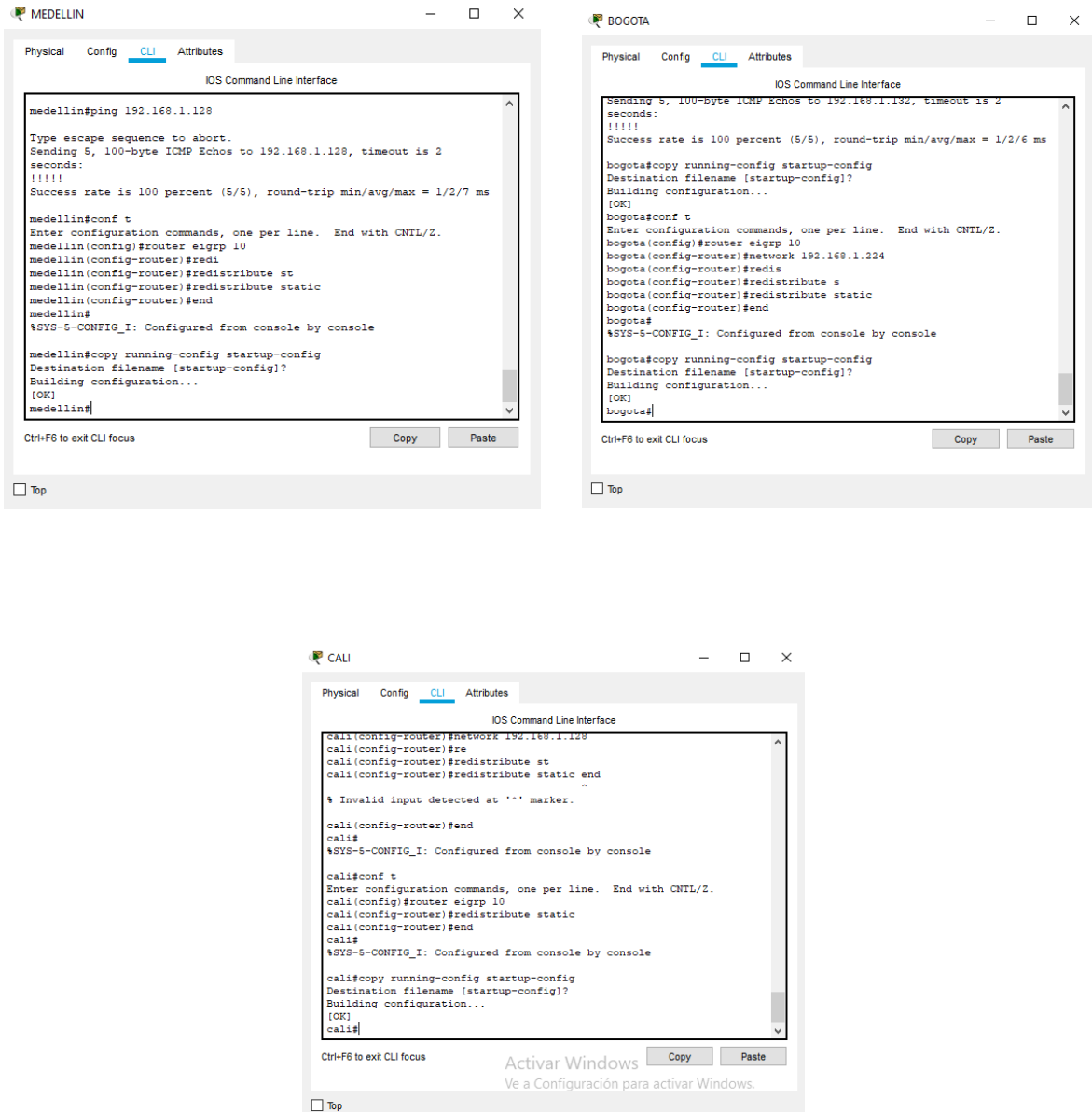


Ilustración 20: Protocolo EIGRP a todos los Routers

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



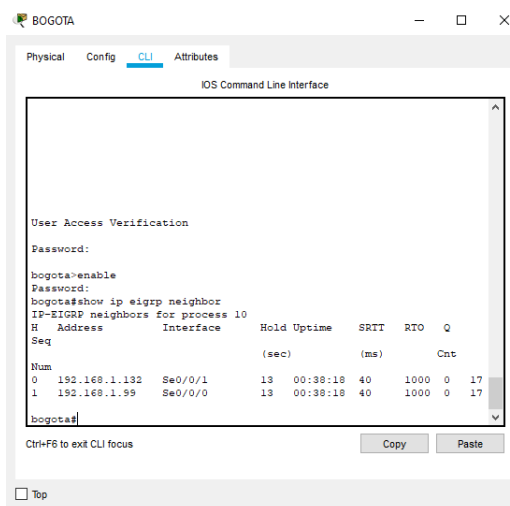
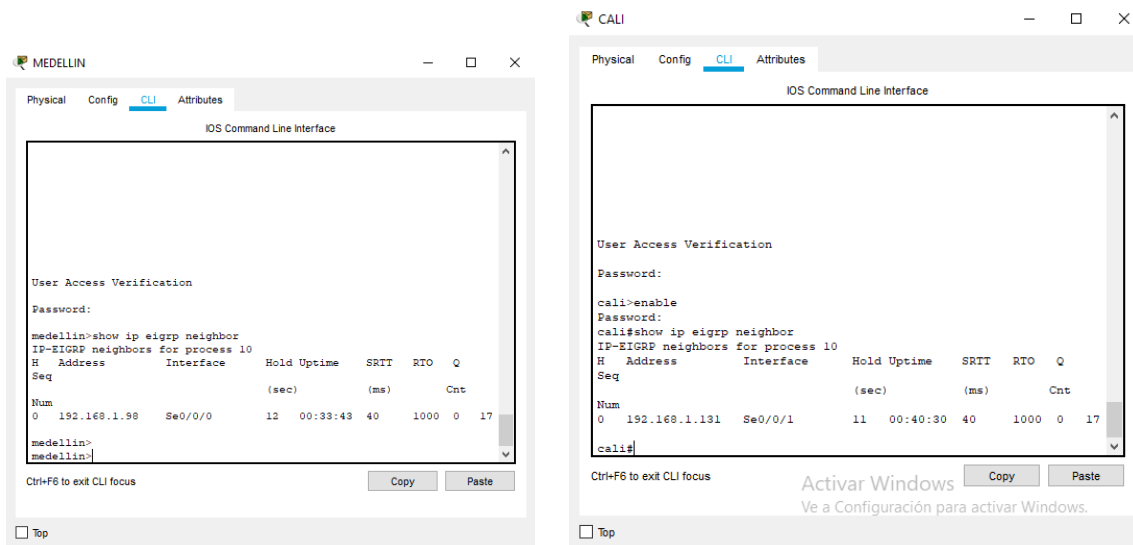


Ilustración 21: Vecindad entre Routers

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





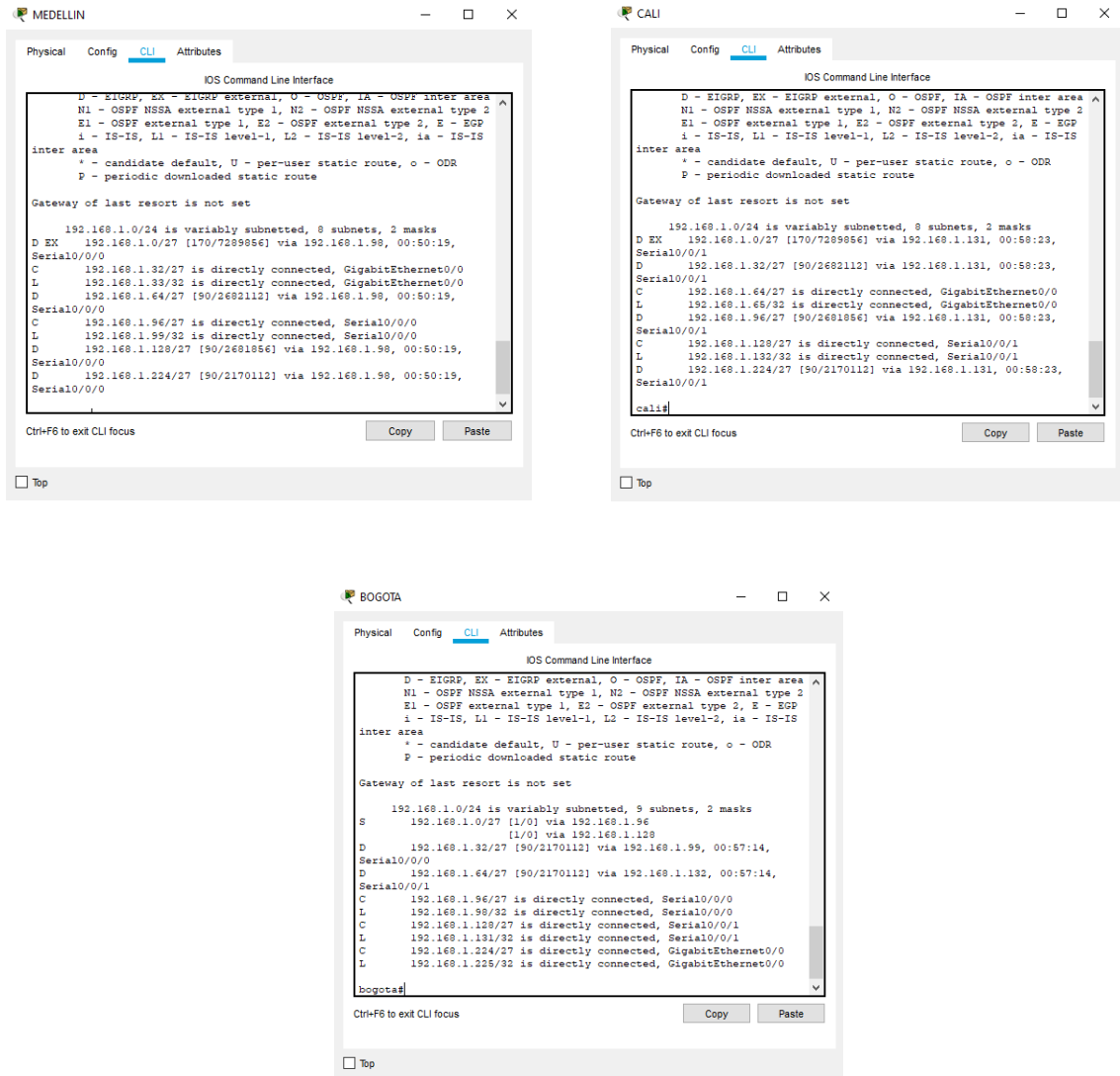


Ilustración 22: Tablas de Enrutamiento

- 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.



```

C:\>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=3ms TTL=253
Reply from 192.168.1.33: bytes=32 time=11ms TTL=253
Reply from 192.168.1.33: bytes=32 time=15ms TTL=253
Reply from 192.168.1.33: bytes=32 time=11ms TTL=253

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 15ms, Average = 10ms

C:\>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168.1.35: bytes=32 time=2ms TTL=125
Reply from 192.168.1.35: bytes=32 time=12ms TTL=125
Reply from 192.168.1.35: bytes=32 time=17ms TTL=125
Reply from 192.168.1.35: bytes=32 time=14ms TTL=125

Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 17ms, Average = 11ms
  
```

Ilustración 23: Conectividad Cali a Medellín

```

C:\>ping 192.168.1.226

Pinging 192.168.1.226 with 32 bytes of data:

Reply from 192.168.1.226: bytes=32 time=2ms TTL=126
Reply from 192.168.1.226: bytes=32 time=12ms TTL=126
Reply from 192.168.1.226: bytes=32 time=17ms TTL=126
Reply from 192.168.1.226: bytes=32 time=14ms TTL=126

Ping statistics for 192.168.1.226:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 17ms, Average = 11ms

C:\>ping 192.168.1.226

Pinging 192.168.1.226 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.226: bytes=32 time=2ms TTL=126
Reply from 192.168.1.226: bytes=32 time=10ms TTL=126
Reply from 192.168.1.226: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.1.226:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 11ms, Average = 7ms
  
```

Ilustración 24: Conectividad Cali a Bogotá

## 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.

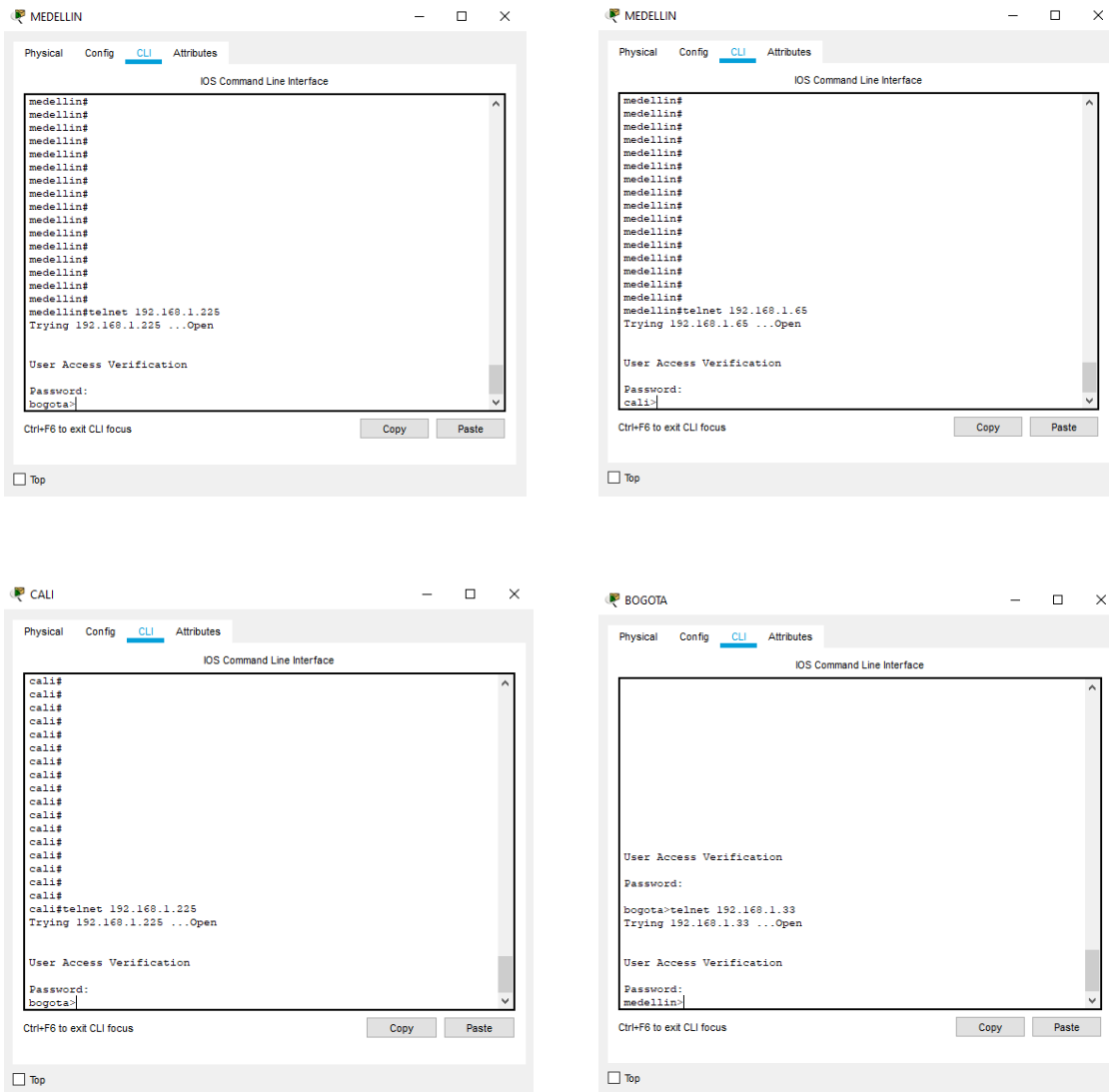


Ilustración 25: Conexiones Telnet

- b. 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.



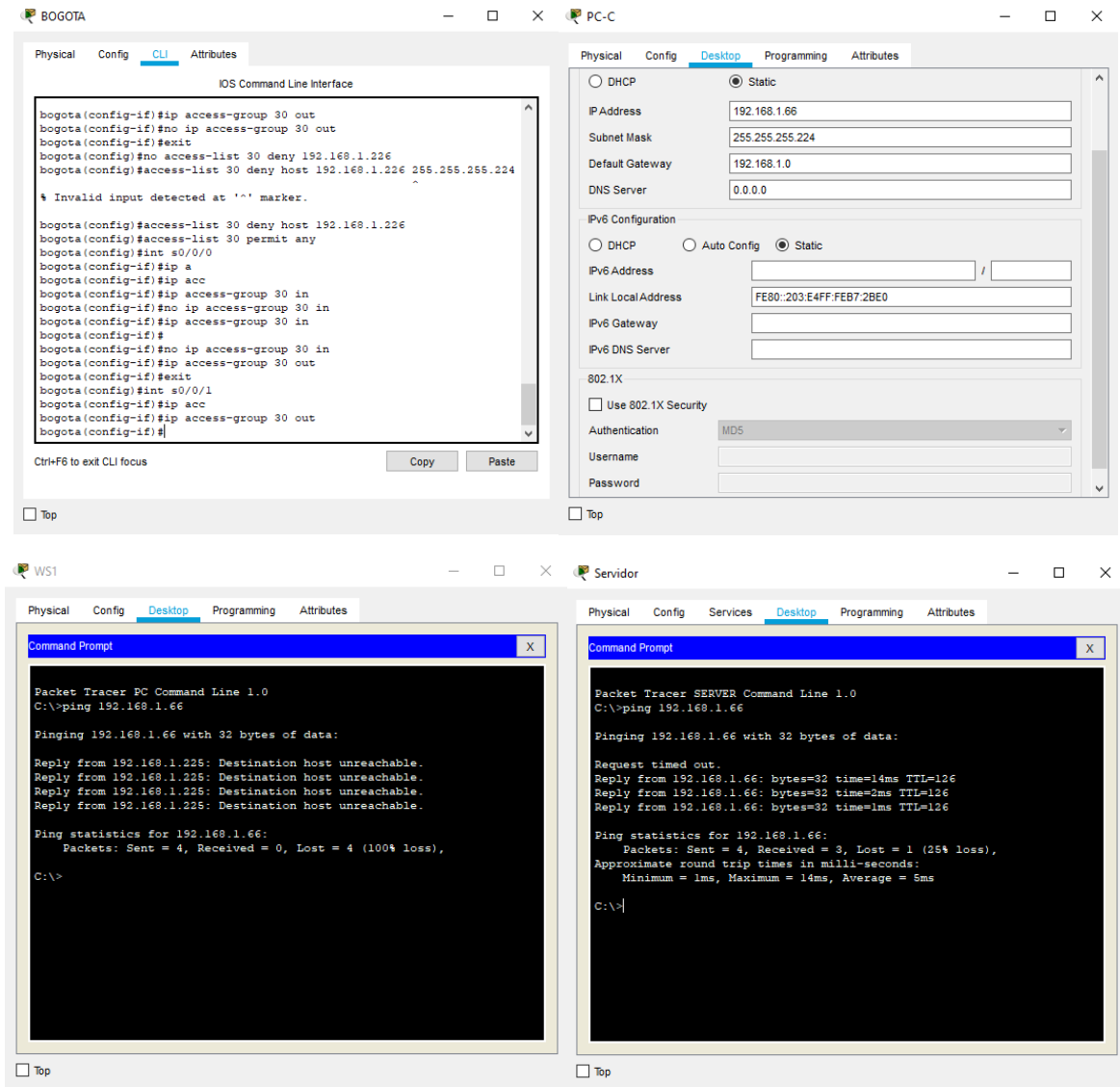


Ilustración 26: Listas de Acceso Bogotá

- c. 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.



```
MEDELLIN
Physical Config CLI Attributes
IOS Command Line Interface
medellin>enable
Password:
medellin#conf t
Enter configuration commands, one per line. End with CNTL/Z.
medellin(config)#access
medellin(config)#access-list 30 deny host 192.168.1.35
medellin(config)#access-list 30 deny host 192.168.1.36
medellin(config)#access-list 30 permit any
medellin(config)#int s0/0/0
medellin(config-if)#ip acc
medellin(config-if)#ip access-group 30 out
medellin(config-if)#no ip access-group 30 out
medellin(config-if)#exit
medellin(config)#no access-list 30 deny host 192.168.1.35
medellin(config)#no access-list 30 deny host 192.168.1.36
medellin(config)#no access-list 30 permit any
medellin(config)#no access-list 30 deny host 192.168.1.66
medellin(config)#no access-list 30 deny host 192.168.1.67
medellin(config)#access-list 30 deny host 192.168.1.66
medellin(config)#access-list 30 deny host 192.168.1.67
medellin(config)#access-list 30 permit any
medellin(config)#int s0/0/0
medellin(config-if)#ip acce
medellin(config-if)#ip access-group 30 out
medellin(config-if)#
```

Ilustración 27: Listas de Acceso Medellín

The image shows two side-by-side screenshots of PC configuration windows. The left window is for PC-B and the right is for PC-C. Both windows have tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is selected in both. The configuration fields are as follows:

Field	PC-B	PC-C
IP Address	192.168.1.36	192.168.1.66
Subnet Mask	255.255.255.224	255.255.255.224
Default Gateway	192.168.1.0	192.168.1.0
DNS Server	0.0.0.0	0.0.0.0
IPv6 Configuration	Static	Static
IPv6 Address		
Link Local Address	FE80::20B:BEFF:FE05:2E93	FE80::203:E4FF:FEB7:2BE0
IPv6 Gateway		
IPv6 DNS Server		
802.1X	Use 802.1X Security: <input type="checkbox"/>	Use 802.1X Security: <input type="checkbox"/>
Authentication	MDS	MDS
Username		
Password		

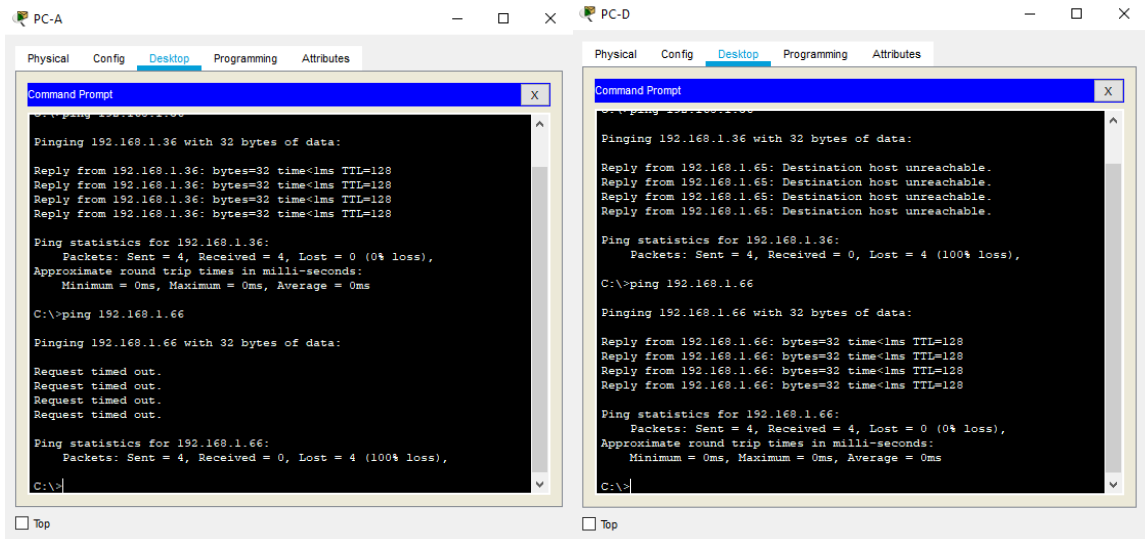


Ilustración 28: Ping entre Medellín y Cali

### 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	Conexión
	WS_1	Router BOGOTA	Conexión
	Servidor	Router CALI	Conexión
	Servidor	Router MEDELLIN	Conexión
TELNET	LAN del Router MEDELLIN	Router CALI	Sin Conexión
	LAN del Router CALI	Router CALI	Conexión



	LAN del Router MEDELLIN	Router MEDELLIN	Conexión
	LAN del Router CALI	Router MEDELLIN	Sin Conexión
PING	LAN del Router CALI	WS_1	Sin Ping
	LAN del Router MEDELLIN	WS_1	Sin Ping
	LAN del Router MEDELLIN	LAN del Router CALI	Sin Ping
PING	LAN del Router CALI	Servidor	Ping
	LAN del Router MEDELLIN	Servidor	Ping
	Servidor	LAN del Router MEDELLIN	Ping
	Servidor	LAN del Router CALI	Ping
	Router CALI	LAN del Router MEDELLIN	Ping
	Router MEDELLIN	LAN del Router CALI	Ping



## 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.

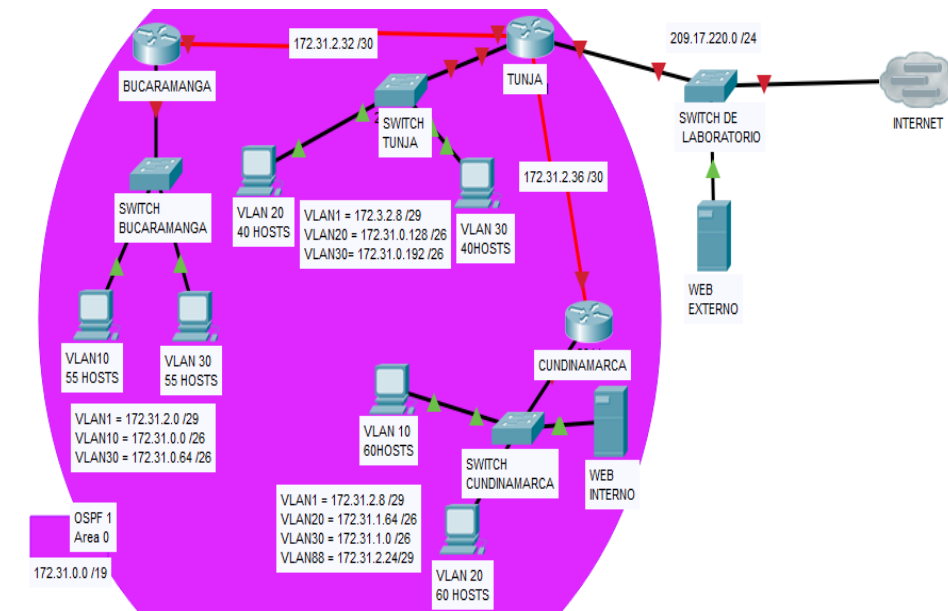


Ilustración 29: Topología Escenario 2

## Desarrollo

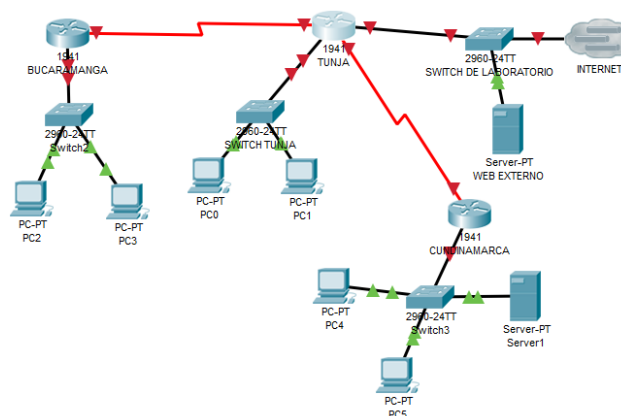


Ilustración 30: Construcción Escenario 2



Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:

- Configuración básica.

```
IOS Command Line Interface
memory.
Processor board ID F1X152400K5
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#aa
Router(config)#hostname tunja
tunja(config)#int g0/0
tunja(config-if)#ip address 209.17.220.1 255.255.255.0
tunja(config-if)#no shutdown

tunja(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
Ctrl+F6 to exit CLI focus
```

```
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to down
tunja(config-if)#no shutdown
tunja(config-if)#
tunja(config-if)#int s0/0/0
tunja(config-if)#ip address 172.31.2.33 255.255.255.252
tunja(config-if)#no shutdown

tunja(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
tunja(config-if)#
Ctrl+F6 to exit CLI focus
```

```
IOS Command Line Interface
tunja>conf t
-
% Invalid input detected at '^' marker.
tunja>enable
Password:
tunja#conf t
Enter configuration commands, one per line. End with CNTL/Z.
tunja(config)#int s0/0/1
tunja(config-if)#ip address 172.31.2.37 255.255.255.252
tunja(config-if)#no shutdown

tunja(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
tunja(config-if)#clock rate 128000
tunja(config-if)#exit
tunja(config)#int s0/0/0
tunja(config-if)#clock 128000
^
% Invalid input detected at '^' marker.
tunja(config-if)#clock rate 128000
tunja(config-if)#exit
tunja(config)#
Ctrl+F6 to exit CLI focus
```

```
IOS Command Line Interface
bucaramanga(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up
bucaramanga(config-if)#int s0/0/0
bucaramanga(config-if)#ip address 172.31.2.34 255.255.255.252
bucaramanga(config-if)#no shutdown

bucaramanga(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
bucaramanga(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up
Ctrl+F6 to exit CLI focus
```

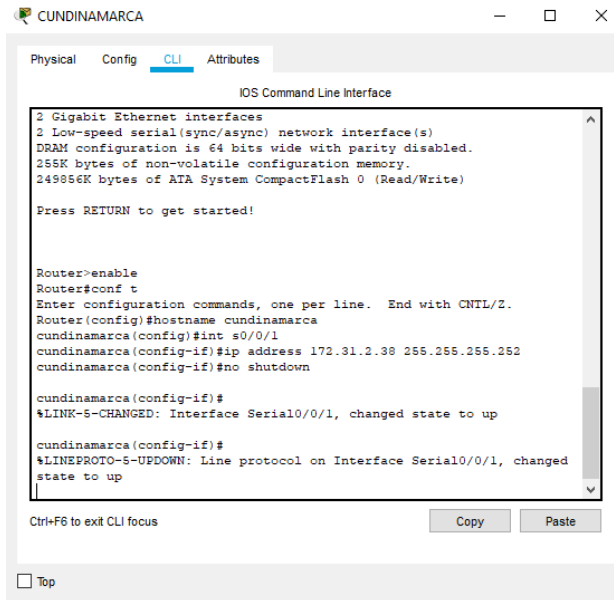
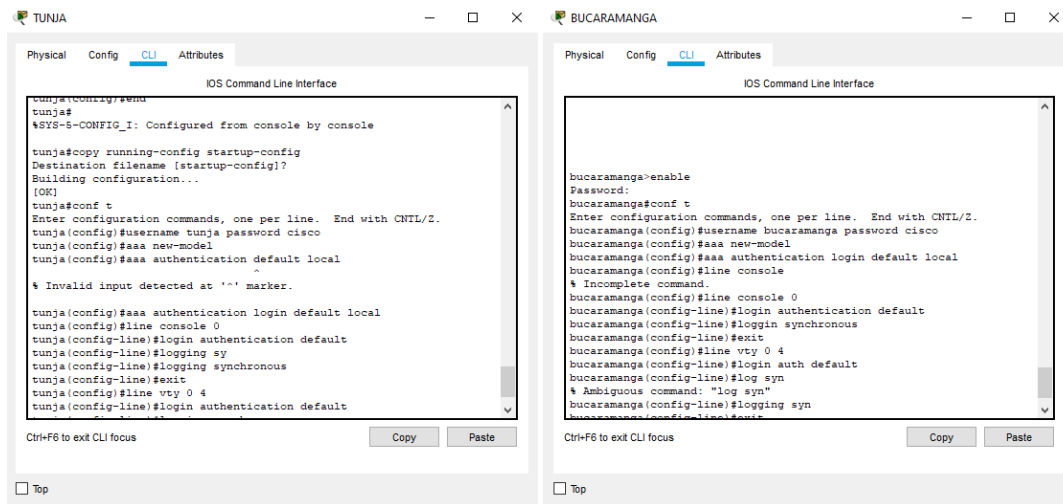


Ilustración 31: Configuración Básica Routers

- Autenticación local con AAA.



```

cundinamarca>enable
Password:
cundinamarca#conf t
Enter configuration commands, one per line. End with CNTL/Z.
cundinamarca(config)#username cundinamarca password cisco
% Invalid input detected at '^' marker.
cundinamarca(config)#username cundinamarca password cisco
cundinamarca(config)#aaa new-model
cundinamarca(config)#aaa authentication login default local
cundinamarca(config)#line console 0
cundinamarca(config-line)#login authentication default
cundinamarca(config-line)#logging synchronous
cundinamarca(config-line)#exit
cundinamarca(config)#line vty 0 4
cundinamarca(config-line)#login authentication default
cundinamarca(config-line)#logging synchronous
cundinamarca(config-line)#exit
cundinamarca(config)#
  
```

Ilustración 32: Configuración AAA a todos los Routers

- Cifrado de contraseñas.

```

TUNJA>enable
Password:
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#service password-encryption
TUNJA(config)#
  
```

```

BUCARAMANGA>enable
Password:
BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#service password-encryption
BUCARAMANGA(config)#
  
```



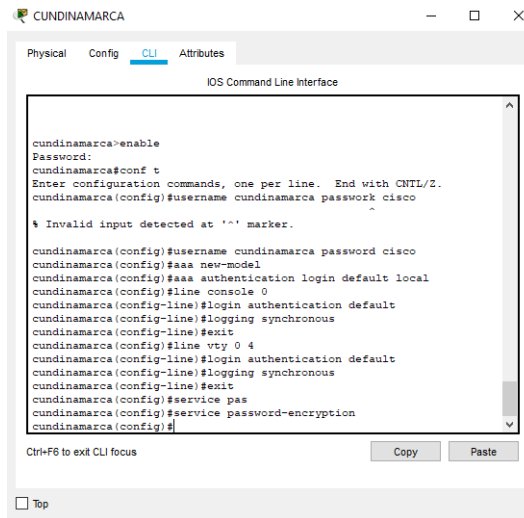
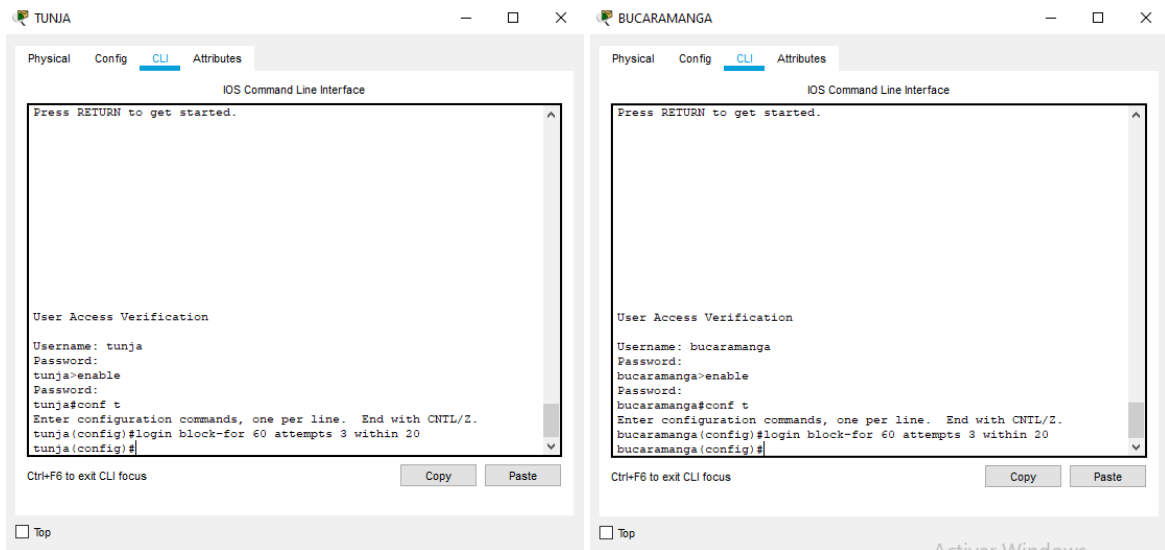


Ilustración 33: Cifrado de Contraseñas en los Routers

- Un máximo de intentos para acceder al router.



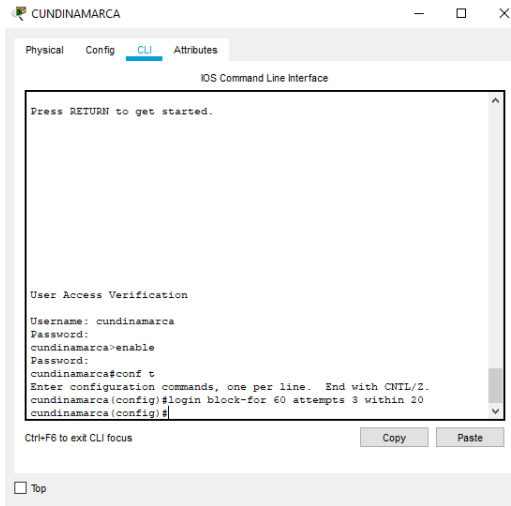
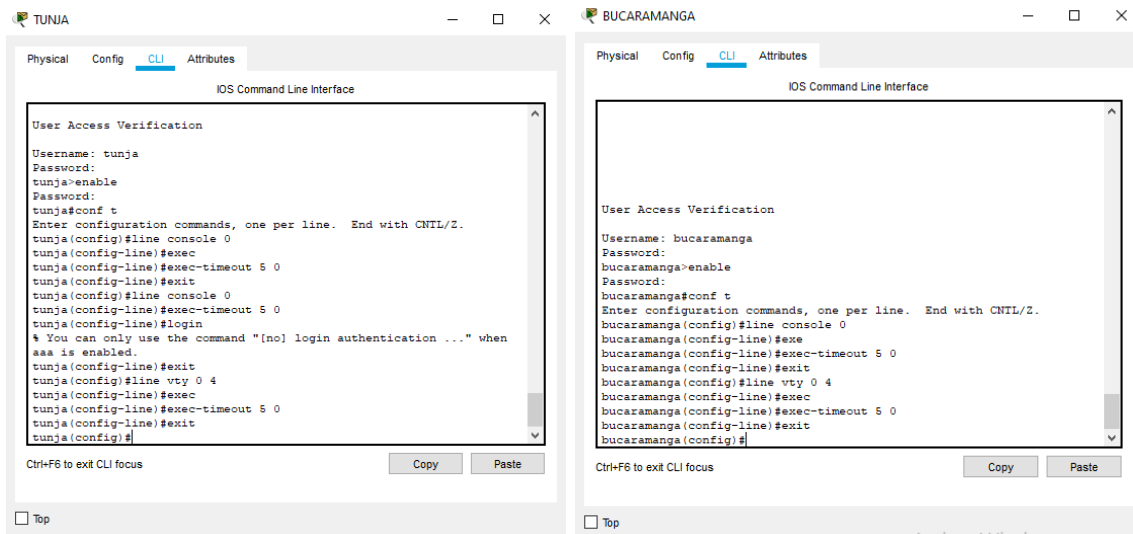


Ilustración 34: Máximo de Intentos para entrar a los Routers

- Máximo tiempo de acceso al detectar ataques.



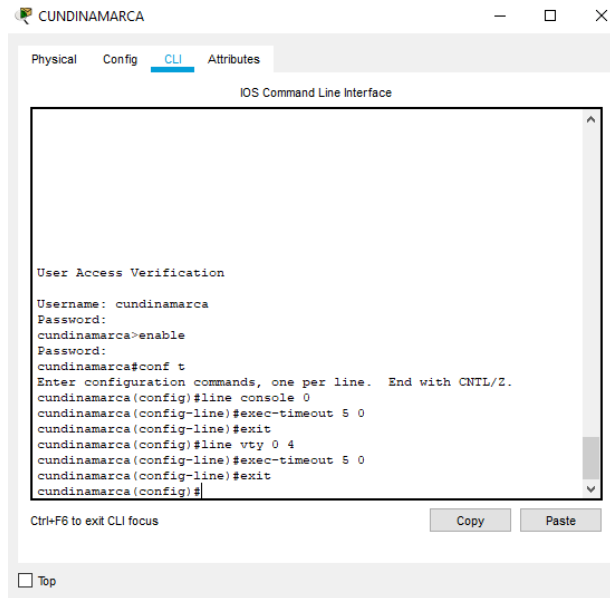


Ilustración 35: Limitación al Detectar Ataques en los Routers

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

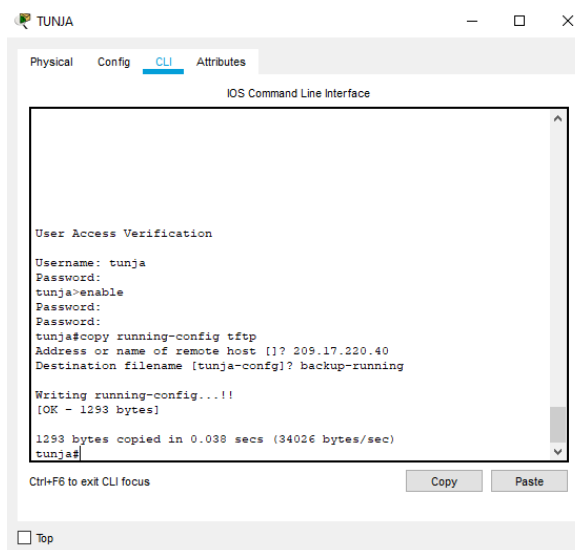


Ilustración 36: Archivos de seguridad de los Routers a TFTP



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

The image shows two side-by-side screenshots of IOS Command Line Interface (CLI) windows. The left window is titled 'BUCARAMANGA' and the right window is titled 'CUNDINAMARCA'. Both windows show the configuration of interfaces and DHCP pools.

```
bucaramanga(config-if)#exit
bucaramanga(config)#int g0/1.1
bucaramanga(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.1,
changed state to up
bucaramanga(config-subif)#encapsulation dot1Q 1 native
bucaramanga(config-subif)#ip address 172.31.2.1 255.255.255.248
bucaramanga(config-subif)#exit
bucaramanga(config)#int g0/1.10
bucaramanga(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1.10, changed state to up
bucaramanga(config-subif)#encapsulation dot1Q 10
bucaramanga(config-subif)#ip address 172.31.0.1 255.255.255.192
bucaramanga(config-subif)#ip helper-address 172.31.2.33
bucaramanga(config-subif)#ip access-group 101 in
bucaramanga(config-subif)#exit
bucaramanga(config)#
```

```
cundinamarca(config-subif)#encapsulation dot1Q 20
cundinamarca(config-subif)#ip address 172.31.1.1 255.255.255.192
cundinamarca(config-subif)#ip helper-address 172.31.2.38
cundinamarca(config-subif)#ip helper-address 172.31.2.37
cundinamarca(config-subif)#ip access-group 102 in
cundinamarca(config-subif)#exit
cundinamarca(config)#int g0/1.10
cundinamarca(config-subif)#ip helper-address 172.31.2.37
cundinamarca(config-subif)#exit
cundinamarca(config)#int g0.1.88
% Invalid input detected at '^' marker.
cundinamarca(config)#int g0/1.88
cundinamarca(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.88, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1.88, changed state to up
cundinamarca(config-subif)#encapsulation dot1Q 88 native
cundinamarca(config-subif)#ip address 172.31.2.25 255.255.255.248
cundinamarca(config-subif)#exit
cundinamarca(config)#
```

The image shows a screenshot of the IOS Command Line Interface (CLI) window for a router named 'TUNJA'. The window displays the 'User Access Verification' process and the configuration of DHCP excluded addresses.

```
User Access Verification
Username: tunja
Password:
tunja>enable
Password:
Password:
tunja#conf t
Enter configuration commands, one per line. End with CNTL/Z.
tunja(config)#ip dhcp excluded-address 172.31.1.65 172.31.1.70
tunja(config)#ip dhcp excluded-address 172.31.1.1 172.31.1.5
tunja(config)#ip dhcp excluded-address 172.31.0.1 172.31.0.5
tunja(config)#ip dhcp excluded-address 172.31.0.65 172.31.0.70
tunja(config)#
```

Ilustración 37: Configuración DHCP de los Routers



Switch0

Physical Config **CLI** Attributes

IOS Command Line Interface

```

Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#exit
Switch(config)#int range fa0/1-10
Switch(config-if-range)#switchpor access vlan 10
Switch(config-if-range)#write

* Invalid input detected at '' marker.

Switch(config-if-range)#do write
Building configuration...
[OK]
Switch(config-if-range)#exit
Switch(config)#int range f0/11-20
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#exit
Switch(config)#int range fa0/1-10
Switch(config-if-range)#switchpor access vlan 10
Switch(config-if-range)#sw
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#exit
Switch(config)#
          
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

SWITCH BUCARAMANGA

Physical Config **CLI** Attributes

IOS Command Line Interface

```

Switch(config-if)#switchport access VLAN 1
Switch(config-if)#interface VLAN 1
Switch(config-if)#ip address 172.31.2.0 255.255.255.248
Bad mask /29 for address 172.31.2.0
Switch(config-if)#ip address 172.31.2.2 255.255.255.248
Switch(config-if)#ip defa
Switch(config-if)#ip default
Switch(config-if)#ip default-gateway 172.31.2.1
Switch(config)#int f0/4
Switch(config-if)#switchport access VLAN 10
Switch(config-if)#switchport mode access
Switch(config-if)#exit
Switch(config)#int f0/15
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access VLAN 30
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access VLAN 30
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access VLAN 10
Switch(config-if)#switchport access VLAN 10
Switch(config-if)#switchport access VLAN 1
Switch(config-if)#switchport access VLAN 30
Switch(config-if)#switchport mode access
Switch(config-if)#
          
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

TUNJA

Physical Config **CLI** Attributes

IOS Command Line Interface

```

tunja(config)#int g0/1.20
tunja(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1.20, changed state to up

tunja(config-subif)#encapsulation dot1Q 20
tunja(config-subif)#ip address 172.31.0.129 255.255.255.192
tunja(config-subif)#ip access
tunja(config-subif)#ip access-group 102 in
tunja(config-subif)#exit
tunja(config)#int g0/1.30
tunja(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1.30, changed state to up

tunja(config-subif)#encapsulation dot1Q 30
tunja(config-subif)#ip address 172.31.0.193 255.255.255.192
tunja(config-subif)#ip ac
tunja(config-subif)#ip access-group 103 in
tunja(config-subif)#exit
tunja(config)#
          
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

SWITCH CUNDINAMARCA

Physical Config **CLI** Attributes

IOS Command Line Interface

```

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
to up

Switch(config-if)#exit
Switch(config)#int g0/1
Switch(config-if)#svi
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up

Switch(config-if)#exit
Switch(config)#int range
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down

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

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Ilustración 38: Configuración DHCP Switches





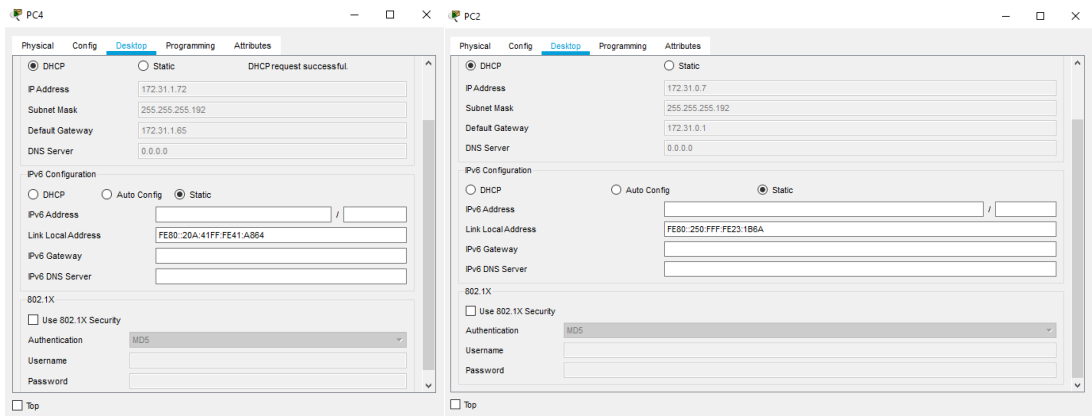


Ilustración 39: Asignación DHCP

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

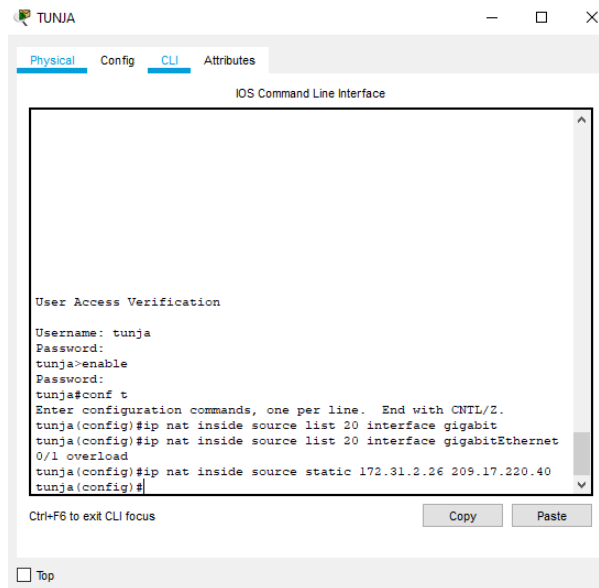


Ilustración 40: Configuración NAT



#### 4. El enrutamiento deberá tener autenticación.

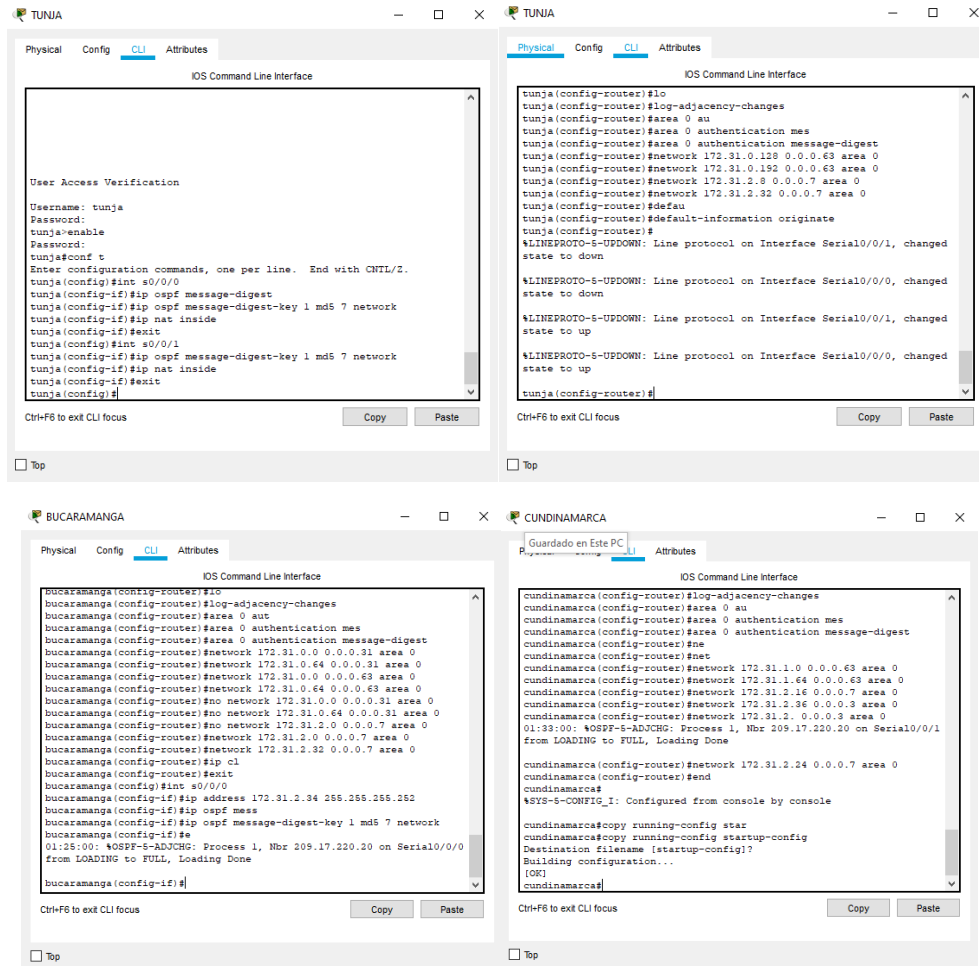


Ilustración 41: Autenticación al enrutamiento de cada Router

#### 5. Listas de control de acceso:

- Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.
- Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.

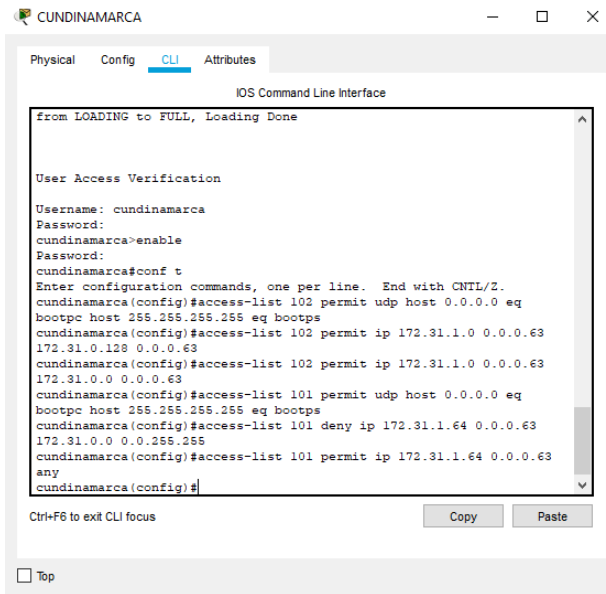


Ilustración 42: Listas de Control de Acceso Cundinamarca

- Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.
- Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.

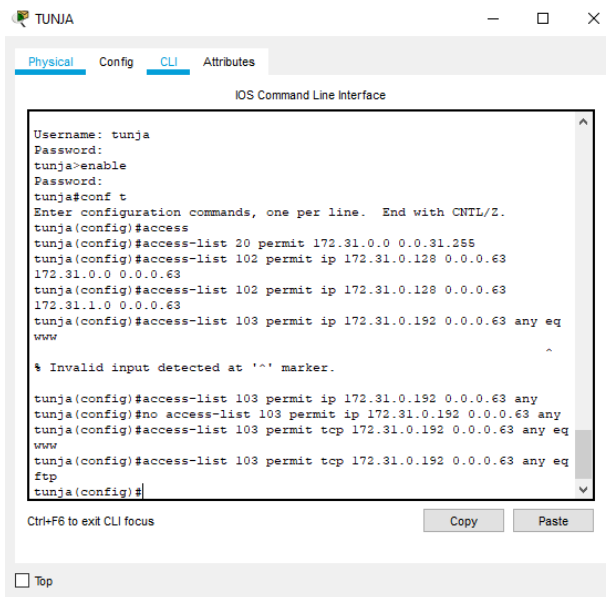


Ilustración 43: Listas de Control de Acceso Tunja

- Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.

- Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.

Ilustración 44: Listas de Control de Acceso Bucaramanga

- Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.

Ilustración 45: IP's de VLAN distintas



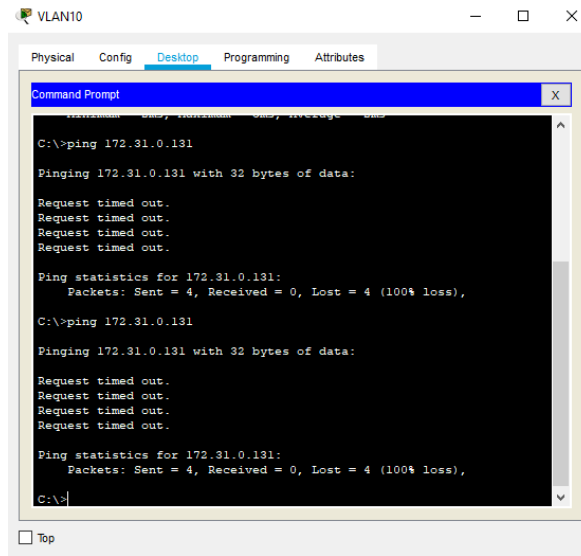


Ilustración 46: No hay ping para otra VLAN

- Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen acceso a los routers e internet.

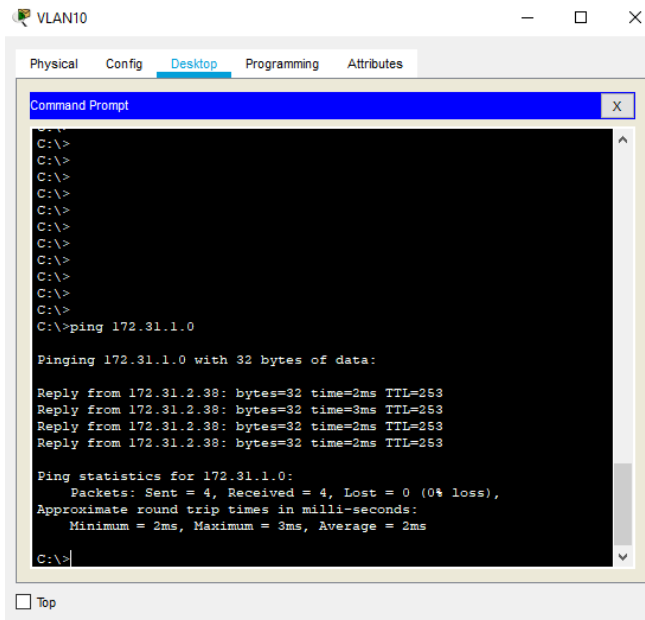


Ilustración 47: Acceso a los Router



6. VLSM: utilizar la dirección 172.31.0.0 /18 para el direccionamiento.

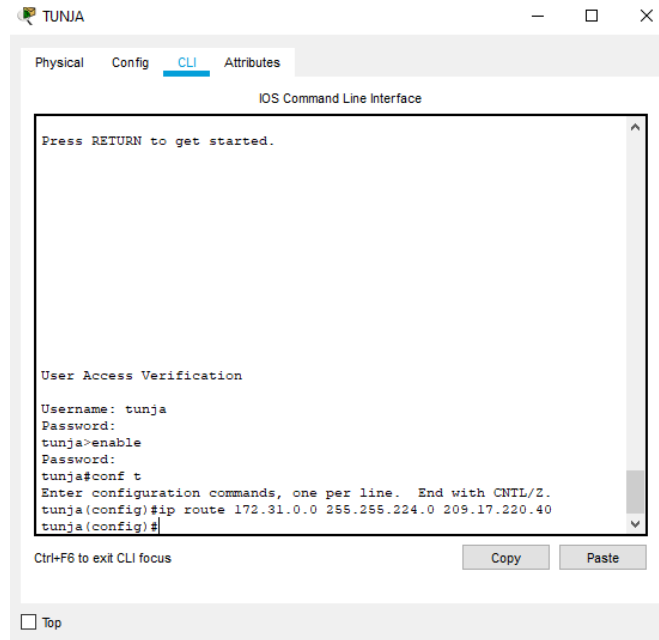


Ilustración 48: Direccionamiento

**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



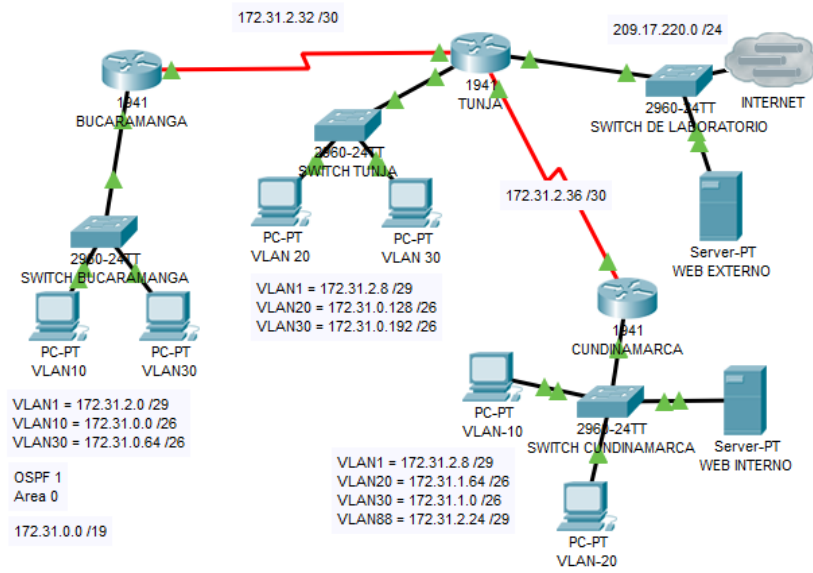


Ilustración 49: Conexión de Toda la Red

## Conclusiones

- Se apropiaron los conocimientos adquiridos y se resolvieron los ejercicios con éxito. Es importante poner en primer plano el diseño inicial de una red, para que al desarrollarse no se cometan errores en el proceso y se pueda solventar la problemática o situación tratada.
- Los aspectos de seguridad para una red sea pública o privada, deben ser lo principal en el diseño inicial, pues gracias a esto se delimita la accesibilidad de una red y así mismo se asegura que el manejo general sea por parte de la red principal, esto lo permiten las listas de acceso.
- Para rebajar costos en una red y asegurar su escalabilidad, se debe tener en cuenta el uso de DHCP para asignar una dirección única a cada host.



## Bibliografía

- CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Disponible en <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>
- CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Disponible en <https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>
- CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Disponible en <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>

