

# **PRUEBA DE HABILIDADES PRÁCTICAS**

**CRISTIAM HUMBERTO GOMEZ QUIJANO**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA  
PROGRAMA INGENIERÍA DE SISTEMAS  
BUCARAMANGA  
2019**

# **PRUEBA DE HABILIDADES PRÁCTICAS**

CRISTIAM HUMBERTO GOMEZ QUIJANO

Trabajo de grado para optar por el título de Ingeniero de sistemas

DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA  
PROGRAMA INGENIERÍA DE SISTEMAS  
BUCARAMANGA  
2019

## CONTENIDO

	Pág.
1. INTRODUCCIÓN.....	6
2. OBJETIVOS .....	7
2.1 OBJETIVO GENERAL .....	7
2.2 OBJETIVOS ESPECÍFICOS .....	7
3. DESARROLLO DEL PROYECTO .....	8
3.1 ESCENARIO 1 .....	8
3.1.1 Asignación de direcciones IP: .....	10
3.1.2 Configuración básica: .....	11
3.1.3 Configuración de enrutamiento .....	19
3.1.4 Configuración de las listas de acceso .....	23
3.1.5 Comprobación de la red instalada.....	24
3.2 ESCENARIO 2 .....	30
3.2.1 Desarrollo del diagrama de red de la empresa.....	32
3.2.3 Configuración de Switches y habilitación de las VLAN para permitir su enrutamiento.....	34
3.2.4 Configuración de puertos en los router y DHCP con el router de Tunja para las LAN de Bucaramanga y Cundinamarca.....	36
3.2.4 Configuración OSPF con autenticación.....	39
3.2.5 Configuración de NAT estático y de sobrecarga .....	41
3.2.6 Establecer una lista de control de acceso de acuerdo con los criterios señalados. ....	44
CONCLUSIONES .....	55
BIBLIOGRAFÍA.....	57

## RESUMEN

Hoy día la tecnología es parte fundamental de nuestro mundo ya que ha cambiado de forma drástica todo lo que hacemos dejando de ser establecida como un lujo y pasando a ser una necesidad básica. Es importante destacar que gran parte del avance tecnológico radica en la modernización de la forma en que nos comunicamos y como integramos servicios, por este motivo el diplomado tomado como modalidad de grado en la Universidad Nacional Abierta y a Distancia "UNAD" ofrece la oportunidad de que sus egresados puedan aprender los principios básicos de enrutamiento y generen bases para seguir en una carrera enfocada en las telecomunicaciones a través de la implementación de simuladores apoyados en el desarrollo de prácticas, evaluaciones y contenidos propios del portal Netacad. En Diplomado estaba dividido en el módulo CCNA1 el cual permite conocer los pilares básicos de las redes y el módulo CCNA2 que permitió traer a la práctica los principios básicos de routing y switching. En este proyecto se pondrá en práctica algunos de los contenidos abordados durante el curso los cuales nos trasladan a un escenario real que permite evaluar los conocimientos adquiridos y generar una experiencia de algunos posibles casos que se pudieran presentar en un entorno laboral otorgando un valor adicional al estudiante de Ingeniería generado en la práctica y en la construcción de nuevo conocimiento basado en la investigación y soportando en los contenidos analizados.

**PALABRAS CLAVE:** Ingeniería, routing, switching, Diplomado, enrutamiento

## **ABSTRACT**

Today, technology is a fundamental part of our world since everything we do has changed drastically, becoming a luxury and becoming a basic necessity. It is important to highlight that a large part of the technological advance lies in the modernization of the way in which we communicate and how we integrate services, for this reason the diploma taken as a degree modality at the National Open and Distance University "UNAD" offers the opportunity for its graduates can learn the basic principles of routing and generate bases to continue in a career focused on telecommunications through the implementation of simulators supported by the development of practices, evaluations and content of the Netacad portal. In Diploma it was divided into the CCNA1 module which allows to know the basic pillars of the networks and the CCNA2 module that allowed to implement the basic principles of routing and switching. In this project, some of the contents addressed during the course will be put into practice, which will take us to a real scenario that allows us to evaluate the knowledge acquired and generate an experience of some possible cases that could occur in a work environment, giving additional value to the Engineering student generated in practice and in the construction of new knowledge based on research and supporting the analyzed contents.

**PALABRAS CLAVE:** Engineering, routing, switching, routing

## 1. INTRODUCCIÓN

El diplomado de profundización Cisco, permite explorar y aplicar los contenidos aprendidos durante el análisis y prácticas de las temáticas desarrolladas en los módulos CCNA1 y CCNA2 en los cuales se conocen los principios de las redes y los principios de routing y switching con lo que se analizará dos escenarios donde se involucra la investigación y la puesta en práctica de los conocimientos adquiridos.

Para los ejercicios se aplicaron las técnicas convenientes para que permitiera su comprensión, solución y generación de nuevo conocimiento basado en la práctica en aspectos o equipos como routers, switches, servidores, seguridad en los dispositivos, routing, Vlans, Protocolo OSPF, NAT, DHCP, Listas de control de acceso (ACL) entre otros principios que acoplados ilustran perfectamente un pequeño escenario real de una red con varios dispositivos y manejo de protocolos de enrutamiento.

## **2. OBJETIVOS**

### **2.1 OBJETIVO GENERAL**

Implementar todos los conocimientos adquiridos durante el desarrollo del curso para resolver apropiadamente los 2 escenarios propuestos.

### **2.2 OBJETIVOS ESPECÍFICOS**

- Identificar dispositivos y establecer la conexión de la red
- Inicializar los dispositivos y configurar los parámetros básicos de enrutamiento y seguridad.
- Aplicar los protocolos EIGRP y OSPF según corresponda o solicite.
- Implementar el uso de NAT y DHCP en los dispositivos
- Implementar y gestionar el uso de VLANS
- Configurar la restricción de los equipos a través de la implementación de ACL (listas de control de acceso)
- Cumplir con lo solicitado en materia de conectividad en los diferentes puntos de la red.

### 3. DESARROLLO DEL PROYECTO

Durante el desarrollo de los dos escenarios se puede evidenciar la importancia que tiene saber distribuir la red de manera eficiente, aplicando correctamente los protocolos de enrutamiento que garanticen la convergencia de la red y la implementación de la seguridad que en parte es dada por las contraseñas establecidas en cada dispositivo, pero se complementa con el uso eficiente de VLANs y Listas de control de acceso (ACL).

#### 3.1 Escenario 1

En este escenario se puede evidenciar la importancia del uso de protocolos de enrutamiento, para el caso EIGRP ya que facilita la convergencia de la red y disminuye el tráfico no deseado. De igual forma se puede apreciar como las listas de acceso proporcionan una regulación efectiva en la red.

#### Descripción del problema

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.

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.



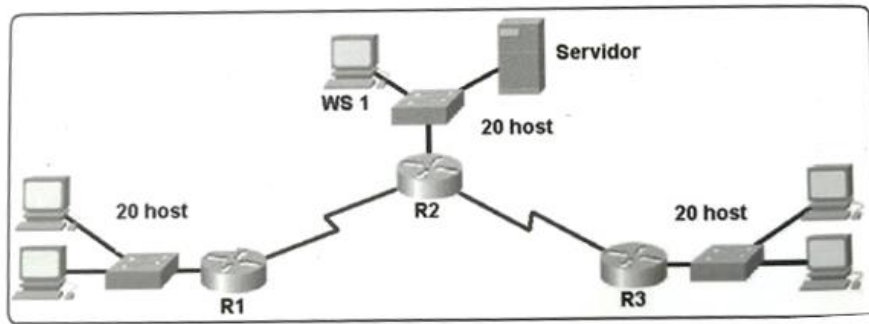


Figura 1. Diagrama de distribución de equipos

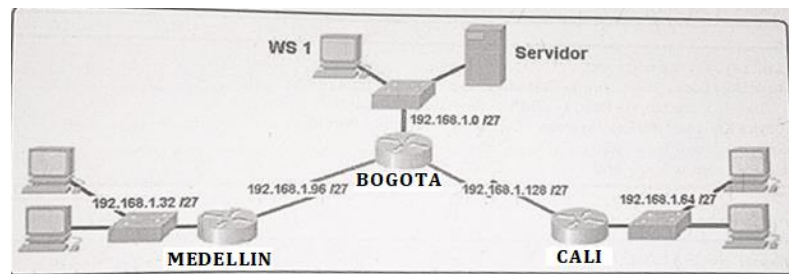


Figura 2. Esquema de red

## Desarrollo

Diagrama e interconexión de componentes utilizando herramienta packet tracer para simular la red solicitada.

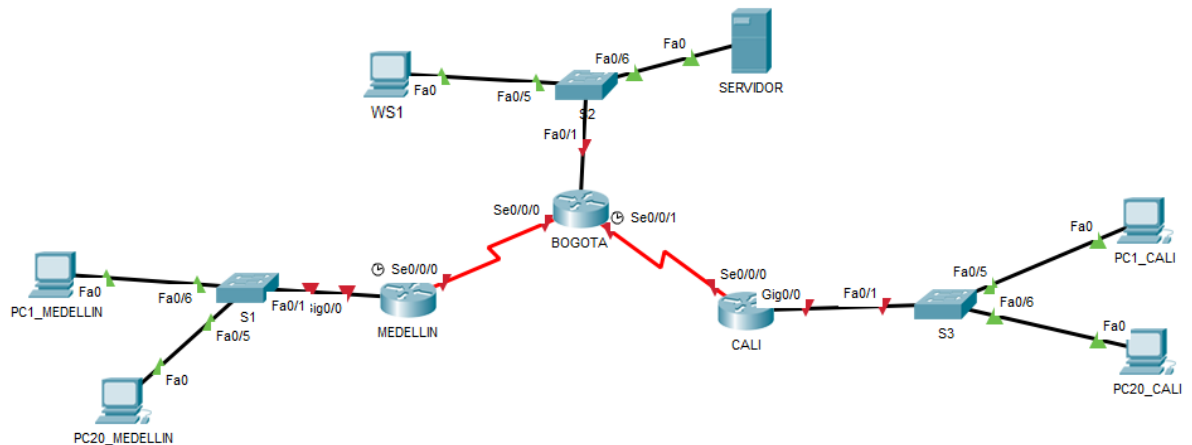


Figura 3. Diagrama de interconexión de componentes

### 3.1.1 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. Para el ejercicio tomaremos las primeras 5 subredes.

Sub N°	Subred	Rango de Host	Mascara	Broadcast
1	192.168.1.0	192.168.1.1-192.168.1.30	255.255.255.224	192.168.1.31
2	192.168.1.32	192.168.1.33-192.168.1.62	255.255.255.224	192.168.1.63
3	192.168.1.64	192.168.1.65-192.168.1.94	255.255.255.224	192.168.1.95
4	192.168.1.96	192.168.1.97-192.168.1.126	255.255.255.224	192.168.1.127
5	192.168.1.128	192.168.1.129-192.168.1.158	255.255.255.224	192.168.1.159
6	192.168.1.160	192.168.1.161-192.168.1.190	255.255.255.224	192.168.1.191
7	192.168.1.192	192.168.1.193-192.168.1.222	255.255.255.224	192.168.1.223
8	192.168.1.224	192.168.1.225-192.168.1.254	255.255.255.224	192.168.1.255

- b) Asignar una dirección IP a la red: Asignamos una de las subredes a cada tramo de la red.

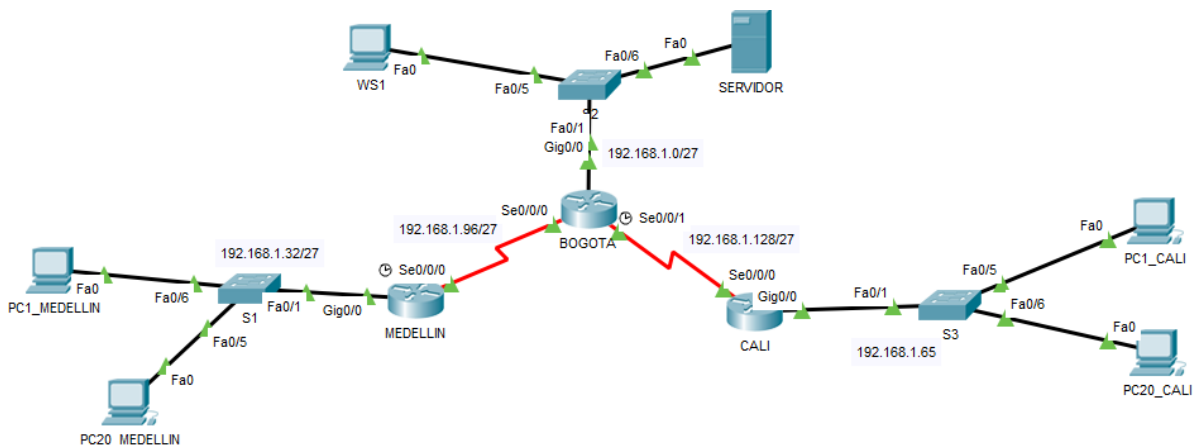


Figura 4 Asignación de direcciones IP

### 3.1.2 Configuración básica:

- a. Tabla de direccionamiento IP en base al modelo: En este paso se realiza la asignación del direccionamiento a la red para cada dispositivo e interfaz.

DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	MASCARA	GATEWAY
Router MEDELLIN	S0/0/0 DCE	192.168.1.97	255.255.255.224	
	G0/0	192.168.1.33	255.255.255.224	
Router BOGOTA	S0/0/0	192.168.1.98	255.255.255.224	
	S0/0/1 DCE	192.168.1.129	255.255.255.224	
	G0/0	192.168.1.1	255.255.255.224	
Router CALI	S0/0/0	192.168.1.130	255.255.255.224	
	G0/0	192.168.1.65	255.255.255.224	
PC1_MEDELLIN	FA0/1	192.168.1.34	255.255.255.224	192.168.1.33
PC20_MEDELLIN	FA0/1	192.168.1.53	255.255.255.224	192.168.1.33
WS1	FA0/1	192.168.1.2	255.255.255.224	192.168.1.1
SERVIDOR	FA0/1	192.168.1.21	255.255.255.224	192.168.1.1
PC1_CALI	FA0/1	192.168.1.66	255.255.255.224	192.168.1.65
PC20_CALI	FA0/1	192.168.1.85	255.255.255.224	192.168.1.65

- b. Configuración De Dispositivos: Se realiza la configuración lógica a los routers, switches y host de acuerdo con la tabla de direccionamiento y los parámetros de seguridad solicitados, de igual forma se valida tablas de enrutamiento y vecinos.

ROUTERS		
MEDELLIN	BOGOTA	CALI
no ip domain-lookup hostname MEDELLIN service password-encryption enable secret class banner motd %Prohibido el acceso no autorizado a este dispositivo% line con 0 password cisco login line vty 0 15	no ip domain-lookup hostname BOGOTA service password-encryption enable secret class banner motd %Prohibido el acceso no autorizado a este dispositivo% line con 0 password cisco login line vty 0 15	no ip domain-lookup hostname CALI service password-encryption enable secret class banner motd %Prohibido el acceso no autorizado a este dispositivo% line con 0 password cisco login line vty 0 15

<pre>password cisco loggin synchronous login exit interface g0/0 ip address 192.168.1.33 255.255.255.224 no sh interface S0/0/0 ip address 192.168.1.97 255.255.255.224 no sh exit exit copy running-config startup-config</pre>	<pre>password cisco loggin synchronous login exit interface g0/0 ip address 192.168.1.1 255.255.255.224 no sh interface S0/0/0 ip address 192.168.1.98 255.255.255.224 no sh interface S0/0/1 ip address 192.168.1.129 255.255.255.224 no sh exit exit copy running-config startup-config</pre>	<pre>password cisco loggin synchronous login exit interface g0/0 ip address 192.168.1.65 255.255.255.224 no sh interface S0/0/0 ip address 192.168.1.130 255.255.255.224 no sh exit exit copy running-config startup-config</pre>
--	---	---

<b>SWITCHES</b>		
<b>S1</b>	<b>S2</b>	<b>S3</b>
<pre>no ip domain-lookup hostname S1 service password- encryption enable secret class banner motd %Prohibido el acceso no autorizado a este dispositivo% line con 0 password cisco login loggin synchronous line vty 0 15 password cisco loggin synchronous login exit exit copy running-config startup-config</pre>	<pre>no ip domain-lookup hostname S2 service password- encryption enable secret class banner motd %Prohibido el acceso no autorizado a este dispositivo% line con 0 password cisco login loggin synchronous line vty 0 15 password cisco loggin synchronous login exit exit copy running-config startup-config</pre>	<pre>no ip domain-lookup hostname SbuBUCARAMANGA service password- encryption enable secret class banner motd %Prohibido el acceso no autorizado a este dispositivo% line con 0 password cisco login loggin synchronous line vty 0 15 password cisco loggin synchronous login exit exit copy running-config startup-config</pre>

## Configuración de Host

The image shows two Packet Tracer PC windows. The left window is titled 'PC1\_MEDELLIN' and the right is 'PC20\_MEDELLIN'. Both windows have the 'Desktop' tab selected, showing a 'Command Prompt' window. The Command Prompt in both windows displays the output of the 'ipconfig /all' command, showing network configuration details for the 'FastEthernet0' interface.

```

PC1_MEDELLIN Command Prompt:
Default Gateway.....: 0.0.0.0
C:\>ipconfig /all
FastEthernet0 Connection: (default port)
Connection-specific DNS Suffix...:
Physical Address.....: 0001.424D.2EE2
Link-local IPv6 Address.....: FE80::201:42FF:FE4D:2EE2
IP Address.....: 192.168.1.34
Subnet Mask.....: 255.255.255.224
Default Gateway.....: 192.168.1.33
DNS Servers.....: 0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 Client DUID.....: 00-01-00-01-82-82-A9-4E-00-01-42-4D-2E-E2

PC20_MEDELLIN Command Prompt:
Packet Tracer PC Command Line 1.0
C:\>ipconfig /all
FastEthernet0 Connection: (default port)
Connection-specific DNS Suffix...:
Physical Address.....: 0009.7CA0.D8B2
Link-local IPv6 Address.....: FE80::209:7CFF:FEA0:D8B2
IP Address.....: 192.168.1.53
Subnet Mask.....: 255.255.255.224
Default Gateway.....: 192.168.1.33
DNS Servers.....: 0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 Client DUID.....: 00-01-00-01-BC-E8-E3-B4-00-09-7C-A0-D8-B2
  
```

Figura 5 Configuración IP equipos de Medellín

The image shows two Packet Tracer windows. The left window is titled 'WS1' and the right is 'SERVIDOR'. Both windows have the 'Desktop' tab selected, showing a 'Command Prompt' window. The Command Prompt in both windows displays the output of the 'ipconfig /all' command, showing network configuration details for the 'FastEthernet0' interface.

```

WS1 Command Prompt:
Packet Tracer PC Command Line 1.0
C:\>ipconfig /all
FastEthernet0 Connection: (default port)
Connection-specific DNS Suffix...:
Physical Address.....: 00E0.F775.BCED
Link-local IPv6 Address.....: FE80::2E0:F7FF:FE75:BCED
IP Address.....: 192.168.1.2
Subnet Mask.....: 255.255.255.224
Default Gateway.....: 192.168.1.1
DNS Servers.....: 0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 Client DUID.....: 00-01-00-01-0E-42-77-D1-00-E0-F7-75-BC-ED

SERVIDOR Command Prompt:
Packet Tracer SERVER Command Line 1.0
C:\>ipconfig /all
FastEthernet0 Connection: (default port)
Connection-specific DNS Suffix...:
Physical Address.....: 00D0.D3E8.9C39
Link-local IPv6 Address.....: FE80::2D0:D3FF:FE88:9C39
IP Address.....: 192.168.1.21
Subnet Mask.....: 255.255.255.224
Default Gateway.....: 192.168.1.1
DNS Servers.....: 0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 Client DUID.....: 00-01-00-01-8D-43-21-D7-00-D0-D3-E8-9C-39
  
```

Figura 6 Configuración IP WS1 y Servidor

The image shows two Packet Tracer PC windows. The left window is titled 'PC1\_CALI' and the right is 'PC20\_CALI'. Both windows have the 'Desktop' tab selected, showing a 'Command Prompt' window. The Command Prompt in both windows displays the output of the 'ipconfig /all' command, showing network configuration details for the 'FastEthernet0' interface.

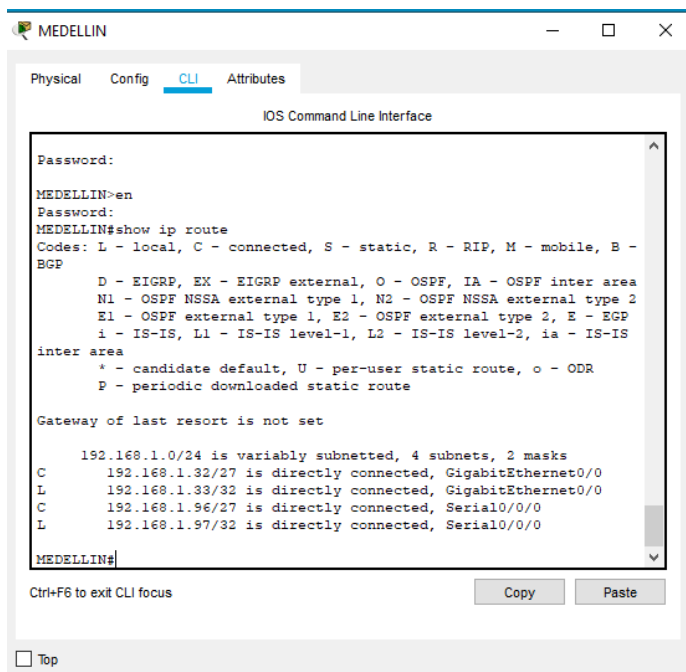
```

PC1_CALI Command Prompt:
Packet Tracer PC Command Line 1.0
C:\>ipconfig /all
FastEthernet0 Connection: (default port)
Connection-specific DNS Suffix...:
Physical Address.....: 000C.CFAD.CBA4
Link-local IPv6 Address.....: FE80::20C:CFFF:FEAD:CBA4
IP Address.....: 192.168.1.66
Subnet Mask.....: 255.255.255.224
Default Gateway.....: 192.168.1.65
DNS Servers.....: 0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 Client DUID.....: 00-01-00-01-03-52-E6-3E-00-0C-CF-AD-CB-A4

PC20_CALI Command Prompt:
Packet Tracer PC Command Line 1.0
C:\>ipconfig /all
FastEthernet0 Connection: (default port)
Connection-specific DNS Suffix...:
Physical Address.....: 0030.A339.4B1C
Link-local IPv6 Address.....: FE80::230:A3FF:FE39:4B1C
IP Address.....: 192.168.1.95
Subnet Mask.....: 255.255.255.224
Default Gateway.....: 192.168.1.65
DNS Servers.....: 0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 Client DUID.....: 00-01-00-01-12-B7-A9-A9-00-30-A3-39-4B-1C
  
```

Figura 7 Configuración IP equipos de Cali

- c. Revisión tablas de enrutamiento y balanceo: Se realiza la revisión de las tablas de enrutamiento de los routers así como validación entre dispositivos vecinos.

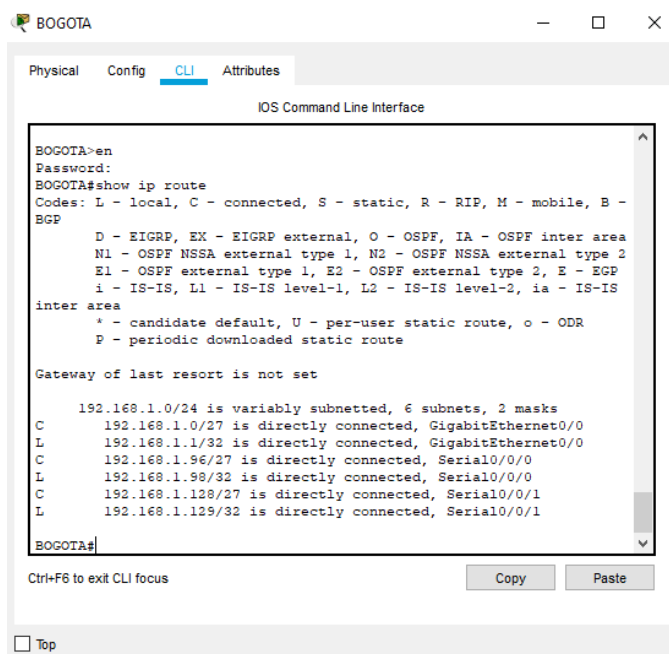


```
MEDELLIN#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C       192.168.1.32/27 is directly connected, GigabitEthernet0/0
L       192.168.1.33/32 is directly connected, GigabitEthernet0/0
C       192.168.1.96/27 is directly connected, Serial0/0/0
L       192.168.1.97/32 is directly connected, Serial0/0/0
MEDELLIN#
```

Figura 8 Tabla de enrutamiento router Medellín



```
BOGOTA#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.1.0/24 is variably subnetted, 6 subnets, 2 masks
C       192.168.1.0/27 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
C       192.168.1.96/27 is directly connected, Serial0/0/0
L       192.168.1.98/32 is directly connected, Serial0/0/0
C       192.168.1.128/27 is directly connected, Serial0/0/1
L       192.168.1.129/32 is directly connected, Serial0/0/1
BOGOTA#
```

Figura 9 Tabla de enrutamiento router Bogotá

```

IOS Command Line Interface
Prohibido el acceso no autorizado a este dispositivo
User Access Verification
Password:
CALI>en
Password:
CALI#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C       192.168.1.64/27 is directly connected, GigabitEthernet0/0
L       192.168.1.65/32 is directly connected, GigabitEthernet0/0
C       192.168.1.128/27 is directly connected, Serial0/0/0
L       192.168.1.130/32 is directly connected, Serial0/0/0
CALI#

```

Figura 10 Tabla de enrutamiento router Cali

- d. Diagnóstico de vecinos con el comando cdp: En este paso podemos validar los dispositivos vecinos a cada router

```

IOS Command Line Interface
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C       192.168.1.64/27 is directly connected, GigabitEthernet0/0
L       192.168.1.65/32 is directly connected, GigabitEthernet0/0
C       192.168.1.128/27 is directly connected, Serial0/0/0
L       192.168.1.130/32 is directly connected, Serial0/0/0

CALI#show cdp ne
CALI#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge
                S - Switch, H - Host, I - IGMP, r - Repeater, P -
Phone
Device ID    Local Intrfce  Holdtme    Capability  Platform  Port
ID
BOGOTA      Ser 0/0/0      142        R           C1900     Ser
0/0/1
S3          Gig 0/0        142        S           2960     Fas
0/1
CALI#

```

Figura 11 Revisión de vecinos router Cali

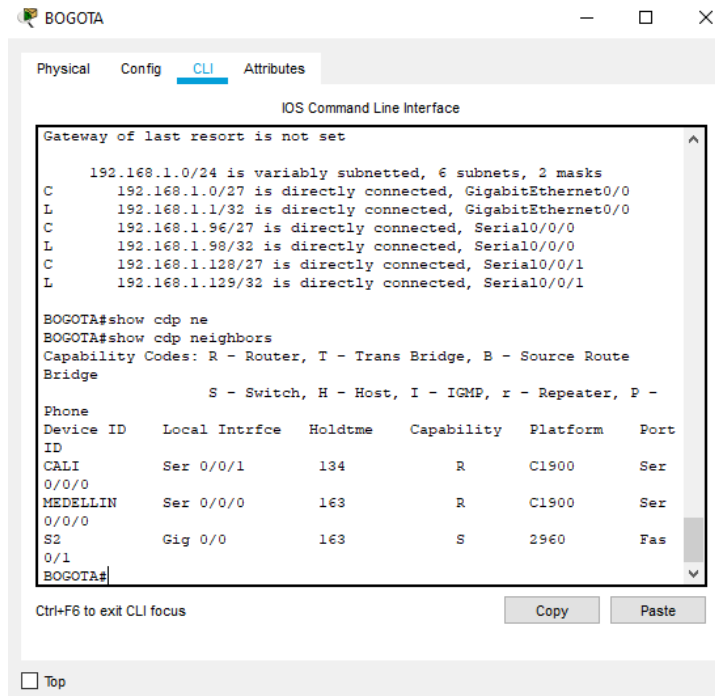


Figura 12 Revisión de vecinos router Bogotá

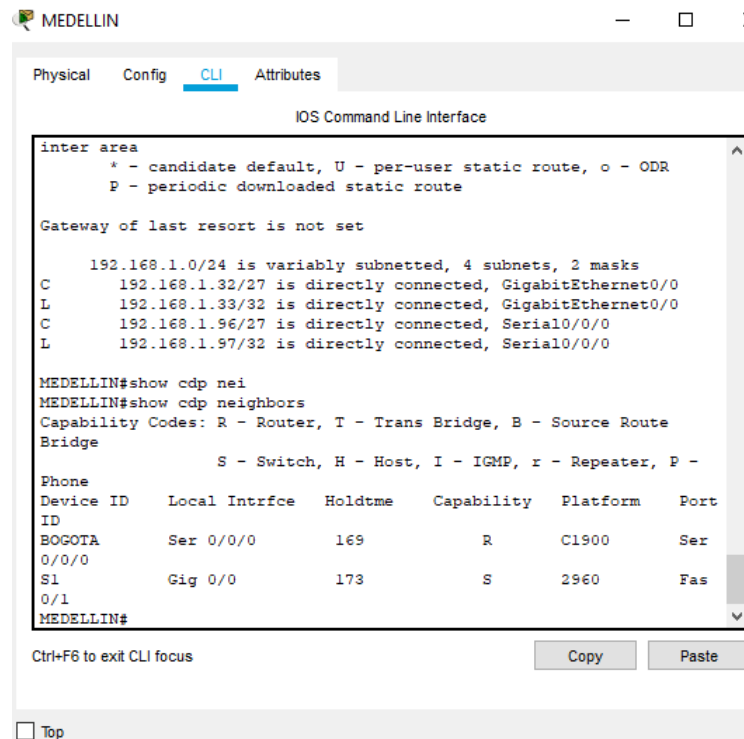


Figura 13 Revisión de vecinos router Medellín



- e. Validación de conectividad en cada tramo de la red: Se realiza prueba ping a las subredes de Medellín Bogotá y Cali para probar conectividad, pero aún los equipos no tienen acceso a redes externas debido a que los routers no tienen cargadas las rutas en las tablas de enrutamiento.

```
PC1_MEDALLIN
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
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=1ms TTL=255
Reply from 192.168.1.33: bytes=32 time=1ms TTL=255
Reply from 192.168.1.33: bytes=32 time=1ms TTL=255
Reply from 192.168.1.33: bytes=32 time=1ms TTL=255
Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 192.168.1.21
Pinging 192.168.1.21 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Ping statistics for 192.168.1.21:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.1.66
Pinging 192.168.1.66 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.1.98
Pinging 192.168.1.98 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.98:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

SERVIDOR
Physical Config Services Desktop Programming Attributes
Command Prompt
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.1.66
Pinging 192.168.1.66 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.1.34
Pinging 192.168.1.34 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>192.168.1.2
Invalid Command.
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=2ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
```

Figura 14 Pruebas ping Host a diferentes tramos de la red

```

MEDELLIN
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up
MEDELLIN#ping 192.168.1.98
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.98, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
MEDELLIN#ping 192.168.1.34
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.34, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/4/18 ms
MEDELLIN#ping 192.168.1.21
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.21, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
MEDELLIN#ping 192.168.1.66
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.66, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
MEDELLIN#

CALI
IOS Command Line Interface
state to up
CALI#ping 192.168.1.66
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.66, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms
CALI#ping 192.168.1.129
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.129, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/20 ms
CALI#ping 192.168.1.34
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.34, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
CALI#ping 192.168.1.21
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.21, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
CALI#

```

Figura 15 Pruebas Ping router Medellín y Cali

```

BOGOTA
IOS Command Line Interface
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.129, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/7 ms
BOGOTA#ping 192.168.1.21
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.21, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms
BOGOTA#ping 192.168.1.34
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.34, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
BOGOTA#ping 192.168.1.66
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.66, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
BOGOTA#

```

Figura 16 Pruebas Ping router Bogotá

### 3.1.3 Configuración de enrutamiento

- a. Configuración EIGRP: Para que los dispositivos de capa 3 puedan tener un conocimiento amplio de la red se procede a configurar el protocolo EIGRP con el que se podrán compartir entre sí las tablas de enrutamiento y por tanto se tendrá acceso entre todos los dispositivos de la red

ROUTER		
MEDELLIN	BOGOTA	CALI
<pre>router eigrp 200 network 192.168.1.32 0.0.0.31 network 192.168.1.96 0.0.0.31 no auto-summary passive-interface g0/0 exit exit copy running-config startup-config</pre>	<pre>router eigrp 200 network 192.168.1.97 0.0.0.31 network 192.168.1.128 0.0.0.31 network 192.168.1.0 0.0.0.31 no auto-summary passive-interface g0/0 exit exit copy running-config startup- config</pre>	<pre>router eigrp 200 network 192.168.1.129 0.0.0.31 network 192.168.1.64 0.0.0.31 no auto-summary passive-interface g0/0 exit exit copy running-config startup- config</pre>

- b. Verificación de dispositivos vecinos con EIGRP: En esta oportunidad se ejecuta el comando `show ip EIGRP neighbors` para conocer los dispositivos vecinos que operan bajo el protocolo EIGRP. Dicho comando se aplica para los 3 routers en donde se evidencia que están correctamente configurados con EIGRP

```
MEDELLIN#sh ip ei nei
IP-EIGRP neighbors for process 200
H   Address           Interface           Hold Uptime       SRTT   RTO   Q   Seq
                               (sec)  (ms)              (ms)   (ms)  Cnt  Num
0   192.168.1.98       Se0/0/0             12    00:10:15    40    1000  0   5
MEDELLIN#
```

Figura 17 Dispositivos vecinos router Medellín

BOGOTA

Physical Config **CLI** Attributes

IOS Command Line Interface

```

BOGOTA#show ip ei nei
IP-EIGRP neighbors for process 200
H   Address          Interface          Hold Uptime      SRTT   RTO   Q   Seq
                               (sec)            (ms)            Cnt   Num
0   192.168.1.97      Se0/0/0           11  00:11:22  40    1000  0   7
1   192.168.1.130    Se0/0/1           11  00:10:52  40    1000  0   7

```

Figura 18 Dispositivos vecinos router Bogotá

CALI

Physical Config **CLI** Attributes

IOS Command Line Interface

```

CALI#sh ip ei nei
IP-EIGRP neighbors for process 200
H   Address          Interface          Hold Uptime      SRTT   RTO   Q
Seq
                               (sec)            (ms)            Cnt
Num
0   192.168.1.129    Se0/0/0           11  00:11:37  40    1000  0   6

```

Figura 19 Dispositivos vecinos router Cali

- c. Tablas de enrutamiento luego de aplicar el protocolo EIGRP: Se realiza la verificación de tablas de enrutamiento en donde se puede verificar que los routers ya tienen un conocimiento amplio de la red y por tanto hay comunicación entre todos los hosts.

```

Physical  Config  CLI  Attributes
IOS Command Line Interface
MEDELLIN#show ip eigrp topology
IP-EIGRP Topology Table for AS 200/ID(192.168.1.97)

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

P 192.168.1.0/27, 1 successors, FD is 2172416
   via 192.168.1.98 (2172416/5120), Serial0/0/0
P 192.168.1.32/27, 1 successors, FD is 5120
   via Connected, GigabitEthernet0/0
P 192.168.1.64/27, 1 successors, FD is 2684416
   via 192.168.1.98 (2684416/2172416), Serial0/0/0
P 192.168.1.96/27, 1 successors, FD is 2169856
   via Connected, Serial0/0/0
P 192.168.1.128/27, 1 successors, FD is 2681856
   via 192.168.1.98 (2681856/2169856), Serial0/0/0
MEDELLIN#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D    192.168.1.0/27 [90/2172416] via 192.168.1.98, 00:03:29, Serial0/0/0
C    192.168.1.32/27 is directly connected, GigabitEthernet0/0
L    192.168.1.33/32 is directly connected, GigabitEthernet0/0
D    192.168.1.64/27 [90/2684416] via 192.168.1.98, 00:03:00, Serial0/0/0
C    192.168.1.96/27 is directly connected, Serial0/0/0
L    192.168.1.97/32 is directly connected, Serial0/0/0
D    192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:03:29, Serial0/0/0
MEDELLIN#

```

Figura 20 Tabla de enrutamiento EIGRP Medellín

```

BOGOTA
Physical Config CLI Attributes
IOS Command Line Interface
BOGOTA#show ip eigrp topology
IP-EIGRP Topology Table for AS 200/ID(192.168.1.129)

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

P 192.168.1.0/27, 1 successors, FD is 5120
   via Connected, GigabitEthernet0/0
P 192.168.1.32/27, 1 successors, FD is 2172416
   via 192.168.1.97 (2172416/5120), Serial0/0/0
P 192.168.1.64/27, 1 successors, FD is 2172416
   via 192.168.1.130 (2172416/5120), Serial0/0/1
P 192.168.1.96/27, 1 successors, FD is 2169856
   via Connected, Serial0/0/0
P 192.168.1.128/27, 1 successors, FD is 2169856
   via Connected, Serial0/0/1

BOGOTA#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
C    192.168.1.0/27 is directly connected, GigabitEthernet0/0
L    192.168.1.1/32 is directly connected, GigabitEthernet0/0
D    192.168.1.32/27 [90/2172416] via 192.168.1.97, 00:05:30, Serial0/0/0
D    192.168.1.64/27 [90/2172416] via 192.168.1.130, 00:05:01, Serial0/0/1
C    192.168.1.96/27 is directly connected, Serial0/0/0
L    192.168.1.98/32 is directly connected, Serial0/0/0
C    192.168.1.128/27 is directly connected, Serial0/0/1
L    192.168.1.129/32 is directly connected, Serial0/0/1

```

Figura 21 Tabla de enrutamiento EIGRP Bogotá

```

CALI
Physical Config CLI Attributes
IOS Command Line Interface
CALI#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D    192.168.1.0/27 [90/2172416] via 192.168.1.129, 00:06:17, Serial0/0/0
D    192.168.1.32/27 [90/2684416] via 192.168.1.129, 00:06:17, Serial0/0/0
C    192.168.1.64/27 is directly connected, GigabitEthernet0/0
L    192.168.1.65/32 is directly connected, GigabitEthernet0/0
D    192.168.1.96/27 [90/2681856] via 192.168.1.129, 00:06:17, Serial0/0/0
C    192.168.1.128/27 is directly connected, Serial0/0/0
L    192.168.1.130/32 is directly connected, Serial0/0/0

CALI#show eig
CALI#show ip ei
CALI#show ip eigrp to
CALI#show ip eigrp topology
IP-EIGRP Topology Table for AS 200/ID(192.168.1.130)

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

P 192.168.1.0/27, 1 successors, FD is 2172416
   via 192.168.1.129 (2172416/5120), Serial0/0/0
P 192.168.1.32/27, 1 successors, FD is 2684416
   via 192.168.1.129 (2684416/2172416), Serial0/0/0
P 192.168.1.64/27, 1 successors, FD is 5120
   via Connected, GigabitEthernet0/0
P 192.168.1.96/27, 1 successors, FD is 2681856
   via 192.168.1.129 (2681856/2169856), Serial0/0/0
P 192.168.1.128/27, 1 successors, FD is 2169856
   via Connected, Serial0/0/0

CALI#show ip route ei
CALI#show ip route eigrp
192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D    192.168.1.0/27 [90/2172416] via 192.168.1.129, 00:06:53, Serial0/0/0
D    192.168.1.32/27 [90/2684416] via 192.168.1.129, 00:06:53, Serial0/0/0
D    192.168.1.96/27 [90/2681856] via 192.168.1.129, 00:06:53, Serial0/0/0

```

Figura 22 Tabla de enrutamiento EIGRP Cali

### 3.1.4 Configuración de las listas de acceso

Se procede a establecer las listas de control de acceso para limitar la conexión entre dispositivos que no deben comunicarse o poseen restricción.

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

DISPOSITIVO	ACL
<b>MEDELLIN</b>	<pre>ip access-list extended SoloServidor permit ip 192.168.1.32 0.0.0.31 192.168.1.0 0.0.0.31 permit tcp 192.168.1.32 0.0.0.31 any eq 23 permit ip 192.168.1.32 0.0.0.31 192.168.1.96 0.0.0.31 permit ip 192.168.1.32 0.0.0.31 192.168.1.32 0.0.0.31 permit ip 192.168.1.32 0.0.0.31 192.168.1.128 0.0.0.31 exit interface g0/0 ip access-group SoloServidor in</pre>
<b>CALI</b>	<pre>ip access-list extended SoloServidorCali permit ip 192.168.1.64 0.0.0.31 192.168.1.0 0.0.0.31 permit tcp 192.168.1.64 0.0.0.31 any eq 23 permit ip 192.168.1.64 0.0.0.31 192.168.1.64 0.0.0.31 permit ip 192.168.1.64 0.0.0.31 192.168.1.128 0.0.0.31 permit ip 192.168.1.64 0.0.0.31 192.168.1.96 0.0.0.31 exit interface g0/0 ip access-group SoloServidorCali in</pre>
<b>BOGOTA</b>	<pre>ip access-list extended AclBogota permit icmp host 192.168.1.21 any echo permit icmp host 192.168.1.21 any echo-reply permit tcp 192.168.1.0 0.0.0.31 any eq 23 permit ip 192.168.1.0 0.0.0.31 192.168.1.0 0.0.0.31 permit ip 192.168.1.0 0.0.0.31 192.168.1.96 0.0.0.31 permit ip 192.168.1.0 0.0.0.31 192.168.1.128 0.0.0.31 exit interface g0/0</pre>

	ip access-group AclBogota in
--	------------------------------

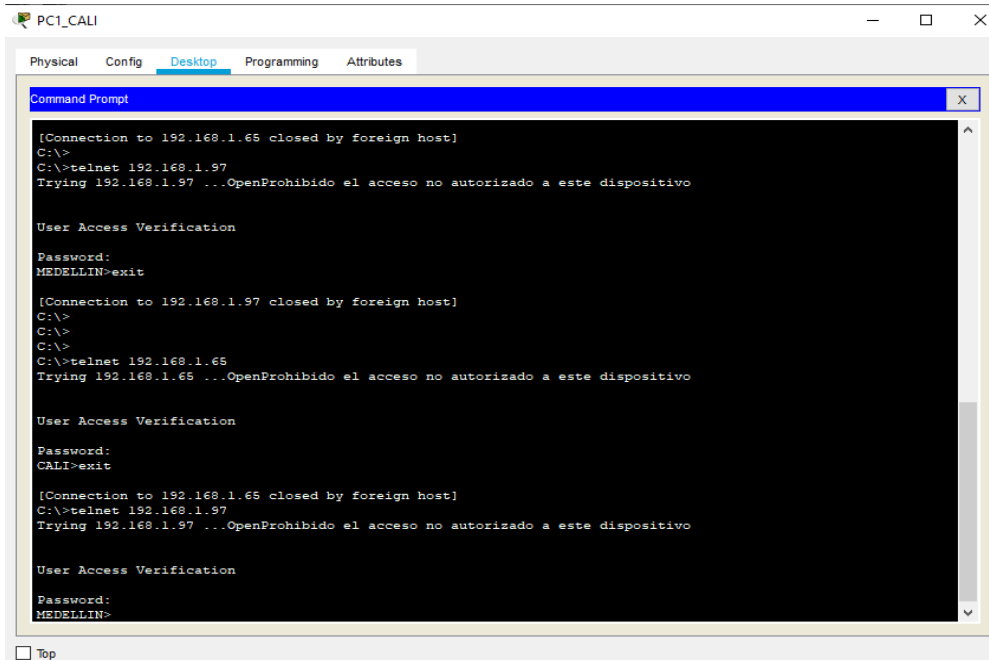
### 3.1.5 Comprobación de la red instalada

En esta etapa se realizan las pruebas registradas en la siguiente tabla con su respectivo resultado.

	ORIGEN	DESTINO	RESULTADO
<b>TELNET</b>	LAN del Router CALI	Router CALI	Exitoso
	LAN del Router CALI	Router MEDELLIN	Exitoso
	LAN del Router MEDELLIN	Router CALI	Exitoso
	LAN del Router MEDELLIN	Router MEDELLIN	Exitoso
<b>TELNET</b>	Router MEDELLIN	Router CALI	Exitoso
	Servidor	Router CALI	Exitoso
	Servidor	Router MEDELLIN	Exitoso
	WS_1	Router BOGOTA	Exitoso
<b>PING</b>	LAN del Router CALI	WS_1	Fallido
	LAN del Router CALI	Servidor	Exitoso
	LAN del Router MEDELLIN	WS_1	Fallido
<b>PING</b>	LAN del Router MEDELLIN	LAN del Router CALI	Fallido
	LAN del Router MEDELLIN	Servidor	Exitoso
	Router CALI	LAN del Router MEDELLIN	Exitoso
	Servidor	LAN del Router MEDELLIN	Exitoso
	Servidor	LAN del Router CALI	Exitoso
	LAN del Router CALI	WS_1	Fallido



## Evidencias de la comprobación



```
PC1_CALI
Physical Config Desktop Programming Attributes
Command Prompt
[Connection to 192.168.1.65 closed by foreign host]
C:\>
C:\>telnet 192.168.1.97
Trying 192.168.1.97 ...OpenProhibido el acceso no autorizado a este dispositivo

User Access Verification
Password:
MEDELLIN>exit

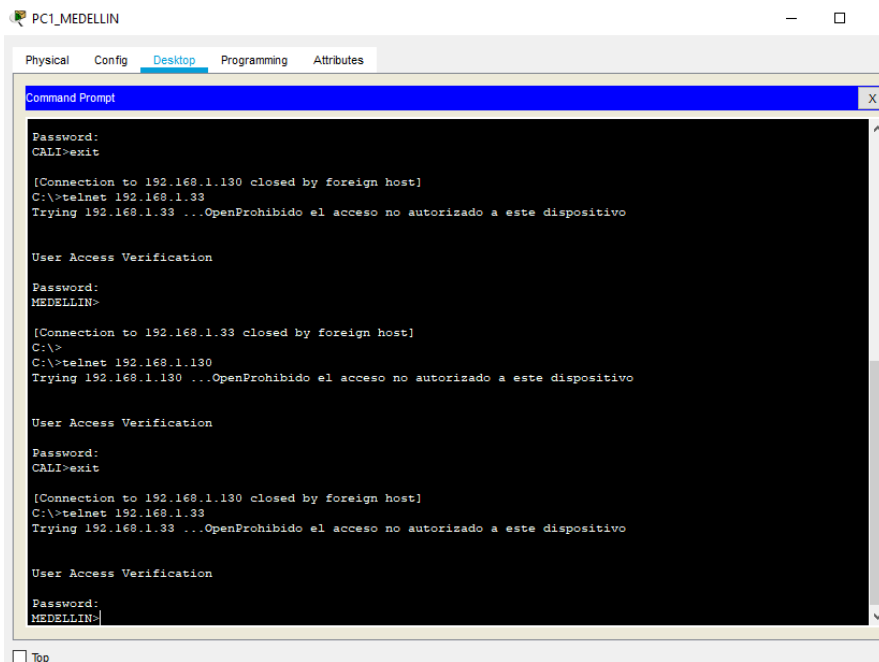
[Connection to 192.168.1.97 closed by foreign host]
C:\>
C:\>
C:\>telnet 192.168.1.65
Trying 192.168.1.65 ...OpenProhibido el acceso no autorizado a este dispositivo

User Access Verification
Password:
CALI>exit

[Connection to 192.168.1.65 closed by foreign host]
C:\>telnet 192.168.1.97
Trying 192.168.1.97 ...OpenProhibido el acceso no autorizado a este dispositivo

User Access Verification
Password:
MEDELLIN>
```

Figura 23 Telnet LAN de Cali al router de Cali y Medellín



```
PC1_MEDELLIN
Physical Config Desktop Programming Attributes
Command Prompt
Password:
CALI>exit

[Connection to 192.168.1.130 closed by foreign host]
C:\>telnet 192.168.1.33
Trying 192.168.1.33 ...OpenProhibido el acceso no autorizado a este dispositivo

User Access Verification
Password:
MEDELLIN>

[Connection to 192.168.1.33 closed by foreign host]
C:\>
C:\>telnet 192.168.1.130
Trying 192.168.1.130 ...OpenProhibido el acceso no autorizado a este dispositivo

User Access Verification
Password:
CALI>exit

[Connection to 192.168.1.130 closed by foreign host]
C:\>telnet 192.168.1.33
Trying 192.168.1.33 ...OpenProhibido el acceso no autorizado a este dispositivo

User Access Verification
Password:
MEDELLIN>
```

Figura 24 Telnet LAN Medellín al router de Cali y Medellín

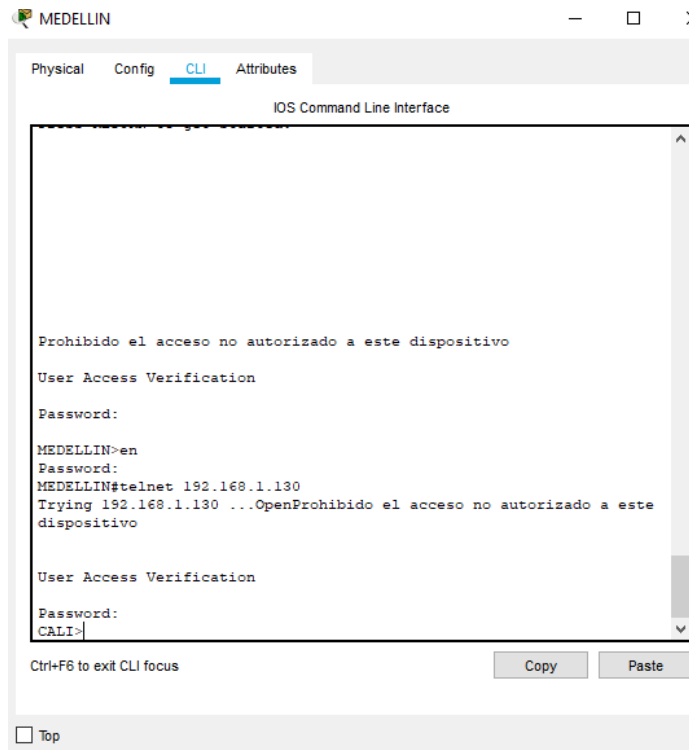


Figura 25 Telnet router de Medellín al router de Cali

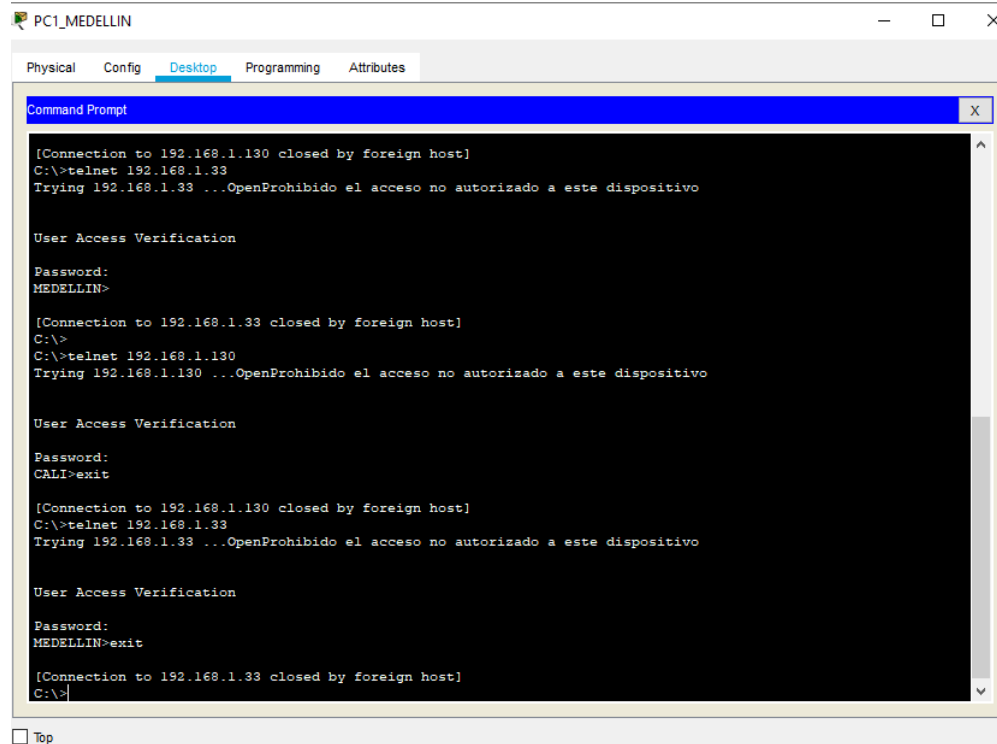


Figura 26 Telnet Servidor al router de Cali y Medellín

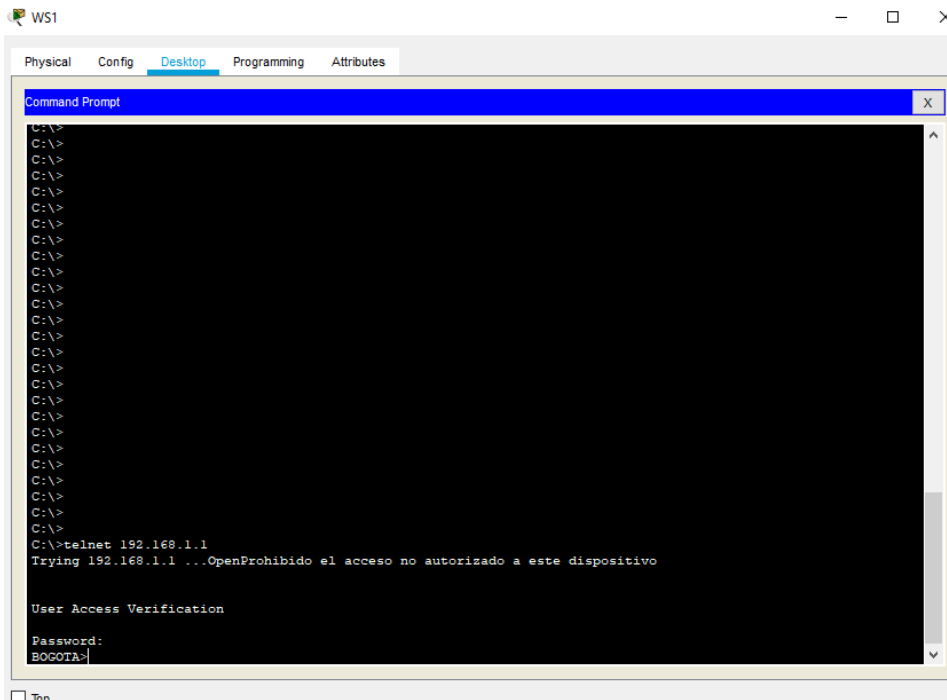


Figura 27 Telnet WS1 al router de Bogotá

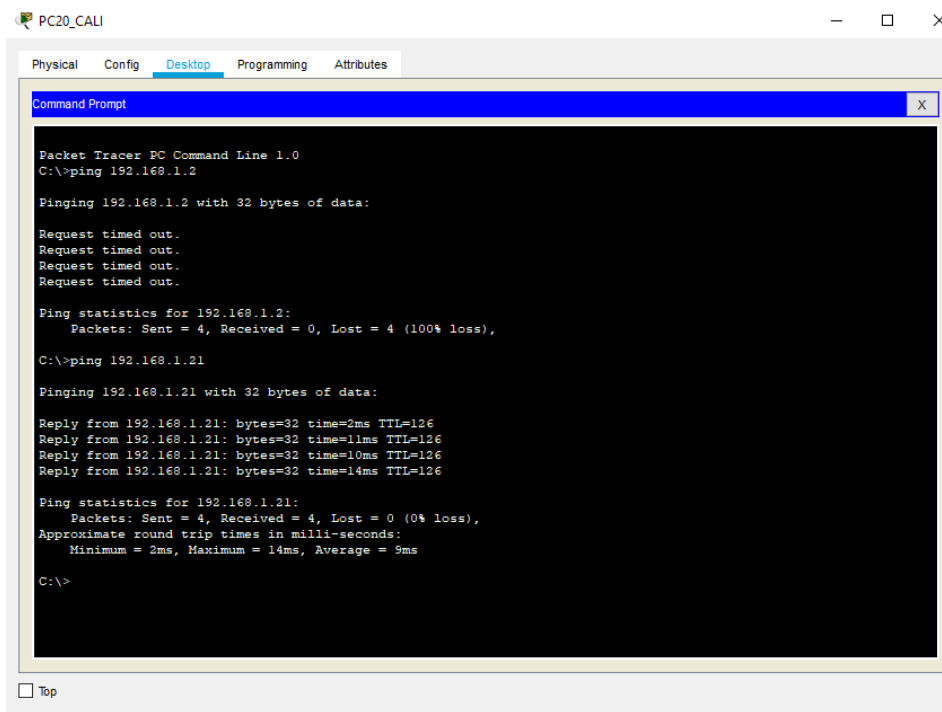


Figura 28 Ping WS1 y Servidor desde LAN Cali

```
PC20_MEDELLIN
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.1.21
Pinging 192.168.1.21 with 32 bytes of data:
Reply from 192.168.1.21: bytes=32 time=1ms TTL=126
Reply from 192.168.1.21: bytes=32 time=19ms TTL=126
Reply from 192.168.1.21: bytes=32 time=1ms TTL=126
Reply from 192.168.1.21: bytes=32 time=13ms TTL=126
Ping statistics for 192.168.1.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 19ms, Average = 8ms
C:\>ping 192.168.1.66
Pinging 192.168.1.66 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

Figura 29 Ping LAN Medellin al WS1, Servidor y LAN de Cali

```
CALI
Physical Config CLI Attributes
IOS Command Line Interface
Password:
CALI>en
Password:
CALI#ping 192.168.1.34
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.34, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/10/15 ms
CALI#ping 192.168.1.33
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.33, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/4/11 ms
CALI#ping 192.168.1.53
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.53, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/13 ms
CALI#
Ctrl+F6 to exit CLI focus
Copy Paste
Top
```

Figura 30 Ping router de Cali a la LAN de Medellín

```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.1.34

Pinging 192.168.1.34 with 32 bytes of data:

Reply from 192.168.1.34: bytes=32 time=1ms TTL=126
Reply from 192.168.1.34: bytes=32 time=13ms TTL=126
Reply from 192.168.1.34: bytes=32 time=16ms TTL=126
Reply from 192.168.1.34: bytes=32 time=26ms TTL=126

Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 26ms, Average = 13ms

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=2ms TTL=254
Reply from 192.168.1.33: bytes=32 time=1ms TTL=254
Reply from 192.168.1.33: bytes=32 time=1ms TTL=254
Reply from 192.168.1.33: bytes=32 time=1ms TTL=254

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 192.168.1.53

Pinging 192.168.1.53 with 32 bytes of data:

Reply from 192.168.1.53: bytes=32 time=1ms TTL=126
Reply from 192.168.1.53: bytes=32 time=6ms TTL=126
Reply from 192.168.1.53: bytes=32 time=11ms TTL=126
Reply from 192.168.1.53: bytes=32 time=18ms TTL=126

Ping statistics for 192.168.1.53:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 18ms, Average = 6ms

C:\>
```

Figura 31 Ping Servidor a la LAN de Medellín y Cali

```
PC20_CALI
Physical Config Desktop Programming Attributes

Command Prompt

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.21

Pinging 192.168.1.21 with 32 bytes of data:

Reply from 192.168.1.21: bytes=32 time=2ms TTL=126
Reply from 192.168.1.21: bytes=32 time=10ms TTL=126
Reply from 192.168.1.21: bytes=32 time=10ms TTL=126
Reply from 192.168.1.21: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 5ms

C:\>
```

Figura 32 Ping LAN de Calí al WS1 y al SERVIDOR

### 3.2 ESCENARIO 2

En este escenario se puede evidenciar la importancia del uso de protocolos de enrutamiento, para el caso OSPF, listas de control de acceso, seguridad con autenticación AAA, NAT y VLANs utilizando VLSM para optimizar el direccionamiento IP de la red.

#### Descripción del problema

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.

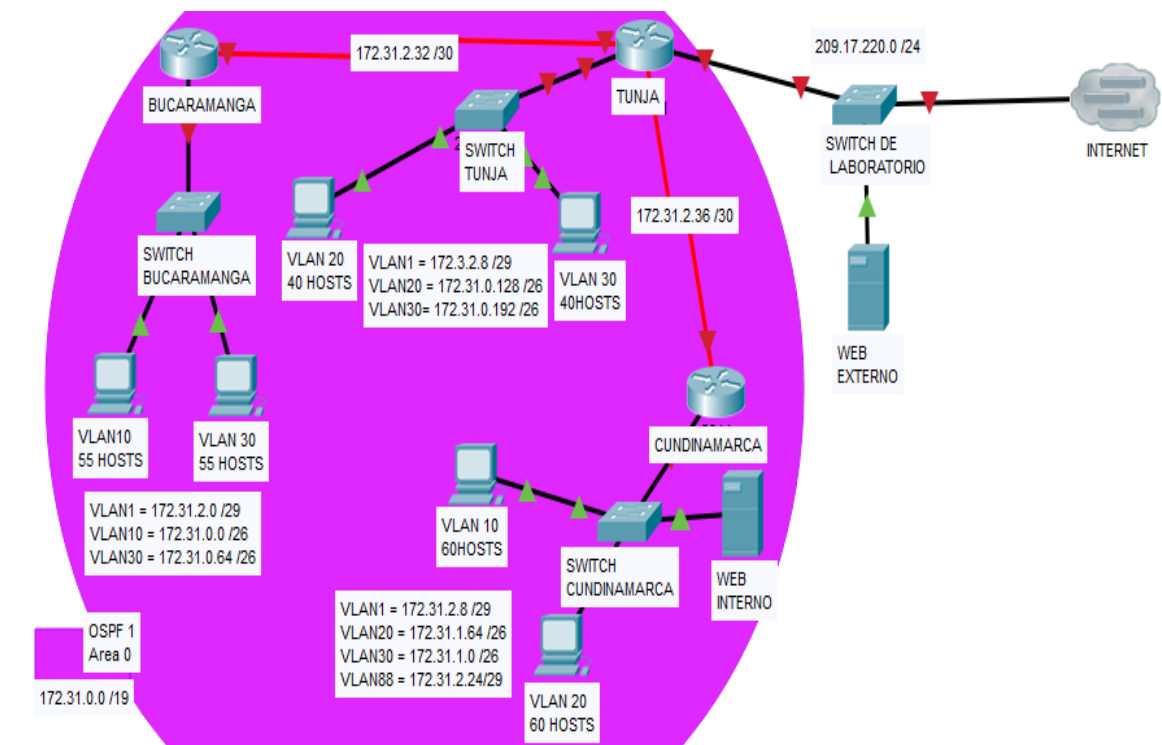


Figura 33 Diagrama escenario 2

Los siguientes son los requerimientos necesarios:

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

- Autenticación local con AAA.
  - Cifrado de contraseñas.
  - Un máximo de internos para acceder al router.
  - Máximo tiempo de acceso al detectar ataques.
  - Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.
2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca
  3. El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).
  4. El enrutamiento deberá tener autenticación.
  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.
    - 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.
    - 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.
    - Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.
    - Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen acceso a los routers e internet.
  6. VLSM: utilizar la dirección 172.31.0.0 /18 para el direccionamiento.

## Desarrollo de la actividad

### 3.2.1 Desarrollo del diagrama de red de la empresa.

Para el desarrollo del problema se agregó por VLAN un host adicional para probar conectividad.

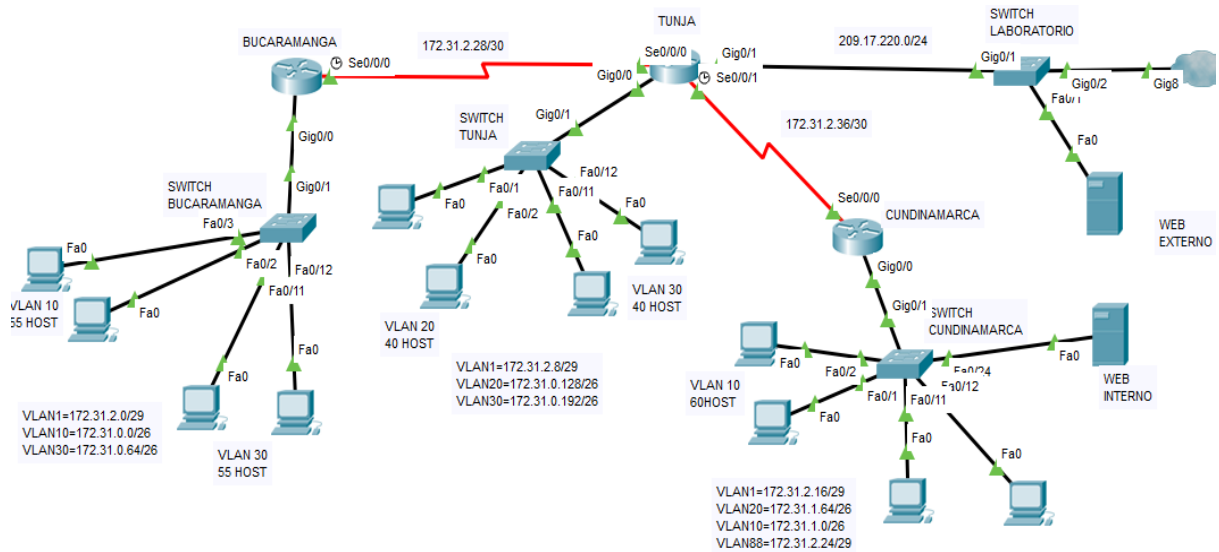


Figura 34 Esquema red empresarial escenario 2

### 3.2.2 Establecer el direccionamiento de los equipos en la red y las VLAN.

DISPOSITIVO	INTERFAZ	DIRECCIÓN IP	MASCARA	GATEWAY
<b>Router BUCARAMANGA</b>	S0/0/0 DCE	172.31.2.29	255.255.255.252	N/A
	G0/0.1	172.31.2.1	255.255.255.248	N/A
	G0/0.10	172.31.0.1	255.255.255.192	N/A
	G0/0.30	172.31.0.66	255.255.255.192	N/A
<b>Router TUNJA</b>	S0/0/0	172.31.2.30	255.255.255.252	N/A
	S0/0/1 DCE	172.31.2.37	255.255.255.252	N/A
	G0/1	209.17.220.1	255.255.255.0	N/A
	G0/0.1	172.31.2.9	255.255.255.248	N/A
	G0/0.20	172.31.0.129	255.255.255.192	N/A
	G0/0.30	172.31.0.193	255.255.255.192	N/A



<b>Router CUNDINAMARCA</b>	S0/0/0	172.31.2.38	255.255.255.252	N/A
	G0/0.1	172.31.2.17	255.255.255.248	N/A
	G0/0.10	172.31.1.1	255.255.255.192	N/A
	G0/0.20	172.31.1.65	255.255.255.192	N/A
	G0/0.88	172.31.2.25	255.255.255.248	N/A
<b>VLAN 1 BUCARAMANGA</b>		172.31.2.2	255.255.255.248	N/A
<b>VLAN 10 BUCARAMANGA</b>		172.31.0.2	255.255.255.192	N/A
<b>VLAN 30 BUCARAMANGA</b>		172.31.0.67	255.255.255.192	N/A
<b>VLAN 1 TUNJA</b>		172.31.2.10	255.255.255.248	N/A
<b>VLAN 20 TUNJA</b>		172.31.0.130	255.255.255.192	N/A
<b>VLAN 30 TUNJA</b>		172.31.0.194	255.255.255.192	N/A
<b>VLAN 1 CUNDINAMARCA</b>		172.31.2.18	255.255.255.248	N/A
<b>VLAN 10 CUNDINAMARCA</b>		172.31.1.0	255.255.255.192	N/A
<b>VLAN 20 CUNDINAMARCA</b>		172.31.1.64	255.255.255.192	N/A
<b>VLAN 88 CUNDINAMARCA</b>		172.31.2.24	255.255.255.248	N/A
<b>WEB EXTERNO</b>		209.17.220.253	255.255.255.0	209.17.220.1
<b>WEB INTERNO</b>		172.31.2.27	255.255.255.248	172.31.2.25

<b>VLANs BUCARAMANGA</b>				
<b>VLAN N°</b>	<b>Subred</b>	<b>Rango de Host</b>	<b>Mascara</b>	<b>Broadcast</b>
1	172.31.2.0	172.31.2.1-172.31.2.6	255.255.255.248	172.31.2.7
10	172.31.0.0	172.31.0.1-172.31.0.62	255.255.255.192	172.31.0.63
30	172.31.0.64	172.31.0.65-172.31.0.126	255.255.255.192	172.31.0.127

<b>VLANs TUNJA</b>				
<b>VLAN N°</b>	<b>Subred</b>	<b>Rango de Host</b>	<b>Mascara</b>	<b>Broadcast</b>
1	172.31.2.8	172.31.2.8-172.31.2.14	255.255.255.248	172.31.2.15
20	172.31.0.128	172.31.0.129-172.31.0.190	255.255.255.192	172.31.0.191
30	172.31.0.192	172.31.0.193-172.31.0.254	255.255.255.192	172.31.0.255

VLANs CUNDINAMARCA				
VLAN N°	Subred	Rango de Host	Mascara	Broadcast
1	172.31.2.16	172.31.2.17-172.31.2.22	255.255.255.248	172.31.2.23
10	172.31.1.0	172.31.1.1-172.31.1.62	255.255.255.192	172.31.1.63
20	172.31.1.64	172.31.1.65-172.31.1.126	255.255.255.192	172.31.1.127
88	172.31.2.24	172.31.2.25-172.31.2.30	255.255.255.248	172.31.2.31

### 3.2.3 Configuración de Switches y habilitación de las VLAN para permitir su enrutamiento

Se realiza la configuración de seguridad en cada dispositivo para proteger de accesos no autorizados y facilitar su gestión.

CONFIGURACIÓN DE SWITCH		
BUCARAMANGA	TUNJA	CUNDINAMARCA
no ip domain-lookup hostname SW_BUCARAMANGA service password- encryption enable secret class banner motd %Prohibido el acceso no autorizado a este dispositivo% line con 0 password cisco login loggin synchronous line vty 0 15 password cisco loggin synchronous login exit exit copy running-config startup- config	no ip domain-lookup hostname SW_TUNJA service password- encryption enable secret class banner motd %Prohibido el acceso no autorizado a este dispositivo% line con 0 password cisco login loggin synchronous line vty 0 15 password cisco loggin synchronous login exit exit copy running-config startup-config	interface vlan 20 ip address 172.31.0.130 255.255.255.192 no sh exit interface vlan 30 ip address 172.31.0.194 255.255.255.192 no sh interface vlan 1 no sh ip address 172.31.2.10 255.255.255.248 exit interface range fa 0/1-10 switchport access vlan 20 exit interface range fa 0/11-20 switchport access vlan 30 exit interface g0/1 switchport mode trunk exit exit copy running-config startup- config

Se realiza la configuración de las VLANs en los Switch de la red empresarial, se configura como troncal el puerto que conecta con el router de la ciudad para darle salida a la LAN y se configuran algunos segmentos de puertos a las diferentes VLANs para el desarrollo del problema.

<b>CONFIGURACIÓN DE VLANs</b>		
<b>BUCARAMANGA</b>	<b>TUNJA</b>	<b>CUNDINAMARCA</b>
<pre>interface vlan 10 ip address 172.31.0.2 255.255.255.192 no sh exit interface vlan 30 ip address 172.31.0.66 255.255.255.192 no sh interface vlan 1 ip address 172.31.2.2 255.255.255.248 no sh exit interface range fa 0/1-10 switchport access vlan 10 exit interface range fa 0/11-20 switchport access vlan 30 exit interface g0/1 switchport mode trunk exit exit copy running-config startup-config</pre>	<pre>interface vlan 20 ip address 172.31.0.130 255.255.255.192 no sh exit interface vlan 30 ip address 172.31.0.194 255.255.255.192 no sh interface vlan 1 no sh ip address 172.31.2.10 255.255.255.248 exit interface range fa 0/1-10 switchport access vlan 20 exit interface range fa 0/11-20 switchport access vlan 30 exit interface g0/1 switchport mode trunk exit exit copy running-config startup-config</pre>	<pre>interface vlan 20 ip address 172.31.1.66 255.255.255.192 no sh exit interface vlan 10 ip address 172.31.1.2 255.255.255.192 no sh interface vlan 1 ip address 172.31.2.18 255.255.255.248 no sh exit interface vlan 88 ip address 172.31.2.25 255.255.255.248 no sh exit interface range fa 0/1-10 switchport access vlan 10 exit interface range fa 0/11-20 switchport access vlan 20 exit interface range fa 0/23-24 switchport access vlan 88 exit interface g0/1 switchport mode trunk exit exit copy running-config startup- config</pre>

### 3.2.4 Configuración de puertos en los router y DHCP con el router de Tunja para las LAN de Bucaramanga y Cundinamarca.

En la presente etapa se configura el direccionamiento en los puertos de los routers y se habilita el broadcast DHCP dirigido al router de tunja en los dispositivos de las LAN de Bucaramanga y Cundinamarca con el comando:

Bucaramanga-> ip helper-address 172.31.2.30

Cundinamarca-> ip helper-address 172.31.2.37

La dirección IP varía de acuerdo con la interfaz por donde ingresa la solicitud de DHCP al router.

CONFIGURACIÓN DE ROUTERS		
BUARAMANGA	TUNJA	CUNDINAMARCA
<pre> int s0/0/0 ip address 172.31.2.29 255.255.255.252 exit Hostname Bucaramanga interface g0/0 ip helper-address 172.31.2.30 no sh exit interface g0/0.10 encapsulation dot1Q 10 ip address 172.31.0.1 255.255.255.192 ip helper-address 172.31.2.30 exit interface g0/0.30 encapsulation dot1Q 30 ip address 172.31.0.65 255.255.255.192 ip helper-address 172.31.2.30 exit interface g0/0.1 encapsulation dot1Q 1 ip address 172.31.2.1 255.255.255.248 </pre>	<pre> hostname TUNJA int s0/0/0 ip address 172.31.2.30 255.255.255.252 no sh int s0/0/1 ip address 172.31.2.37 255.255.255.252 no sh int g0/1 ip address 209.17.220.1 255.255.255.0 no sh int g0/0 no sh interface g0/0 no sh exit interface g0/0.20 encapsulation dot1Q 20 ip address 172.31.0.129 255.255.255.192 exit interface g0/0.30 encapsulation dot1Q 30 ip address 172.31.0.193 255.255.255.192 exit interface g0/0.1 </pre>	<pre> int s0/0/0 ip address 172.31.2.38 255.255.255.252 exit Hostname CUNDINAMARCA interface g0/0 ip helper-address 172.31.2.37 no sh exit interface g0/0.10 encapsulation dot1Q 10 ip address 172.31.1.1 255.255.255.192 ip helper-address 172.31.2.37 exit interface g0/0.20 encapsulation dot1Q 20 ip address 172.31.1.65 255.255.255.192 ip helper-address 172.31.2.37 exit interface g0/0.1 encapsulation dot1Q 1 ip address 172.31.2.17 255.255.255.248 </pre>

<pre>ip helper-address 172.31.2.30 exit exit copy running-config startup-config</pre>	<pre>encapsulation dot1Q 1 ip address 172.31.2.9 255.255.255.248 exit exit copy running-config startup-config</pre>	<pre>ip helper-address 172.31.2.37 exit interface g0/0.88 encapsulation dot1Q 88 ip address 172.31.2.25 255.255.255.248 ip helper-address 172.31.2.37 exit exit copy run star</pre>
---	---	---

Aunque permitamos el broadcast DHCP hacia el router de Tunja desde la LAN de Bucaramanga y Cundinamarca se debe realizar la siguiente configuración adicional en el Router de Tunja para que asigne correctamente la dirección de acuerdo con la VLAN en la que opera cada dispositivo. También es necesario excluir las direcciones que se desean reservar para los equipos que ya les fue asignado de forma manual como es el caso de la ip de la VLAN y de la puerta de enlace asignada a las interfaces utilizadas en el router.

<b>CONFIGURACIÓN DHCP ROUTER TUNJA</b>	
<b>LAN BUCARAMANGA</b>	<b>LAN CUNDINAMARCA</b>
<pre>ip dhcp pool bmangavlan10 network 172.31.0.0 255.255.255.192 default-router 172.31.0.1 exit ip dhcp pool bmangavlan30 network 172.31.0.64 255.255.255.192 default-router 172.31.0.65 ip dhcp pool bmangavlan1 exit ip dhcp pool cundivlan1 network 172.31.2.0 255.255.255.248 default-router 172.31.2.1 exit ip dhcp excluded-address 172.31.0.1 172.31.0.2 ip dhcp excluded-address 172.31.0.65 172.31.0.66 ip dhcp excluded-address 172.31.2.1 172.31.2.2</pre>	<pre>ip dhcp pool cundivlan10 network 172.31.1.0 255.255.255.192 default-router 172.31.1.1 ip dhcp pool cundivlan20 network 172.31.1.64 255.255.255.192 default-router 172.31.1.65 ip dhcp pool cundivlan1 network 172.31.2.16 255.255.255.248 default-router 172.31.2.17 ip dhcp pool cundivlan88 network 172.31.2.48 255.255.255.248 default-router 172.31.2.49 ip dhcp excluded-address 172.31.1.1 172.31.1.2 ip dhcp excluded-address 172.31.1.65 172.31.1.66 ip dhcp excluded-address 172.31.2.17 172.31.2.18 ip dhcp excluded-address 172.31.2.49 172.31.2.50</pre>

El comando `ip dhcp pool [NAME]` me permite crear un pool de DHCP con un identificador determinado. Network establece la red con la que se va a trabajar en ese pool y el `default-router` me dice a qué interfaz debe enviarse el paquete con el direccionamiento asignado.

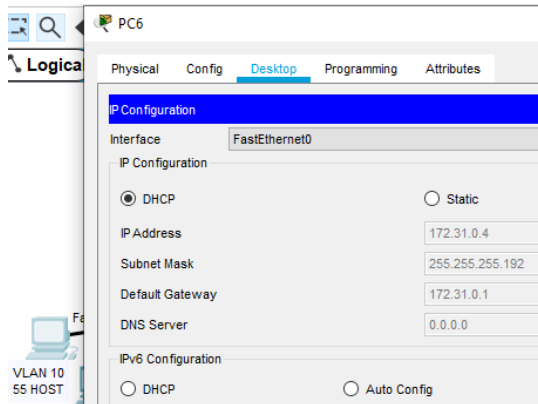


Figura 35 DHCP asignado a host de la VLAN 10 de Bucaramanga

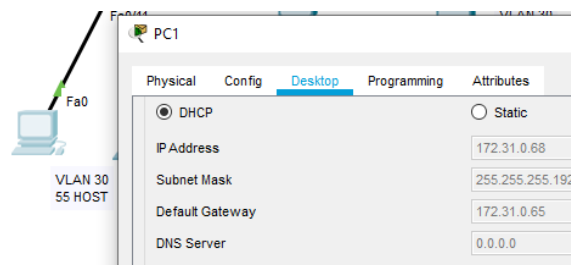


Figura 36 DHCP asignado a host de la VLAN 30 de Bucaramanga

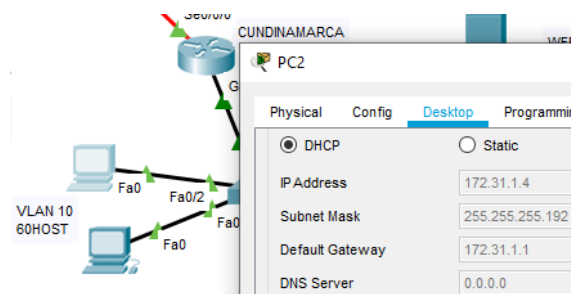


Figura 37 DHCP asignado a host de la VLAN 10 de Cundinamarca

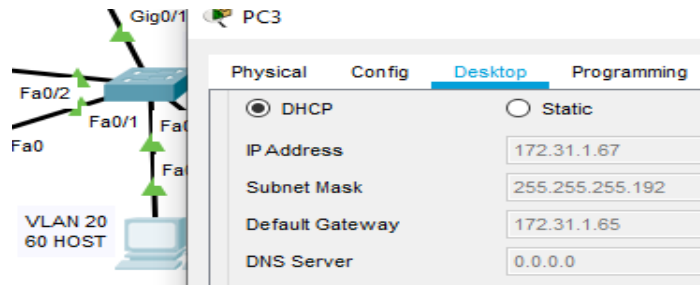


Figura 38 DHCP asignado a host de la VLAN 20 de Cundinamarca

### 3.2.4 Configuración OSPF con autenticación

Se realiza la configuración de OSPF para que los dispositivos puedan compartir las tablas de enrutamiento y se obtenga un alcance completo de la red, de igual forma se configura la autenticación de OSPF para aumentar la seguridad en la red y evitar que se reciban rutas de dispositivos que no tengan configurada correctamente la clave. Esto se logra con el comando:

`ip ospf authentication-key [Clave]` asignándola dentro de la interfaz que estará intercambiando las tablas de direccionamiento. También se configura las interfaces pasivas para evitar que exista tráfico innecesario.

CONFIGURACIÓN OSPF		
BUCARAMANGA	TUNJA	CUNDINAMARCA
<pre>interface s0/0/0 ip ospf authentication-key unad2019 interface s0/0/1 ip ospf authentication-key unad2019 router ospf 1 router-id 1.1.1.1 network 172.31.0.0 0.0.0.63 area 0 network 172.31.0.64 0.0.0.63 area 0 network 172.31.2.0 0.0.0.7 area 0 network 172.31.2.28 0.0.0.3 area 0 passive-interface gigabitEthernet 0/0 area 0 authentication exit exit</pre>	<pre>interface s0/0/0 ip ospf authentication-key unad2019 router ospf 1 router-id 2.2.2.2 network 172.31.2.36 0.0.0.3 area 0 network 209.17.220.0 0.0.0.255 area 0 area 0 authentication passive-interface g0/0 area 0 authentication passive-interface g0/1 area 0 authentication exit exit copy run star</pre>	<pre>interface s0/0/0 ip ospf authentication-key unad2019 router ospf 1 router-id 3.3.3.3 network 172.31.1.0 0.0.0.63 area 0 network 172.31.1.64 0.0.0.63 area 0 network 172.31.2.16 0.0.0.7 area 0 network 172.31.2.24 0.0.0.7 area 0 network 172.31.2.36 0.0.0.3 area 0 passive-interface g0/0 area 0 authentication exit exit copy run star</pre>

```

BUCARAMANGA
Physical Config CLI Attributes
IOS Command Line Interface
Bucaramanga#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 172.31.2.30 to network 0.0.0.0

172.31.0.0/16 is variably subnetted, 13 subnets, 4 masks
C 172.31.0.0/26 is directly connected, GigabitEthernet0/0.10
L 172.31.0.1/32 is directly connected, GigabitEthernet0/0.10
C 172.31.0.64/26 is directly connected, GigabitEthernet0/0.30
L 172.31.0.65/32 is directly connected, GigabitEthernet0/0.30
O 172.31.1.0/26 [110/129] via 172.31.2.30, 02:55:19,
Serial0/0/0
O 172.31.1.64/26 [110/129] via 172.31.2.30, 02:55:19,
Serial0/0/0
C 172.31.2.0/29 is directly connected, GigabitEthernet0/0.1
L 172.31.2.1/32 is directly connected, GigabitEthernet0/0.1
O 172.31.2.16/29 [110/129] via 172.31.2.30, 02:55:19,
Serial0/0/0
O 172.31.2.24/29 [110/129] via 172.31.2.30, 02:55:19,
Serial0/0/0
C 172.31.2.28/30 is directly connected, Serial0/0/0
L 172.31.2.29/32 is directly connected, Serial0/0/0
O 172.31.2.36/30 [110/128] via 172.31.2.30, 02:55:19,
Serial0/0/0
O 209.17.220.0/24 [110/65] via 172.31.2.30, 02:55:19, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.31.2.30, 02:55:19, Serial0/0/0

Bucaramanga#show ip ospf neighbor

Neighbor ID Pri State Dead Time Address
Interface
2.2.2.2 0 FULL/ - 00:00:36 172.31.2.30
Serial0/0/0

```

```

TUNJA
Physical Config CLI Attributes
IOS Command Line Interface
TUNJA#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter are
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

172.31.0.0/16 is variably subnetted, 17 subnets, 4 masks
O 172.31.0.0/26 [110/65] via 172.31.2.29, 02:57:42, Serial0/0/0
O 172.31.0.64/26 [110/65] via 172.31.2.29, 02:57:42, Serial0/0/0
C 172.31.0.128/26 is directly connected, GigabitEthernet0/0.20
L 172.31.0.129/32 is directly connected, GigabitEthernet0/0.20
C 172.31.0.192/26 is directly connected, GigabitEthernet0/0.30
L 172.31.0.193/32 is directly connected, GigabitEthernet0/0.30
O 172.31.1.0/26 [110/65] via 172.31.2.38, 02:57:42, Serial0/0/1
L 172.31.1.64/26 [110/65] via 172.31.2.38, 02:57:42, Serial0/0/1
O 172.31.2.0/28 [110/65] via 172.31.2.29, 02:57:42, Serial0/0/0
C 172.31.2.8/29 is directly connected, GigabitEthernet0/0.1
L 172.31.2.9/32 is directly connected, GigabitEthernet0/0.1
O 172.31.2.16/29 [110/65] via 172.31.2.38, 02:57:42, Serial0/0/1
O 172.31.2.24/29 [110/65] via 172.31.2.38, 02:57:42, Serial0/0/1
C 172.31.2.28/30 is directly connected, Serial0/0/0
L 172.31.2.30/32 is directly connected, Serial0/0/0
C 172.31.2.36/30 is directly connected, Serial0/0/1
L 172.31.2.37/32 is directly connected, Serial0/0/1
O 209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.17.220.0/24 is directly connected, GigabitEthernet0/1
L 209.17.220.1/32 is directly connected, GigabitEthernet0/1
S* 0.0.0.0/0 is directly connected, GigabitEthernet0/1

TUNJA#show ip os
TUNJA#show ip ospf ne
TUNJA#show ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface
1.1.1.1 0 FULL/ - 00:00:38 172.31.2.29 Serial0/0/0
3.3.3.3 0 FULL/ - 00:00:37 172.31.2.38 Serial0/0/1
TUNJA#

```

Figura 39 Tabla de enrutamiento Neighbor en routers de Bucaramanga y Tunja



```

CUNDINAMARCA
Physical Config CLI Attributes
IOS Command Line Interface
CUNDINAMARCA#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 172.31.2.37 to network 0.0.0.0

172.31.0.0/16 is variably subnetted, 14 subnets, 4 masks
O 172.31.0.0/26 [110/129] via 172.31.2.37, 03:00:12,
Serial0/0/0
O 172.31.0.64/26 [110/129] via 172.31.2.37, 03:00:12,
Serial0/0/0
C 172.31.1.0/26 is directly connected, GigabitEthernet0/0.10
L 172.31.1.1/32 is directly connected, GigabitEthernet0/0.10
C 172.31.1.64/26 is directly connected, GigabitEthernet0/0.20
L 172.31.1.65/32 is directly connected, GigabitEthernet0/0.20
O 172.31.2.0/29 [110/129] via 172.31.2.37, 03:00:12,
Serial0/0/0
C 172.31.2.16/29 is directly connected, GigabitEthernet0/0.1
L 172.31.2.17/32 is directly connected, GigabitEthernet0/0.1
C 172.31.2.24/29 is directly connected, GigabitEthernet0/0.88
L 172.31.2.25/32 is directly connected, GigabitEthernet0/0.88
O 172.31.2.28/30 [110/128] via 172.31.2.37, 03:00:22,
Serial0/0/0
C 172.31.2.36/30 is directly connected, Serial0/0/0
L 172.31.2.38/32 is directly connected, Serial0/0/0
O 209.17.220.0/24 [110/65] via 172.31.2.37, 03:00:22, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.31.2.37, 03:00:22, Serial0/0/0

CUNDINAMARCA#show ip osp
CUNDINAMARCA#show ip ospf ne
CUNDINAMARCA#show ip ospf neighbor

Neighbor ID Pri State Dead Time Address
Interface
2.2.2.2 0 FULL/ - 00:00:30 172.31.2.37
Serial0/0/0

```

Figura 40 Tabla de enrutamiento Neighbor en router de Cundinamarca

### 3.2.5 Configuración de NAT estático y de sobrecarga

Para la presente etapa se gestiona el acceso a la red por parte de los equipos a través de un NAT estático y de paso al web interno se le gestiona una IP publica para que pueda tener acceso desde la red externa de la empresa.

<b>CONFIGURACIÓN NAT ROUTER DE TUNJA</b>
enable
conf t
access-list 1 permit
ip nat inside source static 172.31.2.27 209.17.220.254
ip access-list standard NAT_UNAD
permit 172.31.0.0 0.0.255.255
exit
ip nat inside source list NAT_UNAD interface g0/1 overload
int g0/1
ip nat outside
int g0/0
ip nat inside

```
int s0/0/0
ip nat inside
interface s0/0/1
ip nat inside
int s0/0/1
ip nat inside
int g0/0.1
ip nat inside
int g0/0.20
ip nat inside
int g0/0.30
ip nat inside
exit
exit
copy run start

ip route 0.0.0.0 0.0.0.0 g0/1
router ospf 1
default-information originate
copy run start
```

Se valida el funcionamiento del NAT realizando ping al servidor web externo y del servidor externo al servidor web interno demostrando que se tiene salida a la red y de paso que desde fuera se puede tener acceso a la red ya que gracias a la configuración de NAT realizada el router asocia al servidor web interno que tiene asignada la IP 172.31.2.27 y permite el acceso a él asignando una IP externa 209.17.220.254 la cual él personalmente traduce a la IP de la LAN.

The screenshot shows the CLI of a TUNJA router. At the top, there are tabs for Physical, Config, CLI (selected), and Attributes. Below the tabs, the text reads "IOS Command Line Interface". The CLI shows the following commands and their outputs:

```

C 209.17.220.0/24 is directly connected, GigabitEthernet0/1
L 209.17.220.1/32 is directly connected, GigabitEthernet0/1
S* 0.0.0.0/0 is directly connected, GigabitEthernet0/1

TUNJA#show ip os
TUNJA#show ip ospf ne
TUNJA#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address        Interface
1.1.1.1          0     FULL/ -         00:00:38   172.31.2.29   Serial0/0/0
3.3.3.3          0     FULL/ -         00:00:37   172.31.2.38   Serial0/0/1

TUNJA#show ip nat translations
Pro Inside global  Inside local  Outside local  Outside global
--- 209.17.220.254 172.31.2.26   ---            ---

TUNJA#show ip nat translations
Pro Inside global  Inside local  Outside local  Outside global
icmp 209.17.220.1:1 172.31.2.29:1 209.17.220.253:1 209.17.220.253:1
icmp 209.17.220.254:1 172.31.2.27:1 209.17.220.253:1 209.17.220.253:1
icmp 209.17.220.254:2 172.31.2.27:2 209.17.220.253:2 209.17.220.253:2
--- 209.17.220.254 172.31.2.26   ---            ---

TUNJA#

```

Figura 41 NAT en funcionamiento router TUNJA

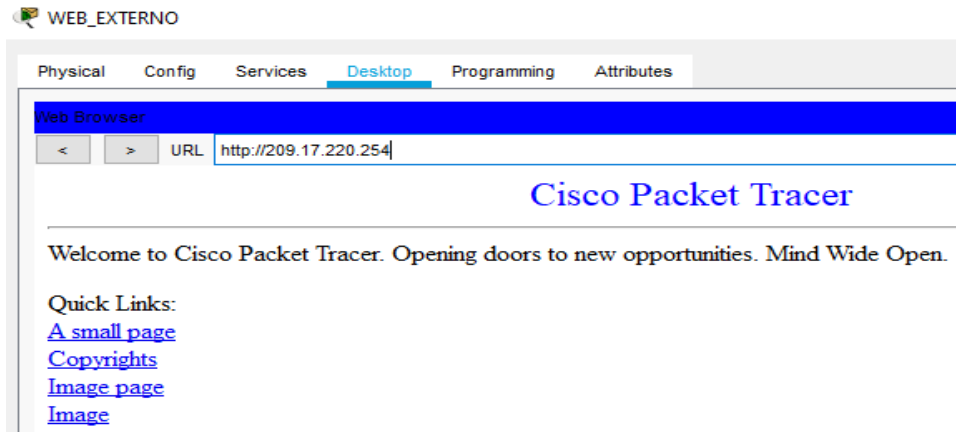


Figura 42 Prueba de acceso a servidor web interno con IP asignada por NAT

**3.2.6 Establecer una lista de control de acceso de acuerdo con los criterios señalados.**

- 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.
- 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.
- 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.
- Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.
- Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen acceso a los routers e internet.

Para resolver los requerimientos de restricciones se establecieron las siguientes ACL en cada router de acuerdo con el alcance por red y dispositivos. Se tuvo muy en cuenta el acceso del equipo de las VLAN de Bucaramanga y Cundinamarca al servidor DHCP que si bien no se menciona en el listado de acceso es evidente que se debe proteger para permitir el direccionamiento de los equipos.

<b>CONFIGURACIÓN ACL ROUTERS</b>		
<b>BUCARAMANGA</b>	<b>TUNJA</b>	<b>CUNDINAMARCA</b>
<pre>ip access-list extended AclBucaramangaSub1 permit tcp any any eq www permit tcp any any eq 443 permit udp any eq bootpc any eq bootps permit tcp any 172.31.2.0 0.0.0.63 eq telnet permit tcp any 172.31.2.28 0.0.0.3 eq telnet</pre>	<pre>ip access-list extended AclTunjaSub1 permit tcp any any eq www permit tcp any any eq 443 permit tcp any 172.31.2.28 0.0.0.3 eq telnet permit tcp any 172.31.2.36 0.0.0.3 eq telnet</pre>	<pre>ip access-list extended AclCundinamarcaSub1 permit tcp any any eq www permit tcp any any eq 443 permit udp any eq bootpc any eq bootps permit tcp any 172.31.2.28 0.0.0.3 eq telnet exit int g0/0.1 ip access-group AclCundinamarcaSub1 in exit</pre>

<pre> permit tcp any 172.31.2.37 0.0.0.3 eq telnet exit int g0/0.1 ip access-group AclBucaramangaSub1 in exit ip access-list extended AclBucaramangaSub30 permit tcp any any eq www permit udp any eq bootpc any eq bootps permit ip any 172.31.1.0 0.0.0.63 deny ip any 172.31.0.0 0.0.255.255 permit ip any any exit int g0/0.30 ip access-group AclBucaramangaSub30 in exit ip access-list extended AclBucaramangaSub10 permit udp any eq bootpc any eq bootps permit ip any 172.31.0.128 0.0.0.63 permit tcp any 172.31.0.0 0.0.255.255 eq www permit ip any 172.31.1.64 0.0.0.63 exit int g0/0.10 ip access-group AclBucaramangaSub10 in exit exit copy run star </pre>	<pre> permit tcp any 172.31.2.8 0.0.0.7 eq telnet exit int g0/0.1 ip access-group AclTunjaSub1 in exit ip access-list extended AclTunjaSub20 permit ip any 172.31.0.0 0.0.0.63 permit ip any 172.31.1.64 0.0.0.63 exit int g0/0.20 ip access-group AclTunjaSub20 in exit ip access-list extended AclTunjaSub30 deny ip any 172.31.0.0 0.0.255.255 permit tcp any any eq www permit tcp any any eq ftp exit int g0/0.30 ip access-group AclTunjaSub30 in </pre>	<pre> ip access-list extended AclCundinamarcaSub10 permit tcp any any eq www permit tcp any any eq 443 permit udp any eq bootpc any eq bootps permit ip any 172.31.0.64 0.0.0.63 deny ip any 172.31.0.0 0.0.255.255 permit ip any any exit int g0/0.10 ip access-group AclCundinamarcaSub10 in exit ip access-list extended AclCundinamarcaSub20 permit tcp any any eq www permit tcp any any eq 443 permit udp any eq bootpc any eq bootps permit ip any 172.31.0.8 0.0.0.7 0.0.0.63 permit ip any 172.31.0.128 0.0.0.63 permit ip any 172.31.0.192 0.0.0.63 permit ip any 172.31.0.0 0.0.0.63 exit int g0/0.20 ip access-group AclCundinamarcaSub20 in exit permit tcp any any eq 443 permit udp any eq bootpc any eq bootps permit tcp any 172.31.2.28 0.0.0.3 eq telnet permit tcp any 172.31.2.36 0.0.0.3 eq telnet permit tcp any 172.31.2.24 0.0.0.7 eq telnet permit udp host 172.31.2.27 host 172.31.2.29 eq tftp permit udp host 172.31.2.27 host 172.31.2.29 range 1025 5000 </pre>
--	--	--

		<pre> permit udp host 172.31.2.27 host 172.31.2.37 eq tftp permit udp host 172.31.2.27 host 172.31.2.37 range 1025 5000 permit udp host 172.31.2.27 host 172.31.2.25 eq tftp permit udp host 172.31.2.27 host 172.31.2.25 range 1025 5000 permit tcp any any eq www permit tcp any any range 1000 1100 exit exit copy run star </pre>
--	--	---

Para las pruebas de las ACL se realizó la modificación a la red agregando equipos para la VLAN administrativa y así analizar el alcance que tiene la misma

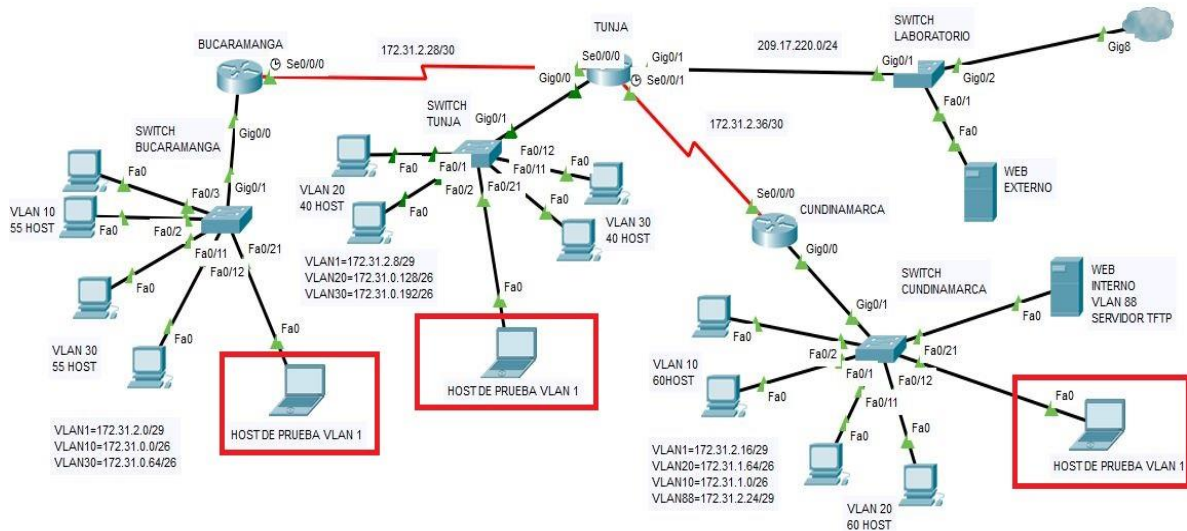


Figura 43 Red con dispositivos agregados para pruebas de la VLAN administrativa

Fire	Last Status	Source	Destination	Type	Color	Time(sec)
	Successful	PC1_VLAN20_CMARCA	PC1_VLAN20_TUNJA	ICMP		0.000
	Failed	PC1_VLAN20_CMARCA	WEB_EXTERNO	ICMP		0.000
	Failed	PC1_VLAN20_CMARCA	PC1_VLAN30_BMANGA	ICMP		0.000

Figura 44 Host VLAN 20 de Cundinamarca sin acceso a internet, pero con acceso a la LAN de Tunja

Fire	Last Status	Source	Destination	Type	Color	Time(sec)
	Successful	PC2_VLAN10_CMARCA	WEB_EXTERNO	ICMP	■	0.000
	Failed	PC1_VLAN10_CMARCA	PC2_VLAN20_TUNJA	ICMP	■	0.000
	Failed	PC1_VLAN10_CMARCA	PC2_VLAN30_TUNJA	ICMP	■	0.000

Figura 45 Host VLAN 10 de Cundinamarca con acceso a internet, pero sin acceso a la LAN de Tunja

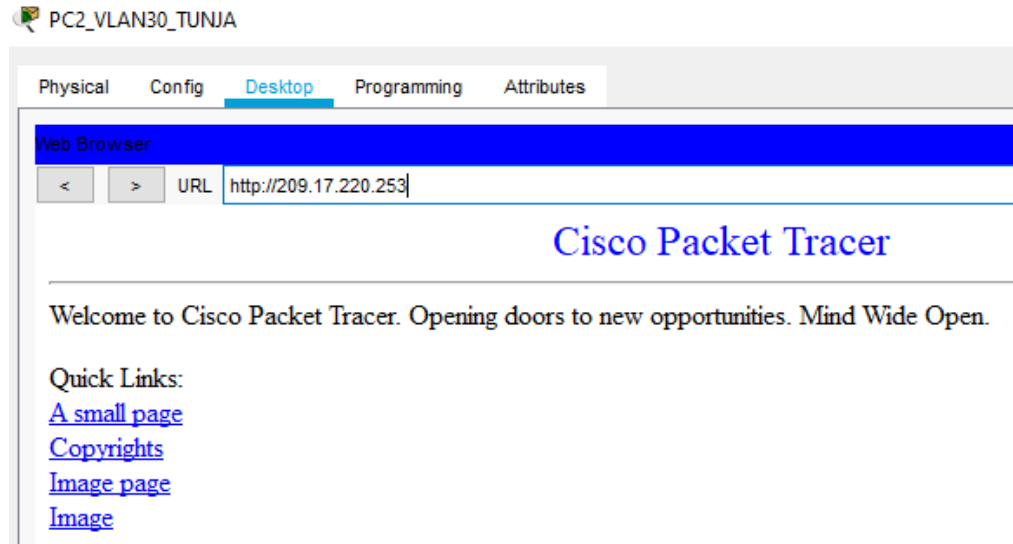


Figura 46 Host VLAN 30 de Tunja con acceso a servidores web y ftp de internet

Fire	Last Status	Source	Destination	Type	Color	Time(sec)
	Successful	PC1_VLAN20_TUNJA	PC2_VLAN20_CMARCA	ICMP	■	0.000
	Successful	PC2_VLAN10_BMANGA	PC1_VLAN10_BMANGA	ICMP	■	0.000
	Failed	PC2_VLAN20_TUNJA	PC2_VLAN30_BMANGA	ICMP	■	0.000

Figura 47 Host de la VLAN 20 de Tunja solo con acceso a la VLAN 20 de Cundinamarca y la VLAN 10 de Bucaramanga

Fire	Last Status	Source	Destination	Type	Color	Time(sec)
	Successful	PC1_VLAN30_BMANGA	PC1_VLAN10_CMARCA	ICMP	■	0.000
	Successful	PC1_VLAN30_BMANGA	WEB_EXTERNO	ICMP	■	0.000
	Failed	PC1_VLAN30_BMANGA	PC1_VLAN30_TUNJA	ICMP	■	0.000

Figura 48 Host de la VLAN 30 de Bucaramanga con acceso a internet y a cualquier VLAN 10

Fire	Last Status	Source	Destination	Type	Color	Time(sec)
	Successful	PC1_VLAN10_BMANGA	PC1_VLAN20_TUNJA	ICMP	Dark Blue	0.000
	Successful	PC1_VLAN10_BMANGA	PC2_VLAN20_CMARCA	ICMP	Dark Green	0.000
	Failed	PC1_VLAN10_BMANGA	WEB_EXTERNO	ICMP	Light Green	0.000

Figura 49 Host de la VLAN 10 de Bucaramanga sin acceso a internet, pero con acceso a la VLAN 20 de Tunja y Cundinamarca

Fire	Last Status	Source	Destination	Type	Color	Time(sec)
	Failed	PC2_VLAN30_BMANGA	PC1_VLAN1_BMANGA	ICMP	Light Green	0.000
	Failed	PC2_VLAN30_BMANGA	PC2_VLAN10_BMANGA	ICMP	Brown	0.000

Figura 50 Host de Bucaramanga sin acceso entre VLANs de la misma ciudad

Fire	Last Status	Source	Destination	Type	Color	Time(sec)
	Failed	PC2_VLAN20_TUNJA	PC1_VLAN1_TUNJA	ICMP	Dark Blue	0.000
	Failed	PC2_VLAN20_TUNJA	PC2_VLAN30_TUNJA	ICMP	Light Green	0.000

Figura 51 Host de Tunja sin acceso entre VLANs de la misma ciudad

Fire	Last Status	Source	Destination	Type	Color	Time(sec)
	Failed	PC2_VLAN10_CMARCA	PC1_VLAN20_CMARCA	ICMP	Light Blue	0.000
	Failed	PC2_VLAN10_CMARCA	PC1_VLAN1_CMARCA	ICMP	Purple	0.000
	Failed	PC2_VLAN10_CMARCA	WEB_INTERNO	ICMP	Yellow-Green	0.000

Figura 52 Host de Cundinamarca sin acceso entre VLANs de la misma ciudad



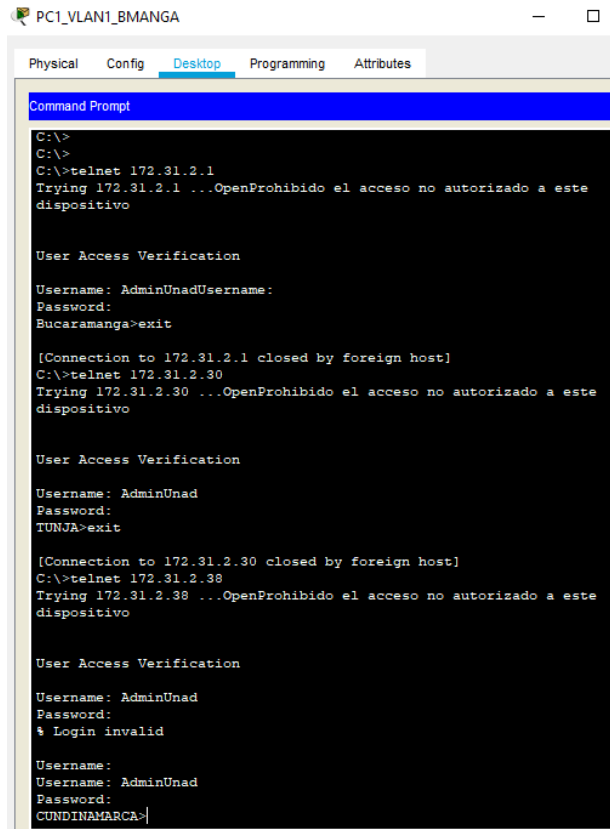


Figura 53 Acceso a routers desde VLAN administrativa

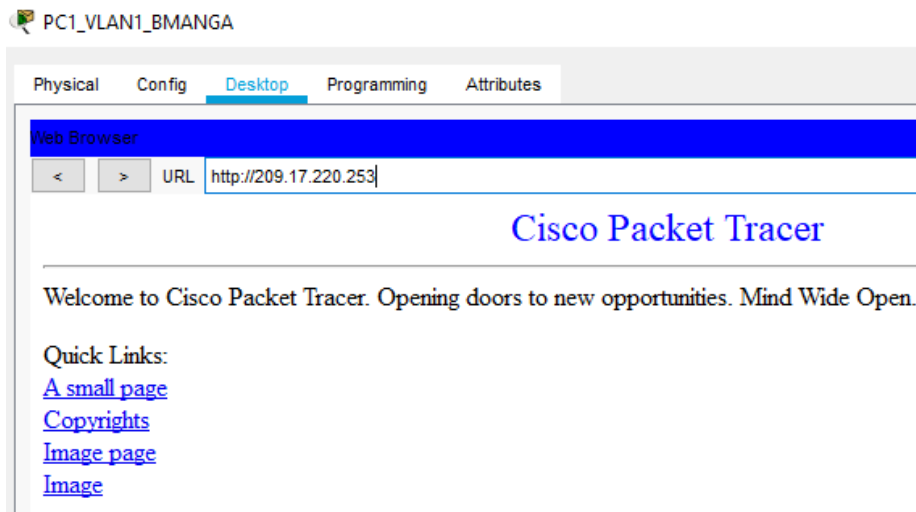


Figura 54 Acceso desde VLAN Administrativa a internet

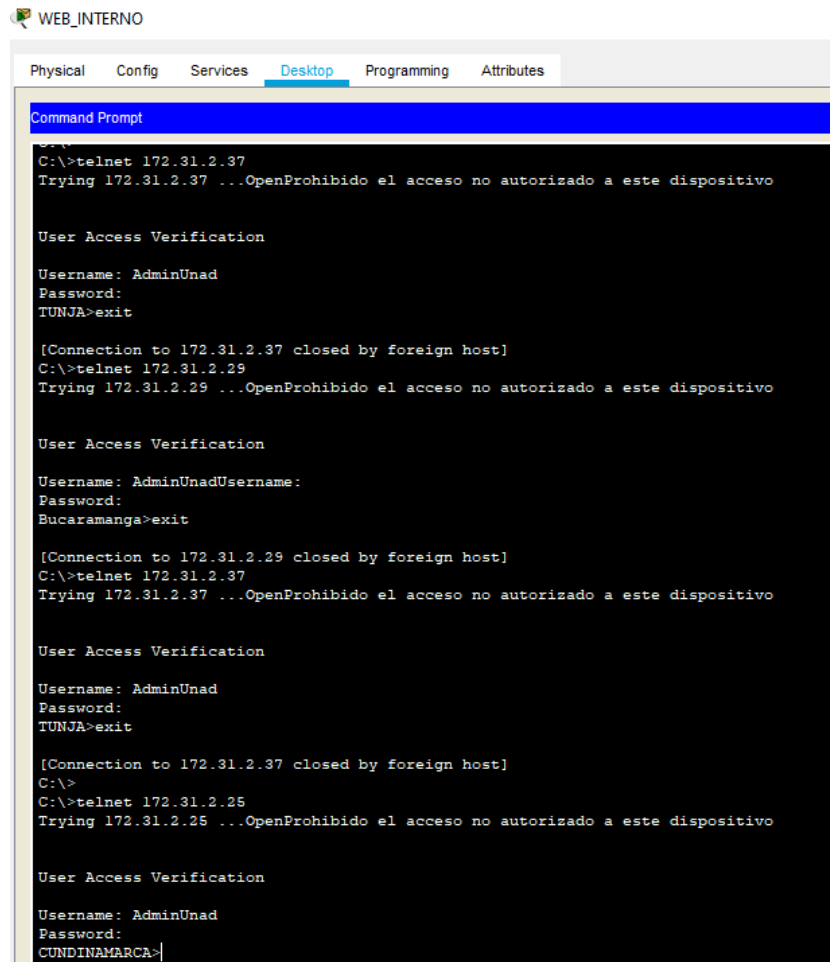


Figura 55 Conexión a routers desde servidor en la VLAN 88

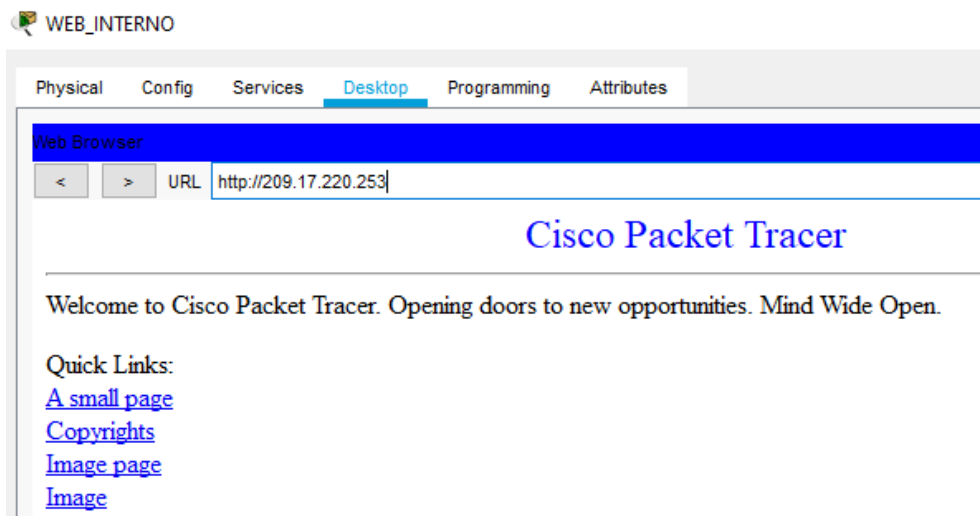


Figura 56 Prueba de conexión VLAN 88 a internet

Este paso no se realiza con todos los equipos de las vlan administrativa ni de servidores ya que el resultado es el mismo al aplicar el código de las listas de acceso generado y se desea simplificar el informe.

Paso 7: Habilitar las opciones en puerto consola y terminal virtual

En este paso se realiza la configuración básica del router con autenticación AAA cifrado de contraseñas, número máximo de intentos de conexión, tiempo de acceso y servidor TFTP para almacenar los archivos de configuración de los routers. Todo esto se logra aplicando a los routers el siguiente código:

<b>CONFIGURACIÓN DE SEGURIDAD RUTERS</b>		
<b>BUCARAMANGA</b>	<b>TUNJA</b>	<b>CUNDINAMARCA</b>
hostmane BUCARAMANGA banner motd %Prohibido el acceso no autorizado a este dispositivo% service password- encryption aaa new-model aaa authentication login AdminAAA local enable username AdminUnad secret cisco2019 enable secret cisco2019 line con 0 login authentication AdminAAA logging synchronous exec-timeout 20 login block-for 180 attempts 5 within 120 line vty 0 15 login authentication AdminAAA logging synchronous exec-timeout 20 exit exit copy run star	hostmane TUNJA banner motd %Prohibido el acceso no autorizado a este dispositivo% service password- encryption aaa new-model aaa authentication login AdminAAA local enable username AdminUnad secret cisco2019 enable secret cisco2019 line con 0 login authentication AdminAAA logging synchronous exec-timeout 20 login block-for 180 attempts 5 within 120 line vty 0 15 login authentication AdminAAA logging synchronous exec-timeout 20 exit exit copy run star	hostmane CUNDINAMARCA banner motd %Prohibido el acceso no autorizado a este dispositivo% service password-encryption aaa new-model aaa authentication login AdminAAA local enable username AdminUnad secret cisco2019 enable secret cisco2019 line con 0 login authentication AdminAAA logging synchronous exec-timeout 20 login block-for 180 attempts 5 within 120 line vty 0 15 login authentication AdminAAA logging synchronous exec-timeout 20 exit exit copy run star

```
PC1_VLAN1_BMANGA
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>telnet 172.31.2.1
Trying 172.31.2.1 ...OpenProhibido el acceso no autorizado a este
dispositivo

User Access Verification

Username: AdminUnadUsername:
Password:
Bucaramanga>exit

[Connection to 172.31.2.1 closed by foreign host]
C:\>telnet 172.31.2.30
Trying 172.31.2.30 ...OpenProhibido el acceso no autorizado a este
dispositivo

User Access Verification

Username: AdminUnad
Password:
TUNJA>exit

[Connection to 172.31.2.30 closed by foreign host]
C:\>telnet 172.31.2.38
Trying 172.31.2.38 ...OpenProhibido el acceso no autorizado a este
dispositivo

User Access Verification

Username: AdminUnad
Password:
% Login invalid

Username:
Username: AdminUnad
Password:
CUNDINAMARCA>
```

Figura 57 Prueba de conexión a los router luego de implementar la seguridad

```

BUCARAMANGA
Physical Config CLI Attributes
IOS Command Line Interface

Prohibido el acceso no autorizado a este dispositivo

User Access Verification

Username: AdminUnad
Password:
Bucaramanga>en
Password:
Bucaramanga#copy runn
Bucaramanga#copy running-config star
Bucaramanga#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Bucaramanga#copy star
Bucaramanga#copy startup-config tftp
Address or name of remote host []? 172.31.2.27
Destination filename [Bucaramanga-config]?

Writing startup-config...!!
[OK - 3048 bytes]

3048 bytes copied in 0.008 secs (381000 bytes/sec)
Bucaramanga#

TUNJA
Physical Config CLI Attributes
IOS Command Line Interface

Prohibido el acceso no autorizado a este dispositivo

User Access Verification

Username: AdminUnad
Password:
TUNJA>en
Password:
TUNJA#copy run
TUNJA#copy running-config star
TUNJA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
TUNJA#copy star
TUNJA#copy startup-config tftp
Address or name of remote host []? 172.31.2.27
Destination filename [TUNJA-config]?

Writing startup-config...!!
[OK - 4016 bytes]

4016 bytes copied in 0.004 secs (1004000 bytes/sec)
TUNJA#

```

Figura 58 Copia de configuración inicial a servidor TFTP desde router Bucaramanga y Tunja

```

CUNDINAMARCA
Physical Config CLI Attributes
IOS Command Line Interface

Prohibido el acceso no autorizado a este dispositivo

User Access Verification

Username: AdminUnad
Password:
CUNDINAMARCA>en
Password:
CUNDINAMARCA#copy runn
CUNDINAMARCA#copy running-config star
CUNDINAMARCA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CUNDINAMARCA#copy star
CUNDINAMARCA#copy startup-config tftp
Address or name of remote host []? 172.31.2.27
Destination filename [CUNDINAMARCA-config]?

Writing startup-config...!!
[OK - 3723 bytes]

3723 bytes copied in 0 secs
CUNDINAMARCA#

```

Figura 59 Copia de configuración inicial a servidor TFTP desde router Cundinamarca

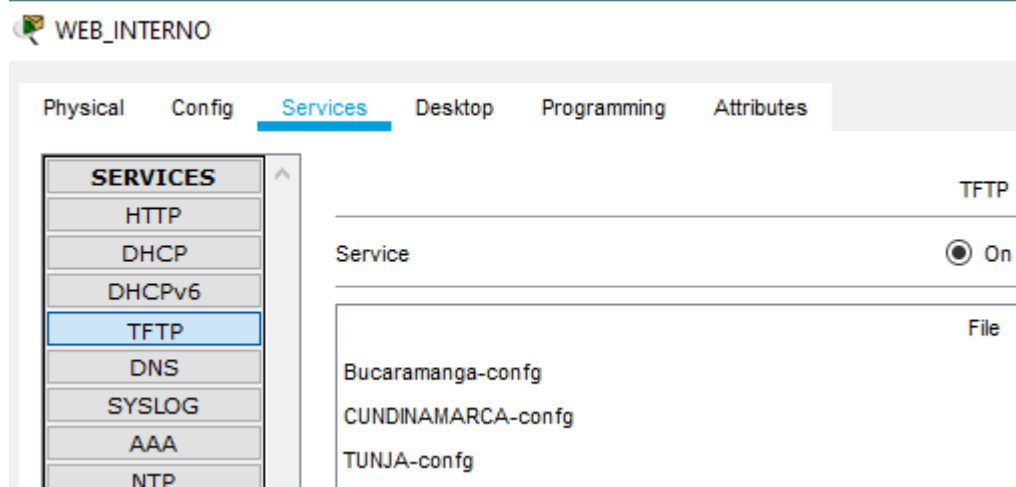


Figura 60 Evidencia de almacenamiento de configuración routers por TFTP

## CONCLUSIONES

La utilización de TFTP permite generar un respaldo a las configuraciones de los dispositivos y facilitar su restauración en caso de presentarse fallas.

Para habilitar DHCP se debe habilitar el ip-helper a los routers ya que por defecto impiden los broadcast y por tanto sería imposible que a un dispositivo le fuese asignado una IP cuando el servidor este fuera de la LAN

La implementación de DHCP puede realizarse desde un router estableciendo el direccionamiento de cada red y de igual forma realizar reservas de direcciones.

La configuración del NAT me permite tener un equipo que esta una red LAN con una IP exterior para que fácilmente pueda ser accedido por los equipos externos a la red de una compañía.

El NAT estático permite genera una ruta por defecto para dirigir todo el tráfico a internet o a otra red cuando el direccionamiento no se encuentre dentro de las tablas de enrutamiento de los equipos.

Tanto EIGRP como OSPF permiten generar de manera eficiente tablas de enrutamiento y su control de distribución gracias a que se puede activar como interfaz pasiva toda aquella que no debe generar tráfico innecesario.

Las listas de control de acceso me permiten asegurar la red asignando permisos a dispositivos, red en general, protocolos y números de puerto de acuerdo con la necesidad de lo que se desea permitir por dispositivo o red.

Las ACL extendidas permiten ser configuradas a gustos agregando o borrando permisos sin la necesidad de ser creadas nuevamente como si ocurriese con las rutas estáticas.

Las rutas extendidas deben por eficiencia de la red ser implementadas en la interfaz más cercana a la salida de los dispositivos que deseamos restringir mientras que las rutas estáticas son más generales y deben ser configuradas lo más cercano posible al destino común de los equipos.

La implementación de VLAN permite tener control sobre los dominios de broadcast en una LAN y así optimizar redes y servicios.

Para permitir acceso sobre las VLAN desde los routers se debe crear subinterfaces que permita a cada VLAN tener una ruta de acceso o Gateway para la gestión de su salida o acceso a otras redes.

Es importante establecer los permisos de acceso en cualquier red a implementar ya que esto garantizará que no se vulnere la seguridad por terceros o incluso personal interno salvaguardando el bien más importante, la información y protegiendo el estado de enlace o disponibilidad del canal de comunicación.



## BIBLIOGRAFÍA

CISCO, Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. {en línea}. {05 de diciembre 2019} disponible en: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>

CISCO, OSPF de una sola área. Principios de Enrutamiento y Conmutación. {en línea}. {05 de diciembre 2019} disponible en: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

CISCO, Listas de control de acceso. Principios de Enrutamiento y Conmutación. {en línea}. {05 de diciembre de 2019} disponible en: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>

CISCO, DHCP. Principios de Enrutamiento y Conmutación. {en línea}. {08 de diciembre de 2019} disponible en: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>

Vesga, J., Principios de Enrutamiento [OVA]. {en línea}. {08 de diciembre 2019} disponible en: [https://1drv.ms/u/s!AmIJYei-NT1lhgOyjWeh6timi\\_Tm](https://1drv.ms/u/s!AmIJYei-NT1lhgOyjWeh6timi_Tm)

Macfarlane, J., Network Routing Basics: Understanding IP Routing in Cisco Systems. {en línea}. {09 de diciembre 2019} disponible en: <http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live>

Lucas, M., Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. {en línea}. {09 de diciembre de 2019} disponible en: <https://1drv.ms/b/s!AmIJYei-NT1lm3L74BZ3bpMiXRx0>

Odom, W., CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. {en línea}. {11 de diciembre 2019} disponible en: <http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf>

CISCO, Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. {en línea}. {11 de diciembre de 2019} disponible en: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>

CISCO, OSPF de una sola área. Principios de Enrutamiento y Conmutación. {en línea}. {11 de diciembre 2019} disponible en: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

CISCO, Listas de control de acceso. Principios de Enrutamiento y Conmutación. {en línea}. {11 de diciembre de 2019} disponible en: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>

CISCO, DHCP. Principios de Enrutamiento y Conmutación. {en línea}. {13 de diciembre de 2019} disponible en: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>

Vesga, J., Principios de Enrutamiento [OVA]. {en línea}. {13 de diciembre de 2019} disponible en: [https://1drv.ms/u/s!AmlJYei-NT1lhgOyjWeh6timi\\_Tm](https://1drv.ms/u/s!AmlJYei-NT1lhgOyjWeh6timi_Tm)

Macfarlane, J., Network Routing Basics : Understanding IP Routing in Cisco Systems. {en línea}. {13 de diciembre de 2019} disponible en: <http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live>

Lucas, M., Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. {en línea}. {13 de diciembre de 2019} disponible en: <https://1drv.ms/b/s!AmlJYei-NT1lm3L74BZ3bpMiXRx0>

Odom, W., CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. {en línea}. {14 de diciembre de 2019} disponible en: <http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf>