

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

**JOINNER ENRIQUE OSORIO**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD  
*ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA***

***INGENIERIA DE SISTEMAS***

***FLORENCIA***

**2019**

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

**JOINNER ENRIQUE OSORIO**

**Trabajo para obtener el título de Ingeniero de Sistemas**

**Director: Ingeniero Juan Carlos Vesga**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA**

**INGENIERIA DE SISTEMAS**

**FLORENCIA**

**2019**

## TABLA DE CONTENIDO

<b>RESUMEN</b> .....	4
<b>ABSTRACT</b> .....	4
<b>INTRODUCCIÓN</b> .....	5
<b>OBJETIVOS</b> .....	6
<b>General</b> .....	6
<b>Específicos</b> .....	6
<b>ESCENARIOS</b> .....	8
<b>Escenario 1</b> .....	8
<b>Escenario 2</b> .....	31
<b>CONCLUSIONES</b> .....	45
<b>REFERENCIAS</b> .....	47

## **RESUMEN**

La siguiente actividad es el desarrollo de una prueba de habilidades prácticas del diplomado de profundización en cisco con el cual demostramos los conocimientos adquiridos durante el desarrollo del curso, mostrando nuestras habilidades de manejo de packet tracer el cual es un software de mucha ayuda pues nos permite simular situaciones y entornos de red que nos permitirán saber cómo debemos hacer las configuraciones cuando nos encontremos en una situación real.

## **ABSTRACT**

The next activity is the development of a test of practical skills of the diploma in deepening in cisco with which we demonstrate the knowledge acquired during the development of the course, showing our packet tracer management skills which is a very helpful software because it allows us simulate situations and network environments that will allow us to know how we should make the configurations when we are in a real situation.

## INTRODUCCIÓN

La siguiente actividad es el desarrollo de una prueba de habilidades prácticas del diplomado de profundización en cisco con el cual demostramos los conocimientos adquiridos durante el desarrollo del curso, mostrando nuestras habilidades de manejo de packet tracer el cual es un software de mucha ayuda pues nos permite simular situaciones y entornos de red que nos permitirán saber cómo debemos hacer las configuraciones cuando nos encontremos en una situación real.

Mediante el estudio de este curso de CCNA1 y CCNA2 pretendemos conocer más a fondo los conceptos y tecnologías básicas que forman una red. Mediante el estudio buscamos desarrollar aptitudes necesarias para planificar e implementar redes pequeñas con una variedad de aplicaciones.

Se realiza la prueba de habilidades prácticas para recordar los conocimientos adquiridos durante el curso.

Actualmente, el diplomado es de gran importancia, ya que nos da un sentido analítico de las cosas y nos ayuda a mejorar en algunos otros cursos de nuestra carrera.

## OBJETIVOS

### General

Realizar informe de la prueba de habilidades practicas del diplomado de cisco

### Específicos.

- Solucionar el ejercicio propuesto en la plataforma de cisco llamado prueba de habilidades practicas
- Demostrar los conocimientos adquiridos durante el desarrollo del diplomado de cisco
  
- ✓ Ejecutar conexiones básicas, acceso a la CLI y exploración de ayuda
- ✓ Realizar configuraciones en las interfaces de administración de los switches
- ✓ Establecer la configuración de los nombres de host y las direcciones IP los switches que utilizan el Sistema operativo Internetwork (IOS) de Cisco mediante la interfaz de línea de comandos (CLI).
- ✓ Verificar la conectividad entre los dispositivos finales.
- ✓ Hacer recopilación de información de la PDU

- ✓ Examinar el proceso de ARP en comunicaciones remotas
- ✓ Identificar las características físicas de los dispositivos de internetworking
- ✓ Verificar la configuración predeterminada del router, configuración inicial y guardar archivos de ejecución

## **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.

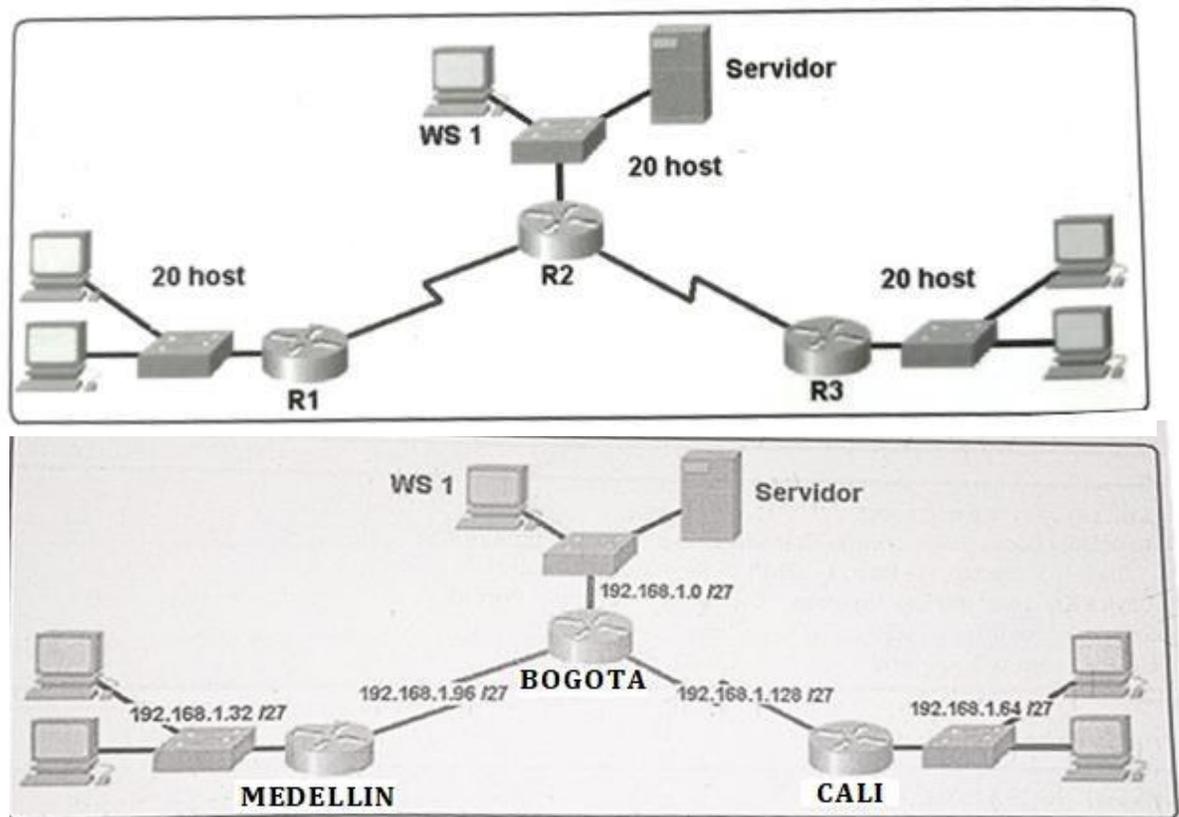


Ilustración 1 - Esquema Escenario1 - Tomado de la Guía de Actividades Diplomado

## 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).

```
MEDELLIN(config)#hostname MEDELLIN
```

```
MEDELLIN(config)#no ip domain-lookup
```

```
MEDELLIN(config)#service password-encryption
```

```
MEDELLIN(config)#enable secret class
```

```
MEDELLIN(config)#line console 0
```

```
MEDELLIN(config-line)#password cisco
```

```
MEDELLIN(config-line)#login
```

```
MEDELLIN(config-line)#LINE VTY 0 15
```

```
MEDELLIN(config-line)#password cisco
```

```
MEDELLIN(config-line)#login
```

```
BOGOTA (config)#hostname BOGOTA
```

```
BOGOTA (config)#no ip domain-lookup
```

```
BOGOTA (config)#service password-encryption
```

```
BOGOTA (config)#enable secret class
```

```
BOGOTA (config)#line console 0
```

```
BOGOTA (config-line)#password cisco
```

```
BOGOTA (config-line)#login
```

BOGOTA (config-line)#LINE VTY 0 15

BOGOTA (config-line)#password cisco

BOGOTA (config-line)#login

CALI (config)#hostname CALI

CALI (config)#no ip domain-lookup

CALI (config)#service password-encryption

CALI (config)#enable secret class

CALI (config)#line console 0

CALI (config-line)#password cisco

CALI (config-line)#login

CALI (config-line)#LINE VTY 0 15

CALI (config-line)#password cisco

CALI (config-line)#login

ISP(config)#no ip domain-lookup

ISP(config)#service password-encryption

ISP(config)#enable secret class

ISP(config)#line console 0

ISP(config-line)#password cisco

```
ISP(config-line)#login
ISP(config-line)#LINE VTY 0 15
ISP(config-line)#password cisco
ISP(config-line)#login
```

```
MEDELLIN>ENABLE
```

```
MEDELLIN#CONF T
```

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

```
MEDELLIN(config)#hostname MEDELLIN
```

```
MEDELLIN1(config)#no ip domain-lookup
```

```
MEDELLIN1(config)#service password-encryption
```

```
MEDELLIN1(config)#enable secret class
```

```
MEDELLIN1(config)#line console 0
```

```
MEDELLIN1(config-line)#password cisco
```

```
MEDELLIN1(config-line)#login
```

```
MEDELLIN1(config-line)#LINE VTY 0 15
```

```
MEDELLIN1(config-line)#password cisco
```

```
MEDELLIN1(config-line)#login
```

BOGOTA>ENABLE

BOGOTA#conf t

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

BOGOTA(config)#no ip domain-lookup

BOGOTA(config)#service password-encryption

BOGOTA(config)#enable secret class

BOGOTA(config)#line console 0

BOGOTA(config-line)#password cisco

BOGOTA(config-line)#login

BOGOTA(config-line)#LINE VTY 0 15

BOGOTA(config-line)#password cisco

BOGOTA(config-line)#login

Router>enable

Router#conf t

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

Router(config)#hostname CALI

CALI(config)#no ip domain-lookup

CALI(config)#service password-encryption

```
CALI(config)#enable secret class
```

```
CALI(config)#line console 0
```

```
CALI(config-line)#password cisco
```

```
CALI(config-line)#login
```

```
CALI(config-line)#LINE VTY 0 15
```

```
CALI(config-line)#password cisco
```

```
CALI(config-line)#login
```

Realizar la conexión física de los equipos con base en la topología de red

En la siguiente ilustración se muestra la configuración de las IP, nombres de cada uno de los equipos.

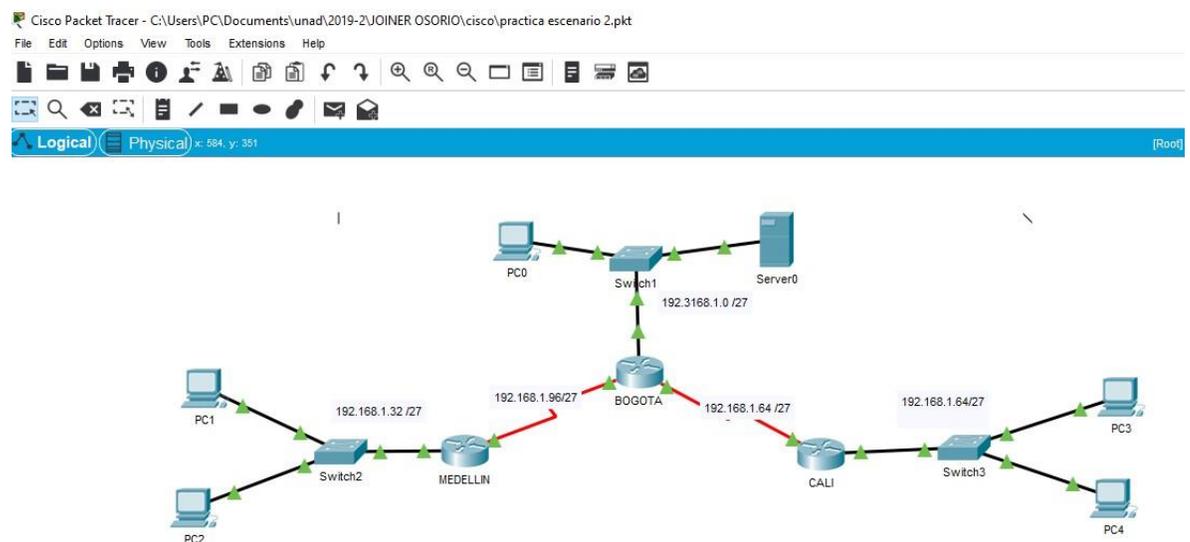


Ilustración 2 - Montaje Escenario 1 en Packet tracer - Fuente: Propia

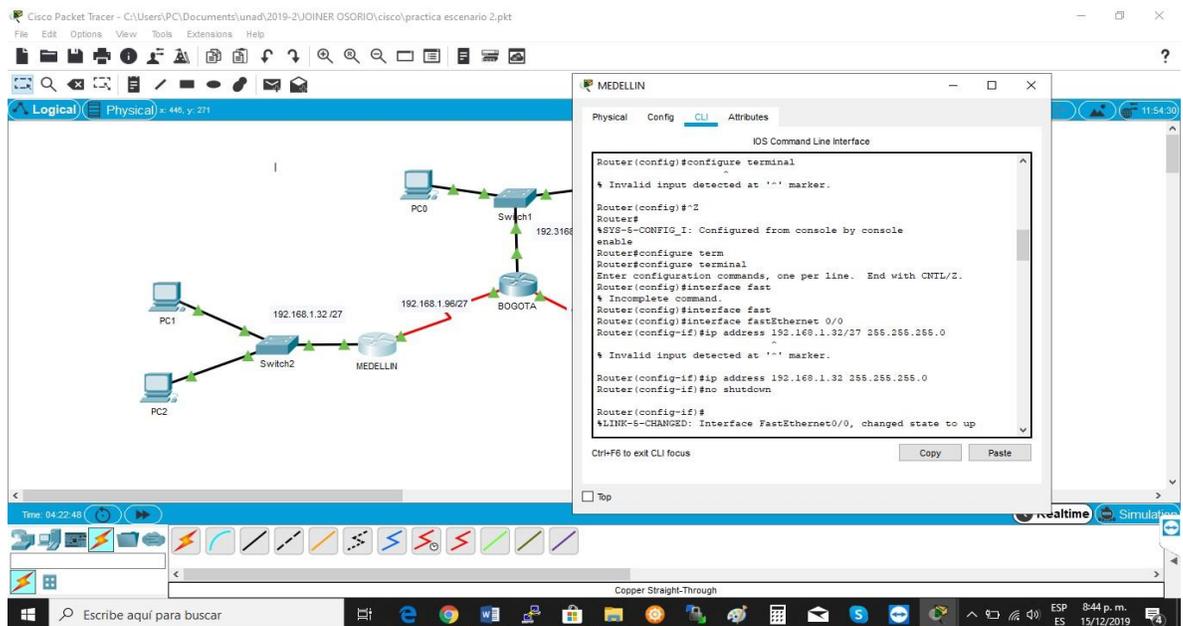


Ilustración 3- Montaje Escenario 1 en Packet tracer - Fuente: Propia

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

### Parte 1: Asignación de direcciones IP:

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

Nombre de Host	Red	Primero	Ultima	Broadcast
Red 1	192.168.1.0	192.168.1.1	192.168.1.30	192.168.1.31
Red 2	192.168.1.32	192.168.1.33	192.168.1.62	192.168.1.63

<b>Red 3</b>	192.168.1.64	192.168.1.65	192.168.1.94	192.168.1.95
<b>Red 4</b>	192.168.1.96	192.168.1.97	192.168.1.126	192.168.1.127
<b>Red 5</b>	192.168.1.128	192.168.1.129	192.168.1.158	192.168.1.159
<b>Red 6</b>	192.168.1.160	192.168.1.161	192.168.1.190	192.168.1.191
<b>Red 7</b>	192.168.1.192	192.168.1.193	192.168.1.222	192.168.1.223
<b>Red 7</b>	192.168.1.224	192.168.1.225	192.168.1.254	192.168.1.255

b. Asignar una dirección IP a la red.

```
Router>ENABLE
```

```
Router#configure terminal
```

```
Router(config)#interface fast
```

```
Router(config)#interface fastEthernet 0/0
```

```
Router(config-if)#ip address 192.168.1.32 255.255.255.0
```

```
Router(config-if)#no shutdown
```

```
Router(config)#interface serial 0/1/0
```

```
Router(config-if)#ip address 162.168.1.96 255.255.0.0
```

```
Router(config-if)#no shutdown
```

## 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	192.168.1.131
Dirección de Ip en interfaz Serial 0/1		192.168.1.130	
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	<b>Eigrp</b>	<b>Eigrp</b>	<b>Eigrp</b>
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

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, este procedimiento se muestra en cada una de las siguientes ilustraciones.

```
MEDELLIN#
MEDELLIN#show ip route
Codes: C - connected, S - static, I - IGRP, 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

      192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/2172416] via 192.168.1.98, 04:21:54,
Serial0/0/0
C       192.168.1.32 is directly connected, FastEthernet0/0
D       192.168.1.64 [90/2684416] via 192.168.1.98, 04:21:54,
Serial0/0/0
C       192.168.1.96 is directly connected, Serial0/0/0
D       192.168.1.128 [90/2681856] via 192.168.1.98, 04:21:54,
Serial0/0/0
MEDELLIN#
```

Ilustración 4 - Configuración ciudad Medellín Escenario 1 - Fuente: Propia

```
BOGOTÁ#
BOGOTÁ#
BOGOTÁ#show ip route
Codes: C - connected, S - static, I - IGRP, 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

      192.168.1.0/27 is subnetted, 5 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0
D       192.168.1.32 [90/2172416] via 192.168.1.99, 04:22:31,
Serial0/0/0
D       192.168.1.64 [90/2172416] via 192.168.1.131, 04:22:31,
Serial0/0/1
C       192.168.1.96 is directly connected, Serial0/0/0
C       192.168.1.128 is directly connected, Serial0/0/1
BOGOTÁ#
```

Ilustración 5 - Configuración ciudad Bogotá Escenario 1 - Fuente Propia

```
CALI#
CALI#show ip route
Codes: C - connected, S - static, I - IGRP, 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

   192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/2172416] via 192.168.1.130, 04:23:10,
Serial0/0/0
D       192.168.1.32 [90/2684416] via 192.168.1.130, 04:23:10,
Serial0/0/0
C       192.168.1.64 is directly connected, FastEthernet0/0
D       192.168.1.96 [90/2681856] via 192.168.1.130, 04:23:10,
Serial0/0/0
C       192.168.1.128 is directly connected, Serial0/0/0

CALI#
```

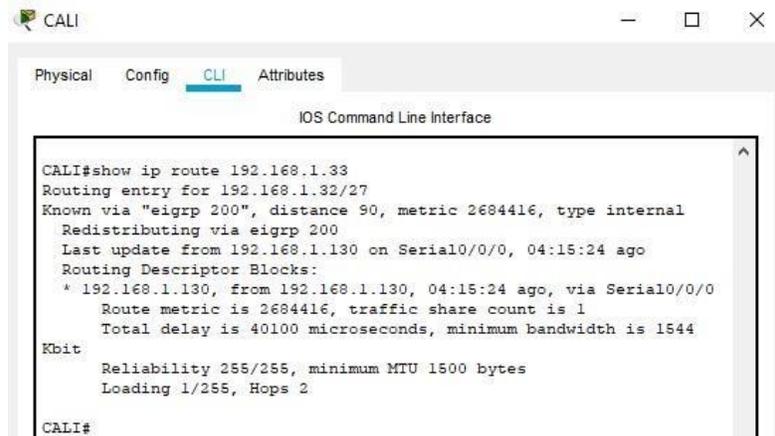
Ilustración 6 - Configuración ciudad Cali Escenario 1 - Fuente: Propia

Luego de la configuración, verificar el balanceo de carga que presentan los routers, descrito en las siguientes ilustraciones.

```
MEDELLIN#
MEDELLIN#show ip route 192.168.1.65
Routing entry for 192.168.1.64/27
Known via "eigrp 200", distance 90, metric 2684416, type internal
  Redistributing via eigrp 200
  Last update from 192.168.1.98 on Serial0/0/0, 04:11:42 ago
  Routing Descriptor Blocks:
    * 192.168.1.98, from 192.168.1.98, 04:11:42 ago, via Serial0/0/0
      Route metric is 2684416, traffic share count is 1
      Total delay is 40100 microseconds, minimum bandwidth is 1544
Kbit
  Reliability 255/255, minimum MTU 1500 bytes
  Loading 1/255, Hops 2

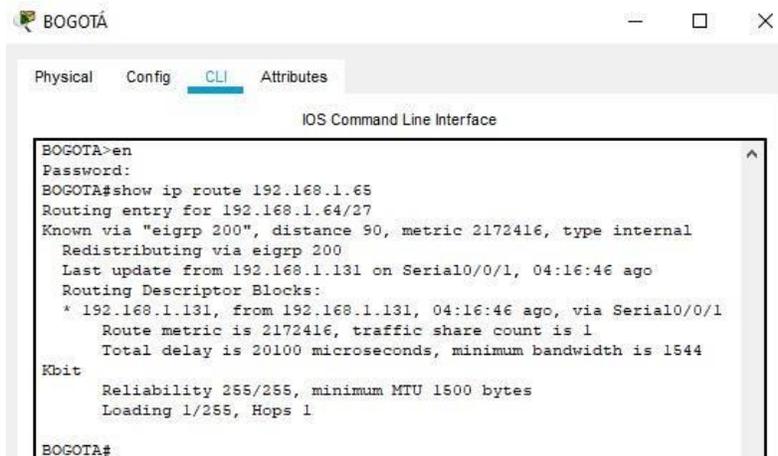
MEDELLIN#
```

Ilustración 7 - Configuración ciudad Medellín Escenario 1 - Fuente: Propia



```
CALI#show ip route 192.168.1.33
Routing entry for 192.168.1.32/27
Known via "eigrp 200", distance 90, metric 2684416, type internal
  Redistributing via eigrp 200
  Last update from 192.168.1.130 on Serial0/0/0, 04:15:24 ago
  Routing Descriptor Blocks:
    * 192.168.1.130, from 192.168.1.130, 04:15:24 ago, via Serial0/0/0
      Route metric is 2684416, traffic share count is 1
      Total delay is 40100 microseconds, minimum bandwidth is 1544
  Kbit
    Reliability 255/255, minimum MTU 1500 bytes
    Loading 1/255, Hops 2
CALI#
```

Ilustración 8 - Configuración ciudad Cali Escenario 1 - Fuente: Propia



```
BOGOTÁ>en
Password:
BOGOTÁ#show ip route 192.168.1.65
Routing entry for 192.168.1.64/27
Known via "eigrp 200", distance 90, metric 2172416, type internal
  Redistributing via eigrp 200
  Last update from 192.168.1.131 on Serial0/0/1, 04:16:46 ago
  Routing Descriptor Blocks:
    * 192.168.1.131, from 192.168.1.131, 04:16:46 ago, via Serial0/0/1
      Route metric is 2172416, traffic share count is 1
      Total delay is 20100 microseconds, minimum bandwidth is 1544
  Kbit
    Reliability 255/255, minimum MTU 1500 bytes
    Loading 1/255, Hops 1
BOGOTÁ#
```

Ilustración 9 - Configuración ciudad Bogotá Escenario 1 - Fuente: Propia

Realizar un diagnóstico de vecinos usando el comando CDP.

```

MEDELLIN#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge
                S - Switch, H - Host, I - IGMP, r - Repeater, P -
Phone
Device ID      Local Intrfce  Holdtme   Capability   Platform   Port
ID
Switch        Fas 0/0        142       S            2950       Fas
0/1
BOGOTA        Ser 0/0/0       129       R            C1841      Ser
0/0/0
MEDELLIN#

```

Ilustración 10 - Configuración ciudad Medellín Escenario 1 - Fuente: Propia

```

BOGOTÁ#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge
                S - Switch, H - Host, I - IGMP, r - Repeater, P -
Phone
Device ID      Local Intrfce  Holdtme   Capability   Platform   Port
ID
Switch        Fas 0/0        173       S            2950       Fas
0/1
CALI          Ser 0/0/1       121       R            C1841      Ser
0/0/0
MEDELLIN     Ser 0/0/0       173       R            C1841      Ser
0/0/0
BOGOTÁ#

```

Ilustración 11 - Configuración ciudad Bogotá Escenario 1 - Fuente: Propia

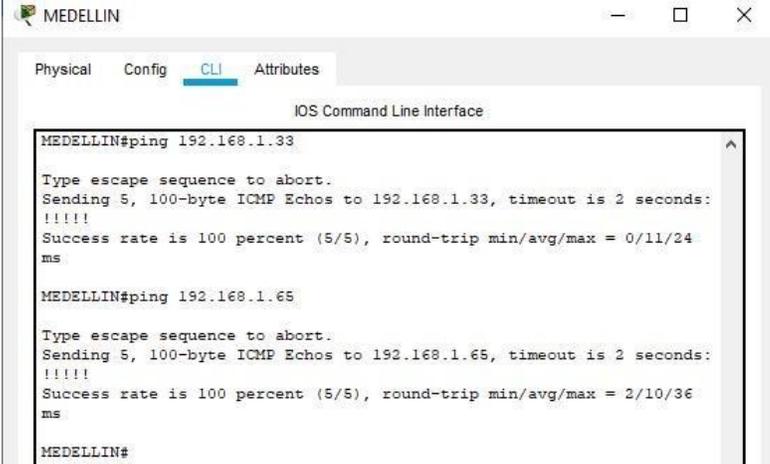
```

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
Switch        Fas 0/0        127       S            2950       Fas
0/1
BOGOTA        Ser 0/0/0       155       R            C1841      Ser
0/0/1
CALI#

```

Ilustración 12 - Configuración ciudad Cali Escenario 1 - Fuente: Propia

Después de la configuración final, realizar una prueba de conectividad en cada tramo de la ruta usando Ping.

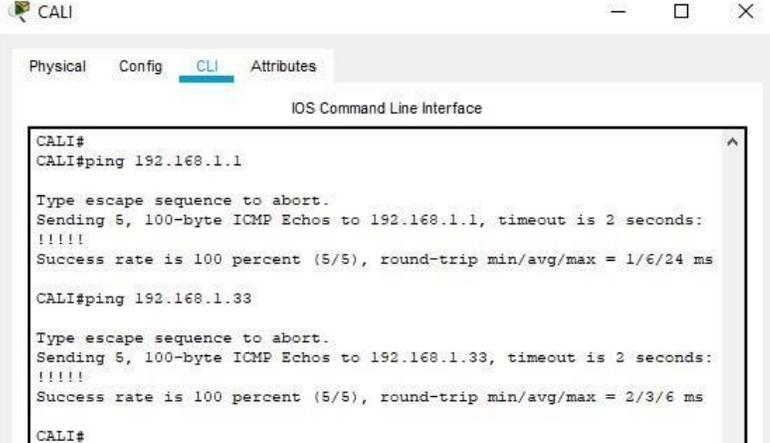


```
MEDELLIN#ping 192.168.1.33
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.33, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/11/24
ms

MEDELLIN#ping 192.168.1.65
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.65, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/10/36
ms

MEDELLIN#
```

Ilustración 13 - Interface Medellín - Fuente: Propia

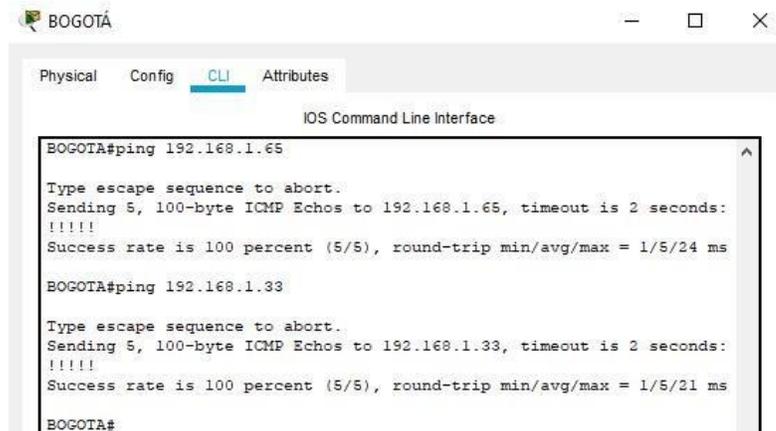


```
CALI#
CALI#ping 192.168.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/24 ms

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 = 2/3/6 ms

CALI#
```

Ilustración 14 - Interface Cali - Fuente: Propia



*Ilustración 15 - Interface Bogotá- Fuente: Propia*

### **Parte 3: Configuración de Enrutamiento.**

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

```
MEDELLIN(config)#router eigrp 200
```

```
MEDELLIN(config-router)#network 192.168.1.0 0.0.0.31
```

```
MEDELLIN(config-router)#network 192.168.1.32 0.0.0.31
```

```
MEDELLIN(config-router)#network 192.168.1.64 0.0.0.31
```

```
MEDELLIN(config-router)#network 192.168.1.96 0.0.0.31
```

```
MEDELLIN(config-router)#network 192.168.1.128 0.0.0.31 CALI(config)#router  
eigrp 200
```

```
CALI(config-router)#network 192.168.1.0 0.0.0.31
```

```
CALI(config-router)#network 192.168.1.32 0.0.0.31
```

```
CALI(config-router)#network 192.168.1.64 0.0.0.31
```

```
CALI(config-router)#network 192.168.1.96 0.0.0.31
```

```
CALI(config-router)#network 192.168.1.128 0.0.0.31
```

```
BOGOTA(config)#router eigrp 200
```

```
BOGOTA(config-router)#network 192.168.1.0 0.0.0.31
```

```
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 192.168.1.96 0.0.0.31
```

```
BOGOTA(config-router)#network 192.168.1.128 0.0.0.31
```

En las ilustraciones se verifica si existe vecindad con los routers configurados con EIGRP.



```
MEDELLIN#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address          Interface           Hold Uptime      SRTT  RTO  Q
Seq
                               (sec)            (ms)            Cnt
Num
0   192.168.1.98      Se0/0/0             14   04:38:20  40   1000  0  8
MEDELLIN#
```

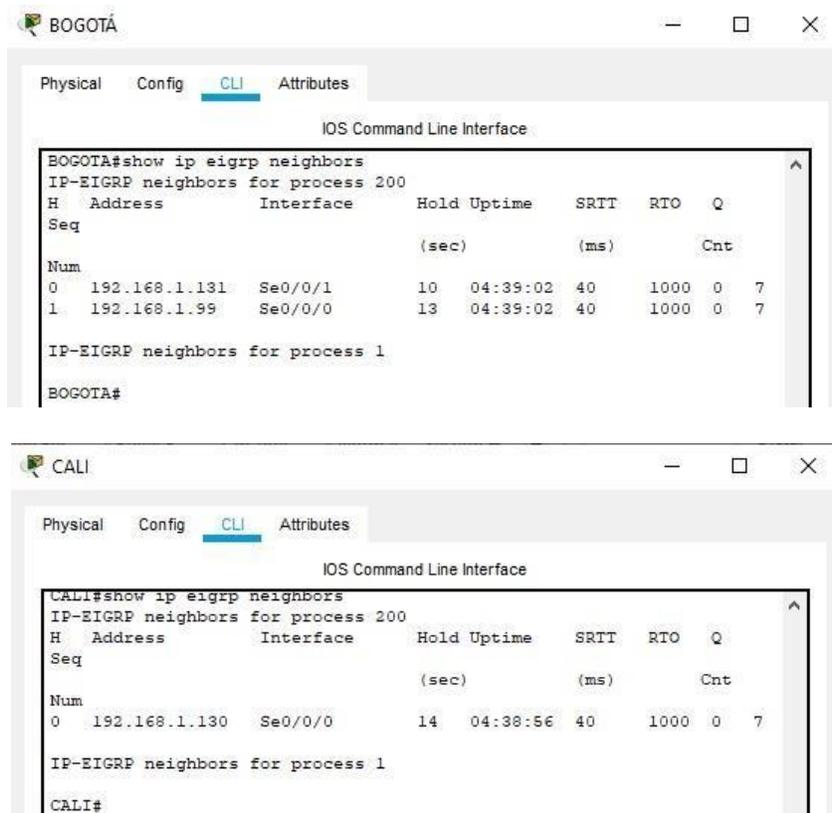


Ilustración 16 - Verificación de Routers - Fuente propia

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

```

MEDELLIN#
MEDELLIN#show ip route
Codes: C - connected, S - static, I - IGRP, 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

      192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/2172416] via 192.168.1.98, 04:40:50,
Serial0/0/0
C       192.168.1.32 is directly connected, FastEthernet0/0
D       192.168.1.64 [90/2684416] via 192.168.1.98, 04:40:50,
Serial0/0/0
C       192.168.1.96 is directly connected, Serial0/0/0
D       192.168.1.128 [90/2681856] via 192.168.1.98, 04:40:50,
Serial0/0/0
MEDELLIN#

```

```

CALI#
CALI#show ip route
Codes: C - connected, S - static, I - IGRP, 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

      192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/2172416] via 192.168.1.130, 04:41:20,
Serial0/0/0
D       192.168.1.32 [90/2684416] via 192.168.1.130, 04:41:20,
Serial0/0/0
C       192.168.1.64 is directly connected, FastEthernet0/0
D       192.168.1.96 [90/2681856] via 192.168.1.130, 04:41:20,
Serial0/0/0
C       192.168.1.128 is directly connected, Serial0/0/0
CALI#

```

```

BOGOTÁ#
BOGOTÁ#show ip route
Codes: C - connected, S - static, I - IGRP, 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

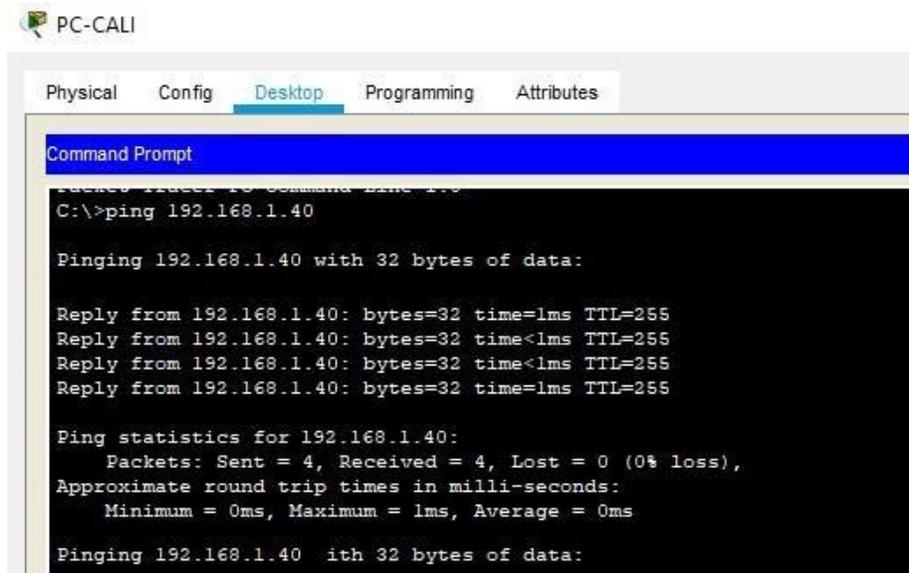
Gateway of last resort is not set

      192.168.1.0/27 is subnetted, 5 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0
D       192.168.1.32 [90/2172416] via 192.168.1.99, 04:41:46,
Serial0/0/0
D       192.168.1.64 [90/2172416] via 192.168.1.131, 04:41:46,
Serial0/0/1
C       192.168.1.96 is directly connected, Serial0/0/0
C       192.168.1.128 is directly connected, Serial0/0/1
BOGOTÁ#

```

Ilustración 17 - Enrutamiento de ciudades - Fuente Propia

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.



```
PC-CALI
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.1.40

Pinging 192.168.1.40 with 32 bytes of data:

Reply from 192.168.1.40: bytes=32 time=1ms TTL=255
Reply from 192.168.1.40: bytes=32 time<1ms TTL=255
Reply from 192.168.1.40: bytes=32 time<1ms TTL=255
Reply from 192.168.1.40: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.40:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

Pinging 192.168.1.40 ith 32 bytes of data:
```

Ilustración 18 - Conectividad entre ciudades Escenario 1 - Fuente propia

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

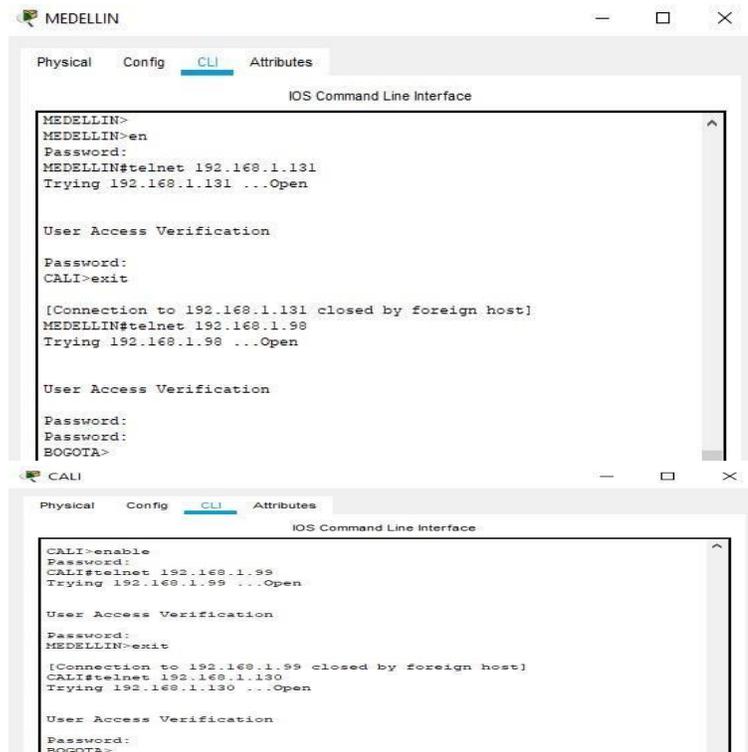
En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo. El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers.

Las condiciones para crear las ACL son las siguientes:

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

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.

a. 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.



The image shows two screenshots of the IOS Command Line Interface (CLI) for two routers, MEDELLIN and CALI. Both screenshots show a telnet session being established from the local router to a remote host.

**MEDELLIN Screenshot:**

```
MEDELLIN>
MEDELLIN>en
Password:
MEDELLIN#telnet 192.168.1.131
Trying 192.168.1.131 ...Open

User Access Verification

Password:
CALI>exit

[Connection to 192.168.1.131 closed by foreign host]
MEDELLIN#telnet 192.168.1.98
Trying 192.168.1.98 ...Open

User Access Verification

Password:
Password:
BOGOTA>
```

**CALI Screenshot:**

```
CALI>enable
Password:
CALI#telnet 192.168.1.98
Trying 192.168.1.98 ...Open

User Access Verification

Password:
MEDELLIN>exit

[Connection to 192.168.1.98 closed by foreign host]
CALI#telnet 192.168.1.130
Trying 192.168.1.130 ...Open

User Access Verification

Password:
BOGOTA>
```

```

BOGOTÁ>en
BOGOTÁ#telnet 192.168.1.99
Trying 192.168.1.99 ...Open

User Access Verification
Password:
MEDELLIN>exit
[Connection to 192.168.1.99 closed by foreign host]
BOGOTÁ#telnet 192.168.1.131
Trying 192.168.1.131 ...Open

User Access Verification
Password:
CALI>
CALI>
CALI>
CALI>
CALI>
CALI>

```

Ilustración 19 - Control de Acceso ciudades - Fuente Propia Packet tracer

## 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	Exitoso
	WS_1	Router BOGOTA	Rechazado
	Servidor	Router CALI	Exitoso
TELNET	Servidor	Router MEDELLIN	Exitoso
	LAN del Router MEDELLIN	Router CALI	Tiempo de conexión agotado; el host remoto no responde
	LAN del Router CALI	Router CALI	Exitoso
	LAN del Router MEDELLIN	Router MEDELLIN	Exitoso

	LAN del Router CALI	Router MEDELLIN	Tiempo de conexión agotado; el host remoto no responde
PING	LAN del Router CALI	WS_1	Tiempo de espera agotado
	LAN del Router MEDELLIN	WS_1	Tiempo de espera agotado
	LAN del Router MEDELLIN	LAN del Router CALI	Tiempo de espera agotado
PING	LAN del Router CALI	Servidor	Exitoso
	LAN del Router MEDELLIN	Servidor	Exitoso
	Servidor	LAN del Router MEDELLIN	Exitoso
	Servidor	LAN del Router CALI	Exitoso
	Router CALI	LAN del Router MEDELLIN	Se acabó el tiempo
	Router MEDELLIN	LAN del Router CALI	Se acabó el tiempo

## 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.

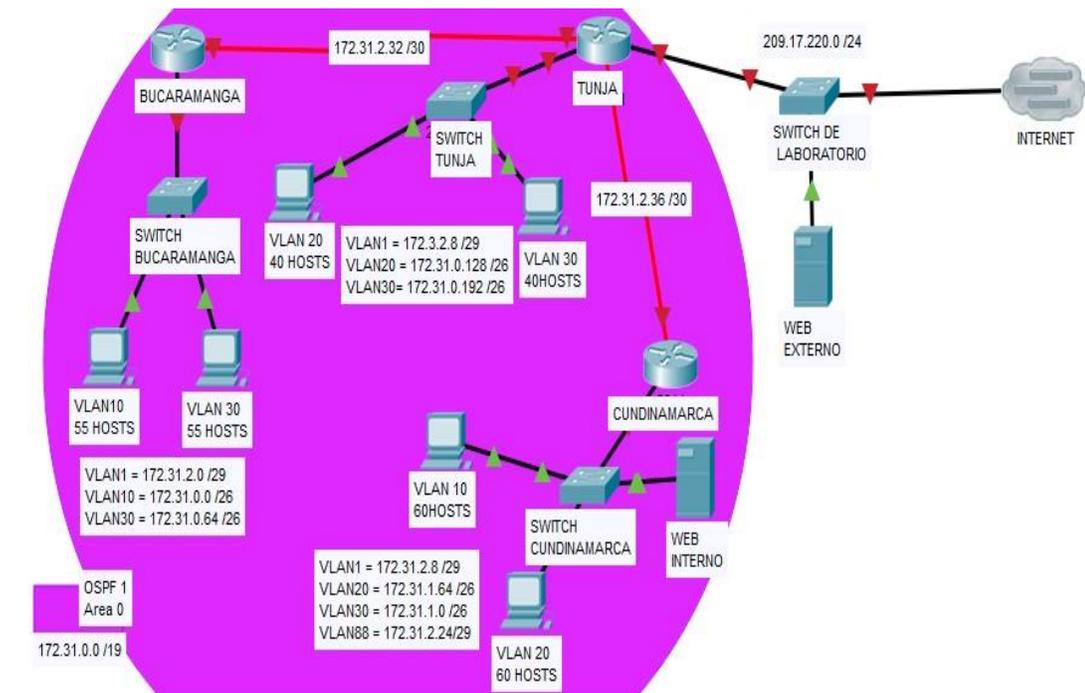


Ilustración 20 - Esquema Escenario 2 - Fuente: Guía de Actividades Diplomado

## Desarrollo

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener lo 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.

```
BUCARAMANGA (config)#hostname BUCARAMANGA
```

```
BUCARAMANGA (config)#no ip domain-lookup
```

```
BUCARAMANGA (config)#service password-encryption
```

```
BUCARAMANGA (config)#enable secret class
```

```
BUCARAMANGA (config)#line console 0
```

```
BUCARAMANGA (config-line)#password cisco
```

```
BUCARAMANGA (config-line)#login
```

```
BUCARAMANGA (config-line)#LINE VTY 0 15
```

```
BUCARAMANGA (config-line)#password cisco
```

```
BUCARAMANGA (config-line)#login
```

```
TUNJA (config)#hostname TUNJA
```

```
TUNJA (config)#no ip domain-lookup
```

```
TUNJA (config)#service password-encryption
```

```
TUNJA (config)#enable secret class
```

```
TUNJA (config)#line console 0
TUNJA (config-line)#password cisco
TUNJA (config-line)#login
TUNJA (config-line)#LINE VTY 0 15
TUNJA (config-line)#password cisco
TUNJA (config-line)#login
```

```
CUNDINAMARCA (config)#hostname CUNDINAMARCA
CUNDINAMARCA (config)#no ip domain-lookup
CUNDINAMARCA (config)#service password-encryption
CUNDINAMARCA (config)#enable secret class
CUNDINAMARCA (config)#line console 0
CUNDINAMARCA (config-line)#password cisco
CUNDINAMARCA (config-line)#login
CUNDINAMARCA (config-line)#LINE VTY 0 15
CUNDINAMARCA (config-line)#password cisco
CUNDINAMARCA (config-line)#login
```

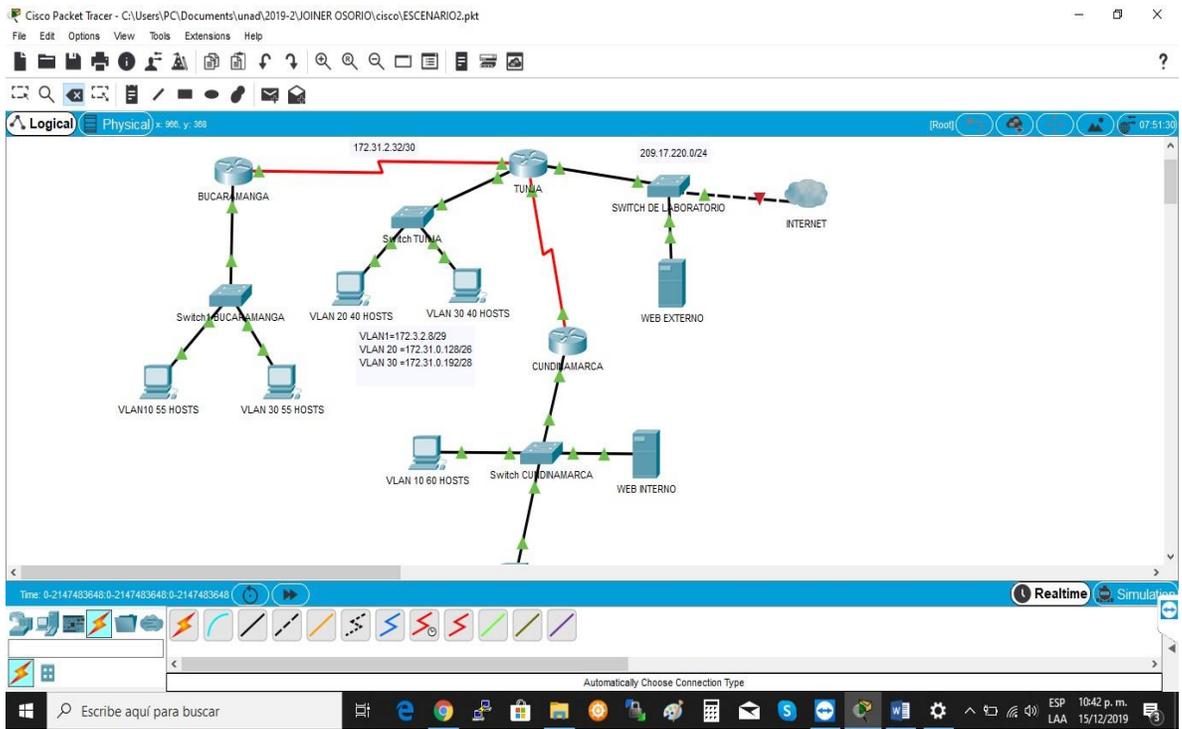


Ilustración 22 - Configuración Equipos Packet Tracer - Fuente Propia

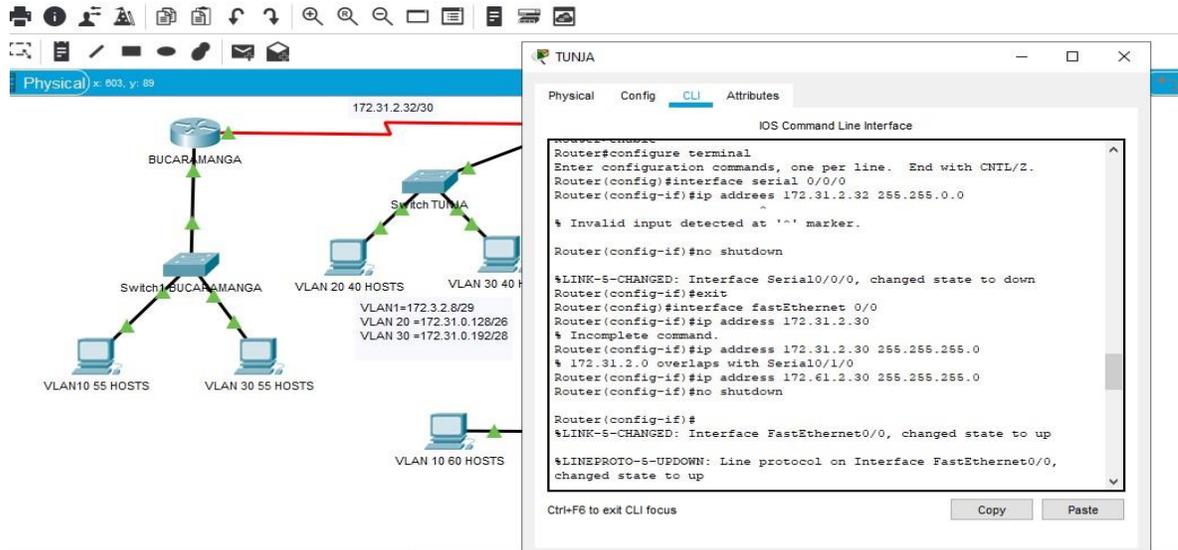


Ilustración 21 - Configuración Equipos Packet Tracer - Fuente Propia

Se utiliza el DHCP pool. LAN Cundinamarca

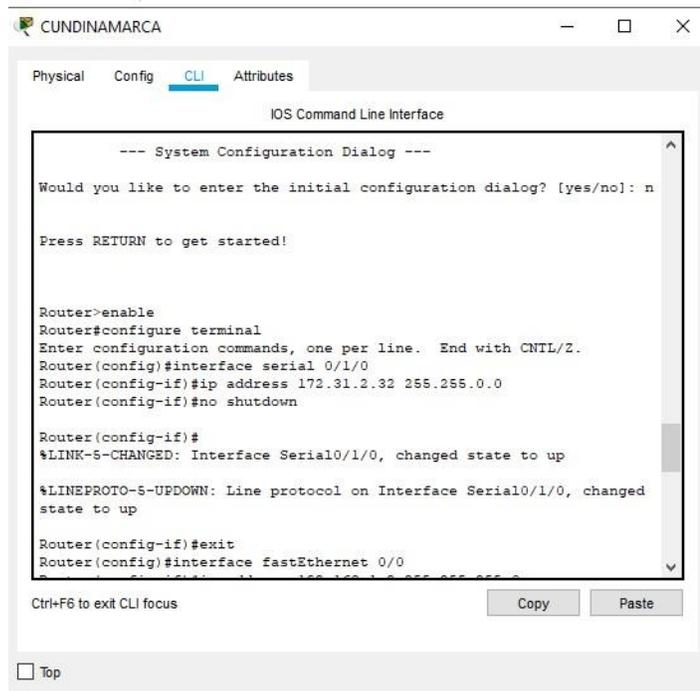


Ilustración 24 - Configuración Cundinamarca - Fuente Propia

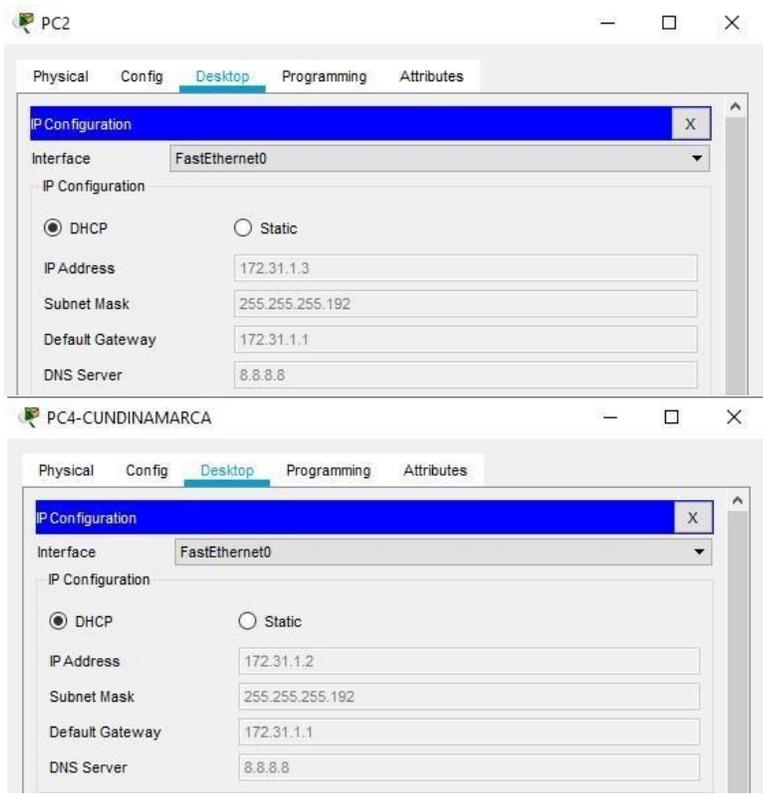


Ilustración 25 - Ilustración 24 - Configuración Cundinamarca - Fuente Propia

Se utiliza el DHCP pool. LAN Bucaramanga

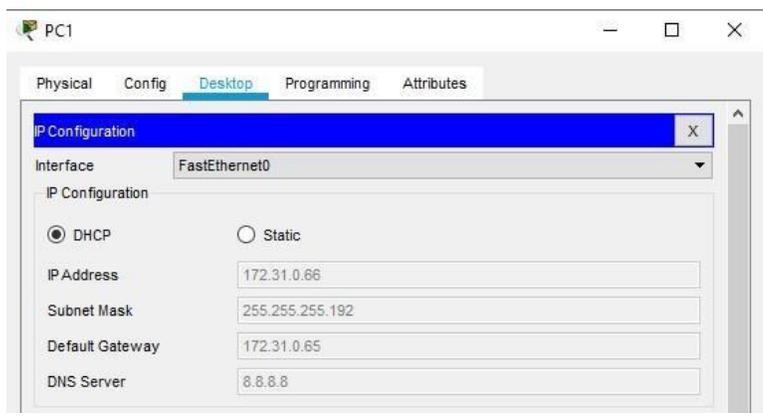




Ilustración 26- Ilustración 24 - Configuración Bucaramanga - Fuente Propia

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

```
TUNJA(config)#ip nat inside source static 172.31.1.67 209.17.220.2
```

```
TUNJA(config)#interface fa0/1
```

```
TUNJA(config-if)#ip nat outside
```

```
TUNJA(config-if)#interface se 0/0/1
```

```
TUNJA(config-if)#ip nat inside
```

```
TUNJA(config-if)#exit
```

```
TUNJA(config)#ip nat inside source static 172.31.1.67 209.17.220.1
```

```
TUNJA(config)#interface fa0/1
```

```
TUNJA(config-if)#ip nat outside
```

```
TUNJA(config-if)#interface se 0/0/1
```

```
TUNJA(config-if)#ip nat inside
```

TUNJA(config-if)#exit

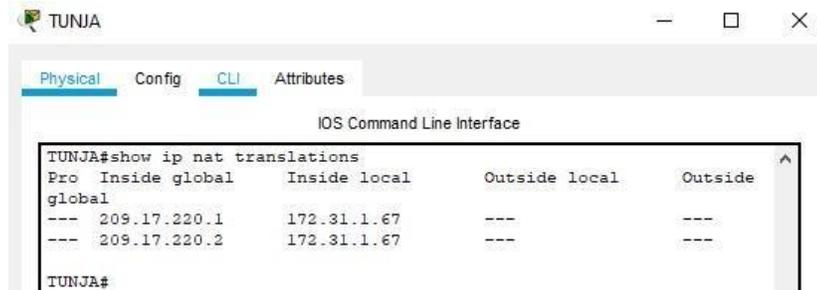


Ilustración 27 - Ilustración 24 - Configuración Tunja - Fuente Propia

Se realiza la configuración de la Nat con sobrecarga (PAT), para esto se crea una access-list donde se agrega cada una de las direcciones que se desean que sean traducidas. A continuación, se usa en la configuración de la nat más la interfaz de salida a internet y el comando overload.

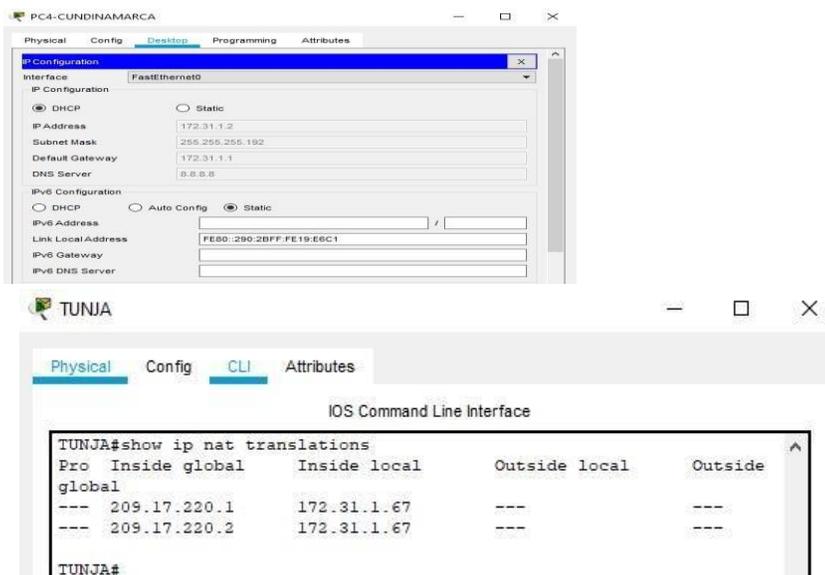


Ilustración 28 - Configuración ciudades - Fuente Propia

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

```
TUNJA(config)#interface se0/0/1
TUNJA(config-if)#ip ospf authentication
TUNJA(config-if)#ip ospf message-digest-key 1 md5 CISCO
TUNJA(config-if)#exit
TUNJA(config)#router ospf 1
TUNJA(config-router)#area 0 authentication
TUNJA(config-router)#
TUNJA(config)#router ospf 1
TUNJA(config-router)#network 172.31.2.32 0.0.0.3 area 0    TUNJA(config-
router)#network 172.31.2.0 0.0.0.7 area 0
TUNJA(config-router)#network 172.31.0.0 0.0.0.63 area 0
TUNJA(config-router)#network 172.31.0.64 0.0.0.63 area 0
TUNJA(config-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.

Se configura de acuerdo a la solicitud

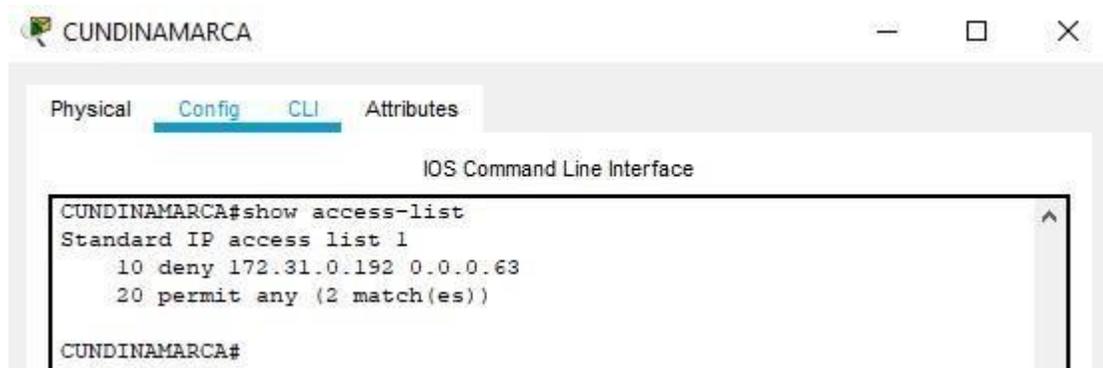
Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.

```
CUNDINAMARCA(config)#access-list 1 deny 172.31.0.192 0.0.0.63
```

```
CUNDINAMARCA(config)#access-list 1 permit any
```

```
CUNDINAMARCA(config)#interface fa0/0
```

```
CUNDINAMARCA(config-if)#ip access-group 1 out
```



*Ilustración 29 - Configuración Cundinamarca - Fuente Propia*

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

```
CUNDINAMARCA(config)#access-list 1 deny 172.31.0.192 0.0.0.63
```

```
CUNDINAMARCA(config)#access-list 1 permit any
```

```
CUNDINAMARCA(config)#interface fa0/0
```

```
CUNDINAMARCA(config-if)#ip access-group 1 out
```

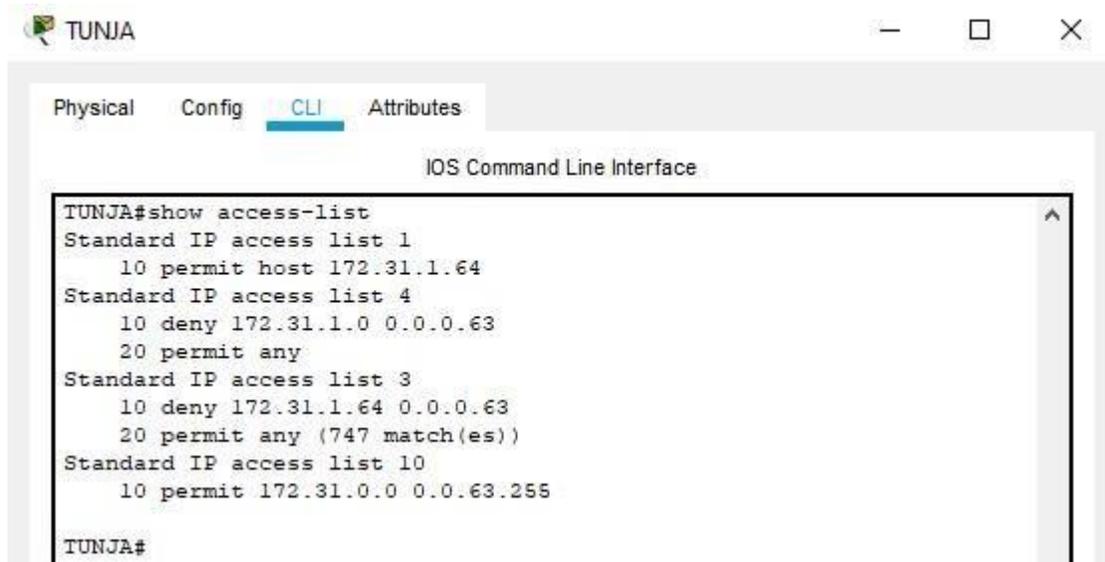
- Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.

```
CUNDINAMARCA(config)#access-list 1 deny 172.31.0.192 0.0.0.63
```

```
CUNDINAMARCA(config)#access-list 1 permit any
```

```
CUNDINAMARCA(config)#interface fa0/0
```

```
CUNDINAMARCA(config-if)#ip access-group 1 out
```



The screenshot shows a window titled 'TUNJA' with a standard Windows-style title bar (minimize, maximize, close). Below the title bar are four tabs: 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is selected and highlighted. The main content area is titled 'IOS Command Line Interface' and displays the output of the command 'show access-list'. The output shows four standard IP access lists:

```
TUNJA#show access-list
Standard IP access list 1
  10 permit host 172.31.1.64
Standard IP access list 4
  10 deny 172.31.1.0 0.0.0.63
  20 permit any
Standard IP access list 3
  10 deny 172.31.1.64 0.0.0.63
  20 permit any (747 match(es))
Standard IP access list 10
  10 permit 172.31.0.0 0.0.63.255
TUNJA#
```

Ilustración 30 - Configuración VLAN Tunja - Fuente Propia

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

10.

```
BUCARAMANGA(config)#access-list 2 permit 209.17.220.0
```

```
BUCARAMANGA (config)#access-list 2 permit host 172.31.0.0
```

```
BUCARAMANGA (config)#access-list 2 deny any
```

```
BUCARAMANGA (config)#interface fa0/0
```

```
BUCARAMANGA (config-if)#ip access-group 2 out
```

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

```
TUNJA(config)#access-list 3 permit 172.31.0.0
```

```
TUNJA(config)#interface fa0/0
```

```
TUNJA(config-if)#ip access-group 3 in
```

```
TUNJA(config-if)#
```

```
CUNDINAMARCA>en
```

```
Password:
```

```
CUNDINAMARCA#conf term
```

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

CUNDINAMARCA(config)#access-list 3 permit 172.31.0.0

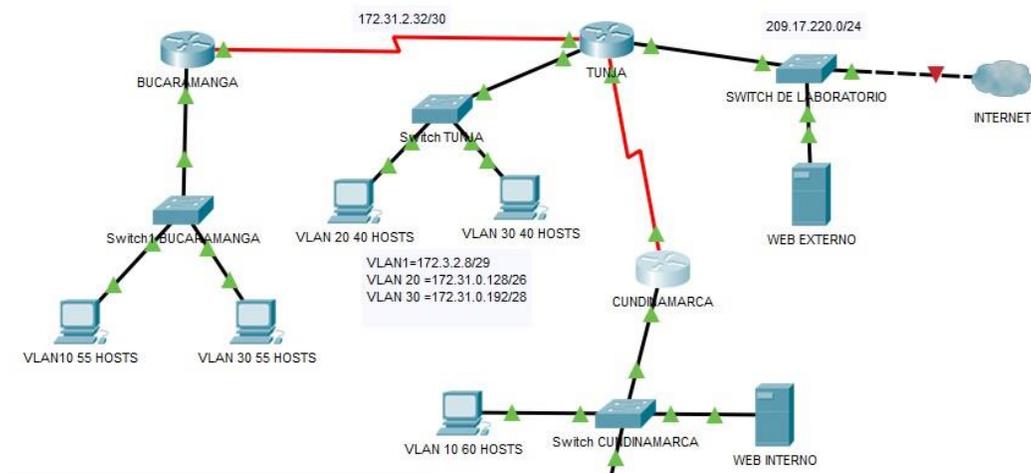
CUNDINAMARCA(config)#interface se0/0/0

CUNDINAMARCA(config-if)#ip access-group 3 in

CUNDINAMARCA(config-if)#

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

Id	Host	Host encontrados	Dirección de red	Mascara de Sub red
1	55	62	172.31.0.0	255.255.255.192
2	55	62	172.31.0.64	255.255.255.192
3	40	62	172.31.0.128	255.255.255.192
4	40	62	172.31.0.192	255.255.255.192
5	60	62	172.31.1.0	255.255.255.192
6	60	62	172.31.1.64	255.255.255.192
7			172.31.1.128	
8			172.31.1.192	
9	6	6	172.31.2.0	255.255.255.248
10	6	6	172.31.2.8	255.255.255.248
11	6	6	172.31.2.16	255.255.255.248
12			172.31.2.24	
13	2	2	172.31.2.32	255.255.255.252
14	2	2	172.31.2.36	255.255.255.252



The screenshot shows the Packet Tracer interface. On the left, the network diagram is visible. On the right, the CLI window for router TUNJA is open, showing the following commands and output:

```

Router>configure terminal
Router#enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 172.31.2.32 255.255.0.0
Router(config-if)#
  
```

The CLI window also shows error messages: "% Invalid input detected at '^' marker." and a "Ctrl+F6 to exit CLI focus" prompt. There are "Copy" and "Paste" buttons at the bottom of the CLI window.

Ilustración 31 - Configuración Final Escenario 2 - Elaborado en Packet Tracer

## CONCLUSIONES

- Se pudo lograr la comprobación de la conectividad de los equipos y encontrar los datos faltantes. También se logró la implementación de las claves de seguridad y la encriptación de las mismas.
- Pudimos identificar el entorno de línea de comando (CLI), incluyendo el ingreso por el modo EXEC de uno de los switch, el cual nos permitió conocer comandos para el ingreso a los modos de configuración tanto global como privilegiado, así mismo la configuración de comandos como lo es Clock (hora)
- Pudimos conocer como el tráfico de un paquete es transmitido de un servidor web a un cliente, así mismo como este paquete se transporta por cada una de las capas de modelo OSI, donde se puede verificar los puertos utilizados, direcciones IP, MAC de cada uno y los diferentes acciones que estos realizan.
- Pudimos identificar mediante la ejecución URL en un web browser como se realiza el proceso de envío y solicitud de paquetes ARP, DNS, HTTP y TCP los cuales viajan a través de los diferentes equipos activos que se encuentran en la red para así desplegarlos en la ventana de un explorador la información solicitada.



## REFERENCIAS

### **Temática: Exploración de la red**

CISCO. (2014). Exploración de la red. Fundamentos de Networking.

Recuperado de <https://static-course->

[assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1](https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1)

### **Temática: Configuración de un sistema operativo de red**

CISCO. (2014). Configuración de un sistema operativo de red. Fundamentos de

Networking. Recuperado de <https://static-course->

[assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1](https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1)

### **Temática: Protocolos y comunicaciones de red**

CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking.

Recuperado de <https://static-course->

[assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1](https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1)

### **Temática: Acceso a la red**

CISCO. (2014). Acceso a la red. Fundamentos de Networking. Recuperado

de <https://static-course->

[assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1](https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1)

**Temática: Ethernet**

CISCO. (2014). Ethernet. Fundamentos de Networking. Recuperado de

<https://staticcourse->

[assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1](https://staticcourse-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1)