

DIPLOMADO DE PROFUNDIZACIÓN CISCO

JOHN HENRY MEDINA GONZALEZ

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA ECBTI

INGENIERIA ELECTRONICA

BOGOTA

2019

DIPLOMADO DE PROFUNDIZACIÓN CISCO

JOHN HENRY MEDINA GONZALEZ

Trabajo presentado como requisito para optar el título de
INGENIERO ELECTRONICO

INGENIERO
GIOVANNI ALBERTO BRACHO

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA ECBTI
INGENIERIA ELECTRONICA

BOGOTA

2019

NOTA DE ACEPTACIÓN

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Bogotá, 15 de diciembre de 2019

DEDICATORIA

A Dios

Quien asumo me guio, me dio fuerzas, paciencia, tolerancia y sobre todo salir avante ante situaciones adversas, y ante todo a no desfallecer en el intento de convertirme en profesional.

A mi familia

Quienes me guiaron por un buen camino, se esforzaron por brindarme apoyo emocional y con su ayuda lograr todos los objetivos que me proponga. A los cuales espero honrar con mis conocimientos y experiencia.

AGRADECIMIENTOS

La universidad Abierta y/a Distancia UNAD, abrió sus puertas brindando la oportunidad de formarme profesionalmente. Los conocimientos adquiridos a través de actividades virtuales, laboratorios, clases presenciales en estos años, permitieron formar no solamente unos conocimientos adecuados como profesional, si no que abren un sin número de puertas, que pretendo abrir y expandir a nuevas aventuras y conocimientos. Mi camino continuo y vienen unas nuevas metas tal vez aún más difíciles, espero seguir contando con mi universidad para cumplirlas.

Agradezco la ayuda brindada por mis compañeros de curso, mis maestros y en general a todos quienes, con su grano de arena, permitieron que se consolidara un ingeniero, un ingeniero con habilidades y destrezas y sobre todo orgulloso de su universidad.

TABLA DE CONTENIDO

1	GLOSARIO	7
2	RESUMEN.....	8
3	ABSTRACT.....	8
4	INTRODUCCIÓN.....	9
5	OBJETIVOS.....	10
5.1	Objetivo General.....	10
5.2	Objetivos Específicos.....	10
6	ESCENARIO 1.....	11
7	ESCENARIO 2.....	36
7.	CONCLUSIONES	50
8.	BIBLIOGRAFIA.....	51

1 GLOSARIO

PACKET TRACER: Packet Tracer es una herramienta de aprendizaje y simulación de redes que trabaja interactivamente, diseñada para instructores y alumnos tecnología Cisco CCNA. Permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales.

ROUTER: Es un dispositivo de hardware que permite la interconexión de ordenadores en red, opera en capa tres de nivel del modelo OSI.

SWITCH: Es un dispositivo que sirve para conectar varios elementos dentro de una red, a saber, un computador, impresora, Consola de videojuegos, en fin, cualquier dispositivo que tenga capacidad de conexión vía Wifi o Ethernet.

DNS: Domain Name System, es un sistema de nomenclatura jerárquico que traduce los nombres de dominio en direcciones numéricas que las máquinas puedan comprender, a este proceso se le denomina resolución de nombres de dominio.

2 RESUMEN

Se analiza, crea, diseña, configura y se realizan las pruebas pertinentes sobre dos escenarios. En el primero se establecen una serie de parámetros para configurar una red en una empresa que posee tres sedes en diferentes ciudades de Colombia. En el segundo escenario una empresa tiene la conexión a internet en una red Ethernet, y se debe adaptar para facilitar la conexión a internet, utilizando las direcciones de la red LAN original.

3 ABSTRACT

The relevant tests on two scenarios are analyzed, created, designed, configured and performed. In the first one, a series of parameters are established to configure a network in a company that has three offices in different cities of Colombia. In the second scenario, a company has an internet connection in an Ethernet network, and it must be adapted to facilitate internet connection, using the addresses of the original LAN.

4 INTRODUCCIÓN

En el presente trabajo se pretende dar a conocer los conocimientos adquiridos en el desarrollo del diplomado Cisco CCNA, se trabaja en conjunto con la herramienta Packet Tracer, en el cual se crea, configura y simula toda la red brindando una representación visual lo cual permite un aprendizaje óptimo sobre este tema.

Se analizan dos escenarios y se realiza la configuración en Packet Tracer demostrando el aprendizaje y las habilidades adquiridas.

5 OBJETIVOS

5.1 OBJETIVO GENERAL

Aplicar de manera sistemática los conocimientos adquiridos durante la formación del diplomado Cisco CCNA, a través de la solución de dos escenarios en los cuales se colocan unos parámetros y configuraciones previamente definidos.

5.2 OBJETIVOS ESPECÍFICOS

Leer e Identificar las actividades a realizar en los escenarios planteados.

Diseñar la topología solicitada y configurar los parámetros básicos en cada dispositivo de la topología.

Realizar los procedimientos pertinentes para adaptar la red a las necesidades solicitadas.

Ejecutar las pruebas garantizando la funcionalidad de las diferentes necesidades planteadas.

6 ESCENARIO 1

Una empresa posee sucursales distribuidas en las ciudades de Bogotá, Medellín y Cali en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

Topología de red

Los requerimientos solicitados son los siguientes:

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

Direccionamiento IP

	Redes				Hosts				
	256	128	64	32	16	8	4	2	# Hosts
Subredes	2	4	8	16	32	64	128	256	
	0	0	0	0	0	0	0	0	
	2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹	2 ⁰	} Valores para encontrar el cuarto octeto
	128	64	32	16	8	4	2	1	
	↓	↓	↓	↓	↓	↓	↓	↓	
	1	1	1	0	0	0	0	0	= 224

Debido a que se necesitan 20 Host en cada red, se realiza la figura 1, el cual identifica la máscara de subred a utilizar para 20 hosts, se identifica el octeto que sirva para contener los 20 host, a continuación, se dibuja una línea al lado izquierdo del host escogido, se identifica que la máscara a utilizar, en este caso clase C es 255.255.255.224

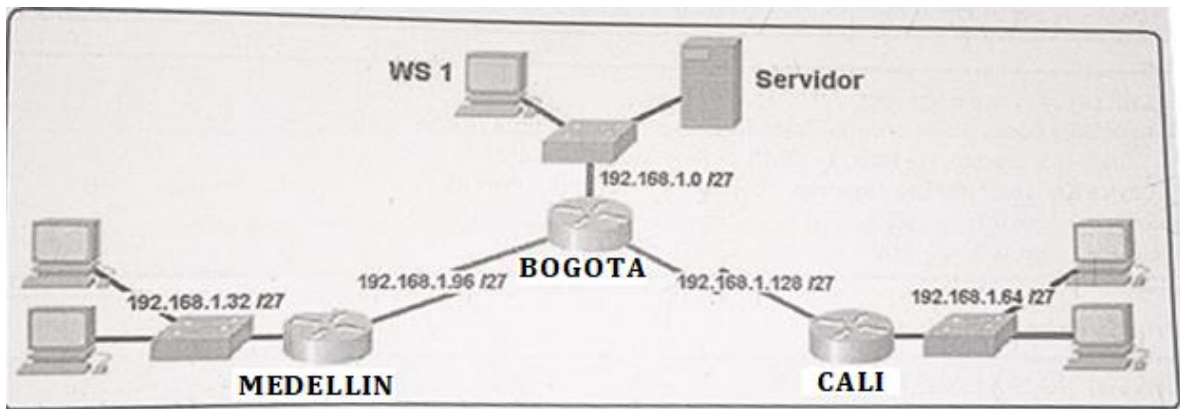
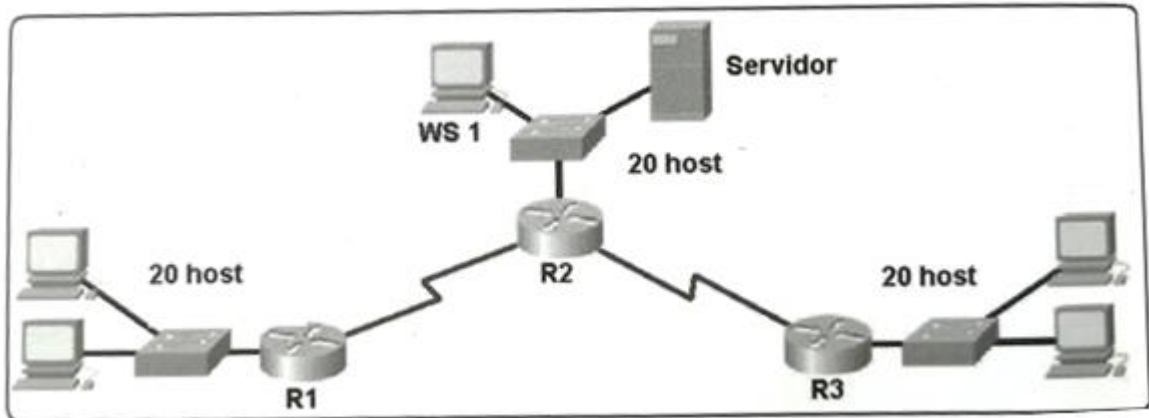
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

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.



Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

```
BOGOTA>en
BOGOTA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#line vty 0 4
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#enable secret cisco
BOGOTA(config)#
```

```

CALI>en
CALI#conf term
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#line vty 0 4
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#exit
CALI(config)#enable secret cisco
CALI(config)#

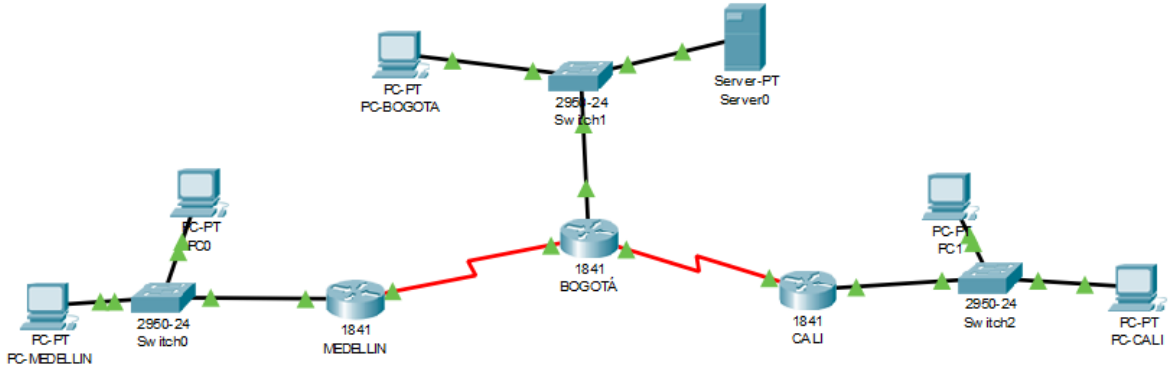
```

```

MEDELLIN>en
MEDELLIN#conf term
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#line vty 0 4
MEDELLIN (config-line)#password cisco
MEDELLIN (config-line)#login
MEDELLIN (config-line)#exit
MEDELLIN (config)#enable secret cisco
MEDELLIN (config)#

```

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 0	192.168.1.0	192.168.1.1	192.168.1.30	192.168.1.31
Red 1	192.168.1.32	192.168.1.33	192.168.1.62	192.168.1.63
Red 2	192.168.1.64	192.168.1.65	192.168.1.94	192.168.1.95
Red 3	192.168.1.96	192.168.1.97	192.168.1.126	192.168.1.127
Red 4	192.168.1.128	192.168.1.129	192.168.1.158	192.168.1.159
Red 5	192.168.1.160	192.168.1.161	192.168.1.190	192.168.1.191
Red 6	192.168.1.192	192.168.1.193	192.168.1.222	192.168.1.223
Red 7	192.168.1.224	192.168.1.225	192.168.1.254	192.168.1.255

b. Asignar una dirección IP a la red.

Se asignan las direcciones ip de acuerdo a la tabla de subneteo.

BOGOTA

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	--	192.168.1.1/27	<not set>	00E0.A362.1501
FastEthernet0/1	Down	--	<not set>	<not set>	00E0.A362.1502
Serial0/0/0	Up	--	192.168.1.98/27	<not set>	<not set>
Serial0/0/1	Up	--	192.168.1.130/27	<not set>	<not set>
Vlan1	Down	1	<not set>	<not set>	00E0.A39D.E7A5

Hostname: BOGOTA

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

CALI

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	--	192.168.1.65/27	<not set>	0001.423D.5601
FastEthernet0/1	Down	--	<not set>	<not set>	0001.423D.5602
Serial0/0/0	Up	--	192.168.1.131/27	<not set>	<not set>
Serial0/0/1	Down	--	<not set>	<not set>	<not set>
Vlan1	Down	1	<not set>	<not set>	0007.EC54.C205

Hostname: CALI

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

MEDELLIN

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	--	192.168.1.33/27	<not set>	0001.C9CA.2501
FastEthernet0/1	Down	--	<not set>	<not set>	0001.C9CA.2502
Serial0/0/0	Up	--	192.168.1.99/27	<not set>	<not set>
Serial0/0/1	Down	--	<not set>	<not set>	<not set>
Vlan1	Down	1	<not set>	<not set>	000C.CF5B.793A

Hostname: MEDELLIN

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

Parte 2: Configuración Básica.

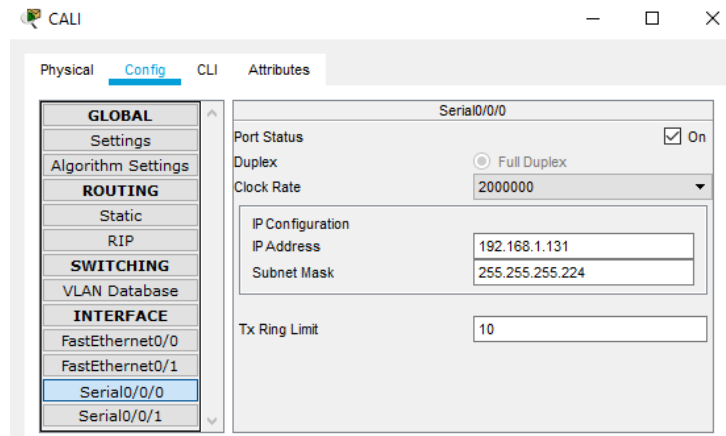
a. Completar la siguiente tabla con la configuración básica de los routers, teniendo en cuenta las subredes diseñadas.

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

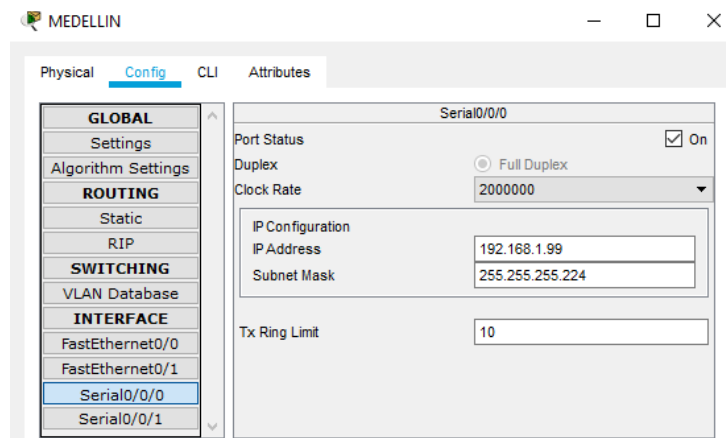
Configuración Router Bogotá

The image displays two screenshots of the Cisco IOS configuration interface for Router Bogotá. The top screenshot shows the configuration for Serial0/0/0, and the bottom screenshot shows the configuration for Serial0/0/1. Both interfaces are configured with Full Duplex and a Clock Rate of 2000000. The IP configuration for Serial0/0/0 is 192.168.1.98 with a Subnet Mask of 255.255.255.224. The IP configuration for Serial0/0/1 is 192.168.1.130 with a Subnet Mask of 255.255.255.224. The Tx Ring Limit is set to 10 for both interfaces.

Configuración Router Cali



Configuración Router Medellín



Se realiza la configuración del sistema autónomo:

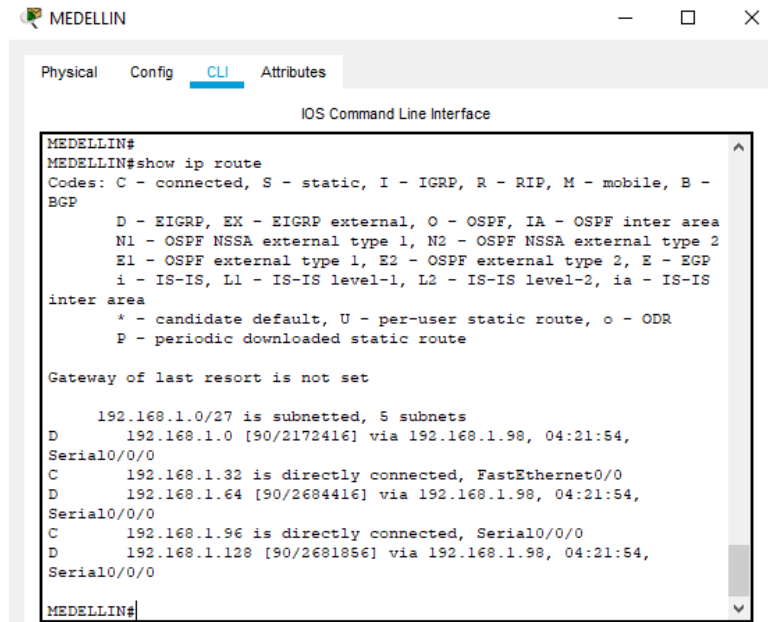
Sistema Autónomo 200, al ingresar con las opciones de eigrp, se asigna el sistema autónomo.

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

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

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

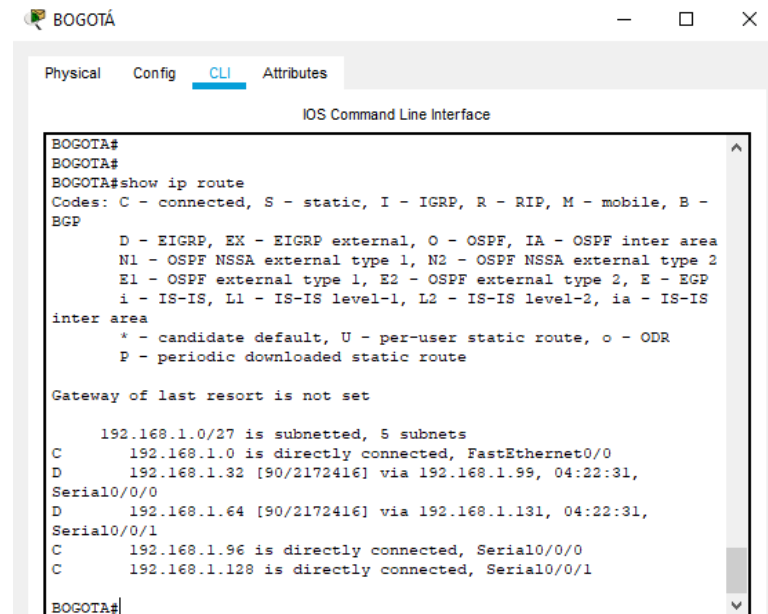
b. Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.



```
MEDELLIN#
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

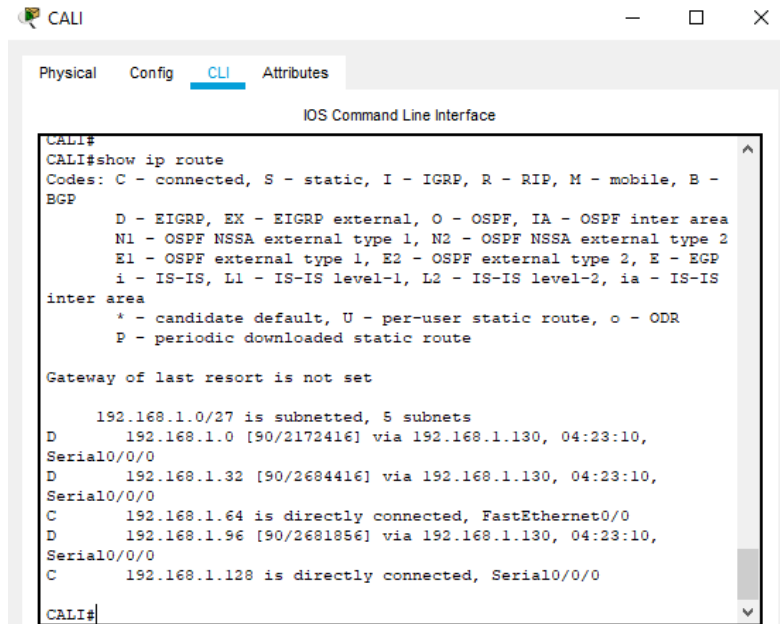
     192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/2172416] via 192.168.1.98, 04:21:54,
Serial0/0/0
C       192.168.1.32 is directly connected, FastEthernet0/0
D       192.168.1.64 [90/2684416] via 192.168.1.98, 04:21:54,
Serial0/0/0
C       192.168.1.96 is directly connected, Serial0/0/0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



```
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#
```



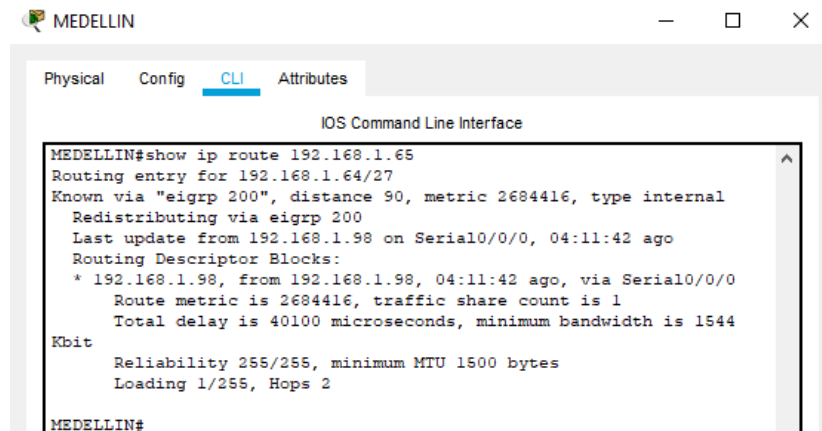
```
CALI#
CALI#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 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#
```

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

El Balanceo de carga describe la funcionalidad en un Router que distribuye paquetes a través de múltiples enlaces según la información de enrutamiento de la capa 3. Si un Router descubre múltiples rutas a un destino, la tabla de enrutamiento se actualiza con múltiples entradas para ese destino.



```
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#
```

```
CALI
Physical Config CLI Attributes
IOS Command Line Interface
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#
```

```
BOGOTÁ
Physical Config CLI Attributes
IOS Command Line Interface
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#
```

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

```
MEDELLIN
Physical Config CLI Attributes
IOS Command Line Interface
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
BOGOTÁ Ser 0/0/0 129 R C1841 Ser
0/0/0
MEDELLIN#
```

```

IOS Command Line Interface
BOGOTA#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge
                S - Switch, H - Host, I - IGMP, r - Repeater, P -
Phone
Device ID      Local Intrfce  Holdtme   Capability   Platform   Port
ID
Switch        Fas 0/0        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
BOGOTA#

```

```

IOS Command Line Interface
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#

```

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

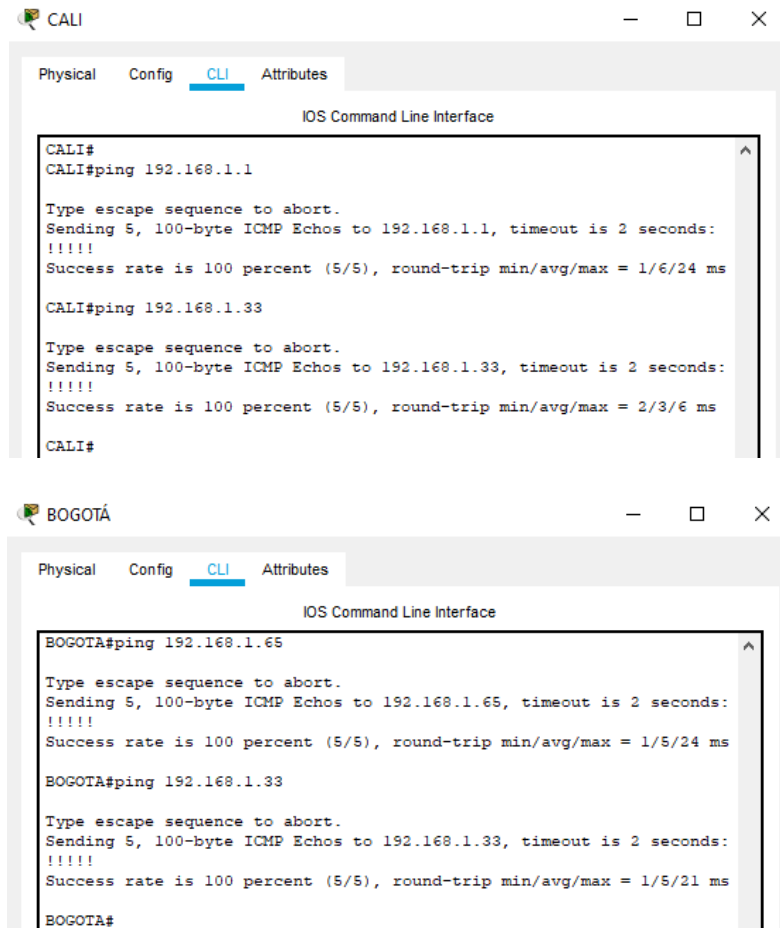
```

IOS Command Line Interface
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#

```



Todos los pings hacia la rutas fueron exitosos

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

```

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

The image shows two screenshots of network device CLI windows. The top window is titled 'MEDELLIN' and the bottom window is titled 'BOGOTÁ'. Both windows show the output of the command 'show ip eigrp neighbors' for process 200.

MEDELLIN Output:

```

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#

```

BOGOTÁ Output:

```

BOGOTÁ#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H Address      Interface      Hold Uptime    SRTT  RTO  Q
Seq
                               (sec)         (ms)          Cnt
Num
0 192.168.1.131 Se0/0/1        10  04:39:02  40   1000  0  7
1 192.168.1.99  Se0/0/0        13  04:39:02  40   1000  0  7

IP-EIGRP neighbors for process 1
BOGOTÁ#

```

IOS Command Line Interface

```

CALI#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H Address          Interface         Hold Uptime      SRTT  RTO  Q
Seq
                               (sec)           (ms)           Cnt
Num
0 192.168.1.130    Se0/0/0          14  04:38:56  40   1000  0  7
IP-EIGRP neighbors for process 1
CALI#

```

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

IOS Command Line Interface

```

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
Physical Config CLI Attributes
IOS Command Line Interface
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

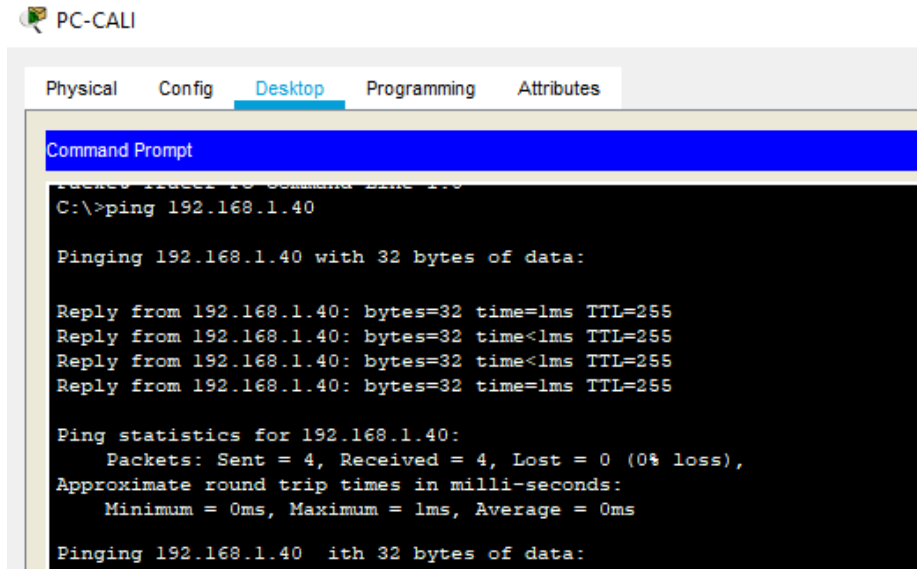
        192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/2172416] via 192.168.1.130, 04:41:20,
Serial0/0/0
D       192.168.1.32 [90/2684416] via 192.168.1.130, 04:41:20,
Serial0/0/0
C       192.168.1.64 is directly connected, FastEthernet0/0
D       192.168.1.96 [90/2681856] via 192.168.1.130,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

```
BOGOTÁ
Physical Config CLI Attributes
IOS Command Line Interface
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, 04:41:46,
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#
```

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



```
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

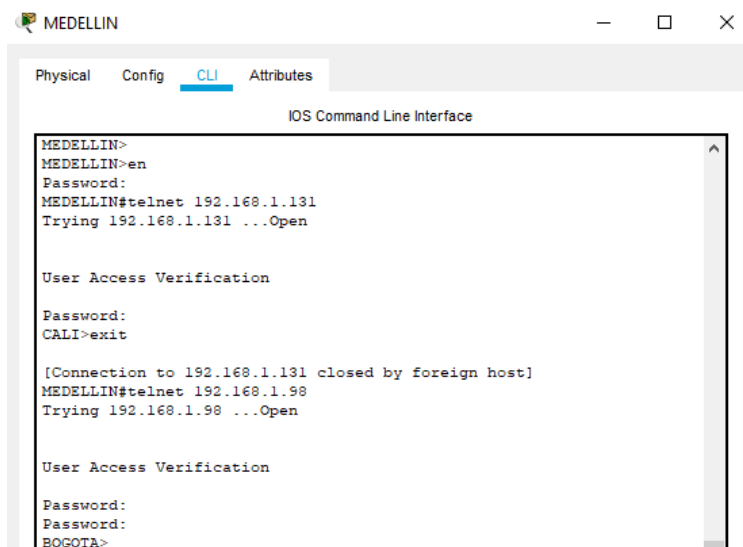
Ping statistics for 192.168.1.40:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

Pinging 192.168.1.40 with 32 bytes of data:
```

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

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

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



```
MEDELLIN
Physical Config CLI Attributes
IOS Command Line Interface
MEDELLIN>
MEDELLIN>en
MEDELLIN#telnet 192.168.1.131
Trying 192.168.1.131 ...Open

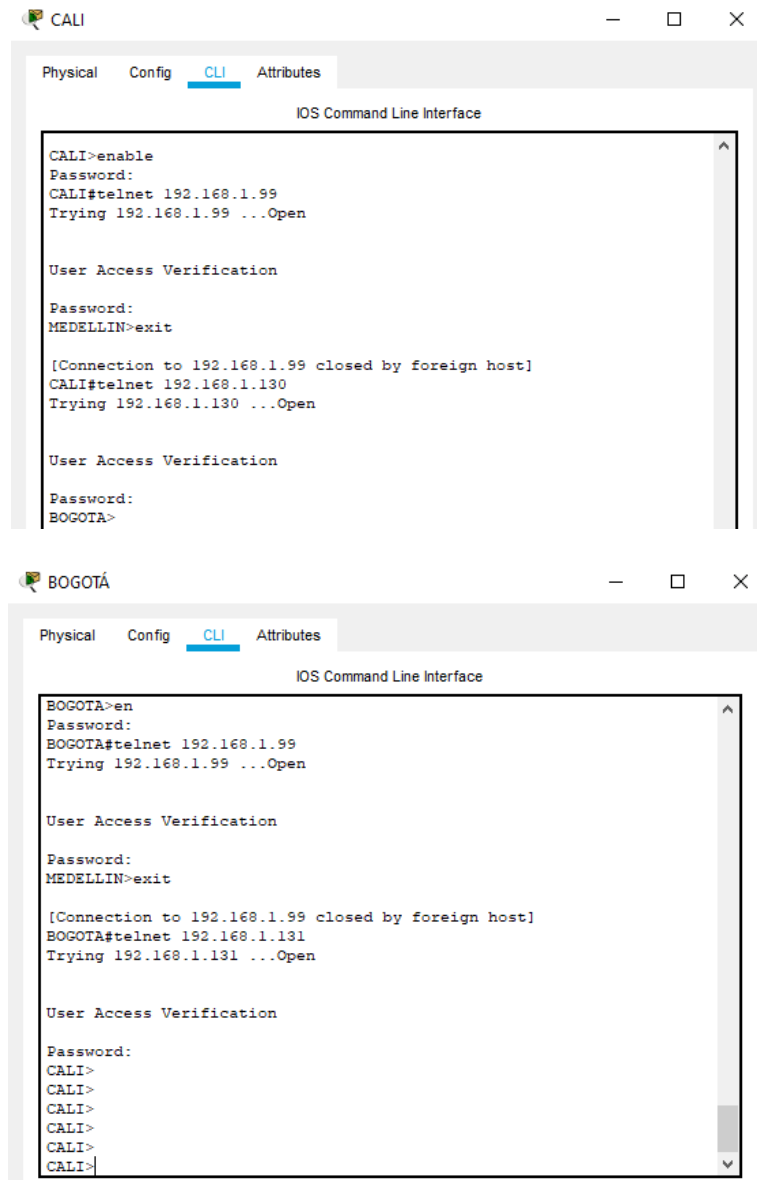
User Access Verification

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

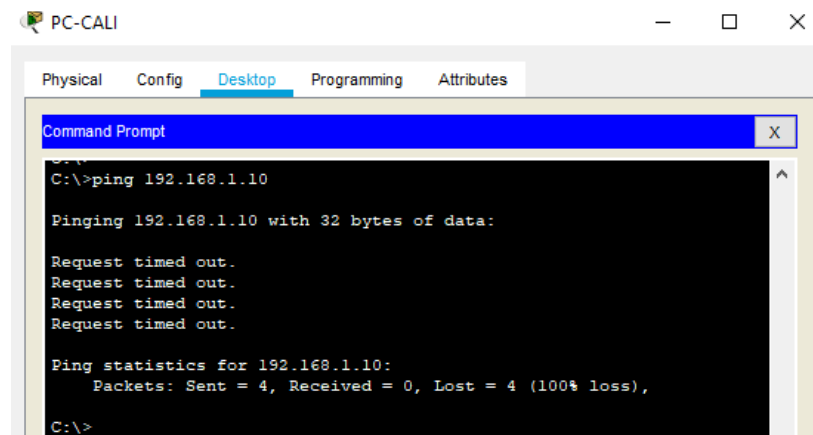
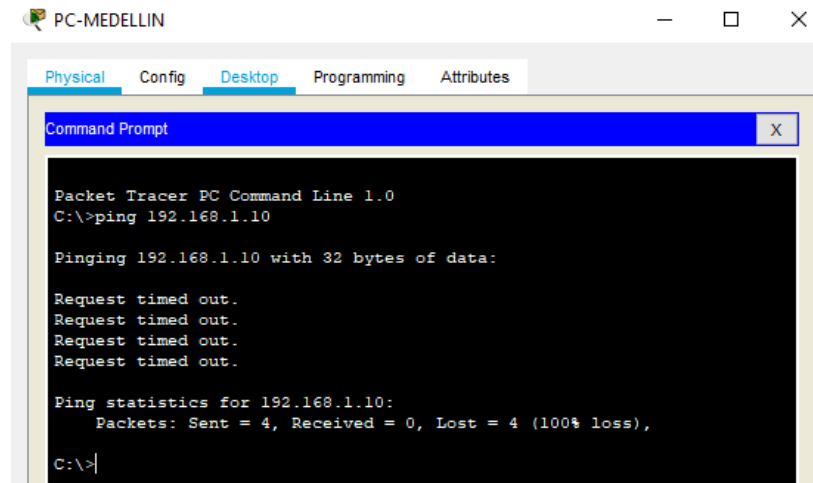
Password:
Password:
BOGOTA>
```



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

```
BOGOTA(config)#access-list 1 deny host 192.168.1.10
BOGOTA(config)#interface fa0/1
BOGOTA(config-if)#ip access-group 1 out
BOGOTA(config-if)#exit
BOGOTA(config)#interface fa0/0
BOGOTA(config-if)#ip access-group 1 out
```

BOGOTA(config-if)#



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

```
CALI(config)#access-list 1 permit host 192.168.1.20
CALI(config)#access-list 1 deny 192.168.1.32 0.0.0.31
CALI(config)#access-list 1 deny 192.168.1.0 0.0.0.31
CALI(config)#interface fa0/0
CALI(config-if)#ip access-group 1 out
CALI(config-if)#exit
```

```

CALI#show access-list
Standard IP access list 1
 10 permit host 192.168.1.20
 20 deny 192.168.1.32 0.0.0.31
 30 deny 192.168.1.0 0.0.0.31 (4 match(es))
CALI#

```

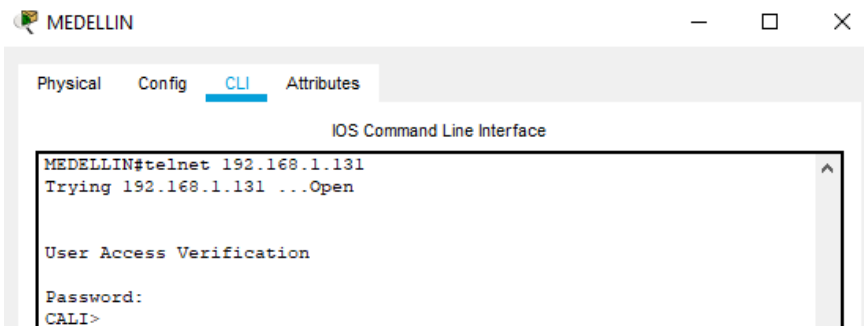
Parte 5: Comprobación de la red instalada.

- a. Se debe probar que la configuración de las listas de acceso fue exitosa.
- b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.

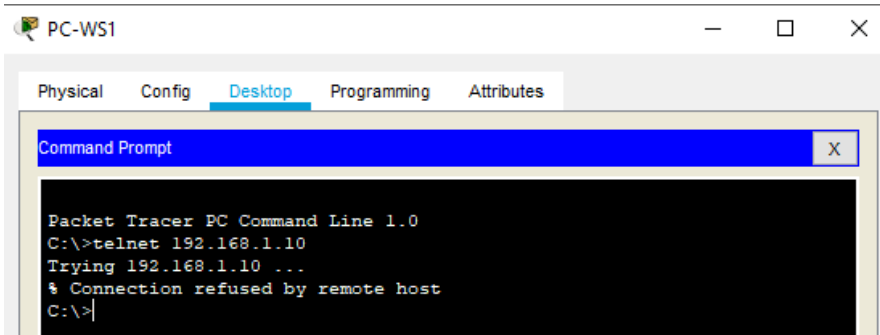
	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	Exitoso
	WS_1	Router BOGOTA	Rechazado
	Servidor	Router CALI	Exitoso
	Servidor	Router MEDELLIN	Exitoso
TELNET	LAN del Router MEDELLIN	Router CALI	Tiempo de conexión agotado; el host remoto no responde
	LAN del Router CALI	Router CALI	Exitoso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

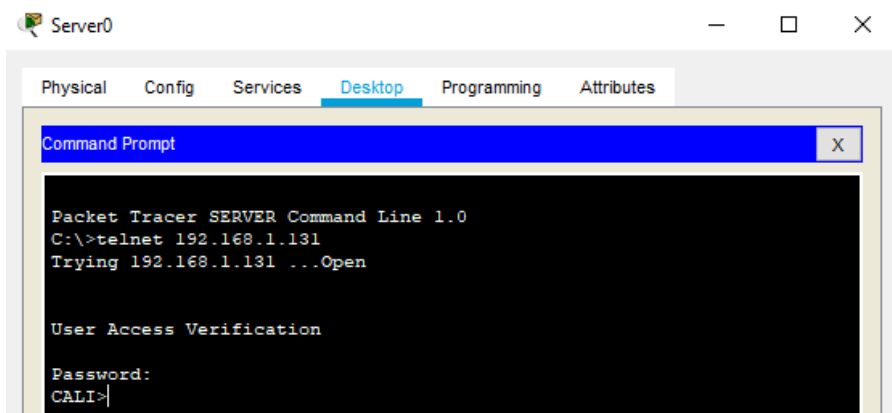
Telnet Router Medellin y Router Cali



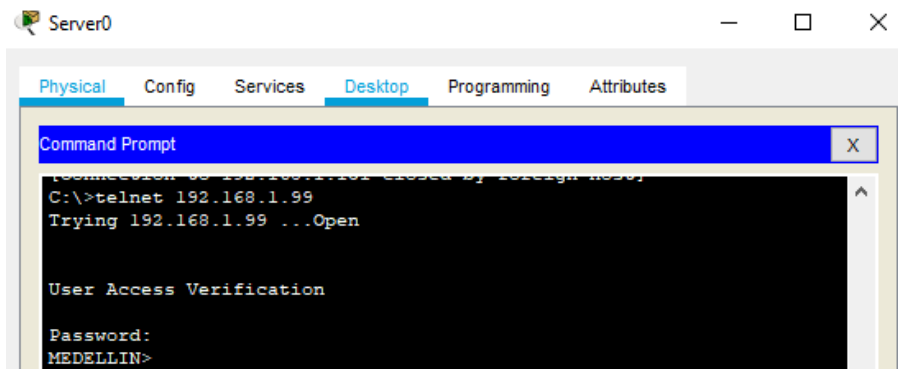
Telnet WS1 a Router Bogota



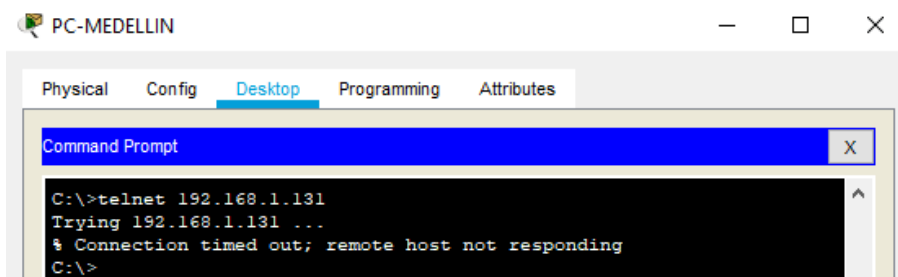
Telnet Servidor – Router Cali



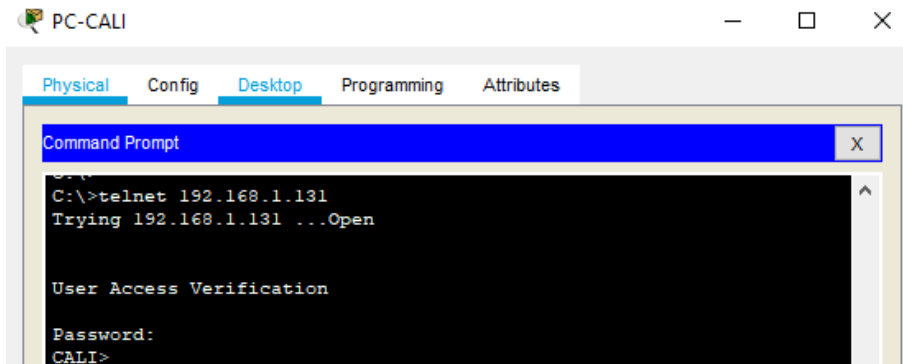
Telnet Servidor – Router Medellin



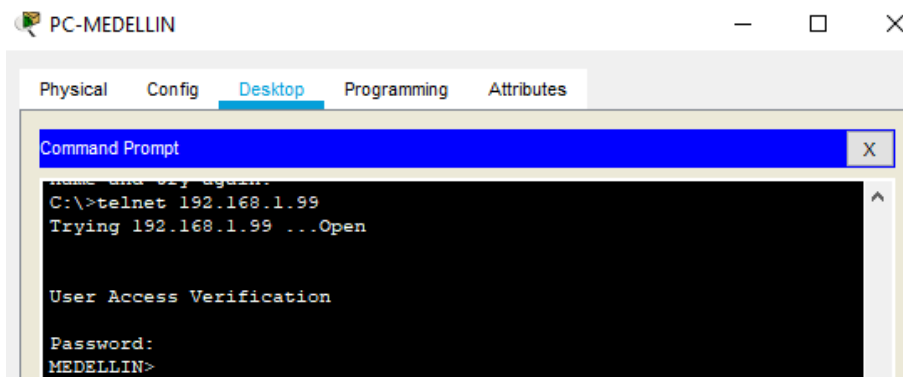
Telnet LAN del Router MEDELLIN Router CALI



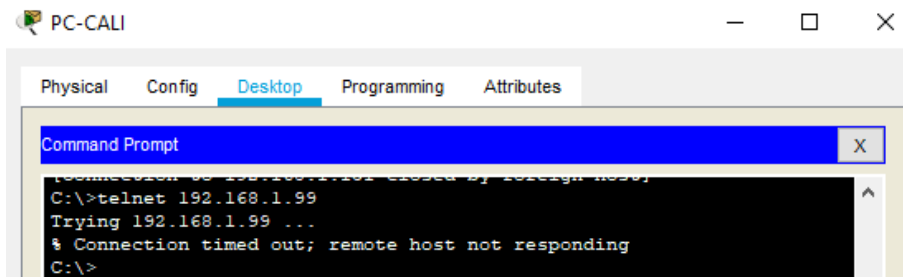
Telnet LAN del Router CALI Router CALI



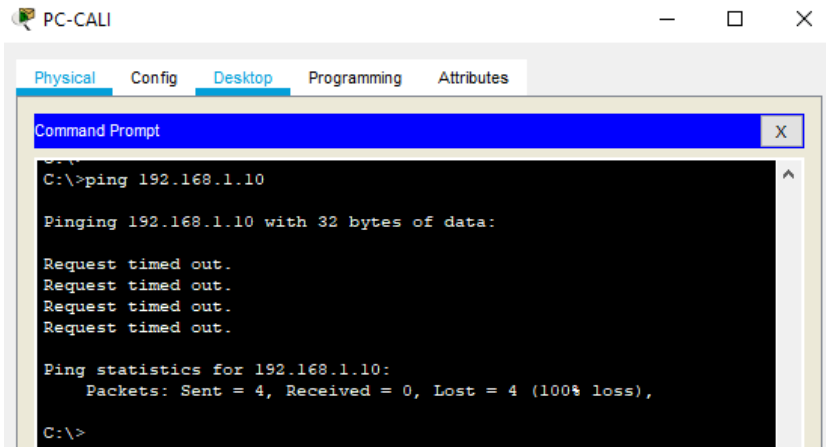
Telnet LAN del Router MEDELLIN Router MEDELLIN



Telnet LAN del Router CALI Router MEDELLIN



Ping LAN del Router CALI WS_1



```
PC-CALI
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.1.10

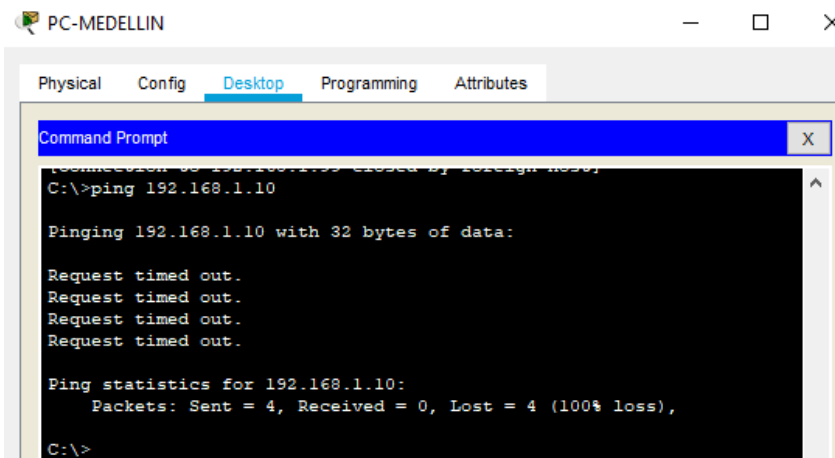
Pinging 192.168.1.10 with 32 bytes of data:

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

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Ping LAN del Router MEDELLIN WS_1



```
PC-MEDELLIN
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.1.10

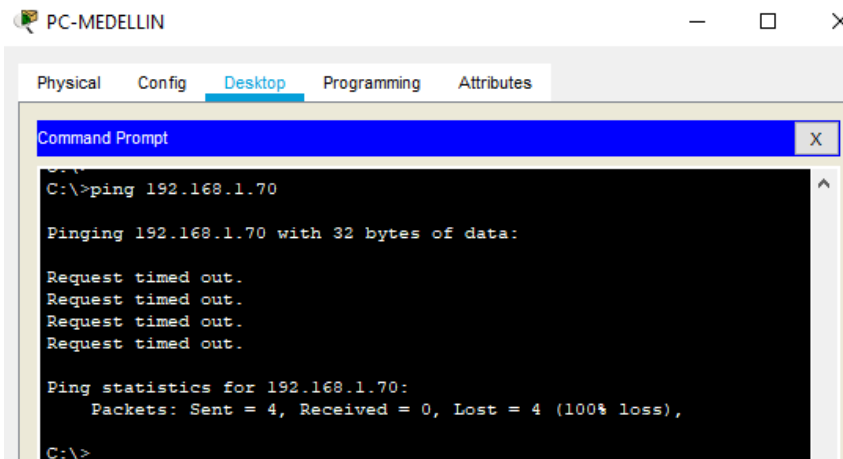
Pinging 192.168.1.10 with 32 bytes of data:

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

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Ping LAN del Router MEDELLIN LAN del Router CALI



```
PC-MEDELLIN
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.1.70

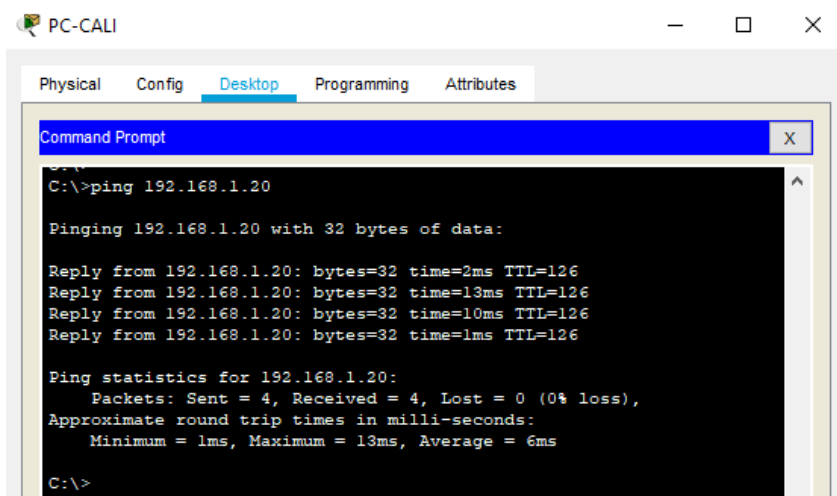
Pinging 192.168.1.70 with 32 bytes of data:

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

Ping statistics for 192.168.1.70:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Ping LAN del Router CALI Servidor



The screenshot shows a window titled "PC-CALI" with a "Command Prompt" window open. The Command Prompt displays the command "ping 192.168.1.20" and its output. The output shows four successful replies with varying round-trip times (2ms, 13ms, 10ms, 1ms) and a ping statistics summary indicating 0% loss.

```
C:\>ping 192.168.1.20

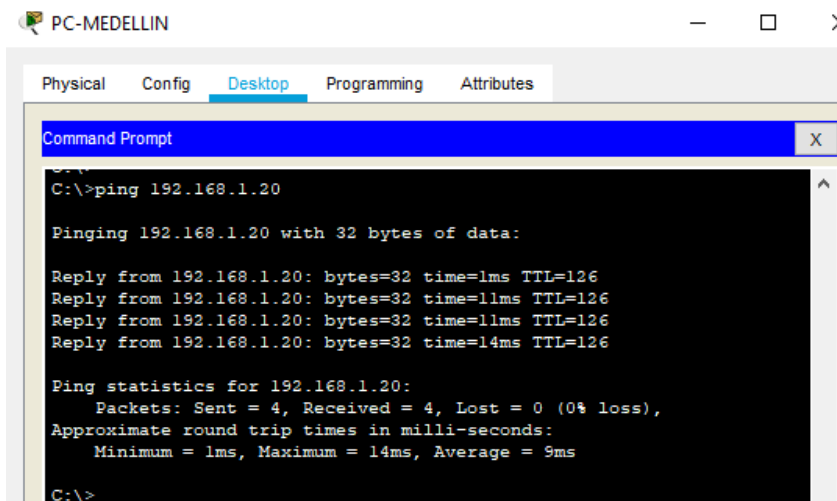
Pinging 192.168.1.20 with 32 bytes of data:

Reply from 192.168.1.20: bytes=32 time=2ms TTL=126
Reply from 192.168.1.20: bytes=32 time=13ms TTL=126
Reply from 192.168.1.20: bytes=32 time=10ms TTL=126
Reply from 192.168.1.20: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 13ms, Average = 6ms

C:\>
```

Ping LAN del Router MEDELLIN Servidor



The screenshot shows a window titled "PC-MEDELLIN" with a "Command Prompt" window open. The Command Prompt displays the command "ping 192.168.1.20" and its output. The output shows four successful replies with round-trip times of 1ms, 11ms, 11ms, and 14ms, and a ping statistics summary indicating 0% loss.

```
C:\>ping 192.168.1.20

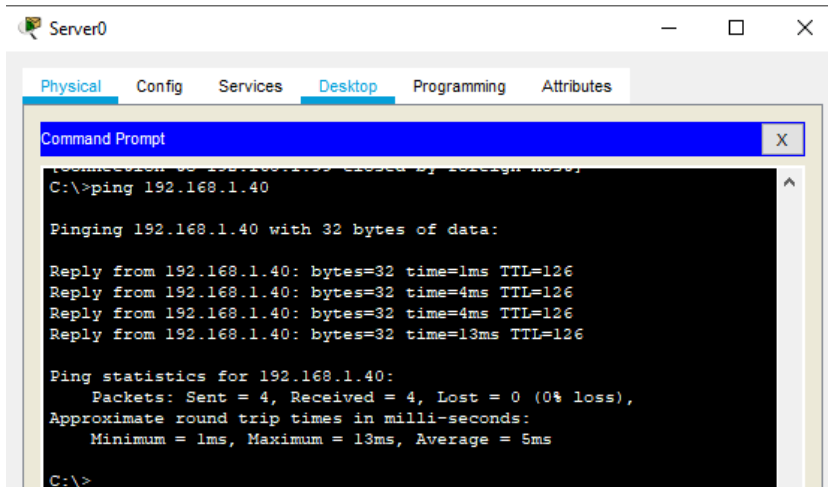
Pinging 192.168.1.20 with 32 bytes of data:

Reply from 192.168.1.20: bytes=32 time=1ms TTL=126
Reply from 192.168.1.20: bytes=32 time=11ms TTL=126
Reply from 192.168.1.20: bytes=32 time=11ms TTL=126
Reply from 192.168.1.20: bytes=32 time=14ms TTL=126

Ping statistics for 192.168.1.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 14ms, Average = 9ms

C:\>
```

Ping Servidor LAN del Router MEDELLIN



```
Server0
Physical Config Services Desktop Programming Attributes
Command Prompt
Connection to 192.168.1.70 closed by foreign host.
C:\>ping 192.168.1.40

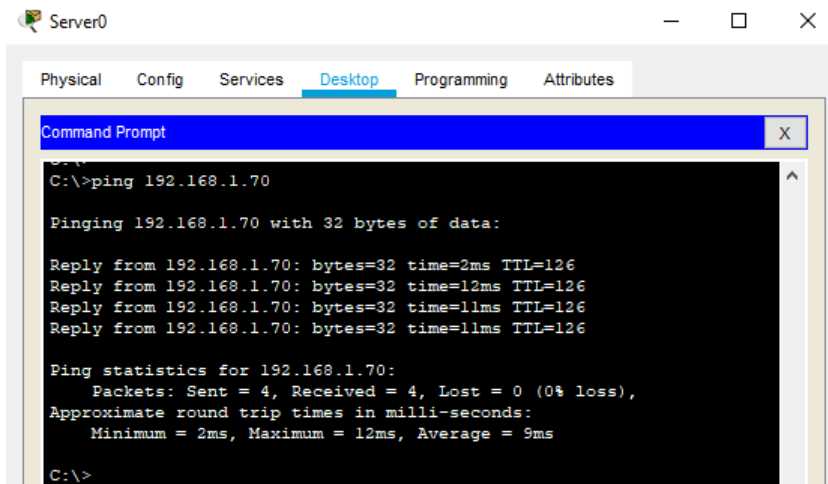
Pinging 192.168.1.40 with 32 bytes of data:

Reply from 192.168.1.40: bytes=32 time=1ms TTL=126
Reply from 192.168.1.40: bytes=32 time=4ms TTL=126
Reply from 192.168.1.40: bytes=32 time=4ms TTL=126
Reply from 192.168.1.40: bytes=32 time=13ms TTL=126

Ping statistics for 192.168.1.40:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 13ms, Average = 5ms

C:\>
```

Ping Servidor LAN del Router CALI



```
Server0
Physical Config Services Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.1.70

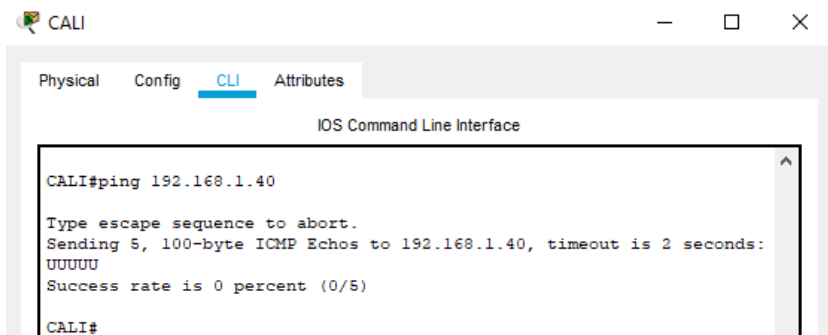
Pinging 192.168.1.70 with 32 bytes of data:

Reply from 192.168.1.70: bytes=32 time=2ms TTL=126
Reply from 192.168.1.70: bytes=32 time=12ms TTL=126
Reply from 192.168.1.70: bytes=32 time=11ms TTL=126
Reply from 192.168.1.70: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.1.70:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 12ms, Average = 9ms

C:\>
```

Ping Router CALI LAN del Router MEDELLIN



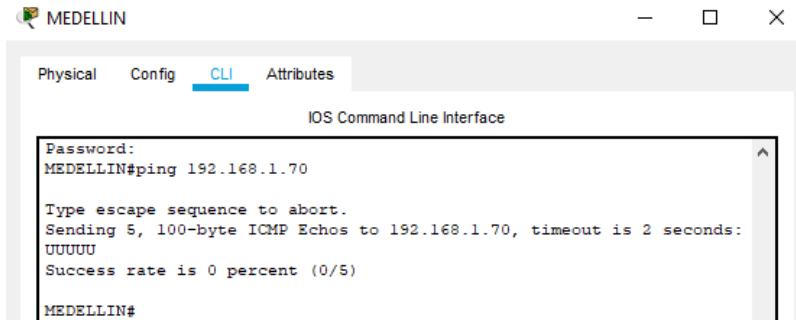
```
CALI
Physical Config CLI Attributes
IOS Command Line Interface

CALI#ping 192.168.1.40

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.40, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)

CALI#
```

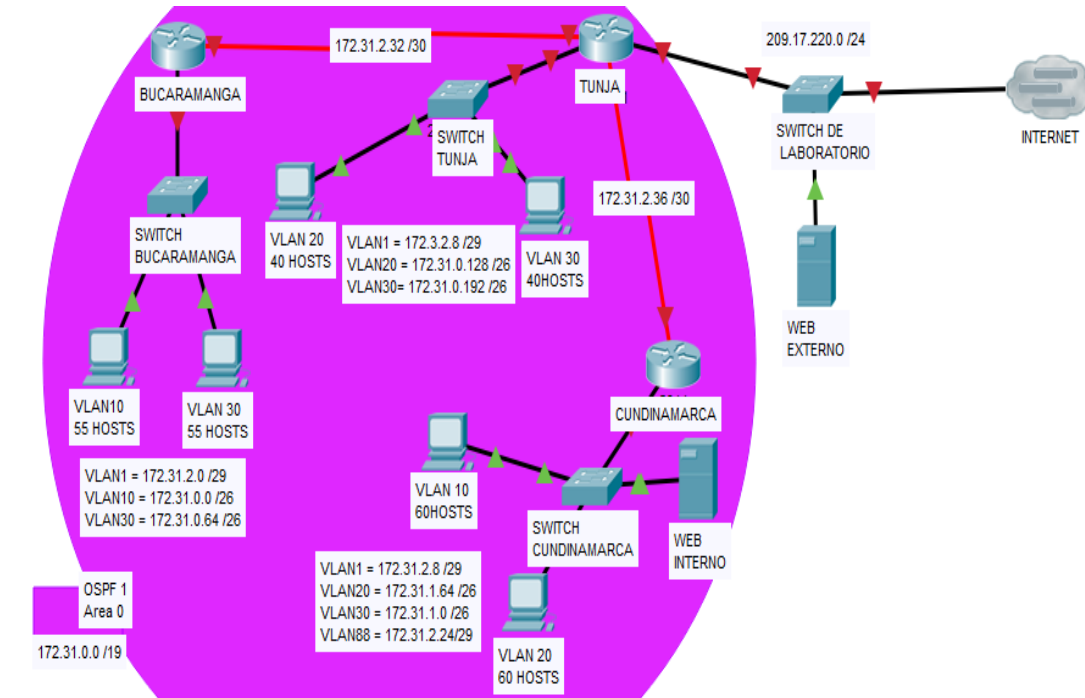
Ping Router MEDELLIN LAN del Router CALI



```
MEDELLIN
Physical Config CLI Attributes
IOS Command Line Interface
Password:
MEDELLIN#ping 192.168.1.70
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.70, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
MEDELLIN#
```

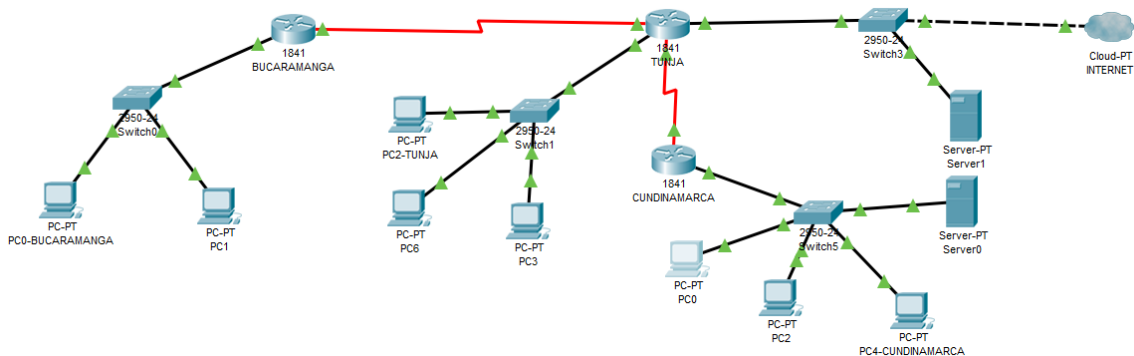
7 ESCENARIO 2

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



Desarrollo

Los siguientes son los requerimientos necesarios:



1. Todos los routers deberán tener los siguiente:

- Configuración básica.

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	--	<not set>	<not set>	0001.4202.1301
FastEthernet0/0.1	Up	--	172.31.2.1/29	<not set>	0001.4202.1301
FastEthernet0/0.10	Up	--	172.31.0.1/26	<not set>	0001.4202.1301
FastEthernet0/0.30	Up	--	172.31.0.65/26	<not set>	0001.4202.1301
FastEthernet0/1	Down	--	<not set>	<not set>	0001.4202.1302
Serial0/0/0	Up	--	172.31.2.33/30	<not set>	<not set>
Serial0/0/1	Down	--	<not set>	<not set>	<not set>
Vlan1	Down	1	<not set>	<not set>	00D0.BAC8.0DC7

Hostname: BUCARAMANGA

Physical Location: Intercity, Home City, Corporate Office, Wiring Closet

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	--	<not set>	<not set>	0030.F242.AB01
FastEthernet0/0.1	Up	--	172.31.2.9/29	<not set>	0030.F242.AB01
FastEthernet0/0.20	Up	--	172.31.0.129/26	<not set>	0030.F242.AB01
FastEthernet0/0.30	Up	--	172.31.0.193/26	<not set>	0030.F242.AB01
FastEthernet0/1	Up	--	209.17.220.1/24	<not set>	0030.F242.AB02
Serial0/0/0	Up	--	172.31.2.34/30	<not set>	<not set>
Serial0/0/1	Up	--	172.31.2.37/30	<not set>	<not set>
Vlan1	Down	1	<not set>	<not set>	0001.C712.0982

Hostname: TUNJA

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	--	<not set>	<not set>	00D0.BAC3.3D01
FastEthernet0/0.1	Up	--	172.31.2.17/29	<not set>	00D0.BAC3.3D01
FastEthernet0/0.20	Up	--	172.31.1.65/26	<not set>	00D0.BAC3.3D01
FastEthernet0/0.30	Up	--	172.31.1.1/26	<not set>	00D0.BAC3.3D01
FastEthernet0/0.88	Up	--	172.31.2.25/29	<not set>	00D0.BAC3.3D01
FastEthernet0/1	Down	--	<not set>	<not set>	00D0.BAC3.3D02
Serial0/0/0	Up	--	172.31.2.38/30	<not set>	<not set>
Serial0/0/1	Down	--	<not set>	<not set>	<not set>
Vlan1	Down	1	<not set>	<not set>	0003.E4DD.E534

Hostname: CUNDINAMARCA

Physical Location: Intercity, Home City, Corporate Office, Wiring Closet

- 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.

Se realiza la siguiente configuración sobre los routers para colocar la autenticación local con aaa, se hace el cifrado de contraseña mediante rsa de 1024 bytes se establece un máximo de intentos de 2 y máximo de tiempo de espera de 60

```

BUCARAMANGA>en
BUCARAMANGA #conf term
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA (config)#line vty 0 4
BUCARAMANGA (config-line)#password cisco
BUCARAMANGA (config-line)#login
BUCARAMANGA (config-line)#exit
BUCARAMANGA (config)#enable secret cisco

```

```

BUCARAMANGA (config)#
BUCARAMANGA(config)#ip domain-name BUCARAMANGA.es
BUCARAMANGA(config)#crypto key generate rsa
% You already have RSA keys defined named
BUCARAMANGA.BUCARAMANGA.es .
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: BUCARAMANGA.BUCARAMANGA.es
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
BUCARAMANGA(config)#ip ssh time-out 60
*mar. 1 0:27:54.589: %SSH-5-ENABLED: SSH 1.99 has been enabled
BUCARAMANGA(config)#ip ssh authentication-retries 2
BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#line vty 0 4
BUCARAMANGA(config-line)#transport input ssh
BUCARAMANGA(config-line)#username Bucaramanga secret password
BUCARAMANGA(config)#

```

```

CUNDINAMARCA>en
CUNDINAMARCA #conf term
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA (config)#line vty 0 4
CUNDINAMARCA (config-line)#password cisco
CUNDINAMARCA (config-line)#login
CUNDINAMARCA (config-line)#exit
CUNDINAMARCA (config)#enable secret cisco
CUNDINAMARCA(config)#ip domain-name CUNDINAMARCA.es
CUNDINAMARCA(config)#crypto key generate rsa
The name for the keys will be: CUNDINAMARCA.CUNDINAMARCA.es
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
CUNDINAMARCA(config)#ip ssh time-out 60
*mar. 1 0:32:51.898: %SSH-5-ENABLED: SSH 1.99 has been enabled
CUNDINAMARCA(config)#ip ssh authentication-retries 2
CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#line vty 0 4
CUNDINAMARCA(config-line)#transport input ssh
CUNDINAMARCA(config-line)#username Cundinamarca secret password

```

CUNDINAMARCA(config)#

TUNJA>en

TUNJA #conf term

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

TUNJA (config)#line vty 0 4

TUNJA (config-line)#password cisco

TUNJA (config-line)#login

TUNJA (config-line)#exit

TUNJA (config)#enable secret cisco

TUNJA(config)#ip domain-name TUNJA.es

TUNJA(config)#crypto key generate rsa

The name for the keys will be: TUNJA.TUNJA.es

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

TUNJA(config)#ip ssh time-out 60

*mar. 1 0:43:46.940: %SSH-5-ENABLED: SSH 1.99 has been enabled

TUNJA(config)#ip ssh authentication-retries 2

TUNJA(config)#aaa new-model

TUNJA(config)#line vty 0 4

TUNJA(config-line)#transport input ssh

TUNJA(config-line)#username Tunja secret password

TUNJA(config)#

Se realiza la siguiente configuración sobre los routers para colocar el servidor tftp

BUCARAMANGA#dir flash:

Directory of flash:/

3 -rw- 33591768 <no date> c1841-advipservicesk9-mz.124-15.T1.bin

2 -rw- 28282 <no date> sigdef-category.xml

1 -rw- 227537 <no date> sigdef-default.xml

64016384 bytes total (30168797 bytes free)

BUCARAMANGA#copy flash: tftp:

Source filename []? c1841-advipservicesk9-mz.124-15.T1.bin

Address or name of remote host []? 172.31.2.20

Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]?

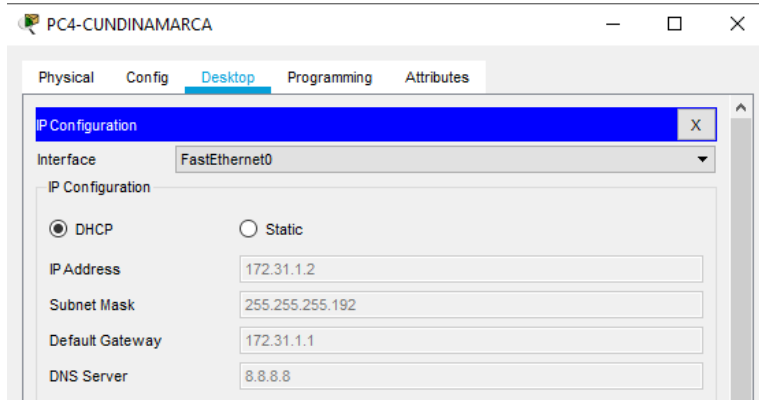
Writing c1841-advipservicesk9-mz.124-15.T1.bin.....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!

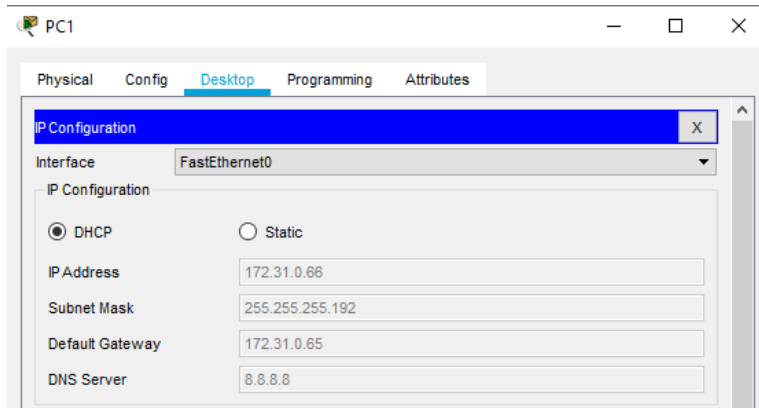
!!

!!

!!

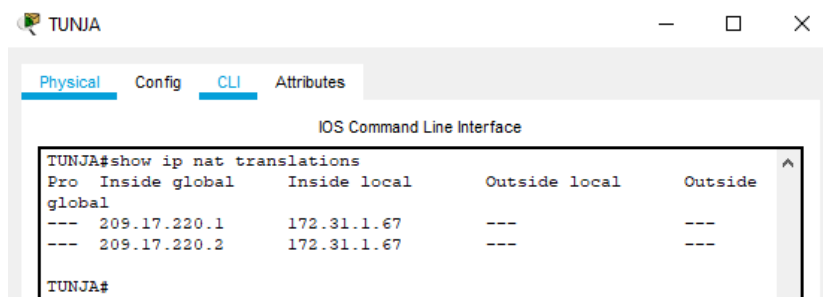


Se utiliza el DHCP pool. LAN Bucaramanga



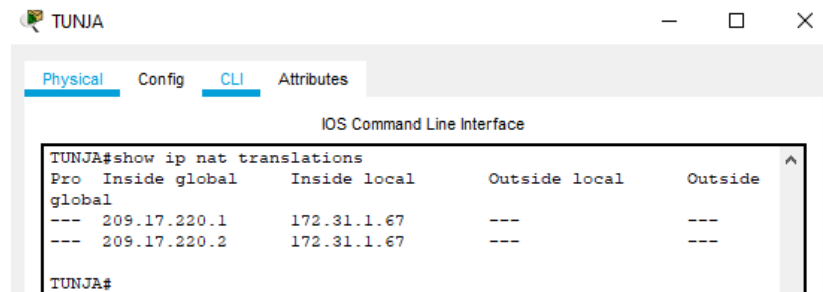
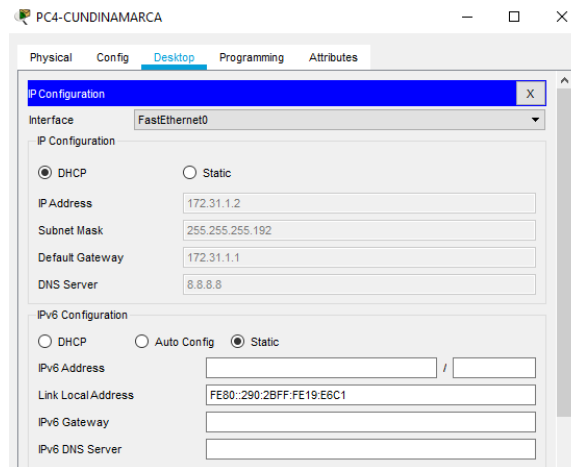
3. El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).

```
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
```



```
TUNJA#show ip nat translations
Pro  Inside global  Inside local  Outside local  Outside
global
---  209.17.220.1   172.31.1.67   ---            ---
---  209.17.220.2   172.31.1.67   ---            ---
TUNJA#
```

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.



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)#
```

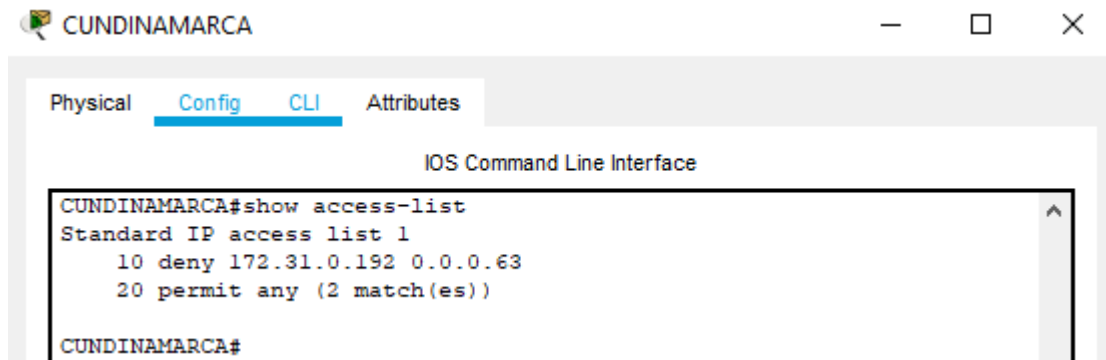
5. Listas de control de acceso:

- 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
```



The screenshot shows a window titled "CUNDINAMARCA" with a standard Windows-style title bar (minimize, maximize, close). The window content is divided into tabs: "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the command "show access-list" and its result: "Standard IP access list 1", "10 deny 172.31.0.192 0.0.0.63", and "20 permit any (2 match(es))". The prompt "CUNDINAMARCA#" is visible at the bottom of the terminal window.

- 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
```

```
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#
```

- 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	Direccion 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

Aspectos a tener en cuenta

- Habilitar VLAN en cada switch y permitir su enrutamiento.
- Enrutamiento OSPF con autenticación en cada router.
- Servicio DHCP en el router Tunja, mediante el helper address, para los routers Bucaramanga y Cundinamarca.

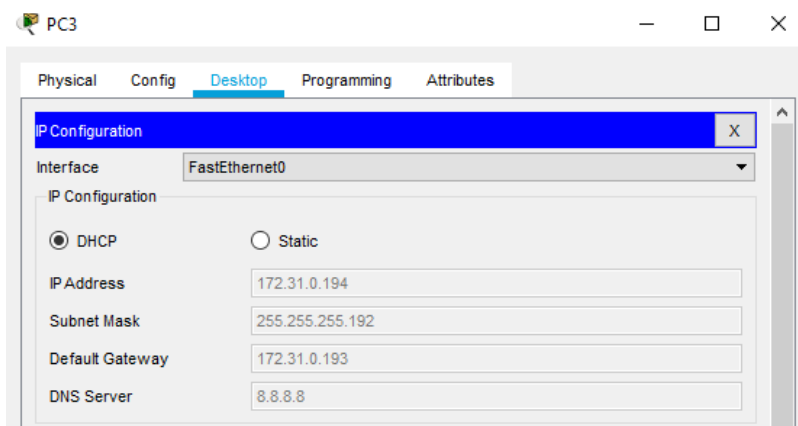
Luego de configurar los pools de direcciones en los router de Bucaramanga y Cundinamarca ingresamos en el modo de configuración del router Tunja, seguidamente entramos en la interfaz por donde vamos a permitir el paso del dhcp que en este caso serían las interfaces y subinterfaces fa0/0, fa0/0.20 y fa0/0.30 para ingresar el comando ip address-helper + la dirección del router que va a proveer el pool de direcciones dhcp

```
TUNJA(config)#no ip dhcp pool 20
```

```

TUNJA(config)#no ip dhcp pool 30
TUNJA(config)#interface fa0/0
TUNJA(config-if)#ip helper-address 172.31.2.33
TUNJA(config-if)#exit
TUNJA(config)#interface fa0/0.20
TUNJA(config-subif)#ip helper-address 172.31.2.38
TUNJA(config-subif)#exit
TUNJA(config)#interface fa0/0.30
TUNJA(config-subif)#ip helper-address 172.31.2.33
TUNJA(config-subif)#exit

```



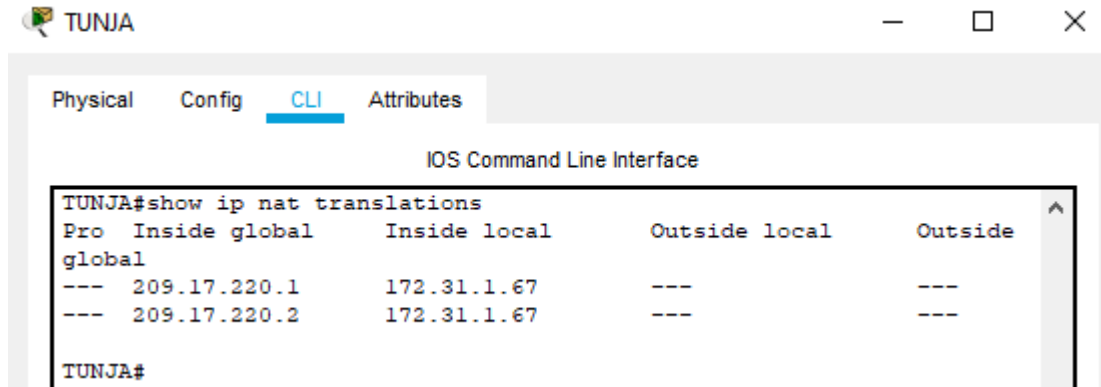
- Configuración de NAT estático y de sobrecarga.

```

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)#interface se0/0/1
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)#interface se0/0/1
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
```



The screenshot shows a window titled 'TUNJA' with a tabbed interface. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The output of the command 'show ip nat translations' is shown in a terminal window. The output is as follows:

```
TUNJA#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside
global
--- 209.17.220.1        172.31.1.67      ---                ---
--- 209.17.220.2        172.31.1.67      ---                ---
TUNJA#
```

- Establecer una lista de control de acceso de acuerdo con los criterios señalados.
- Habilitar las opciones en puerto consola y terminal virtual

7. CONCLUSIONES

Analizar, diseñar, configurar una red desde el parámetro más básico hasta el más complejo, simulando en la herramienta Packet Tracer, reconocer cada uno de los comandos y aplicarlos a nivel profesional en un enrutador físico. El curso de diplomado de CCNA permitió avanzar, recordar y apropiar conocimientos de topologías, redes y modelo OSI. El curso de diplomado de CCNA proporciona herramientas y amplia nuestro campo de conocimientos abriendo puertas en ámbitos laborales como ingeniero.

8. BIBLIOGRAFIA

- Rashid, N. bin A., Othman, M. Z., Johan, R., & Sidek, S. F. bin H. (2019). Cisco Packet Tracer Simulation as Effective Pedagogy in Computer Networking Course. *International Journal of Interactive Mobile Technologies*, 13(10), 4–18. <https://doi-org.bibliotecavirtual.unad.edu.co/10.3991/ijim.v13i10.11283>
- Dumitrache, C. G., Predusca, G., Circiumarescu, L. D., Angelescu, N., & Puchianu, D. C. (2017). Comparative study of RIP, OSPF and EIGRP protocols using Cisco Packet Tracer. 2017 5th International Symposium on Electrical and Electronics Engineering (ISEEE), *Electrical and Electronics Engineering (ISEEE)*, 2017 5th International Symposium On, 1–6. <https://doi-org.bibliotecavirtual.unad.edu.co/10.1109/ISEEE.2017.8170694>
- Creating Ethernet VLANs on Catalyst Switches Cisco. (2017c, 6 junio). Creating Ethernet VLANs on Catalyst Switches. Recuperado 10 diciembre 2019, de <https://www.cisco.com/c/en/us/support/docs/lanswitching/vlan/10023-3.html>
- Cisco Nexus 5000 Series NX-OS Software Configuration Guide Cisco. (2019, 8 mayo). Cisco Nexus 5000 Series NX-OS Software Configuration Guide - Configuring VLANs [Cisco Nexus 5000 Series Switches]. Recuperado 12 diciembre, 2019, de <https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/VLANs.htm>
- Advanced IP Addressing Management Cisco Systems, Inc. (s.f.). CCNP 1: Advanced IP Addressing Management > Objectives. Recuperado 06 diciembre, 2019, de <http://www.ciscopress.com/articles/article.asp?p=330807>
- Configuring a LAN with DHCP and VLANs Cisco. (2007, 26 septiembre). Configuring a LAN with DHCP and VLANs [Support]. Recuperado 06 diciembre, 2019, de <https://www.cisco.com/en/US/docs/routers/access/800/850/software/configuration/guide/dhcpvlan.html>
- Cisco IOS LAN Switching Command Reference Cisco. (2013, 7 octubre). Cisco IOS LAN Switching Command Reference – show vlan through spanning-tree vlan [Support]. Recuperado 07 diciembre, 2019, de https://www.cisco.com/c/en/us/td/docs/ios/lanswitch/command/reference/lsw_book/lsw_s2.html
- IP Addressing Cisco. (2015, 8 diciembre). IP Addressing: DHCP Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) - Configuring the Cisco IOS DHCP Server [Cisco IOS XE 3SE]. Recuperado 08 diciembre, 2019, de <https://www.cisco.com/c/en/us/td/docs/ios->

[xml/ios/ipaddr_dhcp/configuration/xe-3se/3850/dhcp-xe-3se3850-book/config-dhcp-server.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-3se/3850/dhcp-xe-3se3850-book/config-dhcp-server.html)

IP Addressing Cisco. (2017a, 15 julio). IP Addressing: DHCP Configuration Guide, Cisco IOS Release 12.4 - Configuring the Cisco IOS DHCP Client [Support]. Recuperado 09 diciembre, 2019, de https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/12-4/dhcp-12-4-book/config-dhcp-client.html

Configuring InterVLAN Routing with Catalyst Cisco. (2017b, 26 mayo). Configuring InterVLAN Routing with Catalyst 3750/3560/3550 Series Switches. Recuperado 09 diciembre, 2019, de <https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41260-189.html>

Configuring Inter-VLAN Routing with Catalyst 3750 series Cisco. (2017d, 26 mayo). Configuring Inter-VLAN Routing with Catalyst 3750 Series Switches. Recuperado 11 diciembre, 2019, de <https://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-seriesswitches/45002-intervlan3750-45002.html>