

DIPLOMADO DE PROFUNDIZACIÓN CISCO PRUEBA DE HABILIDADES  
PRÁCTICAS CCNP

Diplomado de profundización cisco prueba de habilidades prácticas ccnp

**MIGUEL ANTONIO REDONDO DE LIMA**

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA DE TELECOMUNICACIONES  
BOGOTÁ D.C.

2020

DIPLOMADO DE PROFUNDIZACIÓN CISCO PRUEBA DE HABILIDADES  
PRÁCTICAS CCNP

**MIGUEL ANTONIO REDONDO DE LIMA**

Diplomado de opción de grado presentado para optar el título de  
INGENIERO DE TELECOMUNICACIONES

DIRECTOR:  
MSc. JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA DE TELECOMUNICACIONES  
SANTA MARTA D.T.C.H.

2020

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

---

Firma del Presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

Bogotá D.C. 28 de febrero de 2020

## AGRADECIMIENTOS

Agradezco primero a Dios por hacer posible este sueño, a mi madre por acompañarme y apoyarme en este proceso y a mi padre por guiarme siempre desde el cielo, a todos mis tutores que fueron con los que aprendí todo el fundamento académico que es requerido para obtener mi título, a la Universidad Nacional Abierta y a Distancia UNAD por acogerme como su estudiante y estimular la educación abierta y a distancia por lo que fue una gran opción y a través de este sistema de educación desarrollé competencias y habilidades para la investigación, manejo de software y desarrollo de metodologías, gracias a todos.

## CONTENIDO

AGRADECIMIENTOS .....	4
CONTENIDO .....	5
LISTA DE TABLAS .....	6
LISTA DE FIGURAS .....	7
GLOSARIO .....	9
RESUMEN .....	12
INTRODUCCIÓN .....	14
DESARROLLO .....	15
1. ESCENARIO 1.....	15
2. ESCENARIO 2.....	52
CONCLUSIONES .....	83
BIBLIOGRAFÍA.....	84

## LISTA DE TABLAS

Tabla 1. Subnetea en 8 partes .....	17
Tabla 2. Direcciones IP .....	20
Tabla 3. Configuración básica de los routers .....	21
Tabla 4. Tabla de condiciones de prueba .....	44
Tabla 5. VLSM .....	82

## LISTA DE FIGURAS

Figura 1. Escenario 1 .....	16
Figura 2. Simulación del escenario 1 .....	17
Figura 3. Red de Medellín PC 0 .....	23
Figura 4. Red de Medellín PC 1 .....	23
Figura 5. Red de Cali PC 2 .....	24
Figura 6. Red de Cali PC 3 .....	24
Figura 7. Red de Bogotá WS1 .....	24
Figura 8. Red de Bogotá Server 0 .....	25
Figura 9. Configuración Sucursal Medellín .....	26
Figura 10. Diagnostico sucursal Bogotá.....	29
Figura 11. Diagnostico sucursal Medellín .....	30
Figura 12. Conectividad de la ruta -Ping .....	31
Figura 13. Routers - Bogotá .....	33
Figura 14. Comprobación tablas de enrutamientos- Bogotá .....	36
Figura 15. Comprobación tablas de enrutamientos- Medellín.....	37
Figura 16. Comprobación tablas de enrutamientos- Cali .....	38
Figura 17. Diagnóstico para comprobar que cada uno de los puntos de la red- Medellín .....	39
Figura 18. Verificación LAN .....	41
Figura 19. Lista de acceso exitosa.....	42
Figura 20. Ping desde WS1 hacia PC0 y PC1 .....	43
Figura 21. Ping desde Medellín hacia Server0 y Cali.....	43

Figura 22. Ping desde Cali hacia Server0 y Medellín.....	44
Figura 23. Escenario 2 .....	52
Figura 24. topología del escenario 2.....	53
Figura 25. Server 88 .....	61
Figura 26. PC 10.....	63
Figura 27. PC 11.....	64
Figura 28. PC 14.....	64
Figura 29. PC 15.....	65
Figura 30. Verificación en PC 15 .....	69
Figura 31. Router 0 .....	70
Figura 32, Verificación PC 14 .....	72
Figura 33. Verificación PC 15 .....	73
Figura 34. Verificación PC 13 .....	74
Figura 35 Verificación navegación en PC 13 .....	74
Figura 36. Verificación PC 12 .....	75
Figura 37. Verificación PC 11 .....	76
Figura 38. Verificación PC 10 .....	77
Figura 39. Comando prompt pc 12.....	79
Figura 40 . Destinatario PC 10.....	79
Figura 41. Switch 1 .....	81
Figura 42. Switch2 .....	81



## GLOSARIO

**ACCESS POINT:** Se trata de un dispositivo utilizado en redes inalámbricas de área local (WLAN - Wireless Local Area Network), una red local inalámbrica es aquella que cuenta con una interconexión de computadoras relativamente cercanas, sin necesidad de cables, estas redes funcionan a base de ondas de radio específicas. El Access Point entonces se encarga de ser una puerta de entrada a la red inalámbrica en un lugar específico y para una cobertura de radio determinada, para cualquier dispositivo que solicite acceder, siempre y cuando esté configurado y tenga los permisos necesarios.

**CABLEADO ESTRUCTURADO:** el concepto de cableado estructurado es tender cables de señal en un edificio de manera tal que cualquier servicio de voz, datos, vídeo, audio, tráfico de Internet, seguridad, control y monitoreo esté disponible desde y hacia cualquier roseta de conexión del edificio. Esto es posible distribuyendo cada servicio a través del edificio por medio de un cableado estructurado estándar con cables de cobre o fibra óptica. Esta infraestructura es diseñada, o estructurada para maximizar la velocidad, eficiencia y seguridad de la red. Ninguna inversión en tecnología dura más que el sistema de cableado, que es la base sobre la cual las demás tecnologías operarán.

**INTERNET:** una amplia red global de estaciones de trabajo derivada de una red militar que se comenzó a desarrollar en 1969, en los Estados Unidos (ARPANET). ARPANET fue diseñada para ser confiable, en el sentido de que si una zona de la red era dañada, por un accidente o ataque enemigo, los mensajes entre las otras computadoras serían automáticamente redireccionados; lo que hizo que este tipo de red se popularizara y se convirtiera en el estándar actual de comunicación entre computadoras. Internet se apoya en varias tecnologías, entre ellas la familia de protocolos TCP/IP.

**IPV4:** versión 4 del protocolo IP (Internet Protocol). Es el estándar actual de Internet para identificar dispositivos conectados a esta red.

**ROUTER:** dispositivo físico o lógico que permite encaminar la conexión entre redes TCP/IP, es el encargado de que los paquetes de información lleguen a su destino.

**SWITCH:** dispositivo capaz de enlazar físicamente varios ordenadores de forma activa, enviando los datos exclusivamente al ordenador al que van destinados.

**TOPOLOGÍA DE RED:** es el término técnico que se utiliza para describir la disposición física en la que está configurada una red.

**RED LAN:** (Local Area Network) Red de Área Local. Como su nombre indica, es una red de ordenadores de tamaño pequeño/medio localizada en un edificio (como máximo). Se conectan los ordenadores a través de tarjetas de red, y las arquitecturas más conocidas son Ethernet y Token-Ring.

**RED WAN:** (Wide Area Network) Red de ordenadores extensa, se entiende que va más allá de un edificio.

**DIRECCIÓN IP:** una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del protocolo TCP/IP.

**CABLEADO HORIZONTAL:** El cableado horizontal es la porción del sistema de cableado de las telecomunicaciones que va del área de trabajo a la conexión cruzada horizontal en el armario de telecomunicaciones.

**CABLEADO VERTICAL (BACKBONE):** El propósito del cableado del backbone es proporcionar interconexiones entre cuartos de entrada de servicios de edificio, cuartos de equipo y cuartos de telecomunicaciones. El cableado del backbone incluye la conexión vertical entre pisos en edificios de varios pisos. El cableado del backbone incluye medios de transmisión (cable), puntos principales e intermedios de conexión cruzada y terminaciones mecánicas. El cableado vertical realiza la interconexión entre los diferentes gabinetes de telecomunicaciones y la sala de equipamiento.

**CIFRADO:** En criptografía un cifrado, es un procedimiento que utilizando un algoritmo (algoritmo de cifrado) con cierta clave (clave de cifrado) transforma un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender, a toda persona que no tenga la

clave secreta (clave de descifrado) del algoritmo que se usa para poder descifrarlo (algoritmo de descifrado). Por tanto tenemos dos algoritmos (el de cifrado y el de descifrado) y dos claves (clave de cifrado y clave de descifrado). Estas dos claves pueden ser iguales (criptografía simétrica) o no (criptografía asimétrica).

**POP OF PRESENCE (POP):** Punto de presencia (POP) es un lugar preparado por un ISP para conectar a sus usuarios a través de Internet. En los POP, los routers, el backbone se conectan a la red troncal de Internet para dar cabida a la conectividad de los usuarios que están instalados.

## RESUMEN

Este proyecto está orientado al conocimiento y aplicación del nuevo sistema LAN-WAN el cual está orientado a la conceptualización, configuración y resolución de problemas de protocolos de enrutamiento de tipo vector distancia y estado de enlace, para el desarrollo de una efectiva gestión tecnológica de acuerdo a las exigencias de un mundo globalizado en el área de las telecomunicaciones, incorporando distintas herramientas tecnológicas modernas lo cual conlleva a la creatividad, innovación como factores determinantes para obtener soluciones que permitan el éxito de la investigación. Corresponde la actividad a la prueba de habilidades como última evaluación del Diplomado de profundización CCNP, la prueba de habilidades está compuesta por dos escenarios diferentes, donde se evidencia por medio de la solución lo aprendido durante el desarrollo de todo el diplomado.

Palabras clave: CISCO, CCNP, Redes, Electrónica, Protocolo IP.

## ABSTRACT

This project is oriented to the knowledge and application of the new LAN-WAN system which is oriented to the conceptualization, configuration and resolution of routing protocols of distance vector type and link state, for the development of an effective technological management agreement to the demands of a globalized world in the area of telecommunications, incorporating different modern technological tools which leads to creativity, innovation as determining factors to obtain solutions that allow research success. The activity corresponds to the skills test as the last evasion of the CCNP deepening Diploma, the skills test is composed of two different scenarios, where it is evidenced through the solution what was learned during the development of the entire diploma.

Keywords: CISCO, CCNP, Networking, Electronics, IP Protocol.

## INTRODUCCIÓN

Las telecomunicaciones son necesarias para suministrar toda información, lo cual permite el fácil acceso a una inmensa red de información, proporcionan un desempeño rápido y factible para todo tipo de datos, canales de comunicación inmediata, capacidad de un excelente almacenamiento, automatización de trabajos, interactividad y la digitalización de toda la información que se requiera en el momento. La revolución tecnológica que existe en el mundo actualmente es proporcionada gracias a los avances significativos de CISCO

Este documento muestra la combinación de los módulos del diplomado CCNA y CCNP de CISCO, al brindar desde lo aprendido la solución a la propuesta de dos escenarios usando las redes de datos, por medio de los dispositivos activos router y switch simulados en herramientas como Packet Tracer. En la primera parte se realizó la configuración y conexión de los dispositivos presentados en la figura indicada, teniendo en cuenta lo aprendido para el direccionamiento IP, protocolos de enrutamiento y lo relacionado con la topología de red indicada.

Se realizó en el segundo escenario también el direccionamiento IP, etherchannels, VLANs y todo lo correspondiente para brindar la solución a este escenario; para llegar al final a las conclusiones de todo lo aprendido e indicar las dificultades que hallamos en estos dos retos.

## DESARROLLO

### 1. ESCENARIO 1

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

#### **Topología de red**

Los requerimientos solicitados son los siguientes:

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

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

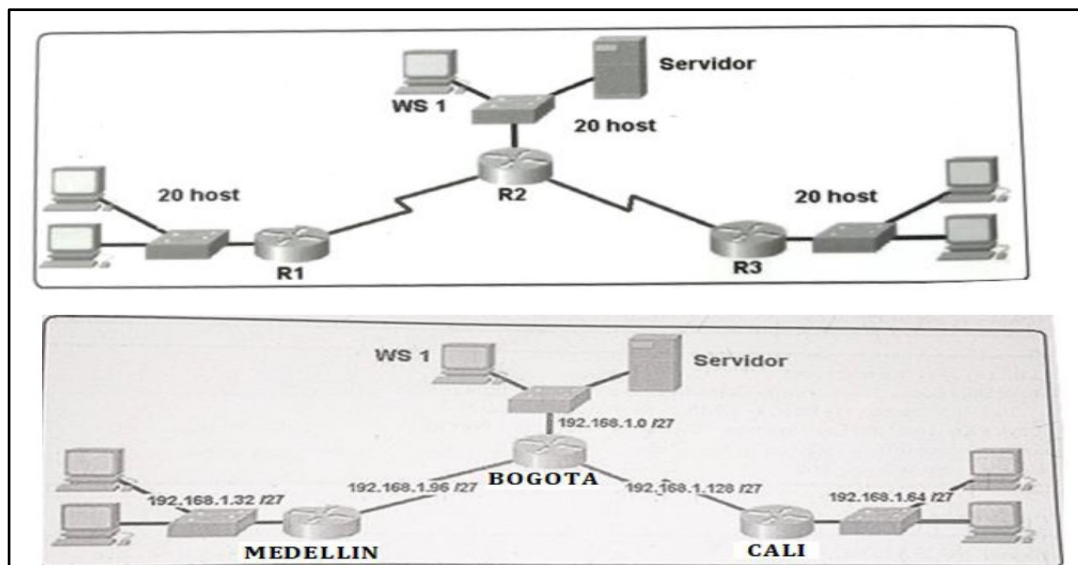
Parte 3: La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.

Parte 4: Implementar la seguridad en la red, se debe restringir el acceso y comunicación entre hosts de acuerdo con los requerimientos del administrador de red.

Parte 5: Comprobación total de los dispositivos y su funcionamiento en la red.

Parte 6: Configuración final.

Figura 1. Escenario 1



A continuación, los códigos para la solución.

Como trabajo inicial se debe realizar lo siguiente.

Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

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

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

#### **Parte 1: Asignación de direcciones IP:**

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

#### **Subneteo de la red 192.168.1.0 /24**

Se comienza con la red 192.168.1.0 la cual se subnetea en 8 partes obteniéndose:



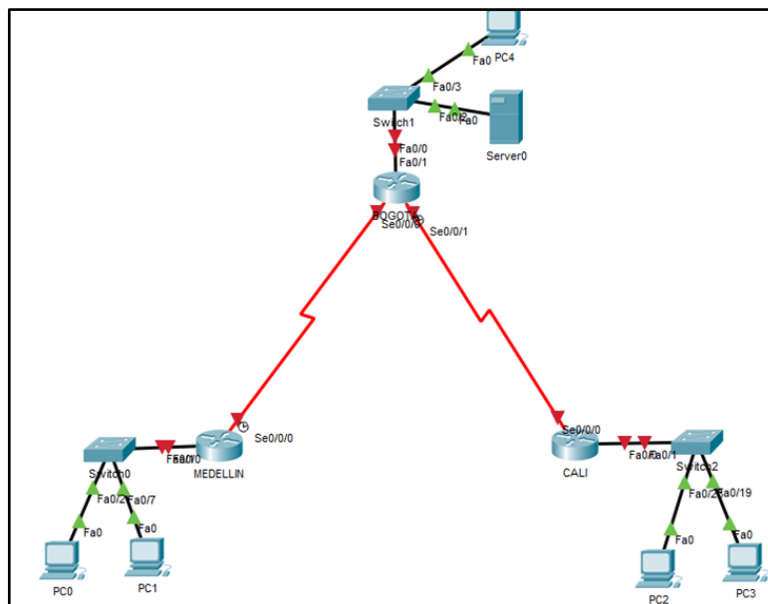
Tabla 1. Subnetea en 8 partes

Subred	Número de hosts	Tamaño de asignación	Dirección de red	Prefijo	Máscara de red	Rango de direcciones disponibles	Broadcast
1	20	30	192.168.1.0	/27	255.255.255.224	192.168.1.1 - 192.168.1.30	192.168.1.31
2	20	30	192.168.1.32	/27	255.255.255.224	192.168.1.33 - 192.168.1.62	192.168.1.63
3	20	30	192.168.1.64	/27	255.255.255.224	192.168.1.65 - 192.168.1.94	192.168.1.95
4	20	30	192.168.1.96	/27	255.255.255.224	192.168.1.97 - 192.168.1.126	192.168.1.127
5	20	30	192.168.1.128	/27	255.255.255.224	192.168.1.129 - 192.168.1.158	192.168.1.159
6	20	30	192.168.1.160	/27	255.255.255.224	192.168.1.161 - 192.168.1.190	192.168.1.191
7	20	30	192.168.1.192	/27	255.255.255.224	192.168.1.193 - 192.168.1.222	192.168.1.223
8	20	30	192.168.1.224	/27	255.255.255.224	192.168.1.225 - 192.168.1.254	192.168.1.255

Se utilizan las primeras 5 subredes para la asignación en los dispositivos.

Se utilizan router 2811 para la simulación en packetr tracer

Figura 2. Simulación del escenario 1



```
Router(config)#hostname bogota
bogota(config)#no ip domain-lookup
bogota(config)#service password-encryption
bogota(config)#banner motd $El Acceso no autorizado est prohibido$
bogota(config)#enable secret class1
bogota(config)#line console 0
bogota(config-line)#password cisco1
bogota(config-line)#login
bogota(config-line)#line vty 0 15
bogota(config-line)#password cisco1
bogota(config-line)#login
```

```
Router(config)#hostname medellin
medellin(config)#no ip domain-lookup
medellin(config)#service password-encryption
medellin(config)#banner motd $El Acceso no autorizado est prohibido$
medellin(config)#enable secret class1
medellin(config)#line console 0
medellin(config-line)#password cisco1
medellin(config-line)#login
medellin(config-line)#line vty 0 15
medellin(config-line)#password cisco1
medellin(config-line)#login
```

```
Router(config)#hostname cali
cali(config)#no ip domain-lookup
cali(config)#service password-encryption
cali(config)#banner motd $El Acceso no autorizado est prohibido$
cali(config)#enable secret class1
```

```
cali(config)#line console 0
cali(config-line)#password cisco1
cali(config-line)#login
cali(config-line)#line vty 0 15
cali(config-line)#password cisco1
cali(config-line)#login
```

```
Switch(config)#hostname switchbogota
switchbogota(config)#no ip domain-lookup
switchbogota(config)#service password-encryption
switchbogota(config)#banner motd $El Acceso no autorizado est prohibido$
switchbogota(config)#enable secret class1
switchbogota(config)#line console 0
switchbogota(config-line)#password cisco1
switchbogota(config-line)#login
switchbogota(config-line)#line vty 0 15
switchbogota(config-line)#password cisco1
switchbogota(config-line)#login
```

```
Switch#conf term
switchmedellin(config)#hostname switchmedellin
switchmedellin(config)#no ip domain-lookup
switchmedellin(config)#service password-encryption
switchmedellin(config)#banner motd $El Acceso no autorizado est prohibido$
switchmedellin(config)#enable secret class1
switchmedellin(config)#line console 0
switchmedellin(config-line)#password cisco1
switchmedellin(config-line)#login
switchmedellin(config-line)#line vty 0 15
```

```
switchmedellin(config-line)#password cisco1
switchmedellin(config-line)#login
```

```
Switch(config)#hostname switchcali
switchcali(config)#no ip domain-lookup
switchcali(config)#service password-encryption
switchcali(config)#banner motd $El Acceso no autorizado est prohibido$
switchcali(config)#enable secret class1
switchcali(config)#line console 0
switchcali(config-line)#password cisco1
switchcali(config-line)#login
switchcali(config-line)#line vty 0 15
switchcali(config-line)#password cisco1
switchcali(config-line)#login
switchcali(config-line)#
```

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

Tabla 2. Direcciones IP

<b>sucursar</b>	<b>Dirección ip</b>
Bogota-LAN	192.168.1.0/27
Medellín-LAN	192.168.1.32/27
Cali-LAN	192.168.1.64/27
Bogota-Medellín	192.168.1.96/27
Bogota-Cali	192.168.1.128/27

Disponible	192.168.1.160/27
Disponible	192.168.1.192/27
Disponible	192.168.1.224/27

**Parte 2: Configuración Básica.**

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

Tabla 3. Configuración básica de los routers

	Router1	Router2	Router3
Nombre de Host	Medellin	Bogota	Cali
Dirección de Ip en interfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.231
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	Eigrp	Eigrp	Eigrp
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

Se realiza la configuración correspondiente en cada uno de los routers del direccionamiento realizado:

**Router Cali.**

```
cali(config)#int s0/0/0
cali(config-if)#ip address 192.168.1.231 255.255.255.224
cali(config-if)#no shutdown
```

```
cali(config-if)#int f0/0
cali(config-if)#ip address 192.168.1.65 255.255.255.224
cali(config-if)#no shutdown
```

```
cali(config-if)#router eigrp 200
cali(config-router)#no auto-summary
cali(config-router)#network 192.168.1.0
cali(config-router)#end
cali#
```

### **Router Bogotá.**

```
bogota(config)#int s0/0/0
bogota(config-if)#ip address 192.168.1.98 255.255.255.224
bogota(config-if)#no shutdown
bogota(config-if)#int s0/0/1
bogota(config-if)#ip address 192.168.1.130 255.255.255.224
bogota(config-if)#no shutdown
```

```
bogota(config-if)#int f0/0
bogota(config-if)#ip address 192.168.1.1 255.255.255.224
bogota(config-if)#no shutdown
```

```
bogota(config-if)#router eigrp 200
bogota(config-router)#no auto-summary
bogota(config-router)#network 192.168.1.0
bogota(config-router)#end
```

### **Router Medellín.**

```
medellin(config)#int s0/0/0
medellin(config-if)#ip address 192.168.1.99 255.255.255.224
medellin(config-if)#no shutdown

medellin(config-if)#
```

```
medellin(config-if)#int f0/0
medellin(config-if)#ip address 192.168.1.33 255.255.255.224
medellin(config-if)#no shutdown
```

```
medellin(config-if)#
medellin(config-if)#router eigrp 200
medellin(config-router)#no auto-summary
medellin(config-router)#network 192.168.1.0
medellin(config-router)#end
```

### Asignación de direcciones a Dispositivos finales

#### En la red MEDELLÍN encontramos a PC0 y PC1

Figura 3. Red de Medellín PC 0

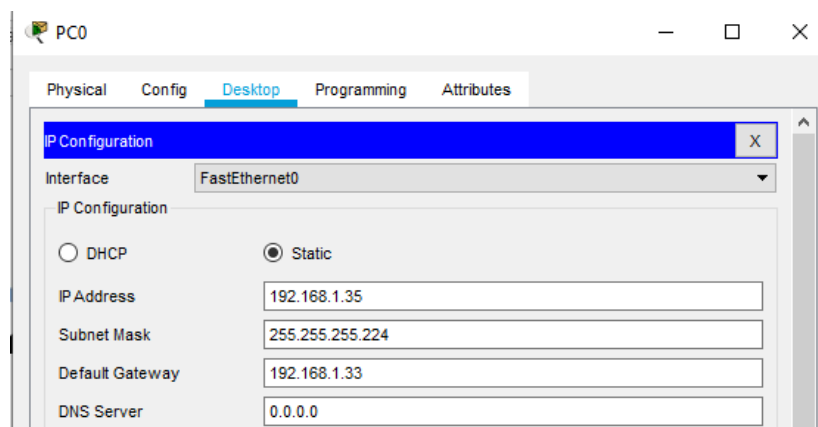
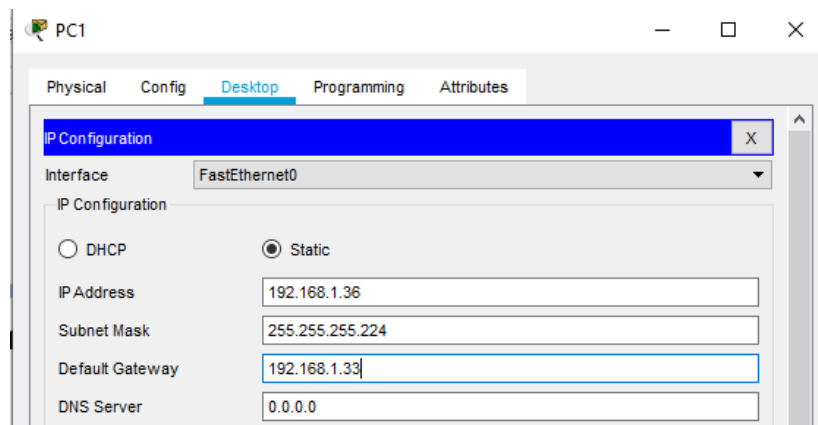


Figura 4. Red de Medellín PC 1



En la red CALI encontramos a PC2 y PC3

Figura 5. Red de Cali PC 2

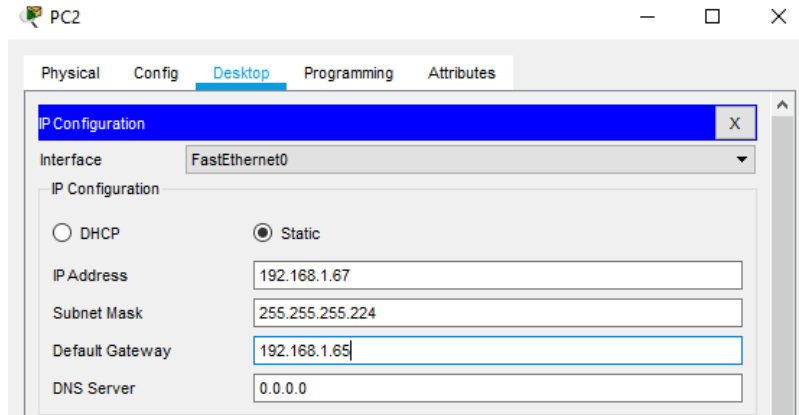
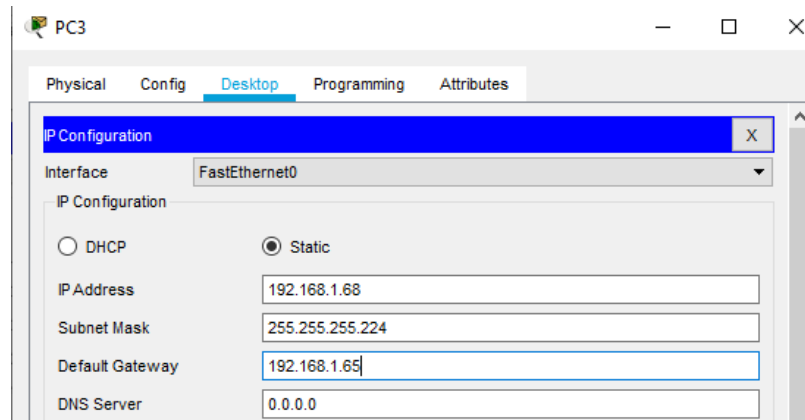


Figura 6. Red de Cali PC 3



En la red BOGOTÁ encontramos a WS1 y Server0

Figura 7. Red de Bogotá WS1

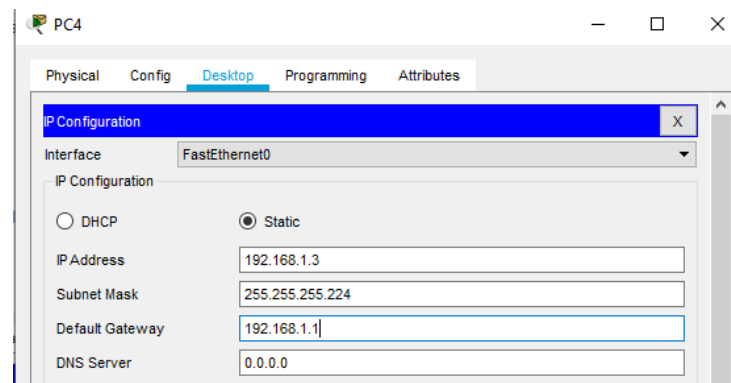
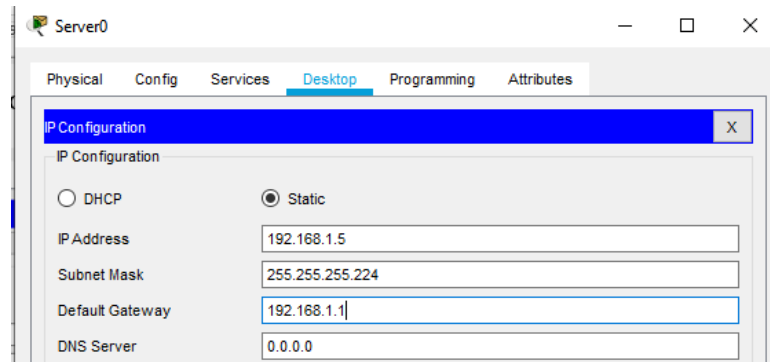




Figura 8. Red de Bogotá Servel 0



**C**

**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.**

Para la verificación de la tabla de enrutamiento se utiliza el comando **show ip route** en cada router

Para 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

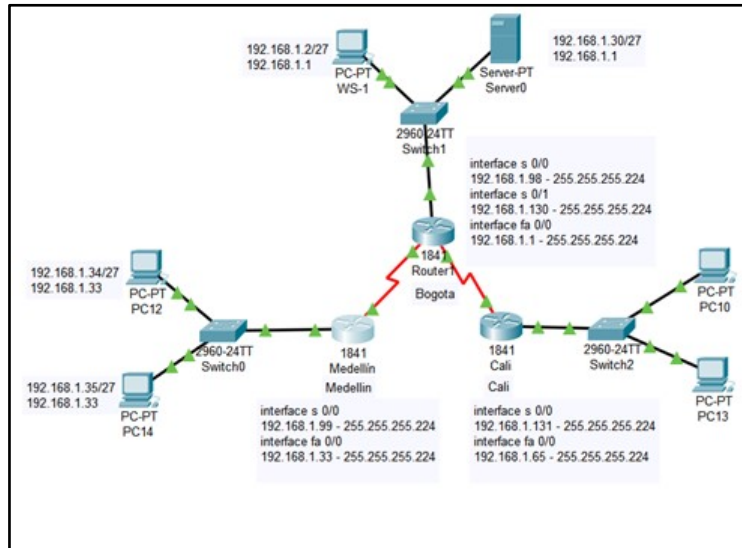
Gateway of last resort is not set

192.168.1.0/27 is subnetted, 5 subnets

D 192.168.1.0 [90/2172416] via 192.168.1.98, 00:04:41, 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, 00:03:38, 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, 00:03:44, Serial0/0/0

Figura 9. Configuración Sucursal Medellín



**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, 00:03:47, Serial0/0/0  
 D 192.168.1.32 [90/2684416] via 192.168.1.130, 00:03:47, 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, 00:03:47, Serial0/0/0

C 192.168.1.128 is directly connected, Serial0/0/0

bogota#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, 00:04:34, Serial0/0/0

D 192.168.1.64 [90/2172416] via 192.168.1.231, 00:03:31, 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

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

medellin#show ip eigrp topology

IP-EIGRP Topology Table for AS 200/ID(192.168.1.99)

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

r - Reply status

P 192.168.1.0/27, 1 successors, FD is 2172416

via 192.168.1.98 (2172416/28160), Serial0/0/0

P 192.168.1.32/27, 1 successors, FD is 28160

via Connected, FastEthernet0/0  
P 192.168.1.64/27, 1 successors, FD is 2684416  
via 192.168.1.98 (2684416/2172416), Serial0/0/0  
P 192.168.1.96/27, 1 successors, FD is 2169856  
via Connected, Serial0/0/0  
P 192.168.1.128/27, 1 successors, FD is 2681856  
via 192.168.1.98 (2681856/2169856), Serial0/0/0

cali#show ip eigrp topology

IP-EIGRP Topology Table for AS 200/ID(192.168.1.231)

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

P 192.168.1.0/27, 1 successors, FD is 2172416  
via 192.168.1.130 (2172416/28160), Serial0/0/0  
P 192.168.1.32/27, 1 successors, FD is 2684416  
via 192.168.1.130 (2684416/2172416), Serial0/0/0  
P 192.168.1.64/27, 1 successors, FD is 28160  
via Connected, FastEthernet0/0  
P 192.168.1.96/27, 1 successors, FD is 2681856  
via 192.168.1.130 (2681856/2169856), Serial0/0/0  
P 192.168.1.128/27, 1 successors, FD is 2169856  
via Connected, Serial0/0/0

**bogota#show ip eigrp topology**

IP-EIGRP Topology Table for AS 200/ID(192.168.1.130)

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

P 192.168.1.0/27, 1 successors, FD is 28160  
 via Connected, FastEthernet0/0  
 P 192.168.1.32/27, 1 successors, FD is 2172416  
 via 192.168.1.99 (2172416/28160), Serial0/0/0  
 P 192.168.1.64/27, 1 successors, FD is 2172416  
 via 192.168.1.231 (2172416/28160), Serial0/0/1  
 P 192.168.1.96/27, 1 successors, FD is 2169856  
 via Connected, Serial0/0/0  
 P 192.168.1.128/27, 1 successors, FD is 2169856  
 via Connected, Serial0/0/1

**d. Realizar un diagnóstico de vecinos cuando el comando cdp.**

```
bogota#show cdp neighbor
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Infrfce Holdtme Capability Platform Port ID
switchbogota
Fas 0/0 176 S 2960 Fas 0/1
medellin Ser 0/0/0 145 R C1841 Ser 0/0/0
cali Ser 0/0/1 148 R C1841 Ser 0/0/0
```

Figura 10. Diagnostico sucursal Bogotá

Device ID	Local Infrfce	Holdtme	Capability	Platform	Port ID
switchbogota	Fas 0/0	135	S	2960	Fas 0/1
cali	Ser 0/0/1	143	R	C1841	Ser 0/0/0
MEDELLIN	Ser 0/0/0	144	R	C1841	Ser 0/0/0

```

medellin#show cdp neighbor
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
switchmedellin
Fas 0/0 231 S 2960 Fas 0/1
bogota Ser 0/0/0 136 R C1841 Ser 0/0/0

```

Figura 11. Diagnostico sucursal Medellin

```

MEDELLIN#
MEDELLIN#show cdp neighbor
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
switchmedellin
                Fas 0/0        147      S           2960      Fas 0/1
bogota         Ser 0/0/0        148      R           C1841     Ser 0/0/0
MEDELLIN#

```

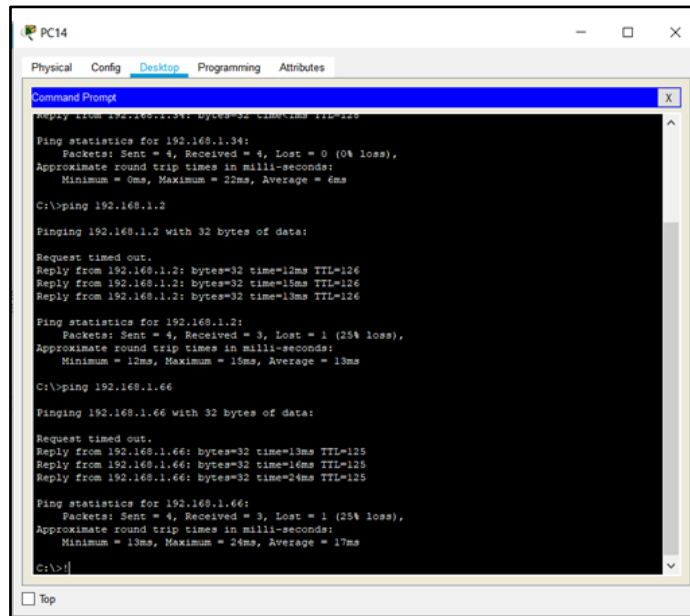
```

cali#show cdp neighbor
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
switchcali Fas 0/0 126 S 2960 Fas 0/1
bogota Ser 0/0/0 126 R C1841 Ser 0/0/1

```

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

Figura 12. Conectividad de la ruta -Ping



```
PC14
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 192.168.1.34: bytes=32 time=6ms TTL=126
Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 22ms, Average = 6ms

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=12ms TTL=126
Reply from 192.168.1.2: bytes=32 time=15ms TTL=126
Reply from 192.168.1.2: bytes=32 time=13ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 15ms, Average = 13ms

C:\>ping 192.168.1.66

Pinging 192.168.1.66 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.66: bytes=32 time=13ms TTL=125
Reply from 192.168.1.66: bytes=32 time=16ms TTL=125
Reply from 192.168.1.66: bytes=32 time=24ms TTL=125

Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 24ms, Average = 17ms

C:\>
```

### Parte 3: Configuración de Enrutamiento.

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

Este paso ya estaba hecho antes, se realizó junto con la configuración de las interface de los routers, de todas maneras lo indico nuevamente:

```
medellin(config-if)#
medellin(config-if)#router eigrp 200
medellin(config-router)#no auto-summary
medellin(config-router)#network 192.168.1.0
medellin(config-router)#end
medellin#
```

```
cali(config-if)#router eigrp 200
cali(config-router)#no auto-summary
cali(config-router)#network 192.168.1.0
cali(config-router)#end
cali#
```

```
bogota(config-if)#
bogota(config-if)#router eigrp 200
bogota(config-router)#no auto-summary
bogota(config-router)#network 192.168.1.0
bogota(config-router)#end
bogota#
```

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

```
bogota#show ip eigrp neighbor
IP-EIGRP neighbors for process 200
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.1.99 Se0/0/0 13 00:04:34 40 1000 0 7
1 192.168.1.231 Se0/0/1 12 00:03:31 40 1000 0 7
```



Figura 13. Routers - Bogotá

```
bogota#show ip eigrp neighbor
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 13 00:16:13 40 1000 0 7
1 192.168.1.99 Se0/0/0 13 00:16:11 40 1000 0 7
bogota#
```

```
medellin#show ip eigrp neighbor
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 11 00:04:40 40 1000 0 7
```

```
cali#show ip eigrp neighbor
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 12 00:03:47 40 1000 0 8
```

```
bogota#show ip eigrp topology
IP-EIGRP Topology Table for AS 200/ID(192.168.1.130)
```

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

```
P 192.168.1.0/27, 1 successors, FD is 28160
via Connected, FastEthernet0/0
P 192.168.1.32/27, 1 successors, FD is 2172416
via 192.168.1.99 (2172416/28160), Serial0/0/0
P 192.168.1.64/27, 1 successors, FD is 2172416
via 192.168.1.231 (2172416/28160), Serial0/0/1
```

P 192.168.1.96/27, 1 successors, FD is 2169856  
via Connected, Serial0/0/0  
P 192.168.1.128/27, 1 successors, FD is 2169856  
via Connected, Serial0/0/1

**medellin#show ip eigrp topology**

IP-EIGRP Topology Table for AS 200/ID(192.168.1.99)

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

P 192.168.1.0/27, 1 successors, FD is 2172416  
via 192.168.1.98 (2172416/28160), Serial0/0/0  
P 192.168.1.32/27, 1 successors, FD is 28160  
via Connected, FastEthernet0/0  
P 192.168.1.64/27, 1 successors, FD is 2684416  
via 192.168.1.98 (2684416/2172416), Serial0/0/0  
P 192.168.1.96/27, 1 successors, FD is 2169856  
via Connected, Serial0/0/0  
P 192.168.1.128/27, 1 successors, FD is 2681856  
via 192.168.1.98 (2681856/2169856), Serial0/0/0

**cali#show ip eigrp topology**

IP-EIGRP Topology Table for AS 200/ID(192.168.1.231)

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

P 192.168.1.0/27, 1 successors, FD is 2172416

via 192.168.1.130 (2172416/28160), Serial0/0/0  
P 192.168.1.32/27, 1 successors, FD is 2684416  
via 192.168.1.130 (2684416/2172416), Serial0/0/0  
P 192.168.1.64/27, 1 successors, FD is 28160  
via Connected, FastEthernet0/0  
P 192.168.1.96/27, 1 successors, FD is 2681856  
via 192.168.1.130 (2681856/2169856), Serial0/0/0  
P 192.168.1.128/27, 1 successors, FD is 2169856  
via Connected, Serial0/0/0

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

## **SHOW IP ROUTE**

bogota#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, 00:04:34, Serial0/0/0  
 D 192.168.1.64 [90/2172416] via 192.168.1.231, 00:03:31, 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

Figura 14. Comprobación tablas de enrutamientos- Bogotá

```
bogota#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, 00:24:50, Serial0/0/0
D       192.168.1.64 [90/2172416] via 192.168.1.131, 00:24:51, 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
bogota#
```

```
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, 00:04:41, 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, 00:03:38, 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, 00:03:44, Serial0/0/0

Figura 15. Comprobación tablas de enrutamientos- Medellín

```
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, 00:23:59, 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, 00:23:59, 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, 00:23:59, Serial0/0/0
MEDELLIN#|
```

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, 00:03:47, Serial0/0/0  
D 192.168.1.32 [90/2684416] via 192.168.1.130, 00:03:47, 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, 00:03:47, Serial0/0/0  
C 192.168.1.128 is directly connected, Serial0/0/0

Figura 16. Comprobación tablas de enrutamientos- 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 are
       * - 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, 00:25:48, Serial0/0/0
D       192.168.1.32 [90/2684416] via 192.168.1.130, 00:25:47, 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, 00:25:48, Serial0/0/0
C       192.168.1.128 is directly connected, Serial0/0/0

cali#
```

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

Figura 17. Diagnóstico para comprobar que cada uno de los puntos de la red-Medellín

```
MEDELLIN#!
MEDELLIN#
MEDELLIN#ping 192.168.1.34

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.34, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/1/4 ms

MEDELLIN#ping 192.168.1.35

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.35, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/12 ms

MEDELLIN#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/14 ms

MEDELLIN#ping 192.168.1.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.30, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/7/15 ms

MEDELLIN#ping 192.168.1.66

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.66, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/11/20 ms

MEDELLIN#ping 192.168.1.67

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.67, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 13/13/14 ms

MEDELLIN#!
```

Verificamos que hay respuesta de las configuraciones

#### 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.

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 131 permit ip host 192.168.1.30 any
```

```
bogota(config)#int f0/0
```

```
bogota(config-if)#ip access-group 131 in
```

```
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.**

```
medellin(config)#access-list 131 permit ip 192.168.1.32 0.0.0.31 host 192.168.1.30
```

```
medellin(config)#int f0/0
```

```
medellin(config-if)#ip access-group 131 in
```

```
medellin(config-if)#
```

```
cali(config)#access-list 131 permit ip 192.168.1.64 0.0.0.31 host 192.168.1.30
```

```
cali(config)#int f0/0
```

```
cali(config-if)#ip access-group 131 in
```

```
cali(config-if)#
```



Figura 18. Verificación LAN

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.34

Pinging 192.168.1.34 with 32 bytes of data:

Reply from 192.168.1.34: bytes=32 time=lms TTL=128
Reply from 192.168.1.34: bytes=32 time<lms TTL=128
Reply from 192.168.1.34: bytes=32 time<lms TTL=128
Reply from 192.168.1.34: bytes=32 time<lms TTL=128

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

C:\>ping 192.168.1.66

Pinging 192.168.1.66 with 32 bytes of data:

Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.30

Pinging 192.168.1.30 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.30: bytes=32 time=15ms TTL=126
Reply from 192.168.1.30: bytes=32 time=lms TTL=126
Reply from 192.168.1.30: bytes=32 time=22ms TTL=126

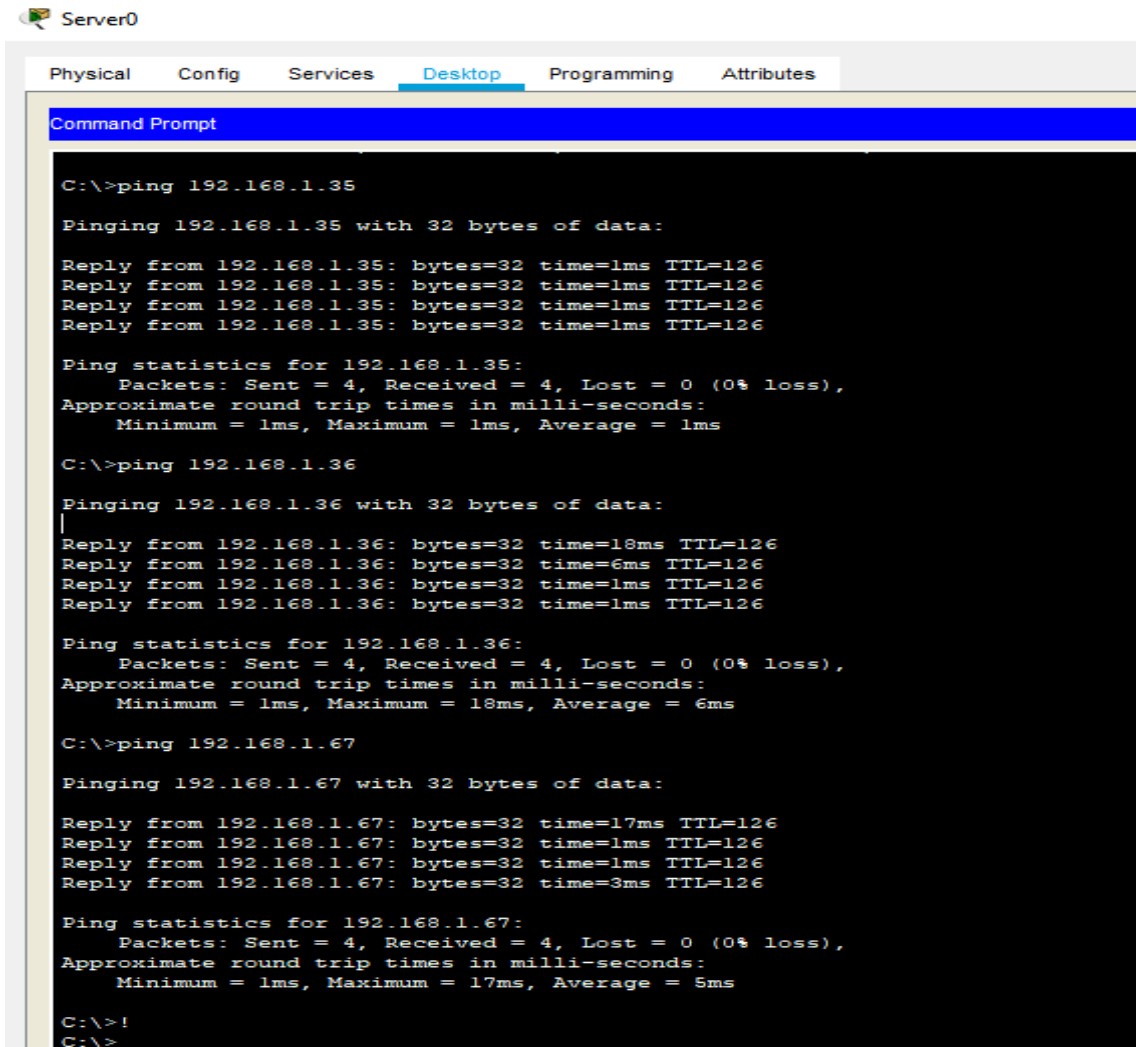
Ping statistics for 192.168.1.30:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = lms, Maximum = 22ms, Average = 12ms

C:\>|
```

### Parte 5: Comprobación de la red instalada.

- a. Se debe probar que la configuración de las listas de acceso fue exitosa.

Figura 19. Lista de acceso exitosa



The screenshot shows a Windows Server 2008 desktop environment. The taskbar includes icons for 'Server0' and several application windows: 'Physical', 'Config', 'Services', 'Desktop' (active), 'Programming', and 'Attributes'. The 'Desktop' window displays a 'Command Prompt' with the following text:

```
C:\>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168.1.35: bytes=32 time=1ms TTL=126
Reply from 192.168.1.35: bytes=32 time=1ms TTL=126
Reply from 192.168.1.35: bytes=32 time=1ms TTL=126
Reply from 192.168.1.35: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 192.168.1.36

Pinging 192.168.1.36 with 32 bytes of data:

Reply from 192.168.1.36: bytes=32 time=18ms TTL=126
Reply from 192.168.1.36: bytes=32 time=6ms TTL=126
Reply from 192.168.1.36: bytes=32 time=1ms TTL=126
Reply from 192.168.1.36: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 18ms, Average = 6ms

C:\>ping 192.168.1.67

Pinging 192.168.1.67 with 32 bytes of data:

Reply from 192.168.1.67: bytes=32 time=17ms TTL=126
Reply from 192.168.1.67: bytes=32 time=1ms TTL=126
Reply from 192.168.1.67: bytes=32 time=1ms TTL=126
Reply from 192.168.1.67: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.1.67:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 17ms, Average = 5ms

C:\>!
C:\>
```

Figura 20. Ping desde WS1 hacia PC0 y PC1

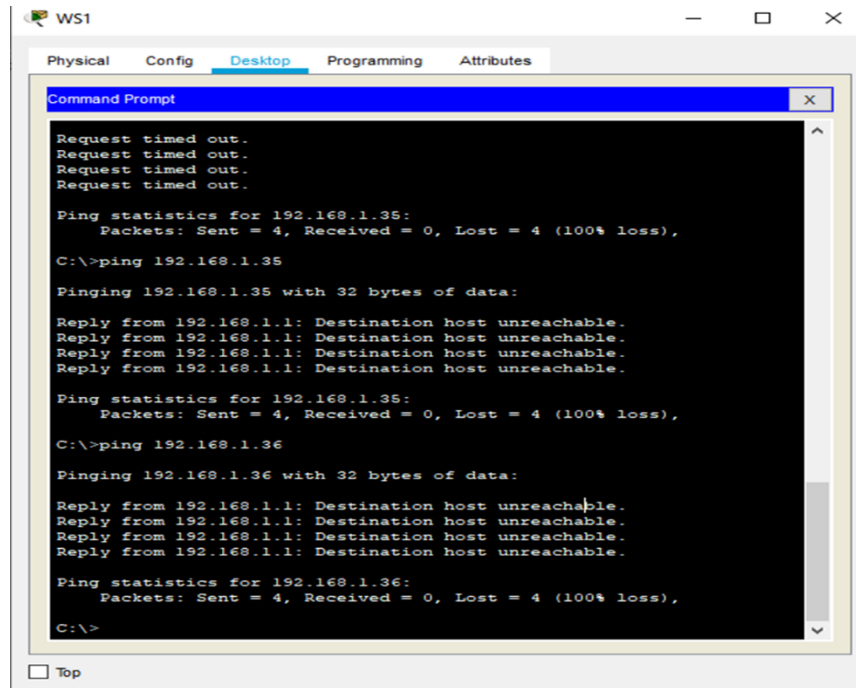


Figura 21. Ping desde Medellín hacia Server0 y Cali

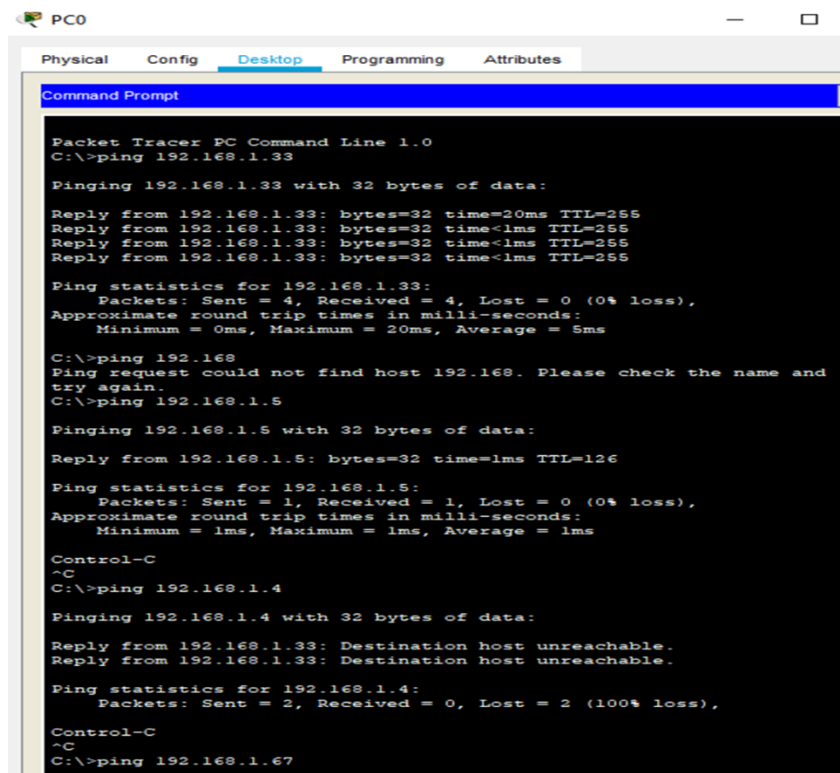


Figura 22. Ping desde Cali hacia Server0 y Medellín

```

PC2
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 192.168.1.5 with 32 bytes of data:
Reply from 192.168.1.5: bytes=32 time=11ms TTL=126
Reply from 192.168.1.5: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.5:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 11ms, Average = 6ms

Control-C
^C
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.

Ping statistics for 192.168.1.4:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

Control-C
^C
C:\>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168.1.65: Destination host unreachable.

Ping statistics for 192.168.1.35:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Control-C
^C
C:\>ping 192.168.1.36

Pinging 192.168.1.36 with 32 bytes of data:

Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.
Reply from 192.168.1.65: Destination host unreachable.

Ping statistics for 192.168.1.36:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),

Control-C
^C
C:\>|
    
```

b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.

Tabla 4. Tabla de condiciones de prueba

	ORIGEN	DESTINO	RESULTADO
<b>TELNET</b>	Router MEDELLÍN	Router CALI	Éxito
	WS 1	Router BOGOTÁ	Falla
	Servidor	Router CALI	Éxito
	Servidor	Router MEDELLÍN	Éxito
<b>TELNET</b>	LAN del Router MEDELLIN	Router CALI	Falla
	LAN del Router CALI	Router CALI	Falla
	LAN del Router MEDELLIN	Router MEDELLÍN	Falla
	LAN del Router CALI	Router MEDELLÍN	Falla
<b>PING</b>	LAN del Router CALI	WS 1	Falla
	LAN del Router	WS 1	Falla

	MEDELLIN		
	LAN del Router MEDELLIN	LAN del Router CALI	Falla
<b>PING</b>	LAN del Router CALI	Servidor	Éxito
	LAN del Router MEDELLIN	Servidor	Éxito
	Servidor	LAN del Router MEDELLÍN	Éxito
	Servidor	LAN del Router CALI	Éxito
	Router CALI	LAN del Router MEDELLÍN	Falla
	Router MEDELLÍN	LAN del Router CALI	Falla

	<b>Router MEDELLIN</b>	<b>Router CALI</b>	Medellin#telnet 192.168.1.131 Trying 192.168.1.131 ... % Connection timed out; remote host not responding Medellin#!
	<b>WS_1</b>	<b>Router BOGOTA</b>	C:\>telnet 192.1683.1.1 telnet request could not find host 192.1683.1.1. Please check the name and try again.
	<b>Servidor</b>	<b>Router CALI</b>	Trying 192.168.1.131 ...Open User Access Verification
	<b>Servidor</b>	<b>Router MEDELLI N</b>	Trying 192.168.1.99 ...Open User Access Verification
	<b>LAN del</b>	<b>Router</b>	Trying 192.168.1.131 ... %

	<b>Router MEDELLIN</b>	<b>CALI</b>	Connection timed out; remote host not responding
	<b>LAN del Router CALI</b>	<b>Router CALI</b>	Trying 192.168.1.65 ...Open
	<b>LAN del Router MEDELLIN</b>	<b>Router MEDELLIN</b>	Trying 192.168.1.33 ...Open
	<b>LAN del Router CALI</b>	<b>Router MEDELLIN</b>	Trying 192.168.1.99 ... % Connection timed out; remote host not responding
	<b>LAN del Router CALI</b>	<b>WS_1</b>	<p>C:\&gt;ping 192.168.1.4</p> <p>Pinging 192.168.1.4 with 32 bytes of data:</p> <p>Reply from 192.168.1.65: Destination host unreachable.</p> <p>Reply from 192.168.1.65: Destination host unreachable.</p> <p>Reply from 192.168.1.65: Destination host unreachable.</p> <p>Reply from 192.168.1.65: Destination host unreachable.</p> <p>Ping statistics for 192.168.1.4: Packets: Sent = 4, Received</p>

			= 0, Lost = 4 (100% loss),
	<b>LAN del Router MEDELLIN</b>	<b>WS_1</b>	<p>C:\&gt;ping 192.168.1.4</p> <p>Pinging 192.168.1.4 with 32 bytes of data:</p> <p>Reply from 192.168.1.33: Destination host unreachable.</p> <p>Reply from 192.168.1.33: Destination host unreachable.</p> <p>Reply from 192.168.1.33: Destination host unreachable.</p> <p>Reply from 192.168.1.33: Destination host unreachable.</p> <p>Ping statistics for 192.168.1.4: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),</p>
	<b>LAN del Router MEDELLIN</b>	<b>LAN del Router CALI</b>	<p>C:\&gt;ping 192.168.1.67</p> <p>Pinging 192.168.1.67 with 32 bytes of data:</p> <p>Reply from 192.168.1.33: Destination host unreachable.</p> <p>Reply from 192.168.1.33: Destination host unreachable.</p>

			<p>Reply from 192.168.1.33: Destination host unreachable.</p> <p>Reply from 192.168.1.33: Destination host unreachable.</p> <p>Ping statistics for 192.168.1.67:</p> <p>Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),</p>
	<b>LAN del Router CALI</b>	<b>Servidor</b>	<p>C:\&gt;ping 192.168.1.5</p> <p>Pinging 192.168.1.5 with 32 bytes of data:</p> <p>Reply from 192.168.1.5: bytes=32 time=1ms TTL=126</p> <p>Reply from 192.168.1.5: bytes=32 time=11ms TTL=126</p> <p>Reply from 192.168.1.5: bytes=32 time=1ms TTL=126</p> <p>Reply from 192.168.1.5: bytes=32 time=8ms TTL=126</p> <p>Ping statistics for 192.168.1.5: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 11ms, Average = 5ms</p>
	<b>LAN del Router</b>	<b>Servidor</b>	C:\>ping 192.168.1.5



	<b>MEDELLIN</b>		<p>Pinging 192.168.1.5 with 32 bytes of data:</p> <p>Reply from 192.168.1.5: bytes=32 time=1ms TTL=126</p> <p>Reply from 192.168.1.5: bytes=32 time=11ms TTL=126</p> <p>Reply from 192.168.1.5: bytes=32 time=1ms TTL=126</p> <p>Reply from 192.168.1.5: bytes=32 time=8ms TTL=126</p> <p>Ping statistics for 192.168.1.5: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 11ms, Average = 5ms</p>
	<b>Servidor</b>	<b>LAN del Router MEDELLIN</b>	<p>C:\&gt;ping 192.168.1.35</p> <p>Pinging 192.168.1.35 with 32 bytes of data:</p> <p>Reply from 192.168.1.35: bytes=32 time=2ms TTL=126</p> <p>Reply from 192.168.1.35: bytes=32 time=2ms TTL=126</p> <p>Reply from 192.168.1.35: bytes=32 time=8ms TTL=126</p> <p>Reply from 192.168.1.35:</p>

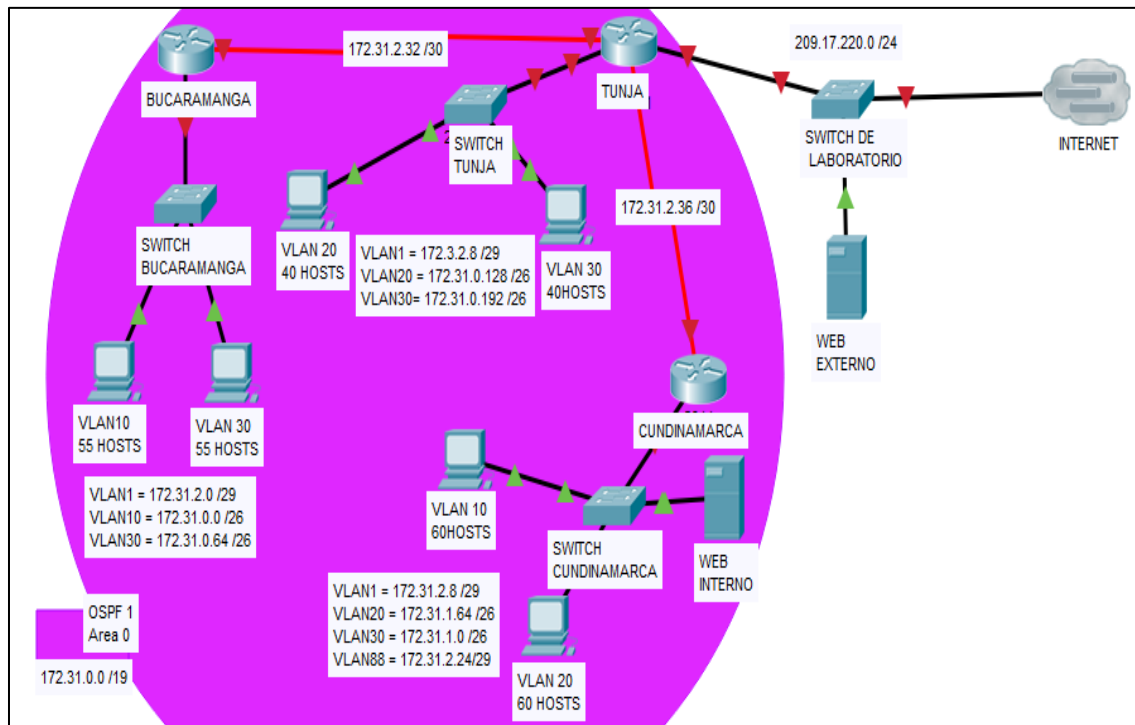
			<p>bytes=32 time=6ms TTL=126</p> <p>Ping statistics for 192.168.1.35:</p> <p>Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),</p> <p>Approximate round trip times in milli-seconds:</p> <p>Minimum = 2ms, Maximum = 8ms, Average = 4ms</p>
	<b>Servidor</b>	<b>LAN del Router CALI</b>	<p>C:\&gt;ping 192.168.1.67</p> <p>Pinging 192.168.1.67 with 32 bytes of data:</p> <p>Reply from 192.168.1.67: bytes=32 time=2ms TTL=126</p> <p>Reply from 192.168.1.67: bytes=32 time=2ms TTL=126</p> <p>Reply from 192.168.1.67: bytes=32 time=9ms TTL=126</p> <p>Reply from 192.168.1.67: bytes=32 time=1ms TTL=126</p> <p>Ping statistics for 192.168.1.67:</p> <p>Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),</p> <p>Approximate round trip times in milli-seconds:</p> <p>Minimum = 1ms, Maximum = 9ms, Average = 3ms</p>

	<p><b>Router CALI</b></p>	<p><b>LAN del Router MEDELLI N</b></p>	<pre> 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:  UUUUU  Success rate is 0 percent (0/5)  Cali# </pre>
--	---------------------------	--	---

## 2. ESCENARIO 2

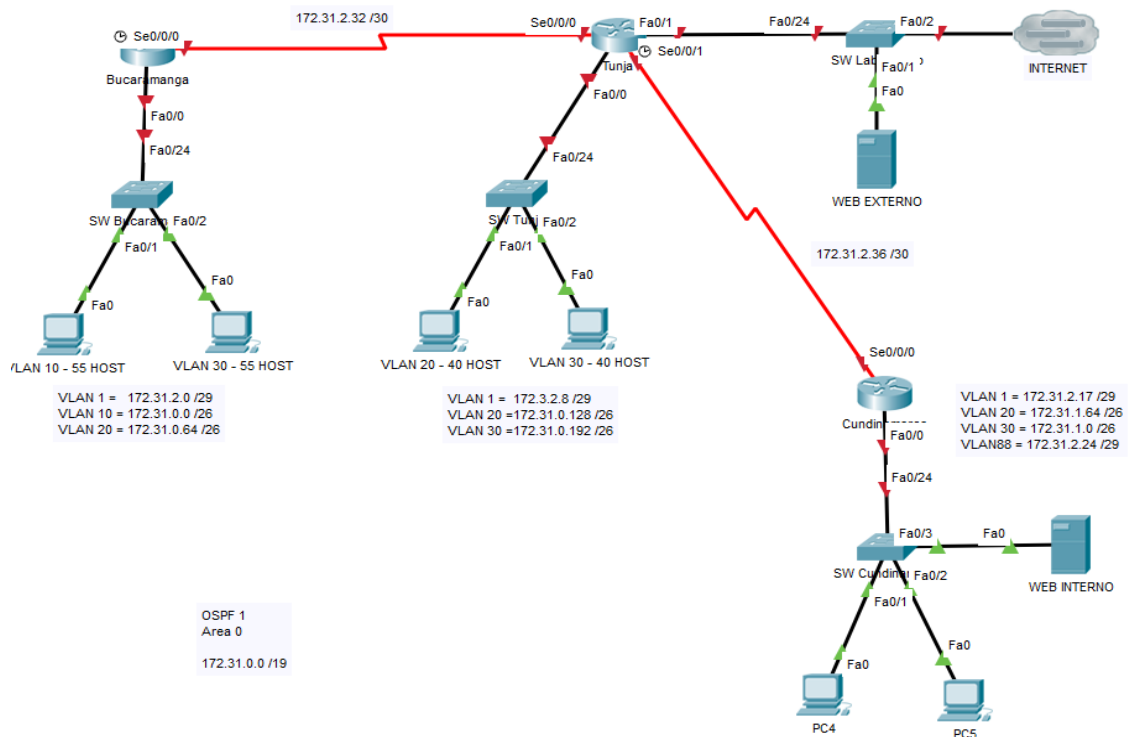
Una empresa tiene la conexión a internet en una red Ethernet, lo cual deben adaptarlo para facilitar que sus routers y las redes que incluyen puedan, por esa vía, conectarse a internet, pero empleando las direcciones de la red LAN original.

Figura 23. Escenario 2



Los siguientes son los requerimientos necesarios:

Figura 24. topología del escenario 2



OSPF 1  
Area 0  
172.31.0.0/19

**Todos los routers deberán tener los siguiente:**

Configuración básica.

Realizamos en este paso la configuración básica de cada uno de los routers, no olvidemos que debemos activar cada una de las interfaces de manera manual, de una vez realizamos la configuración del protocolo de enrutamiento

```
Router(config)#hostname bucaramanga
bucaramanga(config)#no ip domain-lookup
bucaramanga(config)#banner motd $El Acceso no autorizado est prohibido$
bucaramanga(config)#enable secret class1
bucaramanga(config)#line console 0
bucaramanga(config-line)#password cisco1
bucaramanga(config-line)#login
bucaramanga(config-line)#line vty 0 15
bucaramanga(config-line)#password cisco1
bucaramanga(config-line)#login
```

```
bucaramanga(config)#int f0/0.1
bucaramanga(config-subif)#encapsulation dot1q 1
bucaramanga(config-subif)#ip address 172.31.2.1 255.255.255.248
bucaramanga(config-subif)#int f0/0.10
bucaramanga(config-subif)#encapsulation dot1q 10
bucaramanga(config-subif)#ip address 172.31.0.1 255.255.255.192
bucaramanga(config-subif)#int f0/0.30
bucaramanga(config-subif)#encapsulation dot1q 30
bucaramanga(config-subif)#ip address 172.31.0.65 255.255.255.192
bucaramanga(config-subif)#int f0/0
bucaramanga(config-if)#no shutdown
bucaramanga(config-if)#int s0/0/0
bucaramanga(config-if)#ip address 172.31.2.34 255.255.255.252
bucaramanga(config-if)#no shutdown
bucaramanga(config-if)#
bucaramanga(config-if)#router ospf 1
bucaramanga(config-router)#network 172.31.0.0 0.0.0.63 area 0
bucaramanga(config-router)#network 172.31.0.64 0.0.0.63 area 0
bucaramanga(config-router)#network 172.31.2.0 0.0.0.7 area 0
bucaramanga(config-router)#network 172.31.2.32 0.0.0.3 area 0
bucaramanga(config-router)#end
bucaramanga#
bucaramanga#
```

```
Router(config)#hostname tunja
tunja(config)#no ip domain-lookup
tunja(config)#banner motd $EI Acceso no autorizado est prohibido$
```

```
tunja(config)#enable secret class1
tunja(config)#line console 0
tunja(config-line)#password cisco1
tunja(config-line)#login
tunja(config-line)#line vty 0 15
tunja(config-line)#password cisco1
tunja(config-line)#login
tunja(config)#int f0/0.1
tunja(config-subif)#encapsulation dot1q 1
tunja(config-subif)#ip address 172.3.2.9 255.255.255.248
tunja(config-subif)#int f0/0.20
tunja(config-subif)#encapsulation dot1q 20
tunja(config-subif)#ip address 172.31.0.129 255.255.255.192
tunja(config-subif)#int f0/0.30
tunja(config-subif)#encapsulation dot1q 30
tunja(config-subif)#ip address 172.31.0.193 255.255.255.192
tunja(config-subif)#int f0/0
tunja(config-if)#no shutdown
tunja(config-if)#int s0/0/0
tunja(config-if)#ip address 172.31.2.33 255.255.255.252
tunja(config-if)#no shutdown
tunja(config-if)#int s0/0/1
tunja(config-if)#ip address 172.31.2.37 255.255.255.252
tunja(config-if)#no shutdown
tunja(config-if)#int f0/1
tunja(config-if)#ip address 209.165.220.1 255.255.255.0
tunja(config-if)#no shutdown
tunja(config-if)#router ospf 1
tunja(config-router)#network 172.3.2.8 0.0.0.7 area 0
```

```
tunja(config-router)#network 172.31.0.128 0.0.0.63 area 0
tunja(config-router)#network 172.31.0.192 0.0.0.63 area 0
tunja(config-router)#network 172.31.2.32 0.0.0.3 area 0
tunja(config-router)#network 172.31.2.36 0.0.0.3 area 0
tunja(config-router)#end
tunja#
```

```
Router(config)#hostname cundinamarca
cundinamarca(config)#no ip domain-lookup
cundinamarca(config)#banner motd $El Acceso no autorizado est prohibido$
cundinamarca(config)#enable secret class1
cundinamarca(config)#line console 0
cundinamarca(config-line)#password cisco1
cundinamarca(config-line)#login
cundinamarca(config-line)#line vty 0 15
cundinamarca(config-line)#password cisco1
cundinamarca(config-line)#login
cundinamarca(config)#int f0/0.1
cundinamarca(config-subif)#encapsulation dot1q 1
cundinamarca(config-subif)#ip address 172.31.2.9 255.255.255.248
cundinamarca(config-subif)#int f0/0.20
cundinamarca(config-subif)#encapsulation dot1q 20
cundinamarca(config-subif)#ip address 172.31.1.65 255.255.255.192
cundinamarca(config-subif)#int f0/0.30
cundinamarca(config-subif)#encapsulation dot1q 30
cundinamarca(config-subif)#ip address 172.31.1.1 255.255.255.192
cundinamarca(config-subif)#int f0/0.88
```



```
cundinamarca(config-subif)#encapsulation dot1q 88
cundinamarca(config-subif)#ip address 172.31.2.25 255.255.255.248
cundinamarca(config-subif)#int f0/0
cundinamarca(config-if)#no shutdown
cundinamarca(config-if)#int s0/0/0
cundinamarca(config-if)#ip address 172.31.2.38 255.255.255.252
cundinamarca(config-if)#no shutdown
cundinamarca(config-if)#router ospf 1
cundinamarca(config-router)#network 172.31.1.0 0.0.0.63 area 0
cundinamarca(config-router)#network 172.31.1.64 0.0.0.63 area 0
cundinamarca(config-router)#network 172.31.2.8 0.0.0.7 area 0
cundinamarca(config-router)#network 172.31.2.24 0.0.0.7 area 0
cundinamarca(config-router)#network 172.31.2.36 0.0.0.3 area 0
cundinamarca(config-router)#end
cundinamarca#
```

Se hace la configuración de los SWITCH, también la creación de las VLAN y las respectivas asignaciones de las interfaces a cada una de ellas.

```
Switch(config)#hostname swtichtunja
swtichtunja(config)#vlan 1
swtichtunja(config-vlan)#vlan 20
swtichtunja(config-vlan)#vlan 30
swtichtunja(config-vlan)#int f0/10
swtichtunja(config-if)#switchport mode access
swtichtunja(config-if)#switchport access vlan 20
swtichtunja(config-if)#int f0/14
swtichtunja(config-if)#switchport mode access
swtichtunja(config-if)#switchport access vlan 30
swtichtunja(config-if)#int f0/1
```

```
swichtunja(config-if)#switchport mode trunk
swichtunja(config-if)#int vlan 1
swichtunja(config-if)#ip address 172.3.2.11 255.255.255.248
swichtunja(config-if)#no shutdown
swichtunja(config-if)#ip default-gateway 172.3.2.9
swichtunja(config)#
swichtunja(config)#
```

```
Switch(config)#hostname swithccundinamarca
swithccundinamarca(config)#vlan 1
swithccundinamarca(config-vlan)#vlan 20
swithccundinamarca(config-vlan)#vlan 30
swithccundinamarca(config-vlan)#vlan 88
swithccundinamarca(config-vlan)#exit
swithccundinamarca(config)#int f0/10
swithccundinamarca(config-if)#switchport mode access
swithccundinamarca(config-if)#switchport access vlan 20
swithccundinamarca(config-if)#int f0/14
swithccundinamarca(config-if)#switchport mode access
swithccundinamarca(config-if)#switchport access vlan 30
swithccundinamarca(config-if)#int f0/20
swithccundinamarca(config-if)#switchport mode access
swithccundinamarca(config-if)#switchport access vlan 88
swithccundinamarca(config-if)#int f0/1
swithccundinamarca(config-if)#switchport mode trunk
swithccundinamarca(config-if)#int vlan 1
swithccundinamarca(config-if)#ip address 172.31.2.11 255.255.255.248
swithccundinamarca(config-if)#no shutdown
```

```
switchccundinamarca(config-if)#ip default-gateway 172.31.2.9
Switch(config)#hostname switchbucaramanga
switchbucaramanga(config)#vlan 1
switchbucaramanga(config-vlan)#vlan 10
switchbucaramanga(config-vlan)#vlan 30
switchbucaramanga(config-vlan)#int f0/10
switchbucaramanga(config-if)#switchport mode access
switchbucaramanga(config-if)#switchport access vlan 10
switchbucaramanga(config-if)#int f0/14
switchbucaramanga(config-if)#switchport mode access
switchbucaramanga(config-if)#switchport access vlan 30
switchbucaramanga(config-if)#int f0/1
switchbucaramanga(config-if)#switchport mode trunk
switchbucaramanga(config-if)#int vlan 1
switchbucaramanga(config-if)#ip address 172.31.2.3 255.255.255.248
switchbucaramanga(config-if)#no shutdown
switchbucaramanga(config-if)#ip default-gateway 172.31.2.1
switchbucaramanga(config)#
```

Proceso de autenticación.

### **AAA.**

```
bucaramanga(config-line)#username admin01 secret admin01pass
bucaramanga(config)#aaa new-model
bucaramanga(config)#aaa authentication login aaalocal local
bucaramanga(config)#line console 0
bucaramanga(config-line)#login authentication aaalocal
bucaramanga(config-line)#line vty 0 15
bucaramanga(config-line)#login authentication aaalocal
```

```
tunja(config-line)#username admin01 secret admin01pass
tunja(config)#aaa new-model
tunja(config)#aaa authentication login aaalocal local
tunja(config)#line console 0
tunja(config-line)#login authentication aaalocal
tunja(config-line)#line vty 0 15
tunja(config-line)#login authentication aaalocal
```

```
cundinamarca(config-line)#username admin01 secret admin01pass
cundinamarca(config)#aaa new-model
cundinamarca(config)#aaa authentication login aaalocal local
cundinamarca(config)#line console 0
cundinamarca(config-line)#login authentication aaalocal
cundinamarca(config-line)#line vty 0 15
cundinamarca(config-line)#login authentication aaalocal
```

Cifrado de contraseñas.

**Se realizó con el comando service password-encryption en cada router**

```
bucaramanga(config)#service password-encryption
tunja(config)#service password-encryption
cundinamarca(config)#service password-encryption
```

**Un máximo de internos para acceder al router.**

```
bucaramanga(config-line)#login block-for 20 attempts 10 within 60
tunja(config-line)#login block-for 20 attempts 10 within 60
cundinamarca(config-line)#login block-for 20 attempts 10 within 60
```

### Máximo tiempo de acceso al detectar ataques.

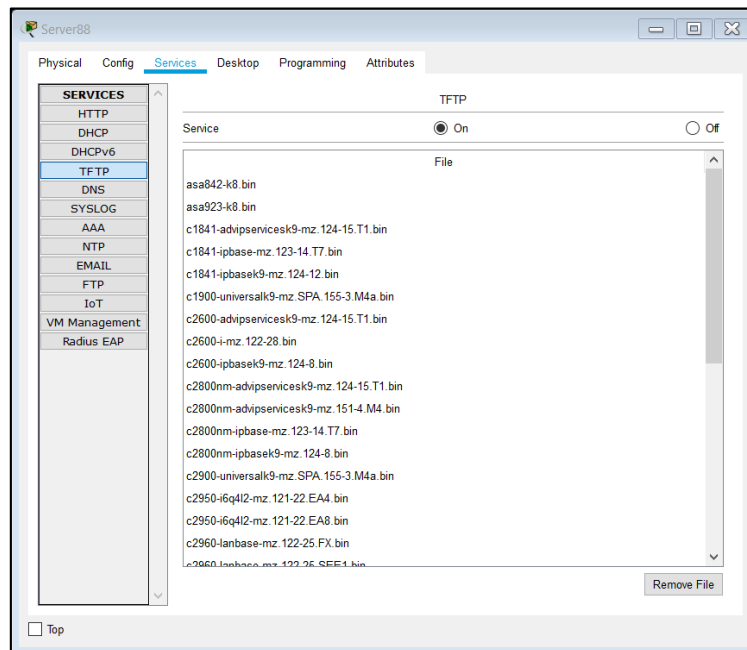
```
bucaramanga(config-line)#login block-for 20 attempts 10 within 60
```

```
tunja(config-line)#login block-for 20 attempts 10 within 60
```

```
cundinamarca(config-line)#login block-for 20 attempts 10 within 60
```

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

Figura 25. Server 88



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

El router encargado de realizar la asignación de direcciones IP es el router de TUNJA, debemos excluir las primeras direcciones IP de cada uno de los rangos IP de las 4 vlan indicadas en BUCARAMANGA y en CUNDINAMARCA y posteriormente debemos crear cada uno de los POOL de direcciones, tal como indico a continuación.

```
tunja(config)#ip dhcp excluded-address 172.31.0.1 172.31.0.3
```

```
tunja(config)#ip dhcp excluded-address 172.31.0.65 172.31.0.67
```

```

tunja(config)#ip dhcp excluded-address 172.31.1.65 172.31.1.67
tunja(config)#ip dhcp excluded-address 172.31.1.1 172.31.1.3
tunja(config)#ip dhcp pool vlan10buc
tunja(dhcp-config)#network 172.31.0.0 255.255.255.192
tunja(dhcp-config)#default-router 172.31.0.1
tunja(dhcp-config)#dns-server 8.8.8.8
tunja(dhcp-config)#ip dhcp pool lan30buc
tunja(dhcp-config)#network 172.31.0.64 255.255.255.192
tunja(dhcp-config)#default-router 172.31.0.65
tunja(dhcp-config)#dns-server 8.8.8.8
tunja(dhcp-config)#ip dhcp pool vlan20cun
tunja(dhcp-config)#network 172.31.1.64 255.255.255.192
tunja(dhcp-config)#default-router 172.31.1.65
tunja(dhcp-config)#dns-server 8.8.8.8
tunja(dhcp-config)#ip dhcp pool vlan30cun
tunja(dhcp-config)#network 172.31.1.0 255.255.255.192
tunja(dhcp-config)#default-router 172.31.1.1
tunja(dhcp-config)#dns-server 8.8.8.8

```

Procedemos a configurar cada uno de los routers con el fin de que estos puedan tener acceso a estos POOL de direcciones.

```

bucaramanga(config)#int f0/0.10
bucaramanga(config-subif)#ip helper-address 172.31.2.33
bucaramanga(config-subif)#int f0/0.30
bucaramanga(config-subif)#ip helper-address 172.31.2.33
bucaramanga(config-subif)#end
bucaramanga#

cundinamarca(config)#int f0/0.20

```

```
cundinamarca(config-subif)#ip helper-address 172.31.2.37
cundinamarca(config-subif)#int f0/0.30
cundinamarca(config-subif)#ip helper-address 172.31.2.37
cundinamarca(config-subif)#end
cundinamarca#
```

Verificar que cada uno de los PC de las VLAN de los routers de Bucarmanga y Cundinamarca obtengan sus direcciones IP empleando DHCP.

Figura 26. PC 10

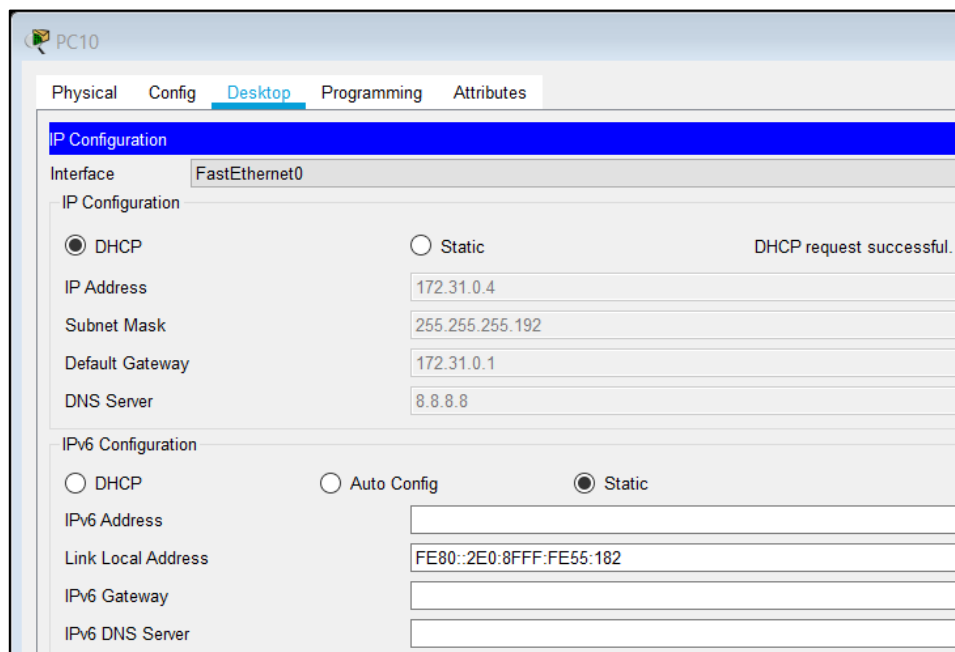


Figura 27. PC 11

The screenshot shows the configuration window for PC11. The 'Desktop' tab is selected. Under 'IP Configuration', the 'DHCP' radio button is selected. The IP Address is 172.31.0.68, Subnet Mask is 255.255.255.192, Default Gateway is 172.31.0.65, and DNS Server is 8.8.8.8. Under 'IPv6 Configuration', the 'Static' radio button is selected. The Link Local Address is FE80::260:2FFF:FE31:C4B6. The interface is FastEthernet0.

Field	Value	
Interface	FastEthernet0	
IP Configuration		
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static	
IP Address	172.31.0.68	
Subnet Mask	255.255.255.192	
Default Gateway	172.31.0.65	
DNS Server	8.8.8.8	
IPv6 Configuration		
<input type="radio"/> DHCP	<input type="radio"/> Auto Config	<input checked="" type="radio"/> Static
IPv6 Address		
Link Local Address	FE80::260:2FFF:FE31:C4B6	
IPv6 Gateway		
IPv6 DNS Server		

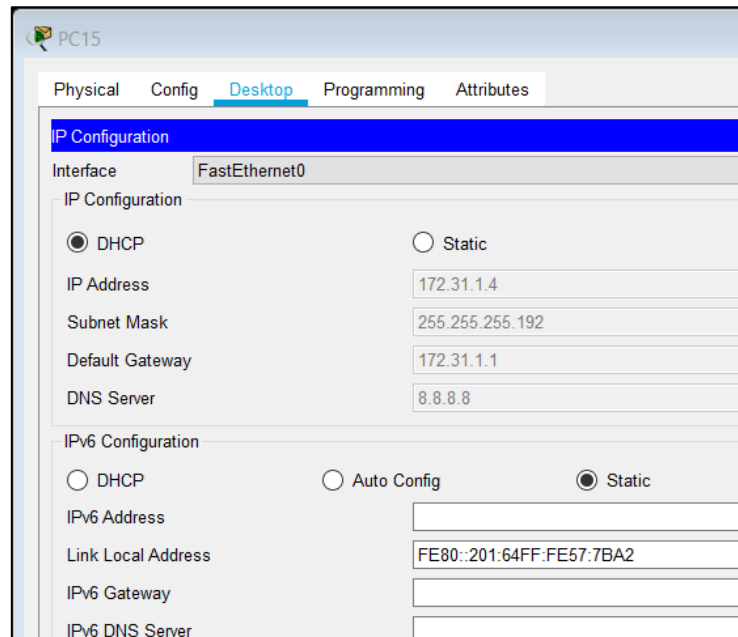
Figura 28. PC 14

The screenshot shows the configuration window for PC14. The 'Desktop' tab is selected. Under 'IP Configuration', the 'DHCP' radio button is selected. The IP Address is 172.31.1.68, Subnet Mask is 255.255.255.192, Default Gateway is 172.31.1.65, and DNS Server is 8.8.8.8. Under 'IPv6 Configuration', the 'Static' radio button is selected. The Link Local Address is FE80::201:42FF:FE16:70E1. The interface is FastEthernet0.

Field	Value	
Interface	FastEthernet0	
IP Configuration		
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static	
IP Address	172.31.1.68	
Subnet Mask	255.255.255.192	
Default Gateway	172.31.1.65	
DNS Server	8.8.8.8	
IPv6 Configuration		
<input type="radio"/> DHCP	<input type="radio"/> Auto Config	<input checked="" type="radio"/> Static
IPv6 Address		
Link Local Address	FE80::201:42FF:FE16:70E1	
IPv6 Gateway		
IPv6 DNS Server		



Figura 29. PC 15



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

Vemos dos tipos de NAT de forma estática para nuestro servidor y con sobrecarga para los demás equipos de nuestra red.

```
tunja(config)#ip nat inside source static 172.31.2.28 209.165.220.10
tunja(config)#access-list 11 permit 172.0.0.0 0.255.255.255
tunja(config)#ip nat inside source list 11 interface f0/1 overload
tunja(config)#int f0/1
tunja(config-if)#ip nat outside
tunja(config-if)#int f0/0.1
tunja(config-subif)#ip nat inside
tunja(config-subif)#int f0/0.20
tunja(config-subif)#ip nat inside
tunja(config-subif)#int f0/0.30
tunja(config-subif)#ip nat inside
```

```
tunja(config-subif)#int s0/0/0
tunja(config-if)#ip nat inside
tunja(config-if)#int s0/0/1
tunja(config-if)#ip nat inside
tunja(config-if)#exit
tunja(config)#ip route 0.0.0.0 0.0.0.0 209.165.220.4
tunja(config)#router ospf 1
tunja(config-router)#default-information originate
tunja(config-router)#end
```

```
tunja#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 209.165.220.4 to network 0.0.0.0**

```
172.3.0.0/29 is subnetted, 1 subnets
C 172.3.2.8 is directly connected, FastEthernet0/0.1
172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks
O 172.31.0.0/26 [110/65] via 172.31.2.34, 00:10:47, Serial0/0/0
O 172.31.0.64/26 [110/65] via 172.31.2.34, 00:10:47, Serial0/0/0
C 172.31.0.128/26 is directly connected, FastEthernet0/0.20
```

```
C 172.31.0.192/26 is directly connected, FastEthernet0/0.30
O 172.31.1.0/26 [110/65] via 172.31.2.38, 00:10:47, Serial0/0/1
O 172.31.1.64/26 [110/65] via 172.31.2.38, 00:10:47, Serial0/0/1
O 172.31.2.0/29 [110/65] via 172.31.2.34, 00:10:47, Serial0/0/0
O 172.31.2.8/29 [110/65] via 172.31.2.38, 00:10:47, Serial0/0/1
O 172.31.2.24/29 [110/65] via 172.31.2.38, 00:10:47, Serial0/0/1
C 172.31.2.32/30 is directly connected, Serial0/0/0
C 172.31.2.36/30 is directly connected, Serial0/0/1
C 209.165.220.0/24 is directly connected, FastEthernet0/1
S* 0.0.0.0/0 [1/0] via 209.165.220.4
```

tunja#

bucaramanga#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 172.31.2.33 to network 0.0.0.0**

```
172.3.0.0/29 is subnetted, 1 subnets
O 172.3.2.8 [110/65] via 172.31.2.33, 00:11:18, Serial0/0/0
172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks
C 172.31.0.0/26 is directly connected, FastEthernet0/0.10
C 172.31.0.64/26 is directly connected, FastEthernet0/0.30
```

O 172.31.0.128/26 [110/65] via 172.31.2.33, 00:11:18, Serial0/0/0  
O 172.31.0.192/26 [110/65] via 172.31.2.33, 00:11:18, Serial0/0/0  
O 172.31.1.0/26 [110/129] via 172.31.2.33, 00:11:18, Serial0/0/0  
O 172.31.1.64/26 [110/129] via 172.31.2.33, 00:11:18, Serial0/0/0  
C 172.31.2.0/29 is directly connected, FastEthernet0/0.1  
O 172.31.2.8/29 [110/129] via 172.31.2.33, 00:11:18, Serial0/0/0  
O 172.31.2.24/29 [110/129] via 172.31.2.33, 00:11:18, Serial0/0/0  
C 172.31.2.32/30 is directly connected, Serial0/0/0  
O 172.31.2.36/30 [110/128] via 172.31.2.33, 00:11:18, Serial0/0/0  
O\*E2 0.0.0.0/0 [110/1] via 172.31.2.33, 00:00:51, Serial0/0/0

bucaramanga#

cundinamarca#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 172.31.2.37 to network 0.0.0.0**

172.3.0.0/29 is subnetted, 1 subnets  
O 172.3.2.8 [110/65] via 172.31.2.37, 00:12:02, Serial0/0/0  
172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks  
O 172.31.0.0/26 [110/129] via 172.31.2.37, 00:11:52, Serial0/0/0  
O 172.31.0.64/26 [110/129] via 172.31.2.37, 00:11:52, Serial0/0/0  
O 172.31.0.128/26 [110/65] via 172.31.2.37, 00:12:02, Serial0/0/0

O 172.31.0.192/26 [110/65] via 172.31.2.37, 00:12:02, Serial0/0/0  
C 172.31.1.0/26 is directly connected, FastEthernet0/0.30  
C 172.31.1.64/26 is directly connected, FastEthernet0/0.20  
O 172.31.2.0/29 [110/129] via 172.31.2.37, 00:11:52, Serial0/0/0  
C 172.31.2.8/29 is directly connected, FastEthernet0/0.1  
C 172.31.2.24/29 is directly connected, FastEthernet0/0.88  
O 172.31.2.32/30 [110/128] via 172.31.2.37, 00:12:02, Serial0/0/0  
C 172.31.2.36/30 is directly connected, Serial0/0/0  
O\*E2 0.0.0.0/0 [110/1] via 172.31.2.37, 00:01:34, Serial0/0/0  
cundinamarca#

Figura 30. Verificación en PC 15

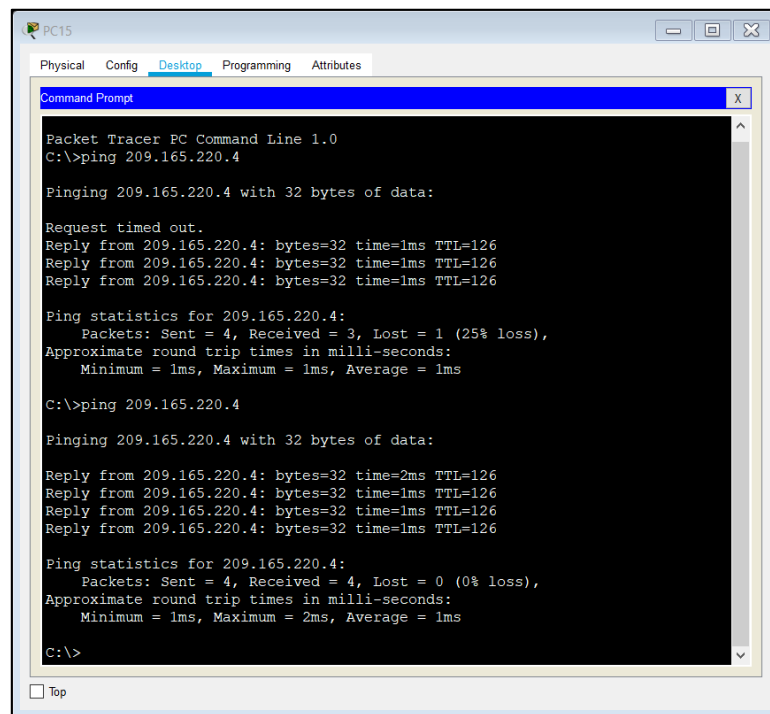
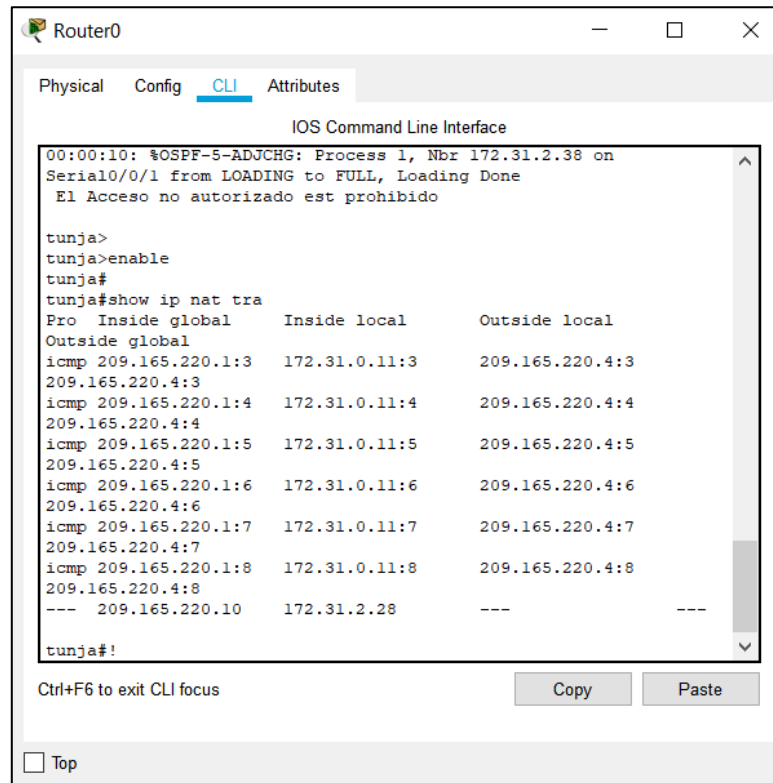


Figura 31. Router 0



The screenshot shows the CLI interface of Router0. The window title is "Router0" and it has tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, showing the "IOS Command Line Interface". The output of the command "show ip nat tra" is displayed as follows:

```
00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.38 on
Serial0/0/1 from LOADING to FULL, Loading Done
El Acceso no autorizado est prohibido

tunja>
tunja>enable
tunja#
tunja#show ip nat tra
Pro  Inside global      Inside local      Outside local
Outside global
icmp 209.165.220.1:3    172.31.0.11:3    209.165.220.4:3
209.165.220.4:3
icmp 209.165.220.1:4    172.31.0.11:4    209.165.220.4:4
209.165.220.4:4
icmp 209.165.220.1:5    172.31.0.11:5    209.165.220.4:5
209.165.220.4:5
icmp 209.165.220.1:6    172.31.0.11:6    209.165.220.4:6
209.165.220.4:6
icmp 209.165.220.1:7    172.31.0.11:7    209.165.220.4:7
209.165.220.4:7
icmp 209.165.220.1:8    172.31.0.11:8    209.165.220.4:8
209.165.220.4:8
--- 209.165.220.10      172.31.2.28      ---             ---
tunja#!
```

At the bottom of the window, there are buttons for "Copy" and "Paste", and a "Top" button.

**El enrutamiento deberá tener autenticación.**

```
bucaramanga#conf t
```

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

```
bucaramanga(config)#int s0/0/0
```

```
bucaramanga(config-if)#ip ospf authentication message-digest
```

```
bucaramanga(config-if)#ip ospf message-digest-key 1 md5 ospfpass
```

```
bucaramanga(config-if)#
```

```
tunja(config)#int s0/0/0
```

```
tunja(config-if)#ip ospf authentication message-digest
```

```
tunja(config-if)#ip ospf message-digest-key 1 md5 ospfpass
```

```
tunja(config-if)#int s0/0/1
```

```
tunja(config-if)#ip ospf authentication message-digest
```

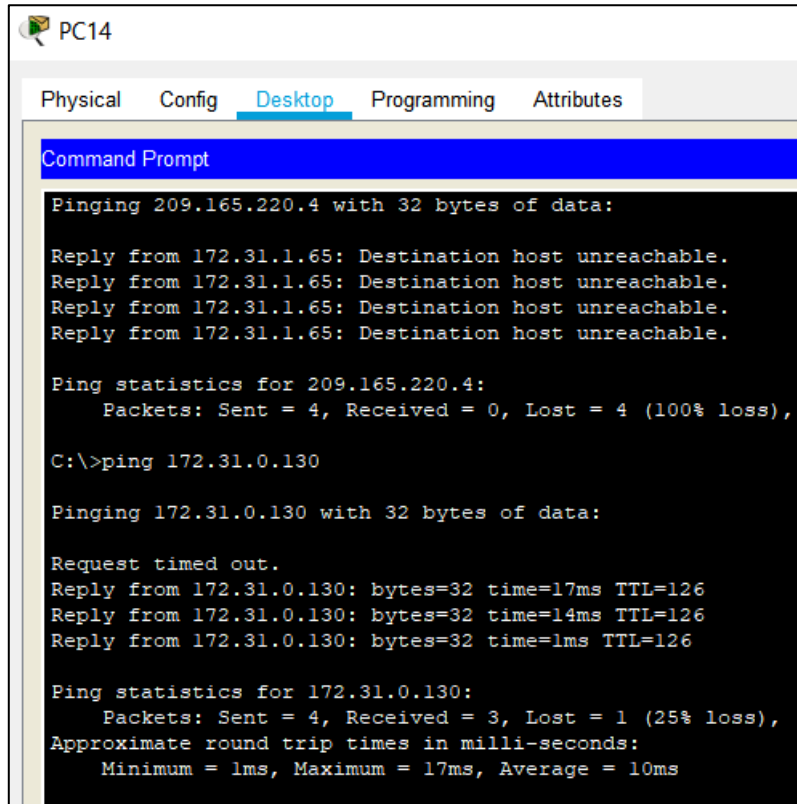
```
tunja(config-if)#ip ospf message-digest-key 1 md5 ospfpass
tunja(config-if)#
```

```
cundinamarca(config)#int s0/0/0
cundinamarca(config-if)#ip ospf authentication message-digest
cundinamarca(config-if)#ip ospf message-digest-key 1 md5 ospfpass
cundinamarca(config-if)#
```

### **Listas de control de acceso:**

```
cundinamarca(config-if)#access-list 131 deny ip 172.31.1.64 0.0.0.63
209.165.220.0 0.0.0.255
cundinamarca(config)#access-list 131 permit ip any any
cundinamarca(config)#int f0/0.20
cundinamarca(config-subif)#ip access-group 131 in
cundinamarca(config-subif)#
```

Figura 32, Verificación PC 14



```
PC14
Physical  Config  Desktop  Programming  Attributes
Command Prompt
Pinging 209.165.220.4 with 32 bytes of data:
Reply from 172.31.1.65: Destination host unreachable.
Reply from 172.31.1.65: Destination host unreachable.
Reply from 172.31.1.65: Destination host unreachable.
Reply from 172.31.1.65: Destination host unreachable.

Ping statistics for 209.165.220.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.31.0.130

Pinging 172.31.0.130 with 32 bytes of data:

Request timed out.
Reply from 172.31.0.130: bytes=32 time=17ms TTL=126
Reply from 172.31.0.130: bytes=32 time=14ms TTL=126
Reply from 172.31.0.130: bytes=32 time=1ms TTL=126

Ping statistics for 172.31.0.130:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 17ms, Average = 10ms
```

No tenemos acceso al servidor, podemos hacer ping a otro dispositivo en la red de Tunja.

**Los hosts de VLAN 30 en Cundinamarca si acceden a internet y no a la red interna de Tunja.**

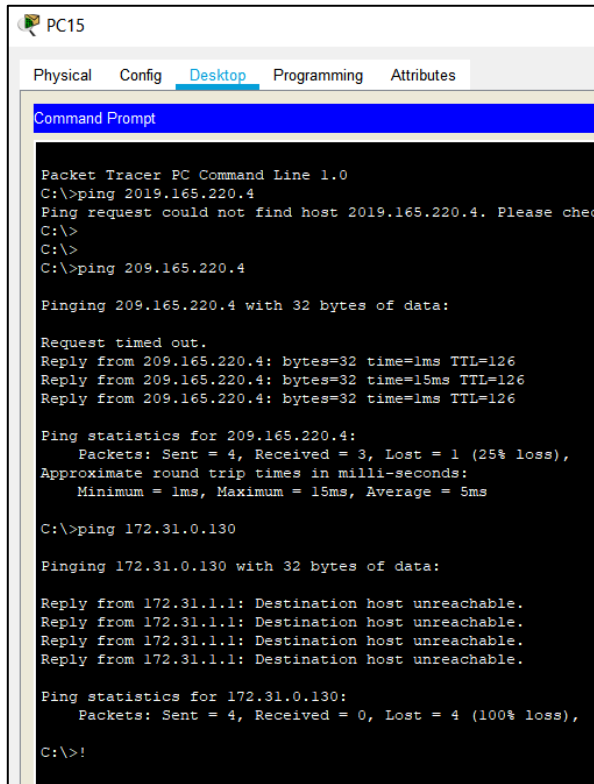
Se hace de nueva el proceso de crear la ACL y la debemos asignar a determinada interfaz indicando si esta es de entrada o de salida

```
cundinamarca(config-subif)#access-list 132 permit ip 172.31.1.0 0.0.0.63
209.165.220.0 0.0.0.255
cundinamarca(config)#access-list 132 deny ip any any
cundinamarca(config)#int f0/0.30
cundinamarca(config-subif)#ip access-group 132 in
```



cundinamarca(config-subif)#

Figura 33. Verificación PC 15



```
PC15
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 2019.165.220.4
Ping request could not find host 2019.165.220.4. Please check
C:\>
C:\>
C:\>ping 209.165.220.4

Pinging 209.165.220.4 with 32 bytes of data:

Request timed out.
Reply from 209.165.220.4: bytes=32 time=1ms TTL=126
Reply from 209.165.220.4: bytes=32 time=15ms TTL=126
Reply from 209.165.220.4: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.220.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 15ms, Average = 5ms

C:\>ping 172.31.0.130

Pinging 172.31.0.130 with 32 bytes of data:

Reply from 172.31.1.1: Destination host unreachable.
Reply from 172.31.1.1: Destination host unreachable.
Reply from 172.31.1.1: Destination host unreachable.
Reply from 172.31.1.1: Destination host unreachable.

Ping statistics for 172.31.0.130:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>!
```

Se verifica la ACL está y se observa que funciona, los dispositivos de la VLAN 30 de Cundinamarca, tiene acceso a internet sin acceso a los dispositivos de TUNJA.

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

### Procedemos a la creación.

```
tunja(config)#access-list 131 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq www
```

```
tunja(config)#access-list 131 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq ftp
```

```
tunja(config)#int f0/0.30
```

```
tunja(config-subif)#ip access-group 131 in
tunja(config-subif)#
```

Figura 34. Verificación PC 13

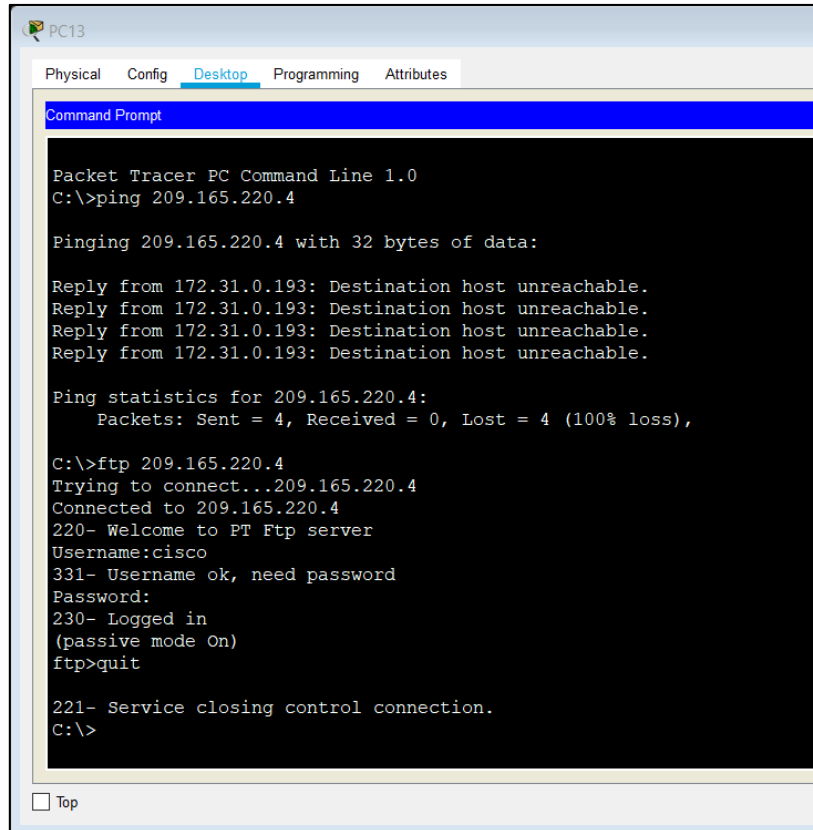
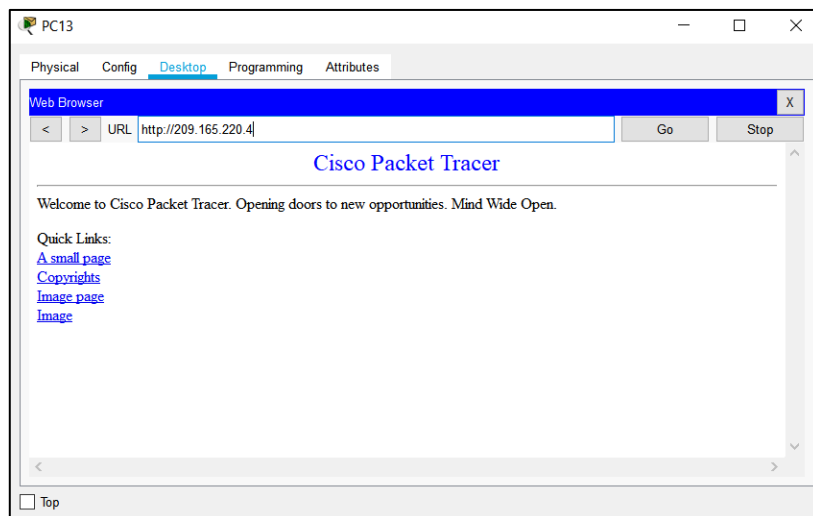


Figura 35 Verificación navegación en PC 13



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

**Debemos crear la ACL 132 y asignarla a la interfaz f0/0.20 de Tunja de entrada.**

```
tunja(config-subif)#access-list 132 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
```

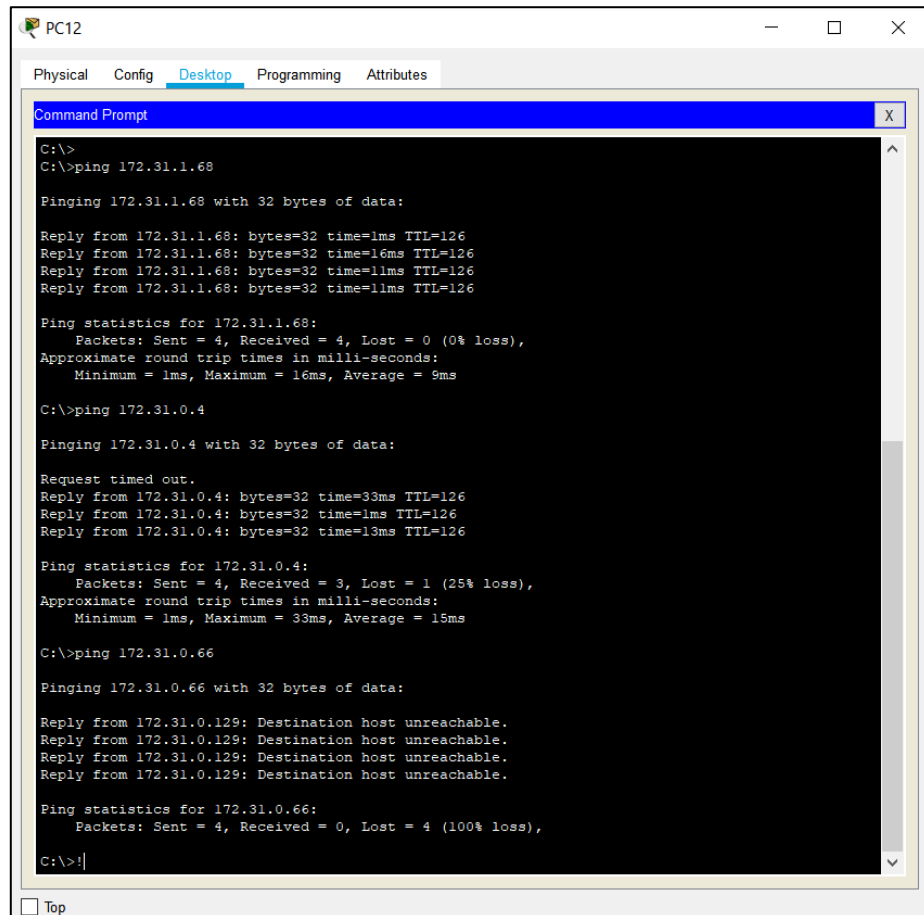
```
tunja(config)#access-list 132 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
```

```
tunja(config)#int f0/0.20
```

```
tunja(config-subif)#ip access-group 132 in
```

```
tunja(config-subif)#
```

Figura 36. Verificación PC 12



Vemos que si podemos llegar a las VLAN indicadas, pero si le damos PING a una VLAN diferente esta nos aparece destino inalcanzable.

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

Creamos la ACL y la asignamos a la interfaz adecuada indicando en este caso que es de entrada.

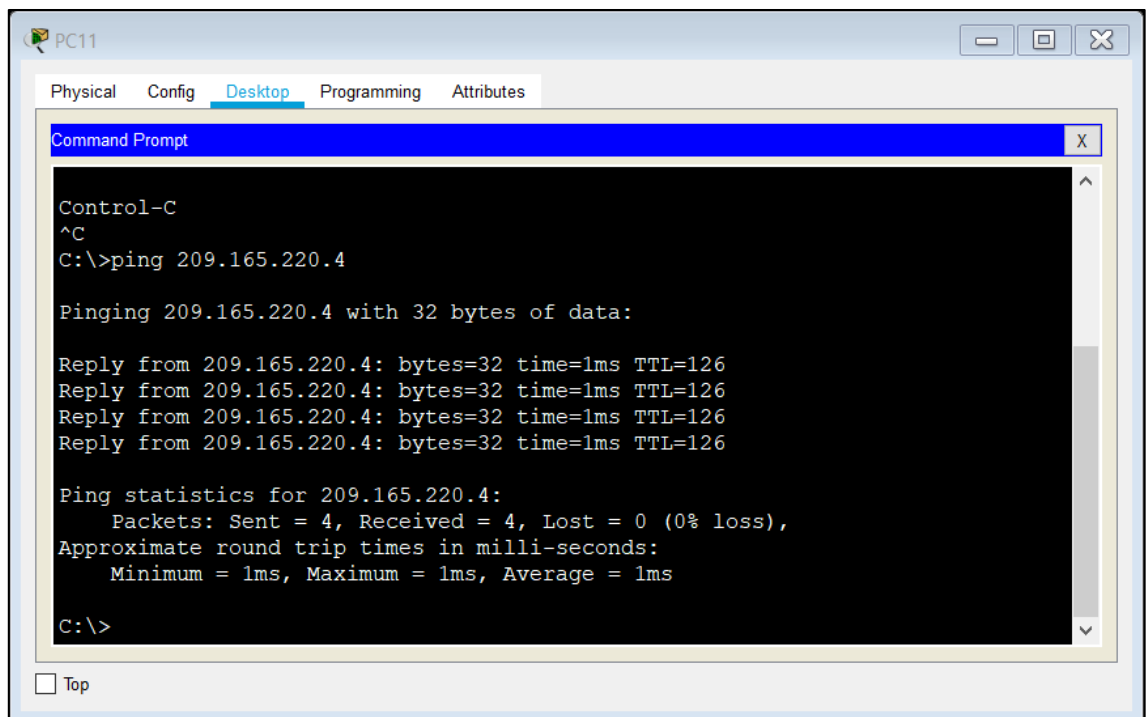
```
bucaramanga(config)#access-list 131 permit ip 172.31.0.64 0.0.0.63 209.165.220.0 0.0.0.255
```

```
bucaramanga(config)#int f0/0.30
```

```
bucaramanga(config-subif)#ip access-group 131 in
```

```
bucaramanga(config-subif)#
```

Figura 37. Verificación PC 11



**Se verifica**

Procedemos a la creación.

```
bucaramanga(config-subif)#access-list 132 permit ip 172.31.0.0 0.0.0.63  
172.31.1.64 0.0.0.63
```

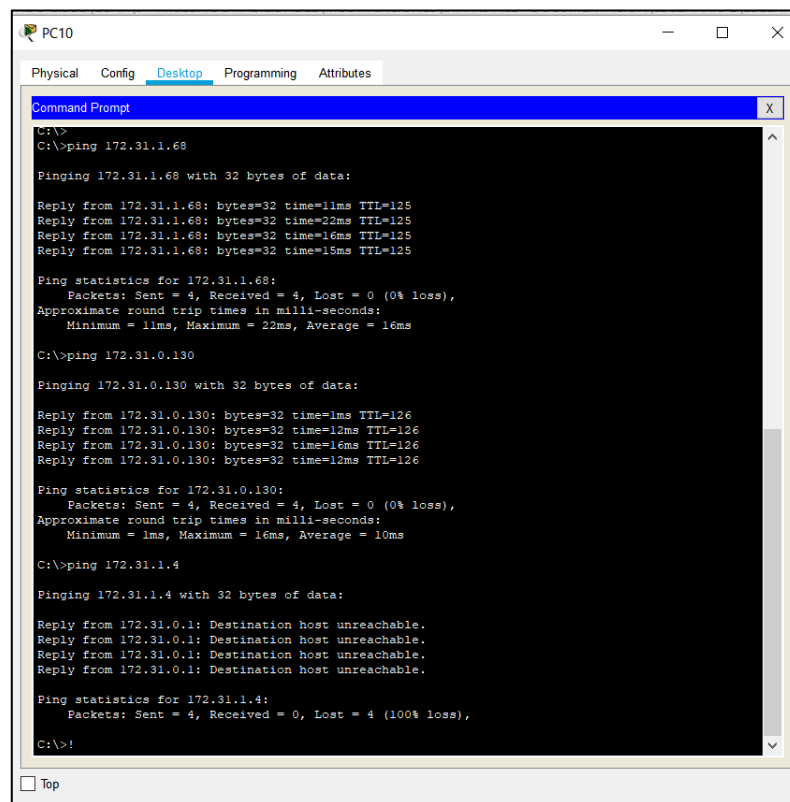
```
bucaramanga(config)#access-list 132 permit ip 172.31.0.0 0.0.0.63  
172.31.0.128 0.0.0.63
```

```
bucaramanga(config)#int f0/0.10
```

```
bucaramanga(config-subif)#ip access-group 132 in
```

```
bucaramanga(config-subif)#
```

Figura 38. Verificación PC 10



```
PC10  
Physical Config Desktop Programming Attributes  
Command Prompt  
C:\>  
C:\>ping 172.31.1.68  
  
Pinging 172.31.1.68 with 32 bytes of data:  
  
Reply from 172.31.1.68: bytes=32 time=11ms TTL=125  
Reply from 172.31.1.68: bytes=32 time=22ms TTL=125  
Reply from 172.31.1.68: bytes=32 time=16ms TTL=125  
Reply from 172.31.1.68: bytes=32 time=15ms TTL=125  
  
Ping statistics for 172.31.1.68:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 11ms, Maximum = 22ms, Average = 16ms  
  
C:\>ping 172.31.0.130  
  
Pinging 172.31.0.130 with 32 bytes of data:  
  
Reply from 172.31.0.130: bytes=32 time=1ms TTL=126  
Reply from 172.31.0.130: bytes=32 time=12ms TTL=126  
Reply from 172.31.0.130: bytes=32 time=16ms TTL=126  
Reply from 172.31.0.130: bytes=32 time=12ms TTL=126  
  
Ping statistics for 172.31.0.130:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 1ms, Maximum = 16ms, Average = 10ms  
  
C:\>ping 172.31.1.4  
  
Pinging 172.31.1.4 with 32 bytes of data:  
  
Reply from 172.31.0.1: Destination host unreachable.  
Reply from 172.31.0.1: Destination host unreachable.  
Reply from 172.31.0.1: Destination host unreachable.  
Reply from 172.31.0.1: Destination host unreachable.  
  
Ping statistics for 172.31.1.4:  
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
  
C:\>!
```

```
bucaramanga(config-subif)#access-list 123 deny ip 172.31.2.0 0.0.0.7  
172.31.0.0 0.0.0.63
```

```
bucaramanga(config)#access-list 123 deny ip 172.31.0.64 0.0.0.63 172.31.0.0  
0.0.0.63
```

```
bucaramanga(config)#access-list 123 permit ip any any
```

```
bucaramanga(config)#int f0/0.10
```

```
bucaramanga(config-subif)#ip access-group 123 out
```

```
bucaramanga(config-subif)#
```

```
tunja(config)#access-list 123 deny ip 172.3.2.8 0.0.0.7 172.31.0.128 0.0.0.63
```

```
tunja(config)#access-list 123 deny ip 172.3.0.192 0.0.0.63 172.31.0.128  
0.0.0.63
```

```
tunja(config)#access-list 123 permit ip any any
```

```
tunja(config)#int f0/0.20
```

```
tunja(config-subif)#ip access-group 123 out
```

```
tunja(config-subif)#
```

```
cundinamarca(config)#access-list 123 deny ip 172.31.2.8 0.0.0.7 172.31.1.64  
0.0.0.63
```

```
cundinamarca(config)#access-list 123 deny ip 172.31.1.0 0.0.0.63 172.31.1.64  
0.0.0.63
```

```
cundinamarca(config)#access-list 123 deny ip 172.31.2.24 0.0.0.7 172.31.1.64  
0.0.0.63
```

```
cundinamarca(config)#access-list 123 permit ip any any
```

```
cundinamarca(config)#int f0/0.20
```

```
cundinamarca(config-subif)#ip access-group 123 out
```

```
cundinamarca(config-subif)#
```

En este caso debemos hacer varias pruebas con el fin de verificar el correcto funcionamiento de las ACL configuradas en los 3 routers.

Figura 39. Comando prompt pc 12

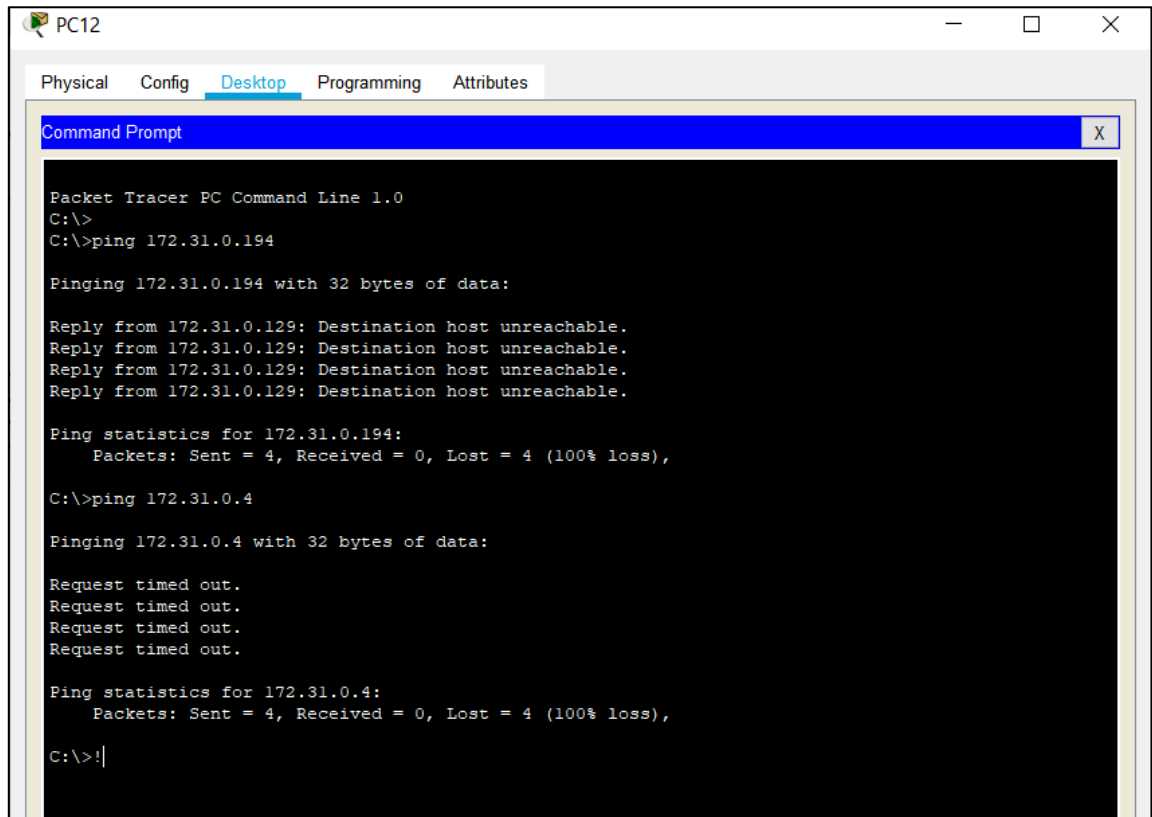
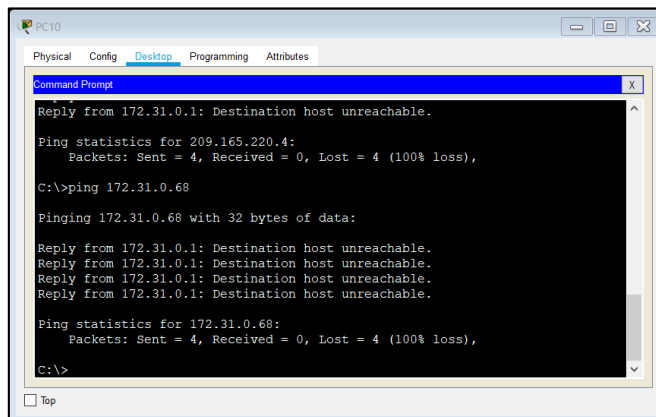


Figura 40 . Destinatario PC 10



Vemos como hosts de las VLAN administrativas y de la VLAN de servidores acceden a los routers e internet.

```
bucaramanga(config-subif)#access-list 10 permit 172.31.2.0 0.0.0.7
bucaramanga(config)#access-list 10 permit 172.3.2.8 0.0.0.7
bucaramanga(config)#access-list 10 permit 172.31.2.8 0.0.0.7
bucaramanga(config)#line vty 0 15
bucaramanga(config-line)#access-class 10 in
bucaramanga(config-line)#
```

```
tunja(config-subif)#access-list 10 permit 172.31.2.0 0.0.0.7
tunja(config)#access-list 10 permit 172.3.2.8 0.0.0.7
tunja(config)#access-list 10 permit 172.31.2.8 0.0.0.7
tunja(config)#line vty 0 15
tunja(config-line)#access-class 10 in
tunja(config-line)#
```

```
cundinamarca(config-subif)#access-list 10 permit 172.31.2.0 0.0.0.7
cundinamarca(config)#access-list 10 permit 172.3.2.8 0.0.0.7
cundinamarca(config)#access-list 10 permit 172.31.2.8 0.0.0.7
cundinamarca(config)#line vty 0 15
cundinamarca(config-line)#access-class 10 in
cundinamarca(config-line)#
```



Figura 41. Switch 1

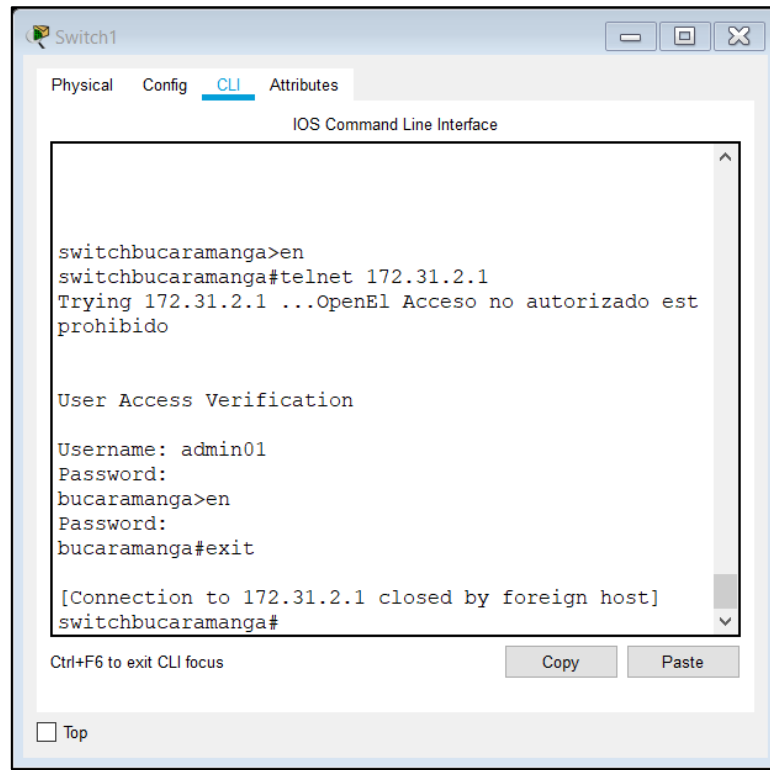
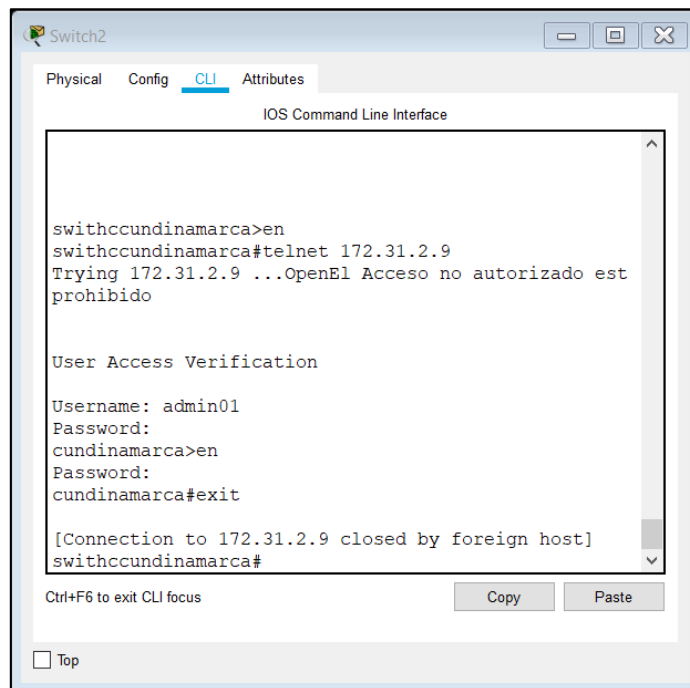


Figura 42. Switch2



VLSM: utilizar la dirección 172.31

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

Tabla 5. VLSM

Sub net Name	Need ed Size	Alloca ted Size	Address	Ma sk	Dec Mask	Assigna ble Range	Broadca st
<b>A</b>	60	62	172.31.0.0	/26	255.255.255.192	172.31.0.1 - 172.31.0.62	172.31.0.63
<b>B</b>	60	62	172.31.0.64	/26	255.255.255.192	172.31.0.65 - 172.31.0.126	172.31.0.127
<b>C</b>	55	62	172.31.0.128	/26	255.255.255.192	172.31.0.129 - 172.31.0.190	172.31.0.191
<b>D</b>	55	62	172.31.0.192	/26	255.255.255.192	172.31.0.193 - 172.31.0.254	172.31.0.255
<b>E</b>	40	62	172.31.1.0	/26	255.255.255.192	172.31.1.1 - 172.31.1.62	172.31.1.63
<b>F</b>	40	62	172.31.1.64	/26	255.255.255.192	172.31.1.65 - 172.31.1.126	172.31.1.127

## CONCLUSIONES

Teniendo como base las practicas realizadas en el periodo de estudio del curso CCNA el análisis del escenario en la actividad práctica prueba de habilidades, realizando la simulación con el programa Packet Tracer que nos permite el diseño y la configuración del escenario propuesto para la solución del problema, y así tener un mejor funcionamiento en todos los problemas porque nos permite realizarlo de una forma muy sencilla y práctica.

Las exigencias en la Academia internacional CISCO permitieron llevar un conocimiento académico apropiado para el manejo de la herramienta de Packet Tracer simulando redes reales.

Los objetivos de este trabajo se realizaron durante el diseño y la configuración del problema planteado, donde un escenario nos brinda una información para poder realizar el procedimiento.

El material utilizado para el desarrollo de la prueba de habilidades prácticas CCNA, como módulos, laboratorios, prácticas simuladas fue proporcionado por la academia internacional CISCO, con el apoyo de los tutores, consejero académico, y equipos reales durante las prácticas virtuales.

## BIBLIOGRAFÍA

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>

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

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

CISCO. (2014). Capa de red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1>

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

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

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>

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1>

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

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>

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

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

CISCO. (2014). Ethernet. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1>

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>

CISCO. (2014). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1>

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

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

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>

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

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

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1>

Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1Im3GQVfFFrjnEGFFU>

Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1Im3L74BZ3bpMiXRx0>

Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de <http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live>

Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de <http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf>

Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de <http://mr-telecomunicaciones.com/wp-content/uploads/2018/09/wendellodom.pdf>

Vesga, J. (2014). Configuración de Switches y Routers [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC>

Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de [https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl\\_pLtPD9](https://1drv.ms/u/s!AmIJYei-NT1IhgCT9VCtl_pLtPD9)

Vesga, J. (2014). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1IhgTctKY-7F5KIRC3>

Vesga, J. (2014). Principios de Enrutamiento [OVA]. Recuperado de [https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi\\_Tm](https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm)