PRUEBA DE HABILIDADES PRÁCTICAS CNNA

DIPLOMADO DE PROFUNDIZACIÓN CISCO

(DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN/WAN)

ESTUDIANTE
JOSE DAVID PEREZ ARANGO

TRABAJO ESCRITO PARA OPTAR POR EL TIUTULO DE:
INGENIERO ELECTRÓNICO

TUTOR:
DIEGO EDINSON RAMIREZ CLARO

DIRECTOR DE DIPLOMADO
PHD. JUAN CARLOS VESGA FERREIRA

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA DE INGENIERIA ELECTRONICA
DIPLOMADO DE PROFUNDIZACIÓN CISCO
DOSQUEBRADAS
DICIEMBRE DE 2019

Contenido

Tabla de Ilustraciones

Resumen

La prueba de habilidades CCNA de CISCO pretende abordar de una manera practica los principios basicos del Roting y el Switching estudiados durante el curso, fortaleciendo las habilidades para conectar, configurar y administrar una red de computadoras con el fin de intercambiar información, recursos y servicios entre estos.

En esta prueba de habilidades se desarrollaran dos escenarios. En el primer escenario, una empresa posee sucursales distribuidas en las ciudades de Bogotá, Medellín y Cali en donde se debera 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. En el Segundo escenario, una empresa tiene la conexión a internet en una red Ethernet, lo cual se debe adaptar 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.

Para el desarrollo de la actividad se cuenta con el programa Packet Tracer, el cual es una herramienta de aprendizaje y simulación de redes interactiva que permite crear topologías de red, configurar dispositivos, insertar paquetes, simular e interactuar con dispositivos finales como PC`s o intermedios (host) como Swich y Routers.

Abstract

The CISCO CCNA skills test attempts to address in a practical way the basic principles of Roting and Switching studied during the course, strengthening the skills to connect, configure and manage a computer network in order to exchange information, resources and services between these.

In this skill test two scenarios will be developed. In the first scenario, a company has branches distributed in the cities of Bogotá, Medellín and Cali where each of the devices that are part of the scenario must be configured and interconnected, in accordance with the guidelines established for IP addressing, protocols of routing and other aspects that are part of the network topology. In the second scenario, a company has an internet connection in an Ethernet network, which must be adapted to facilitate that its routers and the networks they include can, through that route, contact the internet, but using the LAN network addresses original.

For the development of the activity there is the Packet Tracer program, which is a learning and simulation tool for interactive networks that allows you to create network topologies, configure devices, insert packages, simulate and interact with end devices such as PCs or intermediates (host) like Swich and Routers.

Introducción

Una red de computadoras en un elemento indispensable para asegurar la comunicación entre dos o más equipos permitiendo el intercambio de información, recursos y servicios entre estos. De esta manera no solamente las empresas pueden beneficiarse de las potencialidades de las redes de computadoras. A nivel doméstico los usuarios también pueden aprovechar sus bondades para compartir cualquier información que sea de su interés. De este modo, las redes informáticas constituyen uno de los avances tecnológicos mas relevantes en la actualidad.

El presente trabajo se realiza con el fin de realizar 2 escenarios propuestos para la prueba de habilidades CCNA 16-4 2019 del diplomado de profundización cisco. Gracias a este trabajo podremos configurar y administrar dispositivos de Networking, crear herramientas de simulación y laboratorios de acceso remoto con el fin de establecer escenarios LAN/WAN que permitan realizar un análisis sobre diversos protocolos y métricas de enrutamiento, evaluando el comportamiento de enrutadores mediante el uso de comandos de administración de tablas de enrutamiento, por medio del desarrollo de una metodología basada en problemas reales, al dar respuesta a cada uno de los problemas planteados dentro del curso.

1. Objetivos

1.1. Objetivo General

Elaborar los escenarios propuestos para la prueba de habilidades CCNA 16-4 2019 del diplomado de profundización cisco.

1.2. Objetivos Especificos

- Realizar la configuración de la red y de cada uno de los equipos que lo conforman.

- Establecer la conectividad de la red y el óptimo funcionamiento del sistema.

- Poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

- Identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado.

2. 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.

2.1. Topología de red

Los requerimientos solicitados son los siguientes:

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

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

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

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

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

Parte 6: Configuración final.

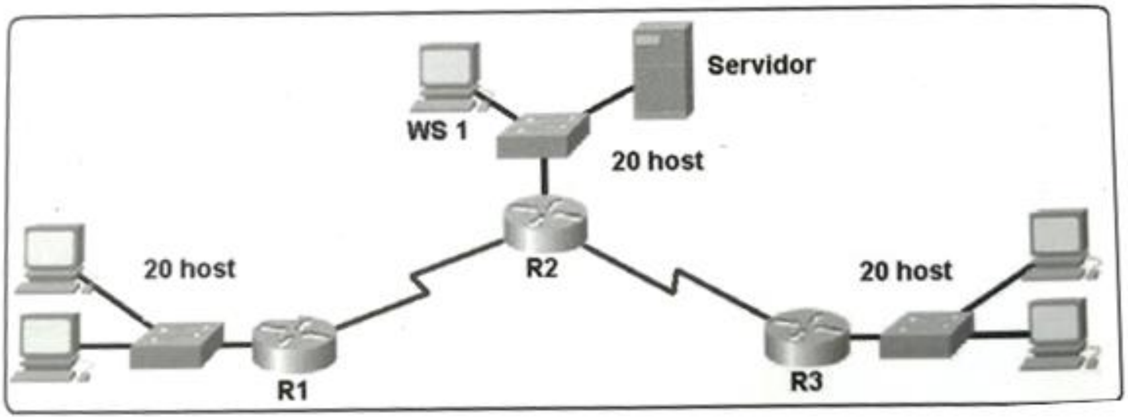


Ilustración 1: Topología de Red

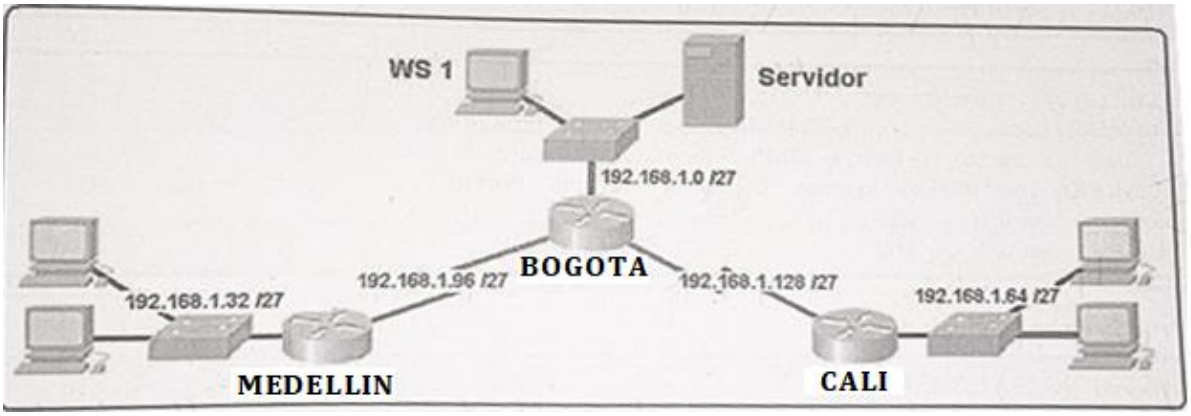


Ilustración 2: Topología de Red con Sucursales

2.2. Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

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

2.3. Parte 1: Asignación de direcciones IP:

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

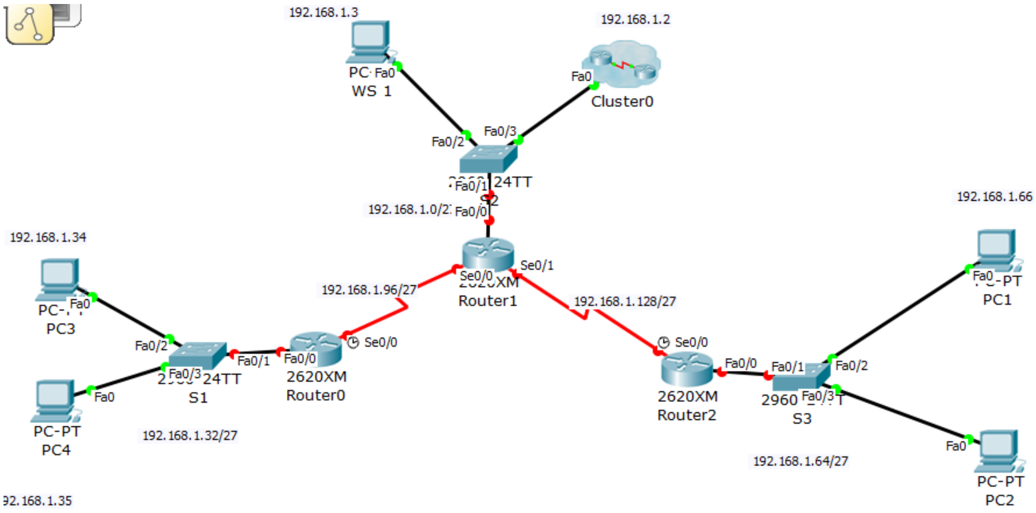
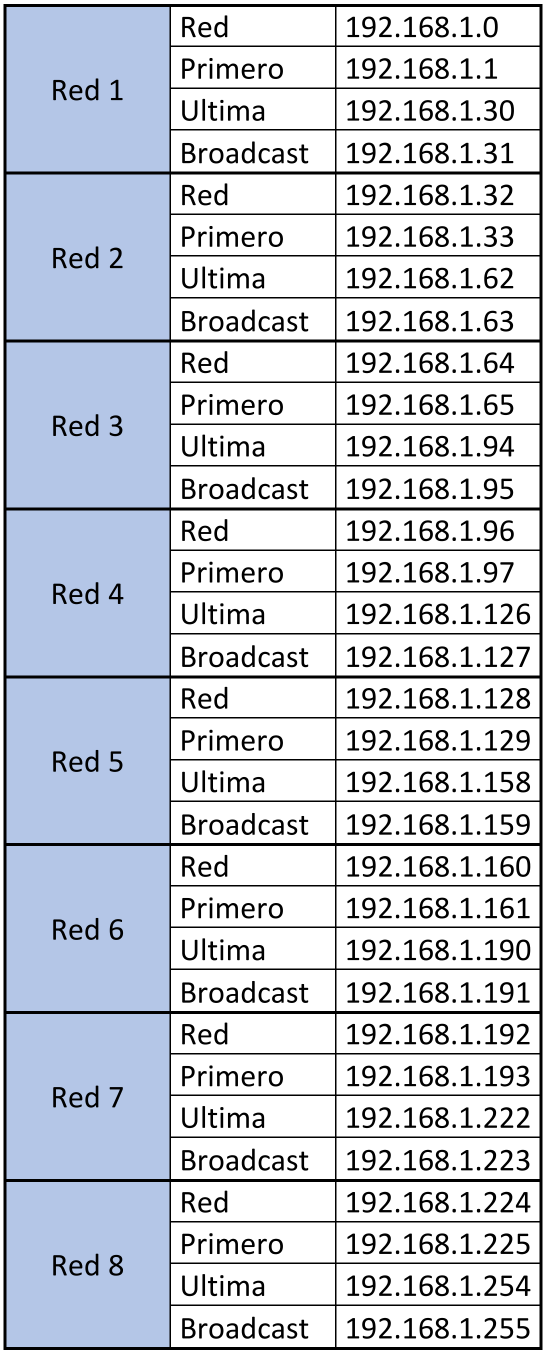


Ilustración 3: Topología de Red en Packet Tracer

Si se toman prestados 3 bits, se crean 8 subredes. **2^3 = 8 subredes.**

Mascara de Subred: 255.255.255.224



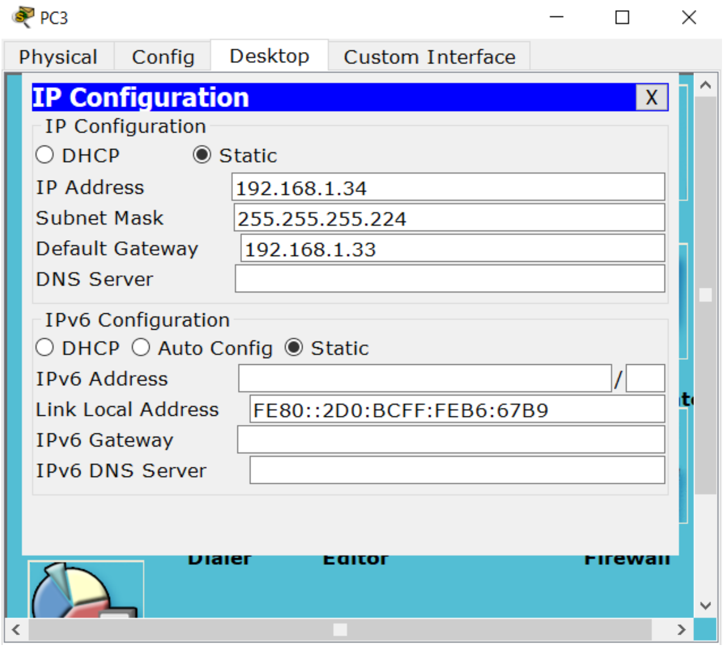
Red 1	Red	192.168.1.0
	Primero	192.168.1.1
	Ultima	192.168.1.30
	Broadcast	192.168.1.31
Red 2	Red	192.168.1.32
	Primero	192.168.1.33
	Ultima	192.168.1.62
	Broadcast	192.168.1.63
Red 3	Red	192.168.1.64
	Primero	192.168.1.65
	Ultima	192.168.1.94
	Broadcast	192.168.1.95
Red 4	Red	192.168.1.96
	Primero	192.168.1.97
	Ultima	192.168.1.126
	Broadcast	192.168.1.127
Red 5	Red	192.168.1.128
	Primero	192.168.1.129
	Ultima	192.168.1.158
	Broadcast	192.168.1.159
Red 6	Red	192.168.1.160
	Primero	192.168.1.161
	Ultima	192.168.1.190
	Broadcast	192.168.1.191
Red 7	Red	192.168.1.192
	Primero	192.168.1.193
	Ultima	192.168.1.222
	Broadcast	192.168.1.223
Red 8	Red	192.168.1.224
	Primero	192.168.1.225
	Ultima	192.168.1.254
	Broadcast	192.168.1.255

Ilustración 4: Subneteo de la Red

b. Asignar una dirección IP a la red.

Se le asigna la siguiente direcciòn IP a la Red: 192.168.1.0 /27

Se configuran los Host de cada una de las Redes.



IP Configuration

IP Configuration

○ DHCP ● Static

IP Address 192.168.1.34

Subnet Mask 255.255.255.224

Default Gateway 192.168.1.33

DNS Server

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

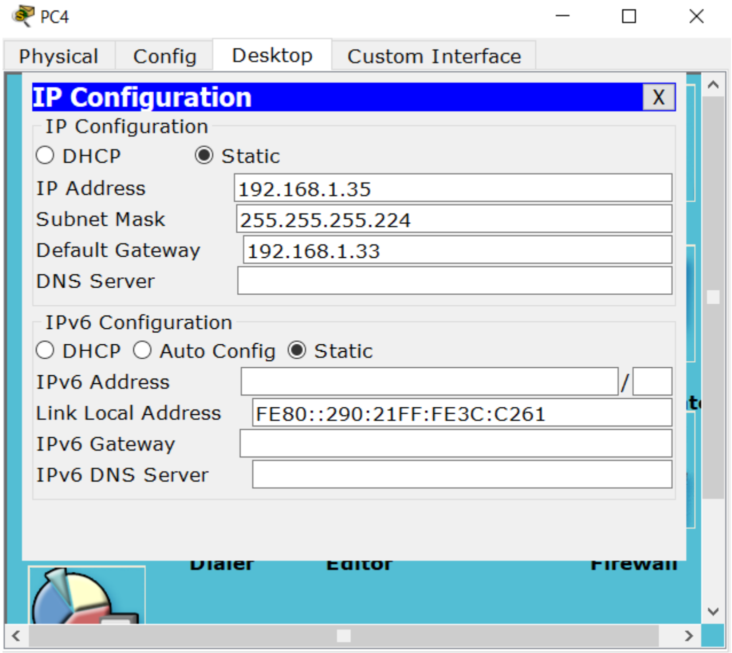
IPv6 Address /

Link Local Address FE80::2D0:BCFF:FEB6:67B9

IPv6 Gateway

IPv6 DNS Server

Ilustración 5: Configuración IP PC3



IP Configuration

IP Configuration

○ DHCP ● Static

IP Address 192.168.1.35

Subnet Mask 255.255.255.224

Default Gateway 192.168.1.33

DNS Server

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

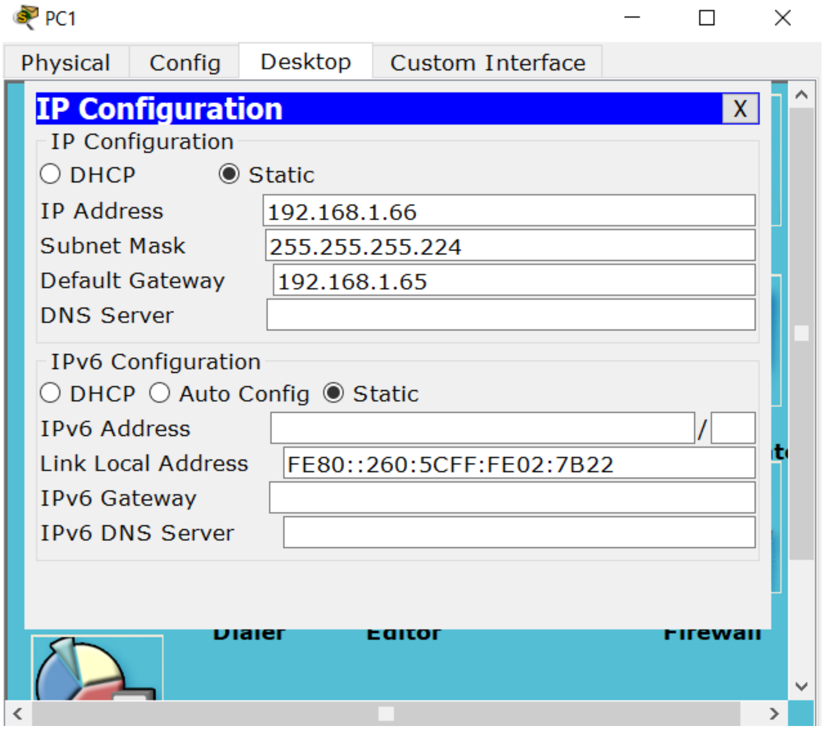
IPv6 Address /

Link Local Address FE80::290:21FF:FE3C:C261

IPv6 Gateway

IPv6 DNS Server

Ilustración 6: Configuración IP PC4



IP Configuration

IP Configuration

○ DHCP ● Static

IP Address: 192.168.1.66

Subnet Mask: 255.255.255.224

Default Gateway: 192.168.1.65

DNS Server:

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

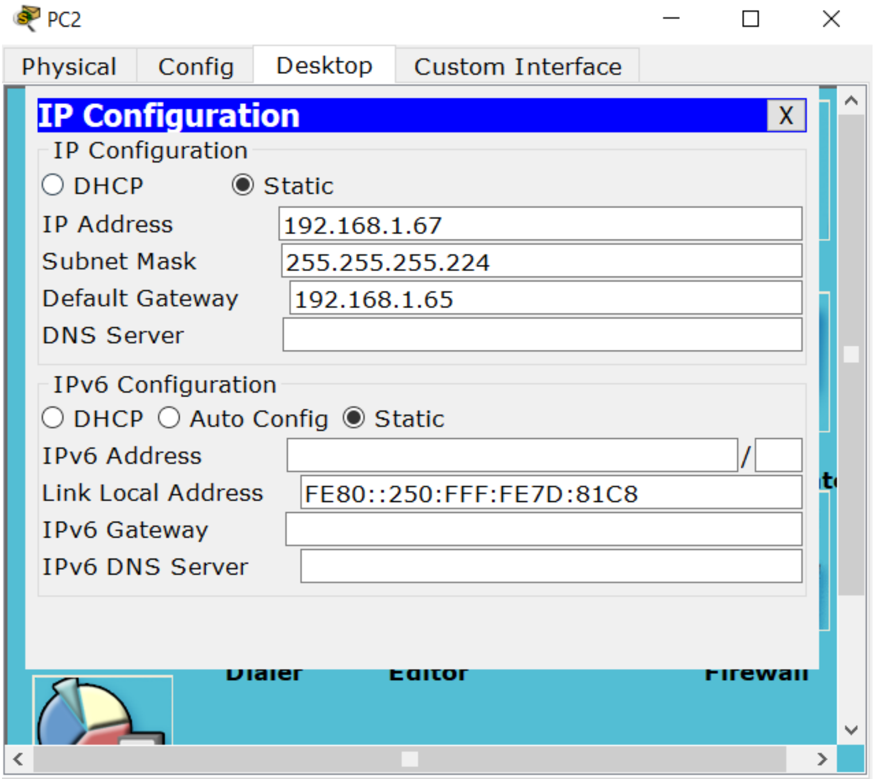
IPv6 Address: /

Link Local Address: FE80::260:5CFF:FE02:7B22

IPv6 Gateway:

IPv6 DNS Server:

Ilustración 7: Configuración IP PC1



IP Configuration

IP Configuration

○ DHCP ● Static

IP Address: 192.168.1.67

Subnet Mask: 255.255.255.224

Default Gateway: 192.168.1.65

DNS Server:

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

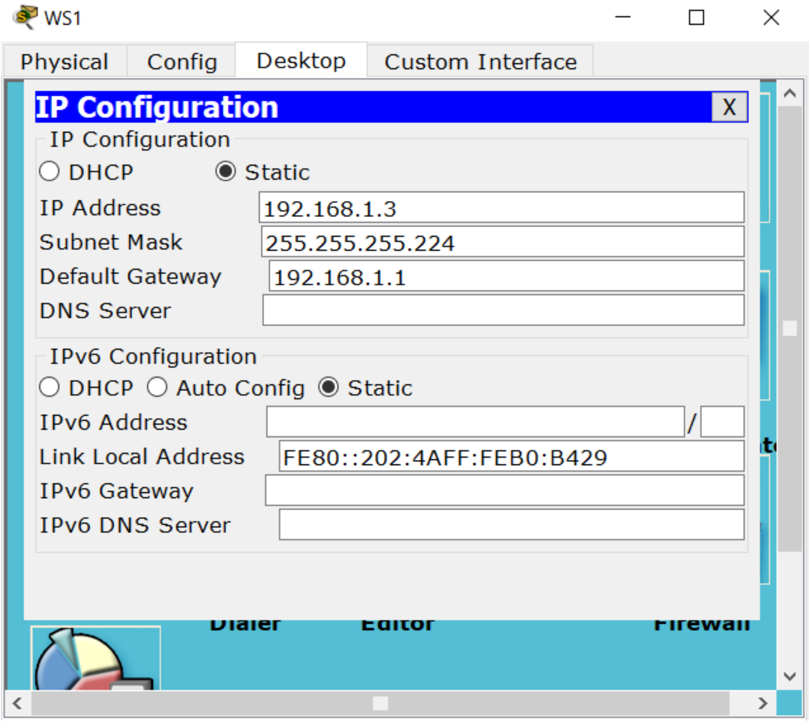
IPv6 Address: /

Link Local Address: FE80::250:FFF:FE7D:81C8

IPv6 Gateway:

IPv6 DNS Server:

Ilustración 8: Configuración IP PC2



WS1

Physical | Config | Desktop | Custom Interface

IP Configuration

IP Configuration

○ DHCP ● Static

IP Address 192.168.1.3

Subnet Mask 255.255.255.224

Default Gateway 192.168.1.1

DNS Server

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

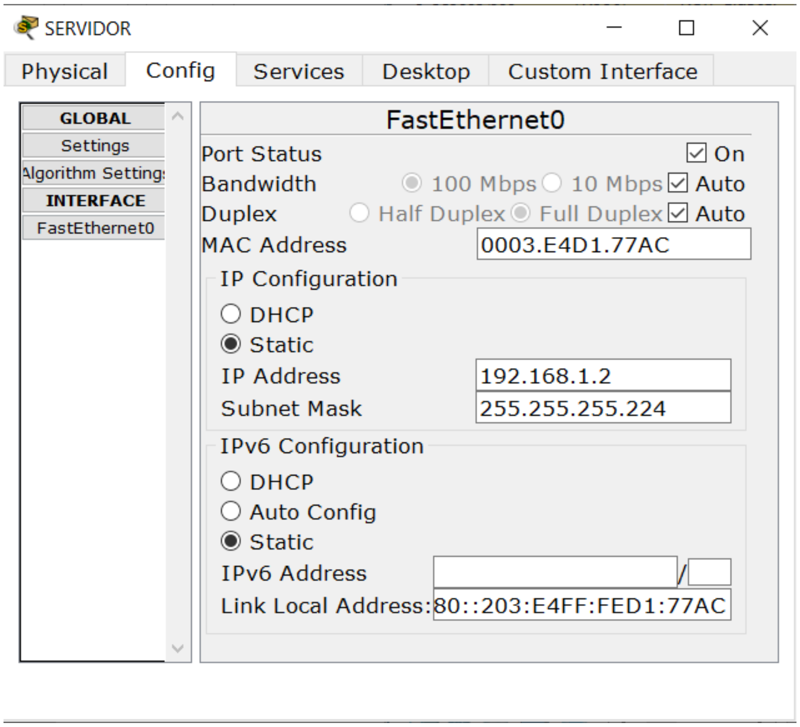
IPv6 Address /

Link Local Address FE80::202:4AFF:FEB0:B429

IPv6 Gateway

IPv6 DNS Server

Ilustración 9: Configuración IP WS1



SERVIDOR

Physical | Config | Services | Desktop | Custom Interface

FastEthernet0

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 0003.E4D1.77AC

IP Configuration

○ DHCP

● Static

IP Address 192.168.1.2

Subnet Mask 255.255.255.224

IPv6 Configuration

○ DHCP

○ Auto Config

● Static

IPv6 Address /

Link Local Address:80::203:E4FF:FED1:77AC

Ilustración 10: Configuración IP SERVIDOR

Se configura el Router BOGOTA

```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname BOGOTA
BOGOTA(config)#interface fastethernet 0/0
BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
BOGOTA(config-if)#exit
BOGOTA(config)#interface serial 0/0
BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#exit
BOGOTA(config)#interface serial0/1
BOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224
BOGOTA(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1, changed state to down
BOGOTA(config-if)#exit
BOGOTA(config)#end
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console
BOGOTA#
```

Se configura el Router MEDELLIN

```
Router>enable
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN
MEDELLIN(config)#interface fastethernet 0/0
MEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.224
MEDELLIN(config-if)#no shutdown
MEDELLIN(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
MEDELLIN(config-if)#exit
MEDELLIN(config)#interface s0/0
MEDELLIN(config-if)#ip address 192.168.1.99 255.255.255.224
MEDELLIN(config-if)#no shutdown
MEDELLIN(config-if)#
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
MEDELLIN(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
MEDELLIN(config-if)#exit
MEDELLIN(config)#end
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN#
```

Se Configura el Router CALI

```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname CALI
CALI(config)#interface fastethernet0/0
CALI(config-if)#ip address 192.168.1.65 255.255.255.224
CALI(config-if)#no shutdown
CALI(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
CALI(config-if)#exit
CALI(config)#interface s0/0
CALI(config-if)#ip address 192.168.1.131 255.255.255.224
CALI(config-if)#no shutdown
CALI(config-if)#
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
CALI(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
CALI(config-if)#exit
CALI(config)#end
CALI#
%SYS-5-CONFIG_I: Configured from console by console
CALI#
```

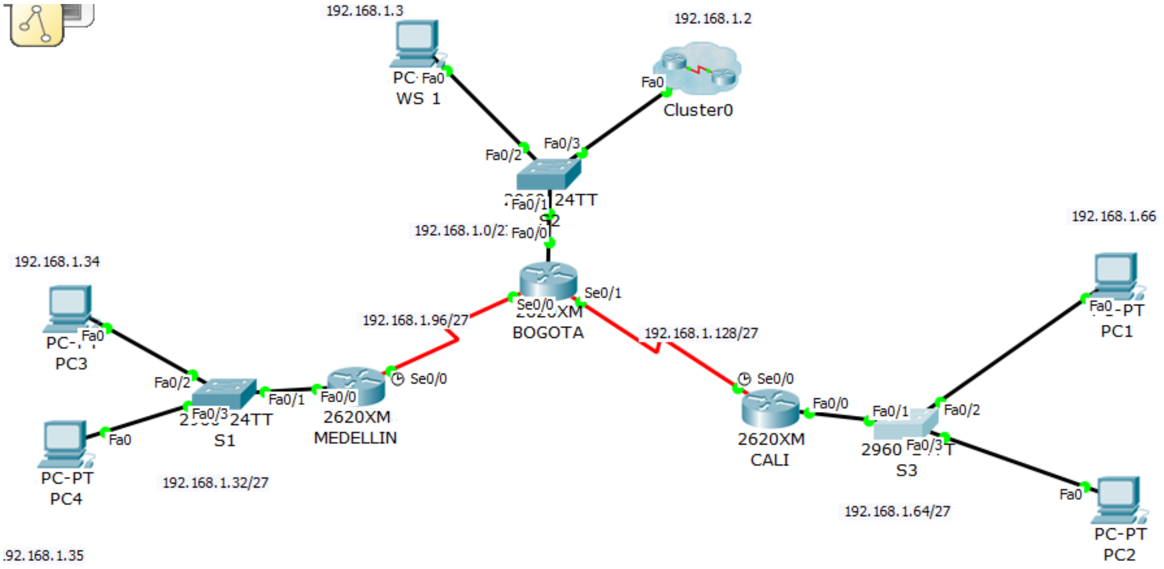


Ilustración 11: Estado de Red con la Configuración de Routers

2.4. Parte 2: Configuración Básica.

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

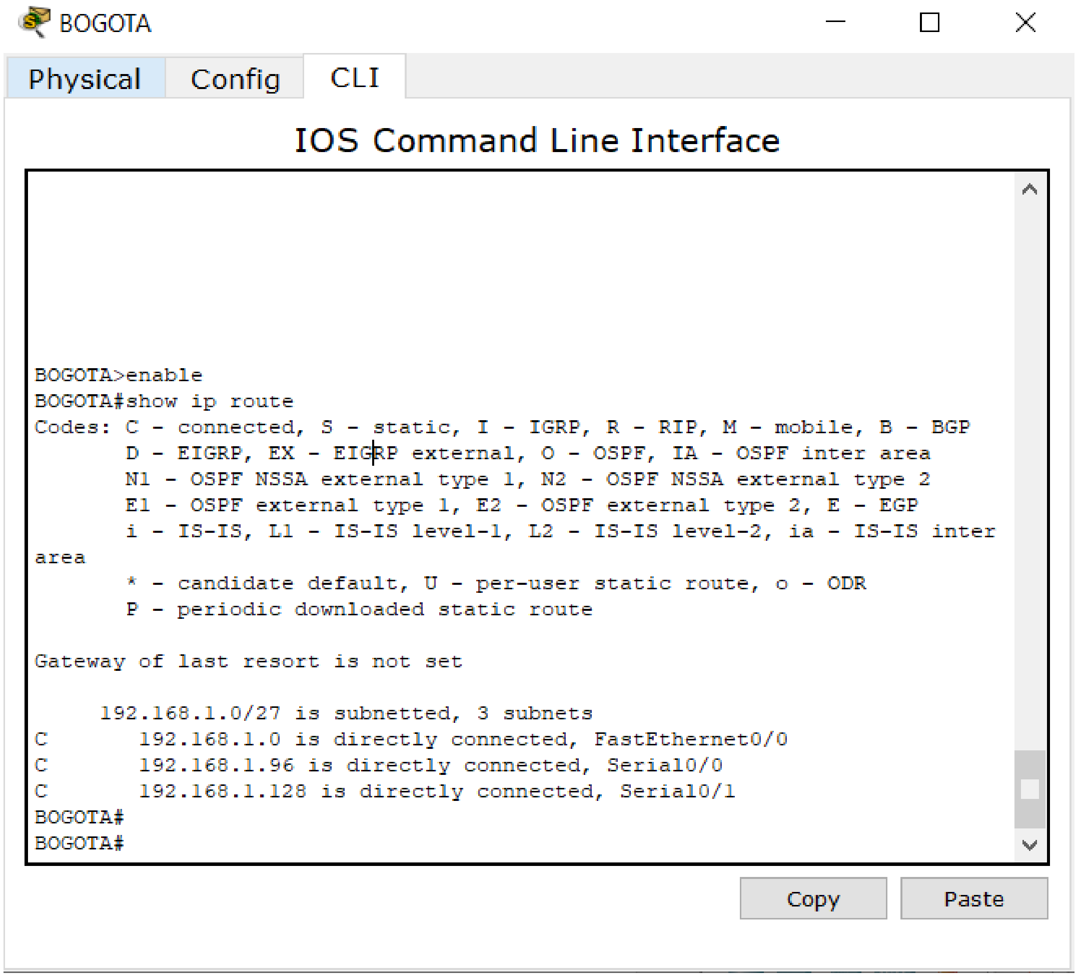
	R1	R2	R3
Nombre de Host	**MEDELLIN**	**BOGOTA**	**CALI**
Dirección de Ip en interfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/1		192.168.1.130	
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	**Eigrp**	**Eigrp**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

Ilustración 12: Configuración Básica Routers

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.

Se muestra la Tabla de enrutamiento Router BOGOTA con el comando show ip route.

BOGOTA>enable
show ip route



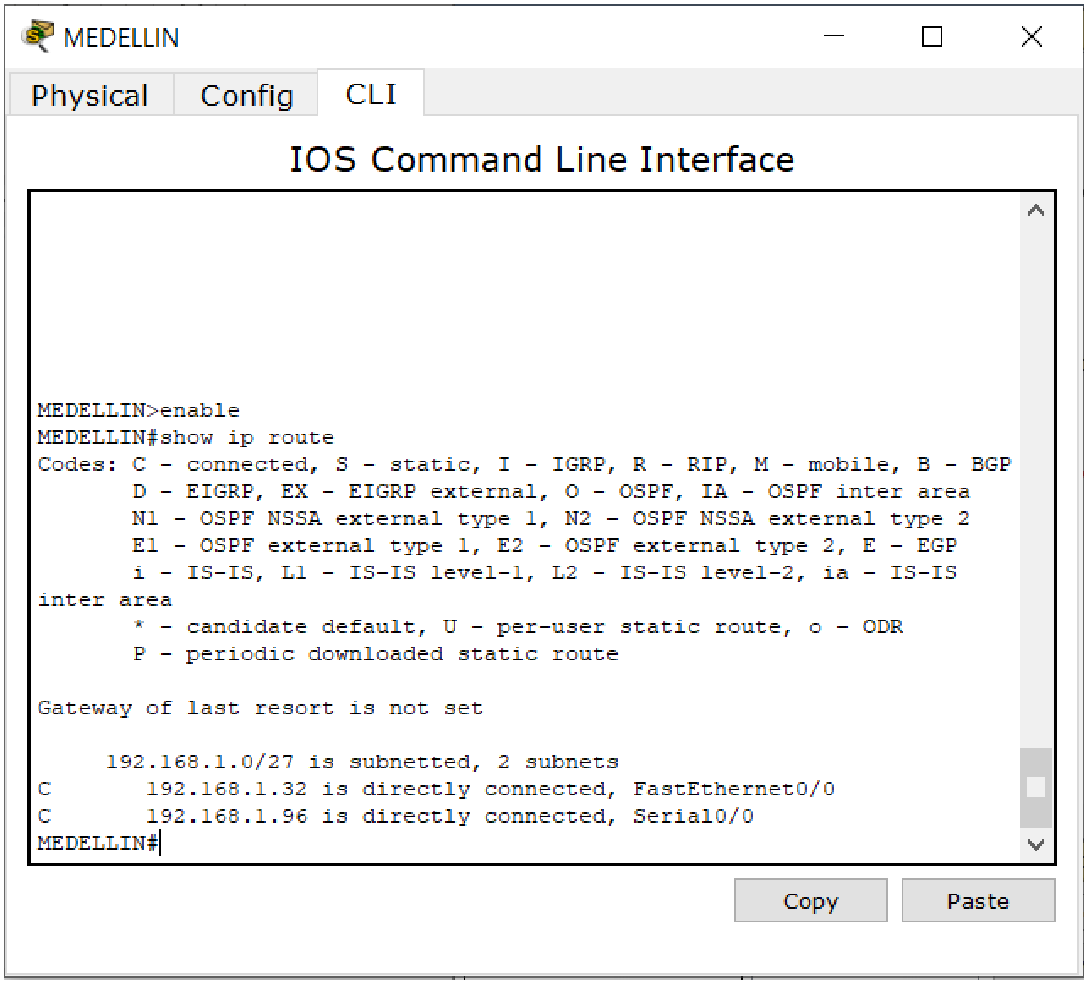
```
BOGOTA>enable
BOGOTA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external 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, 3 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0
C       192.168.1.96 is directly connected, Serial0/0
C       192.168.1.128 is directly connected, Serial0/1
BOGOTA#
BOGOTA#
```

Ilustración 13: Tabla de enrutamiento Router BOGOTA

Se muestra la Tabla de enrutamiento Router MEDELLIN con el comando show ip route.

MEDELLIN>enable

MEDELLIN#show ip route



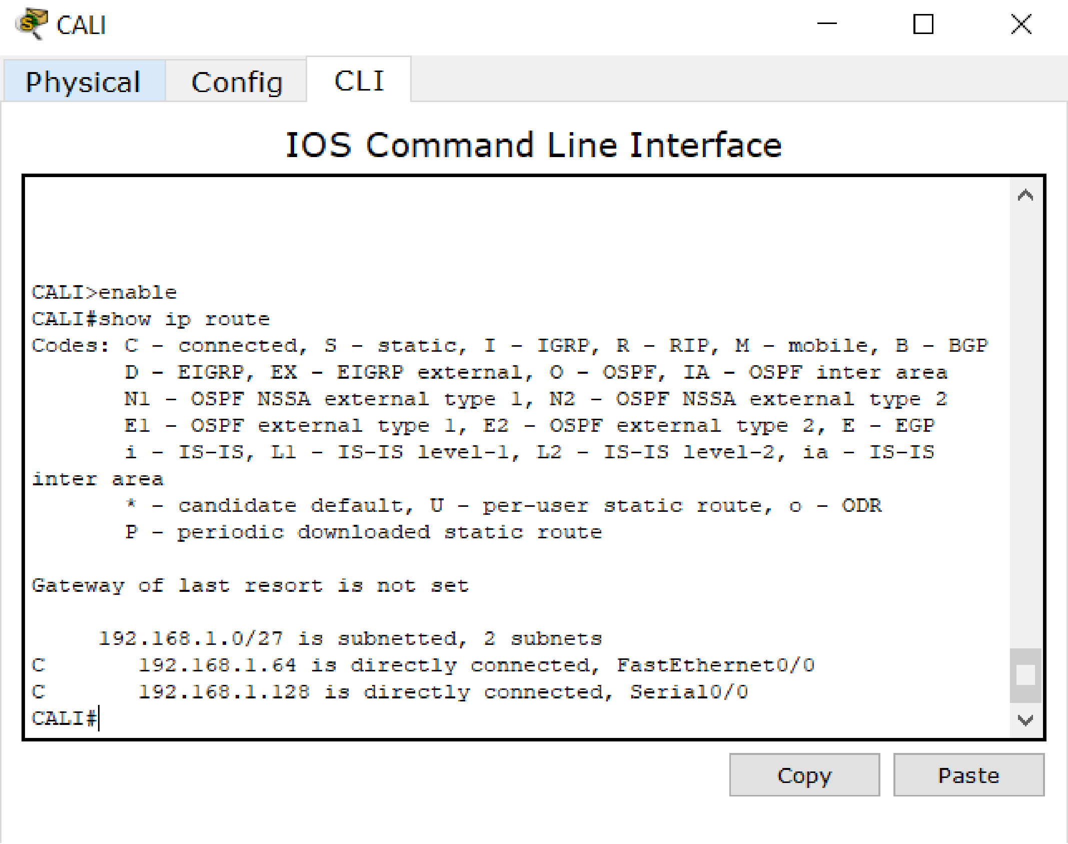
```
MEDELLIN>enable
MEDELLIN#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external 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, 2 subnets
C       192.168.1.32 is directly connected, FastEthernet0/0
C       192.168.1.96 is directly connected, Serial0/0
MEDELLIN#
```

Ilustración 14: Tabla de enrutamiento Router MEDELLIN

Se muestra la Tabla de enrutamiento Router CALI con el comando show ip route.

CALI>enable

CALI#show ip route



```
CALI>enable
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, 2 subnets
C       192.168.1.64 is directly connected, FastEthernet0/0
C       192.168.1.128 is directly connected, Serial0/0
CALI#
```

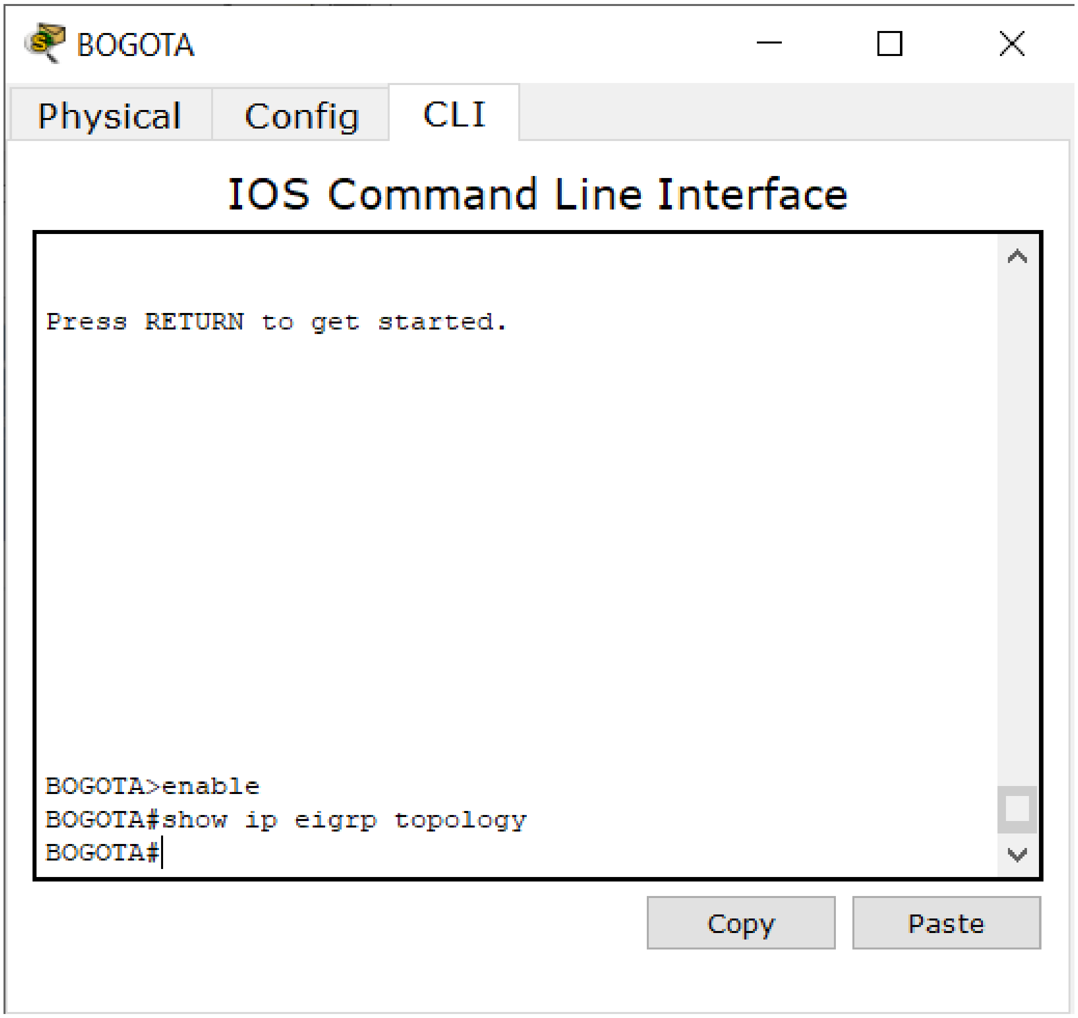
Ilustración 15: Tabla de enrutamiento Router CALI

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

Balanceo de carga en el Router BOGOTA antes de la configuración

BOGOTA>enable

BOGOTA#show ip eigrp topology



```
Press RETURN to get started.




BOGOTA>enable
BOGOTA#show ip eigrp topology
BOGOTA#
```

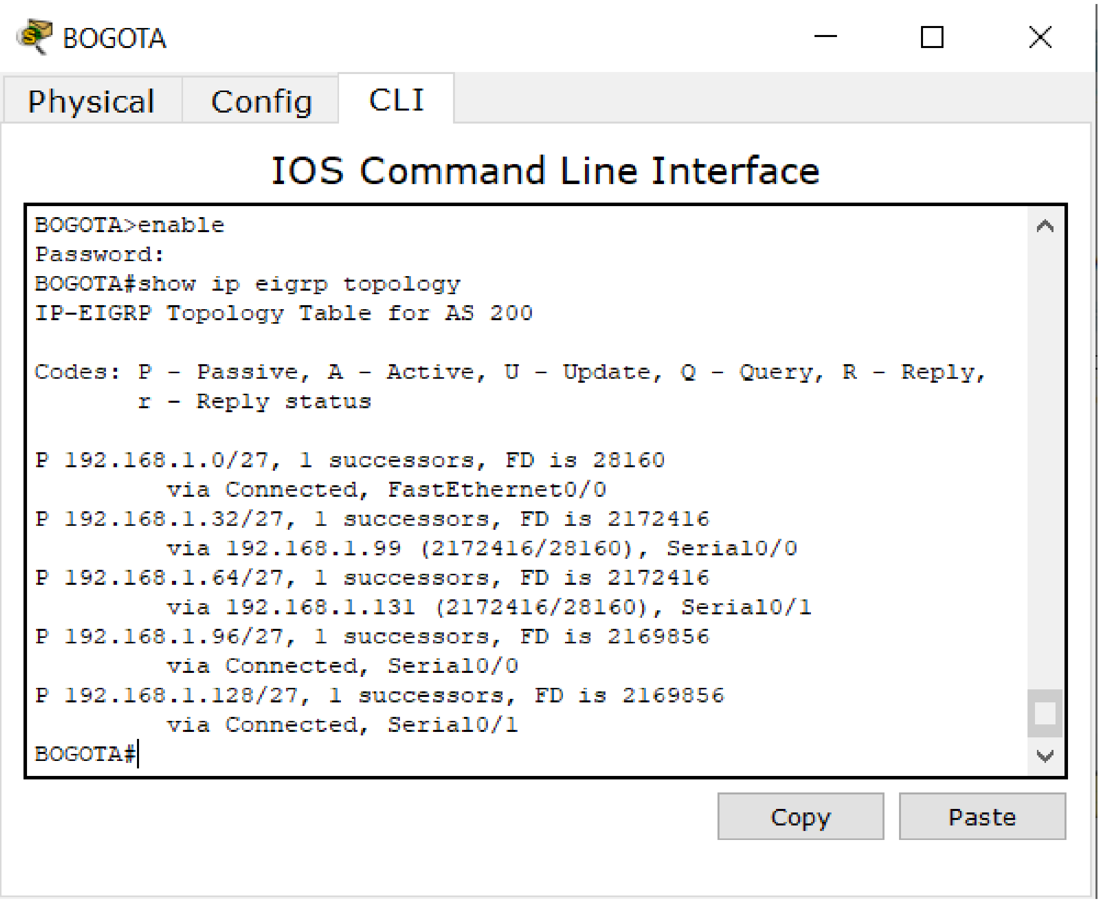
Ilustración 16: Balanceo de carga en el Router BOGOTA antes de la configuración

Balanceo de carga en el Router BOGOTA después de la configuración

BOGOTA>enable

Password:

BOGOTA#show ip eigrp topology



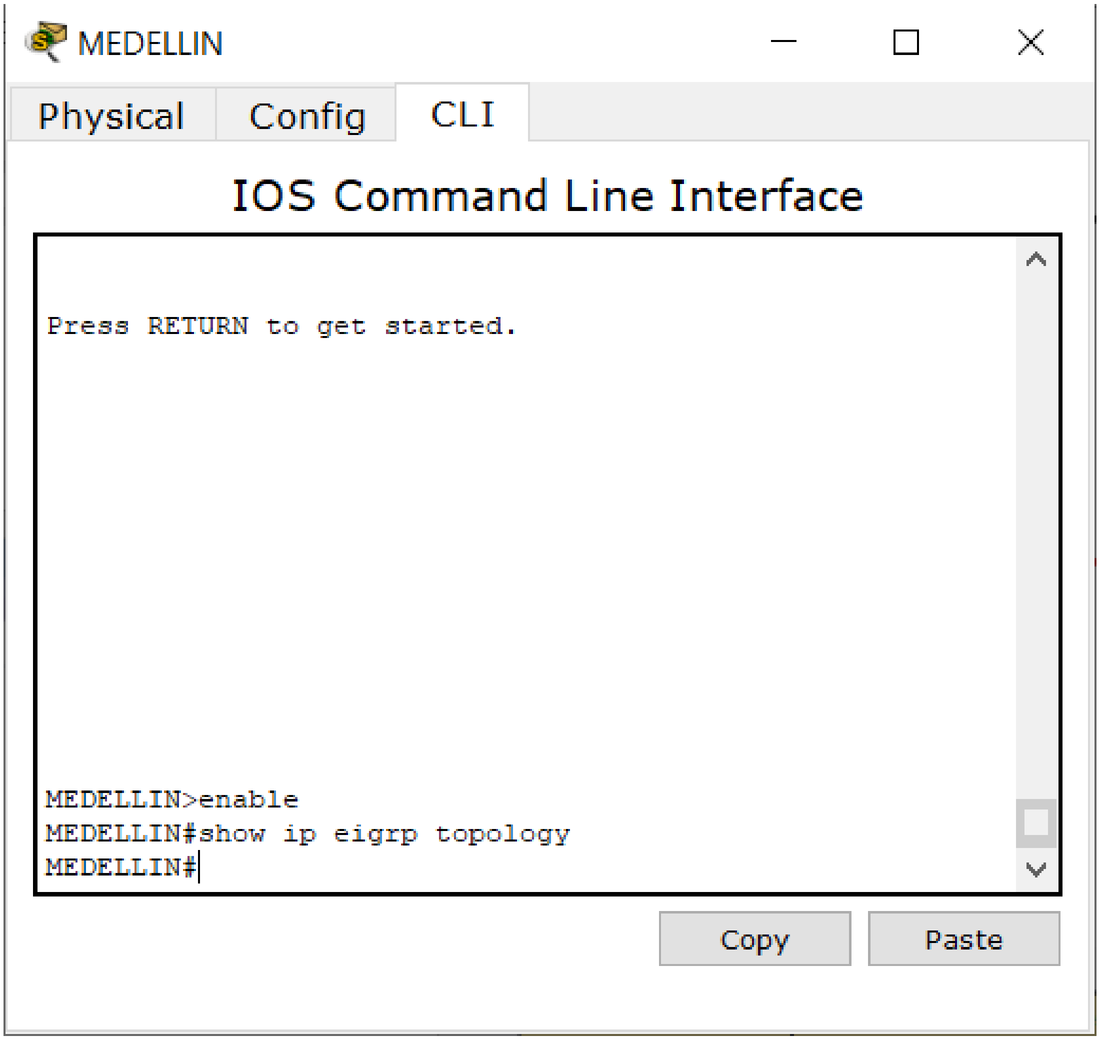
```
BOGOTA>enable
Password:
BOGOTA#show ip eigrp topology
IP-EIGRP Topology Table for AS 200

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
P 192.168.1.64/27, 1 successors, FD is 2172416
         via 192.168.1.131 (2172416/28160), Serial0/1
P 192.168.1.96/27, 1 successors, FD is 2169856
         via Connected, Serial0/0
P 192.168.1.128/27, 1 successors, FD is 2169856
         via Connected, Serial0/1
BOGOTA#
```

Ilustración 17: Balanceo de carga en el Router BOGOTA después de la configuración

Balanceo de carga en el Router MEDELLIN antes de la configuración

MEDELLIN>enable

MEDELLIN#show ip eigrp topology



```
Press RETURN to get started.









MEDELLIN>enable
MEDELLIN#show ip eigrp topology
MEDELLIN#
```

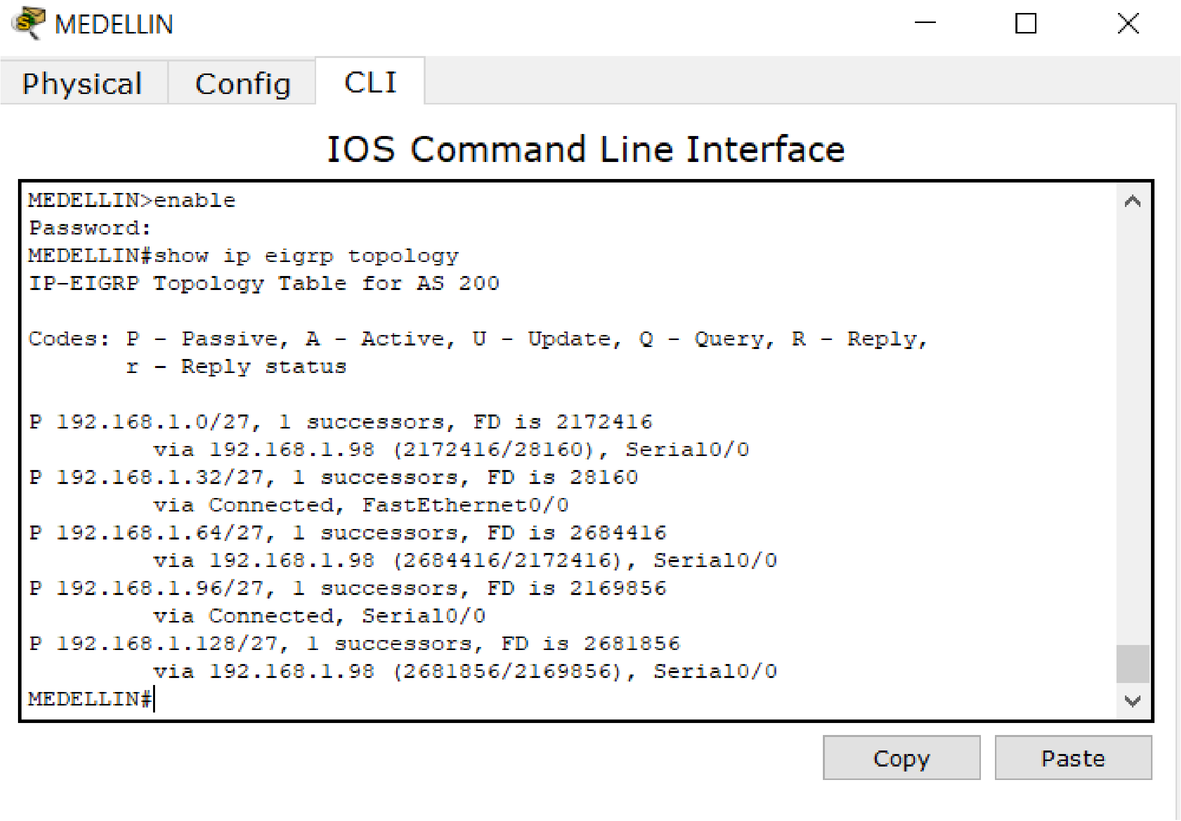
Ilustración 18: Balanceo de carga en el Router MEDELLIN antes de la configuración

Balanceo de carga en el Router MEDELLIN después de la configuración

MEDELLIN>enable

Password:

MEDELLIN#show ip eigrp topology



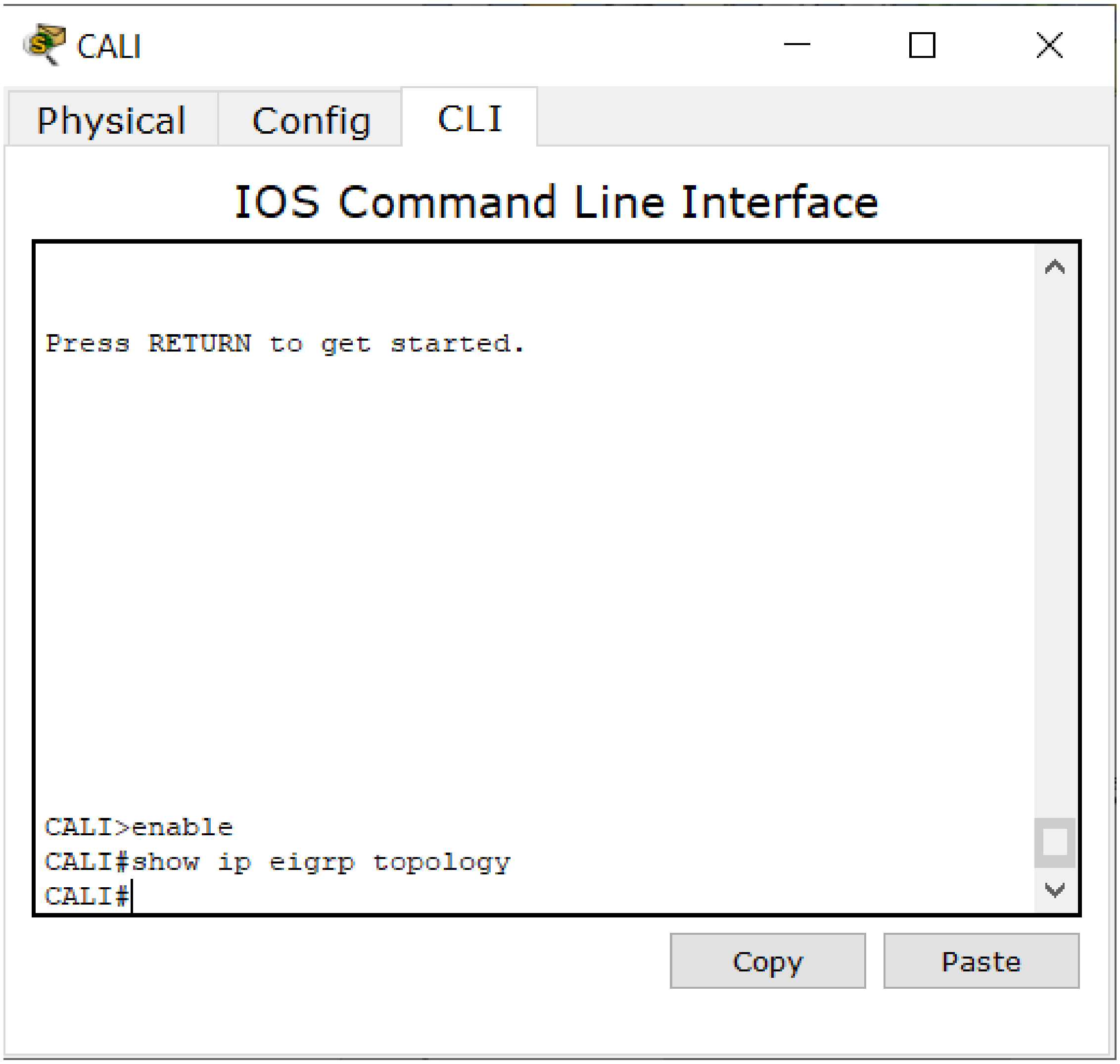
```
MEDELLIN>enable
Password:
MEDELLIN#show ip eigrp topology
IP-EIGRP Topology Table for AS 200

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
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
P 192.168.1.96/27, 1 successors, FD is 2169856
         via Connected, Serial0/0
P 192.168.1.128/27, 1 successors, FD is 2681856
         via 192.168.1.98 (2681856/2169856), Serial0/0
MEDELLIN#
```

Ilustración 19: Balanceo de carga en el Router MEDELLIN después de la configuración

Balanceo de carga en el Router CALI antes de la configuración

CALI>en

CALI#show ip eigrp topology



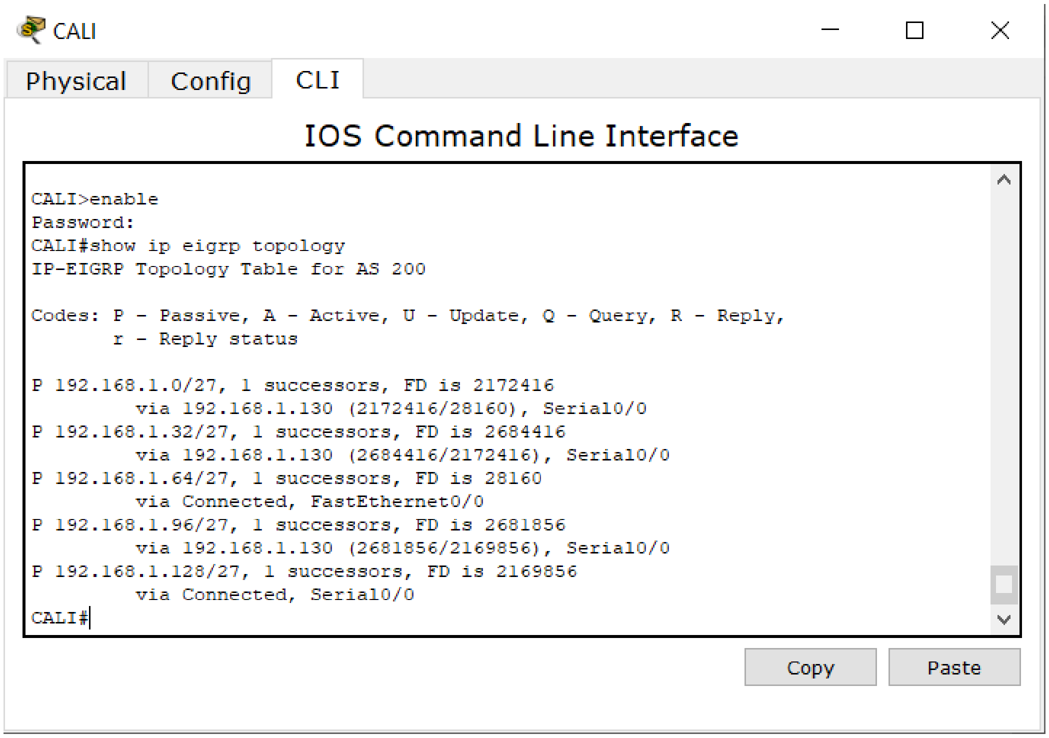
```
Press RETURN to get started.








CALI>enable
CALI#show ip eigrp topology
CALI#
```

Ilustración 20: Balanceo de carga en el Router CALI antes de la configuración

Balanceo de carga en el Router CALI después de la configuración

CALI>enable

Password:
CALI#show ip eigrp topology



```
CALI>enable
Password:
CALI#show ip eigrp topology
IP-EIGRP Topology Table for AS 200

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
P 192.168.1.32/27, 1 successors, FD is 2684416
         via 192.168.1.130 (2684416/2172416), Serial0/0
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
P 192.168.1.128/27, 1 successors, FD is 2169856
         via Connected, Serial0/0
CALI#
```

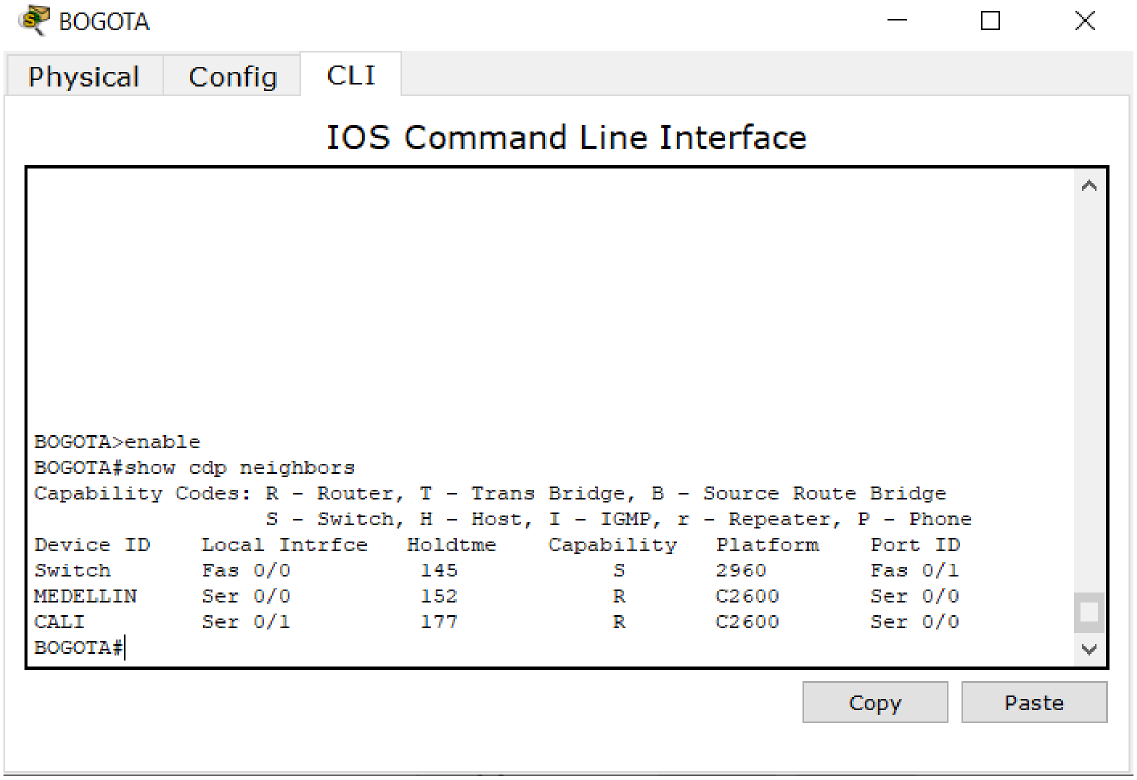
Ilustración 21: Balanceo de carga en el Router CALI después de la configuración

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

Diagnóstico de vecinos en el Router BOGOTA

BOGOTA>enable

BOGOTA#show cdp neighbors



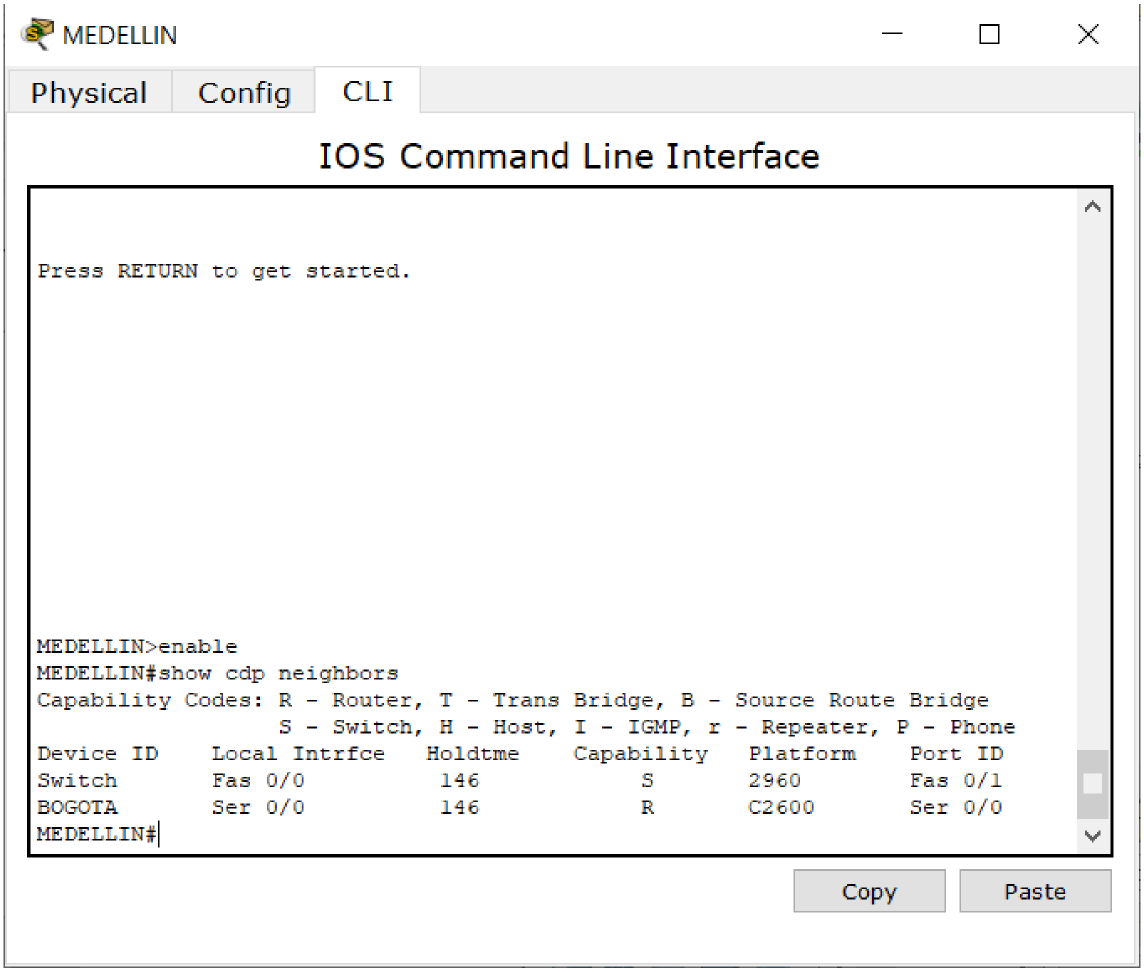
```
BOGOTA>enable
BOGOTA#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Switch       Fas 0/0          145            S        2960        Fas 0/1
MEDELLIN     Ser 0/0          152            R        C2600       Ser 0/0
CALI         Ser 0/1          177            R        C2600       Ser 0/0
BOGOTA#
```

Ilustración 22: Diagnóstico de vecinos en el Router BOGOTA

Diagnóstico de vecinos en el Router MEDELLIN

MEDELLIN>enable

MEDELLIN#show cdp neighbors



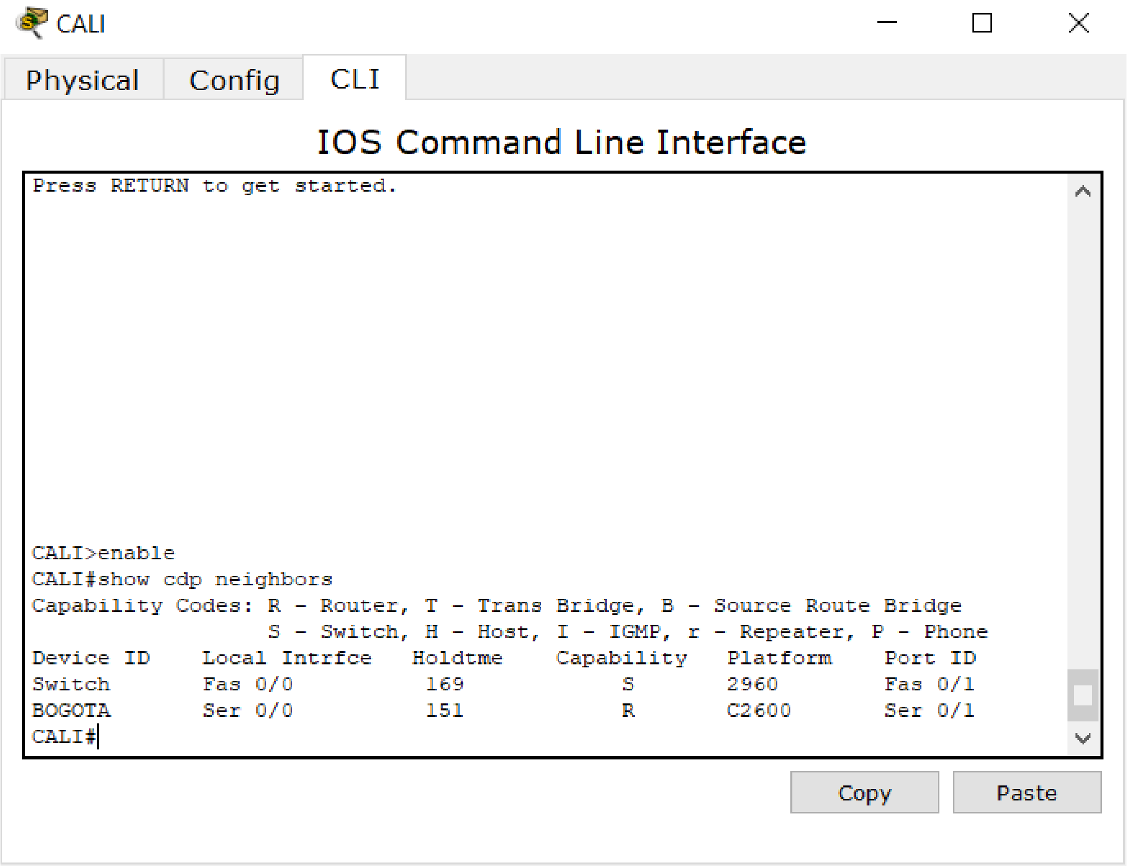
```
Press RETURN to get started.









MEDELLIN>enable
MEDELLIN#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Switch       Fas 0/0          146            S       2960        Fas 0/1
BOGOTA       Ser 0/0          146            R       C2600       Ser 0/0
MEDELLIN#
```

Ilustración 23: Diagnóstico de vecinos en el Router MEDELLIN

Diagnóstico de vecinos en el Router CALI

CALI>enable

CALI#show cdp neighbors

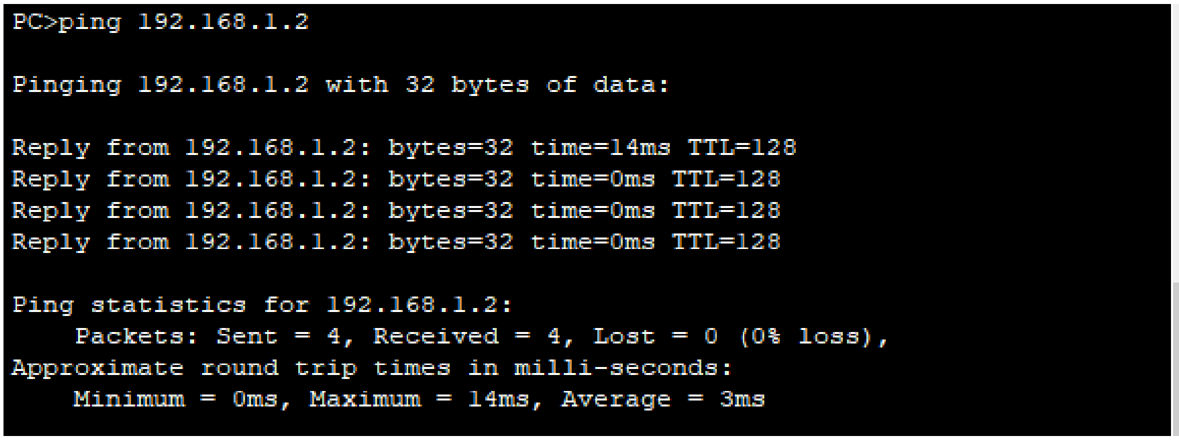


```
Press RETURN to get started.



CALI>enable
CALI#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce    Holdtme    Capability   Platform    Port ID
Switch       Fas 0/0           169            S       2960        Fas 0/1
BOGOTA       Ser 0/0           151            R       C2600       Ser 0/1
CALI#
```

Ilustración 24: Diagnóstico de vecinos en el Router CALI

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

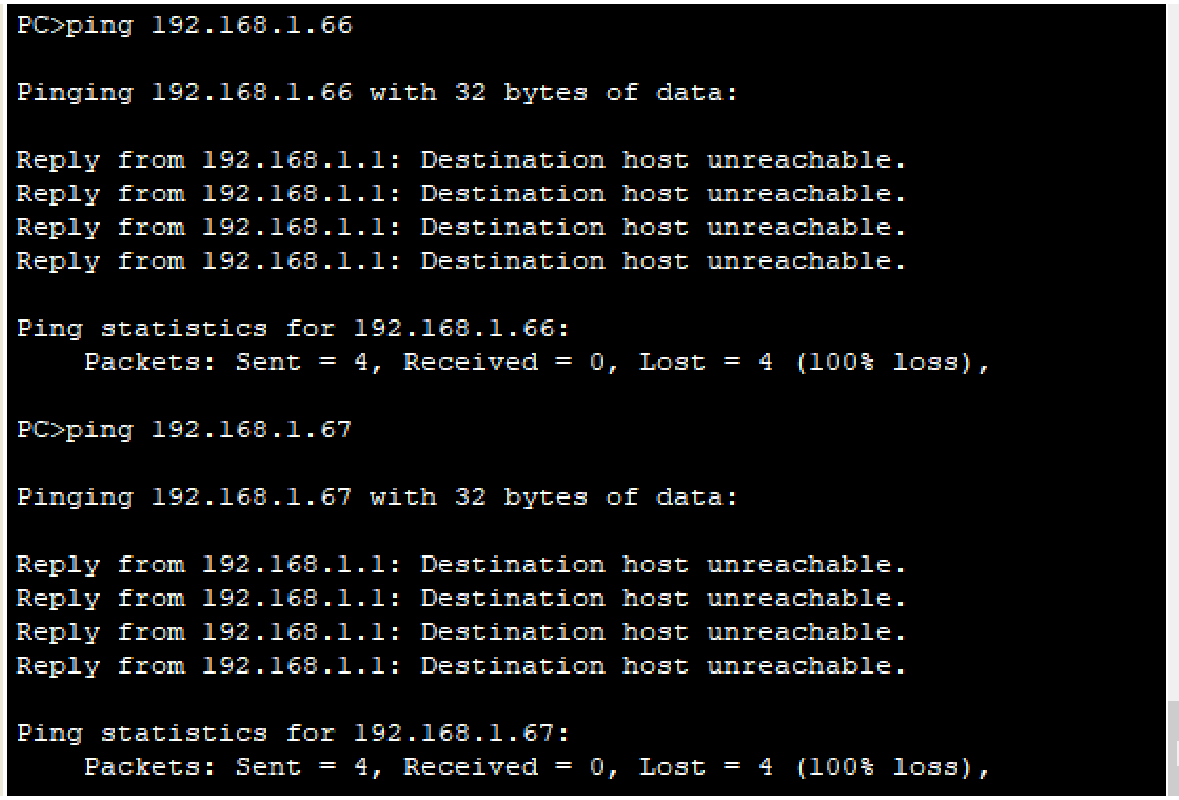
Prueba desde WS 1 a SERVIDOR



```
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=14ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128
Reply from 192.168.1.2: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 14ms, Average = 3ms
```

Ilustración 25: Prueba desde WS 1 a SERVIDOR

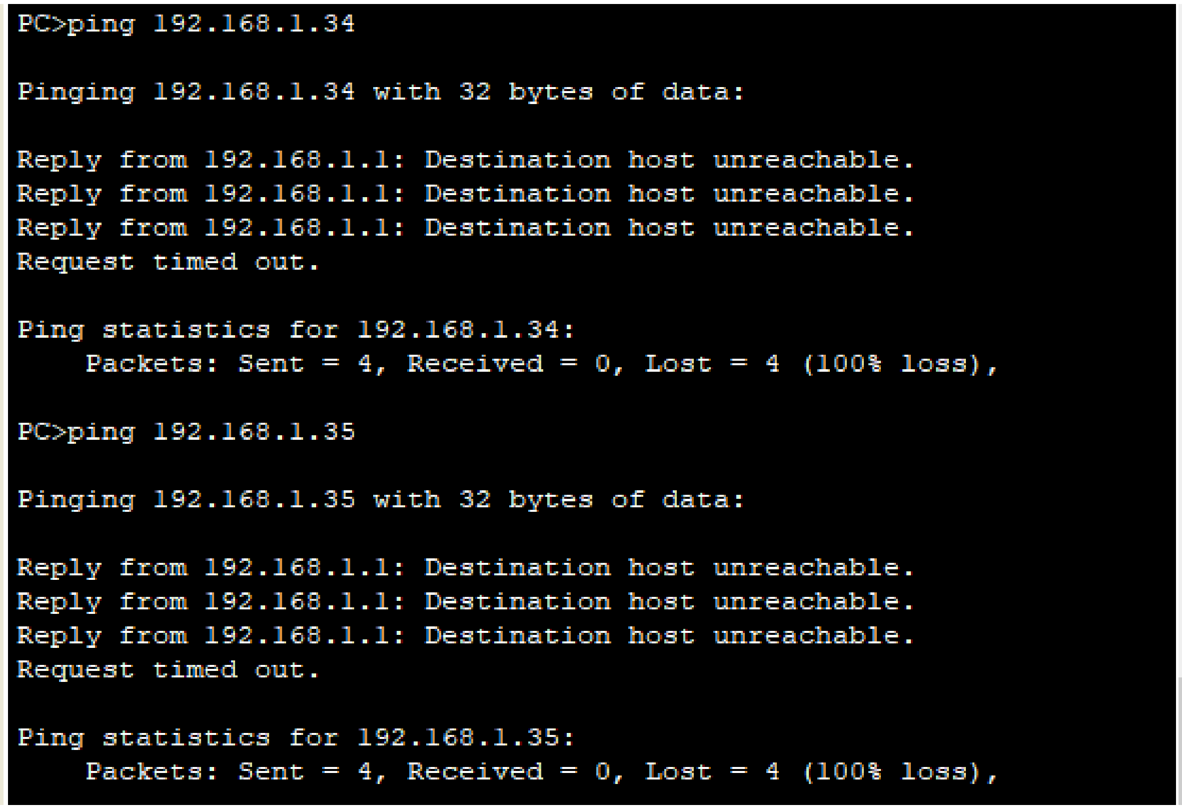
Prueba desde WS 1 a PC1 Y PC2



```
PC>ping 192.168.1.66

Pinging 192.168.1.66 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

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

PC>ping 192.168.1.67

Pinging 192.168.1.67 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.1.67:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ilustración 26: Prueba desde WS 1 a PC1 Y PC2

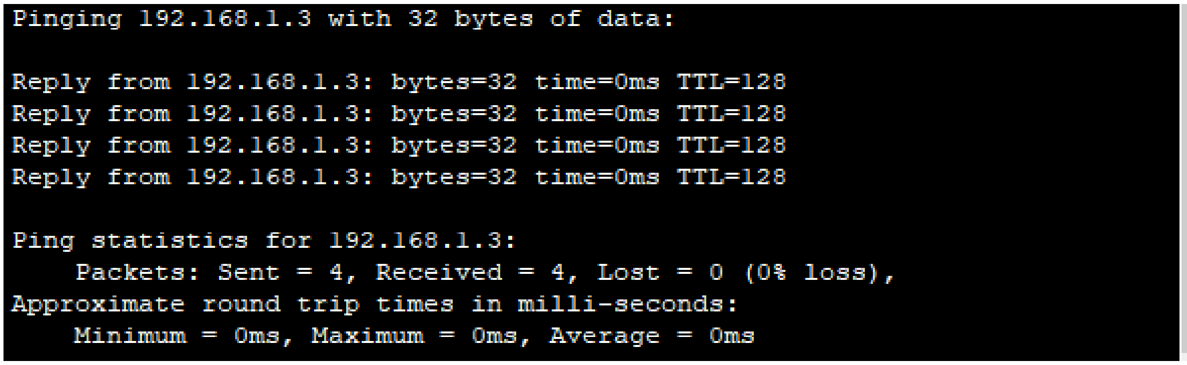
Prueba desde WS 1 a PC3 y PC4



```
PC>ping 192.168.1.34

Pinging 192.168.1.34 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Request timed out.

Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Request timed out.

Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ilustración 27: Prueba desde WS 1 a PC3 y PC4

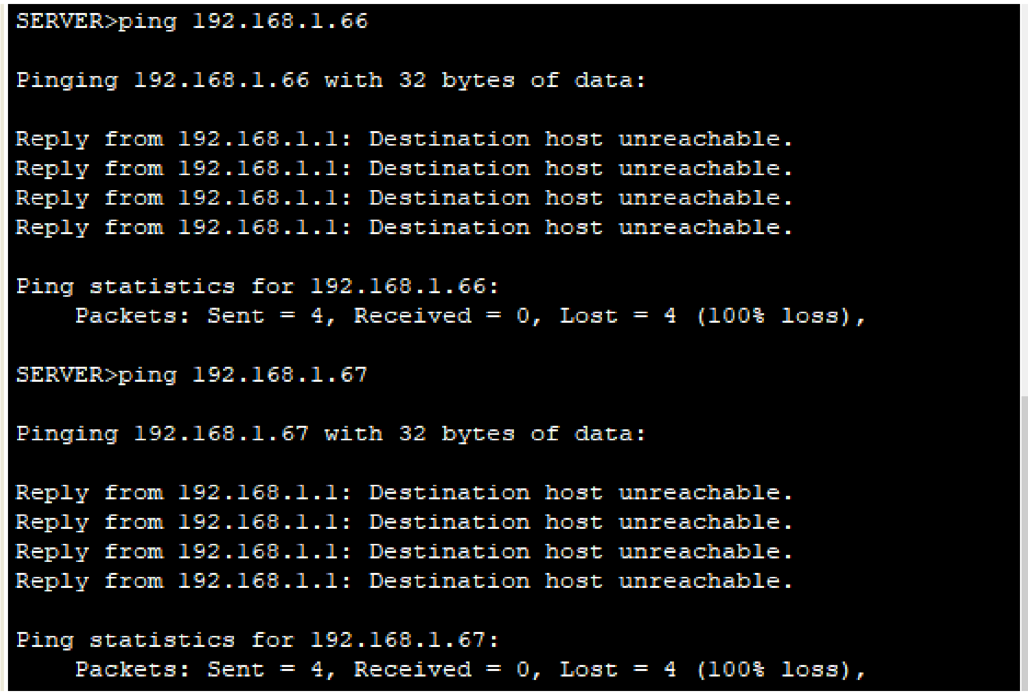
Prueba desde SERVIDOR a WS 1



```
Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128
Reply from 192.168.1.3: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ilustración 28: Prueba desde SERVIDOR a WS 1

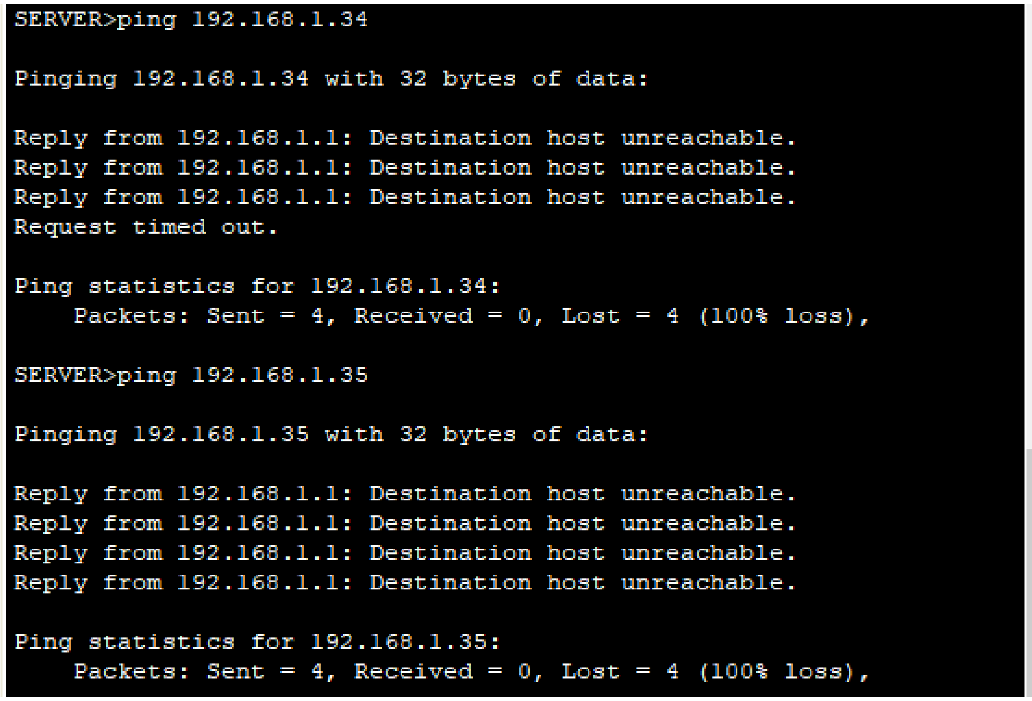
Prueba desde SERVIDOR a PC1 y PC2



```
SERVER>ping 192.168.1.66

Pinging 192.168.1.66 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

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

SERVER>ping 192.168.1.67

Pinging 192.168.1.67 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.1.67:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ilustración 29: Prueba desde SERVIDOR a PC1 y PC2

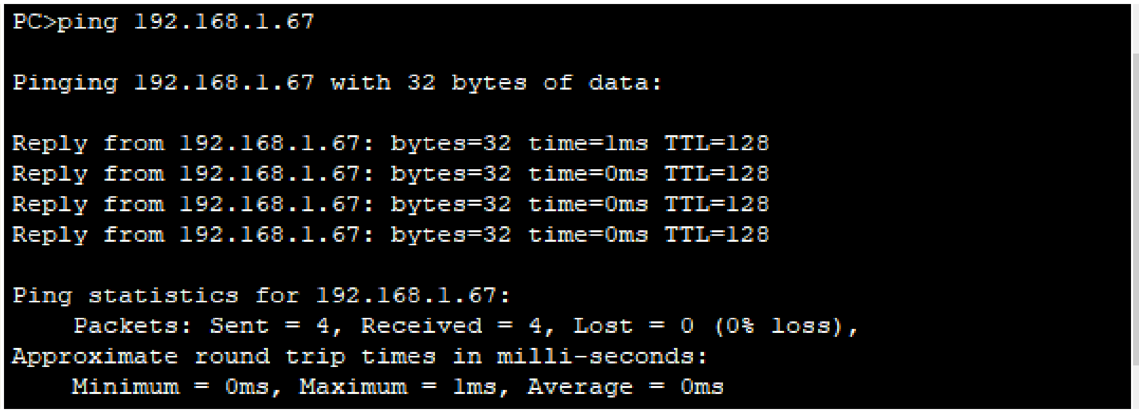
Prueba desde SERVIDOR a PC3 y PC4



```
SERVER>ping 192.168.1.34

Pinging 192.168.1.34 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Request timed out.

Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

SERVER>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.

Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ilustración 30: Prueba desde SERVIDOR a PC3 y PC4

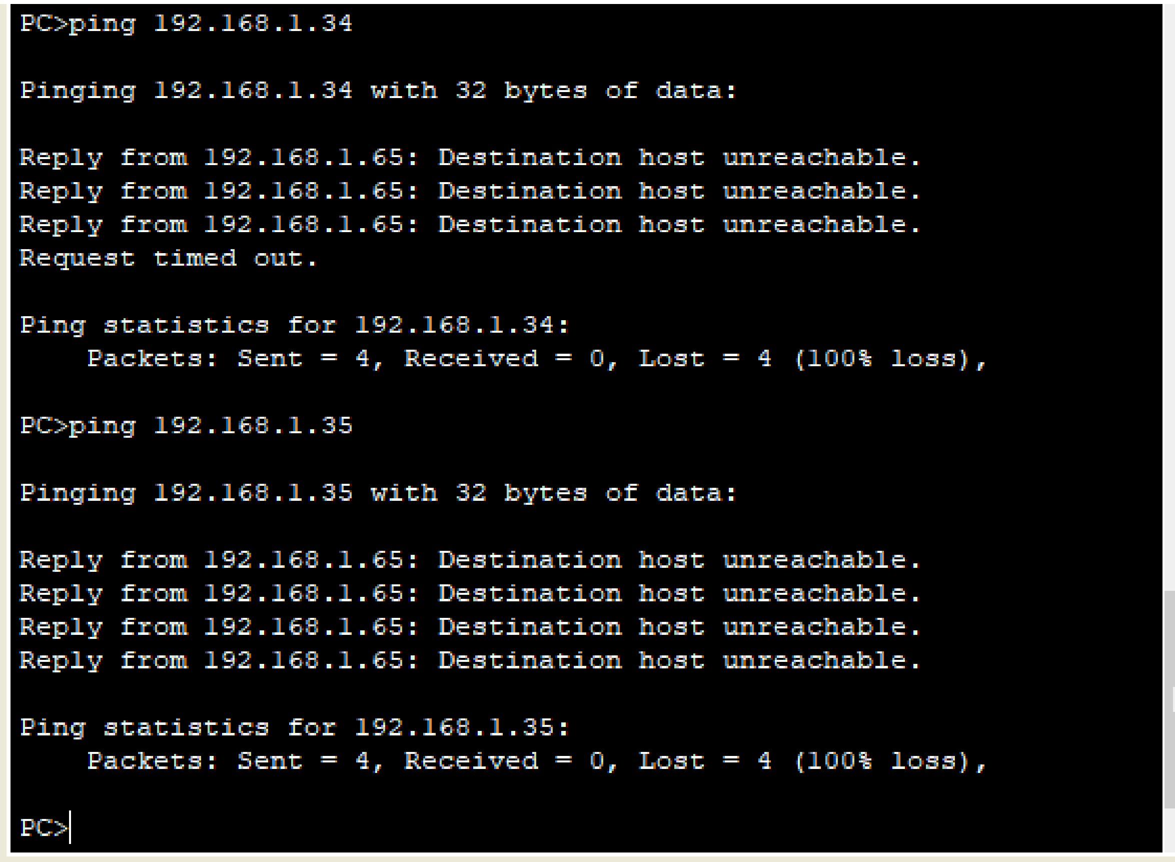
Prueba desde PC1 a PC2



```
PC>ping 192.168.1.67

Pinging 192.168.1.67 with 32 bytes of data:

Reply from 192.168.1.67: bytes=32 time=1ms TTL=128
Reply from 192.168.1.67: bytes=32 time=0ms TTL=128
Reply from 192.168.1.67: bytes=32 time=0ms TTL=128
Reply from 192.168.1.67: bytes=32 time=0ms TTL=128

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

Ilustración 31: Prueba desde PC1 a PC2

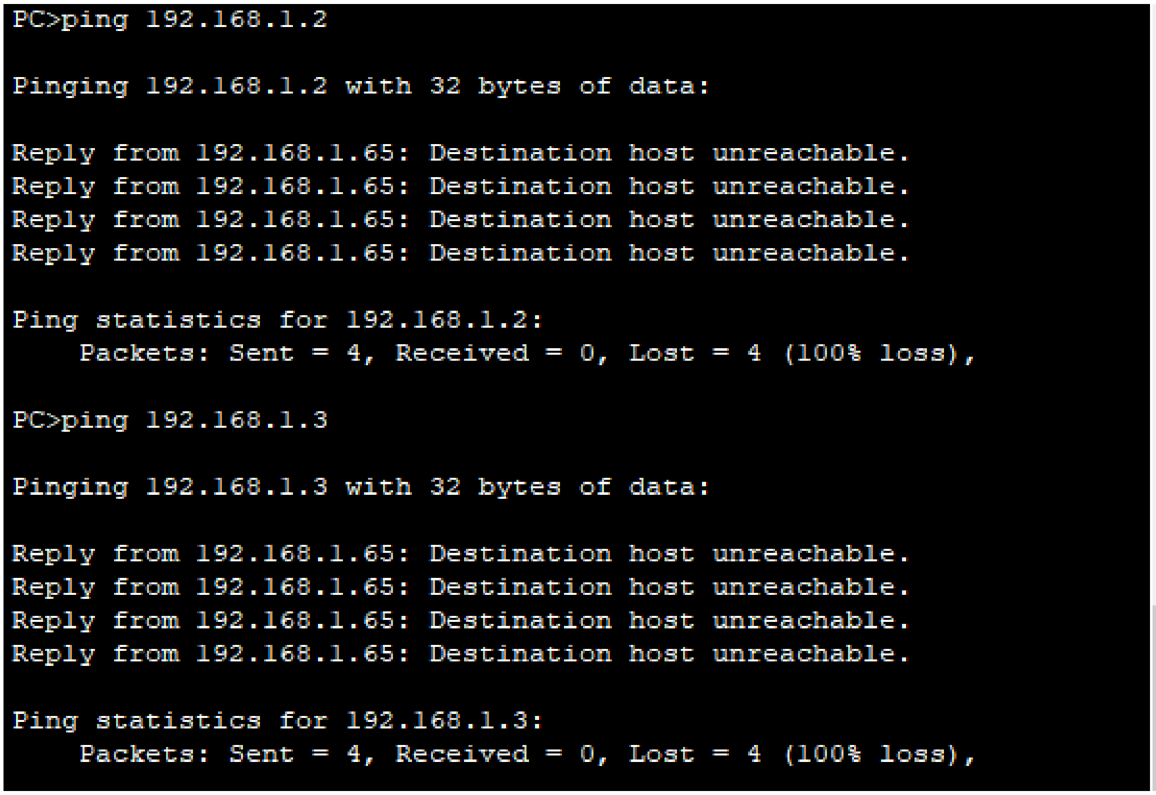
Prueba desde PC1 a PC3 Y PC4



```
PC>ping 192.168.1.34

Pinging 192.168.1.34 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.
Request timed out.

Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.1.35

Pinging 192.168.1.35 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.
Reply from 192.168.1.65: Destination host unreachable.

Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Ilustración 32: Prueba desde PC1 a PC3 Y PC4

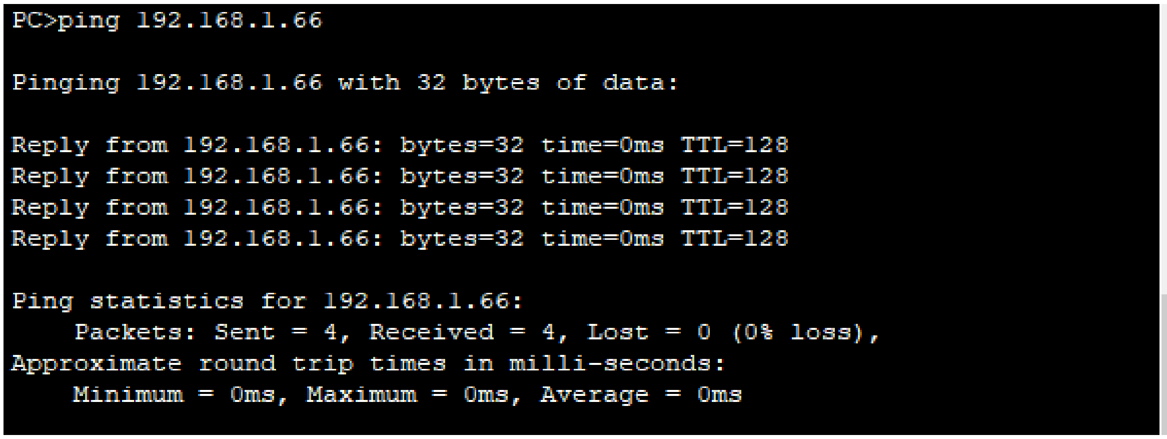
Prueba desde PC1 a WS 1 y SERVIDOR



```
PC>ping 192.168.1.2

Pinging 192.168.1.2 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.
Reply from 192.168.1.65: Destination host unreachable.

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

PC>ping 192.168.1.3

Pinging 192.168.1.3 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.
Reply from 192.168.1.65: Destination host unreachable.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ilustración 33: Prueba desde PC1 a WS 1 y SERVIDOR

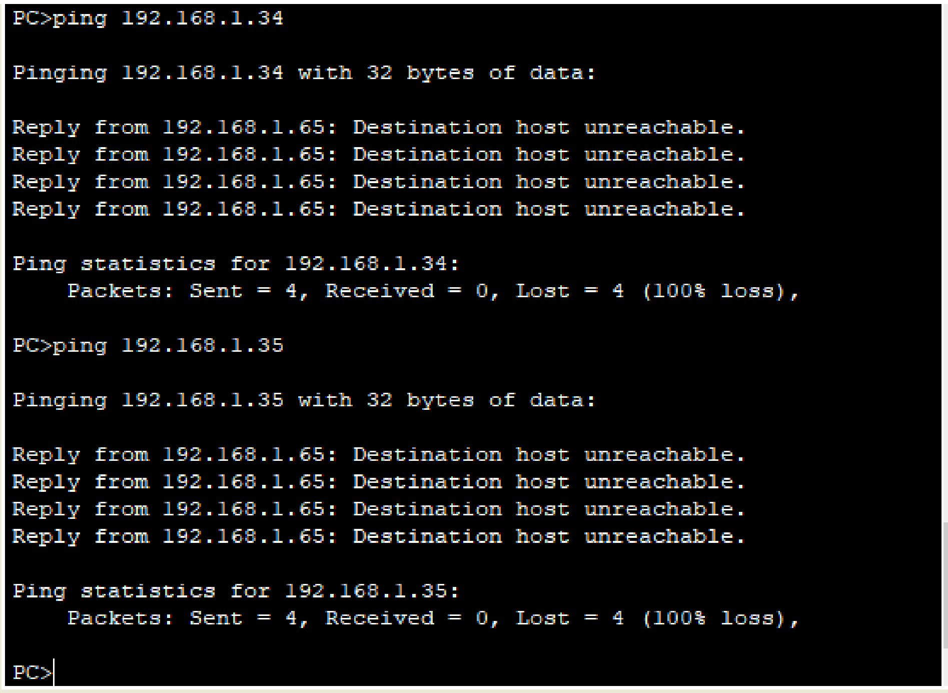
Prueba desde PC2 a PC1



```
PC>ping 192.168.1.66

Pinging 192.168.1.66 with 32 bytes of data:

Reply from 192.168.1.66: bytes=32 time=0ms TTL=128
Reply from 192.168.1.66: bytes=32 time=0ms TTL=128
Reply from 192.168.1.66: bytes=32 time=0ms TTL=128
Reply from 192.168.1.66: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ilustración 34: Prueba desde PC2 a PC1

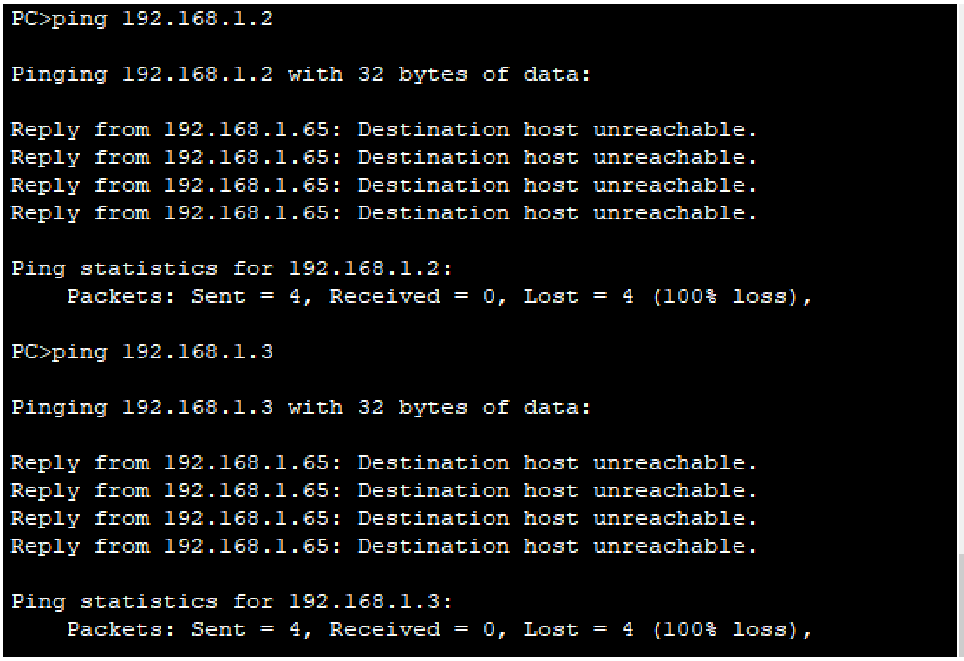
Prueba desde PC2 a PC3 y PC4



```
PC>ping 192.168.1.34

Pinging 192.168.1.34 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.
Reply from 192.168.1.65: Destination host unreachable.

Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.1.35

Pinging 192.168.1.35 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.
Reply from 192.168.1.65: Destination host unreachable.

Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Ilustración 35: Prueba desde PC2 a PC3 y PC4

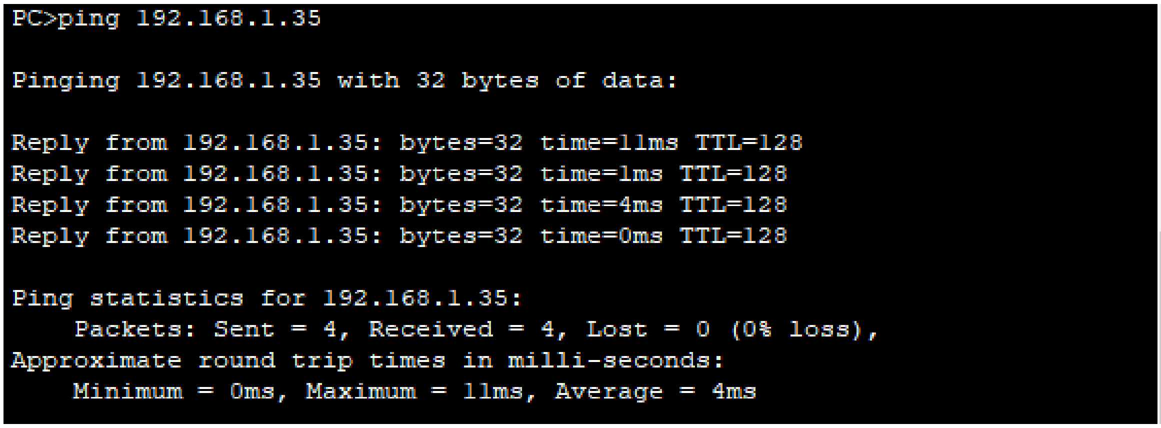
Prueba desde PC2 a WS 1 y SERVIDOR



```
PC>ping 192.168.1.2

Pinging 192.168.1.2 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.
Reply from 192.168.1.65: Destination host unreachable.

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

PC>ping 192.168.1.3

Pinging 192.168.1.3 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.
Reply from 192.168.1.65: Destination host unreachable.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ilustración 36: Prueba desde PC2 a WS 1 y SERVIDOR

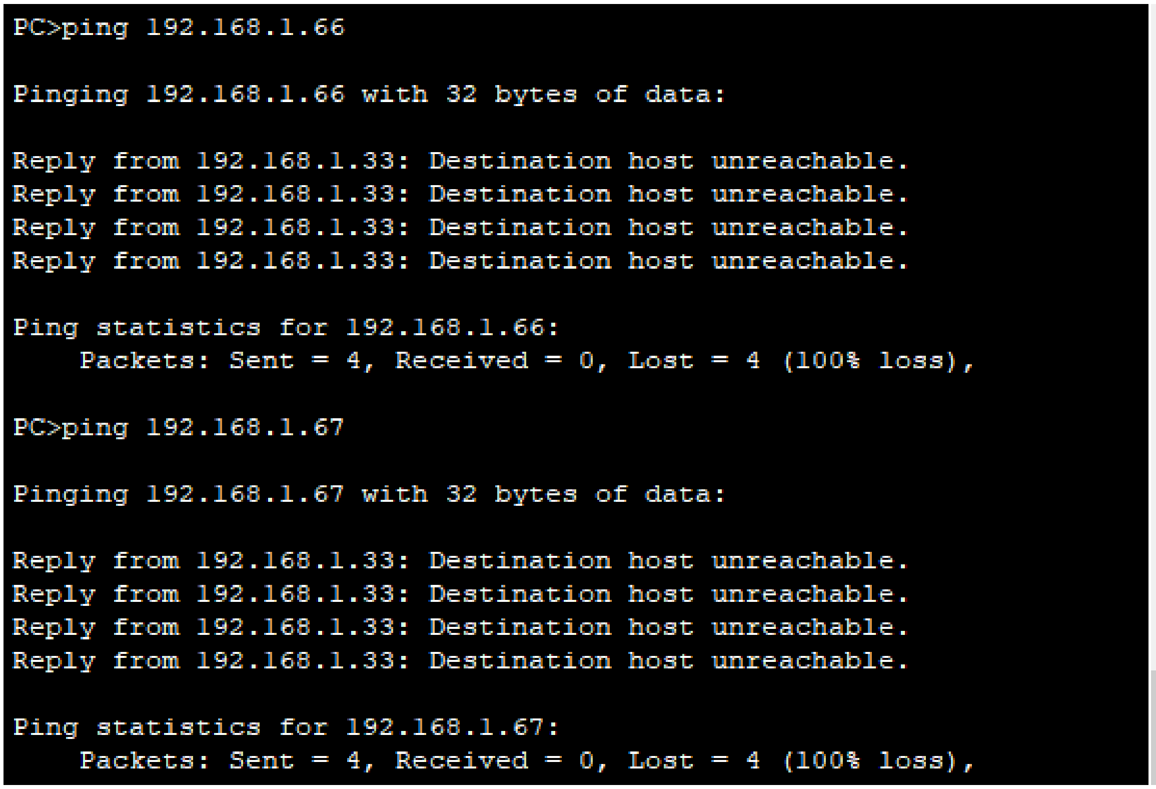
Prueba desde PC3 a PC4



```
PC>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168.1.35: bytes=32 time=11ms TTL=128
Reply from 192.168.1.35: bytes=32 time=1ms TTL=128
Reply from 192.168.1.35: bytes=32 time=4ms TTL=128
Reply from 192.168.1.35: bytes=32 time=0ms TTL=128

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

Ilustración 37: Prueba desde PC3 a PC4

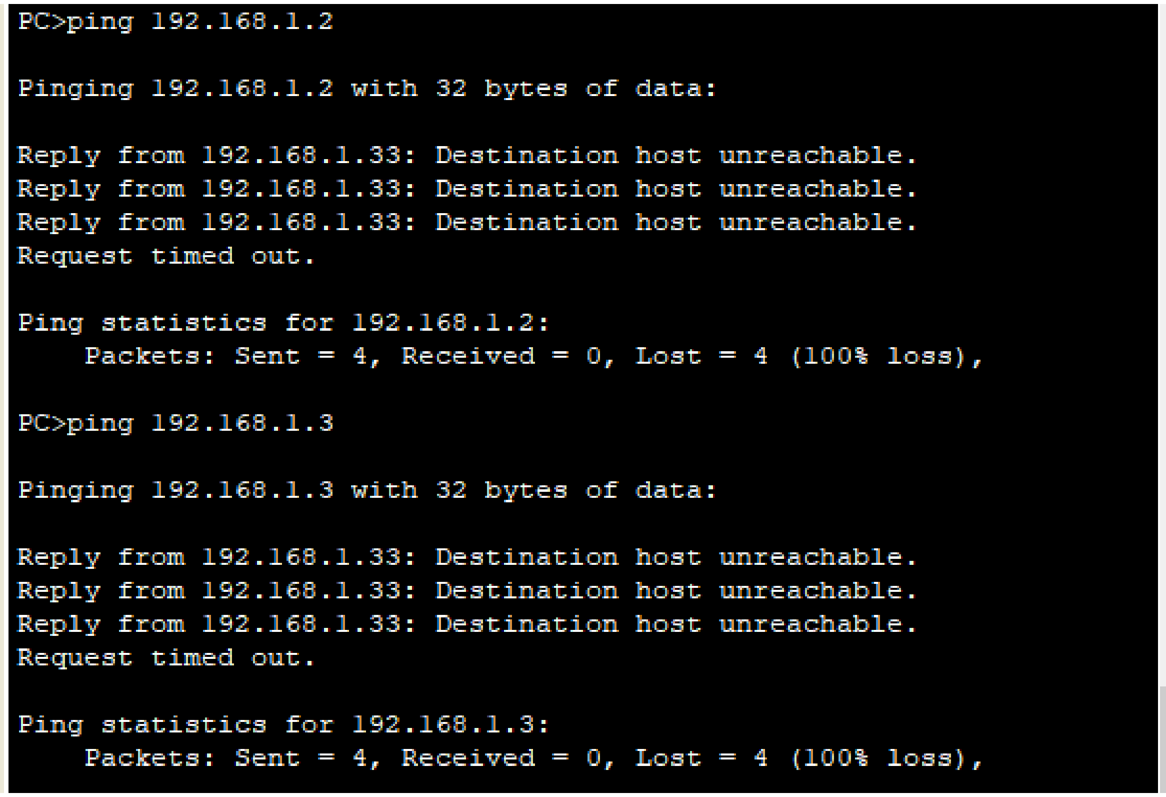
Prueba desde PC3 a PC1 y PC2



```
PC>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),

PC>ping 192.168.1.67

Pinging 192.168.1.67 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 192.168.1.67:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ilustración 38: Prueba desde PC3 a PC4

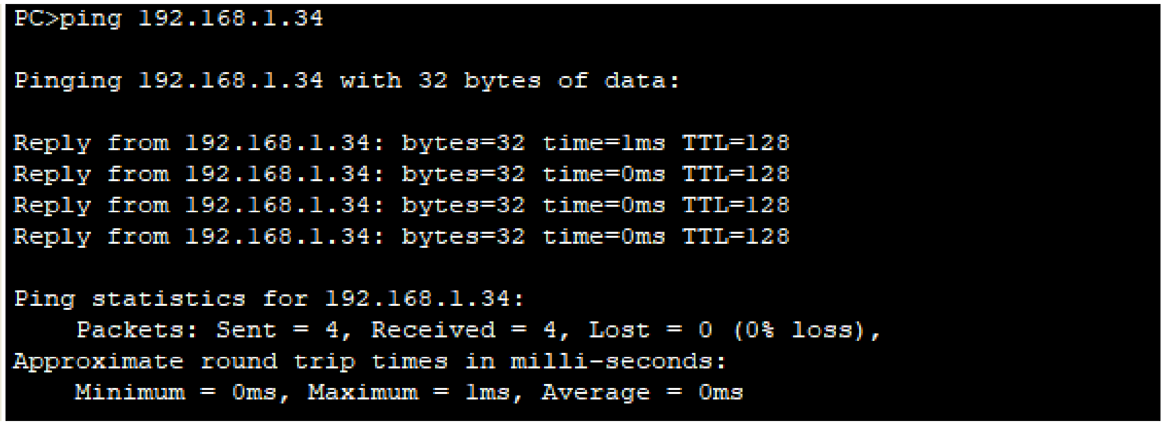
Prueba desde PC3 a SW 1 y SERVIDOR



```
PC>ping 192.168.1.2

Pinging 192.168.1.2 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.
Request timed out.

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

PC>ping 192.168.1.3

Pinging 192.168.1.3 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.
Request timed out.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ilustración 39: Prueba desde PC3 a SW 1 y SERVIDOR

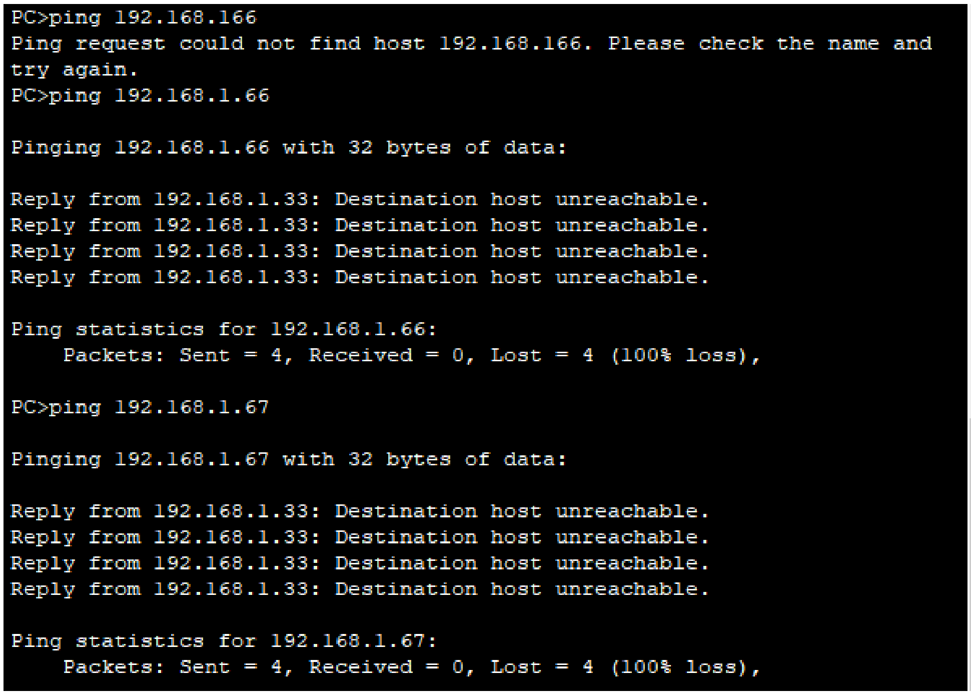
Prueba desde PC4 a PC3



```
PC>ping 192.168.1.34

Pinging 192.168.1.34 with 32 bytes of data:

Reply from 192.168.1.34: bytes=32 time=1ms TTL=128
Reply from 192.168.1.34: bytes=32 time=0ms TTL=128
Reply from 192.168.1.34: bytes=32 time=0ms TTL=128
Reply from 192.168.1.34: bytes=32 time=0ms 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 = 1ms, Average = 0ms
```

Ilustración 40: Prueba desde PC4 a PC3

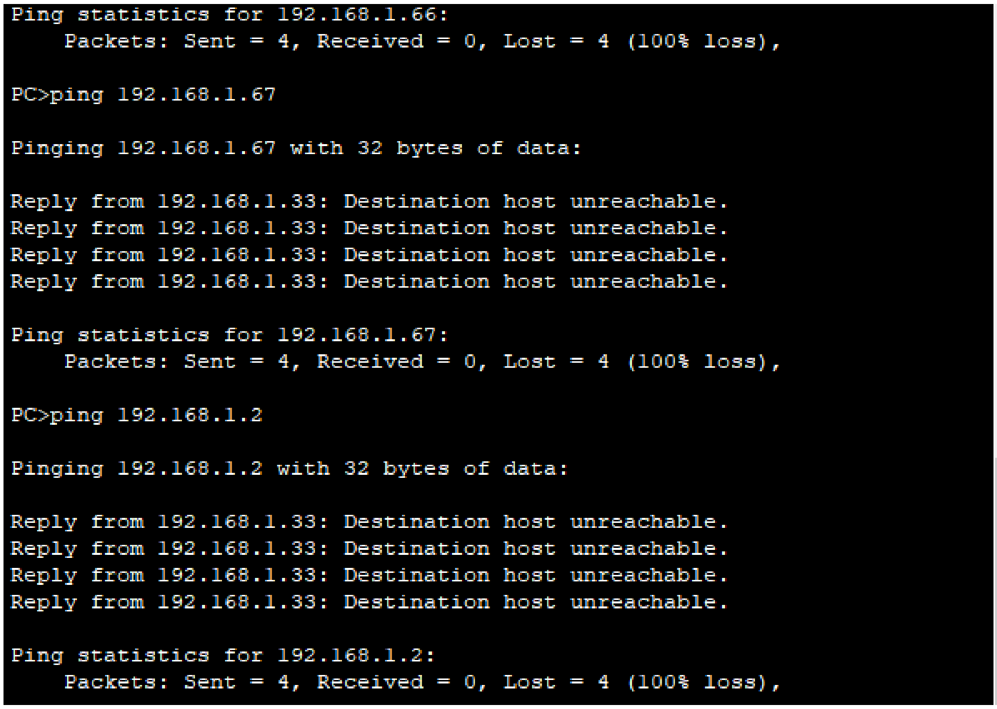
Prueba desde PC4 a PC1 y PC2



```
PC>ping 192.168.166
Ping request could not find host 192.168.166. Please check the name and
try again.
PC>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),

PC>ping 192.168.1.67

Pinging 192.168.1.67 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 192.168.1.67:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ilustración 41: Prueba desde PC4 a PC1 y PC2

Prueba desde PC4 a SW 1 y SERVIDOR



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

PC>ping 192.168.1.67

Pinging 192.168.1.67 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 192.168.1.67:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.168.1.2

Pinging 192.168.1.2 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 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ilustración 42: Prueba desde PC4 a SW 1 y SERVIDOR

2.5. Parte 3: Configuración de Enrutamiento.

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

Enrutamiento EIGRP al Router BOGOTA

```
BOGOTA>enable
BOGOTA#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#router eigrp 200
BOGOTA(config-router)#no auto-summary
BOGOTA(config-router)#network 192.168.1.96
BOGOTA(config-router)#network 192.168.1.0
BOGOTA(config-router)#network 192.168.1.128
BOGOTA(config-router)#end
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console
```

Enrutamiento EIGRP al Router MEDELLIN

```
MEDELLIN> enable
MEDELLIN#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
MEDELLIN(config)#router eigrp 200
MEDELLIN(config-router)#no auto-summary
MEDELLIN(config-router)#network 192.168.1.32
MEDELLIN(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.98 (Serial0/0/0) is up:
new adjacency
```

```
MEDELLIN(config-router)#network 192.168.1.32
MEDELLIN(config-router)#network 192.168.1.96
MEDELLIN(config-router)#end
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
```

Enrutamiento EIGRP al Router CALI

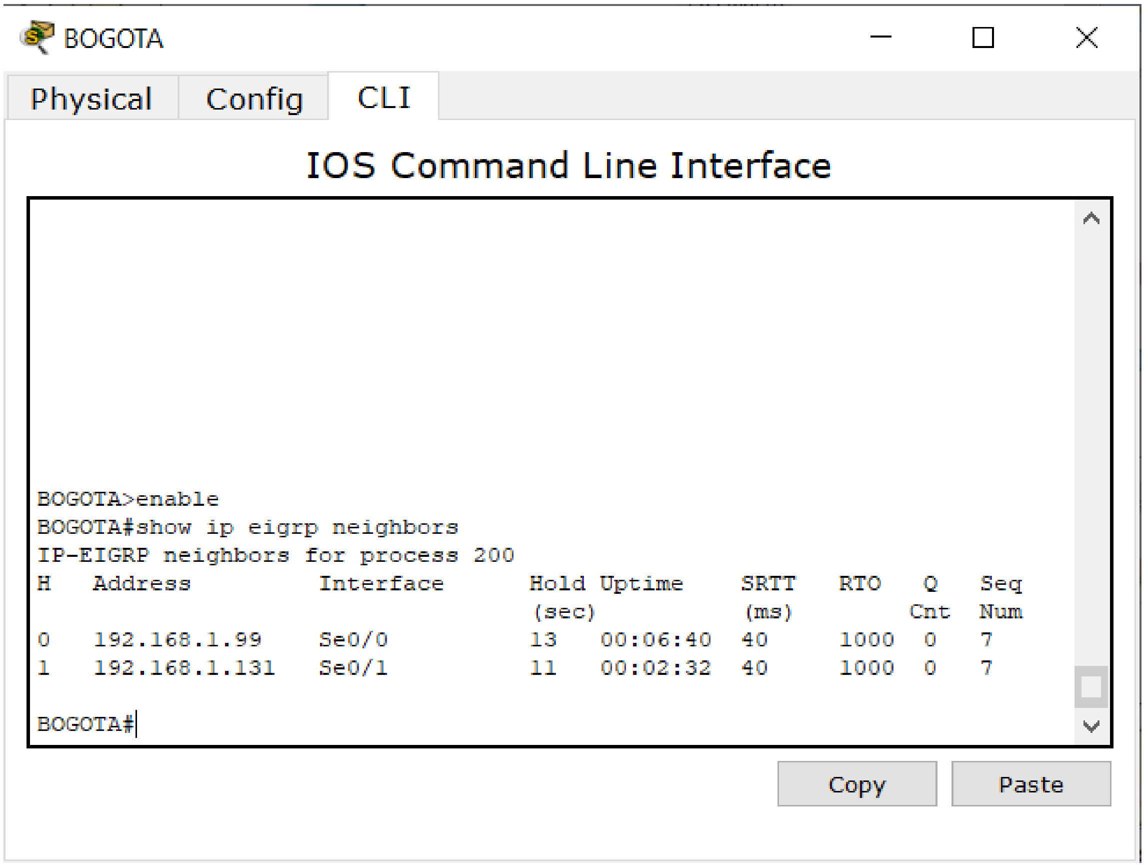
```
CALI>enable
CALI#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CALI(config)#router eigrp 200
CALI(config-router)#no auto-summary
CALI(config-router)#network 192.168.1.128
CALI(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.130 (Serial0/0) is up: new adjacency
CALI(config-router)#network 192.168.1.128
CALI(config-router)#network 192.168.1.64
CALI(config-router)#end
CALI#
%SYS-5-CONFIG_I: Configured from console by console
```

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

Vecindad con el Router BOGOTA

BOGOTA>enable

BOGOTA#show ip eigrp neighbors



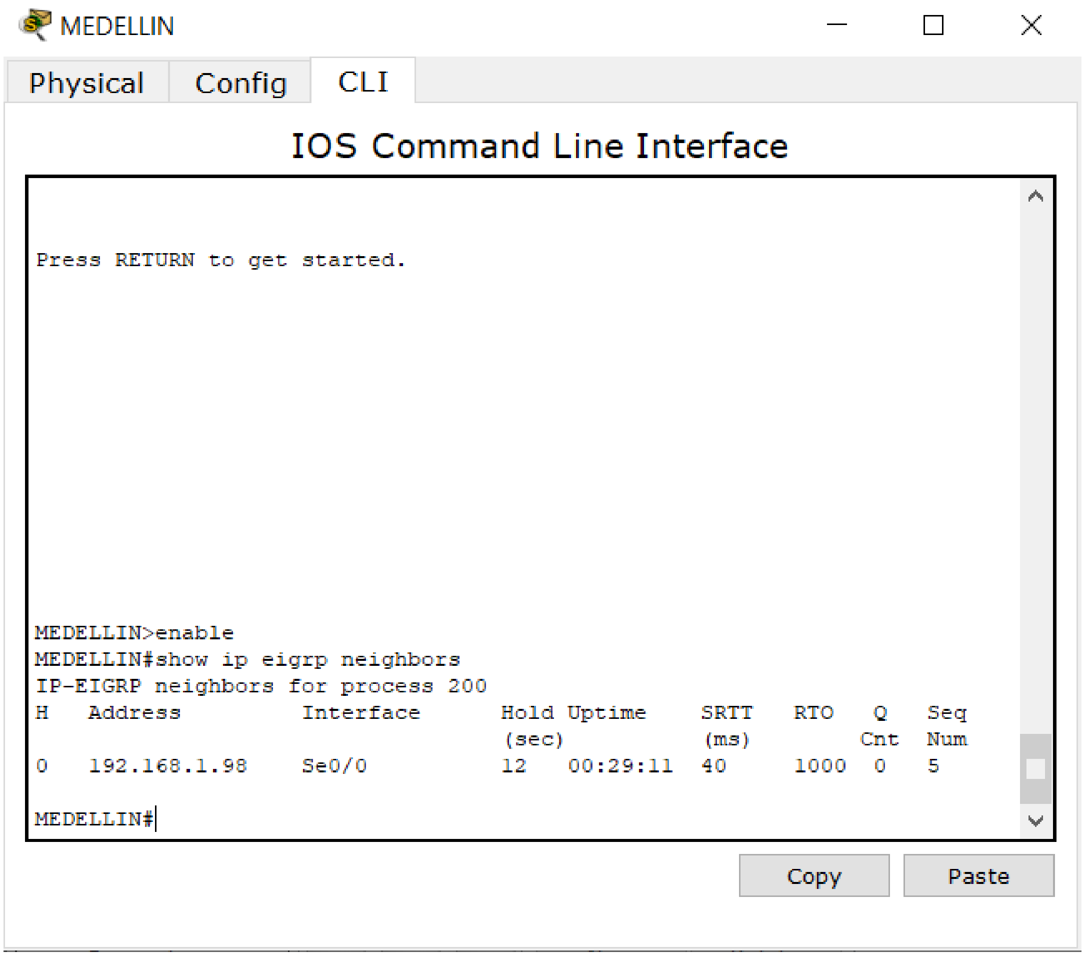
```
BOGOTA>enable
BOGOTA#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address         Interface      Hold Uptime    SRTT   RTO   Q   Seq
                                   (sec)          (ms)        Cnt  Num
0   192.168.1.99    Se0/0          13   00:06:40  40     1000  0   7
1   192.168.1.131   Se0/1          11   00:02:32  40     1000  0   7

BOGOTA#
```

Ilustración 43: Vecindad con el Router BOGOTA

Vecindad con el Router MEDELLIN

MEDELLIN>enable

MEDELLIN#show ip eigrp neighbors



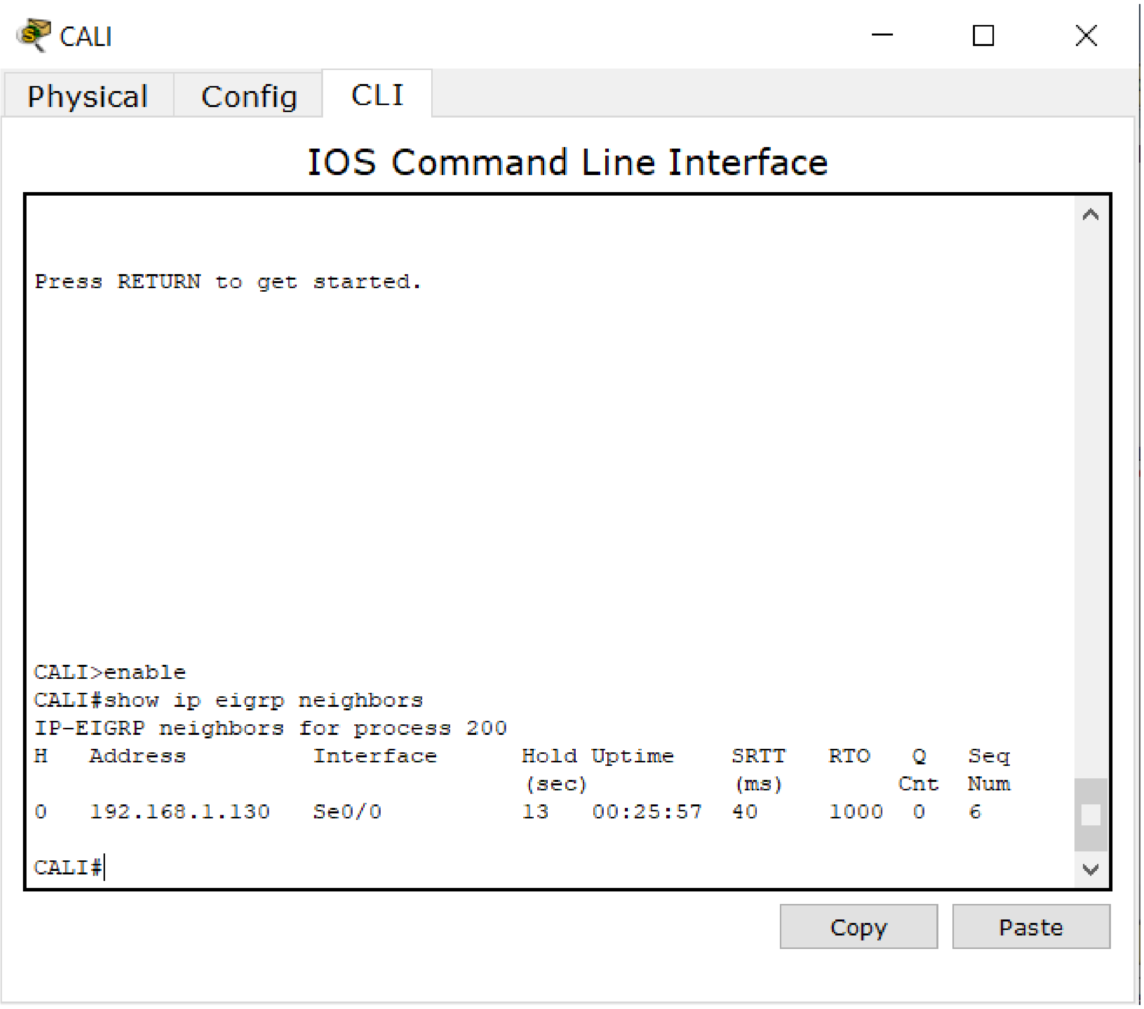
```
Press RETURN to get started.









MEDELLIN>enable
MEDELLIN#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address         Interface      Hold Uptime    SRTT   RTO   Q   Seq
                                   (sec)          (ms)        Cnt  Num
0   192.168.1.98    Se0/0          12   00:29:11  40     1000  0   5

MEDELLIN#
```

Ilustración 44: Vecindad con el Router MEDELLIN

Vecindad con el Router CALI

CALI>enable

CALI#show ip eigrp neighbors



```
Press RETURN to get started.









CALI>enable
CALI#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H   Address         Interface      Hold Uptime     SRTT    RTO    Q    Seq
                                   (sec)           (ms)          Cnt   Num
0   192.168.1.130   Se0/0          13    00:25:57  40      1000   0    6

CALI#
```

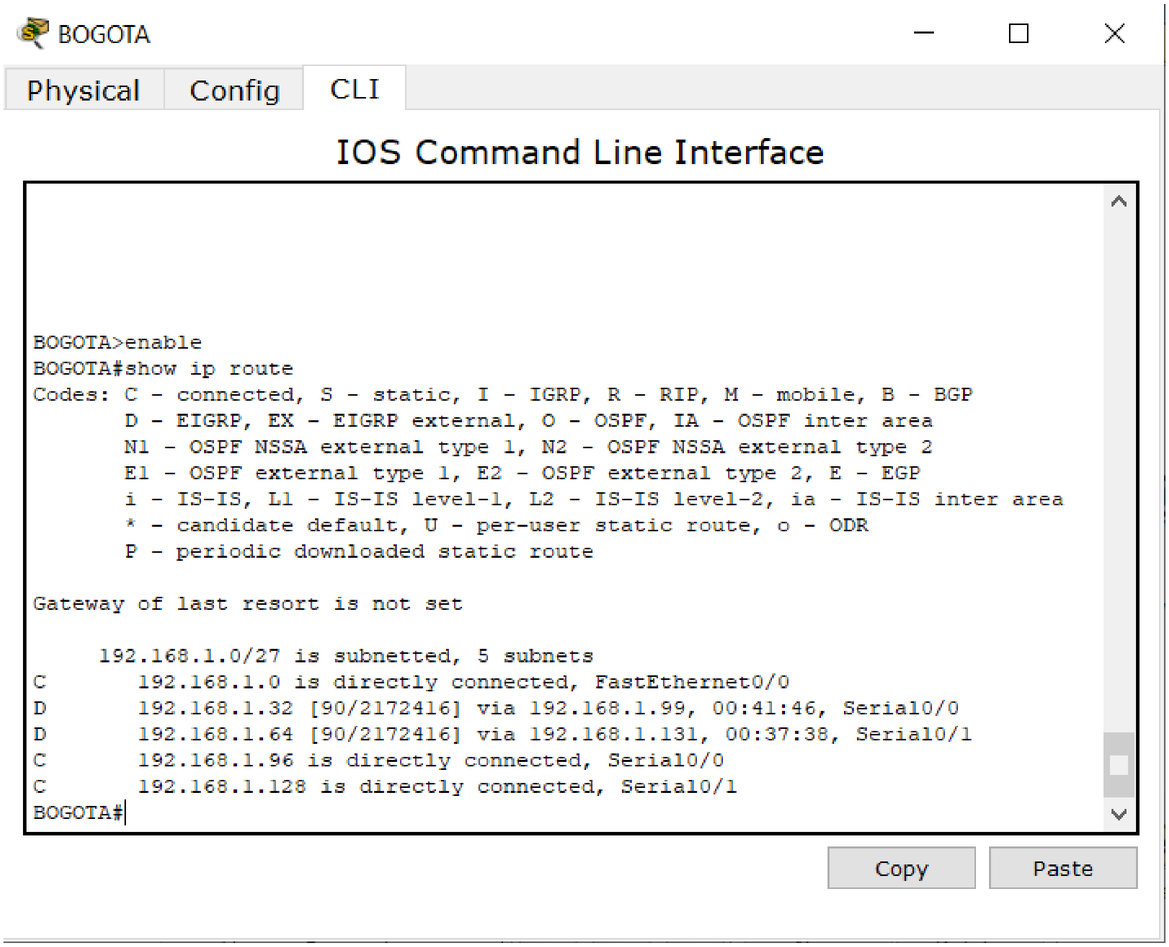
Ilustración 45: Vecindad con el Router CALI

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

Tabla de enrutamiento Router BOGOTA

BOGOTA>enable

BOGOTA#show ip route



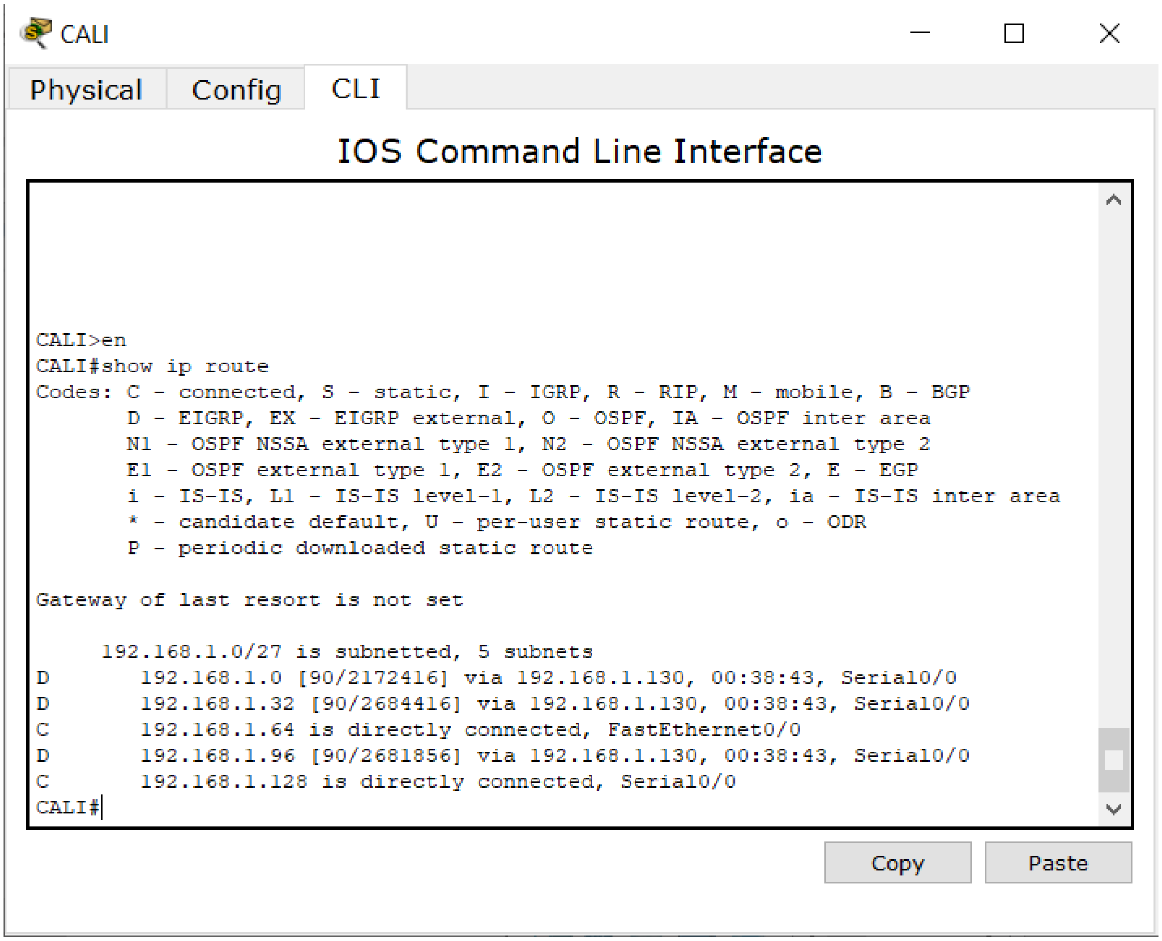
```
BOGOTA>enable
BOGOTA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external 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, 00:41:46, Serial0/0
D       192.168.1.64 [90/2172416] via 192.168.1.131, 00:37:38, Serial0/1
C       192.168.1.96 is directly connected, Serial0/0
C       192.168.1.128 is directly connected, Serial0/1
BOGOTA#
```

Ilustración 46: Tabla de enrutamiento Router BOGOTA

Tabla de enrutamiento Router CALI

CALI>en

CALI#show ip route



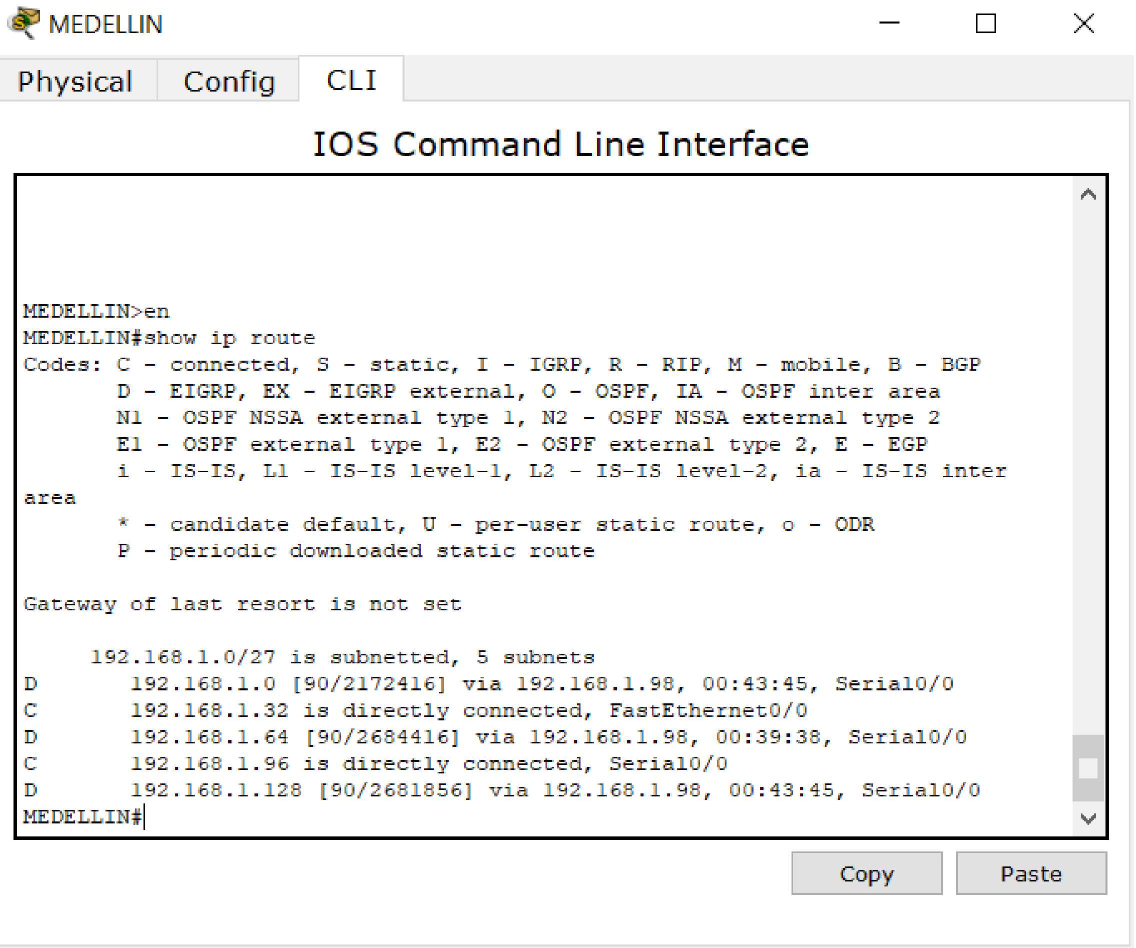
```
CALI>en
CALI#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 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, 00:38:43, Serial0/0
D       192.168.1.32 [90/2684416] via 192.168.1.130, 00:38:43, Serial0/0
C       192.168.1.64 is directly connected, FastEthernet0/0
D       192.168.1.96 [90/2681856] via 192.168.1.130, 00:38:43, Serial0/0
C       192.168.1.128 is directly connected, Serial0/0
CALI#
```

Ilustración 47: Tabla de enrutamiento Router CALI

Tabla de enrutamiento Router MEDELLIN

MEDELLIN>en

MEDELLIN#show ip route

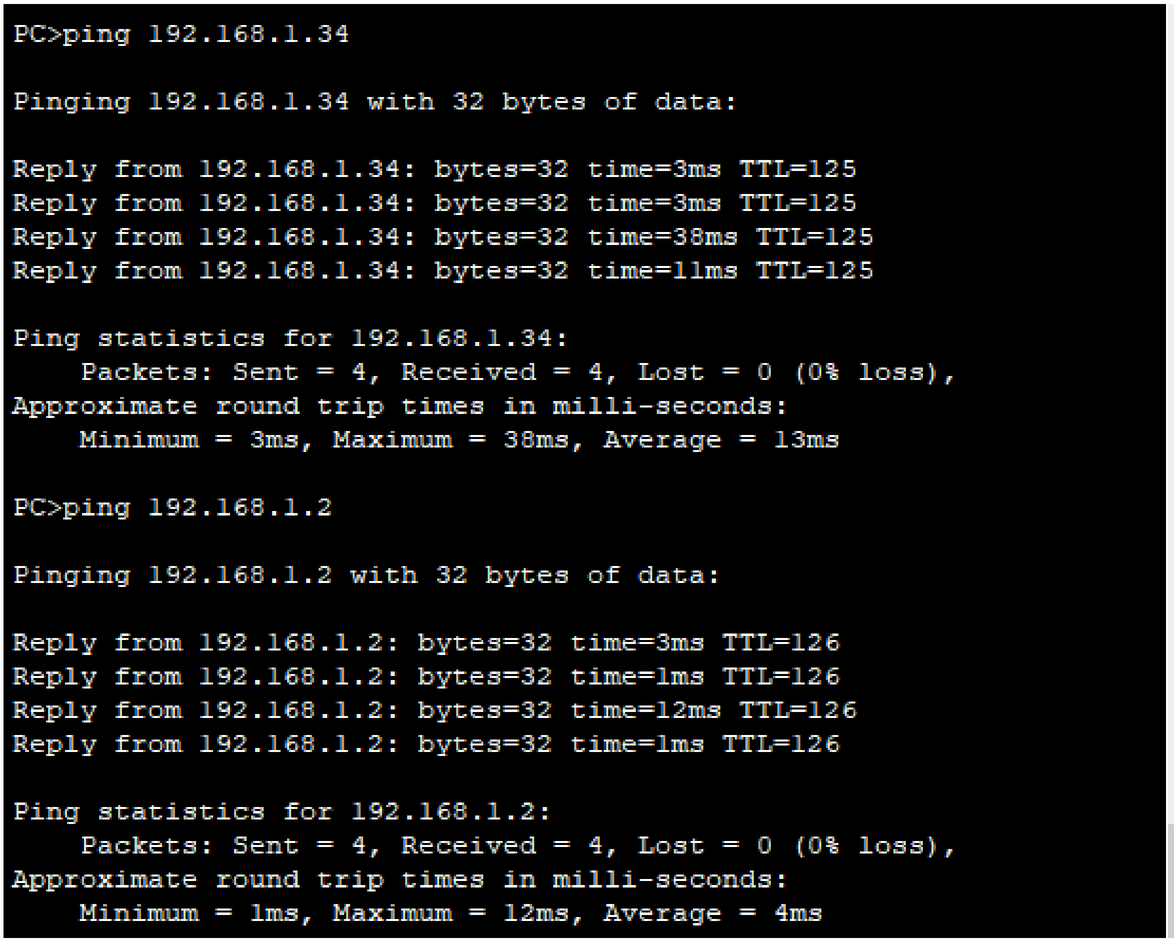


```
MEDELLIN>en
MEDELLIN#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external 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, 00:43:45, Serial0/0
C       192.168.1.32 is directly connected, FastEthernet0/0
D       192.168.1.64 [90/2684416] via 192.168.1.98, 00:39:38, Serial0/0
C       192.168.1.96 is directly connected, Serial0/0
D       192.168.1.128 [90/2681856] via 192.168.1.98, 00:43:45, Serial0/0
MEDELLIN#
```

Ilustración 48: Tabla de enrutamiento Router MEDELLIN

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.

Prueba desde PC1 hasta PC3 y desde PC1 hasta SERVIDOR



```
PC>ping 192.168.1.34

Pinging 192.168.1.34 with 32 bytes of data:

Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=38ms TTL=125
Reply from 192.168.1.34: bytes=32 time=11ms TTL=125

Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 38ms, Average = 13ms

PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=3ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=12ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 12ms, Average = 4ms
```

Ilustración 49: Prueba desde PC1 hasta PC3 y desde PC1 hasta SERVIDOR

2.6. 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.

Habilitar conexión Telnet al Router BOGOTA

```
BOGOTA>en
BOGOTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#line vty 0 4
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#enable secret cisco
BOGOTA(config)#exit
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console
```

Habilitar conexión Telnet al Router MEDELLIN

```
MEDELLIN>en
MEDELLIN#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
MEDELLIN(config)#line vty 0 4
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
MEDELLIN(config)#enable secret cisco
MEDELLIN(config)#exit
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
```

Habilitar conexión Telnet al Router CALI

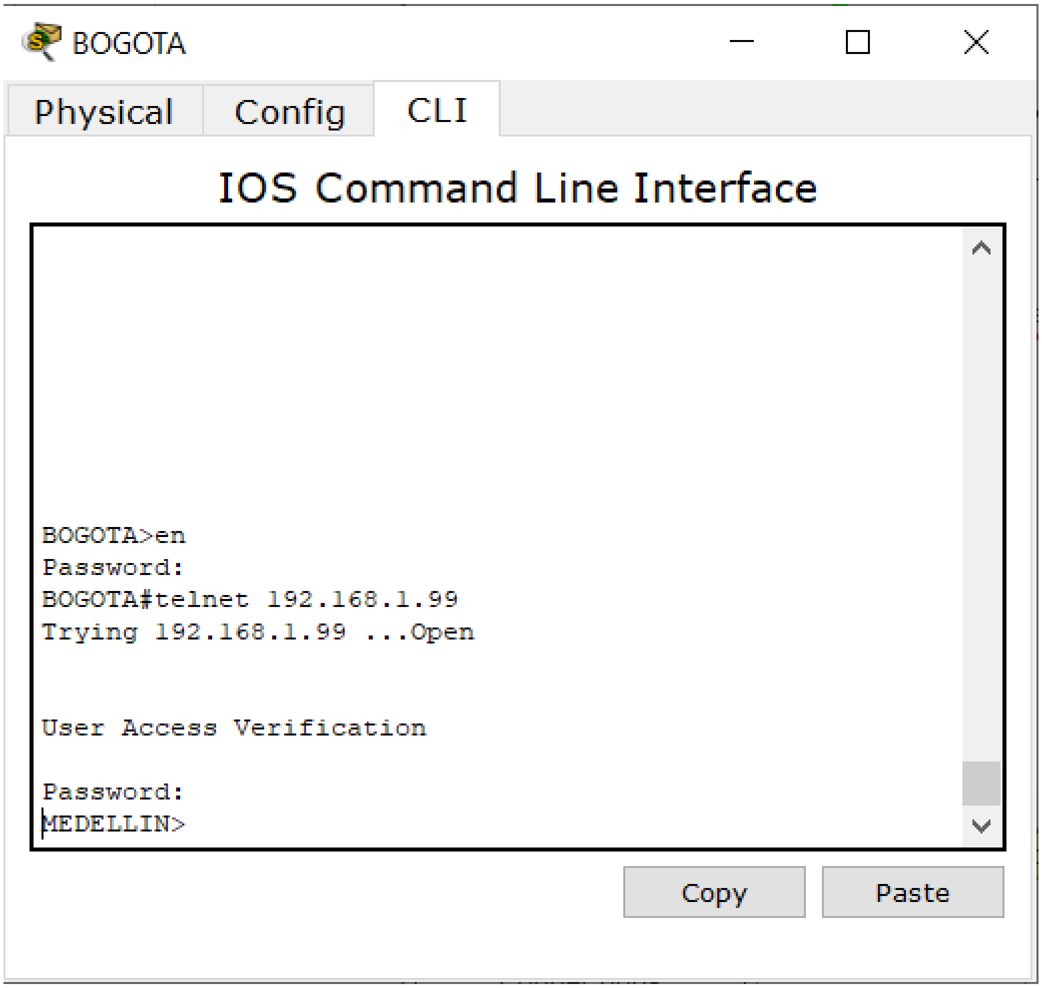
```
CALI>en
CALI#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CALI(config)#line vty 0 4
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#exit
CALI(config)#enable secret cisco
CALI(config)#exit
CALI#
%SYS-5-CONFIG_I: Configured from console by console
```

Telnet desde Router BOGOTA a Router MEDELLIN

BOGOTA>en

Password:

BOGOTA#telnet 192.168.1.99



```
BOGOTA>en
Password:
BOGOTA#telnet 192.168.1.99
Trying 192.168.1.99 ...Open


User Access Verification

Password:
MEDELLIN>
```

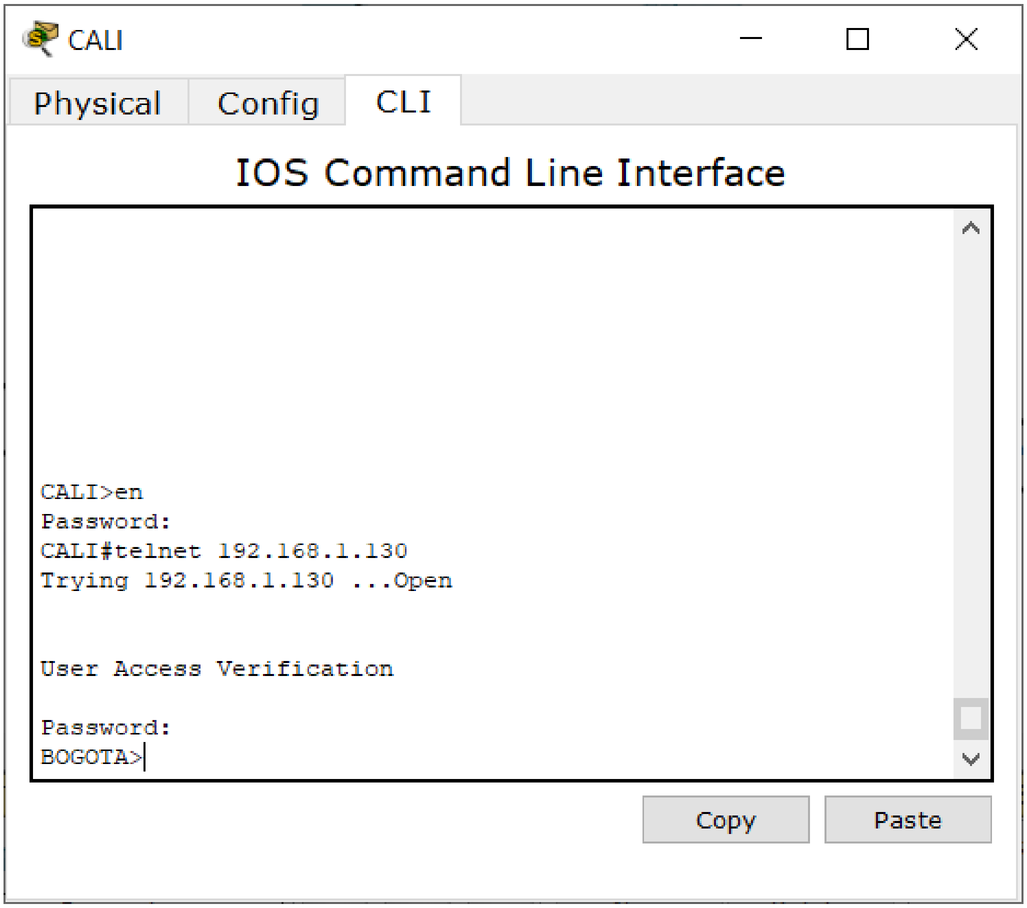
Ilustración 50: Telnet desde Router BOGOTA a Router MEDELLIN

Telnet desde Router CALI a Router BOGOTA

CALI>en

Password:

CALI#telnet 192.168.1.130



```
CALI>en
Password:
CALI#telnet 192.168.1.130
Trying 192.168.1.130 ...Open


User Access Verification

Password:
BOGOTA>
```

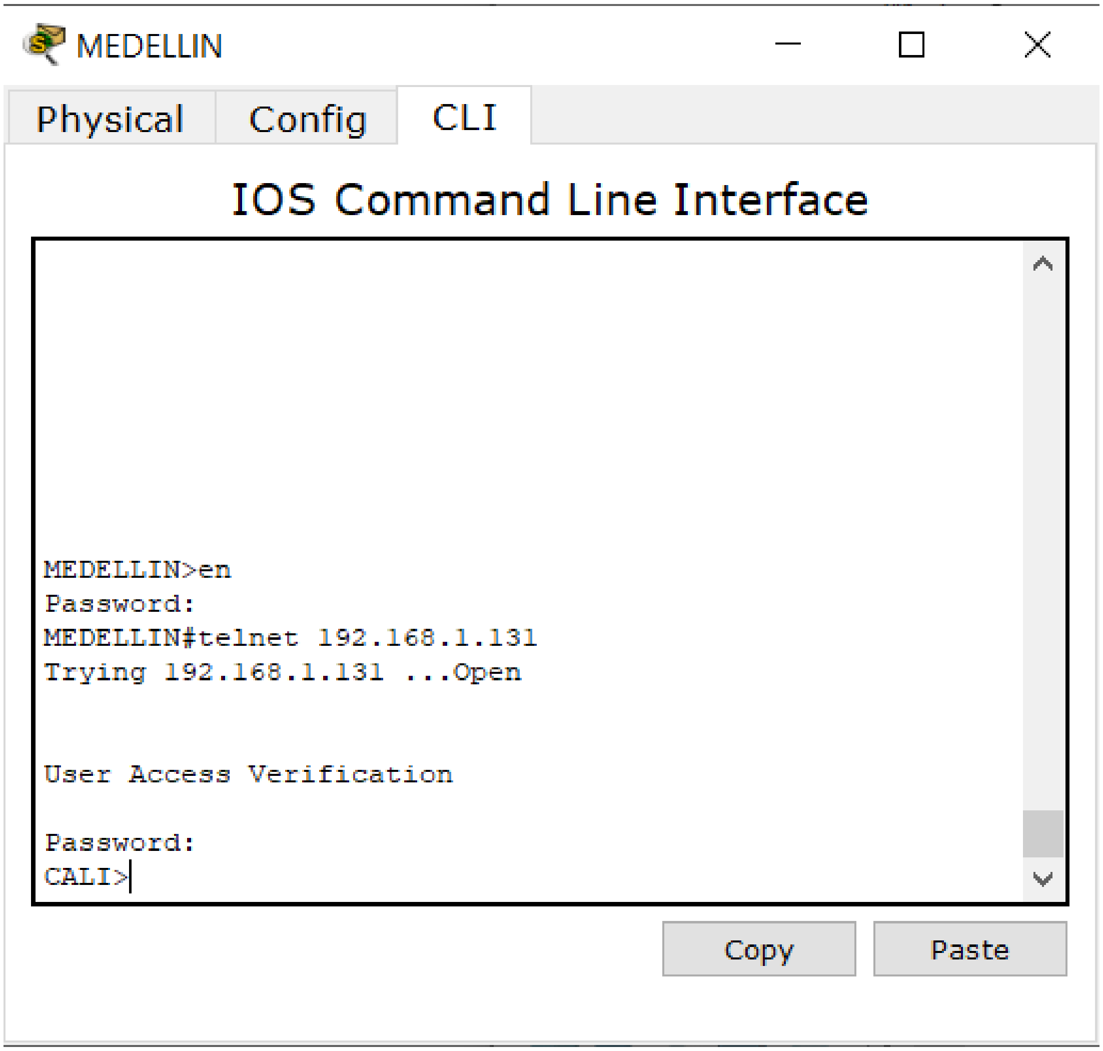
Ilustración 51: Telnet desde Router CALI a Router BOGOTA

Telnet desde Router MEDELLIN a Router CALI

MEDELLIN>en

Password:

MEDELLIN#telnet 192.168.1.131



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


User Access Verification

Password:
CALI>
```

Ilustración 52: Telnet desde Router MEDELLIN a Router CALI

a. 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.

Configuración Router BOGOTA

```
BOGOTA>enable

Password:

BOGOTA#config terminal

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

BOGOTA(config)#ip access-list extended ServerPT

BOGOTA(config-ext-nacl)#permit ip 192.168.1.2 0.0.0.0 0.0.0.0 255.255.255.255

BOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.99 0.0.0.0

BOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.1 0.0.0.0

BOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.131 0.0.0.0

BOGOTA(config-ext-nacl)# exit

BOGOTA(config)#interface fa0/0

BOGOTA(config-if)#ip access-group ServerPT in

BOGOTA(config-if)#end

BOGOTA#

%SYS-5-CONFIG_I: Configured from console by console
```

Configuración Router MEDELLIN

```
MEDELLIN>enable

Password:

MEDELLIN#configure terminal

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

MEDELLIN(config)#ip access-list extended ServerPT

MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.2 0.0.0.0
MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.33 0.0.0.0
MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.98 0.0.0.0
MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.131 0.0.0.0
MEDELLIN(config-ext-nacl)#exit
MEDELLIN(config)#interface fa0/0
MEDELLIN(config-if)#ip access-group ServerPT in
MEDELLIN(config-if)#end
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
```

Configuración Router CALI

```
CALI>enable
Password:
CALI#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#ip access-list extended ServerPT
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.2 0.0.0.0
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.99 0.0.0.0
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.1 0.0.0.0
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.65 0.0.0.0
CALI(config-ext-nacl)#exit
CALI(config)#int fa0/0
CALI(config-if)#ip access-group ServerPT in
CALI(config-if)#end
CALI#
%SYS-5-CONFIG_I: Configured from console by console
```

b. 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.

Configuración Router MEDELLIN

```
MEDELLIN>enable
Password:
MEDELLIN#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#ip access-list extended ServerPT
MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.2 0.0.0.0
MEDELLIN(config-ext-nacl)#exit
MEDELLIN(config)#int f0/0
MEDELLIN(config-if)#ip access-group ServerPT in
MEDELLIN(config-if)#end
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
```

Configuración Router CALI

```
CALI>enable
Password:
CALI#config t
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#ip access-list extended ServerPT
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.2 0.0.0.0
CALI(config-ext-nacl)#exit
CALI(config)#int f0/0
```

CALI(config-if)#ip access-group ServerPT in

CALI(config-if)#end

CALI#

%SYS-5-CONFIG_I: Configured from console by console

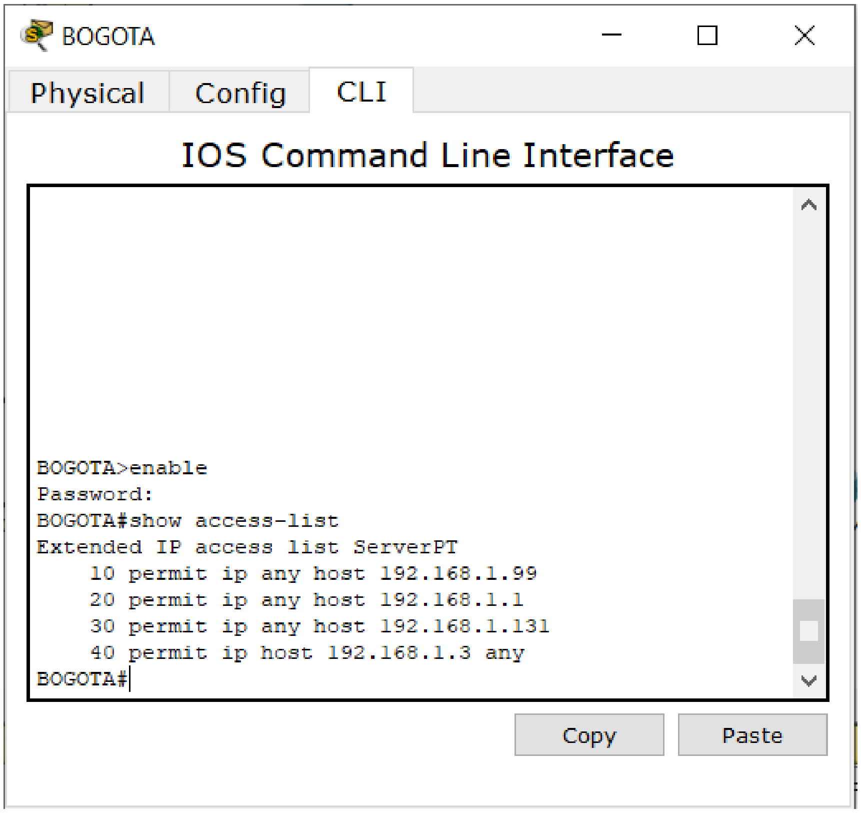
2.7. Parte 5: Comprobación de la red instalada.

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

Listas de Acceso en Router BOGOTA

BOGOTA>enable
Password:

BOGOTA#show access-list



```
BOGOTA>enable
Password:
BOGOTA#show access-list
Extended IP access list ServerPT
    10 permit ip any host 192.168.1.99
    20 permit ip any host 192.168.1.1
    30 permit ip any host 192.168.1.131
    40 permit ip host 192.168.1.3 any
BOGOTA#
```

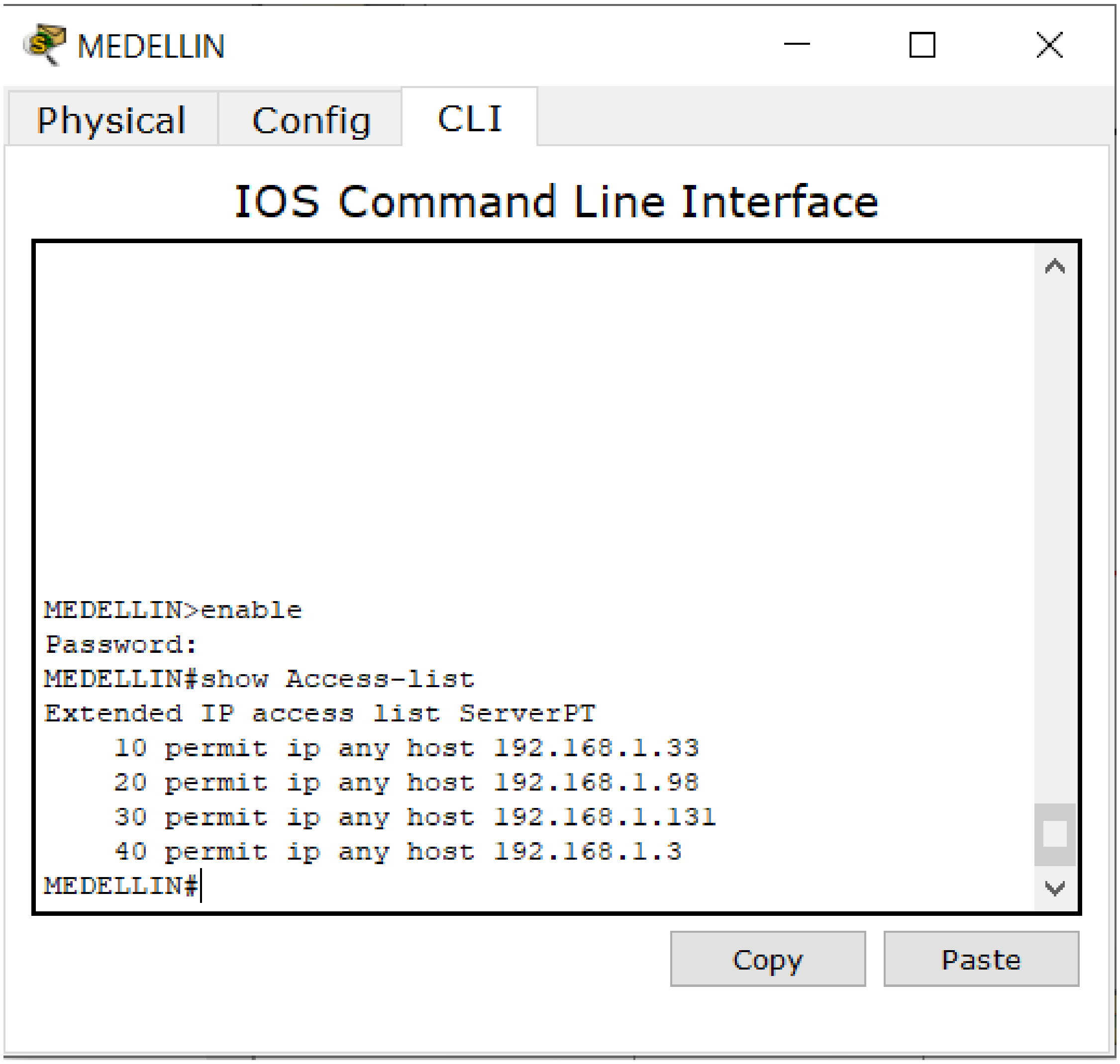
Ilustración 53: Listas de Acceso en Router BOGOTA

Listas de Acceso en Router MEDELLIN

MEDELLIN>enable

Password:

MEDELLIN#show Access-list



```
MEDELLIN>enable
Password:
MEDELLIN#show Access-list
Extended IP access list ServerPT
    10 permit ip any host 192.168.1.33
    20 permit ip any host 192.168.1.98
    30 permit ip any host 192.168.1.131
    40 permit ip any host 192.168.1.3
MEDELLIN#
```

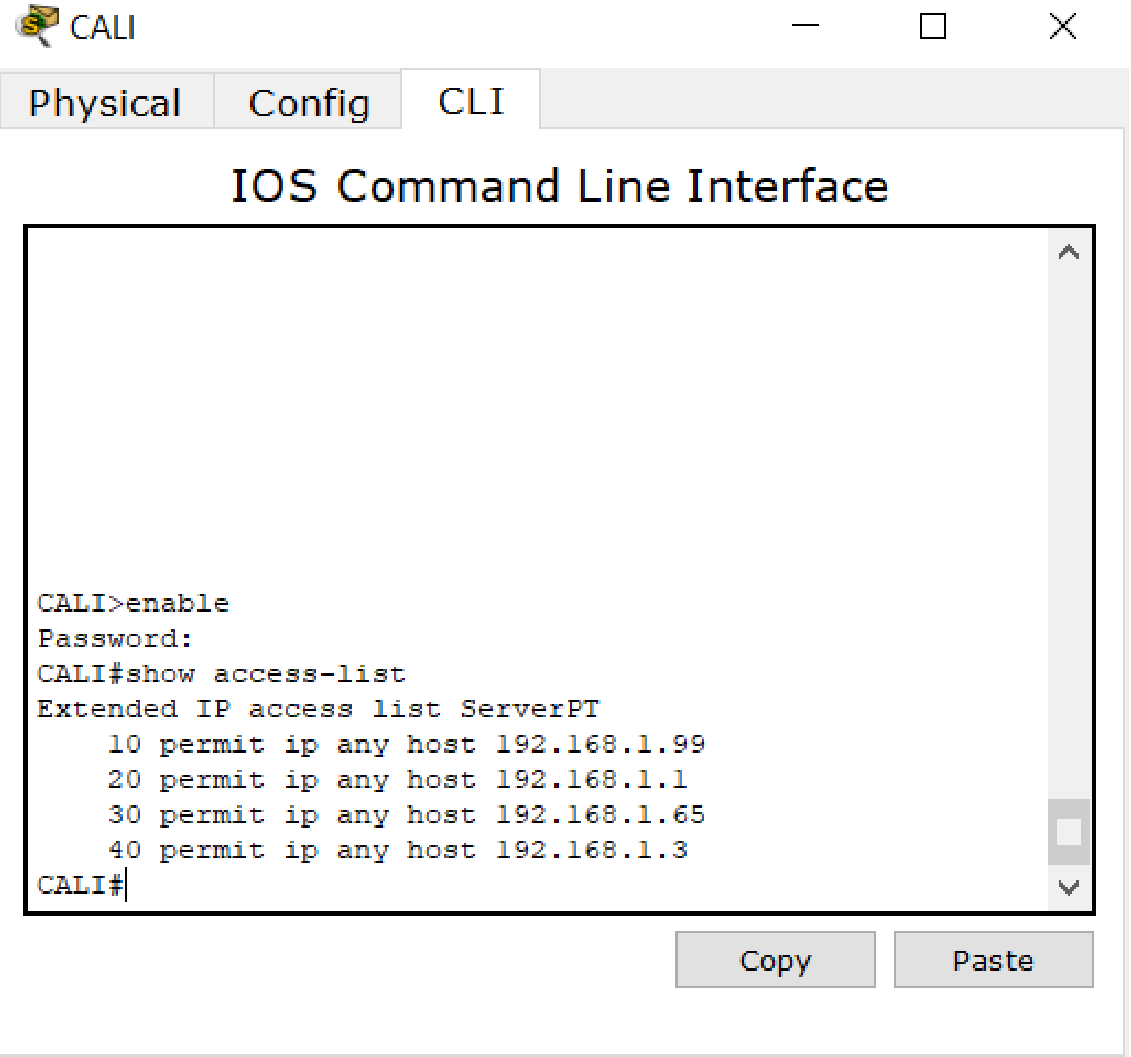
Ilustración 54: Listas de Acceso en Router MEDELLIN

Listas de Acceso en Router CALI

CALI>enable

Password:

CALI#show access-list



```
CALI>enable
Password:
CALI#show access-list
Extended IP access list ServerPT
    10 permit ip any host 192.168.1.99
    20 permit ip any host 192.168.1.1
    30 permit ip any host 192.168.1.65
    40 permit ip any host 192.168.1.3
CALI#
```

Ilustración 55: Listas de Acceso en Router CALI

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

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	CORRECTO
	WS_1	Router BOGOTA	CORRECTO
	Servidor	Router CALI	CORRECTO
	Servidor	Router MEDELLIN	CORRECTO
TELNET	LAN del Router MEDELLIN	Router CALI	FALLA
	LAN del Router CALI	Router CALI	CORRECTO
	LAN del Router MEDELLIN	Router MEDELLIN	CORRECTO
	LAN del Router CALI	Router MEDELLIN	FALLA
PING	LAN del Router CALI	WS_1	FALLA
	LAN del Router MEDELLIN	WS_1	FALLA
	LAN del Router MEDELLIN	LAN del Router CALI	FALLA
PING	LAN del Router CALI	Servidor	CORRECTO
	LAN del Router MEDELLIN	Servidor	CORRECTO
	Servidor	LAN del Router MEDELLIN	CORRECTO
	Servidor	LAN del Router CALI	CORRECTO
	Router CALI	LAN del Router MEDELLIN	CORRECTO
	Router MEDELLIN	LAN del Router CALI	CORRECTO

Tabla 1: Tabla de condiciones de prueba

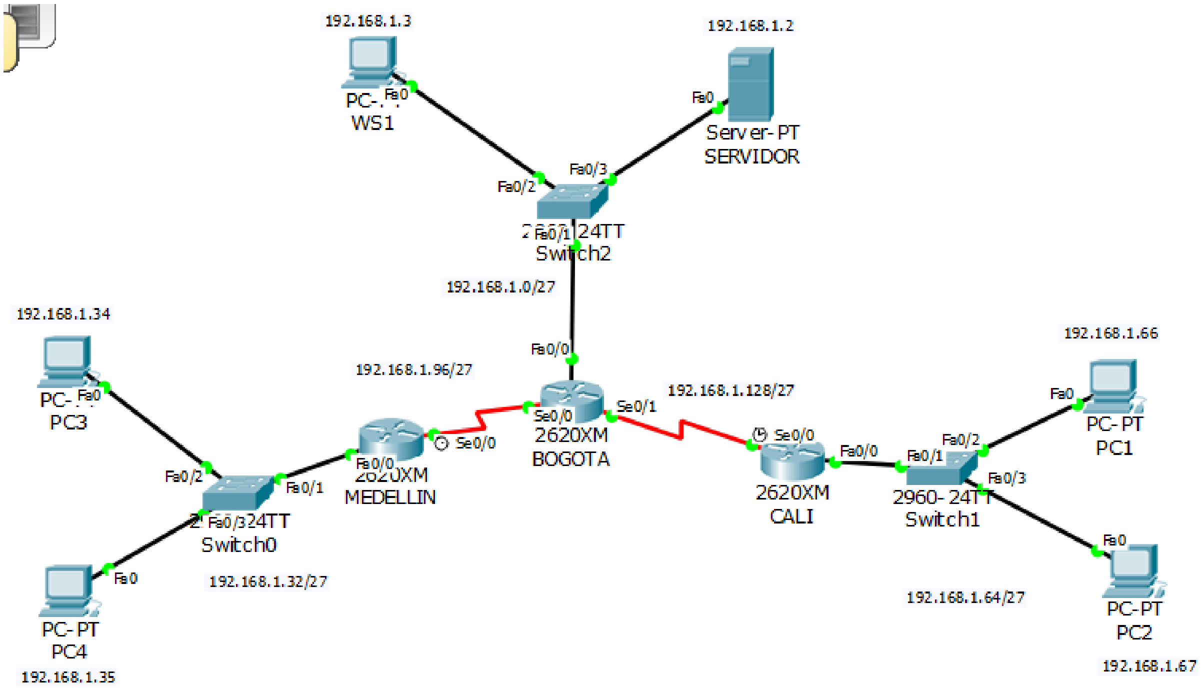


Ilustración 56: Comunicación Final Escenario 1

3. ESCENARIO 2

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

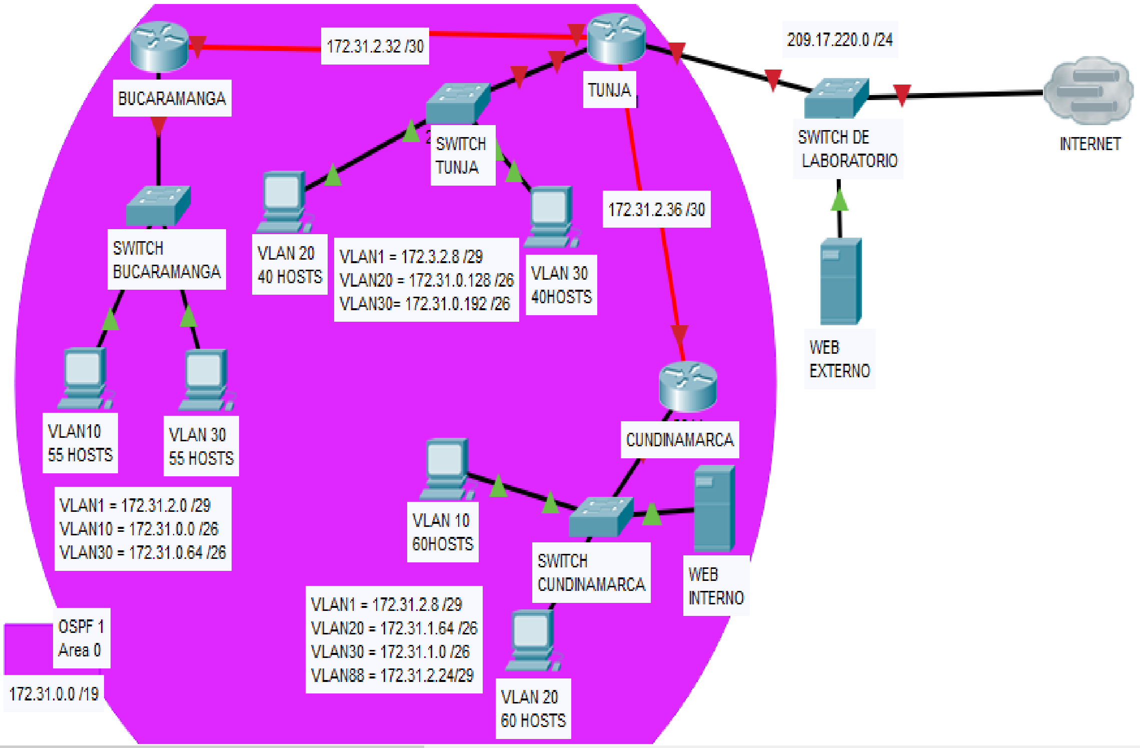


Ilustración 57: Topología Escenario 2

3.1. Desarrollo

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:
    - Configuración básica.
    - Autenticación local con AAA.
    - Cifrado de contraseñas.
    - Un máximo de internos para acceder al router.
    - Máximo tiempo de acceso al detectar ataques.
    - Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.

2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca
3. El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).
4. El enrutamiento deberá tener autenticación.
5. Listas de control de acceso:
    - Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.
    - Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.
    - Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.
    - Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.
    - Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.
    - Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.
    - Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.
    - Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los routers e internet.
    - VLSM: utilizar la dirección 172.31.0.0 /18 para el direccionamiento.

3.2. Aspectos a tener en cuenta

- Habilitar VLAN en cada switch y permitir su enrutamiento.
- Enrutamiento OSPF con autenticación en cada router.
- Servicio DHCP en el router Tunja, mediante el helper address, para los routers Bucaramanga y Cundinamarca.
- Configuración de NAT estático y de sobrecarga.
- Establecer una lista de control de acceso de acuerdo con los criterios señalados.
- Habilitar las opciones en puerto consola y terminal virtual

3.3. Todos los routers deberan tener la siguiente cofiguraciòn

Configuración Router BUCARAMANGA

```
Router>enable
Router#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname BUCARAMANGA
BUCARAMANGA(config)#no ip domain-lookup
BUCARAMANGA(config)#enable secret cisco
BUCARAMANGA(config)#banner motd #ACCESO RESTRINGIDO#
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#password cisco
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#logging synchronous
BUCARAMANGA(config-line)#line vty 0 15
BUCARAMANGA(config-line)#password cisco
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#logging synchronous
BUCARAMANGA(config-line)#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)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up
BUCARAMANGA(config-if)#int s0/0/0
BUCARAMANGA(config-if)#ip address 172.31.2.34 255.255.255.252
BUCARAMANGA(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
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#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#
```

Configuración Router TUNJA

```
Router>enable
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname TUNJA
TUNJA(config)#no ip domain-lookup
TUNJA(config)#enable secret cisco
TUNJA(config)#banner motd #ACCESO RESTRINGIDO#
TUNJA(config)#line console 0
TUNJA(config-line)#password cisco
TUNJA(config-line)#login
TUNJA(config-line)#logging synchronous
TUNJA(config-line)#line vty 0 15
TUNJA(config-line)#password cisco
TUNJA(config-line)#login
TUNJA(config-line)#logging synchronous
TUNJA(config-line)#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)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up
TUNJA(config-if)#int s0/0/0
TUNJA(config-if)#ip address 172.31.2.33 255.255.255.252
TUNJA(config-if)#no shutdown
TUNJA(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
TUNJA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
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
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
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)#
```

```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

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

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)#

01:53:30: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/0/0 from LOADING to FULL, Loading Done

TUNJA(config-router)#network 172.31.2.36 0.0.0.3 area 0

TUNJA(config-router)#end

TUNJA#

%SYS-5-CONFIG_I: Configured from console by console

TUNJA#
```

Configuración Router CUNDINAMARCA

```
Router>enable

Router#conf term

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

Router(config)#hostname CUNDINAMARCA

CUNDINAMARCA(config)#no ip domain-lookup

CUNDINAMARCA(config)#enable secret cisco

CUNDINAMARCA(config)#banner motd #ACCESO RESTRINGIDO#

CUNDINAMARCA(config)#line console 0

CUNDINAMARCA(config-line)#password cisco
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#logging synchronous
CUNDINAMARCA(config-line)#line vty 0 15
CUNDINAMARCA(config-line)#password cisco
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#logging synchronous
CUNDINAMARCA(config-line)#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)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/0.88, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.88, changed state to up
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)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
CUNDINAMARCA(config-if)#router ospf 1
CUNDINAMARCA(config-router)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
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)#
00:17:55: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.220.1 on Serial0/0/0 from LOADING to FULL, Loading Done
CUNDINAMARCA(config-router)#end
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
CUNDINAMARCA#
```

Configuración Switch BUCARAMANGA

```
Switch>enable
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname BUCARAMANGA-SW
BUCARAMANGA-SW(config)#vlan 1
BUCARAMANGA-SW(config-vlan)#vlan 10
BUCARAMANGA-SW(config-vlan)#vlan 30
BUCARAMANGA-SW(config-vlan)#int f0/1
BUCARAMANGA-SW(config-if)#switchport mode access
BUCARAMANGA-SW(config-if)#switchport access vlan 10
BUCARAMANGA-SW(config-if)#int f0/2
BUCARAMANGA-SW(config-if)#switchport mode access
BUCARAMANGA-SW(config-if)#switchport access vlan 30
BUCARAMANGA-SW(config-if)#int f0/3
BUCARAMANGA-SW(config-if)#switchport mode trunk
BUCARAMANGA-SW(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
BUCARAMANGA-SW(config-if)#int vlan 1
BUCARAMANGA-SW(config-if)#ip address 172.31.2.3 255.255.255.248
BUCARAMANGA-SW(config-if)#no shutdown
BUCARAMANGA-SW(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

```
BUCARAMANGA-SW(config-if)#ip default-gateway 172.31.2.1
BUCARAMANGA-SW(config)#exit
BUCARAMANGA-SW#
%SYS-5-CONFIG_I: Configured from console by console
```

Configuración Switch TUNJA

```
Switch>enable
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname TUNJA-SW
TUNJA-SW(config)#vlan 1
TUNJA-SW(config-vlan)#vlan 20
TUNJA-SW(config-vlan)#vlan 30
TUNJA-SW(config-vlan)#int f0/1
TUNJA-SW(config-if)#switchport mode access
TUNJA-SW(config-if)#switchport access vlan 20
TUNJA-SW(config-if)#int f0/2
TUNJA-SW(config-if)#switchport mode access
TUNJA-SW(config-if)#switchport access vlan 30
TUNJA-SW(config-if)#int f0/3
TUNJA-SW(config-if)#switchport mode trunk
TUNJA-SW(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
TUNJA-SW(config-if)#int vlan 1
TUNJA-SW(config-if)#ip address 172.3.2.11 255.255.255.248
```

```
TUNJA-SW(config-if)#no shutdown
TUNJA-SW(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
TUNJA-SW(config-if)#ip default-gateway 172.3.2.9
TUNJA-SW(config)#exit
TUNJA-SW#
%SYS-5-CONFIG_I: Configured from console by console
TUNJA-SW#
```

Configuración Switch CUNDINAMARCA

```
Switch>enable
Switch#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname CUNDINAMARCA-SW
CUNDINAMARCA-SW(config)#vlan 1
CUNDINAMARCA-SW(config-vlan)#vlan 20
CUNDINAMARCA-SW(config-vlan)#vlan 30
CUNDINAMARCA-SW(config-vlan)#vlan 88
CUNDINAMARCA-SW(config-vlan)#exit
CUNDINAMARCA-SW(config)#int f0/1
CUNDINAMARCA-SW(config-if)#switchport mode access
CUNDINAMARCA-SW(config-if)#switchport access vlan 20
CUNDINAMARCA-SW(config-if)#int f0/2
CUNDINAMARCA-SW(config-if)#switchport mode access
CUNDINAMARCA-SW(config-if)#switchport access vlan 30
CUNDINAMARCA-SW(config-if)#int f0/4
```

```
CUNDINAMARCA-SW(config-if)#switchport mode access
CUNDINAMARCA-SW(config-if)#switchport access vlan 88
CUNDINAMARCA-SW(config-if)#int f0/3
CUNDINAMARCA-SW(config-if)#switchport mode trunk
CUNDINAMARCA-SW(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
CUNDINAMARCA-SW(config-if)#int vlan 1
CUNDINAMARCA-SW(config-if)#ip address 172.31.2.11 255.255.255.248
CUNDINAMARCA-SW(config-if)#no shutdown
CUNDINAMARCA-SW(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
CUNDINAMARCA-SW(config-if)#ip default-gateway 172.31.2.9
CUNDINAMARCA-SW(config)#exit
CUNDINAMARCA-SW#
%SYS-5-CONFIG_I: Configured from console by console
```

Configuración Router BUCARAMANGA Autenticación local con AAA

```
ACCESO RESTRINGIDO
User Access Verification
Password:
BUCARAMANGA>enable
Password:
BUCARAMANGA#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#username administrador secret cisco00000
BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#aaa authentication login AUTH local
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#login authentication AUTH
BUCARAMANGA(config-line)#line vty 0 15
BUCARAMANGA(config-line)#login authentication AUTH
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#
```

Configuración Router TUNJA Autenticación local con AAA

```
ACCESO RESTRINGIDO
User Access Verification
Password:
TUNJA>enable
Password:
TUNJA#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
TUNJA(config)#line console 0
TUNJA(config-line)#username administrador secret cisco00000
TUNJA(config)#aaa new-model
TUNJA(config)#aaa authentication login AUTH local
TUNJA(config)#line console 0
TUNJA(config-line)#login authentication AUTH
TUNJA(config-line)#line vty 0 15
TUNJA(config-line)#login authentication AUTH
TUNJA(config-line)#exit
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
TUNJA#
```

Configuración Router CUNDINAMARCA Autenticación local con AAA

```
ACCESO RESTRINGIDO
User Access Verification
Password:
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#username administrador secret cisco00000
CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#aaa authentication login AUTH local
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#login authentication AUTH
CUNDINAMARCA(config-line)#line vty 0 15
CUNDINAMARCA(config-line)#login authentication AUTH
CUNDINAMARCA(config-line)#exit
CUNDINAMARCA(config)#exit
```

```
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
```

Cifrado de contraseñas en Router BUCARAMANGA

```
BUCARAMANGA#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
BUCARAMANGA(config)#service password-encryption
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#
```

Cifrado de contraseñas en Router TUNJA

```
TUNJA#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
TUNJA(config)#service password-encryption
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
```

Cifrado de contraseñas en Router CUNDINAMARCA

```
CUNDINAMARCA#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
CUNDINAMARCA(config)#service password-encryption
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
```

Configuración internos para acceder al Router y tiempo de acceso al detectar ataques en Router BUCARAMANGA

```
BUCARAMANGA#conf term

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

BUCARAMANGA(config)#line console 0

BUCARAMANGA(config-line)#login block-for 10 attempts 3 within 60

BUCARAMANGA(config)#exit

BUCARAMANGA#

%SYS-5-CONFIG_I: Configured from console by console
```

Configuración internos para acceder al Router y tiempo de acceso al detectar ataques en Router TUNJA

```
TUNJA#conf term

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

TUNJA(config)#line console 0

TUNJA(config-line)#login block-for 10 attempts 3 within 60

TUNJA(config)#exit

TUNJA#

%SYS-5-CONFIG_I: Configured from console by console
```

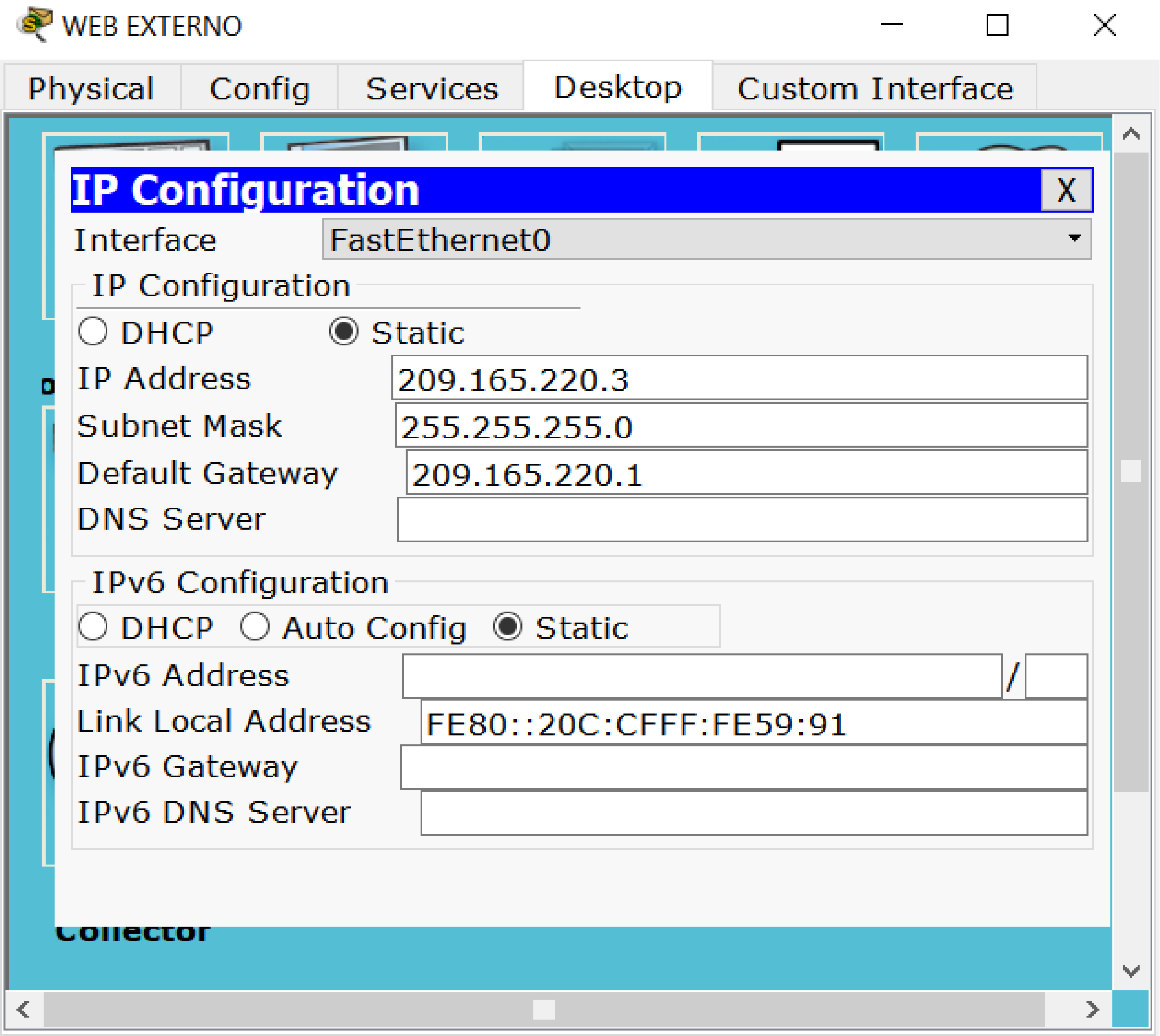
Configuración internos para acceder al Router y tiempo de acceso al detectar ataques en Router CUNDINAMARCA

```
CUNDINAMARCA#conf term

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

CUNDINAMARCA(config)#line console 0

CUNDINAMARCA(config-line)#login block-for 10 attempts 3 within 60

CUNDINAMARCA(config)#exit

CUNDINAMARCA#
```

%SYS-5-CONFIG_I: Configured from console by console

CUNDINAMARCA#

Establecer un servidor TFTP y almacenar todos los archivos necesarios de los routers



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IP Address: 209.165.220.3

Subnet Mask: 255.255.255.0

Default Gateway: 209.165.220.1

DNS Server:

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address: /

Link Local Address: FE80::20C:CFFF:FE59:91

IPv6 Gateway:

IPv6 DNS Server:

Ilustración 58: Configuración WEB EXTERNO

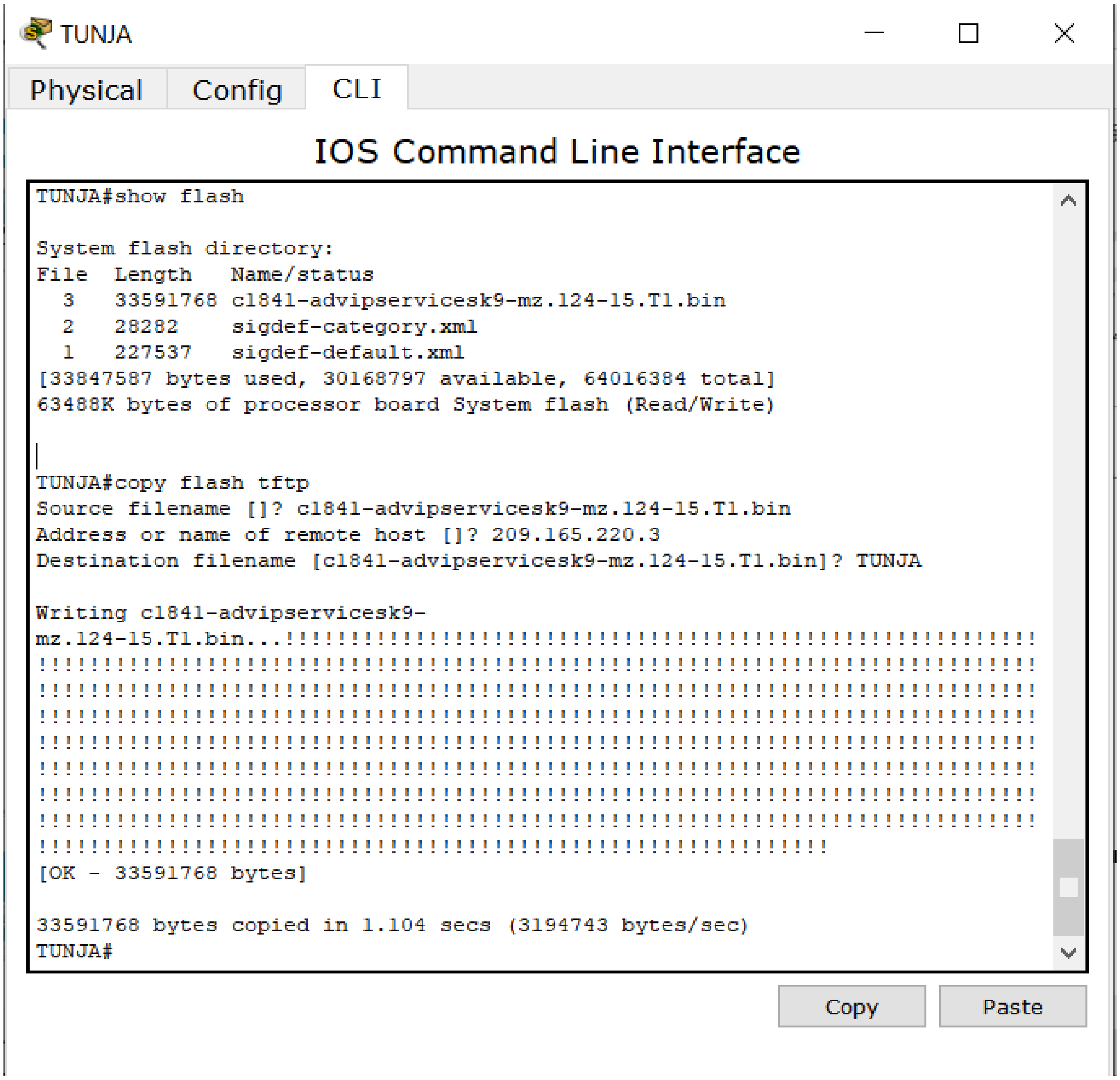
TUNJA#show flash

TUNJA#copy flash tftp

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

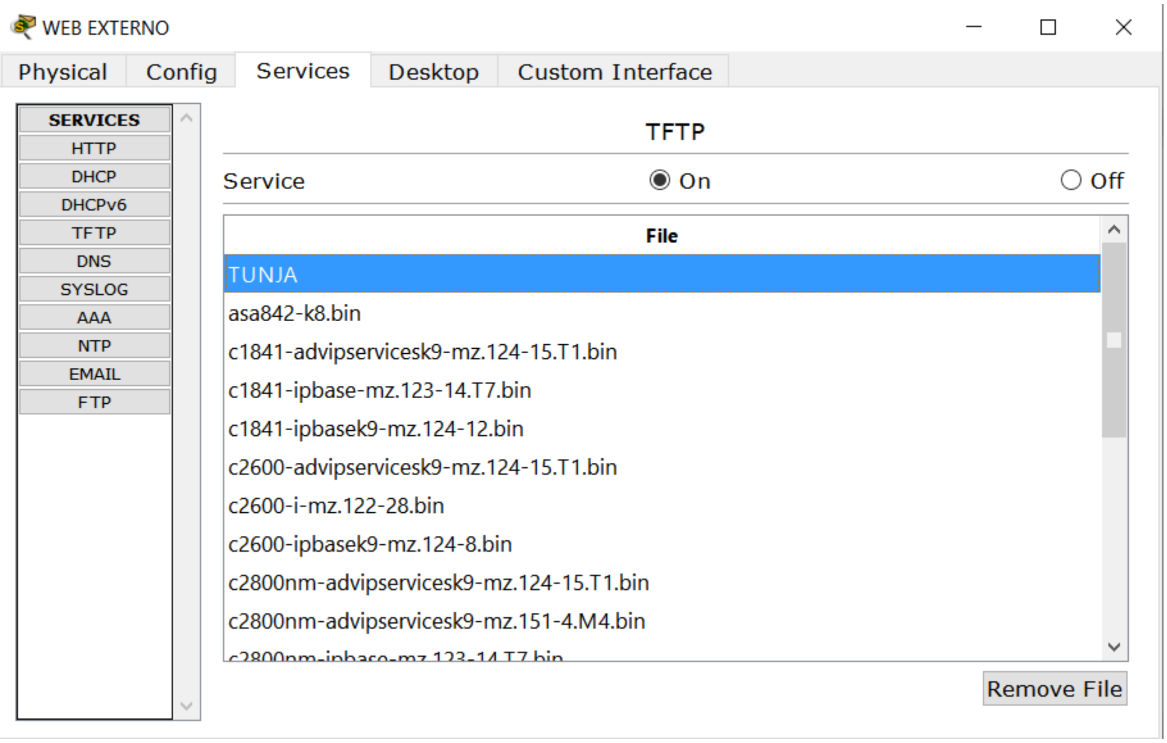
Address or name of remote host []? 209.165.220.3

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



```
TUNJA#show flash

System flash directory:
File  Length   Name/status
  3   33591768 c1841-advipservicesk9-mz.124-15.T1.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[33847587 bytes used, 30168797 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)


TUNJA#copy flash tftp
Source filename []? c1841-advipservicesk9-mz.124-15.T1.bin
Address or name of remote host []? 209.165.220.3
Destination filename [c1841-advipservicesk9-mz.124-15.T1.bin]? TUNJA

Writing c1841-advipservicesk9-
mz.124-15.T1.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 33591768 bytes]

33591768 bytes copied in 1.104 secs (3194743 bytes/sec)
TUNJA#
```

Ilustración 59: Almacenamiento Archivos Router TUNJA



TFTP

Service ● On ○ Off

File
TUNJA
asa842-k8.bin
c1841-advipservicesk9-mz.124-15.T1.bin
c1841-ipbase-mz.123-14.T7.bin
c1841-ipbasek9-mz.124-12.bin
c2600-advipservicesk9-mz.124-15.T1.bin
c2600-i-mz.122-28.bin
c2600-ipbasek9-mz.124-8.bin
c2800nm-advipservicesk9-mz.124-15.T1.bin
c2800nm-advipservicesk9-mz.151-4.M4.bin
c2800nm-ipbase-mz.123-14.T7.bin

Ilustración 60: Servidor TFTP

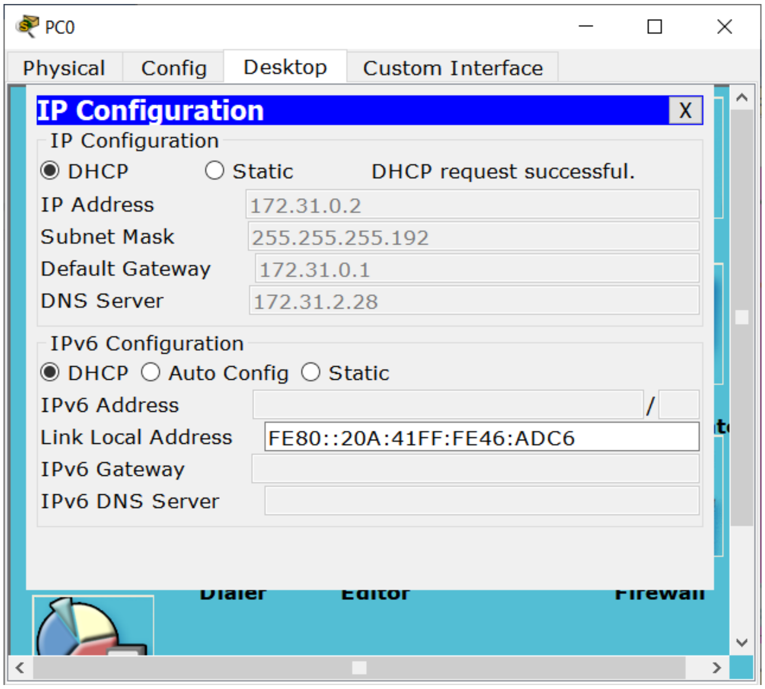
El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca

```
ACCESO RESTRINGIDO
User Access Verification
Username: administrador
Password:
TUNJA>enable
Password:
TUNJA#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
TUNJA(config)#ip dhcp excluded-address 172.31.0.1
TUNJA(config)#ip dhcp excluded-address 172.31.0.65
TUNJA(config)#ip dhcp excluded-address 172.31.1.65
TUNJA(config)#ip dhcp excluded-address 172.31.1.1
TUNJA(config)#ip dhcp pool V10B
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 172.31.2.28
TUNJA(dhcp-config)#ip dhcp pool V30B
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 172.31.2.28
TUNJA(dhcp-config)#ip dhcp pool V20C
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 172.31.2.28
TUNJA(dhcp-config)#ip dhcp pool V30C
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 172.31.2.28
TUNJA(dhcp-config)#exit
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
TUNJA#

ACCESO RESTRINGIDO
User Access Verification
Username: administrador
```

```
Password:
BUCARAMANGA>enable
Password:
BUCARAMANGA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
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#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#
```

```
ACCESO RESTRINGIDO
User Access Verification
Username: administrador
Password:
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
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#
%SYS-5-CONFIG_I: Configured from console by console
CUNDINAMARCA#
```



IP Configuration

IP Configuration

● DHCP ○ Static DHCP request successful.

IP Address 172.31.0.2

Subnet Mask 255.255.255.192

Default Gateway 172.31.0.1

DNS Server 172.31.2.28

IPv6 Configuration

● DHCP ○ Auto Config ○ Static

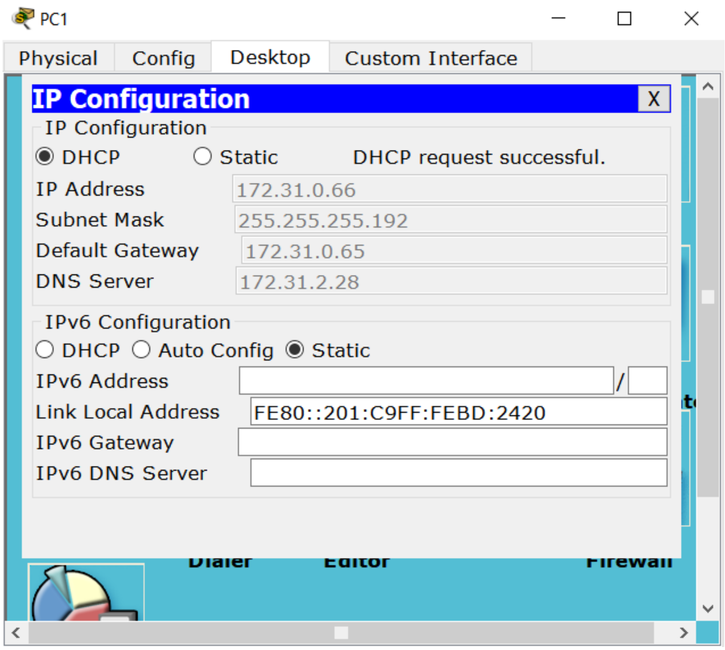
IPv6 Address /

Link Local Address FE80::20A:41FF:FE46:ADC6

IPv6 Gateway

IPv6 DNS Server

Ilustración 61: Configuración PC0



IP Configuration

IP Configuration

● DHCP ○ Static DHCP request successful.

IP Address 172.31.0.66

Subnet Mask 255.255.255.192

Default Gateway 172.31.0.65

DNS Server 172.31.2.28

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

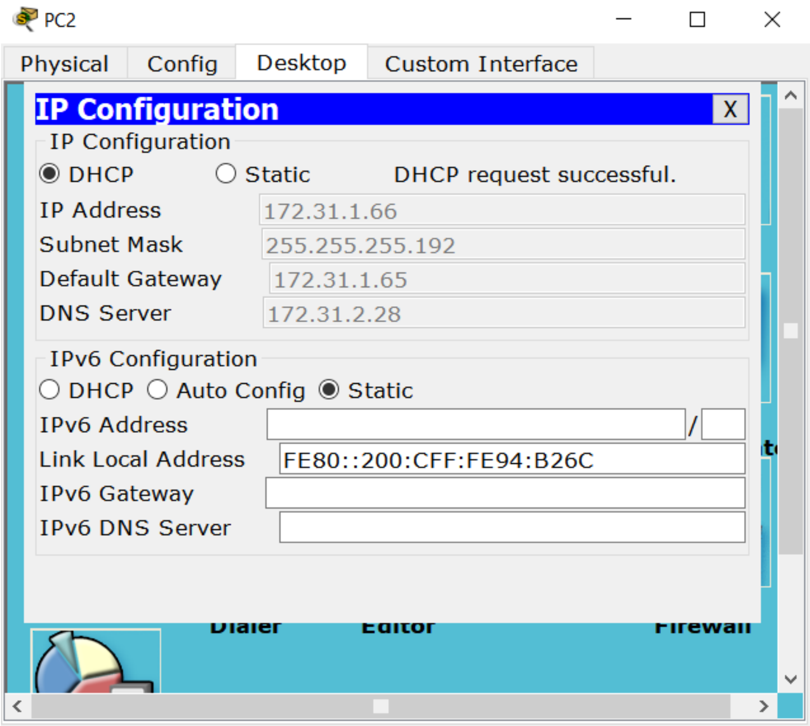
IPv6 Address /

Link Local Address FE80::201:C9FF:FEBD:2420

IPv6 Gateway

IPv6 DNS Server

Ilustración 62: Configuración PC1



PC2

IP Configuration

● DHCP ○ Static DHCP request successful.

IP Address 172.31.1.66

Subnet Mask 255.255.255.192

Default Gateway 172.31.1.65

DNS Server 172.31.2.28

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

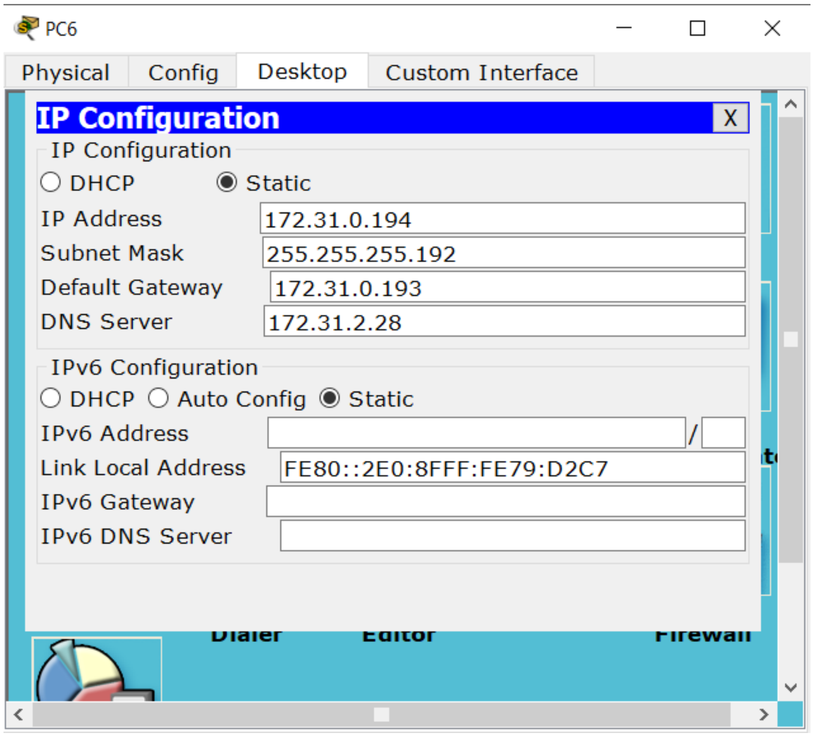
IPv6 Address /

Link Local Address FE80::200:CFF:FE94:B26C

IPv6 Gateway

IPv6 DNS Server

Ilustración 63: Configuración PC2



PC6

IP Configuration

○ DHCP ● Static

IP Address 172.31.0.194

Subnet Mask 255.255.255.192

Default Gateway 172.31.0.193

DNS Server 172.31.2.28

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

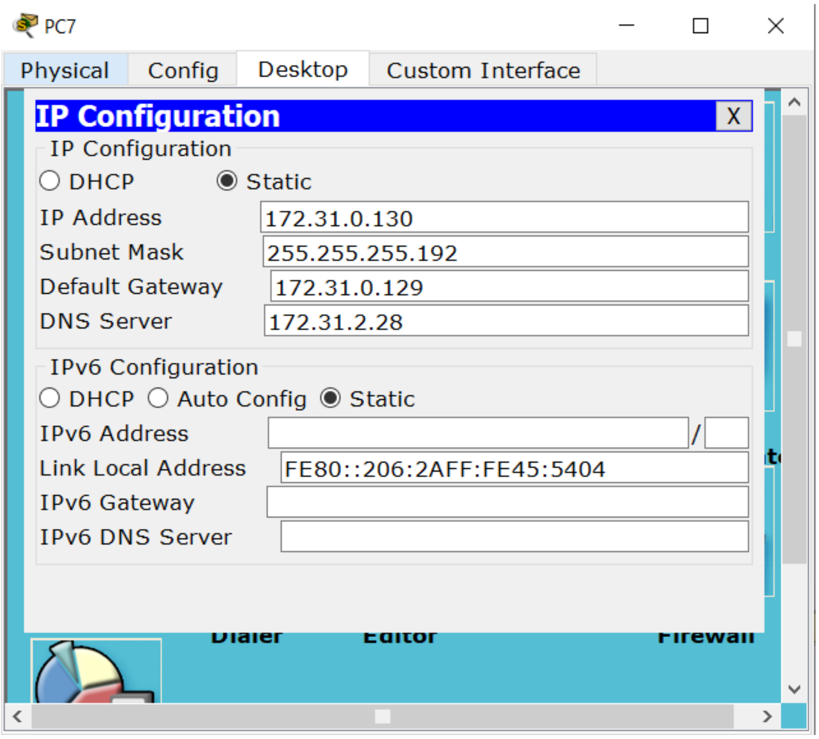
IPv6 Address /

Link Local Address FE80::2E0:8FFF:FE79:D2C7

IPv6 Gateway

IPv6 DNS Server

Ilustración 64: Configuración PC6



IP Configuration

○ DHCP ● Static

IP Address 172.31.0.130

Subnet Mask 255.255.255.192

Default Gateway 172.31.0.129

DNS Server 172.31.2.28

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

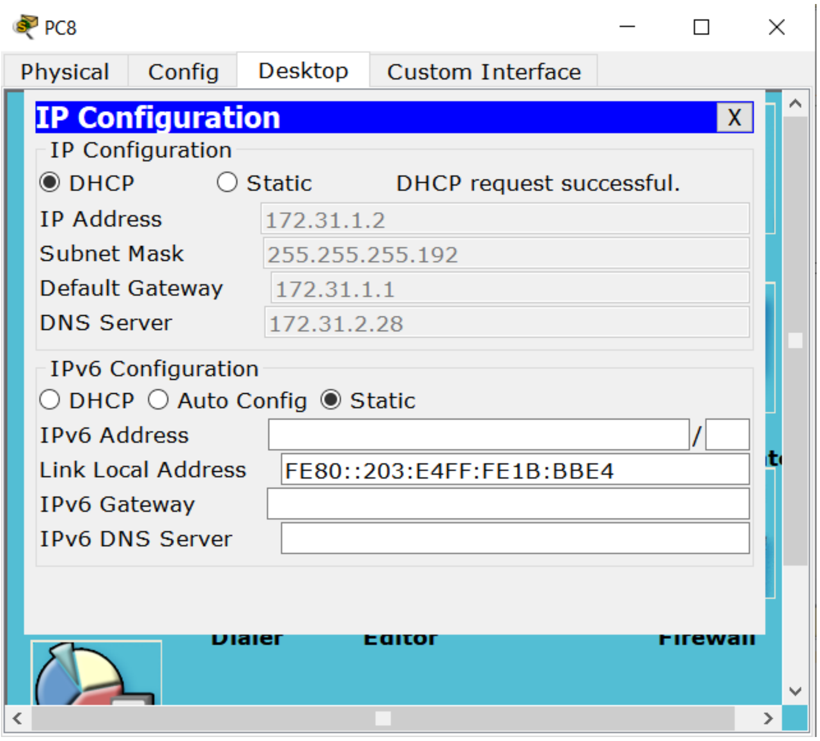
IPv6 Address /

Link Local Address FE80::206:2AFF:FE45:5404

IPv6 Gateway

IPv6 DNS Server

Ilustración 65: Configuración PC7



IP Configuration

● DHCP ○ Static DHCP request successful.

IP Address 172.31.1.2

Subnet Mask 255.255.255.192

Default Gateway 172.31.1.1

DNS Server 172.31.2.28

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

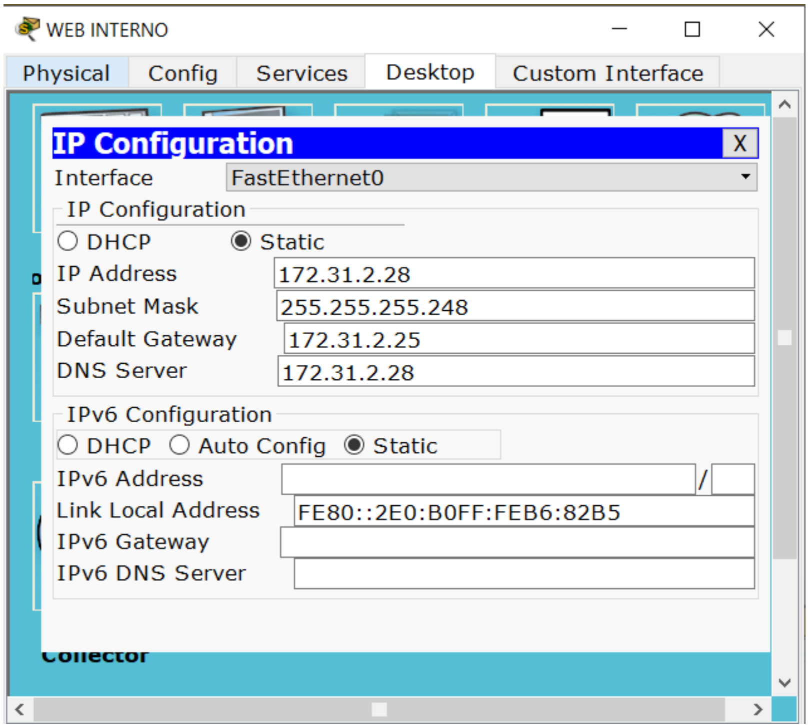
IPv6 Address /

Link Local Address FE80::203:E4FF:FE1B:BBE4

IPv6 Gateway

IPv6 DNS Server

Ilustración 66: Configuración PC8



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IP Address: 172.31.2.28

Subnet Mask: 255.255.255.248

Default Gateway: 172.31.2.25

DNS Server: 172.31.2.28

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

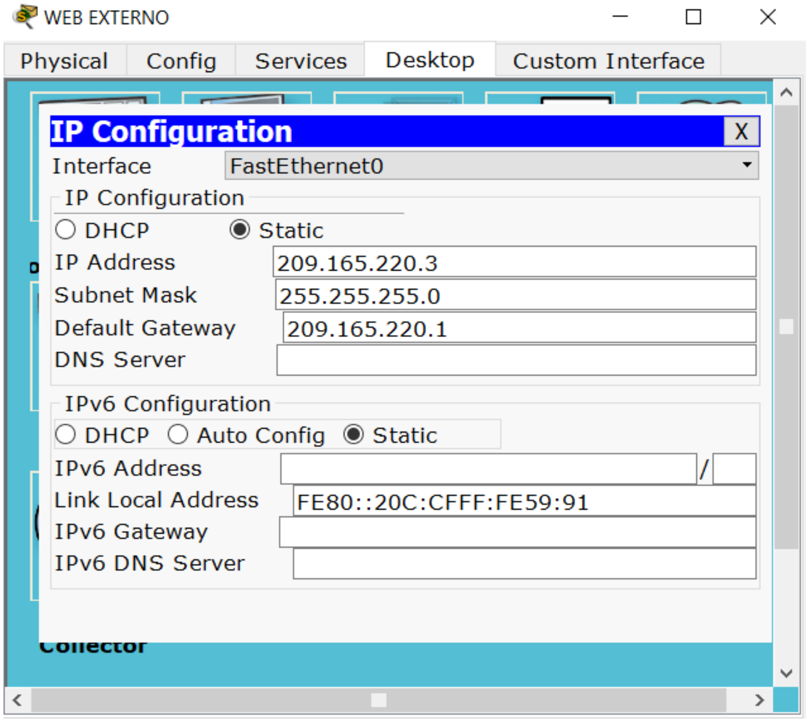
IPv6 Address: /

Link Local Address: FE80::2E0:B0FF:FEB6:82B5

IPv6 Gateway:

IPv6 DNS Server:

Ilustración 67: Configuración WEB INTERNO



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IP Address: 209.165.220.3

Subnet Mask: 255.255.255.0

Default Gateway: 209.165.220.1

DNS Server:

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address: /

Link Local Address: FE80::20C:CFFF:FE59:91

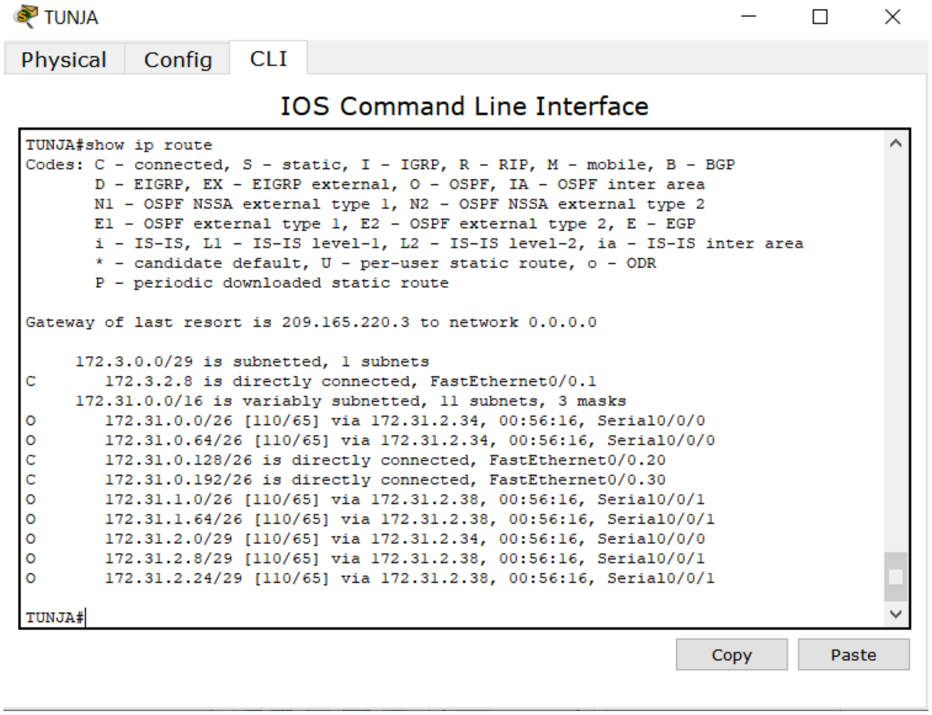
IPv6 Gateway:

IPv6 DNS Server:

Ilustración 68: Configuración WEB EXTERNO

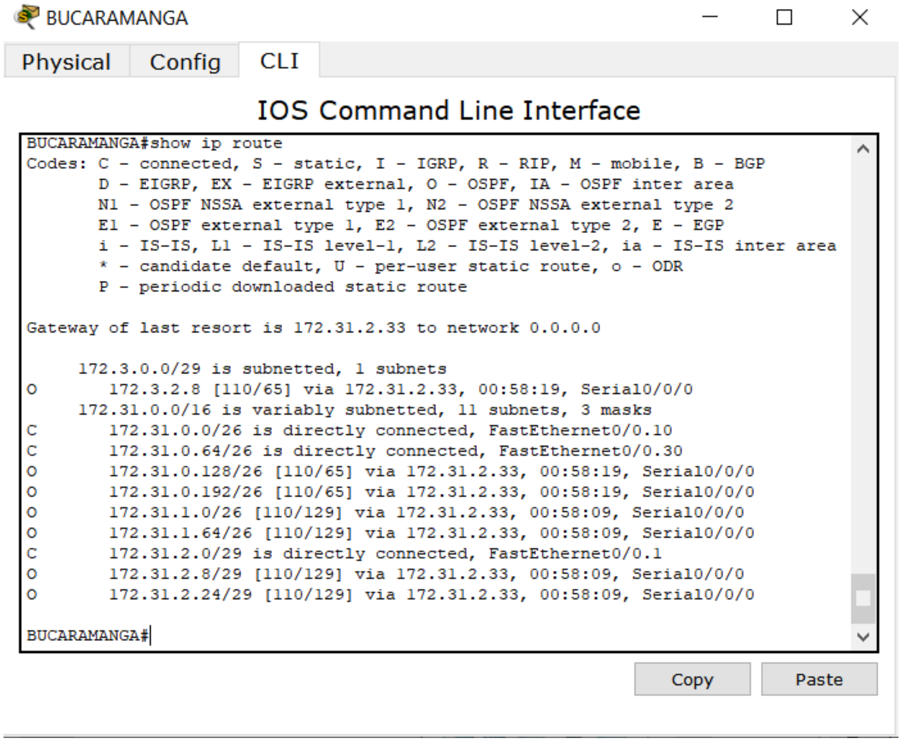
El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).

```
TUNJA#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
TUNJA(config)#ip dhcp pool V10B
TUNJA(dhcp-config)#ip nat inside source static 172.31.2.28 209.165.220.4
TUNJA(config)#access-list 1 permit 172.0.0.0 0.255.255.255
TUNJA(config)#ip nat inside source list 1 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 0.0.0.0 209.165.220.3
TUNJA(config)#router ospf 1
TUNJA(config-router)#default-information originate
TUNJA(config-router)#exit
TUNJA(config)#exit
TUNJA#
```



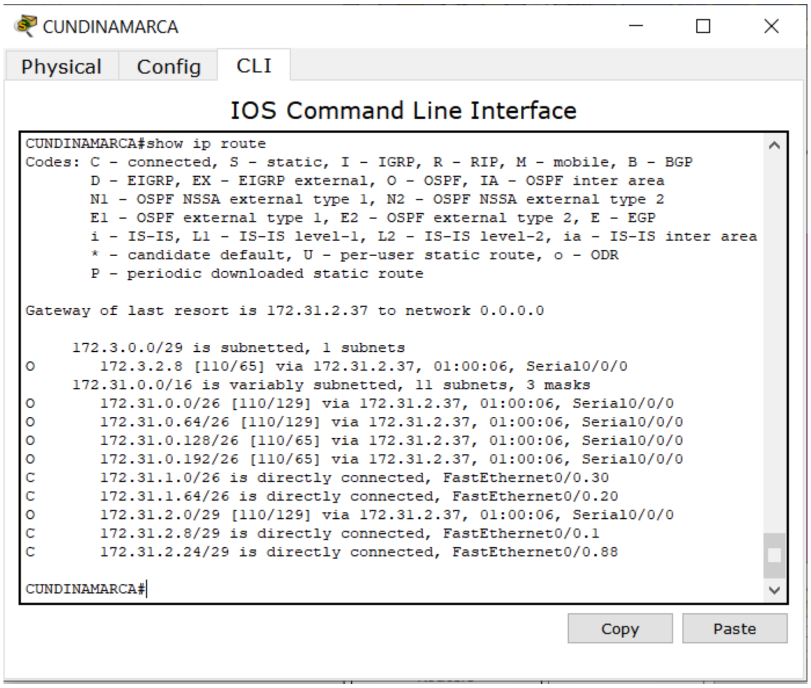
```
TUNJA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - 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 209.165.220.3 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, 00:56:16, Serial0/0/0
O       172.31.0.64/26 [110/65] via 172.31.2.34, 00:56:16, 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, 00:56:16, Serial0/0/1
O       172.31.1.64/26 [110/65] via 172.31.2.38, 00:56:16, Serial0/0/1
O       172.31.2.0/29 [110/65] via 172.31.2.34, 00:56:16, Serial0/0/0
O       172.31.2.8/29 [110/65] via 172.31.2.38, 00:56:16, Serial0/0/1
O       172.31.2.24/29 [110/65] via 172.31.2.38, 00:56:16, Serial0/0/1

TUNJA#
```

Ilustración 69: Ruta IP del Router TUNJA



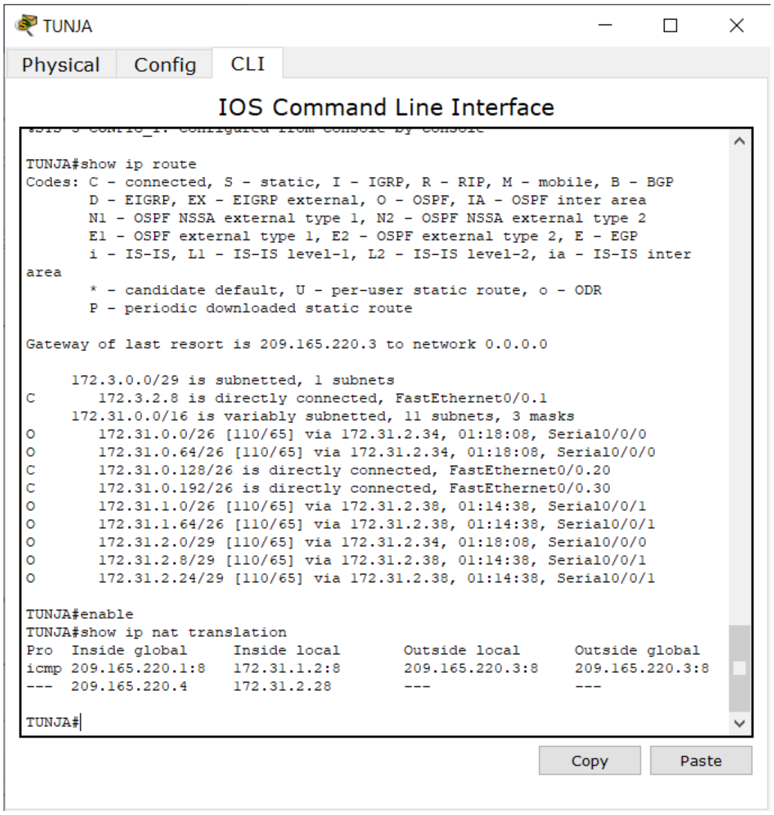
```
BUCARAMANGA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 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, 00:58:19, 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, 00:58:19, Serial0/0/0
O       172.31.0.192/26 [110/65] via 172.31.2.33, 00:58:19, Serial0/0/0
O       172.31.1.0/26 [110/129] via 172.31.2.33, 00:58:09, Serial0/0/0
O       172.31.1.64/26 [110/129] via 172.31.2.33, 00:58:09, 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, 00:58:09, Serial0/0/0
O       172.31.2.24/29 [110/129] via 172.31.2.33, 00:58:09, Serial0/0/0

BUCARAMANGA#
```

Ilustración 70: Ruta IP del Router BUCARAMANGA



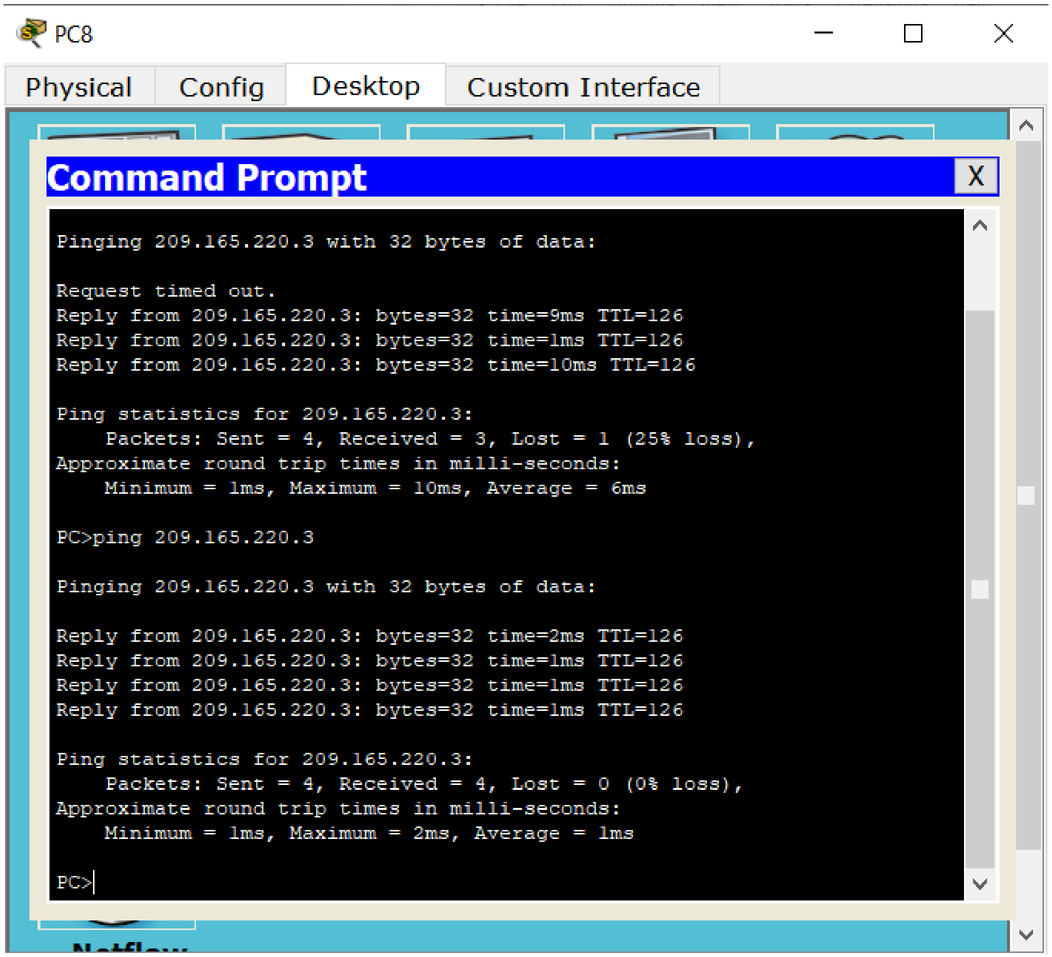
```
CUNDINAMARCA#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 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, 01:00:06, 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, 01:00:06, Serial0/0/0
O       172.31.0.64/26 [110/129] via 172.31.2.37, 01:00:06, Serial0/0/0
O       172.31.0.128/26 [110/65] via 172.31.2.37, 01:00:06, Serial0/0/0
O       172.31.0.192/26 [110/65] via 172.31.2.37, 01:00:06, 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, 01:00:06, 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

CUNDINAMARCA#
```

Ilustración 71: Ruta IP del Router CUNDINAMARCA



```
%SYS-5-CONFIG_I: Configured from console by console

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 209.165.220.3 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, 01:18:08, Serial0/0/0
O       172.31.0.64/26 [110/65] via 172.31.2.34, 01:18:08, 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, 01:14:38, Serial0/0/1
O       172.31.1.64/26 [110/65] via 172.31.2.38, 01:14:38, Serial0/0/1
O       172.31.2.0/29 [110/65] via 172.31.2.34, 01:18:08, Serial0/0/0
O       172.31.2.8/29 [110/65] via 172.31.2.38, 01:14:38, Serial0/0/1
O       172.31.2.24/29 [110/65] via 172.31.2.38, 01:14:38, Serial0/0/1

TUNJA#enable
TUNJA#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.220.1:8   172.31.1.2:8       209.165.220.3:8    209.165.220.3:8
---  209.165.220.4     172.31.2.28        ---                ---

TUNJA#
```

Ilustración 72: Ruta IP del Router TUNJA



```
Pinging 209.165.220.3 with 32 bytes of data:

Request timed out.
Reply from 209.165.220.3: bytes=32 time=9ms TTL=126
Reply from 209.165.220.3: bytes=32 time=1ms TTL=126
Reply from 209.165.220.3: bytes=32 time=10ms TTL=126

Ping statistics for 209.165.220.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 6ms

PC>ping 209.165.220.3

Pinging 209.165.220.3 with 32 bytes of data:

Reply from 209.165.220.3: bytes=32 time=2ms TTL=126
Reply from 209.165.220.3: bytes=32 time=1ms TTL=126
Reply from 209.165.220.3: bytes=32 time=1ms TTL=126
Reply from 209.165.220.3: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.220.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

PC>
```

Ilustración 73: Comunicación entre PC8 y Servidor WEB EXTERNO

El enrutamiento deberá tener autenticación Router BUCARAMANGA

ACCESO RESTRINGIDO

User Access Verification

Username: administrador

Password:

BUCARAMANGA>enable

Password:

BUCARAMANGA#enable

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 cisco000
OSPF: Key 1 already exists
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
```

El enrutamiento deberá tener autenticación Router CUNDINAMARCA

```
ACCESO RESTRINGIDO
User Access Verification
Username: administrador
Password:
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CUNDINAMARCA(config)#int s0/0/0
CUNDINAMARCA(config-if)#ip ospf authentication message-digest
CUNDINAMARCA(config-if)#ip ospf message-digest-key 1 md5 cisco000
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
CUNDINAMARCA#
```

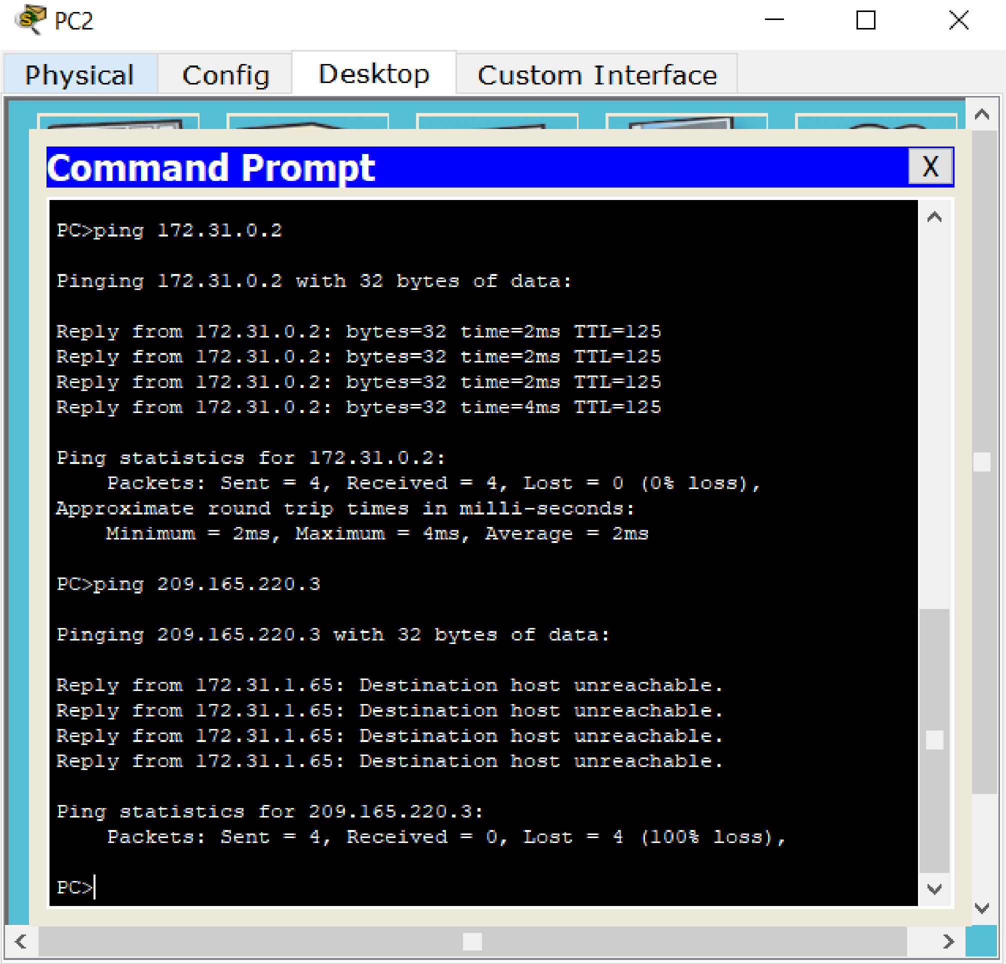
El enrutamiento deberá tener autenticación Router TUNJA

```
ACCESO RESTRINGIDO
User Access Verification
Username: administrador
Password:
TUNJA>enable
Password:
TUNJA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TUNJA(config)#int s0/0/0
TUNJA(config-if)#ip ospf authentication message-digest
TUNJA(config-if)#ip ospf message-digest-key 1 md5 cisco000
TUNJA(config-if)#int s0/0/1
04:24:23: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/0/0 from LOADING to FULL, Loading Done
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 cisco000
TUNJA(config-if)#
04:24:55: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.38 on Serial0/0/1 from LOADING to FULL, Loading Done
TUNJA(config-if)#exit
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
TUNJA#
```

3.4. Listas de control de acceso:

Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja

```
ACCESO RESTRINGIDO
User Access Verification
Username: administrador
Password:
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CUNDINAMARCA(config)#int s0/0/0
CUNDINAMARCA(config-if)#access-list 111 deny ip 172.31.1.64 0.0.0.63 209.165.220.0 0.0.0.255
CUNDINAMARCA(config)#access-list 111 permit ip any any
CUNDINAMARCA(config)#int f0/0.20
CUNDINAMARCA(config-subif)#ip access-group 111 in
CUNDINAMARCA(config-subif)#exit
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
CUNDINAMARCA#
```



```
PC>ping 172.31.0.2

Pinging 172.31.0.2 with 32 bytes of data:

Reply from 172.31.0.2: bytes=32 time=2ms TTL=125
Reply from 172.31.0.2: bytes=32 time=2ms TTL=125
Reply from 172.31.0.2: bytes=32 time=2ms TTL=125
Reply from 172.31.0.2: bytes=32 time=4ms TTL=125

Ping statistics for 172.31.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 2ms

PC>ping 209.165.220.3

Pinging 209.165.220.3 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 209.165.220.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Ilustración 74: Prueba desde PC2

Los host de VLAN10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.

ACCESO RESTRINGIDO

User Access Verification

Username: administrador

Password:

CUNDINAMARCA>en

Password:

CUNDINAMARCA#conf t

```
Enter configuration commands, one per line.  End with CNTL/Z.
CUNDINAMARCA(config)#int f0/0.30
CUNDINAMARCA(config-subif)#access-list 112 permit ip 172.31.1.0 0.0.0.63 209.165.220.0 0.0.0.255
CUNDINAMARCA(config)#access-list 112 deny ip any any
CUNDINAMARCA(config)#int f0/0.30
CUNDINAMARCA(config-subif)#ip access-group 112 in
CUNDINAMARCA(config-subif)#exit
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
CUNDINAMARCA#
```

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

```
ACCESO RESTRINGIDO
User Access Verification
Username: administrador
Password:
TUNJA>enable
Password:
TUNJA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TUNJA(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 80
TUNJA(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 21
TUNJA(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 20
```

TUNJA(config)#int f0/0.30

TUNJA(config-subif)#ip access-group 111 in

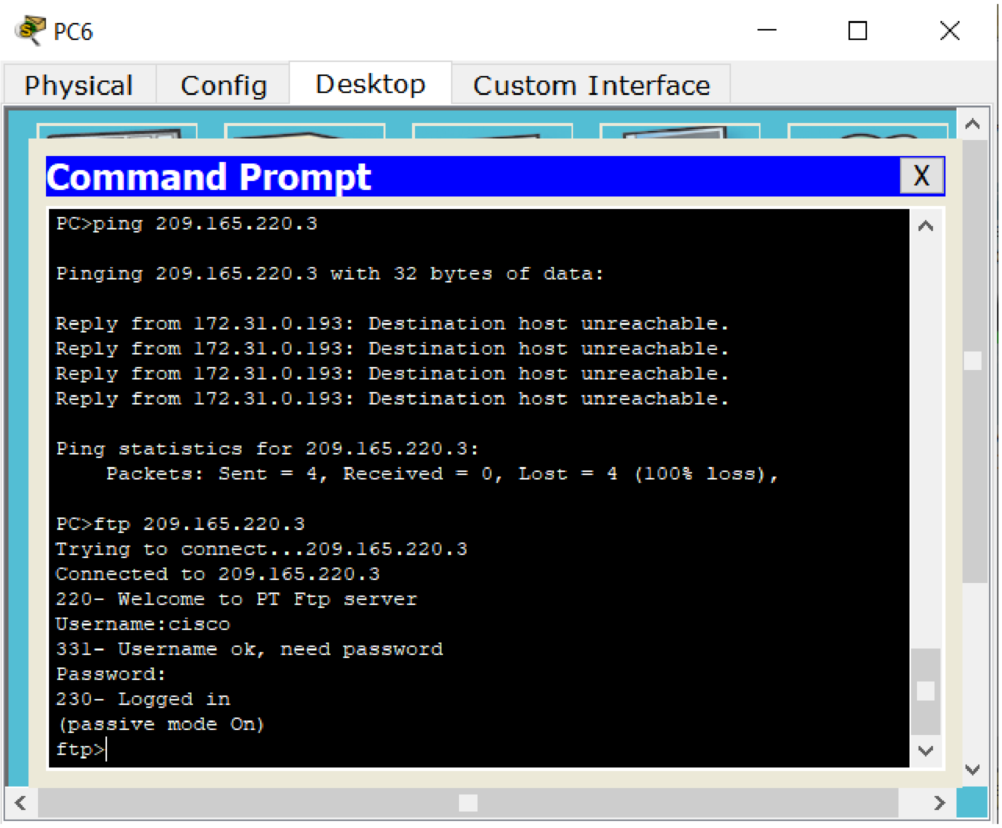
TUNJA(config-subif)#exit

TUNJA(config)#exit

TUNJA#

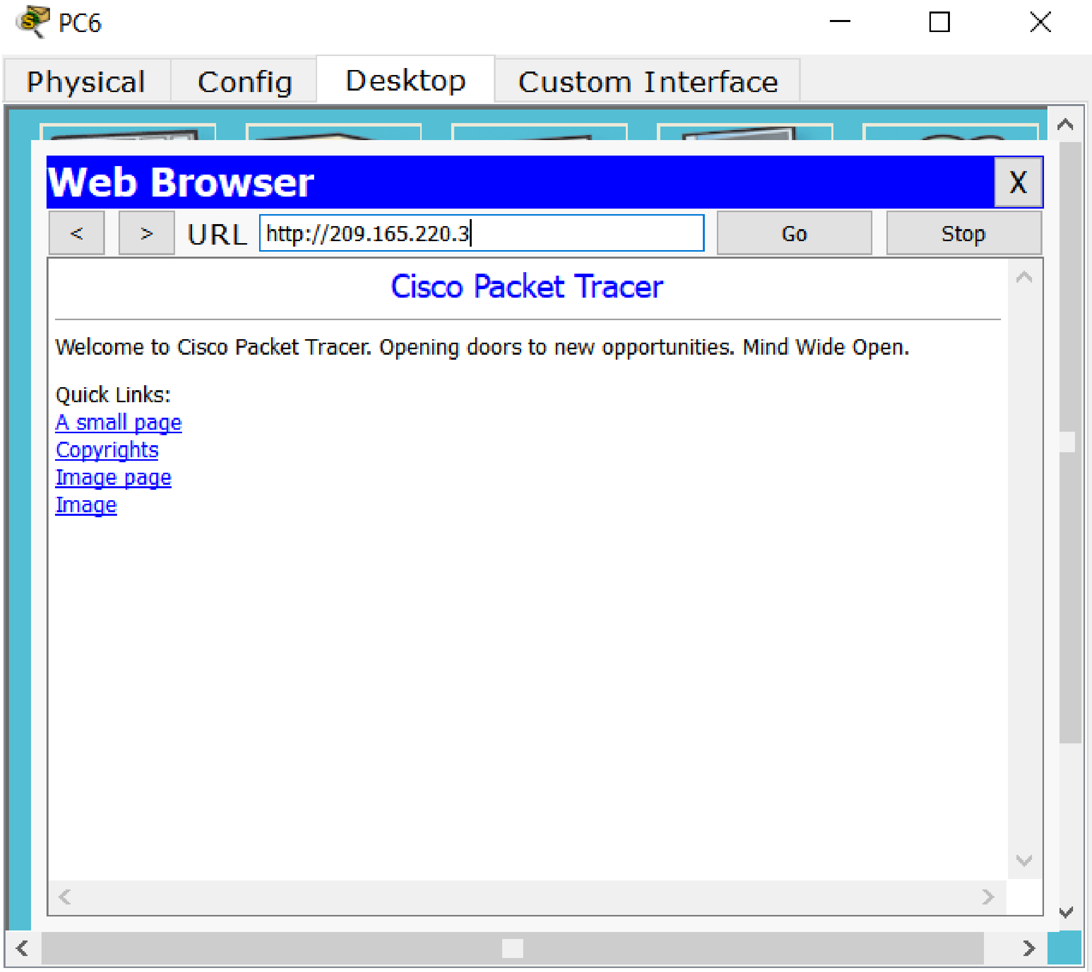
%SYS-5-CONFIG_I: Configured from console by console

TUNJA#



```
PC>ping 209.165.220.3

Pinging 209.165.220.3 with 32 bytes of data:

Reply from 172.31.0.193: Destination host unreachable.
Reply from 172.31.0.193: Destination host unreachable.
Reply from 172.31.0.193: Destination host unreachable.
Reply from 172.31.0.193: Destination host unreachable.

Ping statistics for 209.165.220.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ftp 209.165.220.3
Trying to connect...209.165.220.3
Connected to 209.165.220.3
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Ilustración 75: Prueba desde PC6



http://209.165.220.3

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

Ilustración 76: Prueba desde PC6 a URL

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

ACCESO RESTRINGIDO

User Access Verification

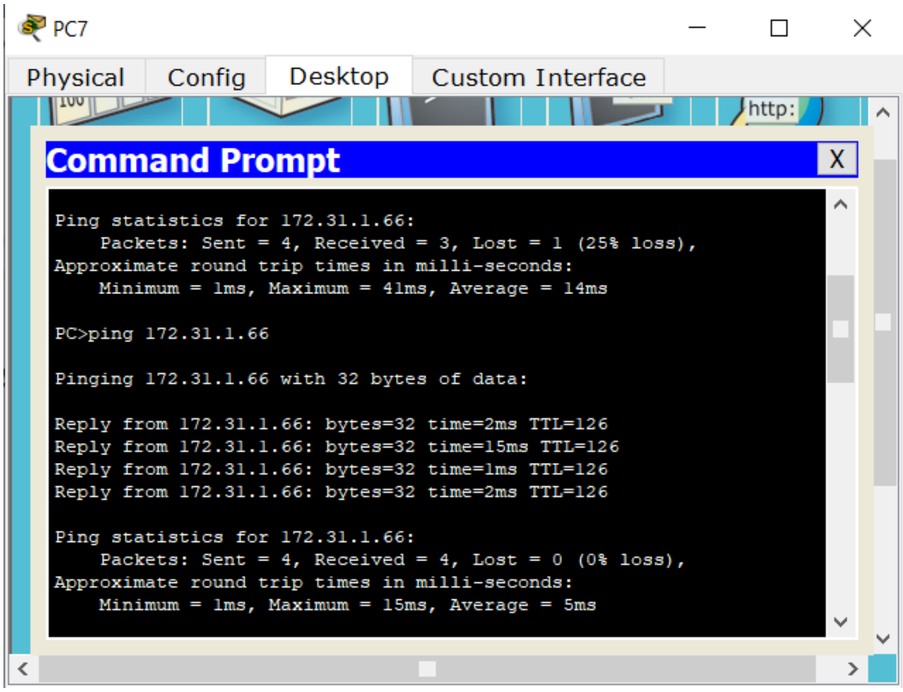
Username: administrador

Password:

TUNJA>en

Password:

```
TUNJA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TUNJA(config)#int f0/0.20
TUNJA(config-subif)#access-list 112 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
TUNJA(config)#access-list 112 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 112 in
TUNJA(config-subif)#exit
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
TUNJA#
```

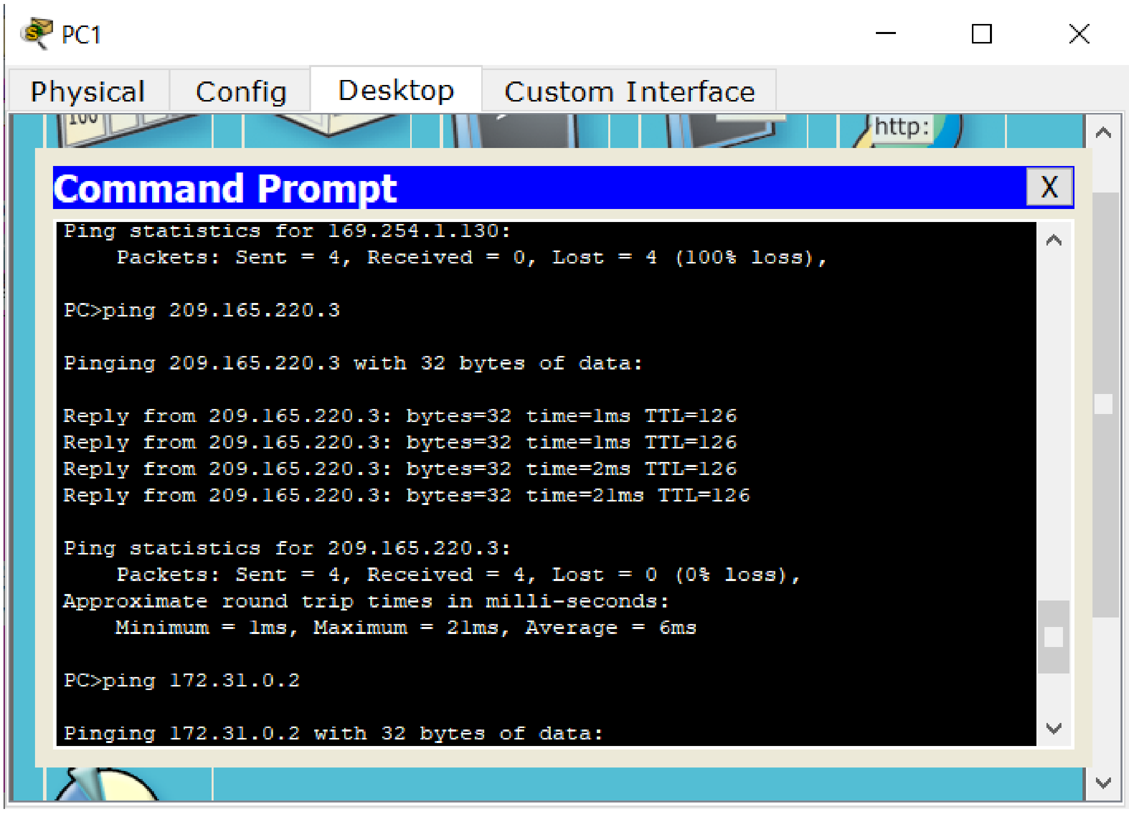


```
Ping statistics for 172.31.1.66:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 41ms, Average = 14ms

PC>ping 172.31.1.66

Pinging 172.31.1.66 with 32 bytes of data:

Reply from 172.31.1.66: bytes=32 time=2ms TTL=126
Reply from 172.31.1.66: bytes=32 time=15ms TTL=126
Reply from 172.31.1.66: bytes=32 time=1ms TTL=126
Reply from 172.31.1.66: bytes=32 time=2ms TTL=126

Ping statistics for 172.31.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 15ms, Average = 5ms
```

Ilustración 77: Prueba desde PC7

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

```
ACCESO RESTRINGIDO
User Access Verification
Username: administrador
Password:
BUCARAMANGA>enable
Password:
BUCARAMANGA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
BUCARAMANGA(config)#access-list 111 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 111 in
BUCARAMANGA(config-subif)#exit
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#
```



```
Ping statistics for 169.254.1.130:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 209.165.220.3

Pinging 209.165.220.3 with 32 bytes of data:

Reply from 209.165.220.3: bytes=32 time=1ms TTL=126
Reply from 209.165.220.3: bytes=32 time=1ms TTL=126
Reply from 209.165.220.3: bytes=32 time=2ms TTL=126
Reply from 209.165.220.3: bytes=32 time=21ms TTL=126

Ping statistics for 209.165.220.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 21ms, Average = 6ms

PC>ping 172.31.0.2

Pinging 172.31.0.2 with 32 bytes of data:
```

Ilustración 78: Prueba desde PC1

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

```
ACCESO RESTRINGIDO

User Access Verification

Username: administrador

Password:

BUCARAMANGA>enable

Password:

BUCARAMANGA#conf t

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

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

BUCARAMANGA(config-subif)#access-list 112 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63

BUCARAMANGA(config)#access-list 112 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 112 in

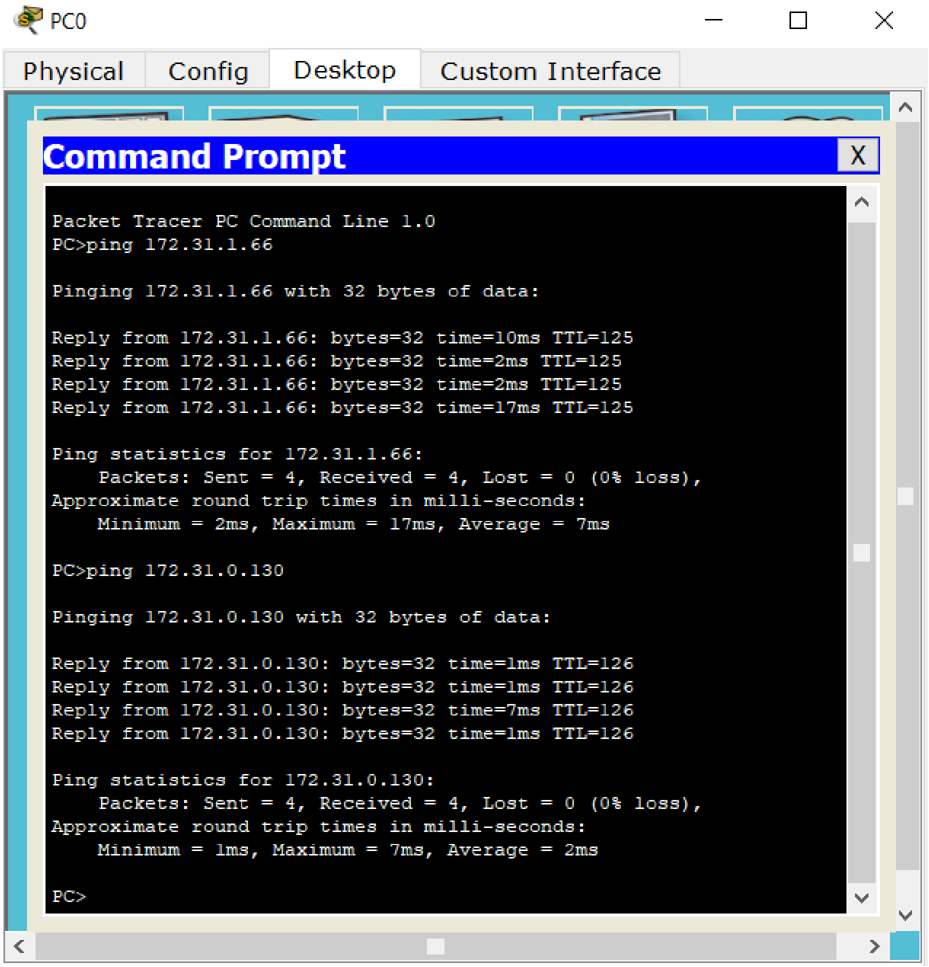
BUCARAMANGA(config-subif)#exit

BUCARAMANGA(config)#exit

BUCARAMANGA#

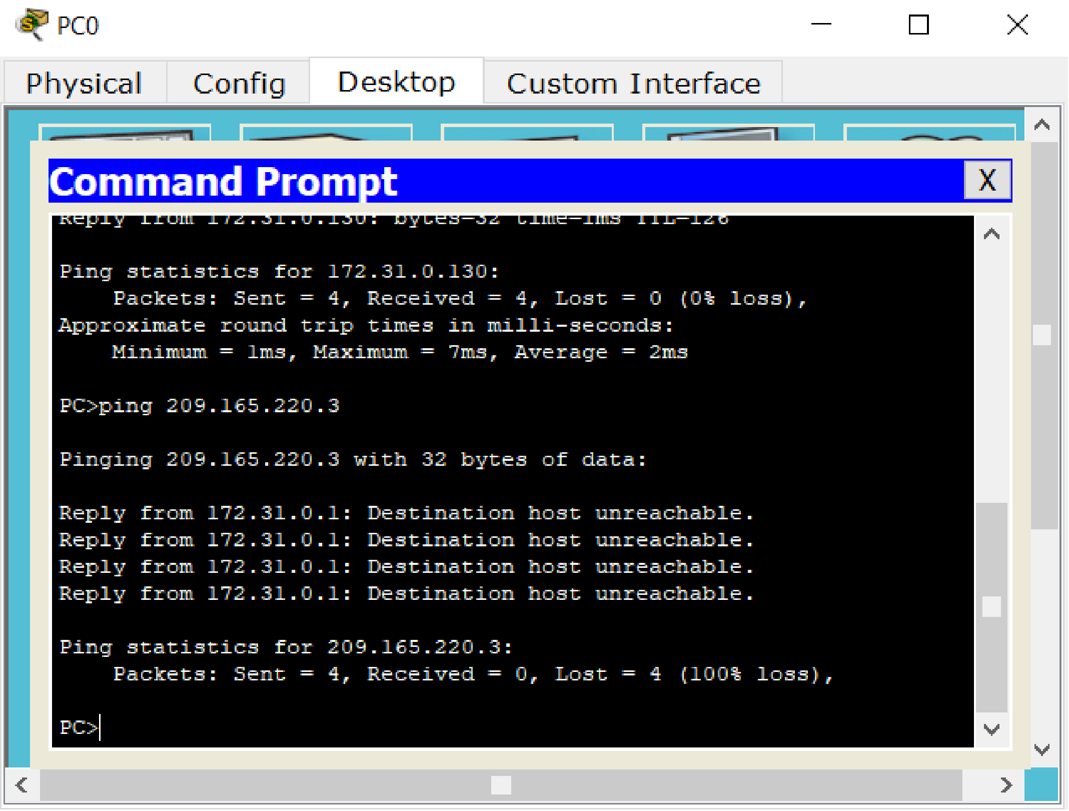
%SYS-5-CONFIG_I: Configured from console by console

BUCARAMANGA#



```
Packet Tracer PC Command Line 1.0
PC>ping 172.31.1.66

Pinging 172.31.1.66 with 32 bytes of data:

Reply from 172.31.1.66: bytes=32 time=10ms TTL=125
Reply from 172.31.1.66: bytes=32 time=2ms TTL=125
Reply from 172.31.1.66: bytes=32 time=2ms TTL=125
Reply from 172.31.1.66: bytes=32 time=17ms TTL=125

Ping statistics for 172.31.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 17ms, Average = 7ms

PC>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=1ms TTL=126
Reply from 172.31.0.130: bytes=32 time=7ms 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 = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 7ms, Average = 2ms

PC>
```

Ilustración 79: Prueba desde PC0



```
Reply from 172.31.0.130: bytes=32 time=1ms 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 = 7ms, Average = 2ms

PC>ping 209.165.220.3

Pinging 209.165.220.3 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 209.165.220.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Ilustración 80: Prueba desde PC0 a Servidor EXTERNO

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

ACCESO RESTRINGIDO

User Access Verification

Username: administrador

Password:

BUCARAMANGA>enable

Password:

BUCARAMANGA#conf t

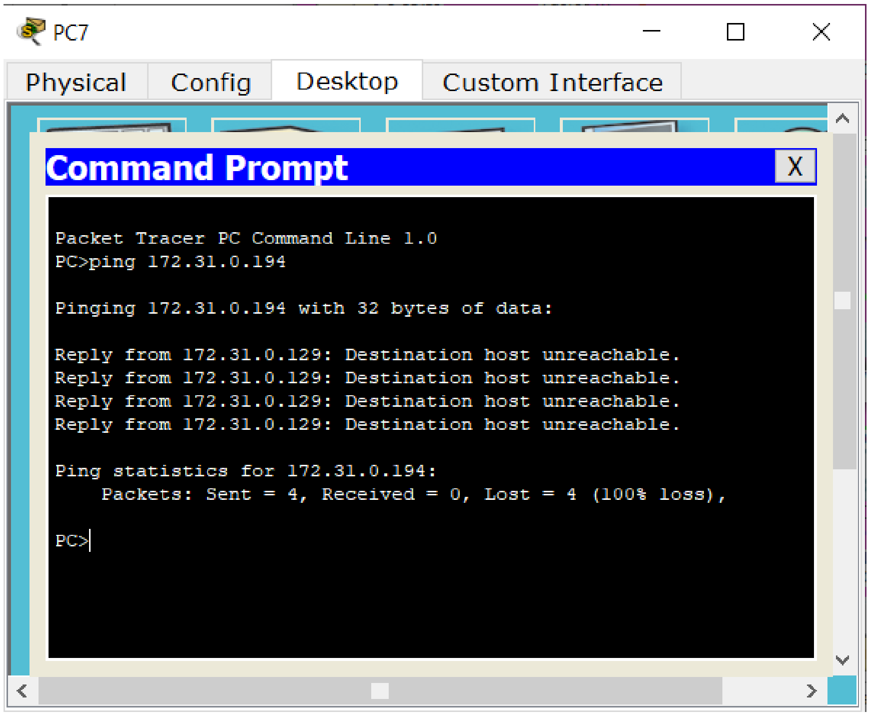
Enter configuration commands, one per line. End with CNTL/Z.

BUCARAMANGA(config)#int f0/0.10

BUCARAMANGA(config-subif)#access-list 113 deny ip 172.31.2.0 0.0.0.7 172.31.0.0 0.0.0.63

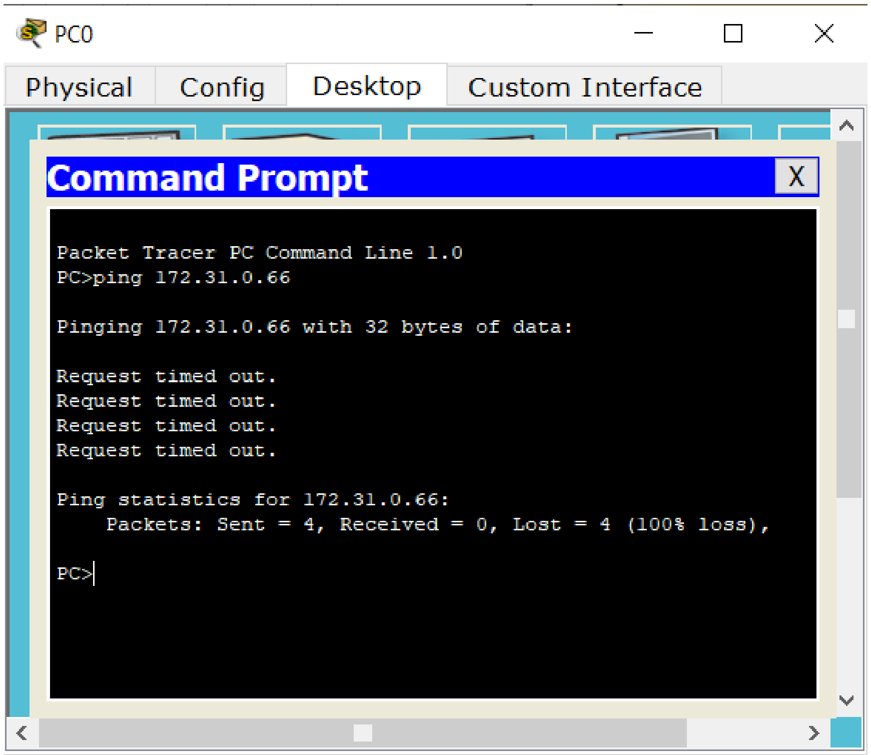
```
BUCARAMANGA(config)#access-list 113 deny ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.0.63
BUCARAMANGA(config)#access-list 113 permit ip any any
BUCARAMANGA(config)#int f0/0.10
BUCARAMANGA(config-subif)#ip access-group 113 out
BUCARAMANGA(config-subif)#exit
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#

ACCESO RESTRINGIDO
User Access Verification
Username: administrador
Password:
TUNJA>enable
Password:
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#access-list 113 deny ip 172.3.2.8 0.0.0.7 172.31.0.128 0.0.0.63
TUNJA(config)#access-list 113 deny ip 172.3.0.192 0.0.0.63 172.31.0.128 0.0.0.63
TUNJA(config)#access-list 113 permit ip any any
TUNJA(config)#int f0/0.20
TUNJA(config-subif)#ip access-group 113 out
TUNJA(config-subif)#exit
TUNJA(config)#exit
TUNJA#
```

```
%SYS-5-CONFIG_I: Configured from console by console
TUNJA#

ACCESO RESTRINGIDO
User Access Verification
Username: administrador
Password:
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CUNDINAMARCA(config)#access-list 113 deny ip 172.31.2.8 0.0.0.7 172.31.1.64 0.0.0.63
CUNDINAMARCA(config)#access-list 113 deny ip 172.31.1.0 0.0.0.63 172.31.1.64 0.0.0.63
CUNDINAMARCA(config)#access-list 113 deny ip 172.31.2.24 0.0.0.7 172.31.1.64 0.0.0.63
CUNDINAMARCA(config)#access-list 113 permit ip any any
CUNDINAMARCA(config)#int f0/0.20
CUNDINAMARCA(config-subif)#ip access-group 113 out
CUNDINAMARCA(config-subif)#exit
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
CUNDINAMARCA#
```



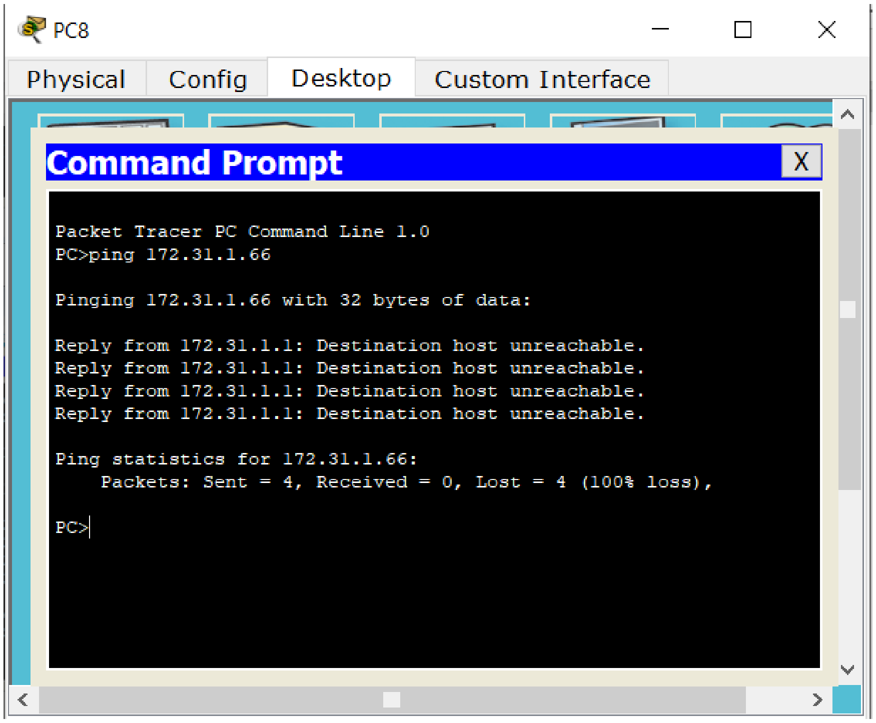
```
Packet Tracer PC Command Line 1.0
PC>ping 172.31.0.194

Pinging 172.31.0.194 with 32 bytes of data:

Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.
Reply from 172.31.0.129: Destination host unreachable.

Ping statistics for 172.31.0.194:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Ilustración 81: Prueba desde PC7



```
Packet Tracer PC Command Line 1.0
PC>ping 172.31.0.66

Pinging 172.31.0.66 with 32 bytes of data:

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

Ping statistics for 172.31.0.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Ilustración 82: Prueba desde PC0



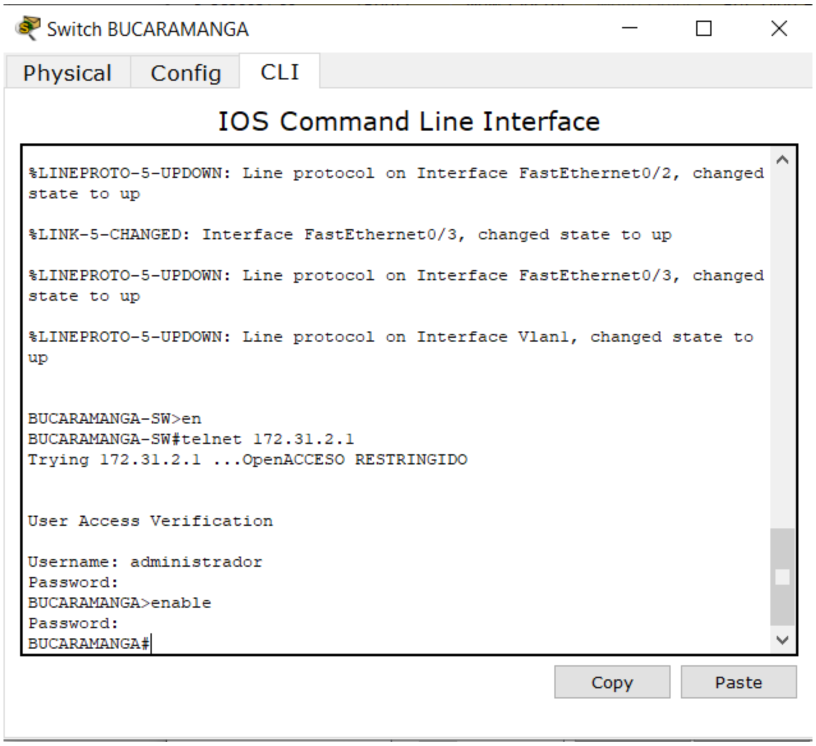
```
Packet Tracer PC Command Line 1.0
PC>ping 172.31.1.66

Pinging 172.31.1.66 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 172.31.1.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Ilustración 83: Prueba desde PC8

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

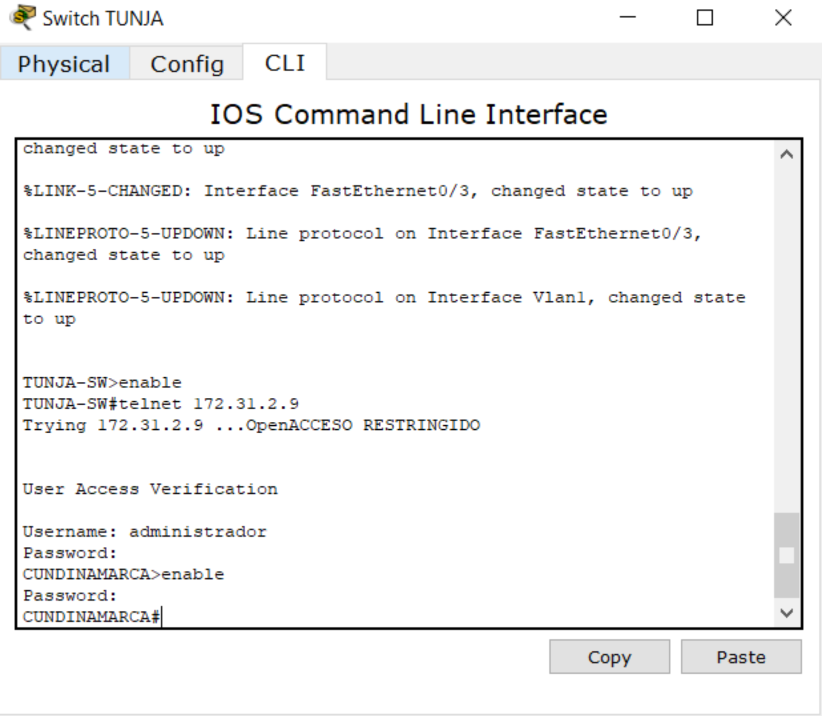
```
ACCESO RESTRINGIDO

User Access Verification

Username: administrador

Password:

BUCARAMANGA>enable

Password:

BUCARAMANGA#config t

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

BUCARAMANGA(config)#int f0/0.10

BUCARAMANGA(config-subif)#access-list 3 permit 172.31.2.0 0.0.0.7
BUCARAMANGA(config)#access-list 3 permit 172.3.2.8 0.0.0.7
BUCARAMANGA(config)#access-list 3 permit 172.31.2.8 0.0.0.7
BUCARAMANGA(config)#line vty 0 15
BUCARAMANGA(config-line)#access-class 3 in
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#

ACCESO RESTRINGIDO
User Access Verification
Username: administrador
Password:
TUNJA>enable
Password:
TUNJA#config t
Enter configuration commands, one per line.  End with CNTL/Z.
TUNJA(config)#int f0/0.20
TUNJA(config-subif)#access-list 3 permit 172.31.2.0 0.0.0.7
TUNJA(config)#access-list 3 permit 172.3.2.8 0.0.0.7
TUNJA(config)#access-list 3 permit 172.31.2.8 0.0.0.7
TUNJA(config)#line vty 0 15
TUNJA(config-line)#access-class 3 in
TUNJA(config-line)#exit
TUNJA(config)#exit
TUNJA#
```

```
%SYS-5-CONFIG_I: Configured from console by console
TUNJA#

ACCESO RESTRINGIDO

User Access Verification
Username: administrador
Password:
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#config t
Enter configuration commands, one per line.  End with CNTL/Z.
CUNDINAMARCA(config)#int f0/0.20
CUNDINAMARCA(config-subif)#access-list 3 permit 172.31.2.0 0.0.0.7
CUNDINAMARCA(config)#access-list 3 permit 172.3.2.8 0.0.0.7
CUNDINAMARCA(config)#access-list 3 permit 172.31.2.8 0.0.0.7
CUNDINAMARCA(config)#line vty 0 15
CUNDINAMARCA(config-line)#access-class 3 in
CUNDINAMARCA(config-line)#exit
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
CUNDINAMARCA#
```



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed
state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to
up


BUCARAMANGA-SW>en
BUCARAMANGA-SW#telnet 172.31.2.1
Trying 172.31.2.1 ...OpenACCESO RESTRINGIDO


User Access Verification

Username: administrador
Password:
BUCARAMANGA>enable
Password:
BUCARAMANGA#
```

Ilustración 84: Prueba desde Switch BUCARAMANGA



```
changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
to up


TUNJA-SW>enable
TUNJA-SW#telnet 172.31.2.9
Trying 172.31.2.9 ...OpenACCESO RESTRINGIDO


User Access Verification

Username: administrador
Password:
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#
```

Ilustración 85: Prueba desde Switch TUNJA

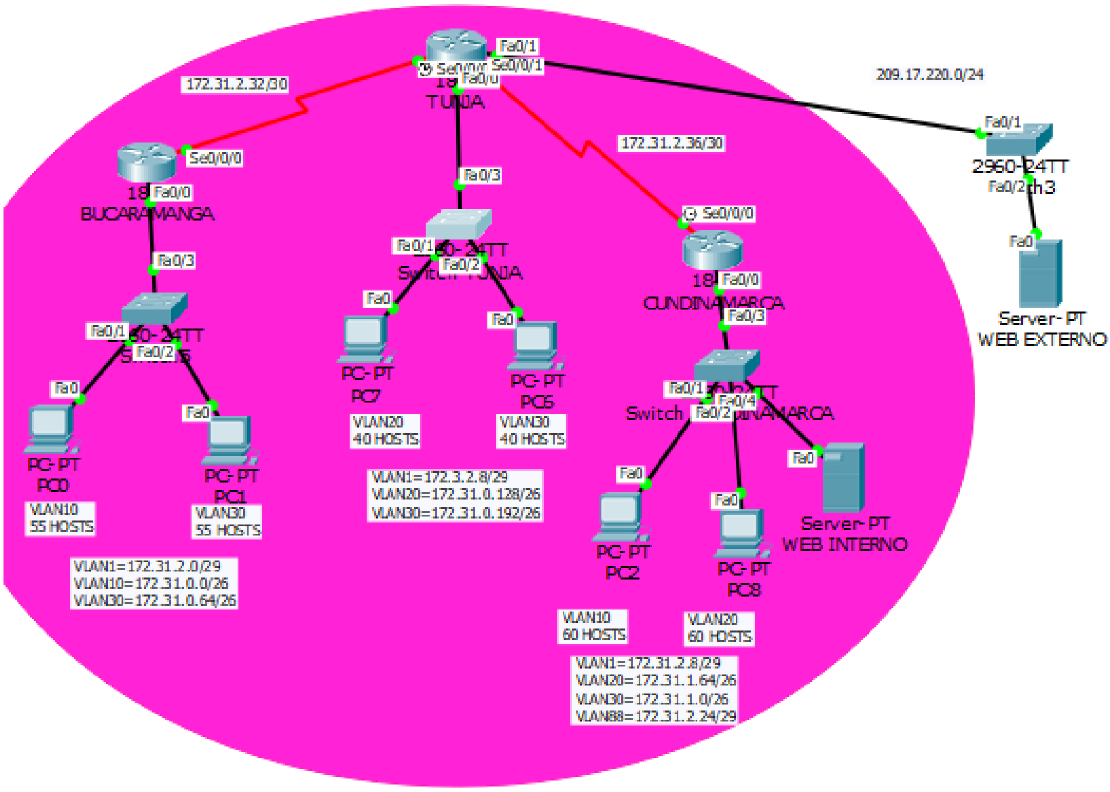


Ilustración 86: Comunicación Final Escenario 2

CONCLUSIONES

- Packet Tracer es la herramienta de aprendizaje y simulación de redes interactiva que permite crear topologías de red, configurar dispositivos, insertar paquetes, simular e interactuar con dispositivos finales como PC`s o intermedios (host) como Swich y Routers. Además de una gran variedad de medios de transmisión en redes LAN y WAN soportando múltiples protocolos como por ejemplo, HTTP, TCP/IP, Telnet, SSH, TFTP, DHCP y DNS 2. TCP/UDP, IPv4, IPv6, Ethernet 802.3 y 802.11.

- Al desarrollar esta actividad se puede concluir que, existen protocolos sencillos y fáciles de implementar, los cuales ayudan a asignar un hostname, como también unas contraseñas de consola y del modo EXEC privilegiado las direcciones Ip de las diferentes interfaces de los distintos dispositivos que conforman una red; haciendo énfasis en el router, donde se pueden usar protocolos para enrutar y comunicar a diferentes redes, tanto LAN como WAN.

- Los switches de capa 3 cada vez se hacen más imprescindible en centros de datos, redes empresariales complejas, aplicaciones comerciales e incluso en proyectos avanzados para clientes, ya que puede ejecutar enrutamiento estático y enrutamiento dinámico utilizando una tabla de direcciones MAC y una tabla de enrutamiento o de direcciones IP.

- Los switches de red Cisco están compuestos por una variedad de configuraciones que permiten administrar y Proteger de manera adecuada los sistemas de comunicaciones y los controles de acceso hacia los mismos, manteniendo así un óptimo desempeño y estabilidad den las comunicaciones

- La función Ping es un comando o una herramienta de diagnóstico que permite hacer una verificación del estado de una determinada conexión de un host local con al menos un equipo remoto de la red. Además, nos permite determinar si una dirección IP específica o host es accesible desde la red o no.

- Es muy importante guardar las configuraciones realizadas en una red y almacenarlas como archivos de copia de seguridad en caso de que se produzca un problema. Esto es una forma de proteger el tiempo y el esfuerzo invertidos en configurar un determinado equipo. Los archivos de configuración y los documentos de red se pueden almacenar en un servidor de protocolo trivial de transferencia de archivos (TFTP) o en una unidad USB. Esta práctica es parte fundamental del desarrollo de algún tipo de tolerancia a fallos dentro de la interconexión de redes construida.

BIBLIOGRAFIA

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). 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). 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). 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). Capa de red. Fundamentos de Networking. Recuperado de https://static-course-ssets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1