

DIPLOMADO DE PROFUNDIZACION CISCO (DISEÑO E IMPEMENTACION DE
SOLUCIONES INTEGRADAS LAN/WAN)

JULIAN CAMILO CARDOZO JARAMILLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
PROGRAMA INGENIERIA ELECTRÓNICA
MEDELLIN
2021

DIPLOMADO DE PROFUNDIZACION CISCO (DISEÑO E IMPEMENTACION DE
SOLUCIONES INTEGRADAS LAN/WAN)

INFORME FINAL DE HABILIDADES PRACTICAS CCNA

Presentado por:
JULIAN CAMILO CARDOZO JARAMILLO

Asesorado por
ING. JUAN CARLOS VESGA
ING. NILSON ALBEIRO FERREIRA MANZANARES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
PROGRAMA INGENIERIA ELECTRÓNICA
MEDELLIN
2021

NOTA DE ACEPTACIÓN

Firma del Presidente del jurado

Firma del Jurado

firma del Jurado

TABLA DE CONTENIDO

INTRODUCCIÓN	9
OBJETIVOS.....	10
2.1 Objetivo General	10
2.2. Objetivos específicos	10
3. DESARROLLO DE LOS ESCENARIOS.....	11
3.1 ESEENARIO 1.....	11
3.1.1 Parte 1: Asignación de direcciones IP	11
3.1.1.1 Subneteo	12
3.1.1.2. Dirección IP de la red.....	12
3.1.2. parte 2 Configuración Básica.....	12
3.1.2.1. Completar la siguiente tabla con la configuración básica de los routers, teniendo en cuenta las subredes diseñadas.....	12
3.1.2.2. Tabla de enrutamiento de cada uno de los Routers.....	13
3.1.2.3 Verificar balanceo de carga que presentan los Routers	14
3.1.2.4 realizar un diagnóstico de vecinos usando el comando cdp.....	15
3.1.3 Configuración de enrutamiento	19
3.1.3.1 Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.....	19
3.1.3.2 Verificar si existe vecindad con los routers configurados con EIGRP	20
3.1.3.3 Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas.....	21
3.1.3.4 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.	22
3.1.4 parte 4: Configuración de las listas de control de acceso.....	24
3.1.4.1 Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red	25
3.1.4.2 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.	26
3.1.4.3 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	27
3.1.5 Parte 5: comprobación de la red instalada.....	28
3.1.5.1 se debe comprobar que la configuración de las listas de acceso fue exitosa	28

Para la verificación de las listas de control de acceso se usa el comando show Access-list con esto verificamos que el control de acceso fue exitoso	28
3.1.5.2 Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e	28
3.2 ESCENARIO 2	30
Desarrollo	30
3.2.1 Todos los Routers deberán tener lo siguiente	30
3.2.1.1 configuración básica	30
3.2.1.2 Autenticación Local con AAA	37
3.2.1.3 Cifrado de contraseñas	38
3.2.1.4 Un máximo de internos para acceder al Router.	38
3.2.1.4 Máximo de intentos para acceder al Router	39
3.2.1.5 Máximo de tiempo de acceso al detectar ataques	39
3.2.1.6 Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers	39
3.2.2 El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca	40
3.2.3 El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).....	43
3.2.4 Autenticación del enrutamiento	46
3.2.5 listas de control de acceso	48
3.2.5.1 Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.	48
3.2.5.2 Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja	49
3.2.5.3 Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet....	50
3.2.5.4 Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.	51
3.2.5.5 Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10	52
3.2.5.6 Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20)y Tunja (VLAN 20), no internet	53
3.2.5.7 Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.....	55
3.2.5.8 Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen acceso a los routers e internet.	57
3.2.6 VLSM: utilizar la dirección 172.31.0.0 /18 para el direccionamiento	59
4. CONCLUSIONES	60
5. BIBLIOGRAFIA	61

LISTA DE TABLAS

Tabla 1. subneteo	12
Tabla 2. tabla de configuración básica	12
Tabla 3. Control de acceso	27
Tabla 4. Tabla de control de acceso	29

LISTA DE FIGURAS

Figura 1 – Topología escenario 1.....	11
Figura 2 – diagnóstico de vecinos router Bogotá	15
Figura 3 - diagnóstico de vecinos router Cali	15
Figura 4 Diagnóstico de vecinos router Medellín.....	16
Figura 5 – prueba de conectividad.....	16
Figura 6. Conectividad desde PC1 a PC2.....	17
Figura 7. Conectividad desde PC1 a router medellin	17
Figura 8. Conectividad desde PC2 A PC1	18
Figura 9. Conectividad desde PC4 a PC3.....	18
Figura 10. Conectividad desde PC3 a PC4.....	19
Figura 10. Prueba de conectividad 1.....	23
Figura 11. Prueba de conectividad 2.....	23
Figura 12. Prueba de conectividad 3.....	24
Figura 13. Configuración de las listas de control de acceso.....	24
Figura 14. Prueba de conectividad entre redes.....	25
Figura 15. Topología de red Escenario 2	30
Figura 16. Cifrado de contraseñas.....	38
Figura 17. Servidor TFTP	39
Figura 18. Configuración DHCP.....	41
Figura 19. Configuración DHCP.....	42
Figura 20. Autenticación de enrutamiento.....	47
Figura 21. Autenticación de enrutamiento.....	48
Figura 22. Control e acceso en Cundinamarca	49
Figura 23. Control de Acceso en Cundinamarca no Tunja	50
Figura 24. Control de acceso en Tunja	51
Figura 25. Control de acceso en Tunja	52
Figura 25. Control de acceso en Cundinamarca	53
Figura 26. Control de acceso en Bucaramanga	54
Figura 27. Control de acceso Cundinamarca	56
Figura 28. Acceso de las VLAN	58

RESUMEN

A través de los escenarios propuestos, se fortalecen los conocimientos necesarios para el diseño de redes mediante el uso del modelo jerárquico, con el fin de optimizar el funcionamiento de las redes trabajadas, y se incorpora el uso de tecnologías y protocolos de comunicación y enrutamiento, así mismo, la emisión de comandos que permiten realizar diagnósticos de conexión, configuraciones de seguridad y avanzadas en Routers, para dar soluciones de red y conectividad.

PALABRAS CLAVES: Acceso, Configuración, Enrutamiento, Red, Router.

ABSTRACT

Through the proposed scenarios, the necessary knowledge for the design of networks is strengthened through the use of the hierarchical model, in order to optimize the operation of the networks worked, and the use of communication and routing technologies and protocols is incorporated, likewise, the issuance of commands that allow connection diagnostics, security configurations and advanced routers, to provide network and connectivity solutions

KEYWORDS: Access, Configuration, Routing, Red, Router.

INTRODUCCIÓN

Con este trabajo se pretende mostrar lo que hemos aprendido en este último semestre, manejado la herramienta Packet Tracer, haciendo simulaciones, configurando dispositivos, topologías de red, simulaciones de conectividad entre otros.

Se desarrollarán 2 ejercicios (Escenarios) o problemas relacionados con la configuración y diseños de redes VLAN, enlaces troncales con Switches Cisco, Router y servidores de igual forma que el enrutamiento entre los mismos.

Se realizarán prácticas sobre equipos reales, con el simulador de Cisco Networking Academy y con Packet Tracer; el cual tiene como objetivo la adquisición y la Formalización de habilidades para el mejor acceso a los equipos y realizar una configuración básica de los distintos aspectos físicos(hardware) y lógicos (software).

OBJETIVOS

2.1 Objetivo General

Analizar y dar solución a los dos escenarios propuestos como prueba de habilidades prácticas del Diplomado de profundización Cisco, poniendo en práctica todos los conceptos estudiados y aprendidos en todos los fundamentos importantes como lo son el ruteo y conmutación de las redes que existen en un conocimiento general y global.

2.2. Objetivos específicos

2.2.1. Aplicar las diferentes configuraciones y conocimientos aprendidos en el diplomado para direcciones IP, RIP, encapsulamiento OSFP, DCHP, ACL, NAT, VLANs según lo indicado.

2.2.2. Diseñar un esquema de direccionamiento según los requerimientos de los escenarios 1 y 2. Describir el paso a paso de cada uno de los procedimientos realizados en la solución de los escenarios propuestos para esta actividad.

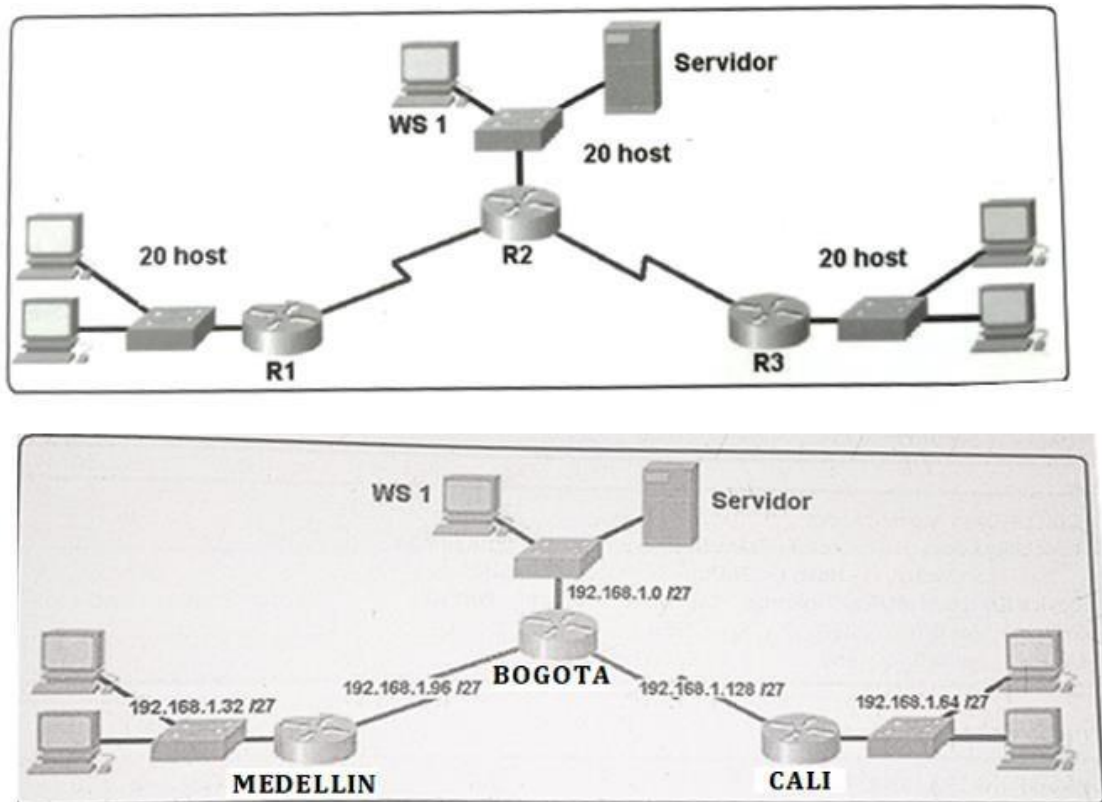
2.2.3. revisar y verificar la conectividad de las configuraciones mediante los comandos ping, tracert, telnet, show ip route, y show ip protocols, en los dos escenarios propuestos para esta práctica final del Diplomado

3. DESARROLLO DE LOS ESCENARIOS

3.1 ESEENARIO 1

Una empresa posee sucursales distribuidas en las ciudades de Bogotá y Medellín, 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.

Figura 1 – Topología escenario 1



Fuente: Guía de actividades prueba de habilidades poractivas Diplomado CCNA

3.1.1 Parte 1: Asignacion de direcciones IP

Para subnetear la red se utiliza la formula 2^n donde n será los números de dígitos del ultimo octeto de la macará 255.255.255.0000. para ello tomamos 3 dígitos de

dicho octeto, quedando como resultado: $2^3 = 8$, lo correcto sería tomarlo a 24 para tener más de 8 subredes dado que de cada red se deben de dejar de utilizar 2 redes que son la dirección de red y la dirección de Broadcast pero siguiendo el gráfico del escenario donde ya hay unas direcciones definidas con una máscara con prefijo 27 se muestra que se utilizó 23 de esa manera se obtienen 8 redes pero se tiene claro que solo será utilizadas 6 redes en total.

3.1.1.1 Subneteo

Tabla 1. subneteo

Subnetting	Network	Broadcast
0	192.168.1.0	192.168.1.31
1	192.168.1.32	192.168.1.63
2	192.168.1.64	192.168.1.95
3	192.168.1.96	192.168.1.127
4	192.168.1.128	192.168.1.159
5	192.168.1.160	192.168.1.191
6	192.168.1.192	192.168.1.223
7	192.168.1.224	192.168.1.255

3.1.1.2. Dirección ip de la red.

Dirección IP a la red: **192.168.1.0/27**

3.1.2. parte 2 Configuración Básica

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

Tabla 2. Tabla de configuración básica

	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	192.168.1.68	192.168.1.130	192.168.1.34
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

Fuente: Guia de actividades prueba de habilidades practicas Diplomado CCNA

3.1.2.2. Tabla de enrutamiento de cada uno de los Routers.

Validación de enrutamiento router Bogotá

Validación de enrutamiento router bogotá

Bogota#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2 E1 - OSPF external type 1, E2 - OSPF
external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-
IS level-2, ia - IS-IS inter

area

* - candidate default, U - per-user static route, o -
ODR P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks
C 192.168.1.0/27 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
D 192.168.1.32/27 [90/2172416] via 192.168.1.99, 00:59:15, Serial0/1/0
D 192.168.1.64/27 [90/2172416] via 192.168.1.131, 00:59:14, Serial0/1/1
C 192.168.1.96/27 is directly connected, Serial0/1/0
L 192.168.1.98/32 is directly connected, Serial0/1/0
C 192.168.1.128/27 is directly connected, Serial0/1/1 L
192.168.1.130/32 is directly connected, Serial0/1/1

Validacion de rutas router medellin

Medellin#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2 E1 - OSPF external type 1, E2 - OSPF
external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-
IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o -
ODR P - periodic downloaded static route

Gateway of last resort is not set

```
192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D 192.168.1.0/27 [90/2172416] via 192.168.1.98, 00:57:09, Serial0/1/0
C 192.168.1.32/27 is directly connected, GigabitEthernet0/0
L 192.168.1.33/32 is directly connected, GigabitEthernet0/0
D 192.168.1.64/27 [90/2684416] via 192.168.1.98, 00:57:08, Serial0/1/0
C 192.168.1.96/27 is directly connected, Serial0/1/0
L 192.168.1.99/32 is directly connected, Serial0/1/0
D 192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:57:09, Serial0/1/0
```

Validacion de rutas router cali

```
Cali#show ip route
```

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

```
Gateway of last resort is not set
```

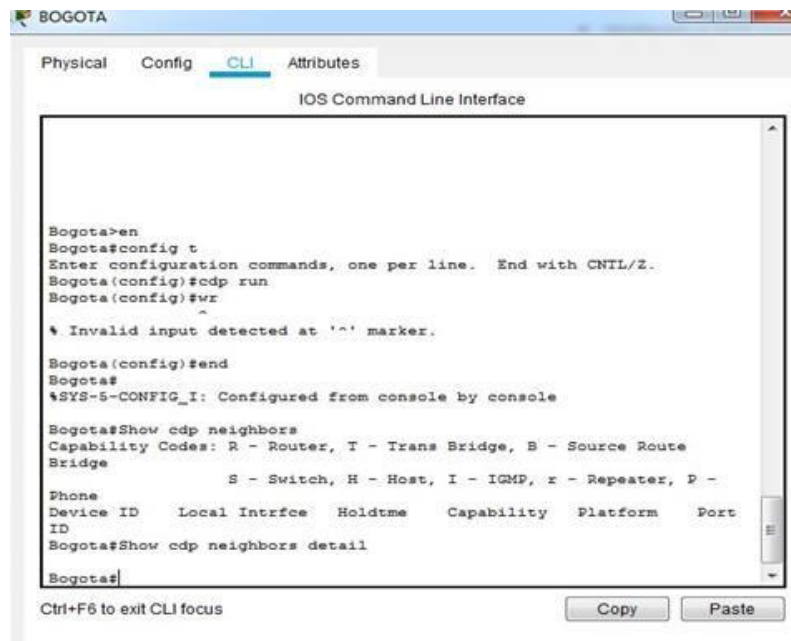
```
192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D 192.168.1.0/27 [90/2172416] via 192.168.1.130, 01:00:17, Serial0/1/0
D 192.168.1.32/27 [90/2684416] via 192.168.1.130, 01:00:17, Serial0/1/0
C 192.168.1.64/27 is directly connected, GigabitEthernet0/0
L 192.168.1.65/32 is directly connected, GigabitEthernet0/0
D 192.168.1.96/27 [90/2681856] via 192.168.1.130, 01:00:17, Serial0/1/0
C 192.168.1.128/27 is directly connected, Serial0/1/0
L 192.168.1.131/32 is directly connected, Serial0/1/0
```

3.1.2.3 Verificar balanceo de carga que presentan los Routers

Para realizar el balanceo se necesita que existan por lo menos dos o más conexiones entre sedes o Routers y como en este caso solo tenemos una conexión por sede o router el balanceo no aplica para este caso.

3.1.2.4 realizar un diagnóstico de vecinos usando el comando cdp

Figura 2 – diagnostico de vecinos router bogotá



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

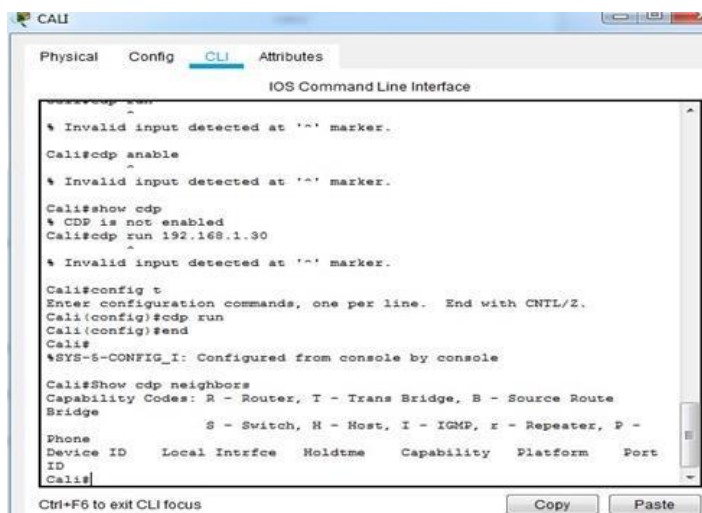
Bogota>en
Bogota#config t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#cdp run
Bogota(config)#vr
^
% Invalid input detected at '^' marker.

Bogota(config)#end
Bogota#
%SYS-5-CONFIG_I: Configured from console by console

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
Bogota#Show cdp neighbors detail
Bogota#
```

Fuente: elaboracion propia

figura 3 - diagnostico de vecinos router cali



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

% Invalid input detected at '^' marker.
Cali#cdp enable
^
% Invalid input detected at '^' marker.

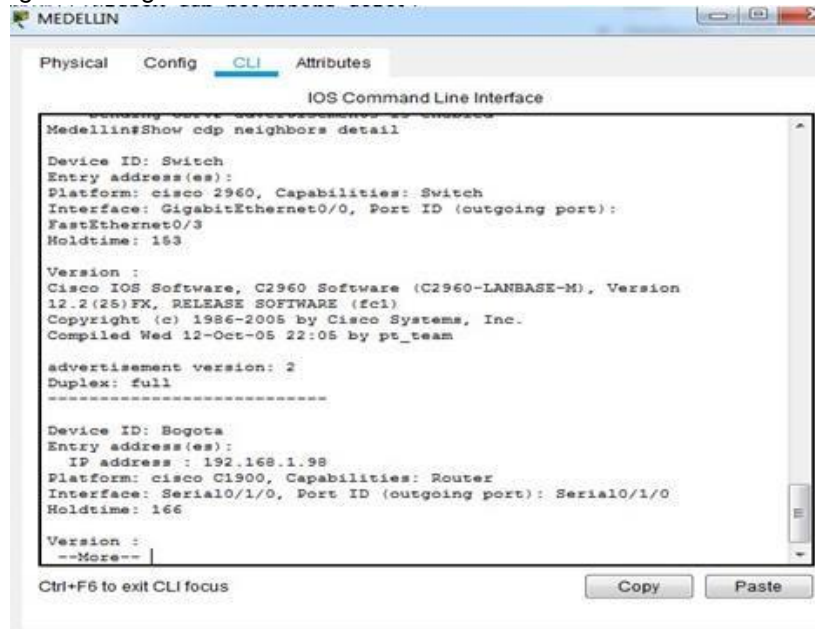
Cali#show cdp
% CDP is not enabled
Cali#cdp run 192.168.1.30
^
% Invalid input detected at '^' marker.

Cali#config t
Enter configuration commands, one per line. End with CNTL/Z.
Cali(config)#cdp run
Cali(config)#end
Cali#
%SYS-5-CONFIG_I: Configured from console by console

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
Cali#
```

Fuente: elaboracion propia

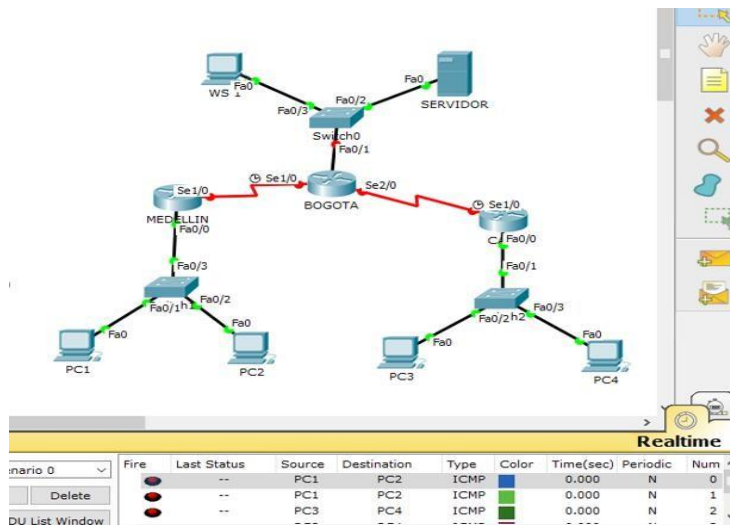
Figura 4 Diagnóstico de vecinos router Medellín



Fuente: elaboración propia

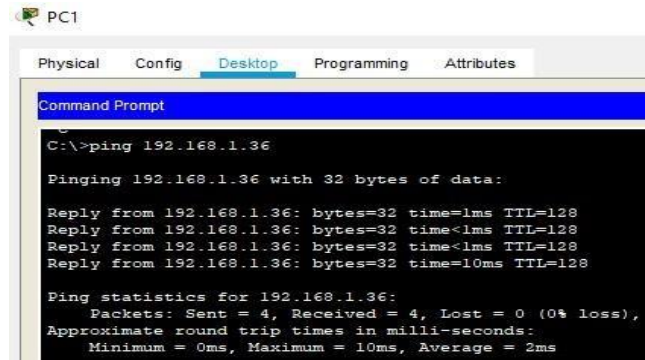
3.1.2.5 prueba de conectividad

Figura 5 – prueba de conectividad



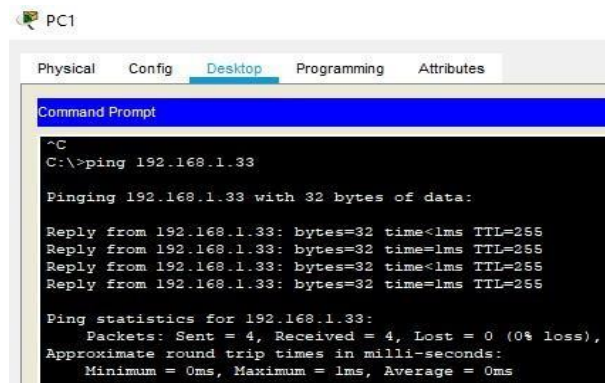
Fuente: elaboración propia

figura 6. Conectividad desde PC1 a PC2



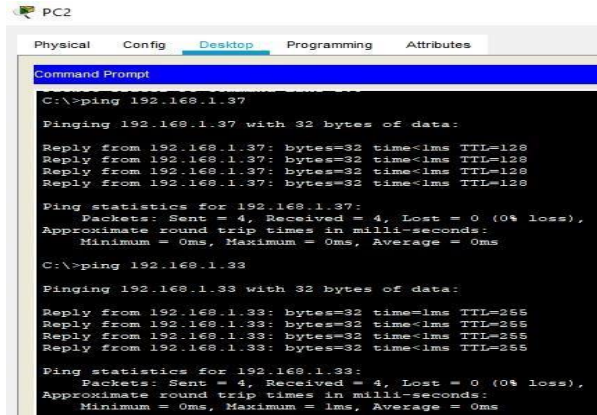
Fuente: elaboración propia

Figura 7. Conectividad desde PC1 a router medellin



Fuente: elaboración propia

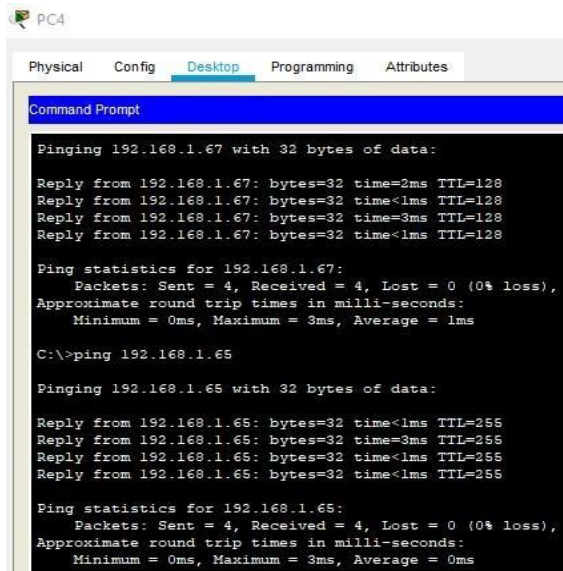
Figura 8. Conectividad desde PC2 A PC1



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.1.37
Pinging 192.168.1.37 with 32 bytes of data:
Reply from 192.168.1.37: bytes=32 time<1ms TTL=128
Reply from 192.168.1.37: bytes=32 time<1ms TTL=128
Reply from 192.168.1.37: bytes=32 time<1ms TTL=128
Reply from 192.168.1.37: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.37:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 192.168.1.33
Pinging 192.168.1.33 with 32 bytes of data:
Reply from 192.168.1.33: bytes=32 time<1ms TTL=255
Reply from 192.168.1.33: bytes=32 time<1ms TTL=255
Reply from 192.168.1.33: bytes=32 time<1ms TTL=255
Reply from 192.168.1.33: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Fuente: Elaboracion propia

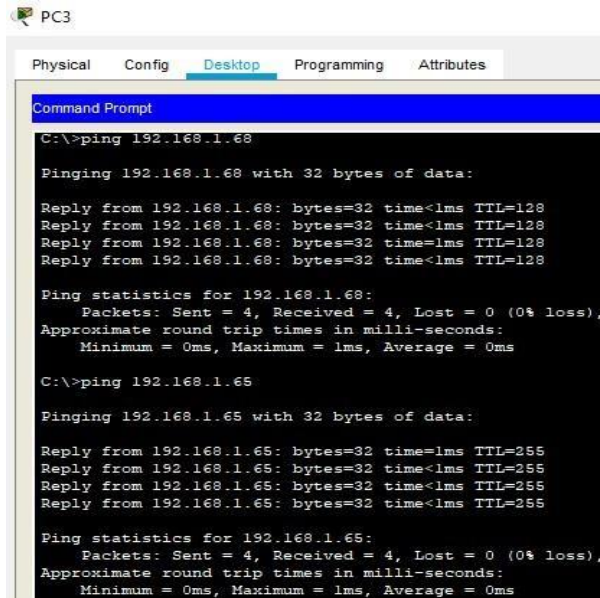
Figura 9. Conectividad desde PC4 a PC3



```
PC4
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 192.168.1.67 with 32 bytes of data:
Reply from 192.168.1.67: bytes=32 time=2ms TTL=128
Reply from 192.168.1.67: bytes=32 time<1ms TTL=128
Reply from 192.168.1.67: bytes=32 time=3ms TTL=128
Reply from 192.168.1.67: bytes=32 time<1ms 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 = 3ms, Average = 1ms
C:\>ping 192.168.1.65
Pinging 192.168.1.65 with 32 bytes of data:
Reply from 192.168.1.65: bytes=32 time<1ms TTL=255
Reply from 192.168.1.65: bytes=32 time=3ms TTL=255
Reply from 192.168.1.65: bytes=32 time<1ms TTL=255
Reply from 192.168.1.65: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.1.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

Fuente:Elaboracion Propia

Figura 10. Conectividad desde PC3 a PC4



```
PC3
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.1.68

Pinging 192.168.1.68 with 32 bytes of data:
Reply from 192.168.1.68: bytes=32 time<1ms TTL=128
Reply from 192.168.1.68: bytes=32 time<1ms TTL=128
Reply from 192.168.1.68: bytes=32 time<1ms TTL=128
Reply from 192.168.1.68: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.68:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.65

Pinging 192.168.1.65 with 32 bytes of data:
Reply from 192.168.1.65: bytes=32 time<1ms TTL=255
Reply from 192.168.1.65: bytes=32 time<1ms TTL=255
Reply from 192.168.1.65: bytes=32 time<1ms TTL=255
Reply from 192.168.1.65: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Fuente: Elaboracion propia

3.1.3 Configuración de enrutamiento

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

Router MEDELLIN

```
MEDELLIN(config)#int S0/0/0
MEDELLIN(config-if)#clock rate 64000
MEDELLIN(config-if)#exit
MEDELLIN(config)#router eigrp 200
MEDELLIN(config-router)#network 192.168.1.0 0.0.0.255
MEDELLIN(config-router)#no auto-summary
MEDELLIN(config-router)#end
```

Router BOGOTA

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

```
BOGOTA(config-router)#network 192.168.1.0 0.0.0.255
BOGOTA(config-roter)#no auto-summary
BOGOTA(config-router)#end
```

Router CALI

```
CALIconfig)#int S0/0/0
CALI(config-if)#clock rate 64000
CALI(config-if)#exit
CALI(config)#router eigrp 200
CALI(config-router)#network 192.168.1.0 0.0.0.255
CALI(config-router)#no auto-summary
CALI(config-router)#end
```

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

Para verificar vecindad entre router se utiliza el comando. **show ip eigrp neighbors**

```
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 Se0/1/0 13 00:14:11 40 1000 0 7
  1   192.168.1.131 Se0/1/1 11 00:06:24 40 1000 0 7
```

```
Medellin>en
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 Se0/1/0 13 00:17:00 40 1000 0 5
```

```
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 Se0/1/0 13 00:10:17 40 1000 0 6
```

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

Para verificar las tablas de enrutamiento se utiliza el comando: **ip route**

Tablas de enrutamiento router **Medellín**

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D 192.168.1.0/27 [90/2172416] via 192.168.1.98, 00:24:48, Serial0/1/0
C 192.168.1.32/27 is directly connected, GigabitEthernet0/0
L 192.168.1.33/32 is directly connected, GigabitEthernet0/0
D 192.168.1.64/27 [90/2684416] via 192.168.1.98, 00:17:01, Serial0/1/0
C 192.168.1.96/27 is directly connected, Serial0/1/0
L 192.168.1.99/32 is directly connected, Serial0/1/0
D 192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:24:48,

Tablas de enrutamiento router **Bogotá**

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

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

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 8 subnets, 2 masks

```
C 192.168.1.0/27 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
D 192.168.1.32/27 [90/2172416] via 192.168.1.99, 00:25:42, Serial0/1/0
D 192.168.1.64/27 [90/2172416] via 192.168.1.131, 00:17:55, Serial0/1/1
C 192.168.1.96/27 is directly connected, Serial0/1/0
L 192.168.1.98/32 is directly connected, Serial0/1/0
C 192.168.1.128/27 is directly connected, Serial0/1/1
L 192.168.1.130/32 is directly connected, Serial0/1/1
```

Tablas de enrutamiento router **Cali**

```
Cali#show ip route
```

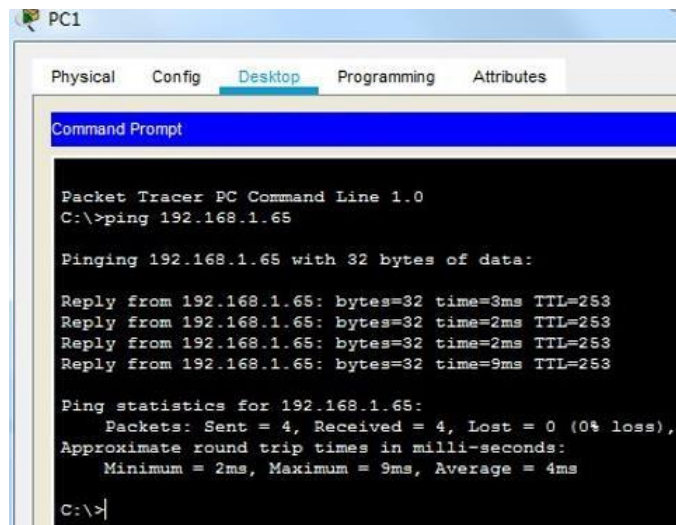
```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2 E1 - OSPF external type 1, E2 - OSPF
external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 -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

```
Gateway of last resort is not set
```

```
192.168.1.0/24 is variably subnetted, 7 subnets, 2 masks
D 192.168.1.0/27 [90/2172416] via 192.168.1.130, 00:13:14, Serial0/1/0
D 192.168.1.32/27 [90/2684416] via 192.168.1.130, 00:13:14, Serial0/1/0
C 192.168.1.64/27 is directly connected, Gi
gabitEthernet0/0
L 192.168.1.65/32 is directly connected, GigabitEthernet0/0
D 192.168.1.96/27 [90/2681856] via 192.168.1.130, 00:13:14, Serial0/1/0
C 192.168.1.128/27 is directly connected, Serial0/1/0
L 192.168.1.131/32 is directly connected, Serial0/1/0
```

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

Figura 10. Prueba de conectividad 1



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.65

Pinging 192.168.1.65 with 32 bytes of data:

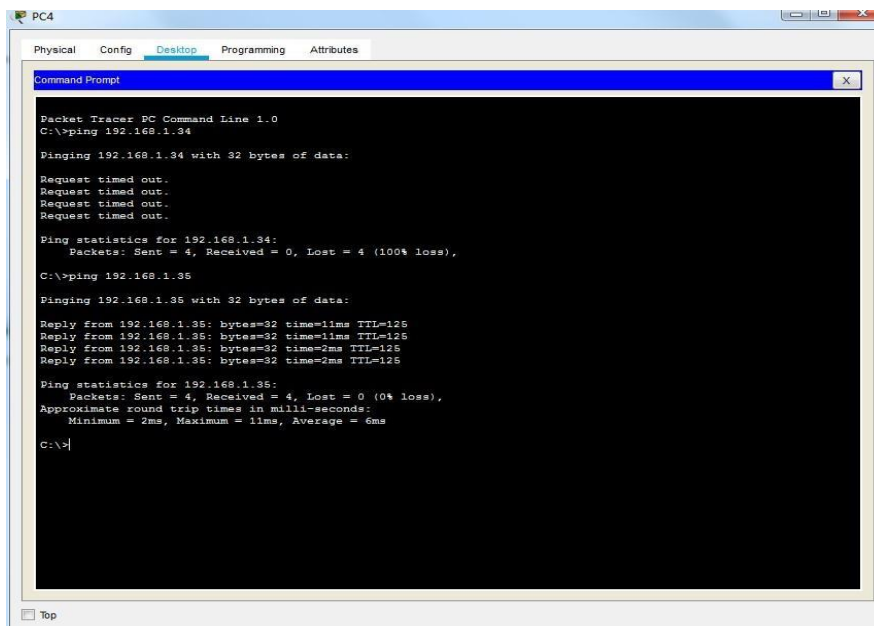
Reply from 192.168.1.65: bytes=32 time=3ms TTL=253
Reply from 192.168.1.65: bytes=32 time=2ms TTL=253
Reply from 192.168.1.65: bytes=32 time=2ms TTL=253
Reply from 192.168.1.65: bytes=32 time=9ms TTL=253

Ping statistics for 192.168.1.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 9ms, Average = 4ms

C:\>
```

Fuente: Elaboracion propia

Figura 11. Prueba de conectividad 2



```
PC4
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.34

Pinging 192.168.1.34 with 32 bytes of data:

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

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

C:\>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:

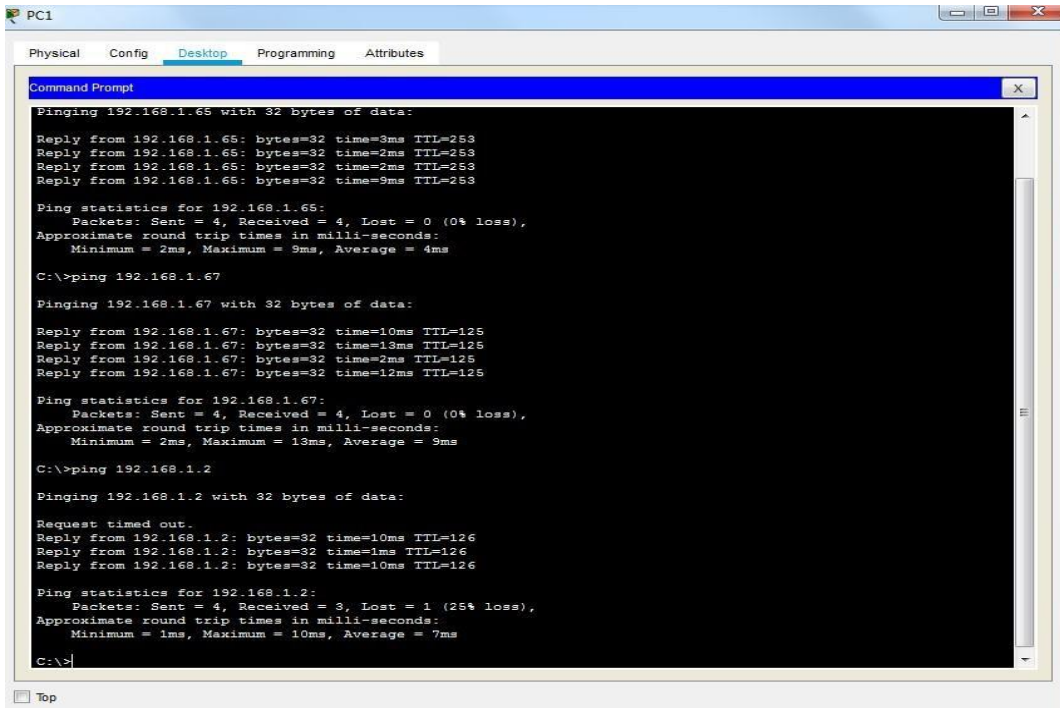
Reply from 192.168.1.35: bytes=32 time=11ms TTL=125
Reply from 192.168.1.35: bytes=32 time=2ms TTL=125
Reply from 192.168.1.35: bytes=32 time=2ms TTL=125
Reply from 192.168.1.35: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 11ms, Average = 6ms

C:\>
```

Fuente: Elaboracion propia

Figura 12. Prueba de conectividad 3



Fuente: Elaboración propia

3.1.4 parte 4: Configuración de las listas de control de acceso

Figura 13. Configuración de las listas de control de acceso

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC2	CALI	ICMP		0.000	N	16	(edit)	(delete)
	Successful	PC4	MEDELLIN	ICMP		0.000	N	19	(edit)	(delete)
	Successful	PC3	PC4	ICMP		0.000	N	20	(edit)	(delete)
	Successful	PC1	PC2	ICMP		0.000	N	21	(edit)	(delete)

Fuente: elaboracion propia

Figura 14. Prueba de conectividad entre redes

```
C:\>ping 192.168.1.131

Pinging 192.168.1.131 with 32 bytes of data:

Reply from 192.168.1.131: bytes=32 time=3ms TTL=253
Reply from 192.168.1.131: bytes=32 time=3ms TTL=253
Reply from 192.168.1.131: bytes=32 time=7ms TTL=253
Reply from 192.168.1.131: bytes=32 time=6ms TTL=253

Ping statistics for 192.168.1.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 7ms, Average = 4ms
```

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

```
MEDELLIN>en
MEDELLIN#conf t
MEDELLIN(config)# access-list 101 permit tcp any host 192.168.1.131 eq
20
MEDELLIN(config)# access-list 101 permit tcp any host 192.168.1.131 eq
80
MEDELLIN(config)# access-list 101 permit tcp any host 192.168.1.98 eq
20
MEDELLIN(config)# access-list 101 permit tcp any host 192.168.1.98 eq
80
MEDELLIN(config)# access-list 101 permit tcp any host 192.168.1.130 eq
20
MEDELLIN(config)# access-list 101 permit tcp any host 192.168.1.130 eq
80
MEDELLIN(config)# access-list 102 permit tcp any host 192.168.1.99 eq
20 MEDELLIN(config)# access-list 102 permit tcp any host 192.168.1.99
eq 80

BOGOTA>en
BOGOTA#conf t
BOGOTA(config)# access-list 101 permit tcp any host 192.168.1.99 eq 20
BOGOTA(config)# access-list 101 permit tcp any host 192.168.1.131 eq
20
BOGOTA(config)# access-list 101 permit tcp any host 192.168.1.99 eq 80
```

```
BOGOTA(config)# access-list 101 permit tcp any host 192.168.1.131 eq 80
```

```
BOGOTA(config)# access-list 102 permit tcp any host 192.168.1.98 eq 20
```

```
BOGOTA(config)# access-list 102 permit tcp any host 192.168.1.130 eq 20
```

```
CALI>en
```

```
CALI#conf t
```

```
CALI(config)# access-list 101 permit tcp any host 192.168.1.99 eq 20
```

```
CALI(config)# access-list 101 permit tcp any host 192.168.1.130 eq 20
```

```
CALI(config)# access-list 101 permit tcp any host 192.168.1.99 eq 80
```

```
CALI(config)# access-list 101 permit tcp any host 192.168.1.130 eq 80
```

```
CALI(config)# access-list 101 permit tcp any host 192.168.1.99 eq 80
```

```
CALI(config)# access-list 101 permit tcp any host 192.168.1.98 eq 20
```

```
CALI(config)# access-list 102 permit tcp any host 192.168.1.131 eq 20
```

```
CALI(config)# access-list 102 permit tcp any host 192.168.1.131 eq 20
```

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

```
BOGOTA (config)# access-list 103 permit tcp any host 192.168.1.70 eq 20
```

```
BOGOTA (config)# access-list 104 deny tcp any host 192.168.1.40 eq 20
```

```
MEDELLIN(config)# access-list 103 permit tcp any host 192.168.1.70 eq 20
```

```
MEDELLIN(config)# access-list 104 deny tcp any host 192.168.1.40 eq 20
```

```
CALI(config)# access-list 103 permit tcp any host 192.168.1.70 eq 20
```

```
CALI(config)# access-list 104 permit tcp any host 192.168.1.70 eq 20
```

Tabla 3. Control de acceso

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	Establecido
	WS_1	Router BOGOTA	Denegado
	Servidor	Router CALI	Establecido
	Servidor	Router MEDELLIN	Establecido
TELNET	LAN del Router MEDELLIN	Router CALI	Denegado
	LAN del Router CALI	Router CALI	Establecido
	LAN del Router MEDELLIN	Router MEDELLIN	Establecido
	LAN del Router CALI	Router MEDELLIN	Denegado
PING	LAN del Router CALI	WS_1	Establecido
	LAN del Router MEDELLIN	WS_1	Establecido
	LAN del Router MEDELLIN	LAN del Router CALI	Establecido
PING	LAN del Router CALI	Servidor	Establecido
	LAN del Router MEDELLIN	Servidor	Establecido
	Servidor	LAN del Router MEDELLIN	Establecido
	Servidor	LAN del Router CALI	Establecido
	Router CALI	LAN del Router MEDELLIN	Establecido
	Router MEDELLIN	LAN del Router CALI	Establecido

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

```

CALI(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 host
192.168.1.2
CALI(config)#access-list 110 permit icmp any echo-reply
CALI(config)#access-list 110 deny ip any

```

3.1.5 Parte 5: comprobacion de la red instalada

3.1.5.1 se debe comprobar que la configuracion de las listas de acceso fue exitosa

Para la verificacion de las listas de control de acceso se usa el comando show Access-list con esto verificamos que el control de acceso fue exitoso

```
MEDELLIN#show Access-list
Extended IP access list Server-PT
10 permit ip any host 192.168.1.3
20 permit ip any host 192.168.1.33
30 permit ip any host 192.168.1.98
40 permit ip any host 192.168.1.131
```

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

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

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

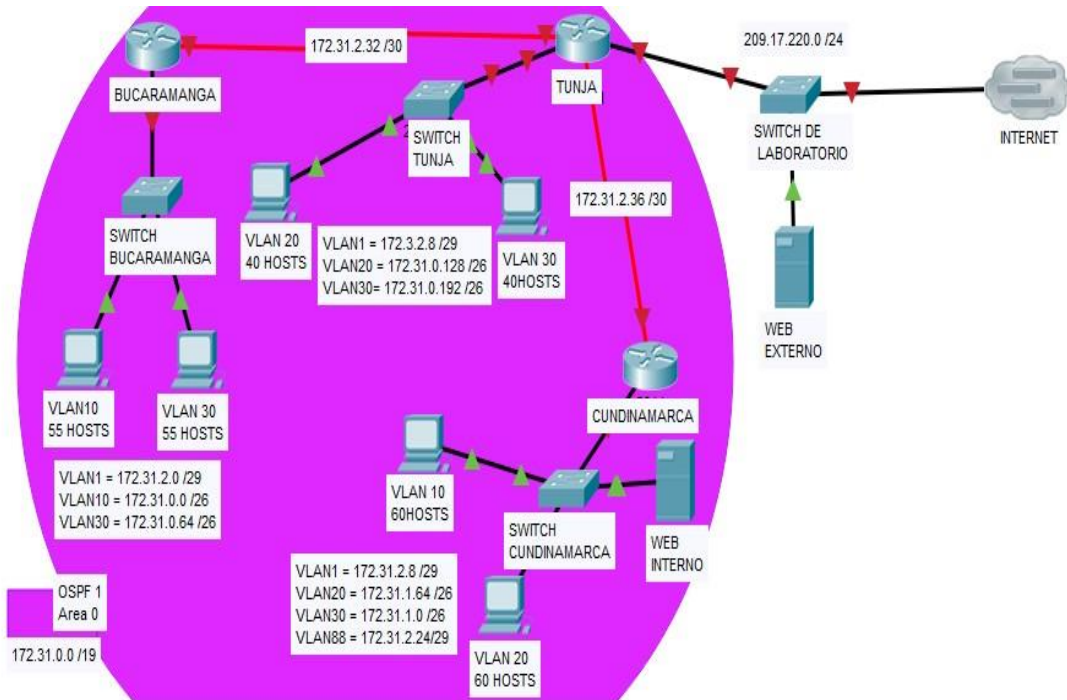
Tabla 4. Tabla de control de acceso

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	Acceso Ok
	WS_1	Router BOGOTA	Acceso Ok
	Servidor	Router CALI	Acceso Ok
	Servidor	Router MEDELLIN	Acceso Ok
TELNET	LAN del Router MEDELLIN	Router CALI	Acceso denegado
	LAN del Router CALI	Router CALI	Acceso Ok
	LAN del Router MEDELLIN	Router MEDELLIN	Acceso Ok
	LAN del Router CALI	Router MEDELLIN	Acceso denegado
PING	LAN del Router CALI	WS_1	Acceso denegado
	LAN del Router MEDELLIN	WS_1	Acceso denegado
	LAN del Router MEDELLIN	LAN del Router CALI	Acceso denegado
	LAN del Router CALI	Servidor	Acceso Ok Acceso Ok
PING	LAN del Router MEDELLIN	Servidor	Ok
	Servidor	LAN del Router MEDELLIN	Acceso Ok
	Servidor	LAN del Router CALI	Acceso Ok
	Router CALI	LAN del Router MEDELLIN	Acceso Ok
	Router MEDELLIN	LAN del Router CALI	Acceso Ok

3.2 ESCENARIO 2

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

Figura 15. Topología de red Escenario 2



Fuente Guía prueba de habilidades prácticas –diplomado CCNA CISCO

Desarrollo

3.2.1 Todos los Routers deberán tener lo siguiente:

3.2.1.1 configuración básica

Router Bucaramanga

```
Router>en  
Router#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#hostname BUCARAMANGA
```

```
BUCARAMANGA(config)#no ip domain-lookup
BUCARAMANGA(config)#service password-
encryption BUCARAMANGA(config)#banner
motd # Enter TEXT message. End with the
character '#'.

```

ACCESO NO AUTORIZADO !

#

```
BUCARAMANGA(config)#enable secret class1
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#password cisco1
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#line vty 0 4
BUCARAMANGA(config-line)#password cisco1
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#int g0/0.1
BUCARAMANGA(config-subif)#encapsulation dot1q 1
BUCARAMANGA(config-subif)#ip address 172.31.2.1 255.255.255.248
BUCARAMANGA(config-subif)#int g0/0.10
BUCARAMANGA(config-subif)#encapsulation dot1q 10
BUCARAMANGA(config-subif)#ip address 172.31.0.1 255.255.255.192
BUCARAMANGA(config-subif)#int g0/0.30
BUCARAMANGA(config-subif)#encapsulation dot1q 30
BUCARAMANGA(config-subif)#ip address 172.31.0.65 255.255.255.192
BUCARAMANGA(config-subif)#int g0/0
BUCARAMANGA(config-if)#no shutdown

```

```
BUCARAMANGA(config-if)#

```

```
BUCARAMANGA(config-if)#int s0/0/0
BUCARAMANGA(config-if)#ip address 172.31.2.34 255.255.255.252
BUCARAMANGA(config-if)#no shut

```

Switch Bucaramanga

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SWITCH-BUCARAMANGA
SWITCH-BUCARAMANGA(config)#vlan 1
SWITCH-BUCARAMANGA(config-vlan)#vlan          10          SWITCH-
BUCARAMANGA(config-vlan)#vlan 30

```

```
SWITCH-BUCARAMANGA(config-vlan)#int f0/10
SWITCH-BUCARAMANGA(config-if)#switchport mode access
SWITCH-BUCARAMANGA(config-if)#
SWITCH-BUCARAMANGA(config-if)#switchport access vlan 10
SWITCH-BUCARAMANGA(config-if)#int f0/14
SWITCH-BUCARAMANGA(config-if)#switchport mode access
SWITCH-BUCARAMANGA(config-if)#switchport access vlan 30
SWITCH-BUCARAMANGA(config-if)#int g0/1
SWITCH-BUCARAMANGA(config-if)#switchport mode trunk
```

```
SWITCH-BUCARAMANGA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
```

```
SWITCH-BUCARAMANGA(config-if)#int vlan 1
SWITCH-BUCARAMANGA(config-if)#ip address 172.31.2.3 255.255.255.248
SWITCH-BUCARAMANGA(config-if)#no shutdown
```

```
SWITCH-BUCARAMANGA(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
```

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

```
SWITCH-BUCARAMANGA(config-if)#ip default-gateway 172.31.2.1
```

Router Tunja

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname TUNJA
TUNJA(config)#no ip domain-lookup
TUNJA(config)#service password-encryption
TUNJA(config)#banner motd #
Enter TEXT message. End with the character '#'.

```

ACCESO NO AUTORIZADO !

#

```
TUNJA(config)#enable secret class1
TUNJA(config)#line console 0
TUNJA(config-line)#password cisco1
TUNJA(config-line)#login
TUNJA(config-line)#line vty 0 4
TUNJA(config-line)#password cisco1
TUNJA(config-line)#login
TUNJA(config-line)#int g0/0.1
TUNJA(config-subif)#encapsulation dot1q 1
TUNJA(config-subif)#ip address 172.3.2.9 255.255.255.248
TUNJA(config-subif)#int g0/0.20
TUNJA(config-subif)#encapsulation dot1q 20
TUNJA(config-subif)#ip address 172.31.0.129 255.255.255.192
TUNJA(config-subif)#int g0/0.30
TUNJA(config-subif)#encapsulation dot1q 30
TUNJA(config-subif)#ip address 172.31.0.193 255.255.255.192
TUNJA(config-subif)#int g0/0
TUNJA(config-if)#no shutdown
```

```
TUNJA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, 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)#int s0/0/1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up
```

```
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 g0/1
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 GigabitEthernet0/1, changed state to up
TUNJA#

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

Switch Tunja

Switch>en

Switch#conf t

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

Switch(config)#hostname SWITCH-TUNJA

SWITCH-TUNJA(config)#vlan 1

SWITCH-TUNJA(config-vlan)#vlan 20 SWITCH-TUNJA(config-
vlan)#vlan 30

SWITCH-TUNJA(config-vlan)#int f0/10

SWITCH-TUNJA(config-if)#switchport mode access

SWITCH-TUNJA(config-if)#switchport access vlan 20

SWITCH-TUNJA(config-if)#int f0/14

SWITCH-TUNJA(config-if)#switchport mode access

SWITCH-TUNJA(config-if)#switchport access vlan 30

SWITCH-TUNJA(config-if)#int g0/1

SWITCH-TUNJA(config-if)#switchport mode trunk

SWITCH-TUNJA(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

SWITCH-TUNJA(config-if)#int vlan 1

SWITCH-TUNJA(config-if)#ip address 172.3.2.11 255.255.255.248

SWITCH-TUNJA(config-if)#no shutdown

Router Cundinamarca

Router>en

Router#conf t

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

Router(config)#hostname CUNDINAMARCA

CUNDINAMARCA(config)#no ip domain-lookup

CUNDINAMARCA(config)#service password-encryption

CUNDINAMARCA(config)#banner motd # Enter TEXT
message. End with the character '#'.
#

ACCESO NO AUTORIZADO !

#

```
CUNDINAMARCA(config)#enable secret class1
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#password cisco1
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#line vty 0 4
CUNDINAMARCA(config-line)#password cisco1
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#int g0/0.1
CUNDINAMARCA(config-subif)#encapsulation dot1q 1
CUNDINAMARCA(config-subif)#ip address 172.31.2.9 255.255.255.248
CUNDINAMARCA(config-subif)#int g0/0.20
CUNDINAMARCA(config-subif)#encapsulation dot1q 20
CUNDINAMARCA(config-subif)#ip address 172.31.1.65 255.255.255.192
CUNDINAMARCA(config-subif)#int g0/0.30
CUNDINAMARCA(config-subif)#encapsulation dot1q 30
CUNDINAMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192
CUNDINAMARCA(config-subif)#int g0/0.88
CUNDINAMARCA(config-subif)#encapsulation dot1q 88
CUNDINAMARCA(config-subif)#ip address 172.31.2.25 255.255.255.248
CUNDINAMARCA(config-subif)#int g0/0
CUNDINAMARCA(config-if)#no shutdown

CUNDINAMARCA(config-if)#

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

Switch Cundinamarca

```
witch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SWITCH-CUNDINAMARCA
SWITCH-CUNDINAMARCA(config)#vlan 1
SWITCH-CUNDINAMARCA(config-vlan)#vlan 20
SWITCH-CUNDINAMARCA(config-vlan)#vlan 30
SWITCH-CUNDINAMARCA(config-vlan)#vlan 88
SWITCH-CUNDINAMARCA(config-vlan)#exit
SWITCH-CUNDINAMARCA(config)#int f0/10
SWITCH-CUNDINAMARCA(config-if)#switchport mode access
SWITCH-CUNDINAMARCA(config-if)#switchport access vlan 20
SWITCH-CUNDINAMARCA(config-if)#int f0/14
SWITCH-CUNDINAMARCA(config-if)#switchport mode access
SWITCH-CUNDINAMARCA(config-if)#switchport access vlan 30
SWITCH-CUNDINAMARCA(config-if)#int f0/20
SWITCH-CUNDINAMARCA(config-if)#switchport mode access
SWITCH-CUNDINAMARCA(config-if)#switchport access vlan 88
SWITCH-CUNDINAMARCA(config-if)#int g0/1
SWITCH-CUNDINAMARCA(config-if)#switchport mode trunk

SWITCH-CUNDINAMARCA(config-if)#

SWITCH-CUNDINAMARCA(config-if)#int vlan 1
SWITCH-CUNDINAMARCA(config-if)#ip          address          172.31.2.11
255.255.255.248 SWITCH-CUNDINAMARCA(config-if)#no shutdown

SWITCH-CUNDINAMARCA(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

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

SWITCH-CUNDINAMARCA(config-if)#ip default-gateway 172.31.2.9
SWITCH-CUNDINAMARCA(config)#
```

3.2.1.2 Autenticacion Local con AAA

Router Bucaramanga

```
BUCARAMANGA>en
```

```
Password:
```

```
BUCARAMANGA#conf t
```

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

```
BUCARAMANGA(config)#username admin secret 123
```

```
BUCARAMANGA(config)#aaa new-model
```

```
BUCARAMANGA(config)#aaa authentication login AAA-LOGIN local
```

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

```
BUCARAMANGA(config-line)#login authentication AAA-LOGIN
```

```
BUCARAMANGA(config-line)#line vty 0 4
```

```
BUCARAMANGA(config-line)#login authentication AAA-LOGIN
```

Router Tunja

```
TUNJA>en Password:
```

```
TUNJA#conf t
```

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

```
TUNJA(config)#username admin secret 123
```

```
TUNJA(config)#aaa new-model
```

```
TUNJA(config)#aaa authentication login AAA-LOGIN local
```

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

```
TUNJA(config-line)#login authentication AAA-LOGIN
```

```
TUNJA(config-line)#line vty 0 4
```

```
TUNJA(config-line)#login authentication AAA-LOGIN
```

Router Cundinamarca

```
CUNDINAMARCA>en
```

```
Password:
```

```
CUNDINAMARCA#conf t
```

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

```
CUNDINAMARCA(config)#username admin secret 123
```

```
CUNDINAMARCA(config)#aaa new-model
```

```
CUNDINAMARCA(config)#aaa authentication login AAA-LOGIN local
```

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

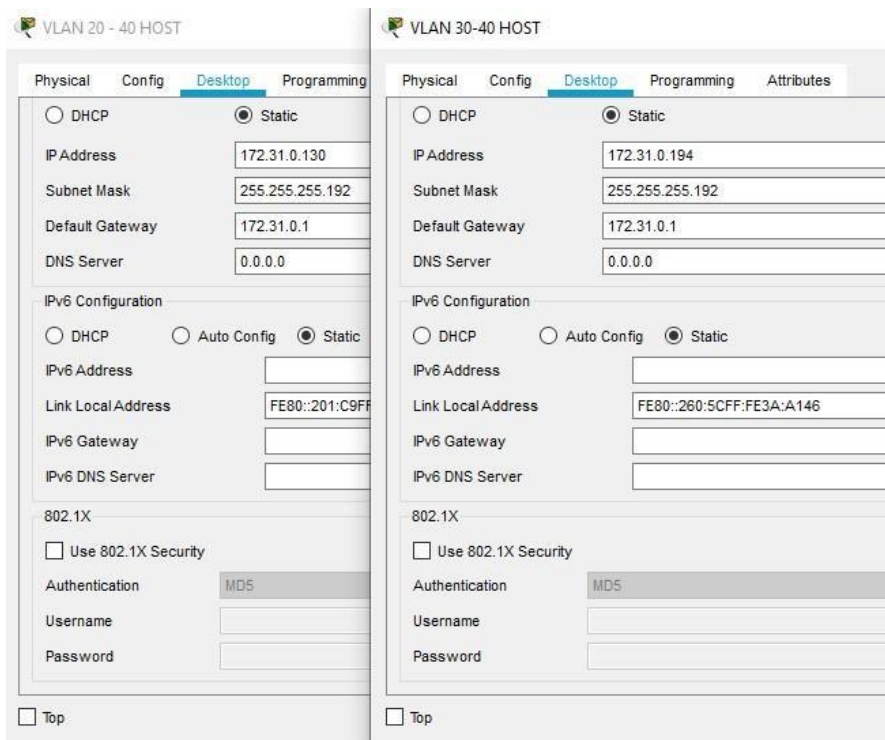
```
CUNDINAMARCA(config-line)#login authentication AAA-LOGIN
```

```
CUNDINAMARCA(config-line)#line vty 0 4
```

```
CUNDINAMARCA(config-line)#login authentication AAA-LOGIN
```

3.2.1.3 Cifrado de contraseñas

Figura 16. Cifrado de contraseñas



Fuente: Elaboración propia

3.2.1.4 Un máximo de internos para acceder al router.

Router Bucaramanga

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

Router Tunja

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

Router Cundinamarca

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

3.2.1.4 Máximo de intentos para acceder al router

Router Bucaramanga

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

Router Tunja

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

Router Cundinamarca

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

3.2.1.5 Máximo de tiempo de acceso al detectar ataques

Router Bucaramanga

BUCARAMANGA(config-line)#login block-for 10 attempts 5 within 60

Router Tunja

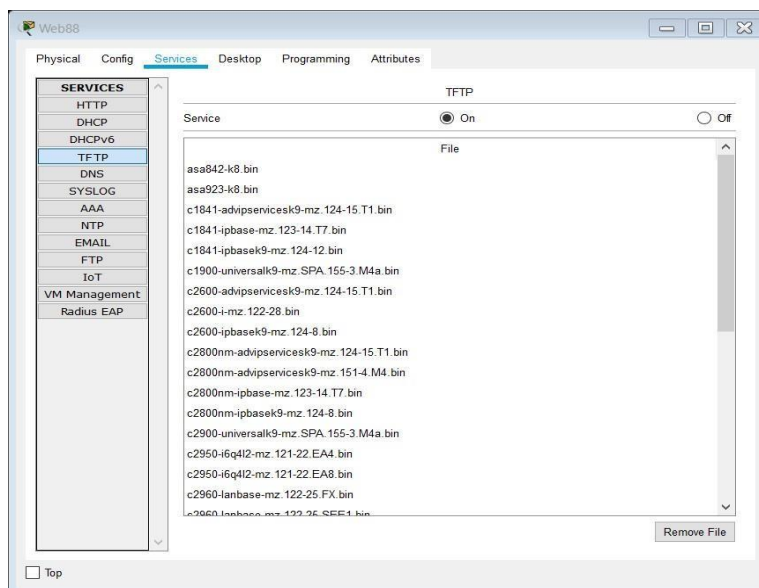
TUNJA(config-line)#login block-for 10 attempts 5 within 60

Router Cundinamarca

CUNDINAMARCA(config-line)#login block-for 10 attempts 5 within 60

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

Figura 17. Servidor TFTP



Fuente: Elaboracion propia

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

```
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#ip dhcp excluded-address 172.31.0.1 172.31.0.4
TUNJA(config)#ip dhcp excluded-address 172.31.0.65 172.31.0.68
TUNJA(config)#ip dhcp excluded-address 172.31.1.65 172.31.1.68
TUNJA(config)#ip dhcp excluded-address 172.31.1.1 172.31.1.4
TUNJA(config)#ip dhcp pool vlan10B
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 172.31.2.27
TUNJA(dhcp-config)#ip dhcp pool vlan30B
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 172.31.2.27
TUNJA(dhcp-config)#ip dhcp pool vlan20C
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 172.31.2.27
TUNJA(dhcp-config)#ip dhcp pool vlan30C
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 172.31.2.27
```

Router Bucaramanga

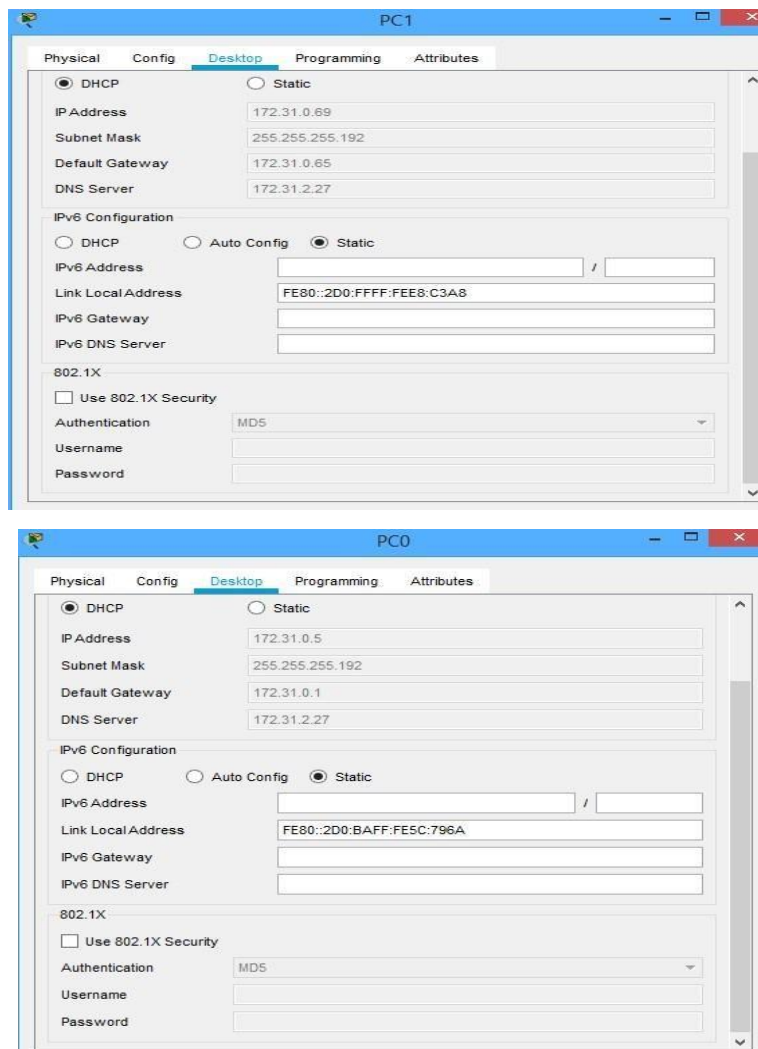
```
BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#login block-for 10 attempts 5 within 60
BUCARAMANGA(config)#int g0/0.10
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.33
BUCARAMANGA(config-subif)#int g0/0.30
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.33
BUCARAMANGA(config-subif)#end
```

Router Cundinamarca

```
Username: admin
Password:
CUNDINAMARCA>e
n
Password:
CUNDINAMARCA#conf t
```

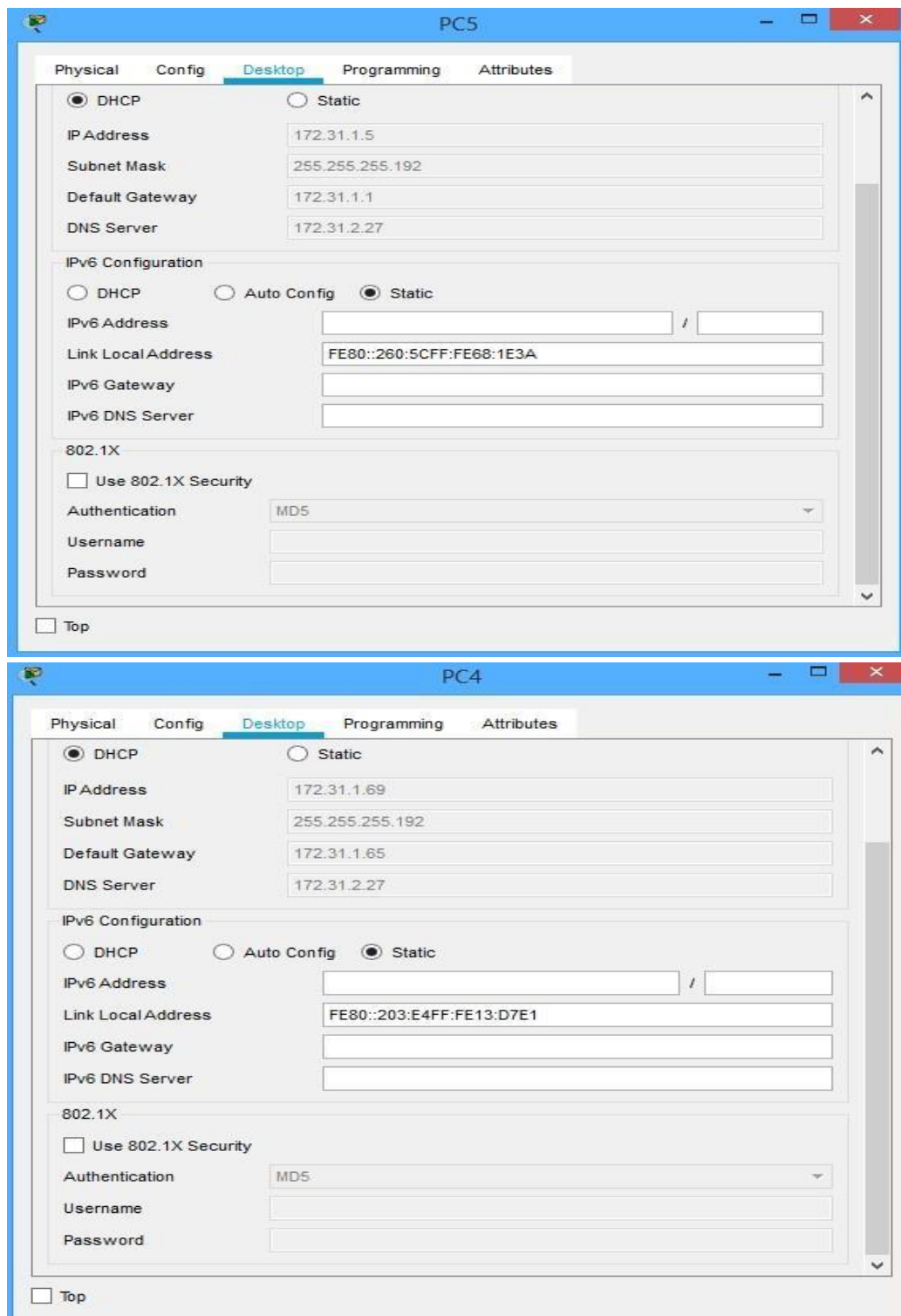
```
Enter configuration commands, one per line. End with CNTL/Z.  
CUNDINAMARCA(config)#int g0/0.20  
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37  
CUNDINAMARCA(config-subif)#int g0/0.30  
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37  
CUNDINAMARCA(config-subif)#end
```

Figura 18. Configuración DHCP



Fuente: elaboración propia

Figura 19. Configuración DHCP



Fuente: Elaboración Propia

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

Router Tunja

```
Username:
admin
Password:
TUNJA>en
Password:
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#ip nat inside source static 172.31.2.27 209.165.220.10
TUNJA(config)#ip access-list standard NAT-ACL
TUNJA(config-std-nacl)#permit 172.31.0.0 0.0.255.255
TUNJA(config-std-nacl)#ip nat inside source list NAT-ACL interface g0/1
overload
TUNJA(config)#int g0/1
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#int g0/0.1
TUNJA(config-subif)#ip nat inside
TUNJA(config-subif)#int g0/0.20
TUNJA(config-subif)#ip nat inside
TUNJA(config-subif)#int g0/0.30
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 0.0.0.0 209.165.220.5
TUNJA(config)#router ospf 1
TUNJA(config-router)#default-information originate
TUNJA(config-router)#end
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
```

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

E1 - OSPF external type 1, E2 - OSPF external type 2, E
- EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-
IS inter area

* - candidate default, U - per-user static route, o -
ODR P - periodic downloaded static route

Gateway of last resort is 209.165.220.5 to network 0.0.0.0

172.3.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.3.2.8/29 is directly connected, GigabitEthernet0/0.1
L 172.3.2.9/32 is directly connected, GigabitEthernet0/0.1
172.31.0.0/16 is variably subnetted, 15 subnets, 4 masks
O 172.31.0.0/26 [110/65] via 172.31.2.34, 01:34:01, Serial0/0/0
O 172.31.0.64/26 [110/65] via 172.31.2.34, 01:34:01, Serial0/0/0
C 172.31.0.128/26 is directly connected, GigabitEthernet0/0.20
L 172.31.0.129/32 is directly connected, GigabitEthernet0/0.20
C 172.31.0.192/26 is directly connected, GigabitEthernet0/0.30
L 172.31.0.193/32 is directly connected, GigabitEthernet0/0.30
O 172.31.1.0/26 [110/65] via 172.31.2.38, 01:26:24, Serial0/0/1
O 172.31.1.64/26 [110/65] via 172.31.2.38, 01:26:24, Serial0/0/1
O 172.31.2.0/29 [110/65] via 172.31.2.34, 01:34:01, Serial0/0/0
O 172.31.2.8/29 [110/65] via 172.31.2.38, 01:26:24, Serial0/0/1
O 172.31.2.24/29 [110/65] via 172.31.2.38, 01:26:24, Serial0/0/1
C 172.31.2.32/30 is directly connected,
Serial0/0/0 L 172.31.2.33/32 is directly
connected, Serial0/0/0 C 172.31.2.36/30 is
directly connected, Serial0/0/1
L 172.31.2.37/32 is directly connected, Serial0/0/1
209.165.220.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.165.220.0/24 is directly connected, GigabitEthernet0/1
L 209.165.220.1/32 is directly connected, GigabitEthernet0/1
S* 0.0.0.0/0 [1/0] via 209.165.220.5

Router Bucaramanga

BUCARAMANGA#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2 E1 - OSPF external type 1, E2 - OSPF
external type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-
IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o -
ODR P - periodic downloaded static route

Gateway of last resort is 172.31.2.33 to network 0.0.0.0
 172.3.0.0/29 is subnetted, 1 subnets
 O 172.3.2.8/29 [110/65] via 172.31.2.33, 01:37:52, Serial0/0/0
 172.31.0.0/16 is variably subnetted, 15 subnets, 4 masks
 C 172.31.0.0/26 is directly connected, GigabitEthernet0/0.10
 L 172.31.0.1/32 is directly connected, GigabitEthernet0/0.10
 C 172.31.0.64/26 is directly connected, GigabitEthernet0/0.30
 L 172.31.0.65/32 is directly connected, GigabitEthernet0/0.30
 O 172.31.0.128/26 [110/65] via 172.31.2.33, 01:37:52, Serial0/0/0
 O 172.31.0.192/26 [110/65] via 172.31.2.33, 01:37:52, Serial0/0/0
 O 172.31.1.0/26 [110/129] via 172.31.2.33, 01:30:06, Serial0/0/0
 O 172.31.1.64/26 [110/129] via 172.31.2.33, 01:30:06, Serial0/0/0
 C 172.31.2.0/29 is directly connected, GigabitEthernet0/0.1
 L 172.31.2.1/32 is directly connected, GigabitEthernet0/0.1
 O 172.31.2.8/29 [110/129] via 172.31.2.33, 01:30:06, Serial0/0/0
 O 172.31.2.24/29 [110/129] via 172.31.2.33, 01:30:06, Serial0/0/0
 C 172.31.2.32/30 is directly connected, Serial0/0/0
 L 172.31.2.34/32 is directly connected, Serial0/0/0
 O 172.31.2.36/30 [110/128] via 172.31.2.33, 01:30:56, Serial0/0/0
 O*E2 0.0.0.0/0 [110/1] via 172.31.2.33, 00:04:43, Serial0/0/0

Router Cundinarmaca

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

Gateway of last resort is 172.31.2.37 to network 0.0.0.0

172.3.0.0/29 is subnetted, 1 subnets
 O 172.3.2.8/29 [110/65] via 172.31.2.37, 01:32:40, Serial0/0/0
 172.31.0.0/16 is variably subnetted, 16 subnets, 4 masks
 O 172.31.0.0/26 [110/129] via 172.31.2.37, 01:32:40, Serial0/0/0
 O 172.31.0.64/26 [110/129] via 172.31.2.37, 01:32:40, Serial0/0/0
 O 172.31.0.128/26 [110/65] via 172.31.2.37, 01:32:40, Serial0/0/0
 O 172.31.0.192/26 [110/65] via 172.31.2.37, 01:32:40, Serial0/0/0

```
C 172.31.1.0/26 is directly connected, GigabitEthernet0/0.30
L 172.31.1.1/32 is directly connected, GigabitEthernet0/0.30
C 172.31.1.64/26 is directly connected, GigabitEthernet0/0.20
L 172.31.1.65/32 is directly connected, GigabitEthernet0/0.20
O 172.31.2.0/29 [110/129] via 172.31.2.37, 01:32:40, Serial0/0/0
C 172.31.2.8/29 is directly connected, GigabitEthernet0/0.1
L 172.31.2.9/32 is directly connected, GigabitEthernet0/0.1
C 172.31.2.24/29 is directly connected, GigabitEthernet0/0.88
L 172.31.2.25/32 is directly connected, GigabitEthernet0/0.88
O 172.31.2.32/30 [110/128] via 172.31.2.37, 01:32:40, Serial0/0/0
C 172.31.2.36/30 is directly connected, Serial0/0/0
L 172.31.2.38/32 is directly connected, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.31.2.37, 00:07:10, Serial0/0/0
```

3.2.4 Autenticación del enrutamiento

```
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 ospfospf
BUCARAMANGA(config-if)#
```

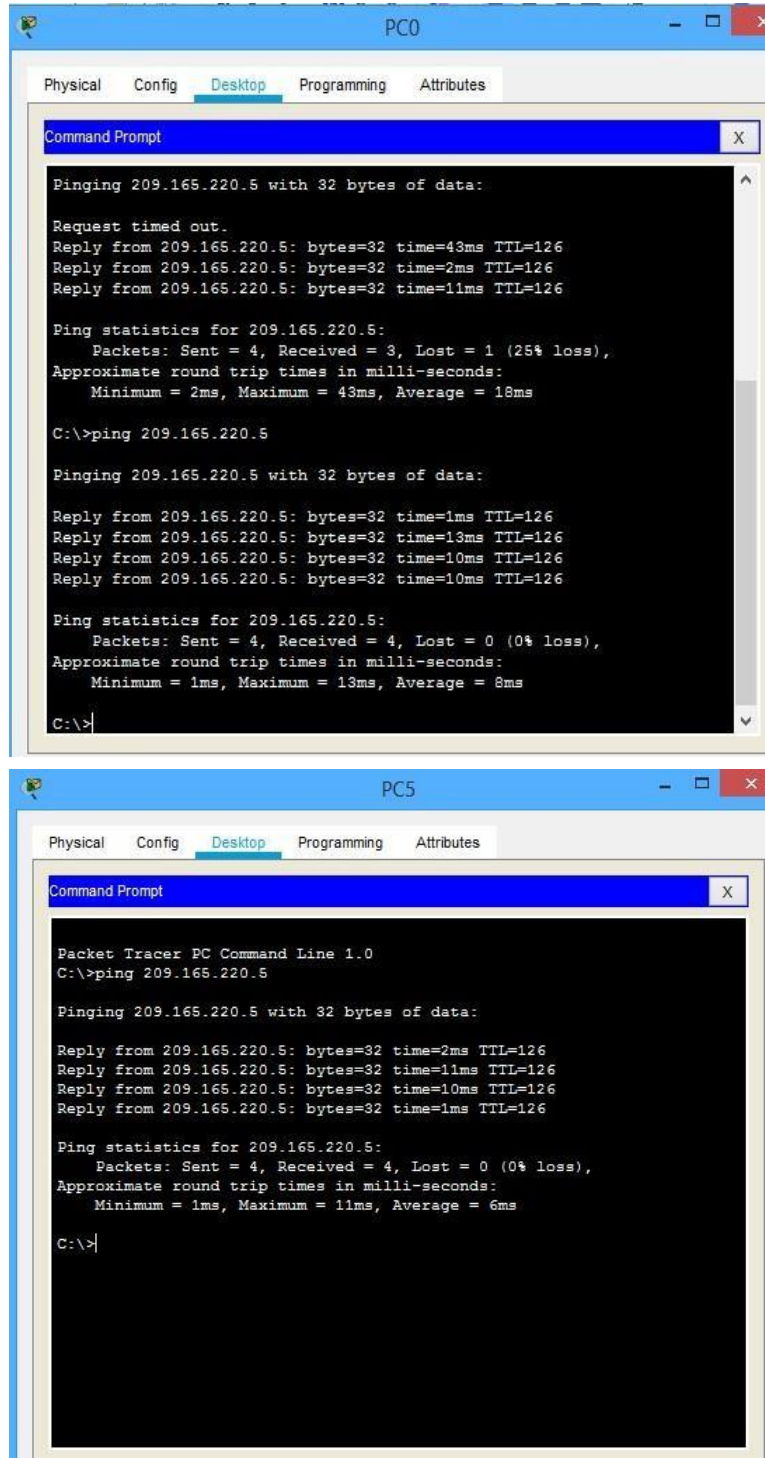
```
CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#int s0/0/0
CUNDINAMARCA(config-if)#ip ospf authentication message-digest
CUNDINAMARCA(config-if)#ip ospf message-digest-key 1 md5 ospfospf
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#
```

```
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 ospfospf
TUNJA(config-if)#int s0/0/1
TUNJA(config-if)#
02:42:15: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/0/0 from
LOADING to FULL, Loading Done
```

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

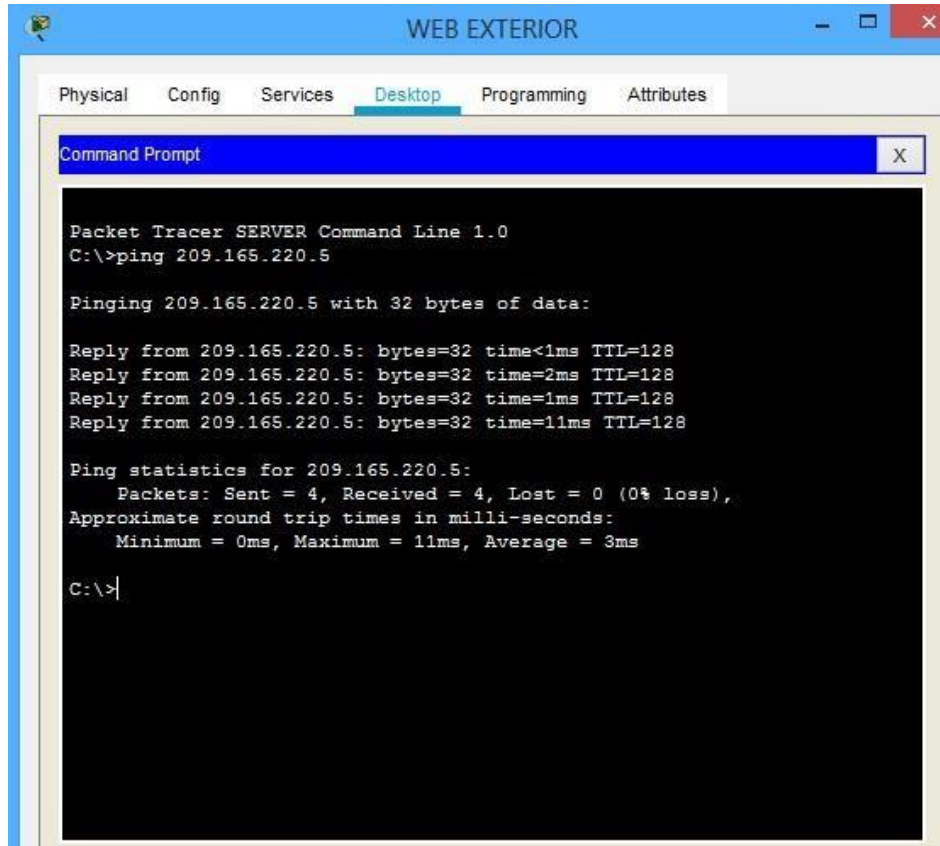
TUNJA(config-if)#ip ospf message-digest-key 1 md5 ospfospf

Figura 20. Autenticación de enrutamiento



Fuente: Elaboración propia

Figura 21. Autenticación de enrutamiento



Fuente: Elaboración propia

3.2.5 listas de control de acceso

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

```
CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#access-list 151 deny ip 172.31.1.64
0.0.0.63
209.165.220.0 0.0.0.255
CUNDINAMARCA(config)#access-list 151 permit ip any any
```

```
CUNDINAMARCA(config)#int g0/0.20
CUNDINAMARCA(config-subif)#ip access-group 151 in
```

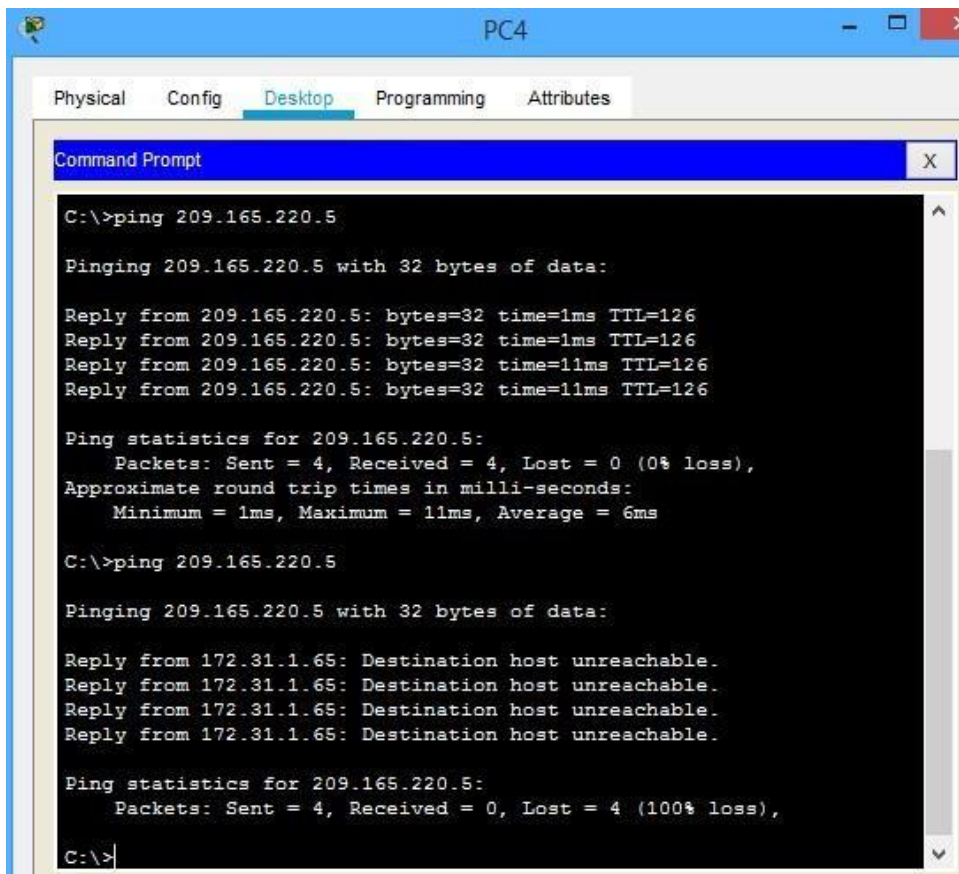


Figura 22. Control e acceso en Cundinamarca

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

```
CUNDINAMARCA(config-subif)#access-list 152 permit ip 172.31.1.0 0.0.0.63
209.165.220.0 0.0.0.255
CUNDINAMARCA(config)#access-list 152 deny ip any any
CUNDINAMARCA(config)#int g0/0.30
CUNDINAMARCA(config-subif)#ip access-group 152 in
```

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

```
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#access-list 151 permit tcp 172.31.0.192 0.0.0.63
209.165.220.0
0.0.0.255 eq 80
TUNJA(config)#access-list 151 permit tcp 172.31.0.192 0.0.0.63
209.165.220.0
0.0.0.255 eq 21
TUNJA(config)#int g0/0.30
TUNJA(config-subif)#ip access-group 151 in
```

Figura 23. Control de Acceso en Cundinamarca no tunja



Fuente: Elaboración propia

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

```
TUNJA(config-subif)#access-list 152 permit ip 172.31.0.128 0.0.0.63
172.31.1.64 0.0.0.63

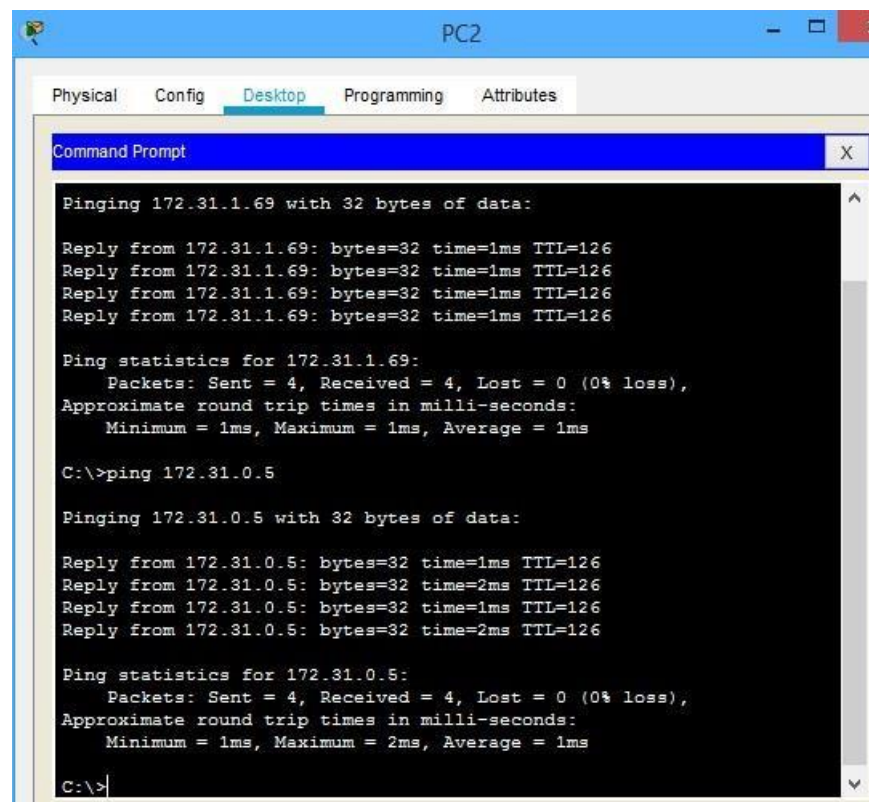
TUNJA(config)#access-list 152 permit ip 172.31.0.128 0.0.0.63 172.31.0.0
0.0.0.63

TUNJA(config)#int g0/0.20

TUNJA(config-subif)#ip access-group 152 in

TUNJA(config-subif)#
```

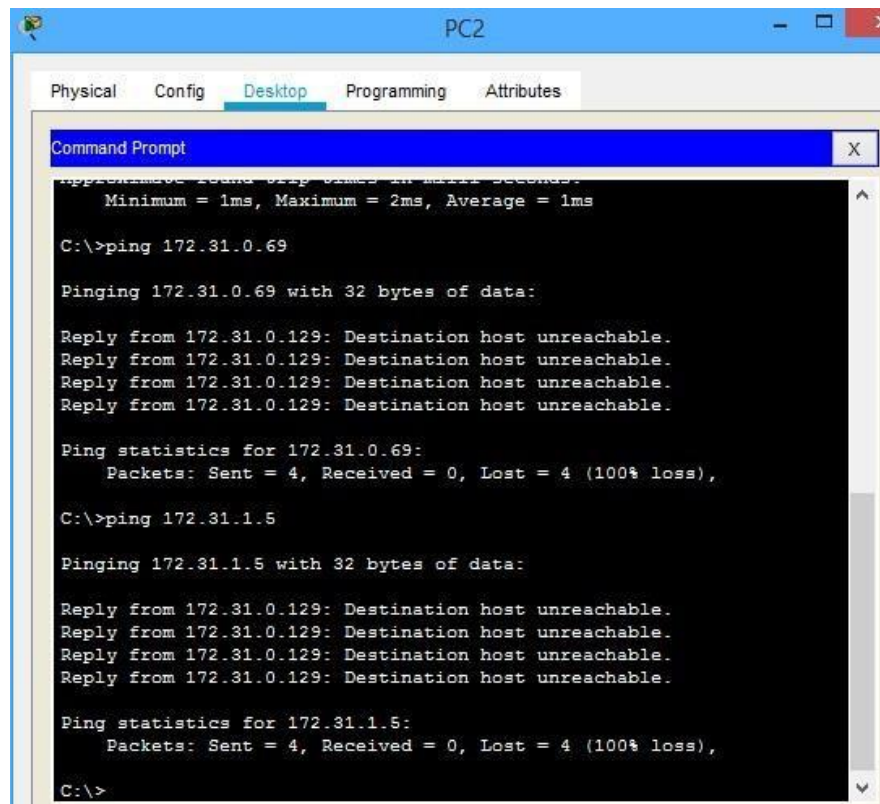
Figura 24. Control de acceso en Tunja



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 172.31.1.69 with 32 bytes of data:
Reply from 172.31.1.69: bytes=32 time=1ms TTL=126
Reply from 172.31.1.69: bytes=32 time=1ms TTL=126
Reply from 172.31.1.69: bytes=32 time=1ms TTL=126
Reply from 172.31.1.69: bytes=32 time=1ms TTL=126
Ping statistics for 172.31.1.69:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\>ping 172.31.0.5
Pinging 172.31.0.5 with 32 bytes of data:
Reply from 172.31.0.5: bytes=32 time=1ms TTL=126
Reply from 172.31.0.5: bytes=32 time=2ms TTL=126
Reply from 172.31.0.5: bytes=32 time=1ms TTL=126
Reply from 172.31.0.5: bytes=32 time=2ms TTL=126
Ping statistics for 172.31.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\>
```

Fuente: Elaboración propia

Figura 25. Control de acceso en tunja

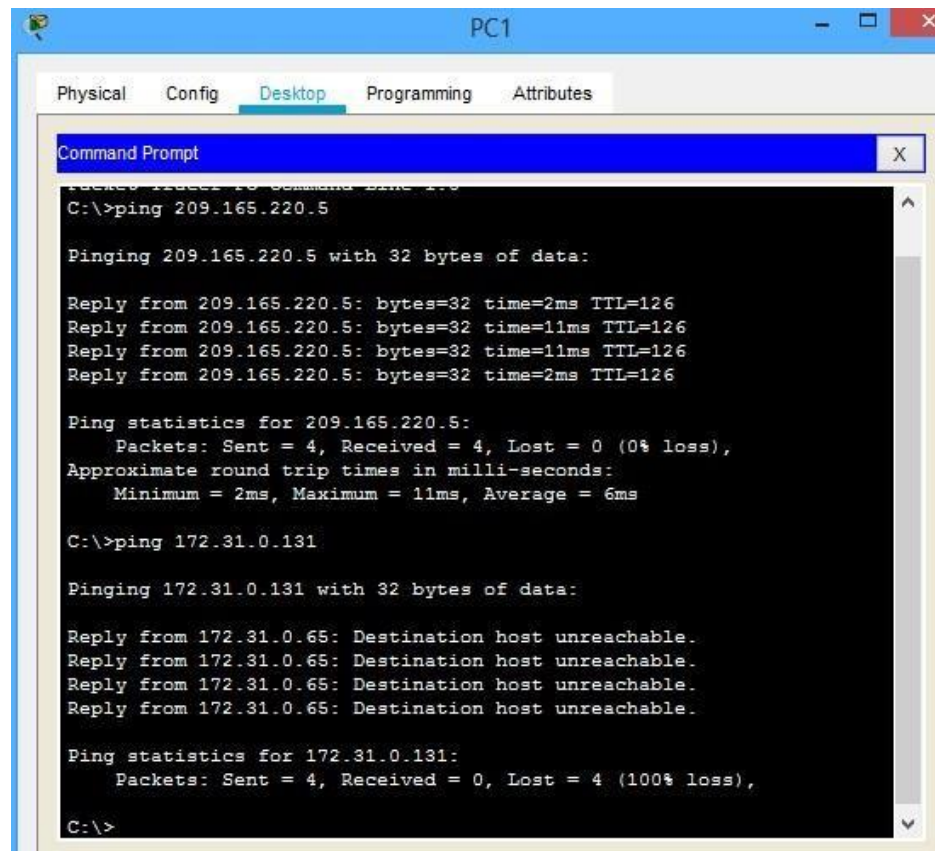


Fuente: Elaboración propia

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

```
BUCARAMANGA(config)#access-list 151 permit ip 172.31.0.64  
0.0.0.63 209.165.220.0 0.0.0.255  
BUCARAMANGA(config)#int g0/0.30  
BUCARAMANGA(config-subif)#ip access-group 151 in  
BUCARAMANGA(config-subif)#
```

Figura 25. Control de acceso en Cundinamarca

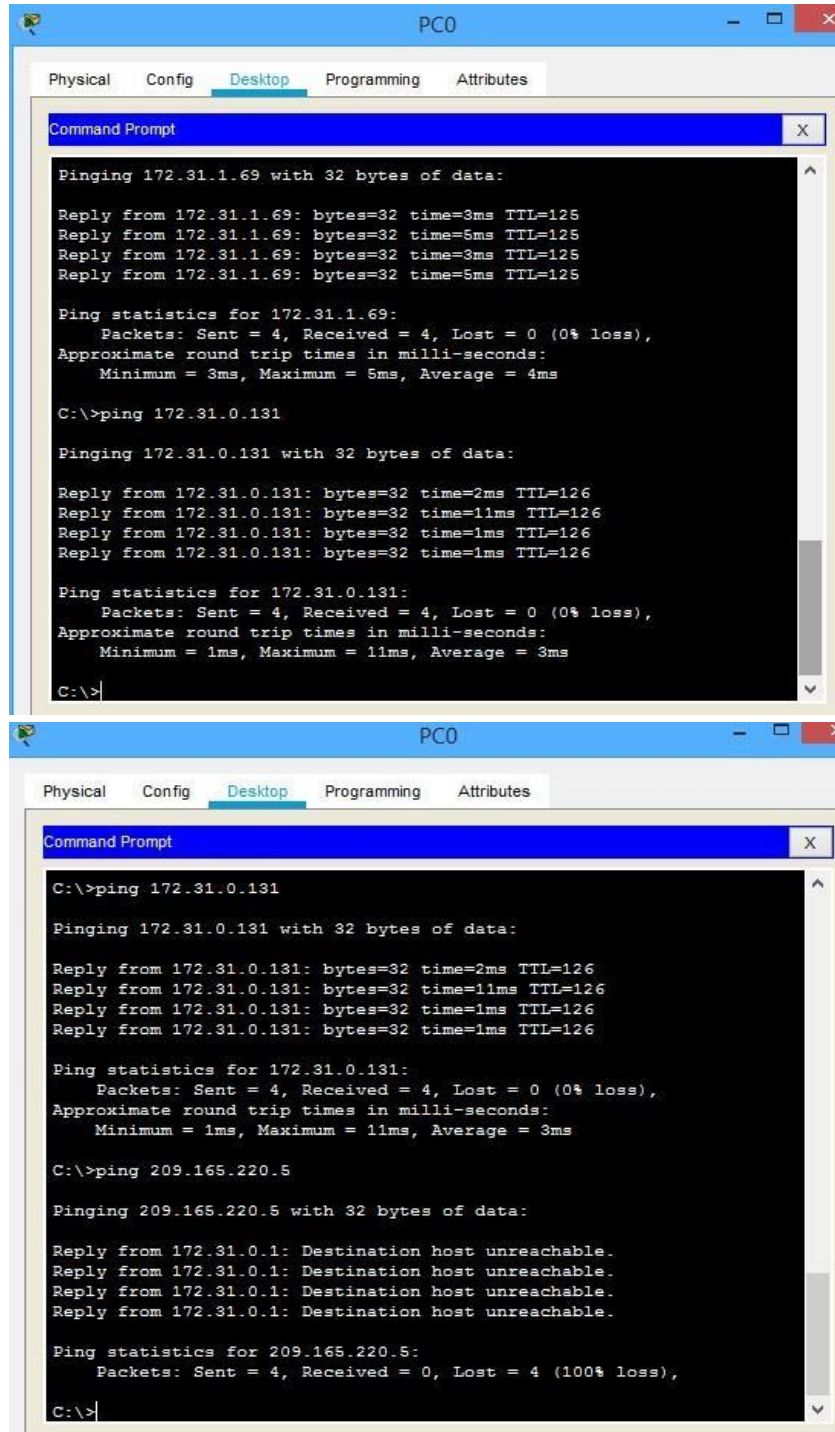


Fuente: Elaboración propia

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

```
BUCARAMANGA(config-subif)#access-list 152 permit ip 172.31.0.0 0.0.0.63
172.31.1.64 0.0.0.63
BUCARAMANGA(config)#
BUCARAMANGA(config)#access-list
152 permit ip 172.31.0.0 0.0.0.63
172.31.0.128 0.0.0.63
BUCARAMANGA(config)#int g0/0.10
BUCARAMANGA(config-subif)#ip access-group 152 in
BUCARAMANGA(config-subif)#
```

Figura 26. Control de acceso en Bucaramanga



Fuente: Elaboración propia

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

```
BUCARAMANGA(config-subif)#access-list 153 deny ip 172.31.2.0
0.0.0.7 172.31.0.0 0.0.0.63
BUCARAMANGA(config)#access-list 153 deny ip 172.31.0.64 0.0.0.63
172.31.0.0 0.0.0.63
BUCARAMANGA(config)#access-list 153 permit ip any any
BUCARAMANGA(config)#int g0/0.10
BUCARAMANGA(config-subif)#ip access-group 153 out
BUCARAMANGA(config-subif)#
```

```
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#access-list 153 deny ip 172.3.2.8 0.0.0.7 172.31.0.128
0.0.0.63
TUNJA(config)#access-list 153 deny ip 172.3.0.192 0.0.0.63 172.31.0.128
0.0.0.63
TUNJA(config)#access-list 153 permit ip any any
TUNJA(config)#int g0/0.20
TUNJA(config-subif)#ip access-group 153 out TUNJA(config-
subif)#
```

```
CUNDINAMARCA(config)#access-list 153 deny ip 172.31.2.8 0.0.0.7
172.31.1.64 0.0.0.63
CUNDINAMARCA(config)#access-list 153 deny ip 172.31.1.0 0.0.0.63
172.31.1.64 0.0.0.63
CUNDINAMARCA(config)#access-list 153 deny ip 172.31.2.24 0.0.0.7
172.31.1.64 0.0.0.63
CUNDINAMARCA(config)#access-list 153 permit ip any any
CUNDINAMARCA(config)#int g0/0.20
CUNDINAMARCA(config-subif)#ip access-group 153 out
CUNDINAMARCA(config-subif)#
```

Figura 27. Control de acceso Cundinamarca

```
Reply from 172.31.0.131: bytes=32 time=2ms TTL=126
Reply from 172.31.0.131: bytes=32 time=11ms TTL=126
Reply from 172.31.0.131: bytes=32 time=1ms TTL=126
Reply from 172.31.0.131: bytes=32 time=1ms TTL=126

Ping statistics for 172.31.0.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 3ms

C:\>ping 209.165.220.5

Pinging 209.165.220.5 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 209.165.220.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.31.1.5

Pinging 172.31.1.5 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 172.31.1.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.31.0.195

Pinging 172.31.0.195 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 172.31.0.195:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 6ms

C:\>ping 209.165.220.5

Pinging 209.165.220.5 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 209.165.220.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.31.1.5

Pinging 172.31.1.5 with 32 bytes of data:

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

Ping statistics for 172.31.1.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Fuente: Elaboración propia

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

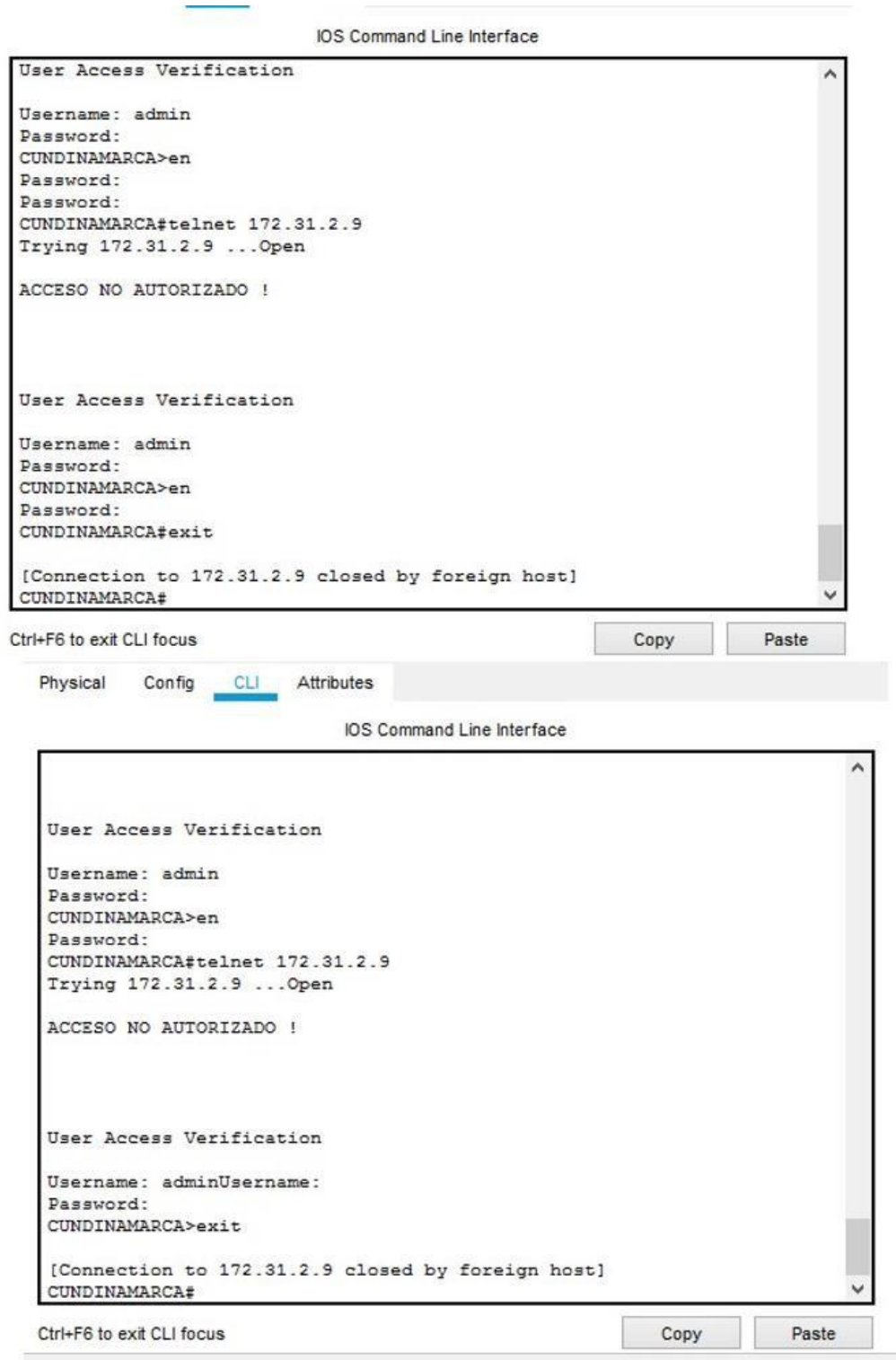
```
BUCARAMANGA(config)#access-list 9 permit 172.31.2.0 0.0.0.7
BUCARAMANGA(config)#access-list 9 permit 172.3.2.8 0.0.0.7
BUCARAMANGA(config)#access-list 9 permit 172.31.2.8 0.0.0.7
BUCARAMANGA(config)#line vty 0 4
BUCARAMANGA(config-line)#access-class 9 in
```

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

```
TUNJA(config)#access-list 9 permit 172.31.2.0 0.0.0.7
TUNJA(config)#access-list 9 permit 172.3.2.8 0.0.0.7
TUNJA(config)#access-list 9 permit 172.31.2.8 0.0.0.7
TUNJA(config)#line vty 0 4
TUNJA(config-line)#access-class 9 in
TUNJA(config-line)#
```

```
CUNDINAMARCA(config-subif)#access-list 9 permit 172.31.2.0 0.0.0.7
CUNDINAMARCA(config)#access-list 9 permit 172.3.2.8 0.0.0.7
CUNDINAMARCA(config)#access-list 9 permit 172.31.2.8 0.0.0.7
CUNDINAMARCA(config)#line vty 0 4
CUNDINAMARCA(config-line)#access-class 9 in
CUNDINAMARCA(config-line)#
```

Figura 28. Acceso de las VLAN



Fuente: Elaboración propia

3.2.6 VLSM: utilizar la dirección 172.31.0.0 /18 para el direccionamiento

```
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

```
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)#
```

00:25:02: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.220.1 on Serial0/0/0 from
LOADING to FULL, Loading Done

```
CUNDINAMARCA(config-router)#end
```

```
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)#
```

00:19:40: %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
```

4. CONCLUSIONES

Para que haya comunicación entre host, cada uno debe estar configurado con los puertos adecuados

El direccionamiento requiere un especial cuidado ya que una mala dirección nos puede tumbar toda una red

Antes de realizar un montaje real de una red, nos debemos cerciorar de su correcto funcionamiento a través de un simulador.

5. BIBLIOGRAFIA

Entorno de conocimiento del Campus virtual de la universidad nacional abierta y adistancia, UNAD, [En línea] [consultado en diciembre de 2019] Disponible en: <https://campus01.unad.edu.co/ecbti54/mod/page/view.php?id=4074>

Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press.[En línea] [Consultado en Diciembre 2019] Disponible en: <https://1drv.ms/b/s!AmIJYei-NT1Im3L74BZ3bpMiXRx0>

Plataforma cisco, [En línea] [consultado en diciembre de 2019] Disponible en: <https://www.netacad.com/>