PRUEBA DE HABILIDADES PRÁCTICAS CCNA

EDUARD FERNANDO ARISTIZABAL GIRALDO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA ESCUELA

DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA DE SISTEMAS

DICIEMBRE DE 2019

PRUEBA DE HABILIDADES PRÁCTICAS CCNA

EDUARD FERNANDO ARISTIZABAL GIRALDO

Diplomado de profundización Cisco (Diseño e implementación de soluciones integradas LAN / WAN) – 203092_33

Tutor

NILSON ALBEIRO FERREIRA MANZANARES

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

INGENIERÍA DE SISTEMAS

DICIEMBRE DE 2019

NOTA DE ACETACION:

PRESIDENTE DEL JURADO

FIRMA JURADO

FIRMA JURADO

Armenia, 11/12/2019

DEDICATORIA

Le dedico a mi familia que me ha apoyado a lograr mis objetivos y metas, a su apoyado emocionalmente para conseguir mis sueños, estando siempre presente para formarme como persona y como un ser humano con valores y responsabilidad frente a todos mis deberes.

AGRADECIMIENTO

Agradezco principalmente a Dios, que me permite todos los días trabajar para alcanzar mis metas, la Universidad Nacional Abierta y a Distancia porque nos brinda la posibilidad de estudiar y prepararnos a distancia, porque por nuestros deberes personales y laborales, me sería imposible estudiar y prepararme como profesional.

CONTENIDO

LISTAS DE TABLAS

TABLA DE FIGURAS

RESUMEN

La Universidad Nacional Abierta y a Distancia, durante el proceso de aprendizaje del DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN) utilizando el aplicativo Cisco PackerTracer y smartlab, programas que permite realizar la simulación de redes, se logró experimentar las diferentes configuraciones de una red.

En el desarrollo de los laboratorios, con las simulaciones se logra adquirir conocimientos CCNA Hosting y Switching, módulos CCNA 1 y CCNA 2, con los conocimientos obtenidos y puestos en práctica se realizó el desarrollo de la actividad final como prueba de las habilidades, donde mediante los escenarios propuestos se coloca en habilidad los conocimientos previamente aprendidos donde se realizan configuraciones NAT, DHCP, RIPV2, VLAN, configuración de direcciones IP y OSPFv2, usando a su vez comandos de para verificación de configuraciones y haciendo las respectivas pruebas de conectividad entre los diferentes siendo así, las soluciones más apropiadas para los ejercicios planteados para esta actividad

ABSTRACT

The National Open and Distance University, during the learning process of the CISCO DEEP DEPLOYMENT (DESIGN AND IMPLEMENTATION OF INTEGRATED LAN / WAN SOLUTIONS) using the Cisco Packet Tracer application and smartlab, programs that allow network simulation, it was possible to experience the Different configurations of a network.

In the development of the laboratories, with the simulations it is possible to acquire knowledge CCNA Hosting and Switching, modules CCNA 1 and CCNA 2, with the knowledge obtained and put into practice the development of the final activity was carried out as a test of the skills, where through The proposed scenarios are the ability to learn previously learned skills where NAT, DHCP, RIPV2, VLAN, IP address configuration and OSPFv2 configurations are performed, using in turn commands to verify configurations and making the respective connectivity tests between the different thus, the most appropriate solutions for the exercises proposed for this activity

INTRODUCCIÓN

La necesidad de tener personal capacitado, competitivo, idóneo en el campo laboral ha sido una de los objetivos más importantes hoy en día para el mercado laboral, porque deben a su vez contar con las competencias necesarias para desarrollar actividades relacionas con las tecnologías de la información y la comunicación (TICS)

Es ahí donde la certificación CCNA permite dar a conocer las habilidades necesarias para trabajar y establecerse en un escenario de redes.

Durante el desarrollo del diplomado de profundización cisco (diseño e implementación de soluciones integradas lan/wan), se lograron obtener conocimientos y experiencias como el enrutamiento basados en elementos Cisco (routers y switches), y evidencia del trabajo se realiza la presentación de la solución de dos escenarios planteados en la guía de actividades, donde se usó el aplicativo Packer Tracert de Cisco, para practicar y simular los ejercicios propuestos para esta actividad final del diplomado de cisco

OBJETIVOS

Objetivo General

Genera las topologías de los diferentes escenarios, en el desarrollo de soluciones LAN y WAN, reforzando nuestros conocimientos y aprendizaje para escalar en la vida laboral y obtener el título de ingeniero que nos ayudara a tener un mejor futuro tanto personal como profesional en el campo de desarrollo

Objetivo Especifico

Profundizar en aspectos de diseño e implementación de soluciones LAN/WAN

Realizando diferentes configuraciones, conocer y complementar protocolos normas

Estándares de seguridad y adquirir conocimientos pertinentes hacia instalaciones seguras

Enrutamientos basados en elementos telemáticos Cisco (routers y switches)

PRUEBA DE HABILIDADES PRACTICAS CCNA

ESCENARIO 1

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

Topología de Red

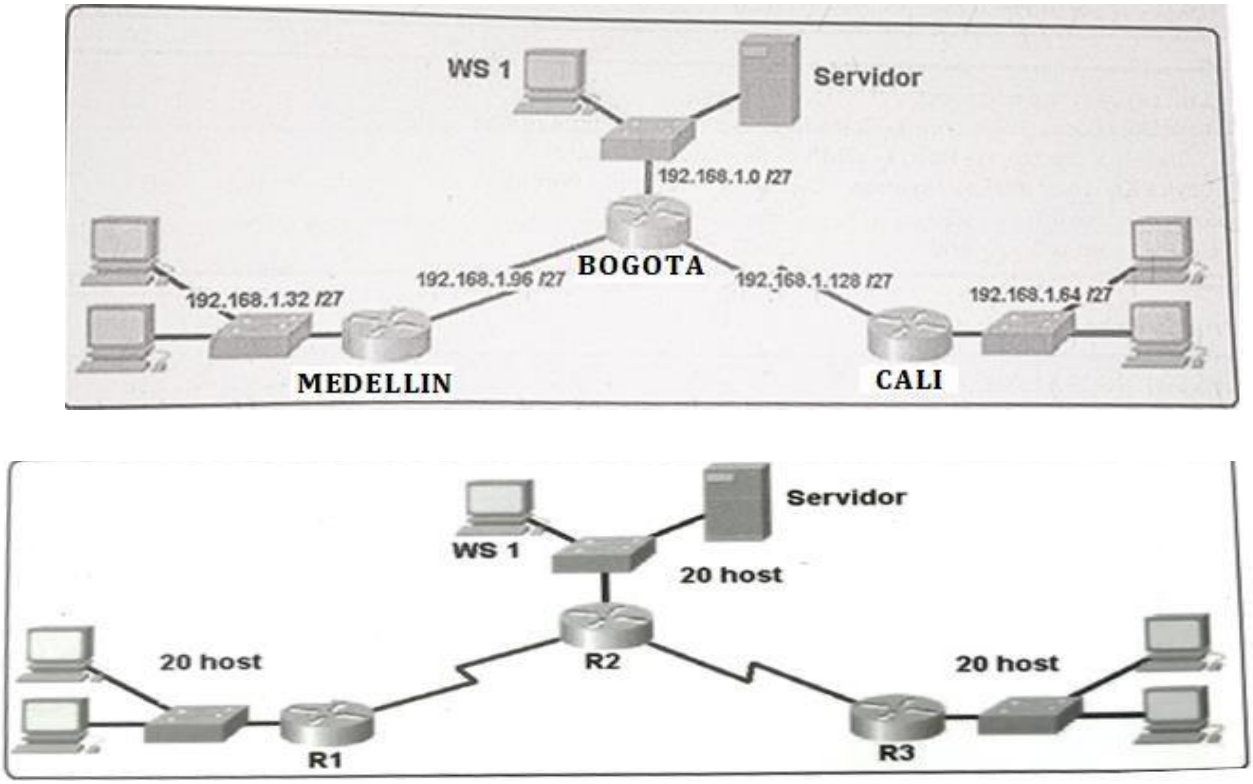

Figura 1 -topología red escenario 1

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.

Configuración Routers Sucursales ROUTER MEDELLIN

#en #config t
#no ip domain-lookup #enable secret cisco #line con 0 #password class #exit
#line vty 0 15 #password class #login
#exit
#service password-encryption #exit
#copy running-config startup-config

Router Bogota

#en #config t
#no ip domain-lookup #enable secret cisco
#line con 0 #password class #exit
#line vty 0 15 #password class #login
#exit
#service password-encryption #exit
#copy running-config startup-config

Router Cali

#en #config t
#no ip domain-lookup #enable secret cisco #line con 0 #password class #exit
#line vty 0 15 #password class #login
#exit
#service password-encryption #exit
#copy running-config startup-config

Parte 1: Asignación de direcciones IP:

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

Numero de subredes	Dirección subred	Broadcast	Mascara
1	192.168.1.0	192.168.1.31	255.255.255.224
2	192.168.1.32	192.168.1.63	255.255.255.224
3	192.168.1.64	192.168.1.95	255.255.255.224
4	192.168.1.96	192.168.1.127	255.255.255.224
5	192.168.1.128	192.168.1.159	255.255.255.224
6	192.168.1.160	192.168.1.191	255.255.255.224
7	192.168.1.192	192.168.1.223	255.255.255.224
8	192.168.1.224	192.168.1.255	255.255.255.224

Tabla 1 – subneteo red

A. Asignar una dirección IP a la red.

192.168.0.1

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

Tabla 2 - direccionamiento switch

Asignación IP Router Medellín

#en #config t #int fa0/0
#ip add 192.168.1.33 255.255.255.224
#no shut #exit #int s1/0
#ip add 192.168.199 255.255.255.224
#no shut #end

Asignación IP Router Cali

#en #config t #int fa0/0
#ip add 192.168.1.65 255.255.255.224
#no shut #exit #int s1/0
#ip add 192.168.131 255.255.255.224
#no shut #end

Asignación IP Router Bogotá
#en #config t #int fa2/0
#ip add 192.168.1.1 255.255.255.224
#no shut #exit #int s0/0
#ip add 192.168.1.98 255.255.255.224
#no shut #exit #int s1/0
#ip add 192.168.1.130 255.255.255.224
#no shut #end

A. 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.

#show ip route

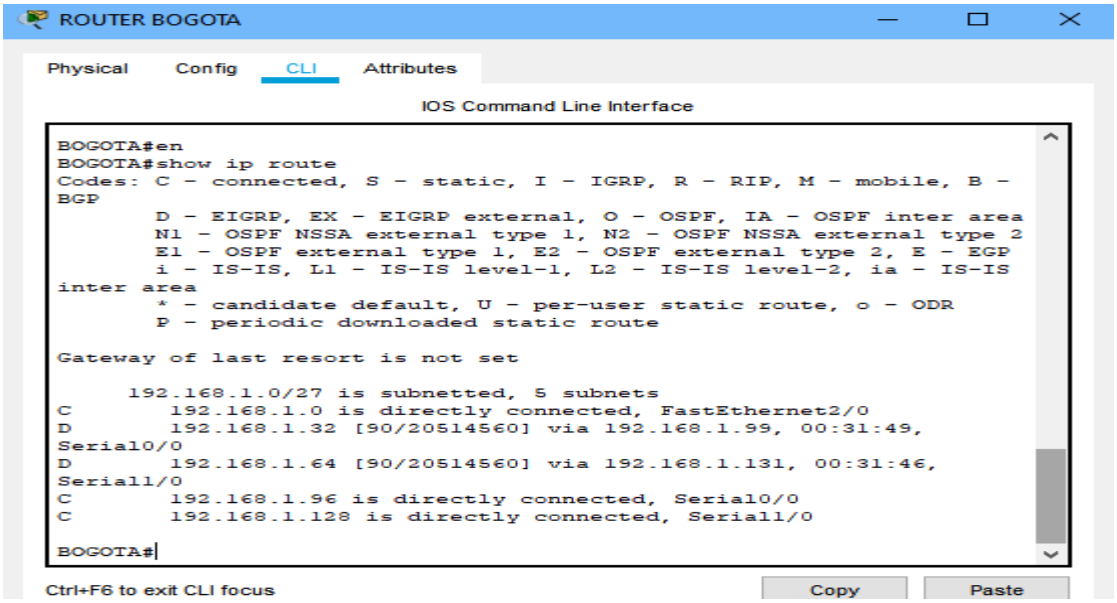

Figura 2 -asignación ip router Bogotá

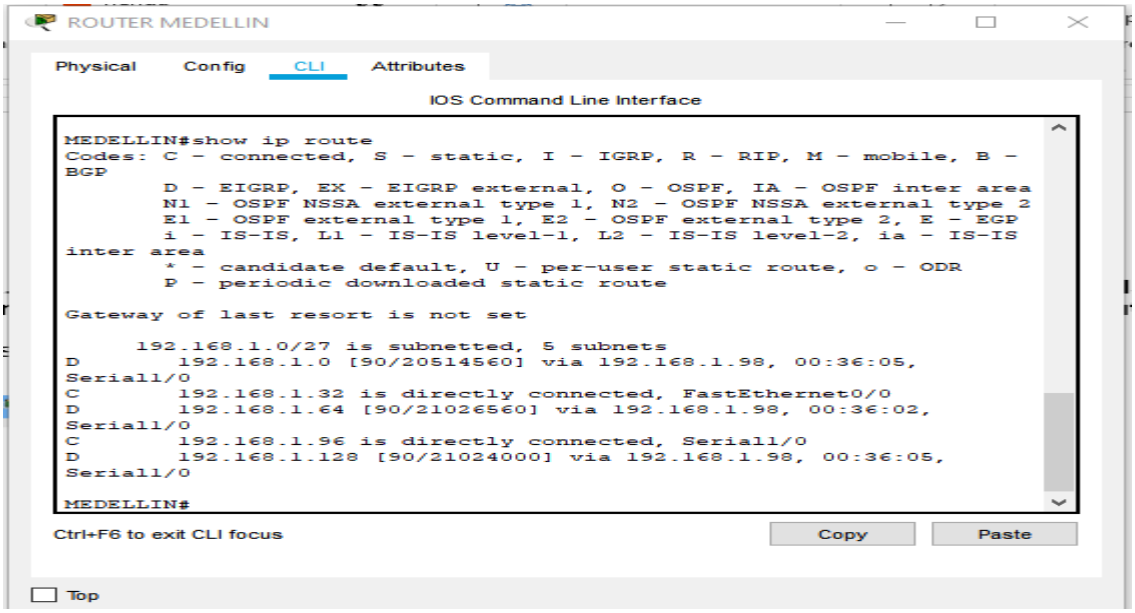

Figura 3 -asignación ip router Medellín

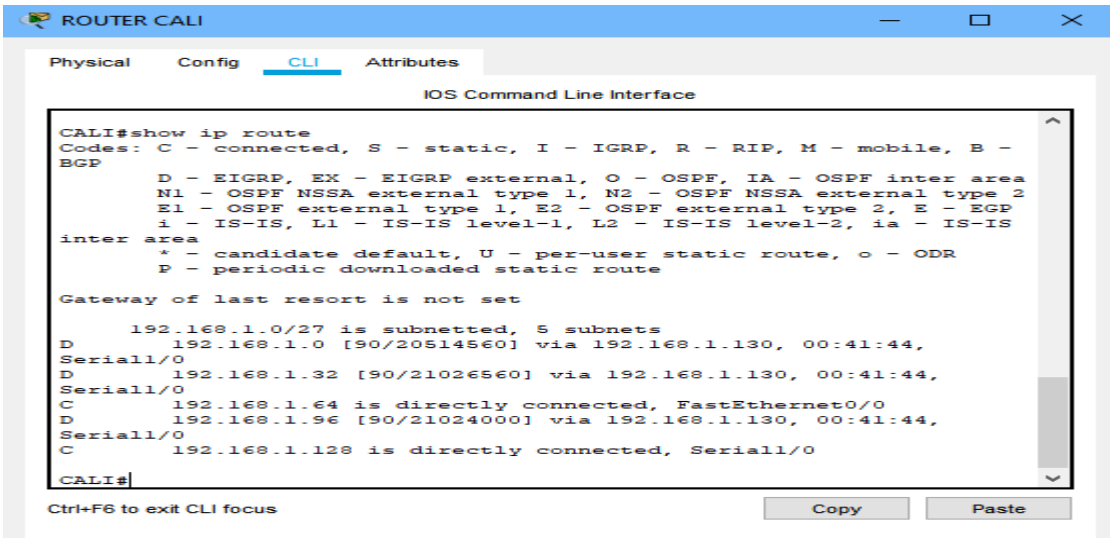

Figura 4-asignacion ip router Cali

a. Verificar el balanceo de carga que presentan los routers. #show ip route

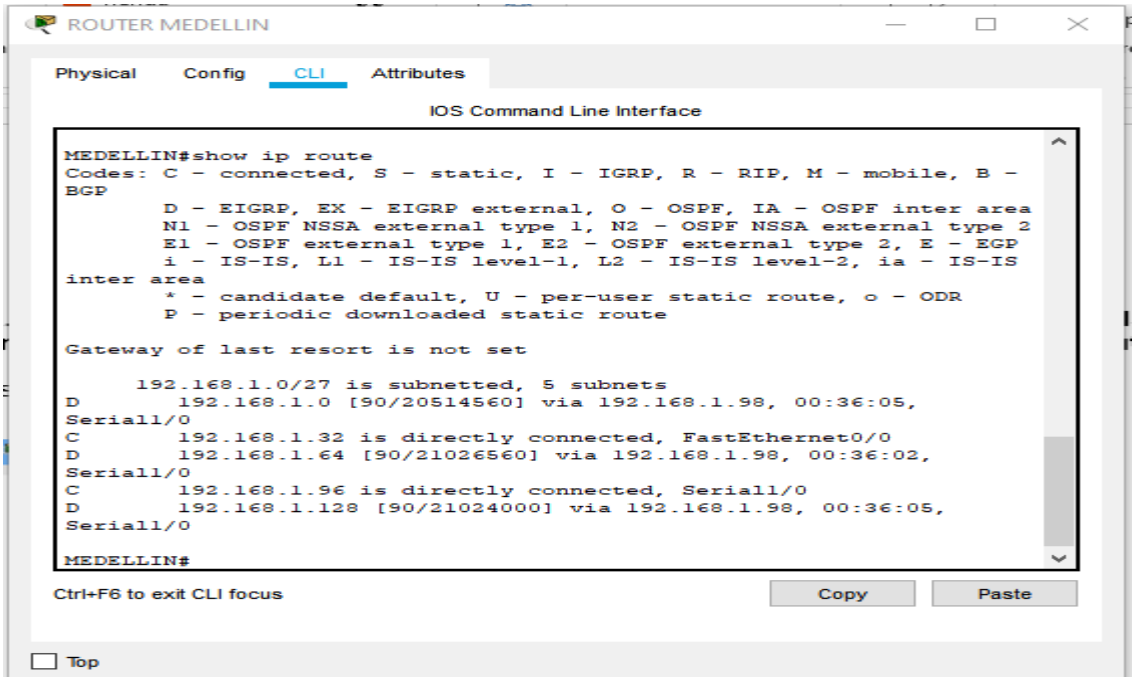

Figura 5-verification balance de cargas Medellín

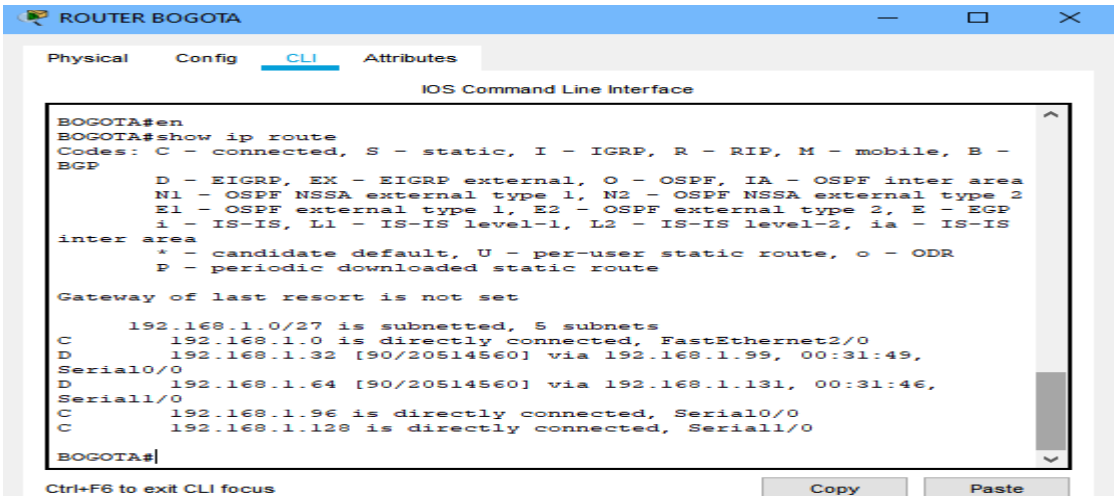

Figura 6-verificación Balance de cargas Bogotá

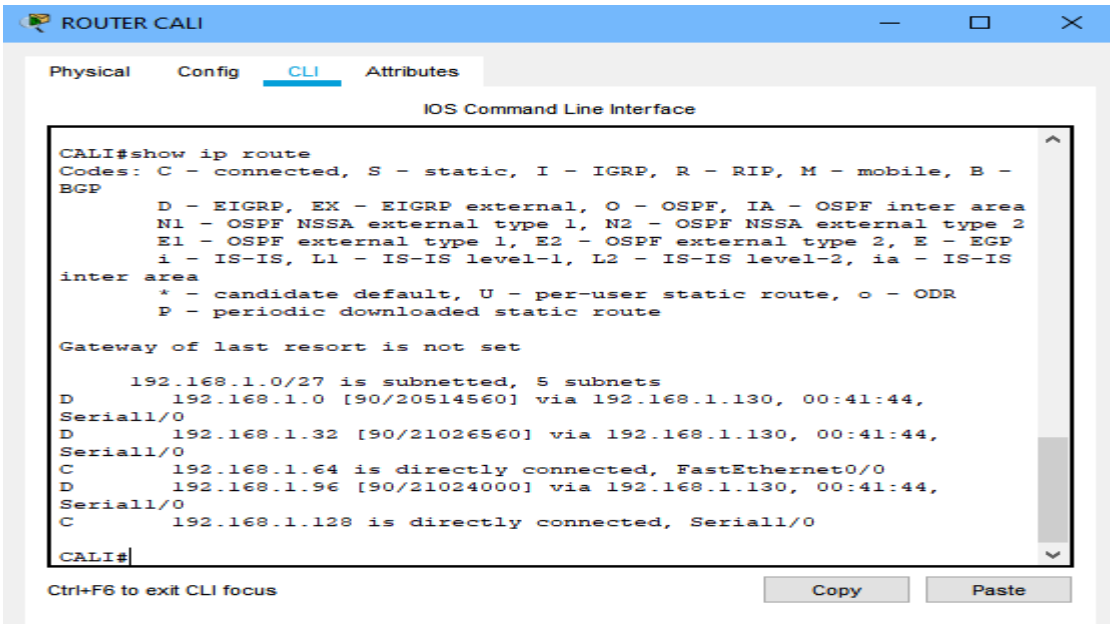

Figura 7-verificación balance de cargas Cali

A .Realizar un diagnóstico de vecinos cuando el comando cdp. #sh cdp neighbors

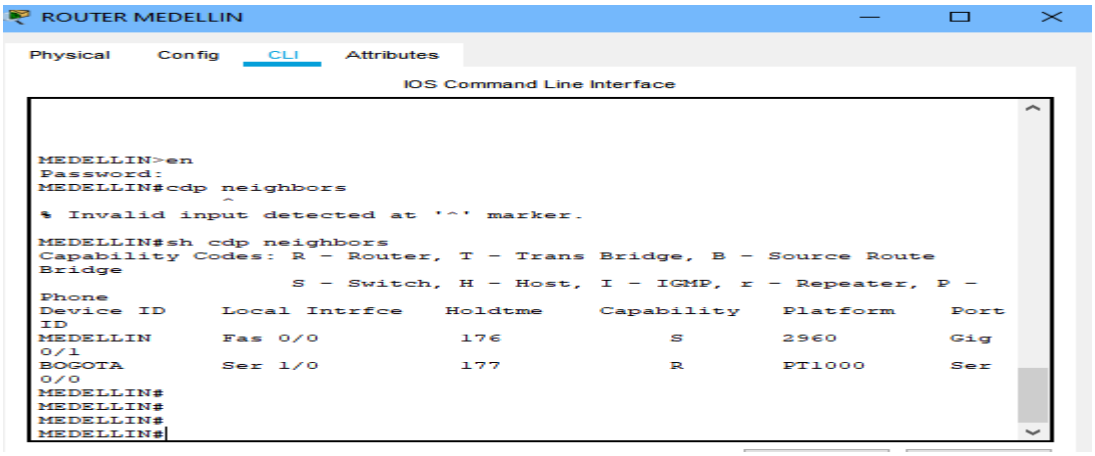

Figura 8-diagnóstico de vecinos Medellín

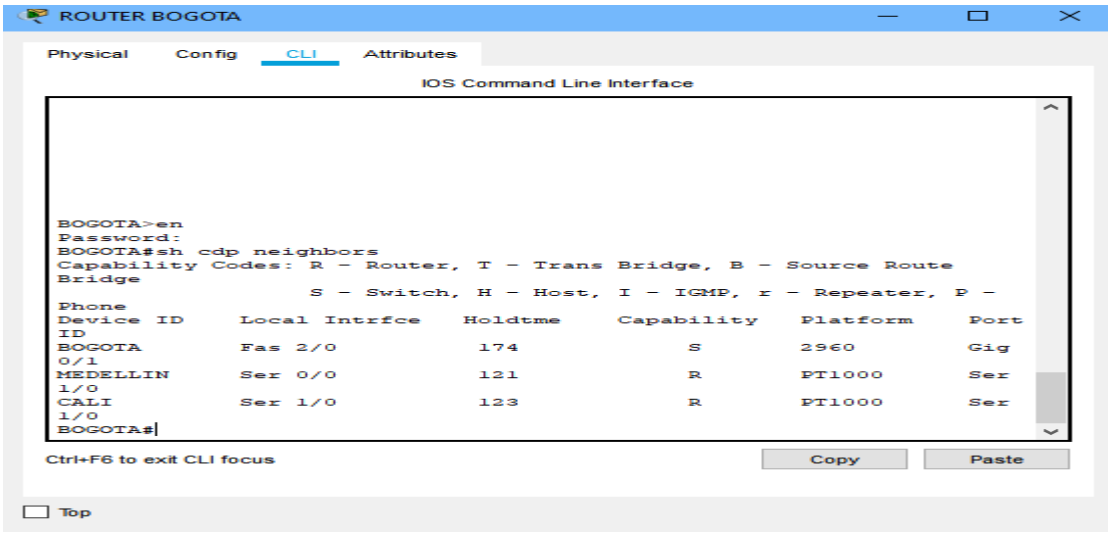

Figura 9-diagnóstico de vecindad Bogotá

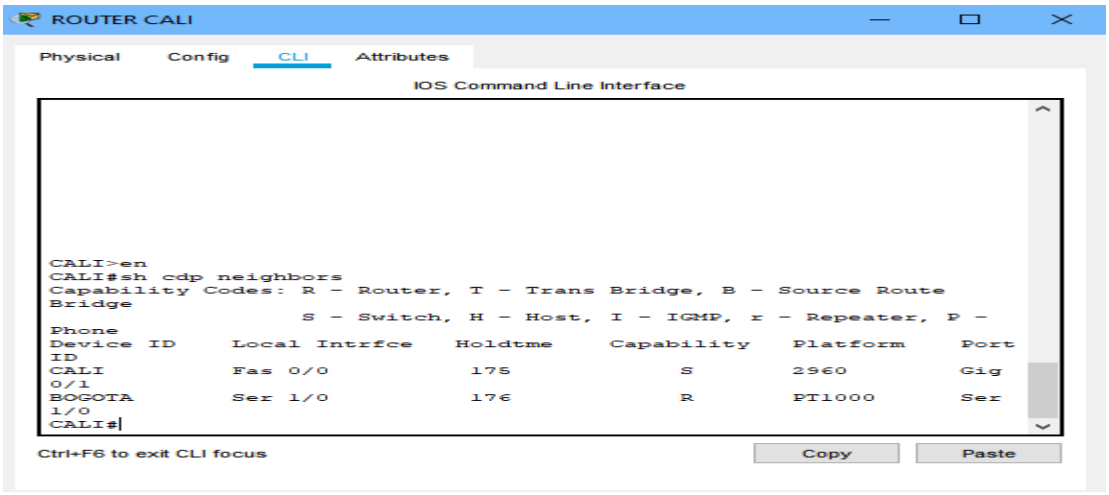

Figura 10-diagnóstico de vecinos Cali

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

192.168.1.99

192.168.1.131

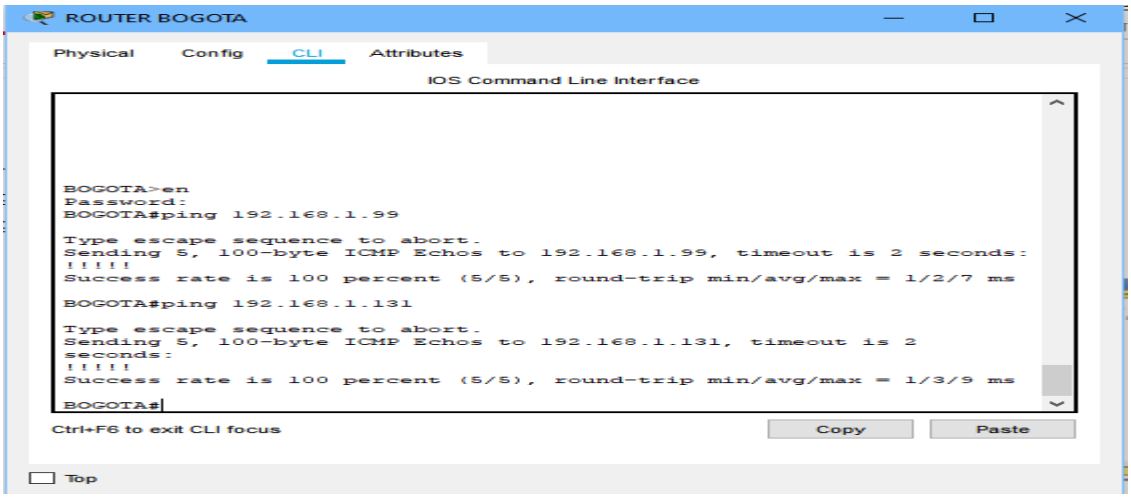

Figura 11-prueba de conectividad tramo

Parte 3: Configuración de Enrutamiento.

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

Enrutamiento router Medellín

#en #config t

#router eigrp 200

#network 192.168.1.32 0.0.0.31

#network 192.168.1.96 0.0.0.31

#no auto-summary

Enrutamiento router Cali

#en #config t

#router eigrp 200

#network 192.168.1.64 0.0.0.31

#network 192.168.1.128 0.0.0.31

#no auto-summary

Enrutamiento router Medellín

#en #config t

#router eigrp 200

#network 192.168.1.96 0.0.0.31

#network 192.168.1.128 0.0.0.31

#network 192.168.1.0 0.0.0.31

#no auto-summary

A. Verificar si existe vecindad con los routers configurados con EIGRP. #sh ip eigrp

neighbors

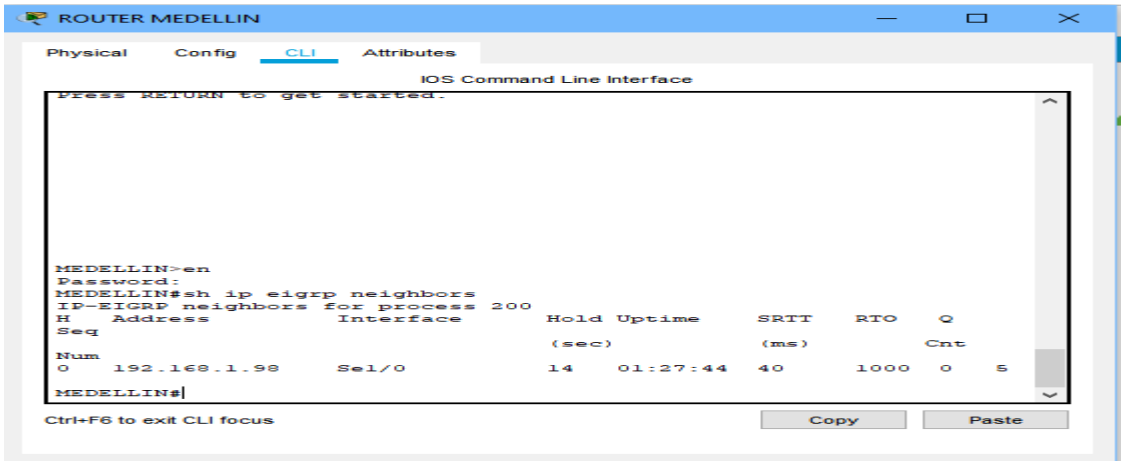

Figura 12-pruebas de vecindad router Medellín

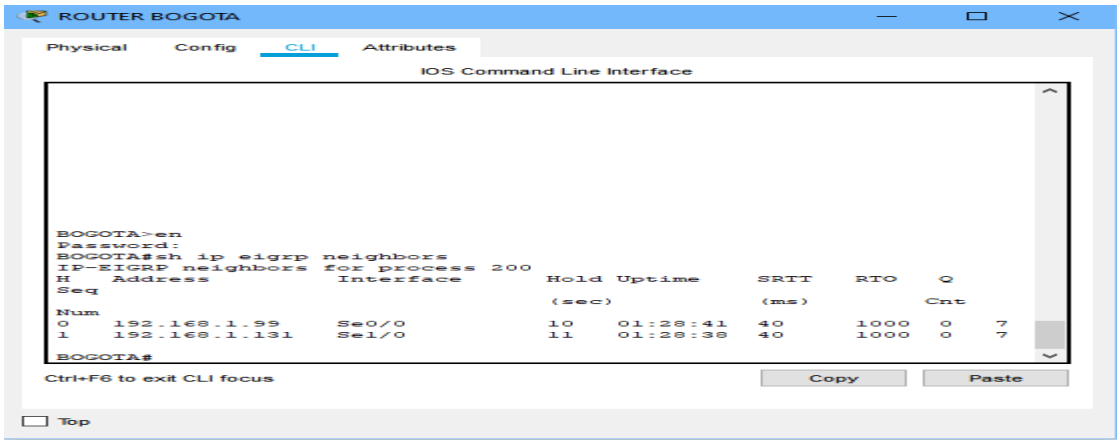

Figura 13-prueba de vecindad router Bogotá

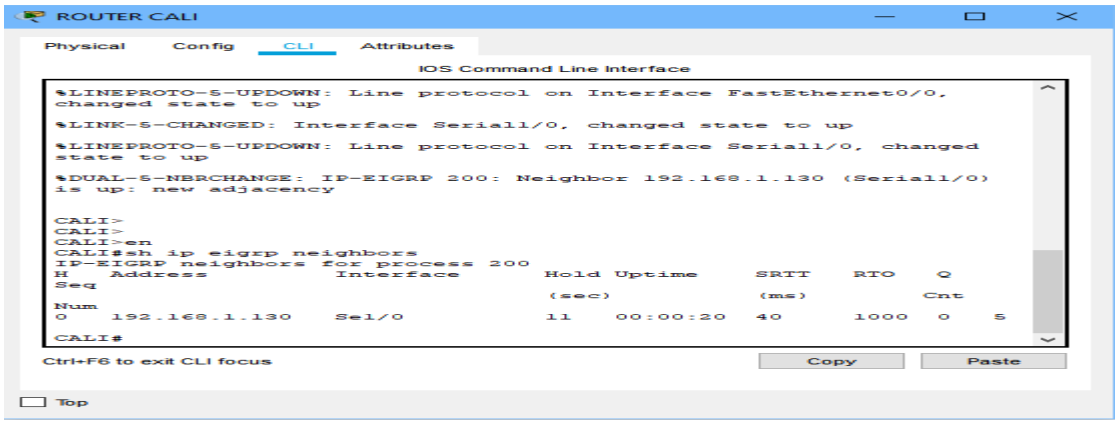

Figura 14-prueba de vecindad router Cali

A. Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas. #sh ip route

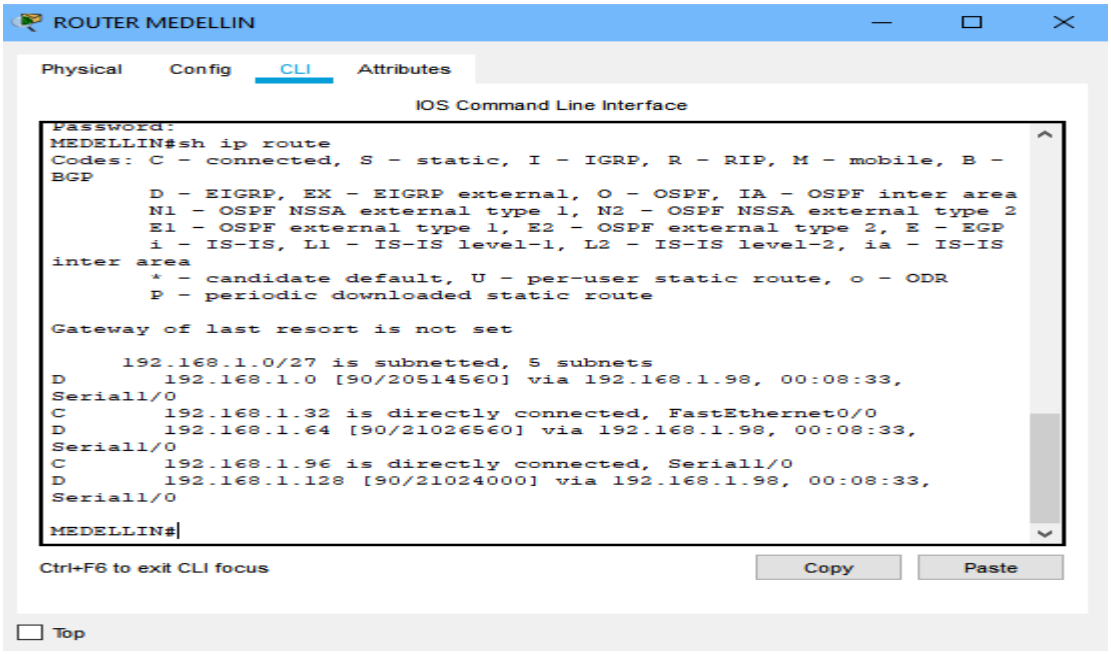

Figura 15-prueba de enrutamiento Medellín

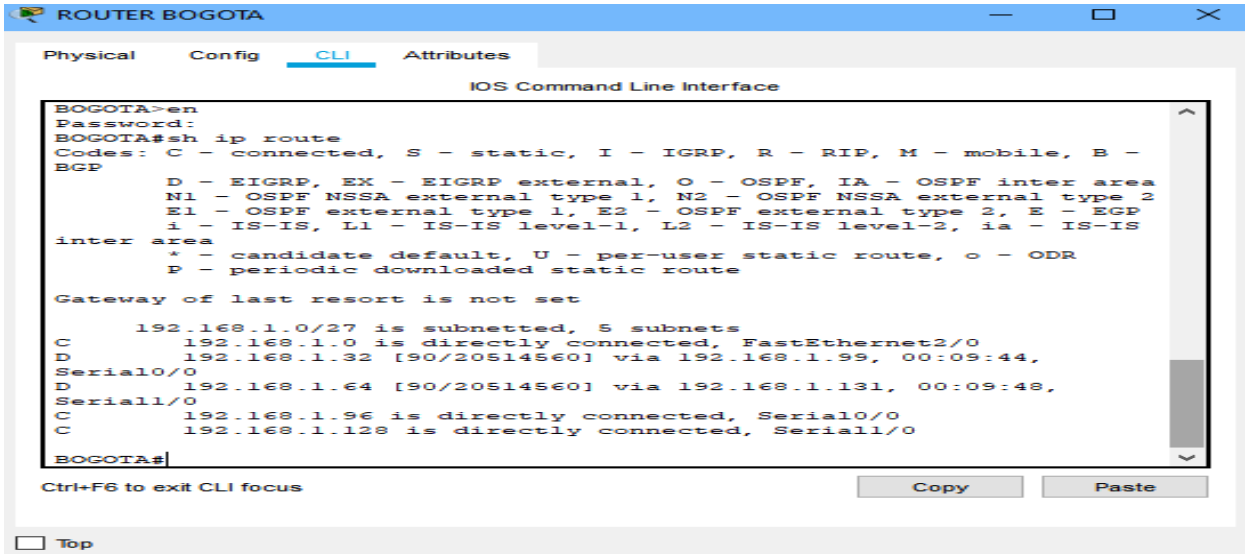

Figura 16-prueba de enrutamiento Bogotá

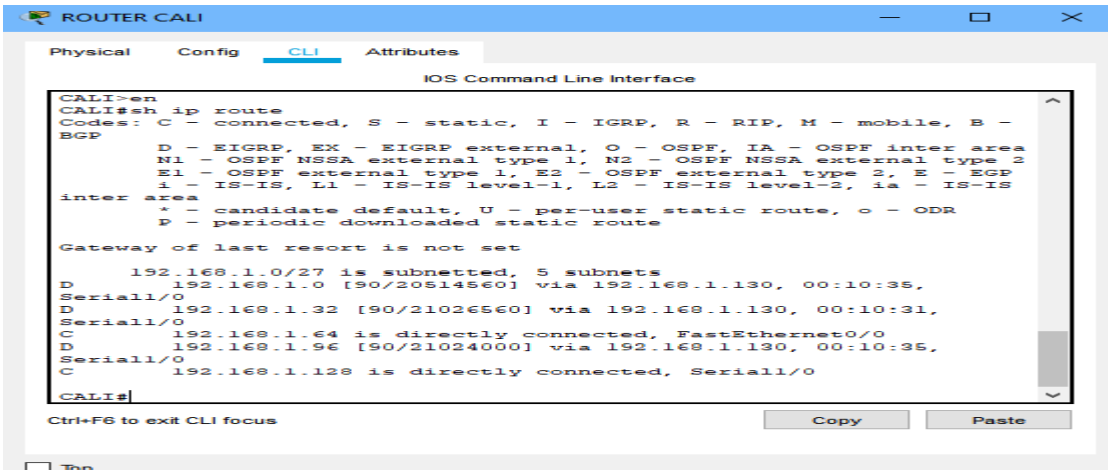

Figura 17-prueba de enrutamiento Cali

Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se pueda 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.

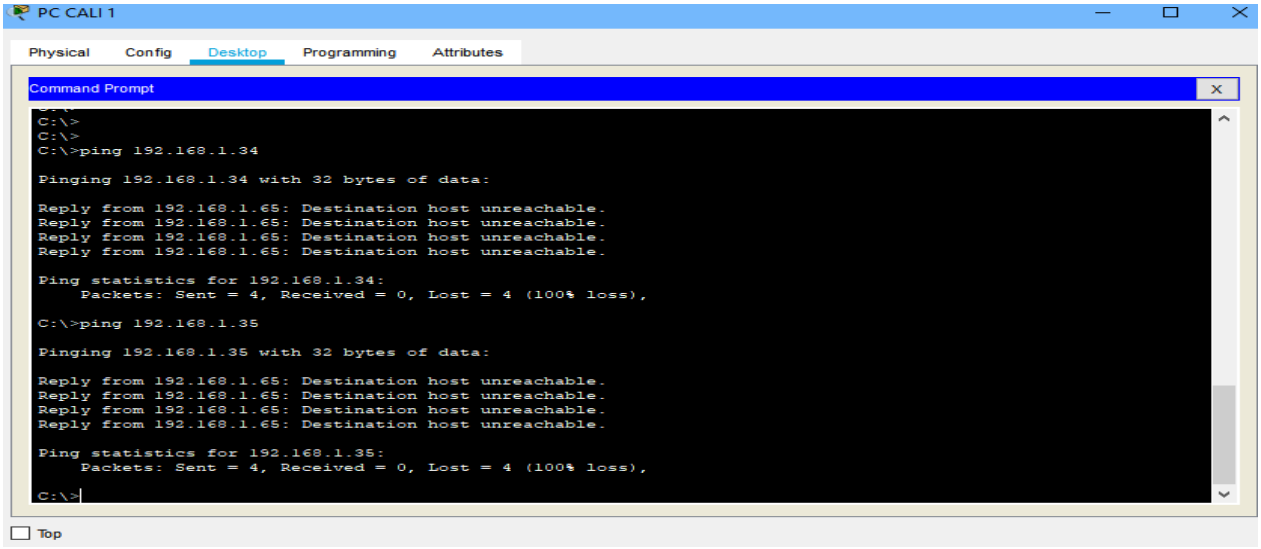

Figura 18-ping host red Medellín

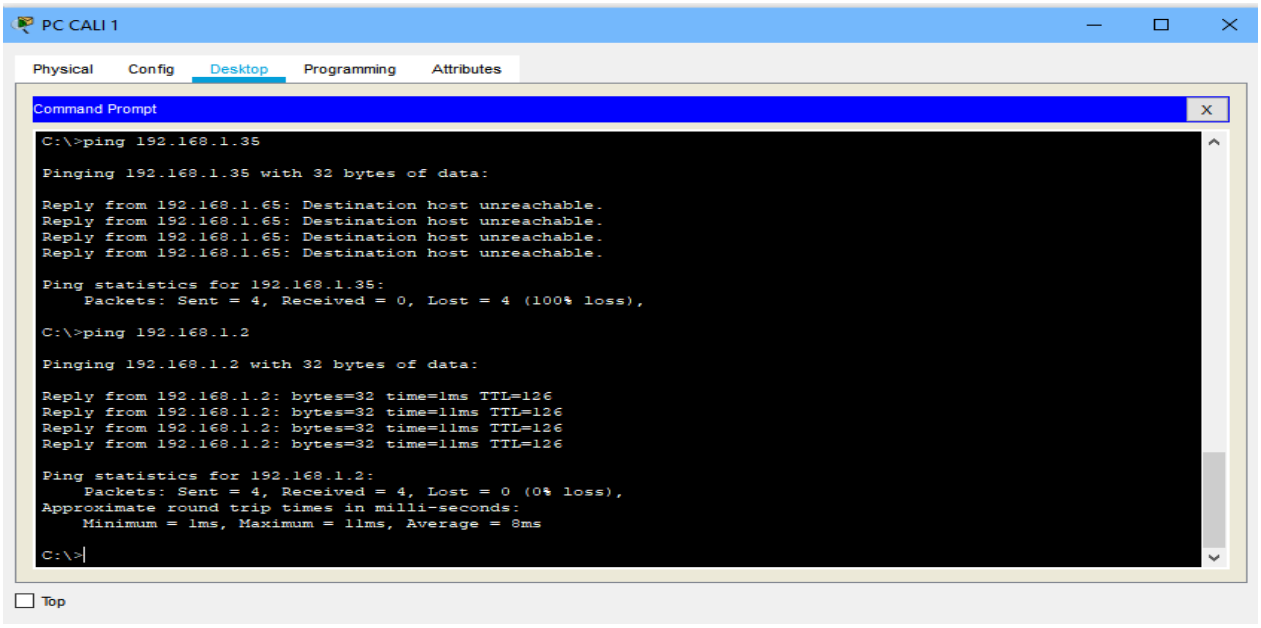

Figura 19-ping servidor Bogotá

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.

Configuración Telnet Medellín

#en
#config t #line vty 0 4
#password class #login
#exit

Configuración Telnet Bogotá
#en
#config t #line vty 0 4
#password class #login
#exit

Configuración Telnet Cali #en

#config t #line vty 0 4
#password class #login
#exit

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

Configuración Router Medellín y Cali

#access-list 110 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.2
#access-list 110 permit icmp any any echo-reply
#access-list 110 deny ip any any
#int fast0/0
#ip access-group 110 in

Configuración Router Bogotá

#access-list 110 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.2
#access-list 110 deny ip any
#int fast0/0
#ip access-group 110 out

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

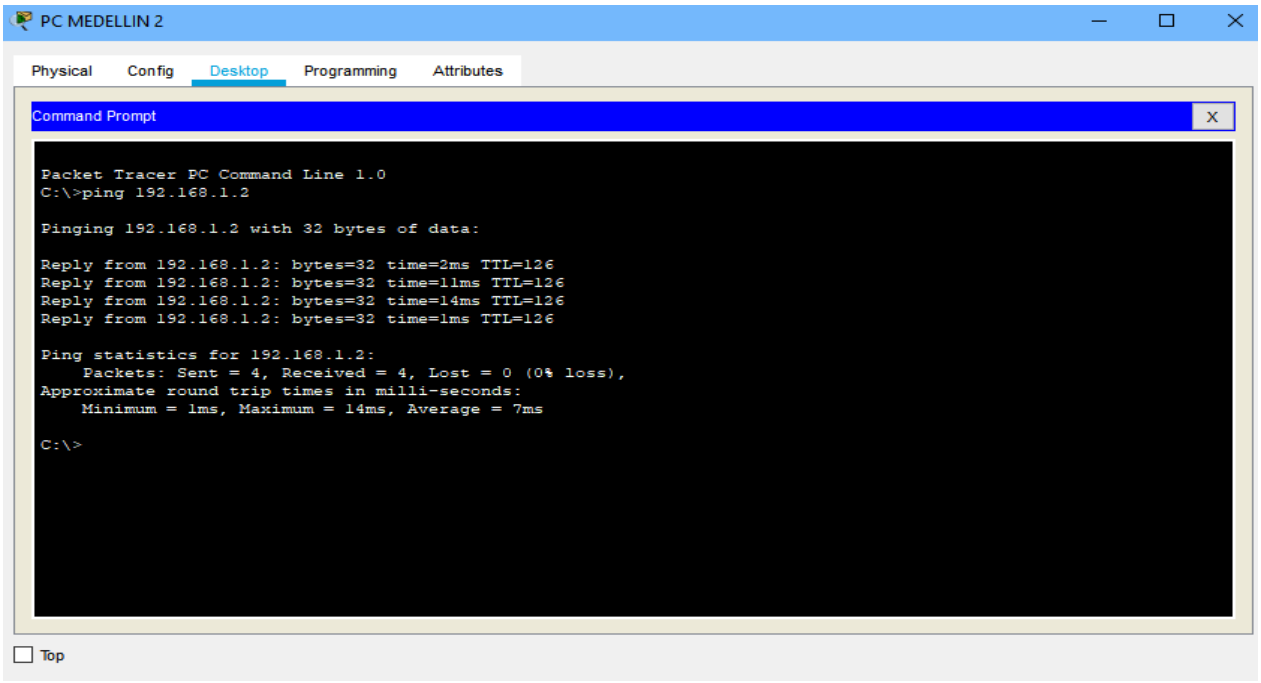

Figura 20-ping equipo Medellín al servidor

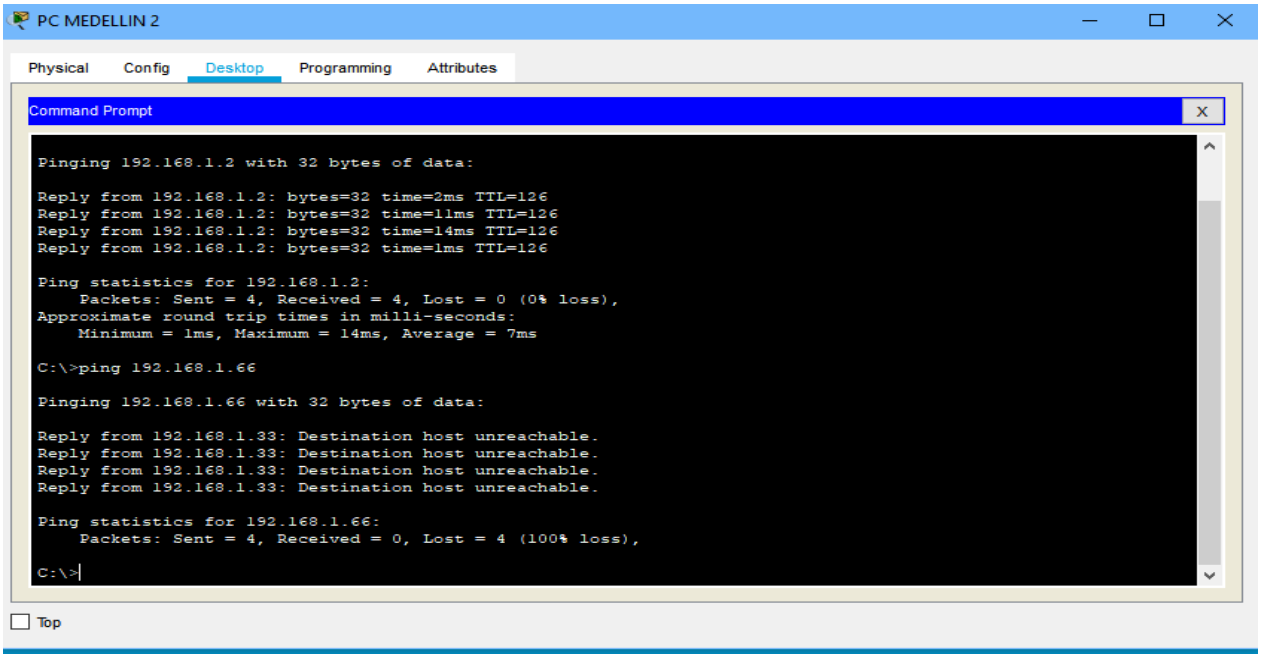

Figura 21-ping equipo Medellín a equipo Cali

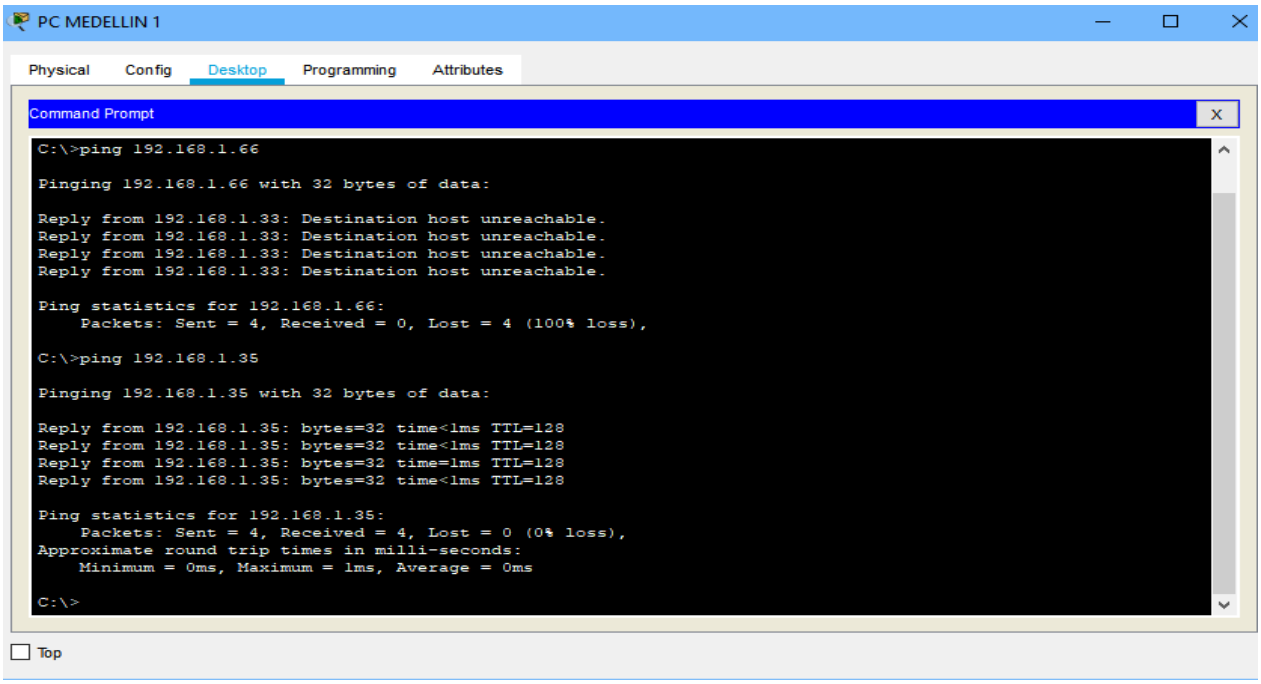

Figura 22-ping entre equipos entre la misma subred

Parte 5: Comprobación de la red instalada.

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

Router Medellín

#show access-list
Extended IP access list 110
10 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.2
20 permit icmp any any echo-reply
30 deny ip any any

Router Bogotá

#show access-list
Extended IP access list 110
10 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.2
20 deny ip any any

Router Cali

#show access-list
Extended IP access list 110
10 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.2
20 permit icmp any any echo-reply
30eny ip any any

A. Comprobar y completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red E.

ORIGEN	DESTINO	RESULTADO
Router MEDELLIN	**Router CALI**	Permitido
WS_1	**Router BOGOTA**	Permitido
Servidor	**Router CALI**	Permitido
Servidor	**Router MEDELLIN**	Permitido
LAN del Router MEDELLIN	**Router CALI**	Denegado
LAN del Router CALI	**Router CALI**	Denegado
LAN del Router MEDELLIN	**Router MEDELLIN**	Denegado
LAN del Router CALI	**Router MEDELLIN**	Denegado
LAN del Router CALI	**WS_1**	Denegado
LAN del Router MEDELLIN	**WS_1**	Denegado
LAN del Router MEDELLIN	**LAN del Router CALI**	Denegado
LAN del Router CALI	**Servidor**	Permitido
LAN del Router MEDELLIN	**Servidor**	Permitido
Servidor	**LAN del Router MEDELLIN**	Permitido
Servidor	**LAN del Router CALI**	Permitido
Router CALI	**LAN del Router MEDELLIN**	Permitido
Router MEDELLIN	**LAN del Router CALI**	Permitido

Tabla 3-Telnet

ESCENARIO 2

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

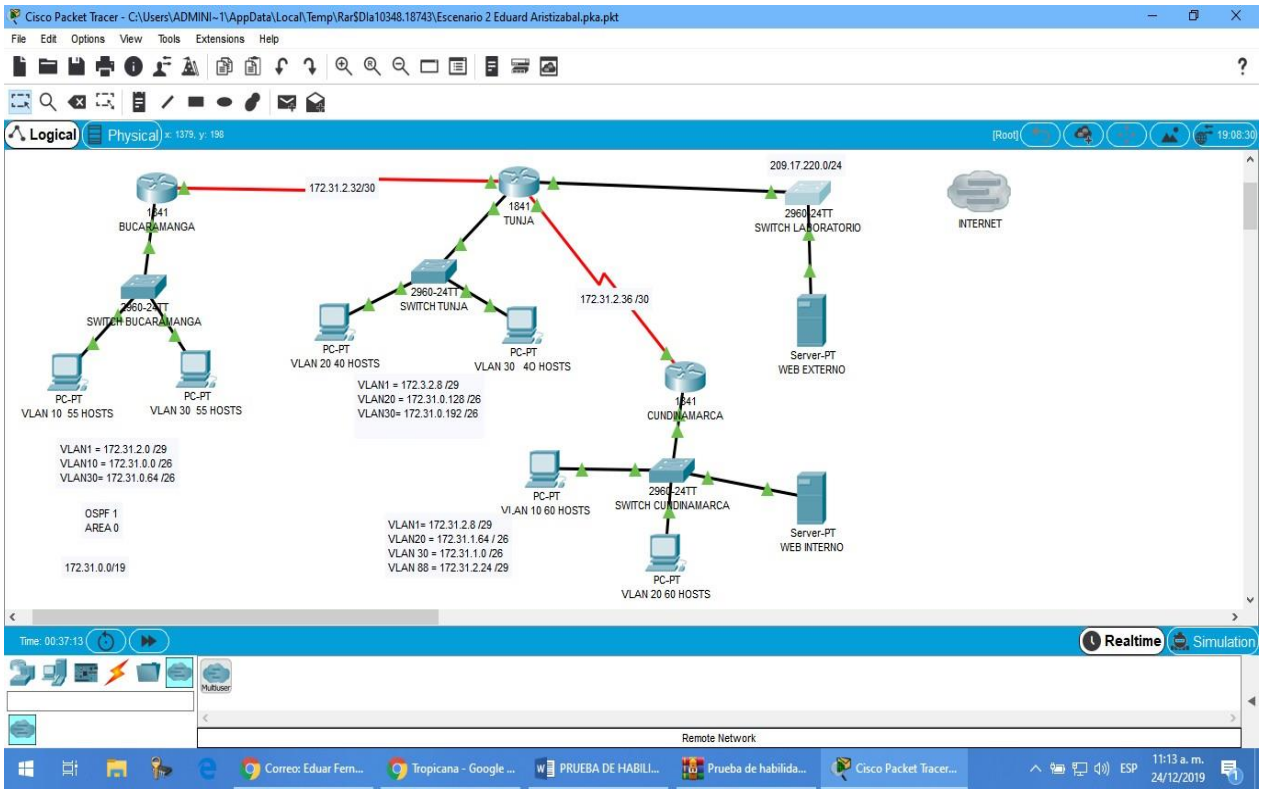

Figura 23-topología escenario 2

Desarrollo

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener el siguiente: Configuración básica.

ROUTER BUCARAMANGA

Router>en
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) #banner motd #ACCESO RESTRINGIDO#
BUCARAMANGA (config)#enable secret consola
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)#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) #
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) #
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 0BUCARAMANGA (config-router)#network 172.31.2.32 0.0.0.3 area 0 BUCARAMANGA(config-router)#end
BUCARAMANGA#
%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
%SYS-5-CONFIG_I: Configured from console by console

ROUTER TUNJA

Router>en 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)#banner motd #ACCESO RESTRINGIDO#
TUNJA(config)#enable secret cisco
TUNJA(config)#line console 0
TUNJA(config-line) #password consola
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) #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) # 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) # 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)#
TUNJA(config-if)#router ospf 1
TUNJA(config-router) #network 172.3.2.8 0.0.0.7 area 0
TUNJA(config-router) #network 172.31.0.128 0.0.0.63 area 0
TUNJA(config-router) #network 172.31.0.192 0.0.0.63 area 0
TUNJA(config-router) #network 172.31.2.32 0.0.0.3 area 0
TUNJA(config-router) #network 172.31.2.36 0.0.0.3 area 0
TUNJA(config-router) #end
TUNJA# TUNJA#
%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 Serial0/0/0, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%SYS-5-CONFIG_I: Configured from console by console

ROUTER CUNDINAMARCA

Router>en
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)#banner motd #Cuidado Acceso Restringido#
CUNDINAMARCA(config)#enable secret consola
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line) #password cisco123

```
CUNDINAMARCA(config-line) #login
CUNDINAMARCA(config-line)#logging synchronous
CUNDINAMARCA(config-line)#line vty 0 15
CUNDINAMARCA(config-line)#password consola
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#logging synchronous
CUNDINAMARCA(config)#int f0/0.1
CUNDINAMARCA(config-subif)#encapsulation dot1q 1
CUNDINAMARCA(config-subif)#ip address 172.31.2.9 255.255.255.248
CUNDINAMARCA(config-subif)#int f0/0.20
CUNDINAMARCA(config-subif)#encapsulation dot1q 20
CUNDINAMARCA(config-subif)#ip address 172.31.1.65 255.255.255.192
CUNDINAMARCA(config-subif)#int f0/0.30
CUNDINAMARCA(config-subif)#encapsulation dot1q 30
CUNDINAMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192
CUNDINAMARCA(config-subif)#int f0/0.88
CUNDINAMARCA(config-subif)#encapsulation dot1q 88
CUNDINAMARCA(config-subif)#ip address 172.31.2.25 255.255.255.248
CUNDINAMARCA(config-subif)#int f0/0
CUNDINAMARCA(config-if)#no shutdown
CUNDINAMARCA(config-if)# CUNDINAMARCA(config-a)#int s0/0/0
CUNDINAMARCA(config-if)#ip address 172.31.2.38 255.255.255.252
CUNDINAMARCA(config-if)#no shutdown
CUNDINAMARCA(config-if)#router ospf 1
CUNDINAMARCA(config-router)#network 172.31.1.0 0.0.0.63 area 0
CUNDINAMARCA(config-router)#network 172.31.1.64 0.0.0.63 area 0
CUNDINAMARCA(config-router)#network 172.31.2.8 0.0.0.7 area 0
CUNDINAMARCA(config-router)#network 172.31.2.24 0.0.0.7 area 0
CUNDINAMARCA(config-router)#network 172.31.2.36 0.0.0.3 area 0
CUNDINAMARCA(config-router)#end
CUNDINAMARCA#
```

%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
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%SYS-5-CONFIG_I: Configured from console by console

CUNDINAMARCA#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
CUNDINAMARCA#
00:14:55: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.220.1 on Serial0/0/0 from LOADING to FULL, Loading Done

SWITCH BUCARAMANGA

Switch>en Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW BUCARAMANGA
BUCARAMANGASW(config)#vlan 1
BUCARAMANGASW(config-vlan)#vlan 10
BUCARAMANGASW(config-vlan)#vlan 30
BUCARAMANGASW(config-vlan)#int f0/20
BUCARAMANGASW(config-if)#switchport mode access
BUCARAMANGASW(config-if)#switchport access vlan 10
BUCARAMANGASW(config-if)#int f0/24
BUCARAMANGASW(config-if)#switchport mode access
BUCARAMANGASW(config-if)#switchport access vlan 30
BUCARAMANGASW(config-if)#int f0/1
BUCARAMANGASW(config-if)#switchport mode trunk
BUCARAMANGASW(config-if)#int vlan 1
BUCARAMANGASW(config-if)#ip address 172.31.2.3 255.255.255.248

BUCARAMANGASW(config-if)#no shutdown

BUCARAMANGASW(config-if)#ip default-gateway 172.31.2.1
BUCARAMANGASW(config)#
BUCARAMANGASW(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

SWITCH TUNJA

Switch>en Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SWTUNJA
TUNJASW(config)#vlan 1
TUNJASW(config-vlan)#vlan 20
TUNJASW(config-vlan)#vlan 30
TUNJASW(config-vlan)#int f0/20
TUNJASW(config-if)#switchport mode access
TUNJASW(config-if)#switchport access vlan 20
TUNJASW(config-if)#int f0/24
TUNJASW(config-if)#switchport mode access
TUNJASW(config-if)#switchport access vlan 30 TUNJASW(config-if)#int f0/1
TUNJASW(config-if)#switchport mode trunk
TUNJASW(config-if)# TUNJASW(config-if)#int vlan 1
TUNJASW(config-if)#ip address 172.3.2.11 255.255.255.248
TUNJASW(config-if)#no shutdown
TUNJASW(config-if)#
TUNJASW(config-if)#ip default-gateway 172.3.2.9
TUNJASW(config)#
TUNJASW(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

SWITCH CUNDINAMARCA

Switch>en Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SWCUNDINAMARCA C
CUNDINAMARCASW(config)#vlan 1
CUNDINAMARCASW(config-vlan)#vlan 20
CUNDINAMARCASW(config-vlan)#vlan 30
CUNDINAMARCASW(config-vlan)#vlan 88
CUNDINAMARCASW(config-vlan)#exit
CUNDINAMARCASW(config)#int f0/20
CUNDINAMARCASW(config-if)#switchport mode access
CUNDINAMARCASW(config-if)#switchport access vlan 20
CUNDINAMARCASW(config-if)#int f0/24
CUNDINAMARCASW(config-if)#switchport mode access
CUNDINAMARCASW(config-if)#switchport access vlan 30
CUNDINAMARCASW(config-if)#int f0/10
CUNDINAMARCASW(config-if)#switchport mode access
CUNDINAMARCASW(config-if)#switchport access vlan 88
CUNDINAMARCASW(config-if)#int f0/1
CUNDINAMARCASW(config-if)#switchport mode trunk
CUNDINAMARCASW(config-if)#
CUNDINAMARCASW(config-if)#int vlan 1
CUNDINAMARCASW(config-if)#ip address 172.31.2.11 255.255.255.248
CUNDINAMARCASW(config-if)#no shutdown
CUNDINAMARCASW(config-if)#
CUNDINAMARCASW(config-if)#ip default-gateway 172.31.2.9
CUNDINAMARCASW(config)#
CUNDINAMARCASW(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
CUNDINAMARCASW(config)#

Autenticación local con AAA.

BUCARAMANGA(config-line)#username admin secret cisco
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

TUNJA(config-line)#username administrador secret cisco12345
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

CUNDINAMARCA(config-line)#username administrador secret cisco12345
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

Cifrado de contraseñas.

BUCARAMANGA(config)#service password-encryption
TUNJA(config)#service password-encryption
CUNDINAMARCA(config)#service password-encryption

Un máximo de internos para acceder al router.

BUCARAMANGA(config-line)#login block-for 5 attempts 4 within 60
TUNJA(config-line)#login block-for 5 attempts 4 within 60
CUNDINAMARCA(config-line)#login block-for 5 attempts 4 within 60

Máximo tiempo de acceso al detectar ataques.

BUCARAMANGA(config-line)#login block-for 5 attempts 4 within 60
TUNJA(config-line)#login block-for 5 attempts 4 within 60
CUNDINAMARCA(config-line)#login block-for 5 attempts 4 within 60

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

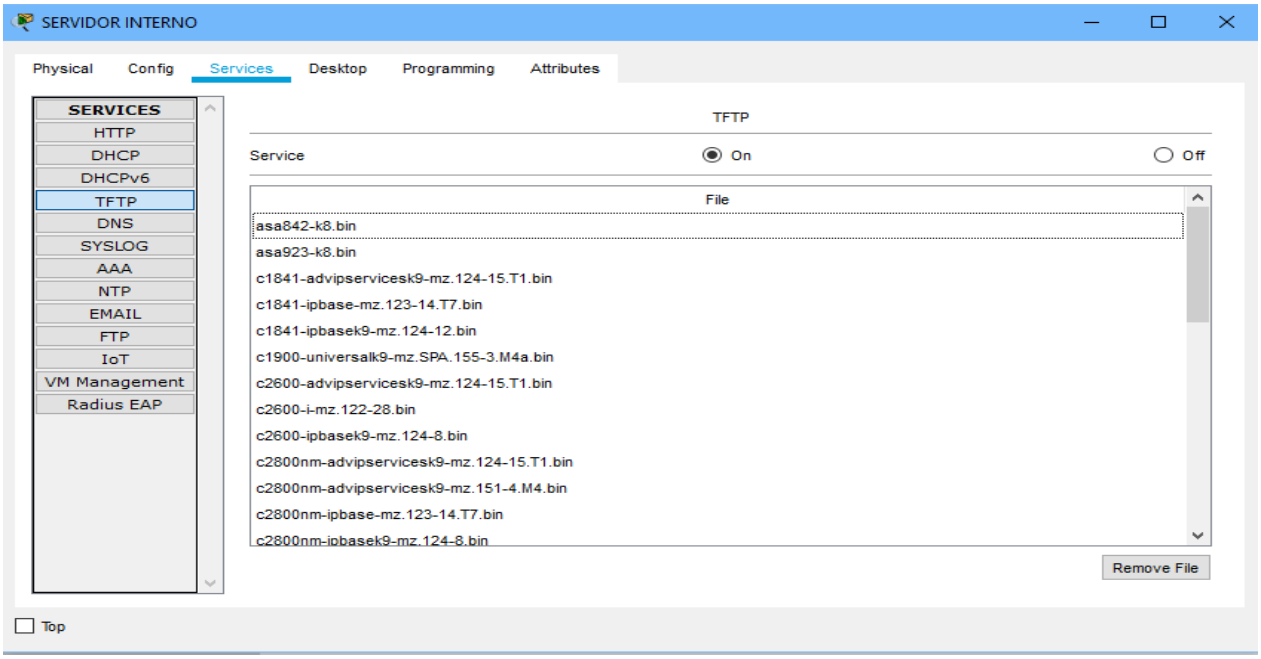

Figura 24-servidor tftp almacenamiento router

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

Tunja

```
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)#
```

Bucaramanga

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

Cundinamarca

```
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

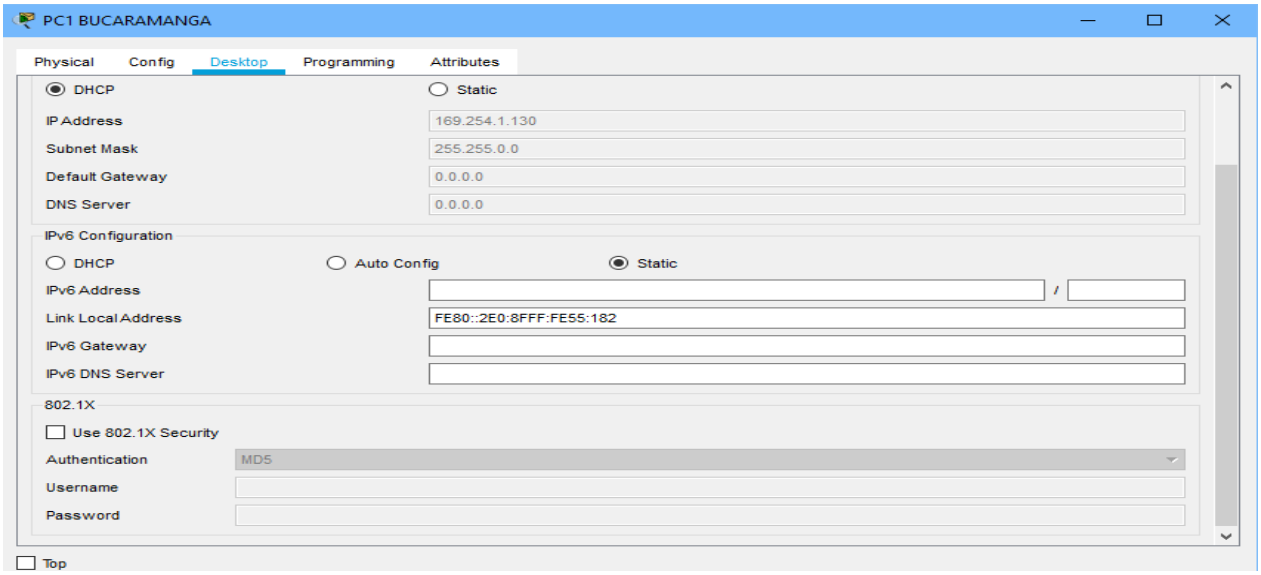

Figura 25-comprobación host Bucaramanga

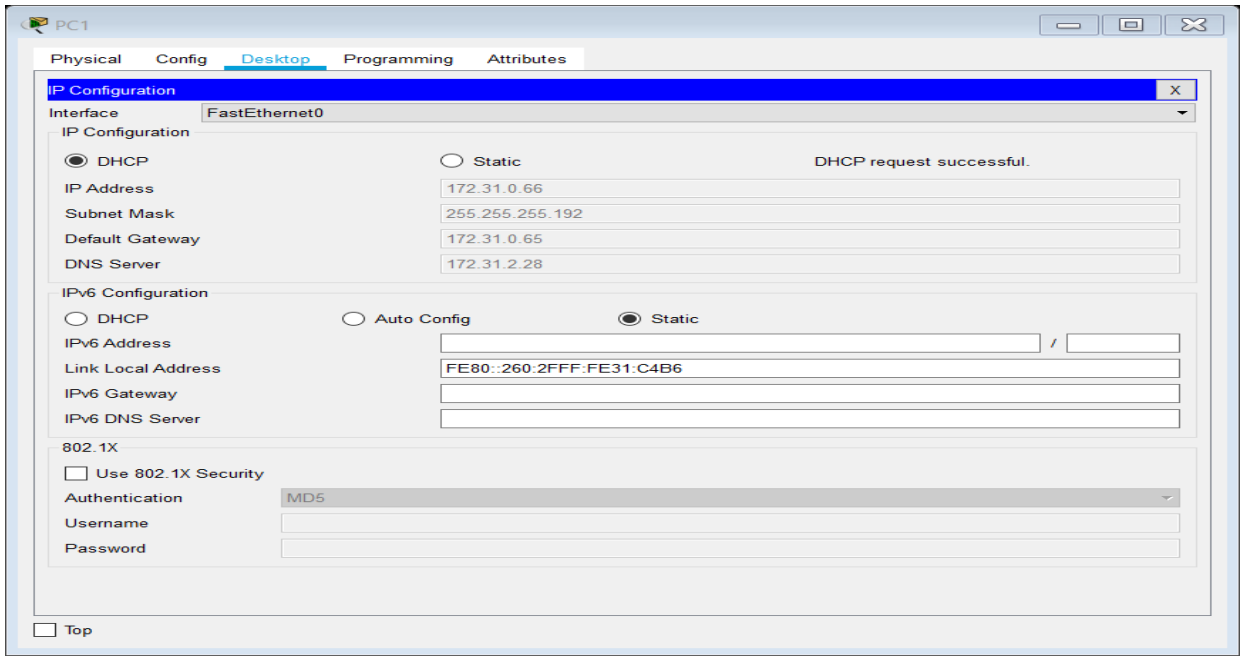

Figura 26-comprobación host Tunja

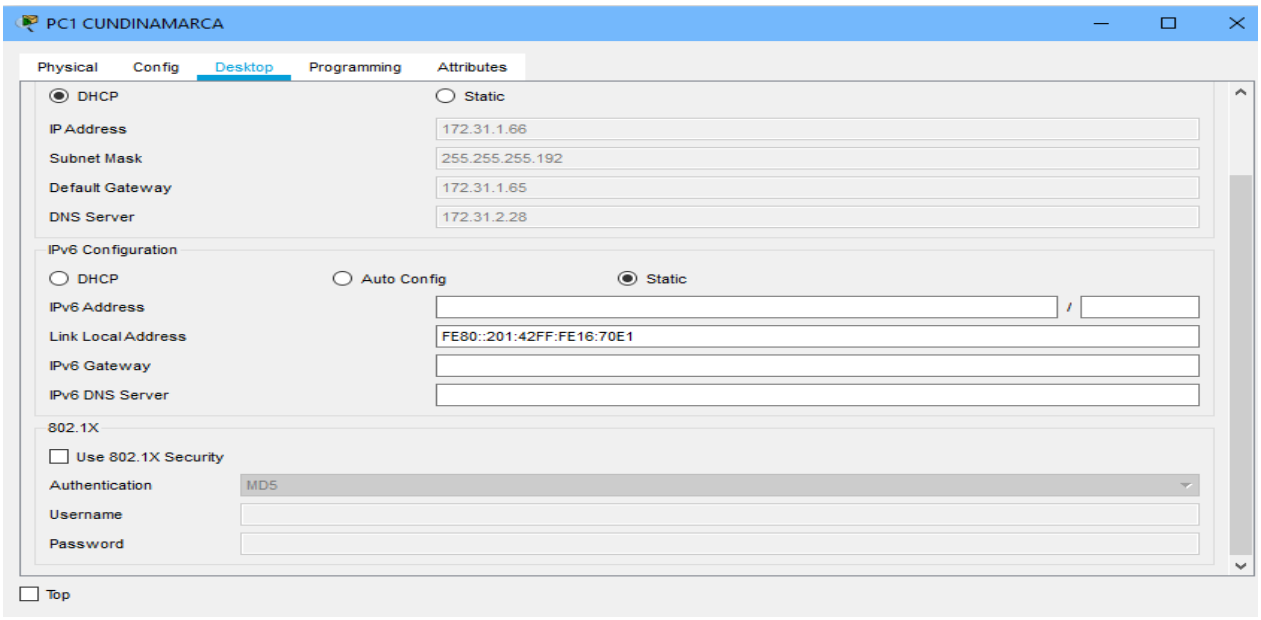

Figura 27-comprobación host Cundinamarca

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

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#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, 00:24:49, Serial0/0/0
O 172.31.0.64/26 [110/65] via 172.31.2.34, 00:24:49, 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, 00:23:33, Serial0/0/1
O 172.31.1.64/26 [110/65] via 172.31.2.38, 00:23:33, Serial0/0/1
O 172.31.2.0/29 [110/65] via 172.31.2.34, 00:24:49, Serial0/0/0
O 172.31.2.8/29 [110/65] via 172.31.2.38, 00:23:33, Serial0/0/1
O 172.31.2.24/29 [110/65] via 172.31.2.38, 00:23:33, Serial0/0/1
C 172.31.2.32/30 is directly connected, Serial0/0/0
C 172.31.2.36/30 is directly connected, Serial0/0/1
C 209.165.220.0/24 is directly connected, FastEthernet0/1
S* 0.0.0.0/0 [1/0] via 209.165.220.3

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, 00:25:08, 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, 00:25:08, Serial0/0/0
O 172.31.0.192/26 [110/65] via 172.31.2.33, 00:25:08, Serial0/0/0
O 172.31.1.0/26 [110/129] via 172.31.2.33, 00:23:42, Serial0/0/0
O 172.31.1.64/26 [110/129] via 172.31.2.33, 00:23:42, 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, 00:23:42, Serial0/0/0
O 172.31.2.24/29 [110/129] via 172.31.2.33, 00:23:42, Serial0/0/0
C 172.31.2.32/30 is directly connected, Serial0/0/0
O 172.31.2.36/30 [110/128] via 172.31.2.33, 00:24:02, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.31.2.33, 00:02:01, Serial0/0/0

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

Gateway of last resort is 172.31.2.37 to network 0.0.0.0

172.3.0.0/29 is subnetted, 1 subnets
O 172.3.2.8 [110/65] via 172.31.2.37, 00:24:15, Serial0/0/0
172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks
O 172.31.0.0/26 [110/129] via 172.31.2.37, 00:24:15, Serial0/0/0
O 172.31.0.64/26 [110/129] via 172.31.2.37, 00:24:15, Serial0/0/0
O 172.31.0.128/26 [110/65] via 172.31.2.37, 00:24:15, Serial0/0/0
O 172.31.0.192/26 [110/65] via 172.31.2.37, 00:24:15, Serial0/0/0
C 172.31.1.0/26 is directly connected, FastEthernet0/0.30
C 172.31.1.64/26 is directly connected, FastEthernet0/0.20
O 172.31.2.0/29 [110/129] via 172.31.2.37, 00:24:15, Serial0/0/0
C 172.31.2.8/29 is directly connected, FastEthernet0/0.1
C 172.31.2.24/29 is directly connected, FastEthernet0/0.88
O 172.31.2.32/30 [110/128] via 172.31.2.37, 00:24:15, Serial0/0/0
C 172.31.2.36/30 is directly connected, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.31.2.37, 00:02:24, Serial0/0/0

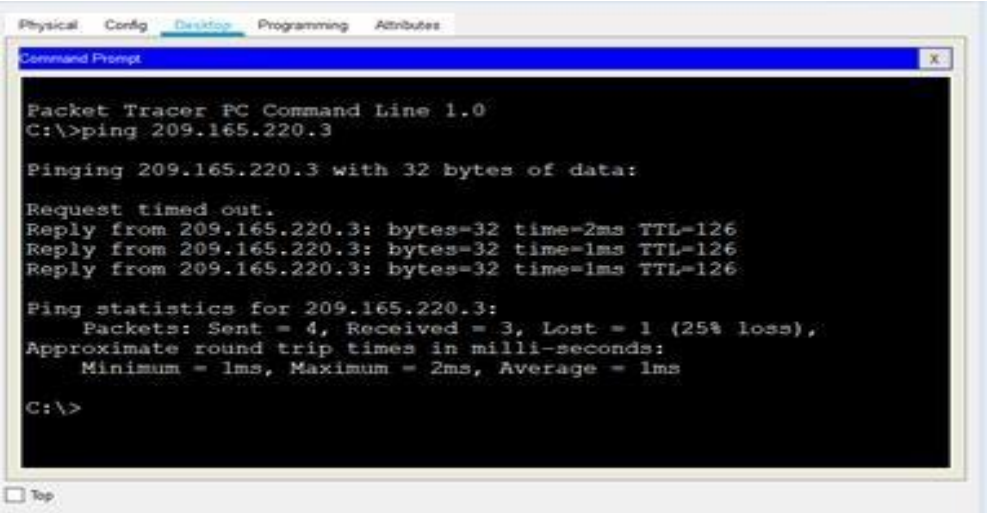

Figura 28-nat estático pruebas Cundinamarca

TUNJA#show ip nat translation
Pro Inside global Inside local Outside local Outside global
icmp 209.165.220.1:1 172.31.1.2:1 209.165.220.3:1 209.165.220.3:1
icmp 209.165.220.1:2 172.31.1.2:2 209.165.220.3:2 209.165.220.3:2
icmp 209.165.220.1:3 172.31.1.2:3 209.165.220.3:3 209.165.220.3:3
icmp 209.165.220.1:4 172.31.1.2:4 209.165.220.3:4 209.165.220.3:4
--- 209.165.220.4 172.31.2.28 --- ---

4.El enrutamiento deberá tener autenticación.

BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#int s0/0/0
BUCARAMANGA(config-if)#ip ospf authentication message-digest
BUCARAMANGA(config-if)#ip ospf message-digest-key 1 md5 cisco123
BUCARAMANGA(config-if)#

CUNDINAMARCA(config)#int s0/0/0
CUNDINAMARCA(config-if)#ip ospf authentication message-digest
CUNDINAMARCA(config-if)#ip ospf message-digest-key 1 md5 cisco123
CUNDINAMARCA(config-if)#

TUNJA#
00:30:20: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
00:30:20: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

TUNJA#
00:31:32: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.38 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Dead timer expired
00:31:32: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.38 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

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 cisco123
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 cisco123
TUNJA(config-if)#
00:31:40: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/0/0 from LOADING to FULL, Loading Done
TUNJA(config-if)#
00:31:42: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.38 on Serial0/0/1 from LOADING to FULL, Loading Done
TUNJA(config-if)#

5.Listas de control de acceso:
Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.

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)#

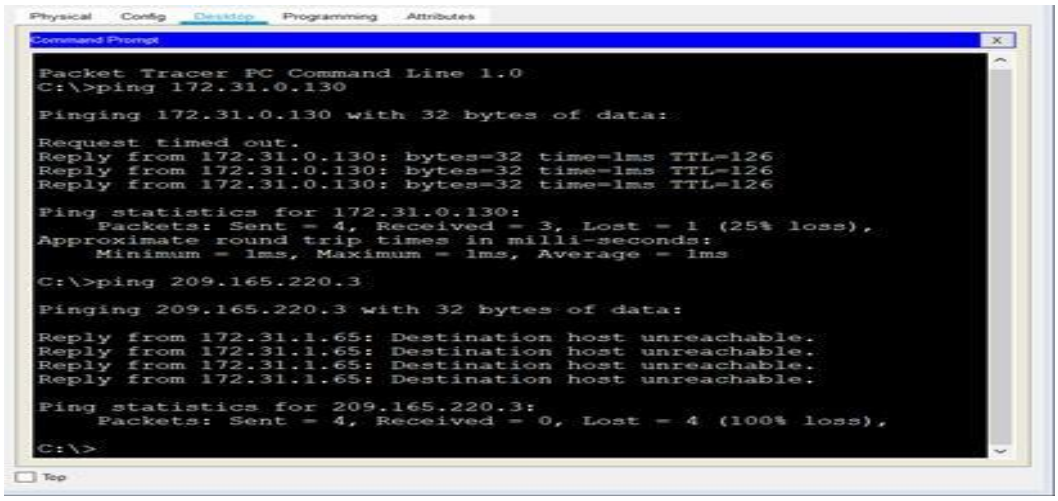

Figura 29-hosts vlan 20 Cundinamarca

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

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)#

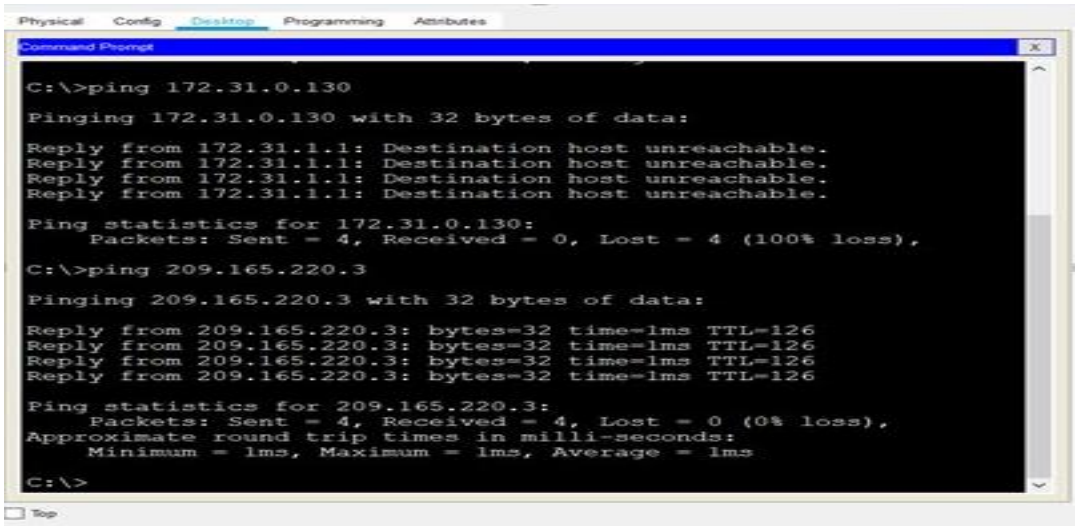

Figura 30-host vlan 10 Cundinamarca

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

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)#

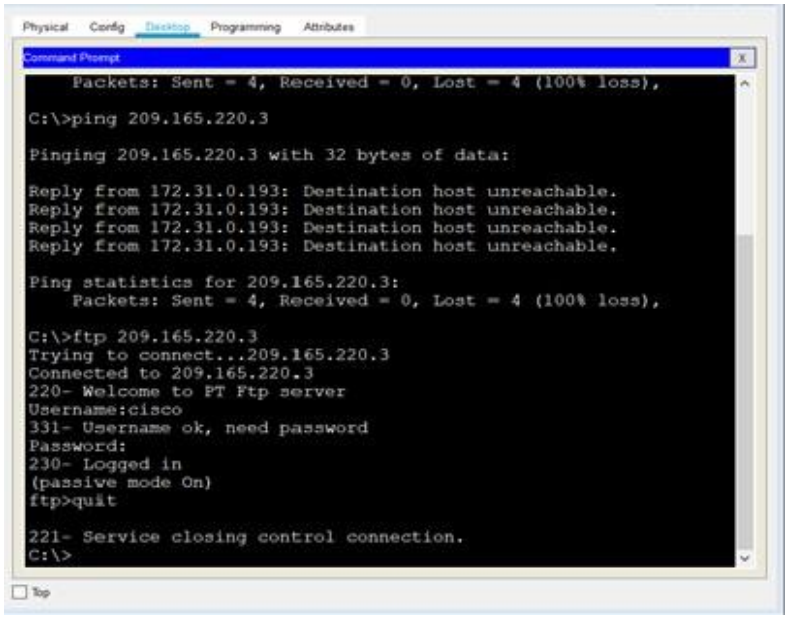

Figura 31-hosts vlan 30 Tunja

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 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)#

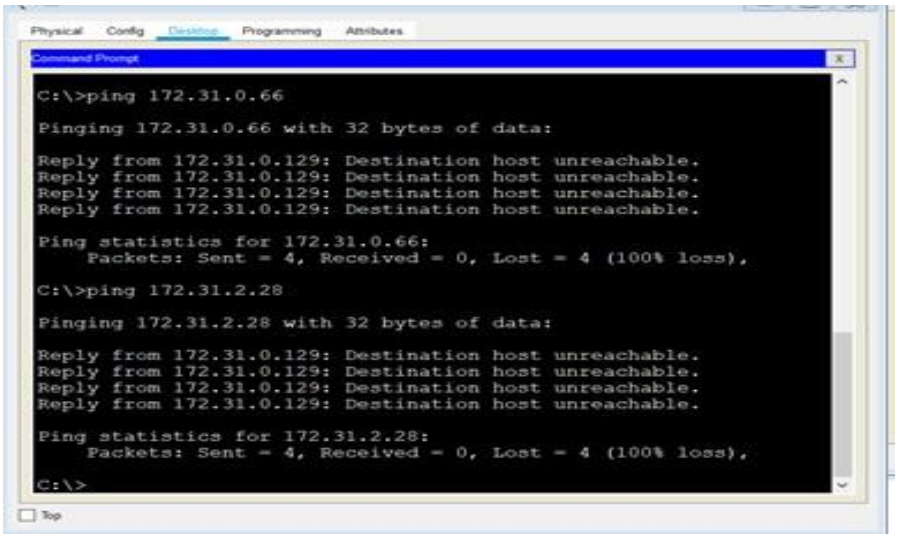

Figura 32-host Vlan 20 Cundinamarca

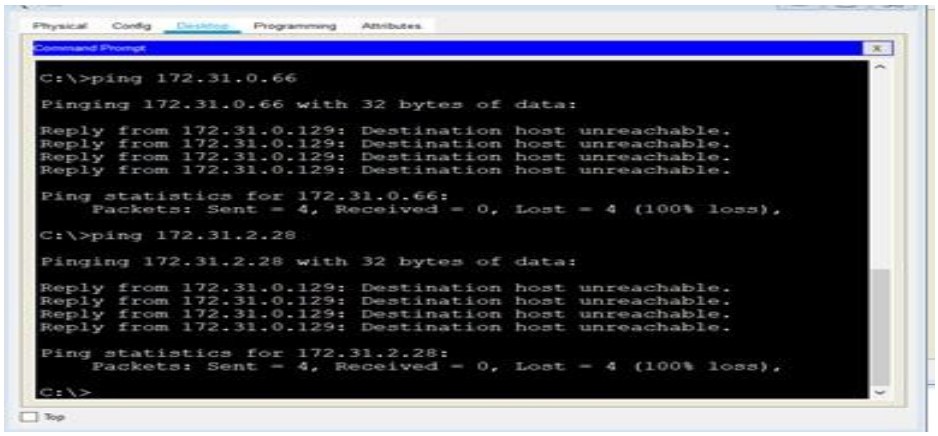

Figura 33-vlan 10 Bucaramanga

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

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)#

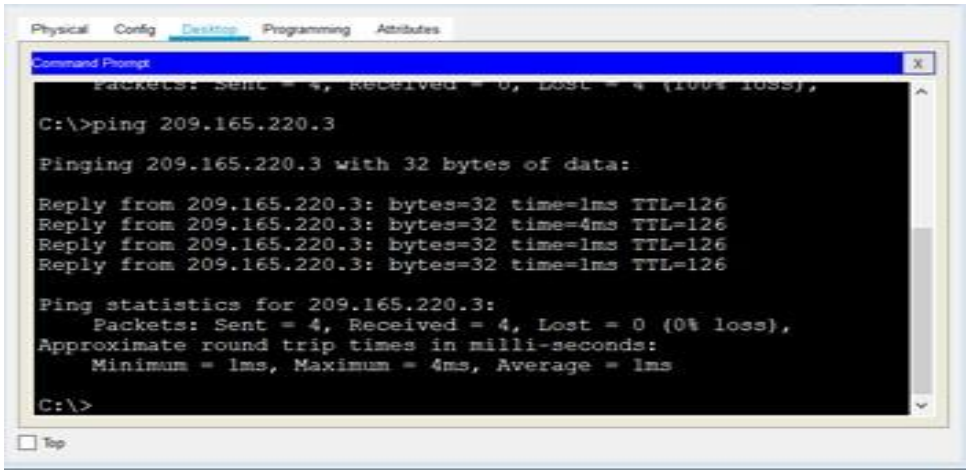

Figura 34-vlan 30 Bucaramanga

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 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)#

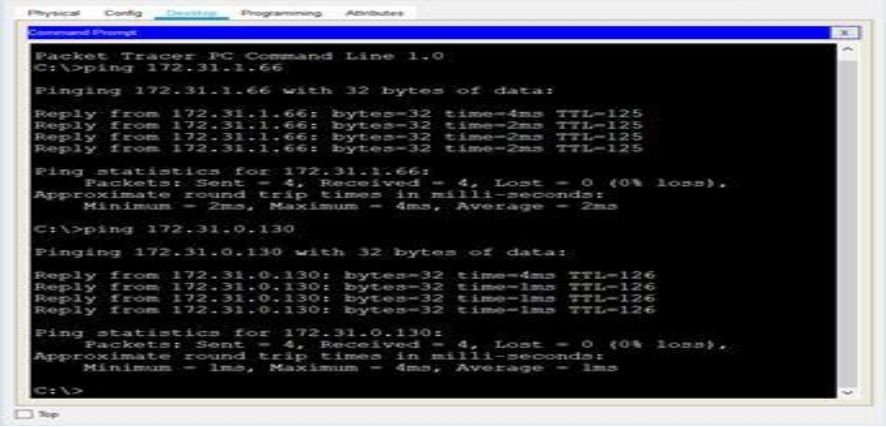

Figura 35-vlan 10 Bucaramanga

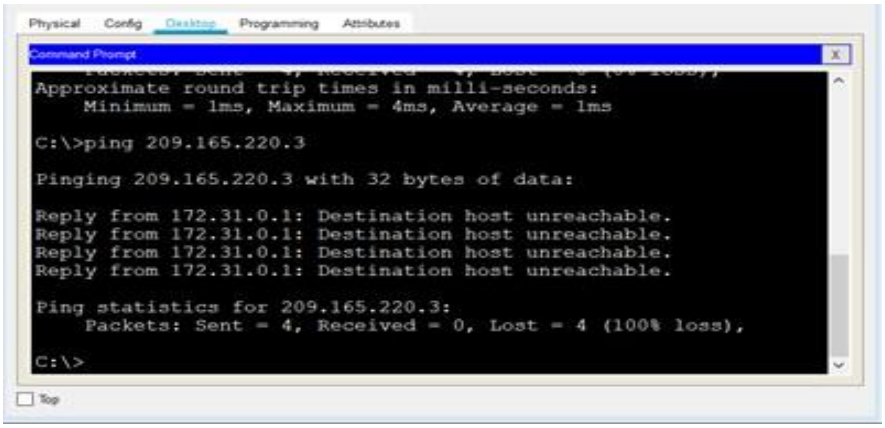

Figura 36-vlan 20 Tunja

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

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)#

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)#

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)#

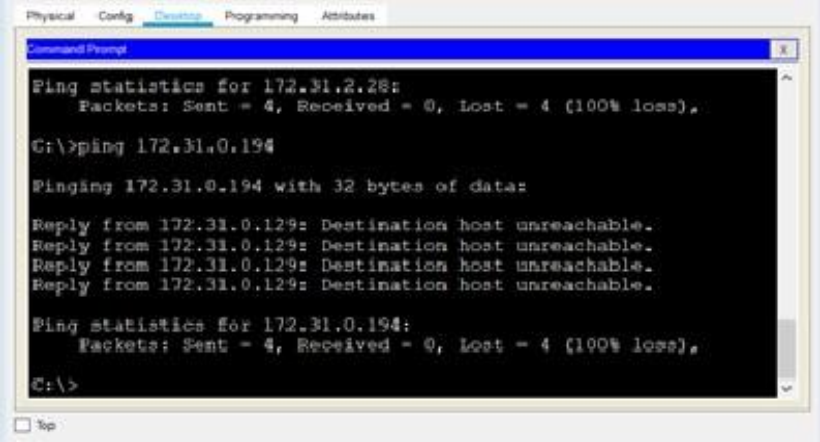

Figura 37-vlan Bucaramanga

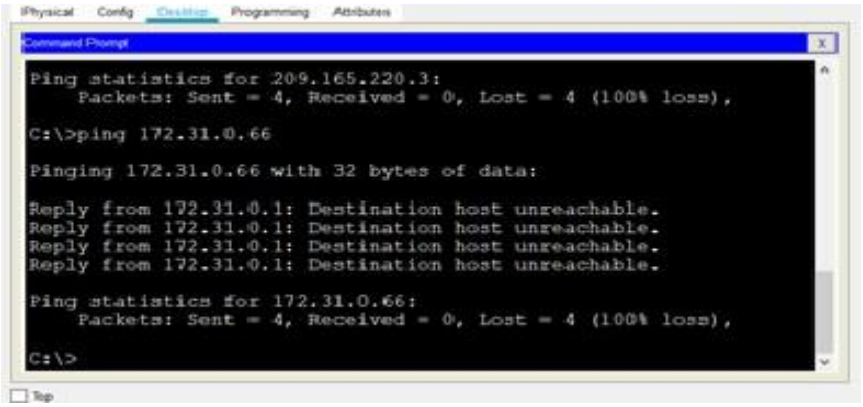

Figura 38-vlan Tunja

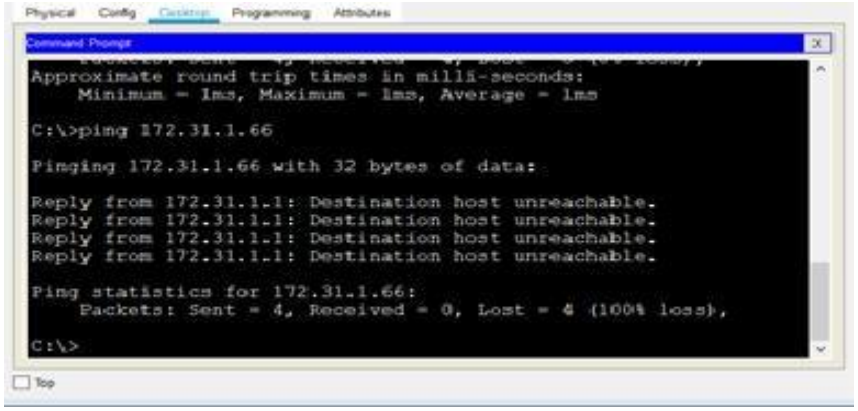

Figura 39-vlan Cundinamarca

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

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)#

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

```
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)#
```

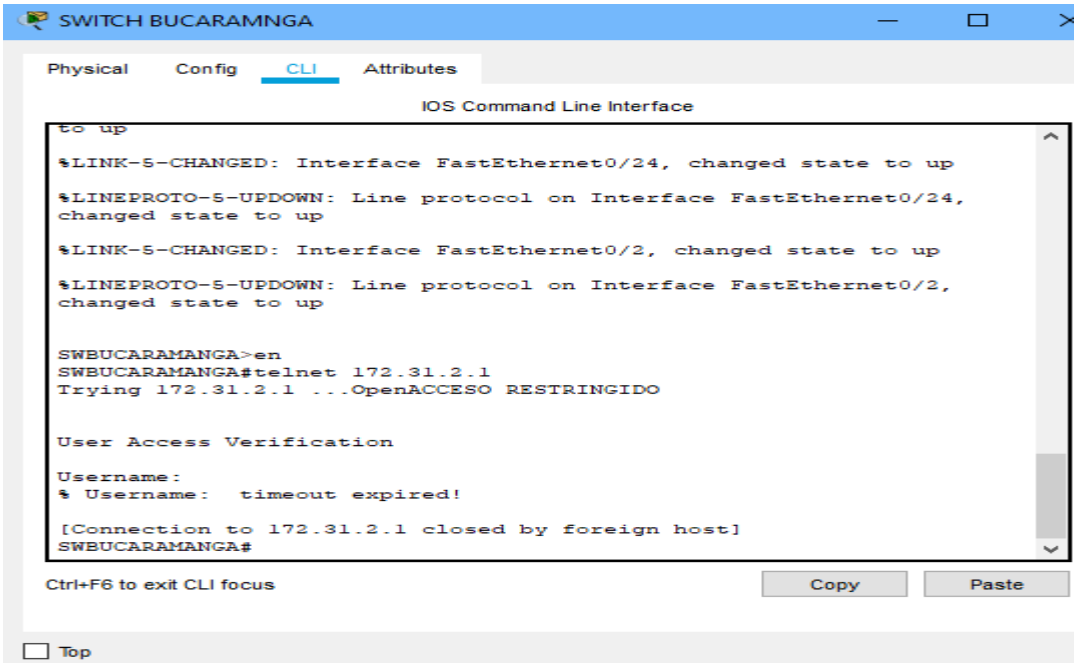

Figura 40-comprobación acceso

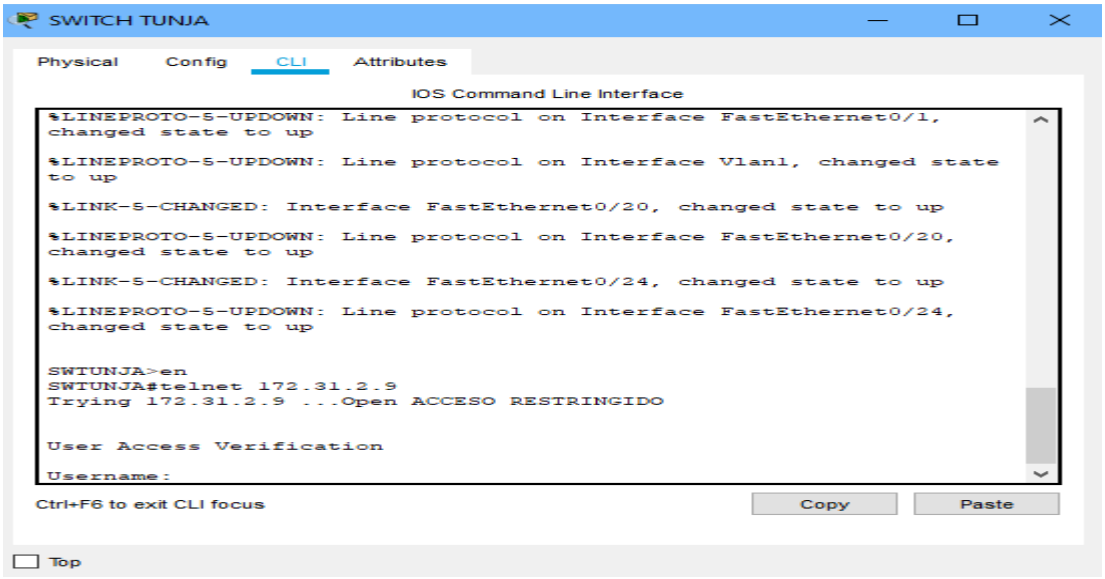

Figura 41-comprobación acceso

CONCLUSIONES

Con el desarrollo del trabajo anterior se dio respuesta y desarrollo a las actividades propuestas en los escenarios, poniendo a pruebas el conocimiento y destrezas desarrolladas durante el proceso de formación como la utilización del protocolo dhcp el cual nos permite asignar direcciones ip y el cual es aplicable para grandes redes, la utilización el aplicativo packet tracer en su versión 7.2.2 realizando el desarrollo correcto, la simulación y configuración de los dispositivos, logrando desarrollar un paso a paso de cada uno de los escenarios logrando la ejecución de los comandos como ping, trace,route, show ip router, entre otros; como también la verificación del direccionamiento IP, etherchannels y VLANs.

Es muy importante la aplicación y seguir practicando todos los temas visto durante el diplomado, para desarrollar mayores destrezas para mejorar y desempeñarlos en esta área tan importante del área TIC

REFERENCIAS BIBLIOGRÁFICAS

CISCO. (s.f.). Principios básicos de routing y switching: Listas de Control de Acceso. (2017), Tomado de: https://static-courseassets.s3.amazonaws.com/RSE503/es/index.html#9.0.1

Principios básicos de routing y switching: Traducción de direcciones de red para IPv4. (2017), Tomado de: https://static-courseassets.s3.amazonaws.com/RSE503/es/index.html#11.0

Tecnologías, S., Switching, L., VTP), V., & Configuración, N. (2018). Configuración de conexión troncal ISL y 802.1q entre un switch CatOS y un router externo (ruteo InterVLAN). Retrieved from https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-4000-series-switches/24064-171.html

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

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

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

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