DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

PRUEBA HABILIDADES PRACTICAS

SOLUCIÓN DE DOS ESTUDIOS DE CASO SOPORTADOS EN TECNOLOGÍA CISCO

PRESENTADO A

NILSON ALBEIRO FEREIRA

PRESENTADO POR

LEON SANTIAGO SANCHEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
INGENIERIA DE SISTEMAS
ESCUELA DE CIENCIAS BASICAS Y TECNOLOGIAS E INGENIERIAS
CEAD TURBO
2019

Tabla de contenido

Resumen 8
Abstrac 9
Introducción 10
Objetivos 11
General 11
Específicos 11
Descripción De los Escenarios Propuestos Para La Prueba De Habilidades 12
Escenario 1 12
Topología de red 12
Desarrollo Escenario 1 13
Parte 1: Asignación de direcciones IP: 13
Parte 2: Configuración Básica 14
Asignación de Direcciones IP Escenario 1 14
ROUTER BOGOTA 14
ROUTER MEDELLIN 16
ROUTER CALI 17
CONTRASEÑAS todos los dispositivos se configuraron con la contraseña leon2019 18
CONFIGURANDO LOS ROUTERS PARA EL LINE VTY 0 4 20
Realizar un diagnóstico de vecinos usando el comando cdp 21
PRUEBAS DE PING 24
Parte 3: Configuración de Enrutamiento. 28
SE CONFIGURA EL USO DEL PRPOTOCOLO DE ENRUTAMIENTO EIGRP EN EL ROUTER DE BOGOTA 28
SE CONFIGURA EL USO DEL PRPOTOCOLO DE ENRUTAMIENTO EIGRP EN EL ROUTER DE MEDELLIN 28
SE CONFIGURA EL USO DEL PRPOTOCOLO DE ENRUTAMIENTO EIGRP EN EL ROUTER DE BOGOTA 29
Parte 4: Configuración de las listas de Control de Acceso 29
RBOGOTA 30
RMEDELLIN 31
RCALI 31
a. Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red. 33
Escenario 2 38
Topologia 38
CONFIGURACIÓN DE ROUTERS 40
Se realizan las configuraciones indicadas de acceso y seguridad en el router tunja 40

RTUNJA 40
RCUNDINAMARCA 41
RBUCARAMANGA 43
CONFIGURACION DE SWTICHT 44
- Autenticación local con AAA 46
- Cifrado de contraseñas 47
- Un máximo de intentos para acceder al router 47
- Máximo tiempo de acceso al detectar ataques 47

Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers 48
El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y RCUNDINAMARCA 50
El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT). 52
El enrutamiento deberá tener autenticación. 54
Se Configuran Alas Acl, De Acuerdo A Especificaciones Del Escenario 2 En El Router De Cundinamarca, La Vlan 20 No Accede A Internet Solo A La Red Interna De Tunja, La Vlan 10 De Cundinamarca Accede A Inernet Y No A La Red Interna De Tunja. 55
Los hosts de VLAN 10 en RCUNDINAMARCA si acceden a interfaceernet y no a la red interfaceerna de RTUNJA. 56
Los hosts de VLAN 30 en RTUNJA solo acceden a servidores web y ftp de interfaz 57
Los hosts de VLAN 20 en RTUNJA solo acceden a la VLAN 20 de RCUNDINAMARCA y VLAN 10 de Bucaramanga 58
Los hosts de VLAN 30 de Bucaramanga acceden a interfaceernet y a cualquier equipo de VLAN 10. 60
Los hosts de VLAN 10 en Bucaramanga acceden a la red de RCUNDINAMARCA (VLAN 20) y RTUNJA (VLAN 20), no interfaz 61
Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad. 63
Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los routers e interfaz 65
Conclusiones 67
Bibliografía 68

Tabla de Imágenes

Imagen 1 Escenario I 12
Imagen 2 Diseño Físico de Red 13
Imagen 3 Verificación de vecindad Router Bogota con el comando CDP 21
Imagen 4 Verificación de vecindad Router Medellín con el comando CDP 22
Imagen 5 Verificación de vecindad Router Medellín con el comando CDP 23
Imagen 6 ping de RCALI a RBOGOTA 24
Imagen 7 Ping RMEDELLIN a RCALI 25
Imagen 8 ping RMEDELLIN a RBOGOTA 26
Imagen 9 ping RBOGOTA a RCALI 27
Imagen 10 Verificación acl desde pc2 Medellín a red Bogotá 32
Imagen 11 Verificación acl desde pc2 Medellín a red Cali 32
Imagen 12 Conexión Telnet Router Medellín a Router Cali 34
Imagen 13 Conexión telnet equipo WS1 a Router Bogota 34
Imagen 14 Conexión Telnet servidor a Router cali 35
Imagen 15 Conexión Telnet Servidor a Router Medellín 35
Imagen 16 Conexión Telnet PC3 a Router Cali 36
Imagen 17 Conexión Telnet PC1 a Router Medellín 36
Imagen 18 prueba ping RMedellin 37
Imagen 19 ping Rcali 37
Imagen 20 Topología Escenario 2 38
Imagen 21 Configuración Ip Servidor TFTP 48
Imagen 22 habilitación de servicios TFTP 49
Imagen 23 Habilitación DHCP PC0 51
Imagen 24 Habilitación DHCP PC1 51
Imagen 25 Habilitación DHCP PC4 51
Imagen 26 Habilitación DHCP PC5 52
Imagen 27 Los hosts de VLAN 20 en RCUNDINAMARCA no acceden a interfaceernet, solo a la red interfaceerna de RTUNJA 55
Imagen 28 Los hosts de VLAN 10 en RCUNDINAMARCA si acceden a interfaceernet y no a la red interfaceerna de RTUNJA 56
Imagen 29 Los hosts de VLAN 30 en RTUNJA solo acceden a servidores web y ftp de interfaz 57
Imagen 30 Los hosts de VLAN 30 en RTUNJA solo acceden a servidores web y ftp de interfaz 58
Imagen 31 Los hosts de VLAN 20 en RTUNJA solo acceden a la VLAN 20 de RCUNDINAMARCA y VLAN 10 de Bucaramanga 59
Imagen 32 Los hosts de VLAN 20 en RTUNJA solo acceden a la VLAN 20 de RCUNDINAMARCA y VLAN 10 de Bucaramanga 60
Imagen 33 Los hosts de VLAN 30 de Bucaramanga acceden a interfaceernet y a cualquier equipo de VLAN 10. 61
Imagen 34 Los hosts de VLAN 10 en Bucaramanga acceden a la red de RCUNDINAMARCA (VLAN 20) y RTUNJA (VLAN 20), no interfaz 62
Imagen 35 Los hosts de VLAN 10 en Bucaramanga acceden a la red de RCUNDINAMARCA (VLAN 20) y RTUNJA (VLAN 20), no interfaz 63
Imagen 36 Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad. 64
Imagen 37 Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad. 64
Imagen 38 Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad. 65
Imagen 39 Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los routers e interfaz 66

Resumen

El presente trabajo aborda el desarrollo de los conocimientos adquiridos durante la realización del diplomado como opción de grado CNNA impartido por parte de la UNAD, El diplomado de Diseño e Implementación de Soluciones Integradas LAN – WAN, se basa en la plataforma CISCO la cual es una empresa líder a nivel mundial en brindar soluciones de conectividad e implementación de redes que van desde una LAN en un hogar hasta una WAM a nivel mundial. En este trabajo se abordan 2 escenarios donde en el primer escenario una empresa posee tres sucursales siendo Bogotá la principal interconectando a las Sucursales de Cali y Medellín las cuales se interconectaron entre si al igual que cada una tiene su propia LAN, a los dispositivos se les implementan las medidas de seguridad, distribución de carga, subredes, accesos y restricciones a nivel administrativo.

Abstrac

The present work deals with the development of the knowledge acquired during the completion of the diploma as a CNNA degree option taught by the UNAD, The Diploma of Design and Implementation of Integrated Solutions LAN - WAN, is based on the CISCO platform which is a world-leading company in providing connectivity solutions and network implementation ranging from a LAN in a home to a WAM worldwide. This paper deals with 2 scenarios where in the first scenario a company has three branches, Bogotá being the main one interconnecting the Branches of Cali and Medellin, which interconnected with each other, as each one has its own LAN, the devices are implement security measures, load distribution, subnets, access and restrictions at the administrative level.

Introducción

En este trabajo se abordaron dos escenarios, donde se realizó el diseño y configuración de dos WAN de acuerdo con los criterios suministrados donde se efectuaron la configuración desde 0 de todos los elementos que conforman cada WAN de cada escenario, a los que se le implementaron políticas de seguridad, creación de subredes, balanceo de carga, DHCP, ACL, NAT entre otras

Se mostrará los diversos comandos necesarios para poder lograr dichas configuraciones de manera exitosa.

La solución a los escenarios se realizo en el programa Packet Tracer, en el cual se desarrollo cada uno de los requerimientos propuestos, con la finalidad de aplicar los conocimientos y habilidades adquiridas durante el desarrollo del diplomado.

Objetivos

General

La implementación de 2 redes WAN aplicando los parámetros de conectividad IPV4, Seguridad en los Routers y Switch, creaciones de VLAN, y habilitación de diversos servicios.

Específicos

Cumplir con los siguientes objetivos específicos, para la adquisición de competencias y habilidades ante problemas típicos de Networking

- Identificar que dispositivos utilizar para la construcción de una topología de red.
- Inicializar dispositivos de Networking
- Realizar configuración básica a dispositivos de comunicación como Routers, Switch, Servidores.
- Implementar seguridad en Switch, elaboración de Vlans e inter Vlan Routing.
- Implementar de DHCP y NAT en dispositivos de comunicación.
- Configurar y verificar listas de control de acceso ACL
- Verificar conectividad entre los dispositivos de una topología.

Descripción De los Escenarios Propuestos Para La Prueba De Habilidades

Escenario 1

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

Topología de red

Los requerimientos solicitados son los siguientes:

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

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

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

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

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

Parte 6: Configuración final.

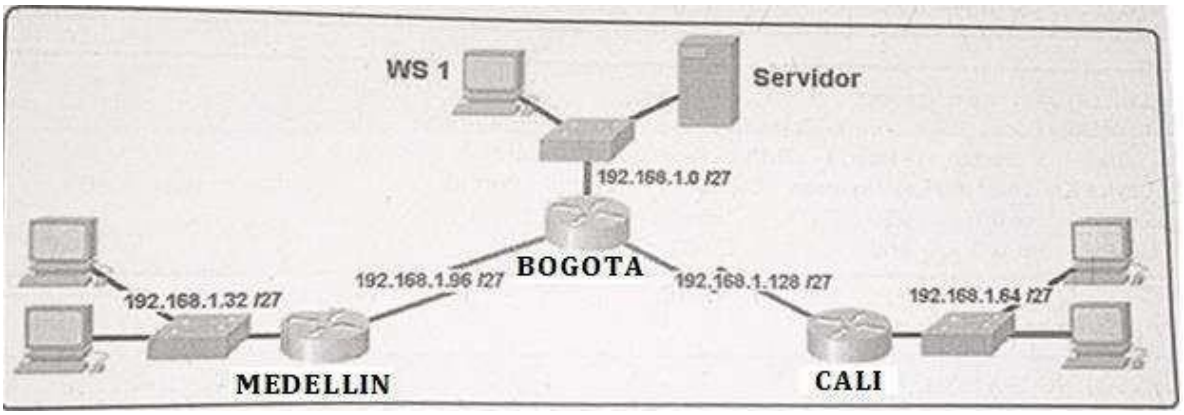

Imagen 1 Escenario I

Desarrollo Escenario 1

Parte 1: Asignación de direcciones IP:

Como primer paso se procede a diseñar el diagrama de red con los equipos necesarios de acuerdo con la topología del escenario. (se le asignan nombres a los equipos, Claves de seguridad y se proceden a interconectar físicamente de acuerdo al tipo de conexión requerida en el escenario.

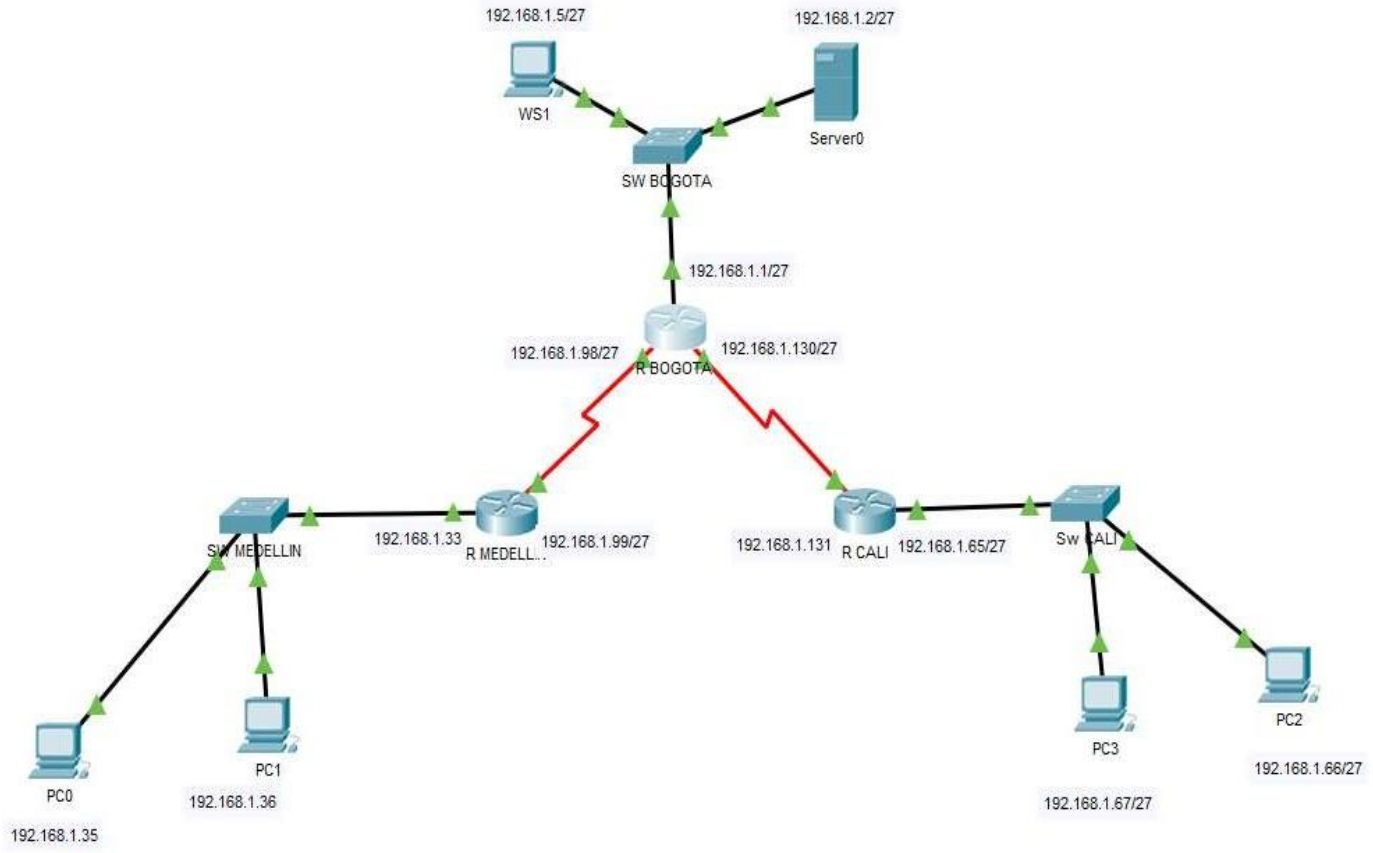

Imagen 2 Diseño Físico de Red

Parte 2: Configuración Básica.

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

Asignación de Direcciones IP Escenario 1

Se procede hacer la asignación de IP a los dispositivos de acuerdo con la siguiente tabla

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

Para desarrollar lo anterior se hiso necesario desde la consola de cada router aplicar las siguientes líneas de comando.

ROUTER BOGOTA

Router>ENABLE

Router#configure terminal

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

Router(config)#hostname RBOGOTA

En este comando se le asigna el nombre RBOGOTA al router

RBOGOTA(config)#interface fastethernet 0/0

Selecciónanos la interfaz fastethernet 0/0

RBOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224

Asignamos una dirección ip a la interfaz y también una mascara de red

RBOGOTA(config-if)#no shutdown

Subimos la interfaz

RBOGOTA(config-if)#

RBOGOTA(config-if)#exit

RBOGOTA(config)#interface serial 0/0

RBOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224

RBOGOTA(config-if)#no shutdown

Se le asigna una ip a la interfaz Serial 0/0 y se sube

RBOGOTA(config-if)#no shutdown

RBOGOTA(config-if)#exit

RBOGOTA(config)#interface serial0/1

RBOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224

RBOGOTA(config-if)#no shutdown

Se le asigna una ip a la interfaz Serial 0/1 y se sube

RBOGOTA(config-if)#exit

RBOGOTA(config)#end

RBOGOTA#

RBOGOTA#enable

RBOGOTA#config terminal

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

RBOGOTA(config)#ip route 192.168.1.64 255.255.255.224 192.168.1.131

RBOGOTA(config)#ip route 192.168.1.32 255.255.255.224 192.168.1.99

Esta es la ruta principal para llegar a los hosts en Internet. Al igual que ruta preferida de la LAN

RBOGOTA(config)#exit

RBOGOTA#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Guardamos la configuración en el archivo de inicio en la NVRAM

ROUTER MEDELLIN

Router>enable

Router#config terminal

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

Router(config)#hostname RMEDELLIN

En este comando se le asigna el nombre RMEDELLIN al router

RMEDELLIN(config)#interface fastethernet 0/0

Selecciónanos la interfaz fastethernet 0/0

RMEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.224

Asignamos una dirección ip a la interfaz y también una máscara de red

RMEDELLIN(config-if)#no shutdown

Subimos la interfaz

RMEDELLIN(config-if)#

RMEDELLIN(config-if)#exit

RMEDELLIN(config)#interface s0/0

RMEDELLIN(config-if)#ip address 192.168.1.99 255.255.255.224

RMEDELLIN(config-if)#no shutdown

Se le asigna una ip a la interfaz Serial 0/0 y se sube

RMEDELLIN(config-if)#

RMEDELLIN(config-if)#

RMEDELLIN(config-if)#exit

RMEDELLIN(config)#end

RMEDELLIN#

RMEDELLIN#enable

RMEDELLIN#config terminal

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

RMEDELLIN(config)#ip route 192.168.1.0 255.255.255.224 192.168.1.97

RMEDELLIN(config)#ip route 192.168.1.64 255.255.255.224 192.168.1.97

Esta es la ruta principal para llegar a los hosts en Internet. Al igual que ruta preferida de la LAN

RMEDELLIN(config)#exit

RMEDELLIN#

RMEDELLIN#copy running-config startup-config

Guardamos la configuración en el archivo de inicio en la NVRAM

Destination filename [startup-config]?

Building configuration...

ROUTER CALI

Router>enable

Router#config terminal

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

Router(config)#hostname RCALI

En este comando se le asigna el nombre RMEDELLIN al router

RCALI(config)#interface fastethernet0/0

Selecciónanos la interfaz fastethernet 0/0

RCALI(config-if)#ip address 192.168.1.65 255.255.255.224

RCALI(config-if)#no shutdown

Se le asigna una ip a la interfaz y se sube

RCALI(config-if)#

RCALI(config-if)#exit

RCALI(config)#interface s0/0

RCALI(config-if)#ip address 192.168.1.131 255.255.255.224

RCALI(config-if)#no shutdown

Se le asigna una ip a la interfaz Serial 0/0 y se sube

RCALI(config-if)#

RCALI(config-if)#exit

RCALI(config)#

RCALI(config)#end

RCALI#

RCALI#enable

RCALI#config terminal

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

RCALI(config)#ip route 192.168.1.0 255.255.255.224 192.168.1.129

RCALI(config)#ip route 192.168.1.32 255.255.255.224 192.168.1.129

RCALI(config)#exit

Esta es la ruta principal para llegar a los hosts en Internet. Al igual que ruta preferida de la LAN

RCALI#

RCALI#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

Guardamos la configuración en el archivo de inicio en la NVRAM

Se procede a realizar la configuración de seguridad, para lo que se establecen contraseñas a los routers y se encriptan las mismas utilizando los siguientes comandos.

CONTRASEÑAS todos los dispositivos se configuraron con la contraseña leon2019

RBOGOTA>enable

RBOGOTA#config terminal

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

RBOGOTA(config)#enable secret leon2019

Se le asigna contraseña al usuario con privilegios

RBOGOTA(config)#line consol 0

RBOGOTA(config-line)#password leon2019

RBOGOTA(config-line)#login

Se le asigna una contraseña a la entrada de consola y se forzó el login

RBOGOTA(config-line)#exit

RMEDELLIN>enable

RMEDELLIN#config terminal

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

RMEDELLIN(config)#enable secret leon2019

Se le asigna contraseña al usuario con privilegios

RMEDELLIN(config)#line consol 0

RMEDELLIN(config-line)#password leon2019

RMEDELLIN(config-line)#login

Se le asigna una contraseña a la entrada de consola y se forzó el login

RMEDELLIN(config-line)#exit

RMEDELLIN(config)#

RCALI>

RCALI>enable

RCALI#config terminal

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

RCALI(config)# enable secret leon2019

Se le asigna contraseña al usuario con privilegios

RCALI(config)#line consol 0

RCALI(config-line)#password leon2019

RCALI(config-line)#login

Se le asigna una contraseña a la entrada de consola y se forzó el login

RCALI(config-line)#exit

RCALI(config)#

RCALI(config)#exit

RCALI#

CONFIGURANDO LOS ROUTERS PARA EL LINE VTY 0 4

RBOGOTA>enable
RBOGOTA#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
RBOGOTA(config)#line vty 0 4
Esta línea es para poder ingresar de manera remota al router de forma telnet o ssh
RBOGOTA(config-line)#password leon2019
Asignamos una clave para poder ingresar de forma remota con mayor nivel de seguridad
RBOGOTA(config-line)#login
RBOGOTA(config-line)#loggin synchronous
Este comando evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento

RBOGOTA(config-line)#exit

RBOGOTA(config)#

RMEDELLIN>enable
RMEDELLIN#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
RMEDELLIN(config)#line vty 0 4
Esta línea es para poder ingresar de manera remota al router de forma telnet o ssh
RMEDELLIN(config-line)#password leon2019
Asignamos una clave para poder ingresar de forma remota con mayor nivel de seguridad
RMEDELLIN(config-line)#login
RMEDELLIN(config-line)#loggin synchronous
Este comando evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento

RMEDELLIN(config-line)#exit

RCALI>enable
RCALI#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
RCALI(config)#line vty 0 4
Esta línea es para poder ingresar de manera remota al router de forma telnet o ssh
RCALI(config-line)#password leon2019
Asignamos una clave para poder ingresar de forma remota con mayor nivel de seguridad

RCALI(config-line)#login
RCALI(config-line)#loggin synchronous

Este comando evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento

RCALI(config-line)#exit

Realizar un diagnóstico de vecinos usando el comando cdp.

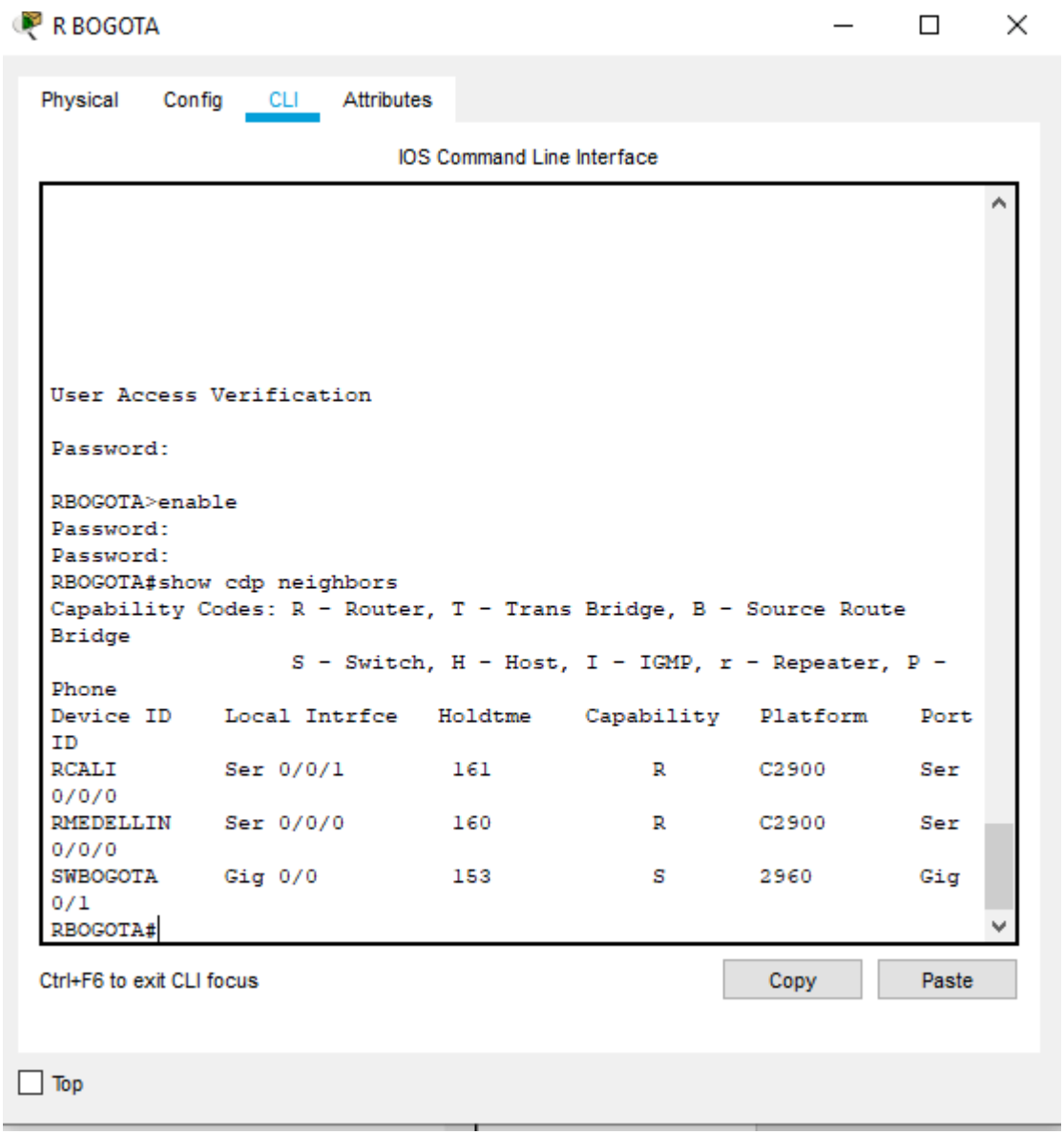

Imagen 3 Verificación de vecindad Router Bogota con el comando CDP

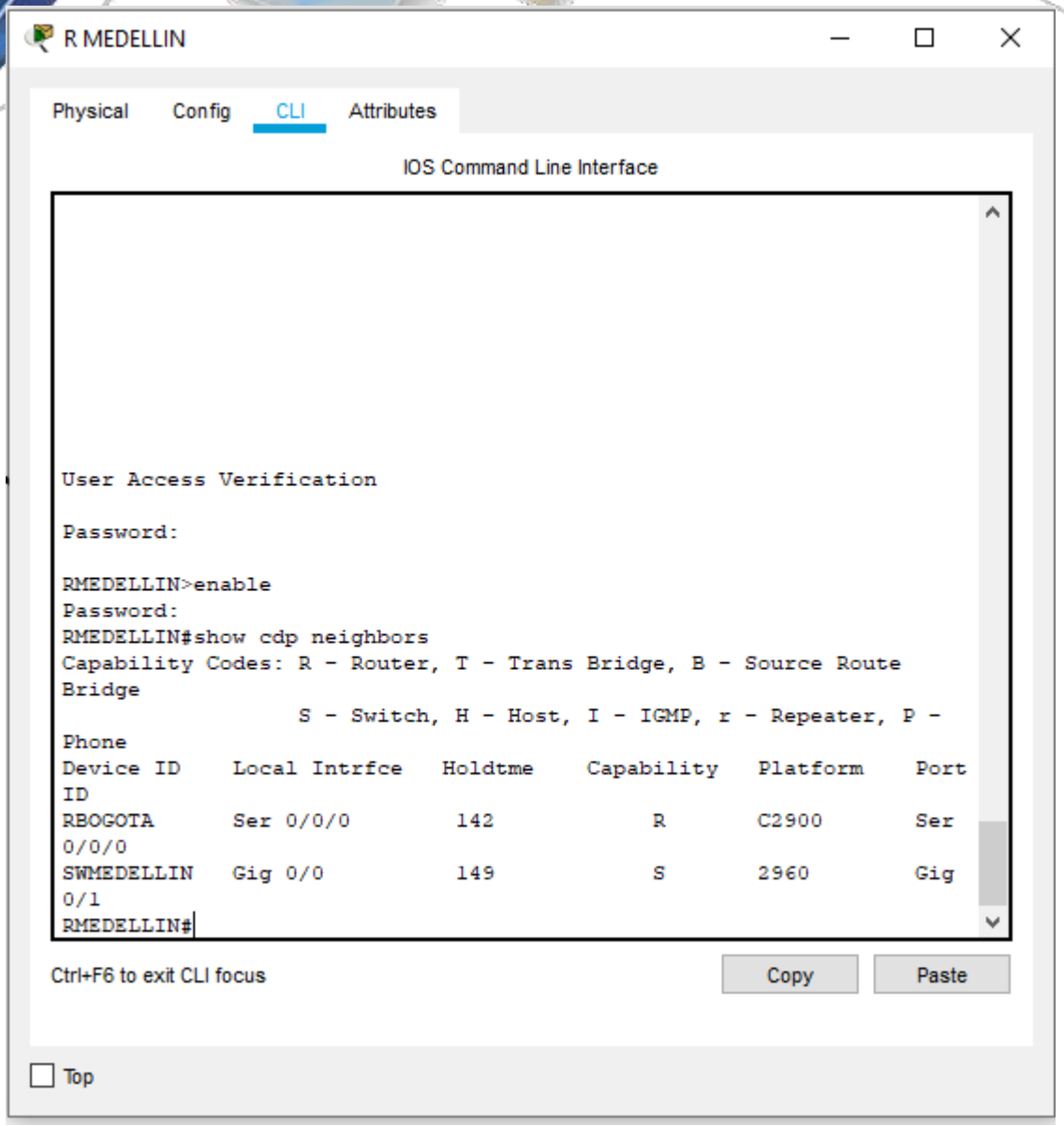

Imagen 4 Verificación de vecindad Router Medellín con el comando CDP

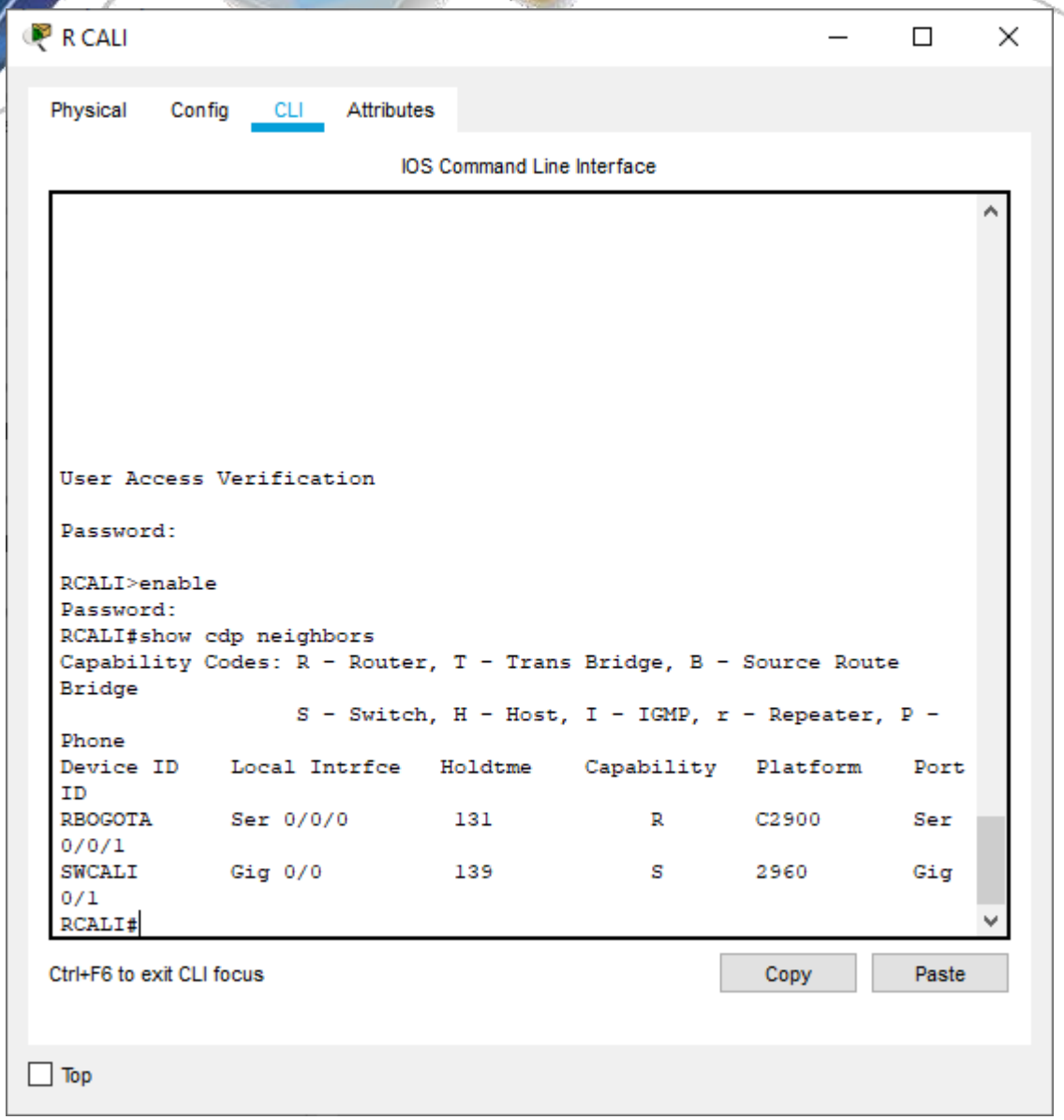

Imagen 5 Verificación de vecindad Router Medellín con el comando CDP

PRUEBAS DE PING

Realizamos pruebas ping de RCALI a RBOGOTA

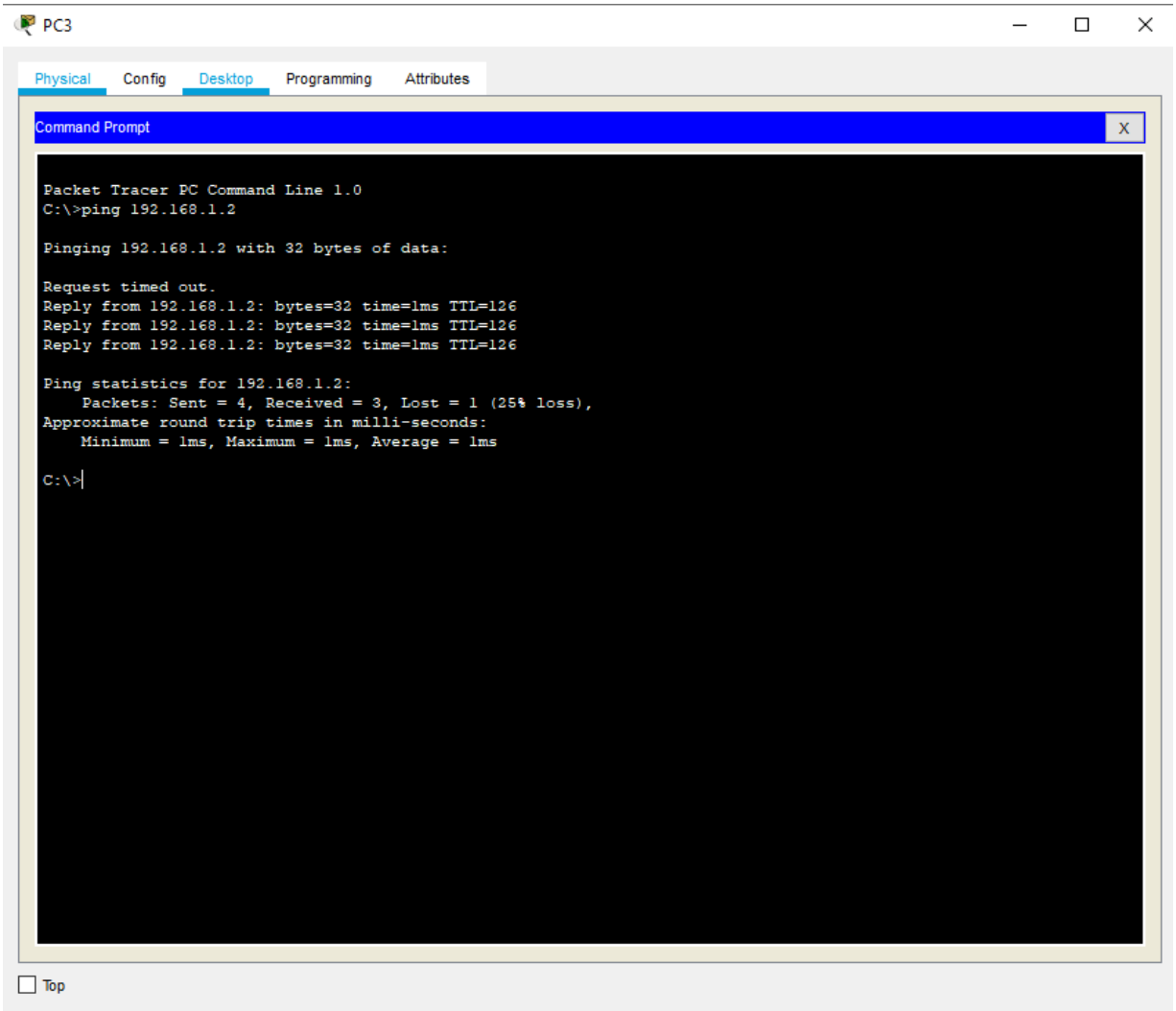

Imagen 6 ping de RCALI a RBOGOTA

Realizamos pruebas ping de RMEDELLIN a RCALI

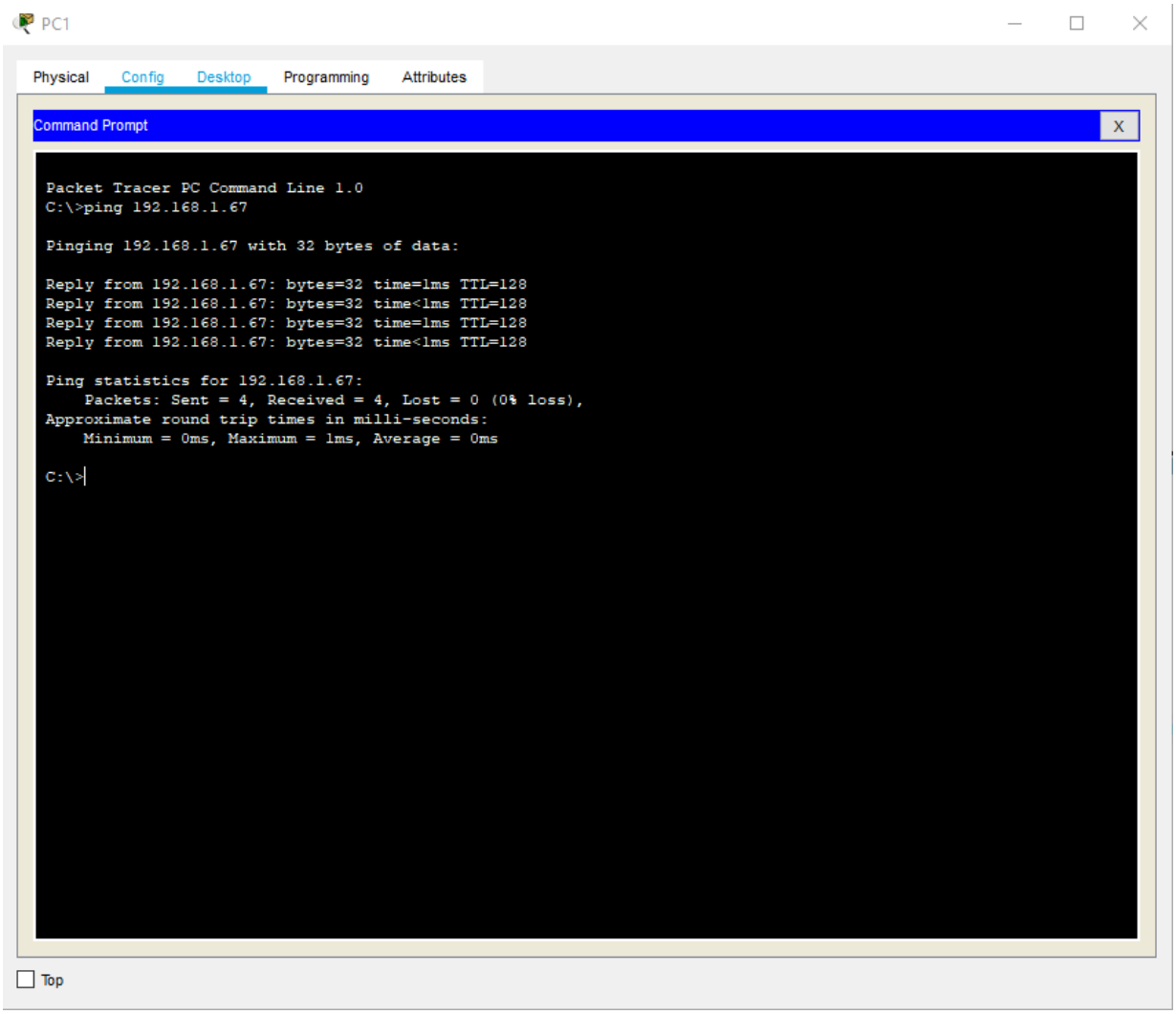

Imagen 7 Ping RMEDELLIN a RCALI

Realizamos pruebas ping de RMEDELLIN a RBOGOTA

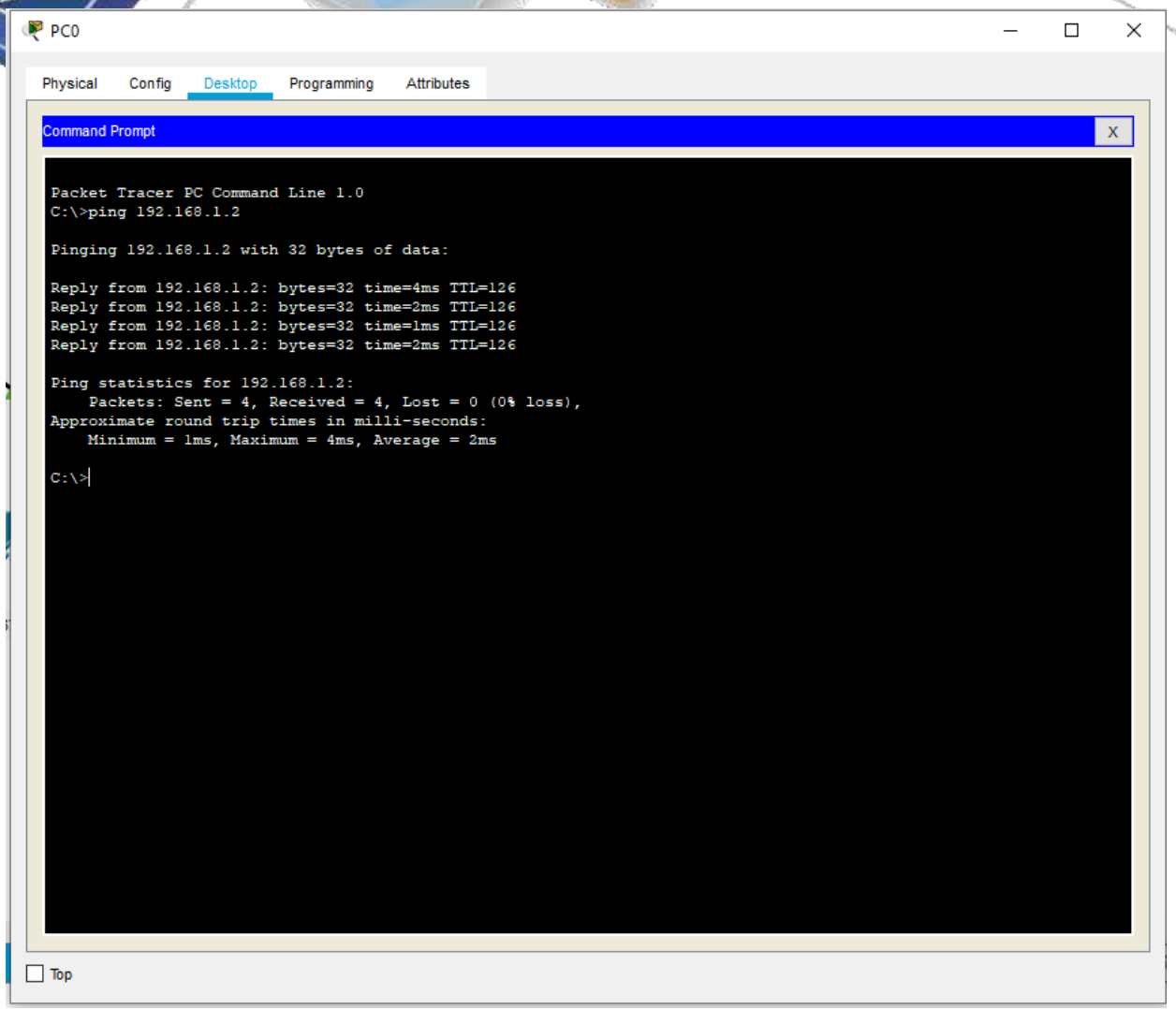

Imagen 8 ping RMEDELLIN a RBOGOTA

Realizamos pruebas ping de RBOGOTA a RCALI

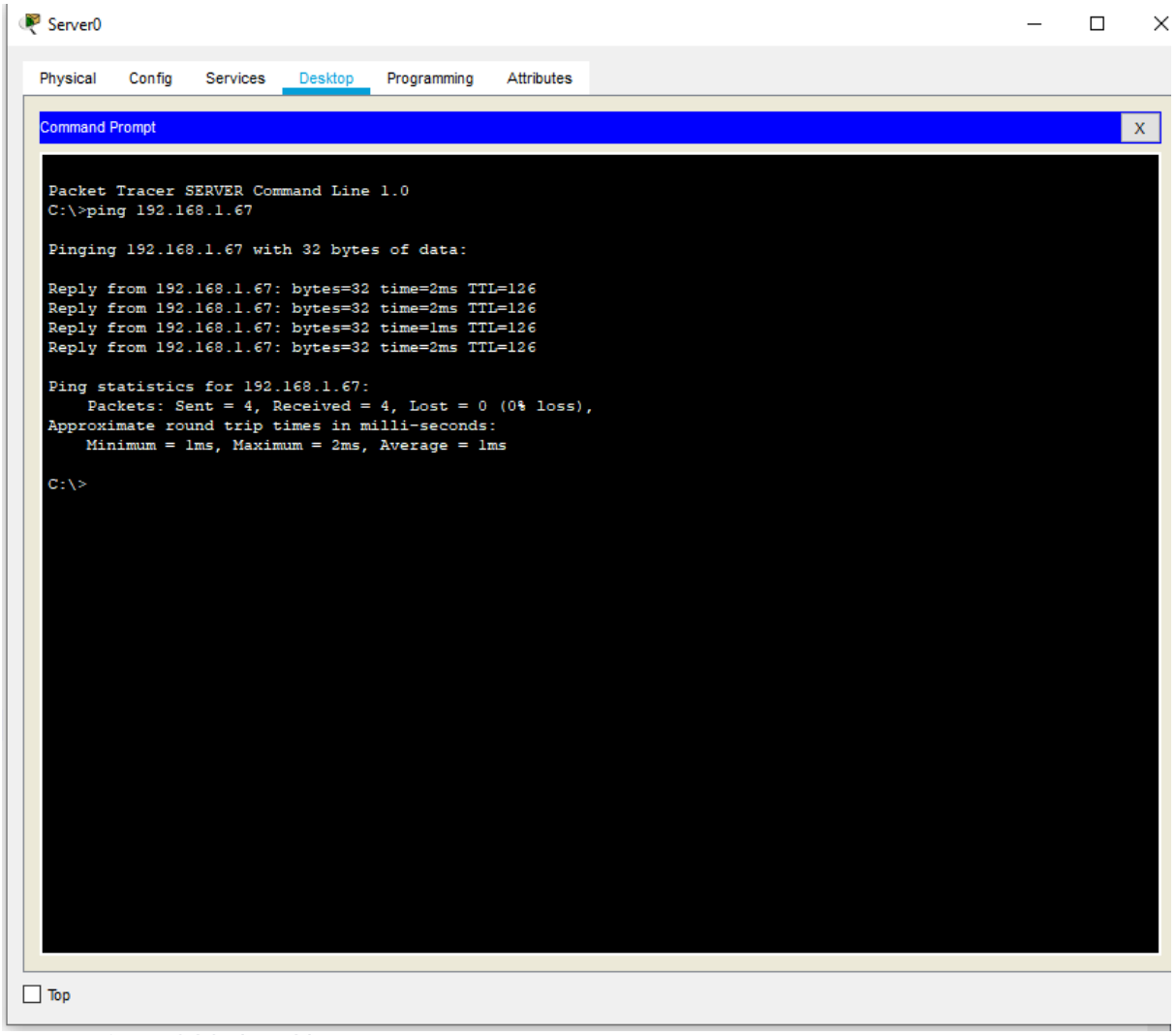

Imagen 9 ping RBOGOTA a RCALI

Parte 3: Configuración de Enrutamiento.

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

SE CONFIGURA EL USO DEL PRPOTOCOLO DE ENRUTAMIENTO EIGRP EN EL ROUTER DE BOGOTA.

RBOGOTA>enable

RBOGOTA#config terminal

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

RBOGOTA(config)#router eigrp 1

RBOGOTA(config-router)#no auto-summary

RBOGOTA(config-router)#network 192.168.1.96

RBOGOTA(config-router)#network 192.168.1.0

RBOGOTA(config-router)#network 192.168.1.128

RBOGOTA(config-router)#end

RBOGOTA#

SE CONFIGURA EL USO DEL PRPOTOCOLO DE ENRUTAMIENTO EIGRP EN EL ROUTER DE MEDELLIN.

RMEDELLIN>ENABLE

RMEDELLIN#config terminal

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

RMEDELLIN(config)#router eigrp 1

RMEDELLIN(config-router)#no auto-summary

RMEDELLIN(config-router)#network 192.168.1.32

MDELLIN(config-router)#network 192.168.1.32

RMEDELLIN(config-router)#network 192.168.1.96

RMEDELLIN(config-router)#end

SE CONFIGURA EL USO DEL PRPOTOCOLO DE ENRUTAMIENTO EIGRP EN EL ROUTER DE BOGOTA.

RCALI>enable

RCALI#config terminal

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

RCALI(config)#router eigrp 1

RCALI(config-router)#no auto-summary

RCALI(config-router)#network 192.168.1.128

Router(config-router)#

RCALI(config-router)#network 192.168.1.128

RCALI(config-router)#network 192.168.1.64

RCALI(config-router)#end

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.

LAS CONEXIONES A TELNET SE HABILITARON EN LOS ROUTERS CON LA CONFIGURACION DE LINE VTY AL INICIIO DE CONFIGURACIÓN DEL ESCENARIO.

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.

RBOGOTA#config terminal

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

RBOGOTA(config)#ip access-list extended ServerPT

RBOGOTA(config-ext-nacl)#permit ip 192.168.1.3 0.0.0.0 0.0.0.0 255.255.255.255

RBOGOTA(config-ext-nacl)#exit

RBOGOTA(config)#interface fa0/0

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

RBOGOTA(config-if)#end
RBOGOTA#

se configura una acl estática que solo permita que el servidor pueda conectarse con las demás redes y los demás host de la red de Bogotá no podrán conectarse sino a su red interna.

RMEDELLIN#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RMEDELLIN(config)#ip access-list extended ServerPT
RMEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.3 0.0.0.0
RMEDELLIN(config-ext-nacl)#exit
RMEDELLIN(config)#interface fa0/0
RMEDELLIN(config-if)#ip access-group ServerPT in
RMEDELLIN(config-if)#end
RMEDELLIN#

se configura una acl extendida en el router de Medellín, para que solo permita que los host de esa red puedan sacar tráfico de red solo al servidor, permitir el tráfico telnet

RCALI#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
RCALI(config)#ip access-list extended ServerPT
RCALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.3 0.0.0.0
RCALI(config-ext-nacl)#exit
RCALI(config)#int fa0/0
RCALI(config-if)#ip access-group ServerPT in
RCALI(config-if)#end
RCALI#

se configura una acl extendida en el router de Cali, para que solo permita que los host de esa red puedan sacar tráfico de red solo al servidor de Bogotá y deniegue la salida del resto de trafico de res a las redes de Medellín y Bogotá.

RBOGOTA
RBOGOTA#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
RBOGOTA(config)#ip access-list extended ServerPT
RBOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.99 0.0.0.0

RBOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.1 0.0.0.0
RBOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.131 0.0.0.0
RBOGOTA(config-ext-nacl)#end
RBOGOTA#

RMEDELLIN

RMEDELLIN#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
RMEDELLIN(config)#ip access-list extended ServerPT
RMEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.33 0.0.0.0
RMEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.98 0.0.0.0
RMEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.131 0.0.0.0
RMEDELLIN(config-ext-nacl)#end
RMEDELLIN#

RCALI

RCALI#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
RCALI(config)#ip access-list extended ServerPT
RCALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.99 0.0.0.0
RCALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.1 0.0.0.0
RCALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.65 0.0.0.0
RCALI(config-ext-nacl)#end
RCALI#

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

se realizan pruebas desde un host de la red de Medellín para comprobar que la acl quedo bien configurada y no permite tráfico de red hacia la red de Bogotá.

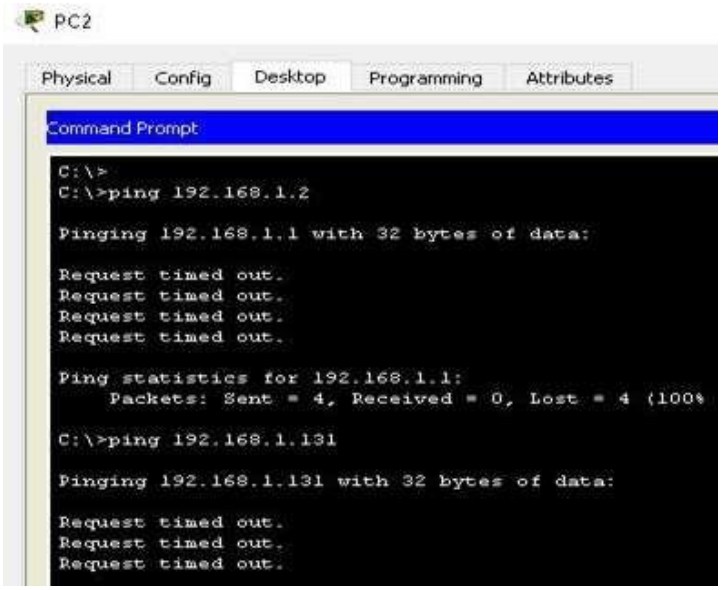

Imagen 10 Verificación acl desde pc2 Medellín a red Bogotá

se realizan pruebas desde un host de la red de Medellín para comprobar que la acl quedo bien configurada y no permite tráfico de red hacia la red de Cali.

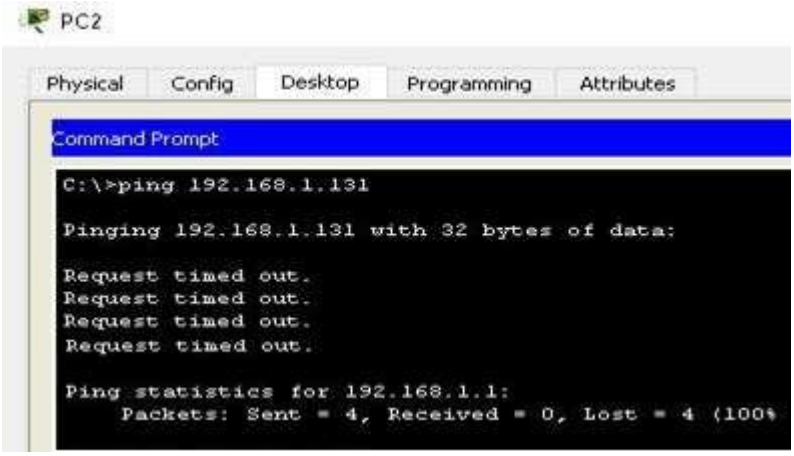

Imagen 11 Verificación acl desde pc2 Medellín a red Cali

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

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	Se conecto
	WS_1	Router BOGOTA	Se conecto
	Servidor	Router CALI	Se conecto
	Servidor	Router MEDELLIN	Se conecto
	LAN del Router MEDELLIN	Router CALI	No conecto
TELNET	LAN del Router CALI	Router CALI	Se conecto
	LAN del Router MEDELLIN	Router MEDELLIN	Se conecto
PING	LAN del Router CALI	Router MEDELLIN	No conecto
	LAN del Router CALI	WS_1	No responde
	LAN del Router MEDELLIN	WS_1	No responde
	LAN del Router MEDELLIN	LAN del Router CALI	No responde
PING	LAN del Router CALI	Servidor	Responde
	LAN del Router MEDELLIN	Servidor	Responde
	Servidor	LAN del Router MEDELLIN	Responde
	Servidor	LAN del Router CALI	Responde
	Router CALI	LAN del Router MEDELLIN	No responde
	Router MEDELLIN	LAN del Router CALI	No responde

Se realiza pruebas de conexio n vía Telnet entre las diferentes sedes como se muestra a continuacio n:

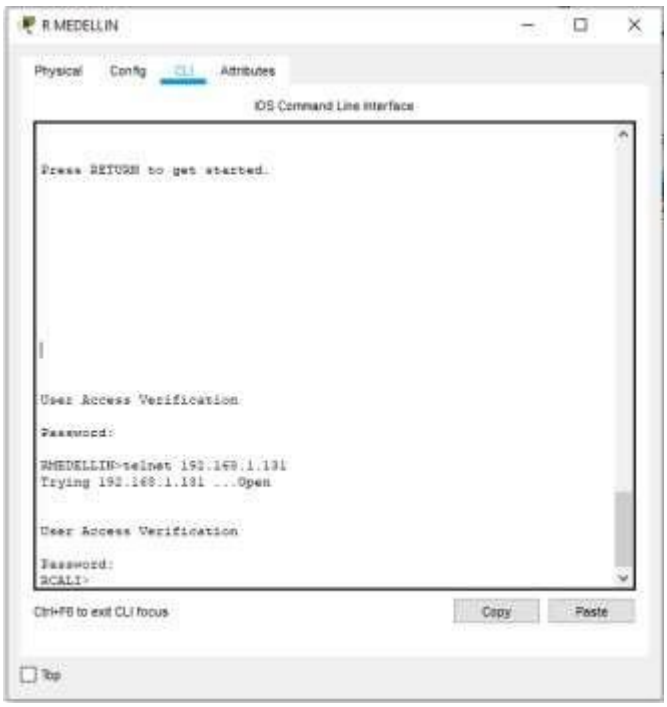

Imagen 12 Conexión Telnet Router Medellín a Router Cali

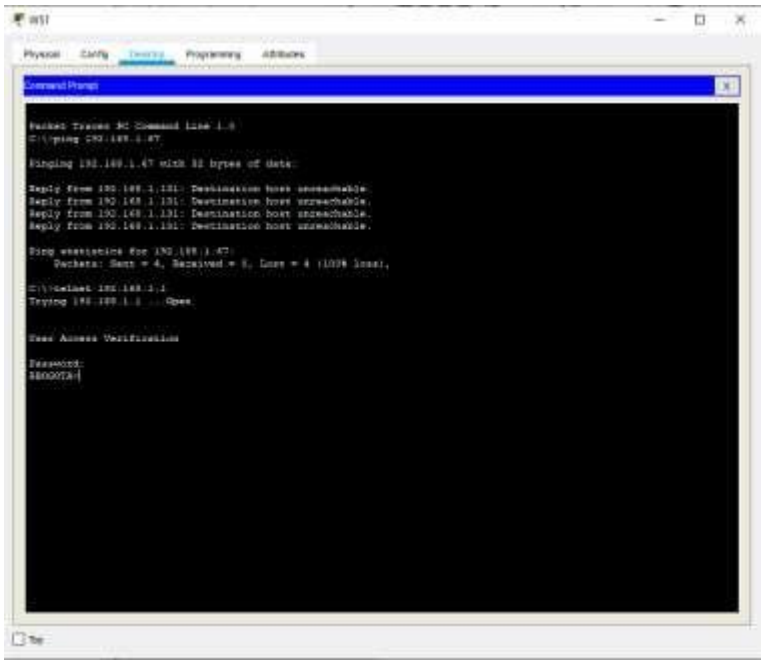

Imagen 13 Conexión telnet equipo WS1 a Router Bogota

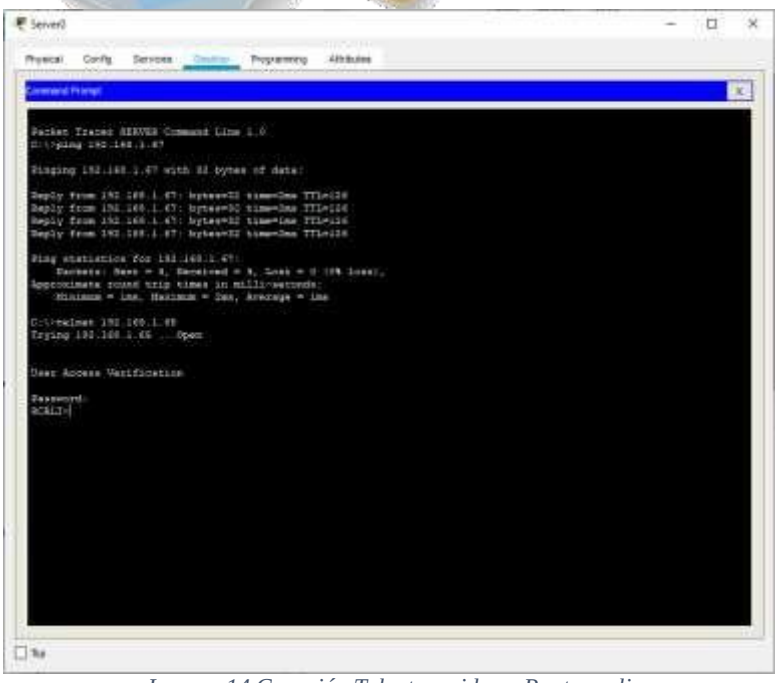

Imagen 14 Conexión Telnet servidor a Router cali

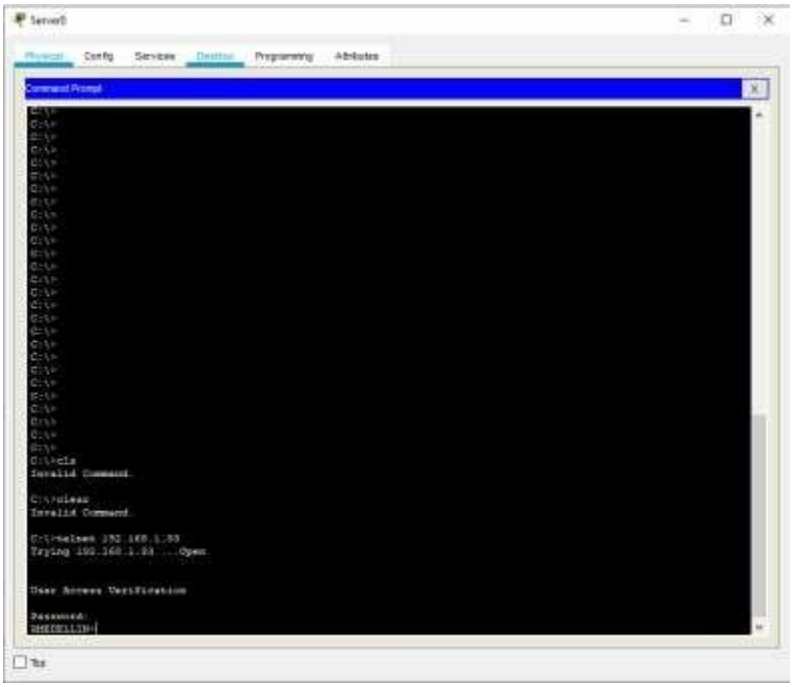

Imagen 15 Conexión Telnet Servidor a Router Medellín

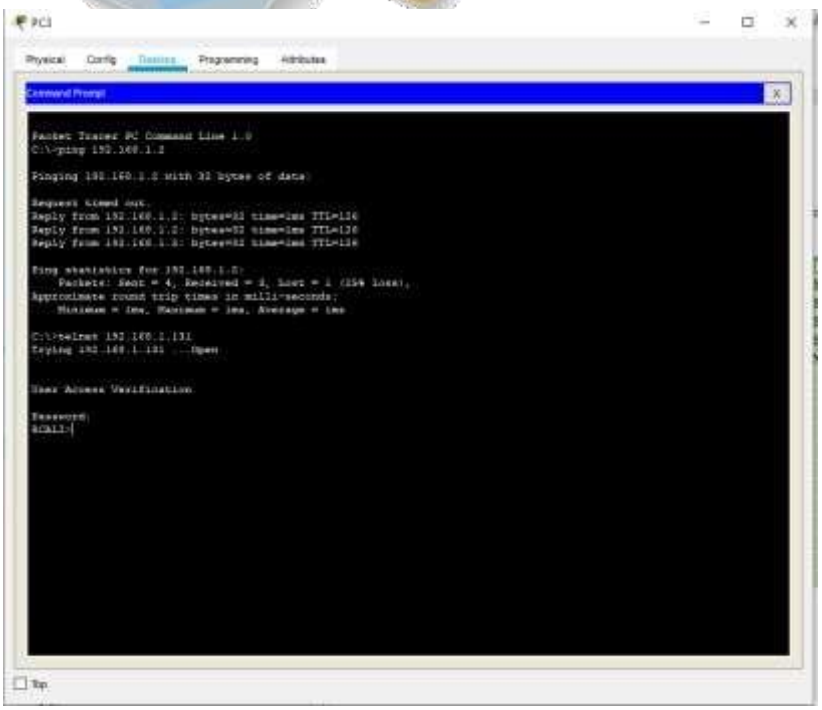

Imagen 16 Conexión Telnet PC3 a Router Cali

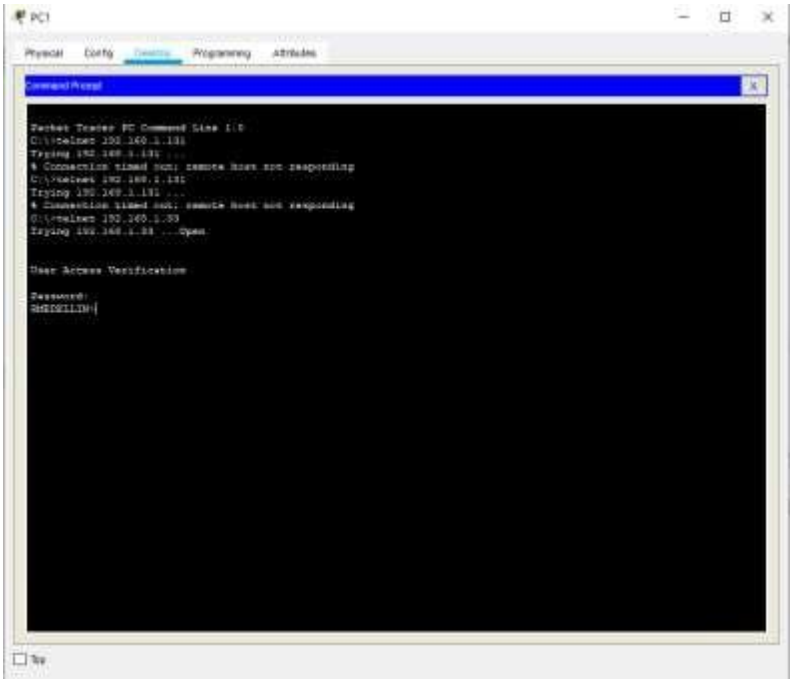

Imagen 17 Conexión Telnet PC1 a Router Medellín

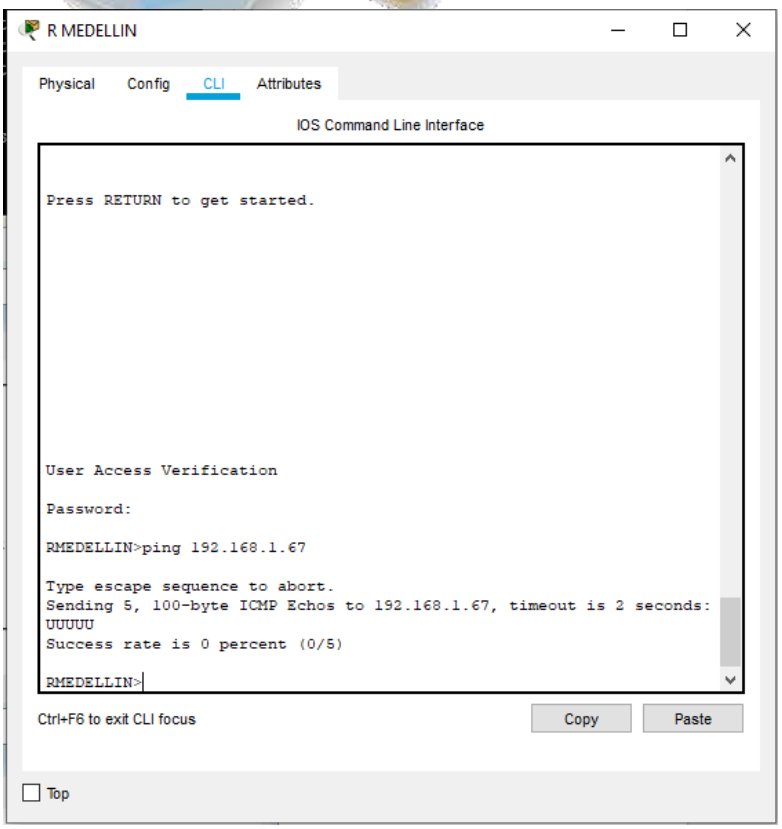

Imagen 18 prueba ping RMedellin

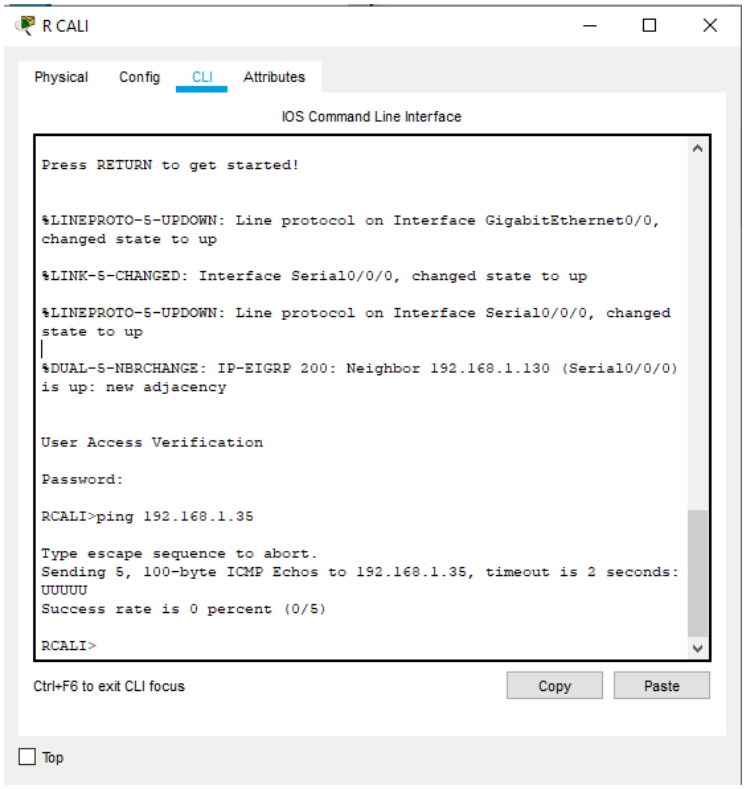

Imagen 19 ping Rcali

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.

Topologia

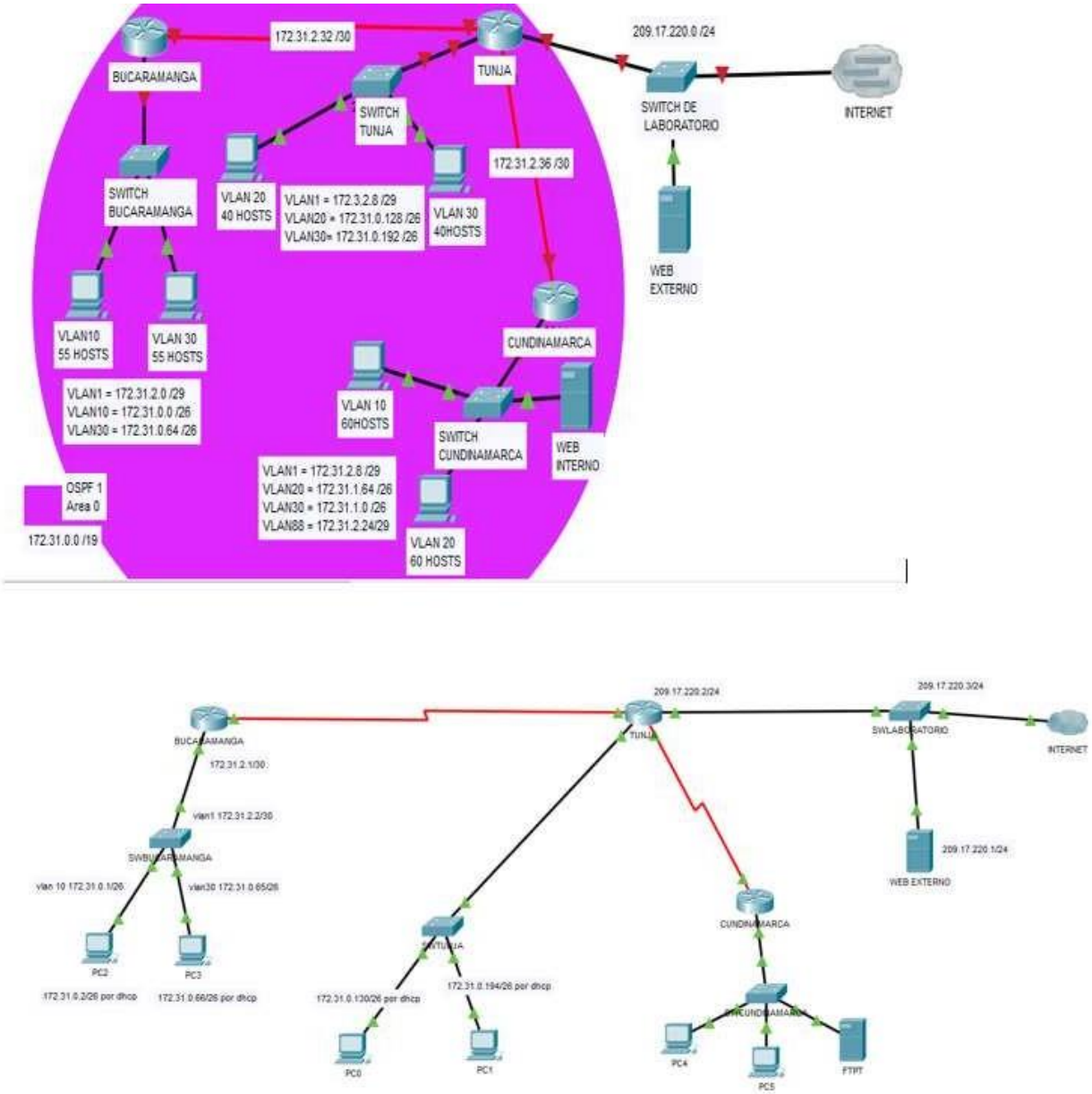

Imagen 20 Topología Escenario 2

Los siguientes son los requerimientos necesarios:

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

2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca
3. El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).

4. El enrutamiento deberá tener autenticación.
5. Listas de control de acceso:
   - Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.
   - Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.
   - Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.
   - Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.
   - Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.
   - Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.
   - Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.
   - Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los routers e internet.

CONFIGURACIÓN DE ROUTERS

Se realizan las configuraciones indicadas de acceso y seguridad en el router tunja

RTUNJA#

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname RTUNJA
RTUNJA(config)#no ip domain-lookup
RTUNJA(config)#enable secret leon2019
RTUNJA(config)#line console 0
RTUNJA(config-line)#password leon2019
RTUNJA(config-line)#login
RTUNJA(config-line)#logging synchronous
RTUNJA(config-line)#line vty 0 15
RTUNJA(config-line)#password leon2019
RTUNJA(config-line)#login
RTUNJA(config-line)#logging synchronous
```

De acuerdo con la tabla de direccionamiento ip realizamos la configuración de las interfaces de red en el router de Tunja, se configura el dchp

```
RTUNJA(config)#interface f0/0.1
RTUNJA(config-subif)#encapsulation dot1q 1
RTUNJA(config-subif)#ip address 172.3.2.9 255.255.255.248
RTUNJA(config-subif)#interface f0/0.20
RTUNJA(config-subif)#encapsulation dot1q 20
RTUNJA(config-subif)#ip address 172.31.0.129 255.255.255.192
RTUNJA(config-subif)#interface f0/0.30
RTUNJA(config-subif)#encapsulation dot1q 30
RTUNJA(config-subif)#ip address 172.31.0.193 255.255.255.192
RTUNJA(config-subif)#interface f0/0
RTUNJA(config-if)#no shutdown
RTUNJA(config-if)#
RTUNJA(config-if)#interface s0/0/0
RTUNJA(config-if)#ip address 172.31.2.37 255.255.255.252
RTUNJA(config-if)#no shutdown
RTUNJA(config-if)#
RTUNJA(config-if)#interface s0/0/1
RTUNJA(config-if)#ip address 172.31.2.33 255.255.255.252
RTUNJA(config-if)#no shutdown
RTUNJA(config-if)#interface f0/1
RTUNJA(config-if)#ip address 209.165.220.1 255.255.255.0
RTUNJA(config-if)#no shutdown
RTUNJA(config-if)#
```

realizamos la configuración del protocolo de enrutamiento ospf con autenticación en el router de Tunja.

```
RTUNJA(config-if)#router ospf 1
RTUNJA(config-router)#network 172.3.2.8 0.0.0.7 area 0
RTUNJA(config-router)#network 172.31.0.128 0.0.0.63 area 0
RTUNJA(config-router)#network 172.31.0.192 0.0.0.63 area 0
RTUNJA(config-router)#network 172.31.2.32 0.0.0.3 area 0
RTUNJA(config-router)#network 172.31.2.36 0.0.0.3 area 0
RTUNJA(config-router)#end
RTUNJA#
```

RCUNDINAMARCA#

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname RCUNDINAMARCA
RCUNDINAMARCA(config)#no ip domain-lookup
RCUNDINAMARCA(config)#enable secret leon2019
RCUNDINAMARCA(config)#line console 0
RCUNDINAMARCA(config-line)#password leon2019
RCUNDINAMARCA(config-line)#login
RCUNDINAMARCA(config-line)#logging synchronous
RCUNDINAMARCA(config-line)#line vty 0 15
RCUNDINAMARCA(config-line)#password leon2019
RCUNDINAMARCA(config-line)#login
RCUNDINAMARCA(config-line)#logging synchronous
```

De acuerdo con la tabla de direccionamiento ip realizamos la configuración de las interfaces de red en el router de Bucaramanga, se configura el dchp

```
RCUNDINAMARCA(config)#interface f0/0.1
RCUNDINAMARCA(config-subif)#encapsulation dot1q 1
RCUNDINAMARCA(config-subif)#ip address 172.31.2.9 255.255.255.248
RCUNDINAMARCA(config-subif)#interface f0/0.20
RCUNDINAMARCA(config-subif)#encapsulation dot1q 20
RCUNDINAMARCA(config-subif)#ip address 172.31.1.65 255.255.255.192
RCUNDINAMARCA(config-subif)#interface f0/0.30
RCUNDINAMARCA(config-subif)#encapsulation dot1q 30
RCUNDINAMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192
RCUNDINAMARCA(config-subif)#interface f0/0.88
RCUNDINAMARCA(config-subif)#encapsulation dot1q 88
RCUNDINAMARCA(config-subif)#ip address 172.31.2.25 255.255.255.248
RCUNDINAMARCA(config-subif)#interface f0/0
RCUNDINAMARCA(config-if)#no shutdown
RCUNDINAMARCA(config-if)#
RCUNDINAMARCA(config-if)#interface s0/0/0
RCUNDINAMARCA(config-if)#ip address 172.31.2.38 255.255.255.252
RCUNDINAMARCA(config-if)#no shutdown
```

realizamos la configuración del protocolo de enrutamiento ospf con autenticación en el router de Bucaramanga.

```
RCUNDINAMARCA(config-if)#router ospf 1
RCUNDINAMARCA(config-router)#network 172.31.1.0 0.0.0.63 area 0
RCUNDINAMARCA(config-router)#network 172.31.1.64 0.0.0.63 area 0
RCUNDINAMARCA(config-router)#network 172.31.2.8 0.0.0.7 area 0
RCUNDINAMARCA(config-router)#network 172.31.2.24 0.0.0.7 area 0
RCUNDINAMARCA(config-router)#network 172.31.2.36 0.0.0.3 area 0
RCUNDINAMARCA(config-router)#end
RCUNDINAMARCA#
```

RBUCARAMANGA#

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname RBUCARAMANGA
RBUCARAMANGA(config)#no ip domain-lookup
RBUCARAMANGA(config)#enable secret leon2019
RBUCARAMANGA(config)#line console 0
RBUCARAMANGA(config-line)#password leon2019
RBUCARAMANGA(config-line)#login
RBUCARAMANGA(config-line)#logging synchronous
RBUCARAMANGA(config-line)#line vty 0 15
RBUCARAMANGA(config-line)#password leon2019
RBUCARAMANGA(config-line)#login
RBUCARAMANGA(config-line)#logging synchronous
RBUCARAMANGA(config)#interface f0/0.1
RBUCARAMANGA(config-subif)#encapsulation dot1q 1
RBUCARAMANGA(config-subif)#ip address 172.31.2.1 255.255.255.248
RBUCARAMANGA(config-subif)#interface f0/0.10
RBUCARAMANGA(config-subif)#encapsulation dot1q 10
RBUCARAMANGA(config-subif)#ip address 172.31.0.1 255.255.255.192
RBUCARAMANGA(config-subif)#interface f0/0.30
RBUCARAMANGA(config-subif)#encapsulation dot1q 30
RBUCARAMANGA(config-subif)#ip address 172.31.0.65 255.255.255.192
RBUCARAMANGA(config-subif)#interface f0/0
RBUCARAMANGA(config-if)#no shutdown
RBUCARAMANGA(config-if)#
RBUCARAMANGA(config-if)#
RBUCARAMANGA(config-if)#interface s0/0/1
RBUCARAMANGA(config-if)#ip address 172.31.2.34 255.255.255.252
RBUCARAMANGA(config-if)#no shutdown
RBUCARAMANGA(config-if)#
RBUCARAMANGA(config-if)#router ospf 1
RBUCARAMANGA(config-router)#network 172.31.0.0 0.0.0.63 area 0
RBUCARAMANGA(config-router)#network 172.31.0.64 0.0.0.63 area 0
RBUCARAMANGA(config-router)#network 172.31.2.0 0.0.0.7 area 0
RBUCARAMANGA(config-router)#network 172.31.2.32 0.0.0.3 area 0
RBUCARAMANGA(config-router)#end
RBUCARAMANGA#
```

CONFIGURACION DE SWTICHT

configuramos los parámetros básicos y de seguridad en el switch de Tunja

SWTUNJA

```
Switch>en
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SWTUNJA
SWTUNJA(config)#vlan 1
SWTUNJA(config-vlan)#vlan 20
SWTUNJA(config-vlan)#vlan 30
SWTUNJA(config-vlan)#interface f0/20
SWTUNJA(config-if)#switchport mode access
SWTUNJA(config-if)#switchport access vlan 20
SWTUNJA(config-if)#interface f0/24
SWTUNJA(config-if)#switchport mode access
SWTUNJA(config-if)#switchport access vlan 30
SWTUNJA(config-if)#interface f0/1
SWTUNJA(config-if)#switchport mode trunk
SWTUNJA(config-if)#
SWTUNJA(config-if)#interface vlan 20
SWTUNJA(config-if)#ip address 172.31.0.129 255.255.255.192
SWTUNJA(config-if)#no shutdown
SWTUNJA(config-if)#
SWTUNJA(config-if)#ip default-gateway 172.31.0.1
SWTUNJA(config)#
```

SWCUNDINAMARCA

configuramos los parámetros básicos y de seguridad en el switch de Cundinamarca

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SWCUNDINAMARCA
SWCUNDINAMARCA(config)#vlan 1
SWCUNDINAMARCA(config-vlan)#vlan 20
SWCUNDINAMARCA(config-vlan)#vlan 30
SWCUNDINAMARCA(config-vlan)#vlan 88
SWCUNDINAMARCA(config-vlan)#exit
SWCUNDINAMARCA(config)#interface f0/20
SWCUNDINAMARCA(config-if)#switchport mode access
SWCUNDINAMARCA(config-if)#switchport access vlan 20
SWCUNDINAMARCA(config-if)#interface f0/24
SWCUNDINAMARCA(config-if)#switchport mode access
SWCUNDINAMARCA(config-if)#switchport access vlan 30
SWCUNDINAMARCA(config-if)#interface f0/10
SWCUNDINAMARCA(config-if)#switchport mode access
```

SWCUNDINAMARCA(config-if)#switchport access vlan 88
SWCUNDINAMARCA(config-if)#interface f0/1
SWCUNDINAMARCA(config-if)#switchport mode trunk

SWCUNDINAMARCA(config-if)#
SWCUNDINAMARCA(config-if)#interface vlan 1
SWCUNDINAMARCA(config-if)#ip address 172.31.2.11 255.255.255.248
SWCUNDINAMARCA(config-if)#no shutdown
SWCUNDINAMARCA(config-if)#
SWCUNDINAMARCA(config-if)#ip default-gateway 172.31.2.9
SWCUNDINAMARCA(config)#

SWBUCARAMANGA#
configuramos los parámetros básicos y de seguridad en el switch de Bucaramanga

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SWBUCARAMANGA
SWBUCARAMANGA(config)#vlan 1
SWBUCARAMANGA(config-vlan)#vlan 10
SWBUCARAMANGA(config-vlan)#vlan 30
SWBUCARAMANGA(config-vlan)#interface f0/20
SWBUCARAMANGA(config-if)#switchport mode access
SWBUCARAMANGA(config-if)#switchport access vlan 10
SWBUCARAMANGA(config-if)#interface f0/24
SWBUCARAMANGA(config-if)#switchport mode access
SWBUCARAMANGA(config-if)#switchport access vlan 30
SWBUCARAMANGA(config-if)#interface f0/1
SWBUCARAMANGA(config-if)#switchport mode trunk
SWBUCARAMANGA(config-if)#interface vlan 1
SWBUCARAMANGA(config-if)#ip address 172.31.2.2 255.255.255.248
SWBUCARAMANGA(config-if)#no shutdown
SWBUCARAMANGA(config-if)#ip default-gateway 172.31.2.1
SWBUCARAMANGA(config)#
SWBUCARAMANGA(config)#

- **Autenticación local con AAA.**

RTUNJA

```
RTUNJA>enable
Password:
RTUNJA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RTUNJA(config)#line console 0
RTUNJA(config-line)#username administrador secret leon2019
RTUNJA(config)#aaa new-model
RTUNJA(config)#aaa authentication login AUTH local
RTUNJA(config)#exit
RTUNJA(config)#line vty 0 15
RTUNJA(config-line)#login authentication AUTH
RTUNJA(config-line)#exit
RTUNJA(config)#line console 0
RTUNJA(config-line)#login authentication AUTH
RTUNJA(config-line)#exit
RTUNJA(config)#exit
RTUNJA#
```

RCUNDINAMARCA

```
CUNDINAMARCA>enable
Password:
RCUNDINAMARCA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RCUNDINAMARCA(config)#line console 0
RCUNDINAMARCA(config-line)#username administrador secret leon2019
RCUNDINAMARCA(config)#aaa new-model
RCUNDINAMARCA(config)#aaa authentication login AUTH local
RCUNDINAMARCA(config)#exit
RCUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
RCUNDINAMARCA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RCUNDINAMARCA(config)#line vty 0 15
RCUNDINAMARCA(config-line)#login authentication AUTH
RCUNDINAMARCA(config-line)#exit
RCUNDINAMARCA(config)#line console 0
RCUNDINAMARCA(config-line)#login authentication AUTH
RCUNDINAMARCA(config-line)#exit
RCUNDINAMARCA(config)#exit
RCUNDINAMARCA#
```

RBUCARAMANGA

```
RBUCARAMANGA>enable
Password:
RBUCARAMANGA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RBUCARAMANGA(config)#line console 0
RBUCARAMANGA(config-line)#username administrador secret leon2019
RBUCARAMANGA(config)#aaa new-model
RBUCARAMANGA(config)#aaa authentication login AUTH local
RBUCARAMANGA(config)#exit
RBUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
RBUCARAMANGA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RBUCARAMANGA(config)#line vty 0 15
RBUCARAMANGA(config-line)#login authentication AUTH
RBUCARAMANGA(config-line)#exit
RBUCARAMANGA(config)#line console 0
RBUCARAMANGA(config-line)#login authentication AUTH
RBUCARAMANGA(config-line)#exit
RBUCARAMANGA(config)#exit
RBUCARAMANGA#
```

- **Cifrado de contraseñas.**

```
RTUNJA(config)#service password-encryption
RCUNDINAMARCA(config)#service password-encryption
BUCARAMANGA(config)#service password-encryption
```

- **Un máximo de intentos para acceder al router.**

```
RTUNJA(config-line)#login block-for 5 attempts 4 within 60
RCUNDINAMARCA(config-line)#login block-for 5 attempts 4 within 60
RBUCARAMANGA(config-line)#login block-for 5 attempts 4 within 60
```

- **Máximo tiempo de acceso al detectar ataques.**

```
RTUNJA(config-line)#login block-for 5 attempts 4 within 60
RCUNDINAMARCA(config-line)#login block-for 5 attempts 4 within 60
RBUCARAMANGA(config-line)#login block-for 5 attempts 4 within 60
```

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

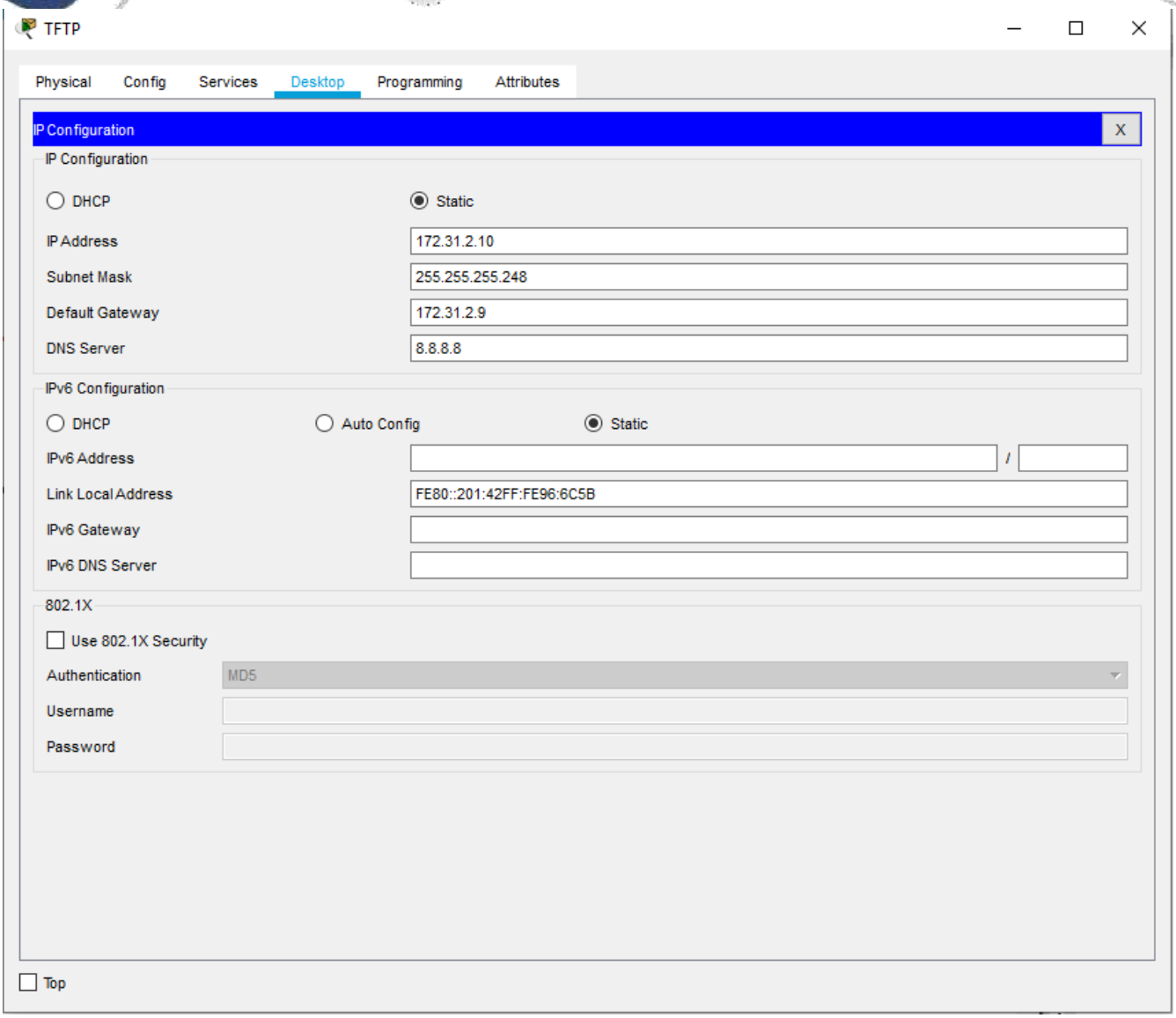

Imagen 21 Configuración Ip Servidor TFTP

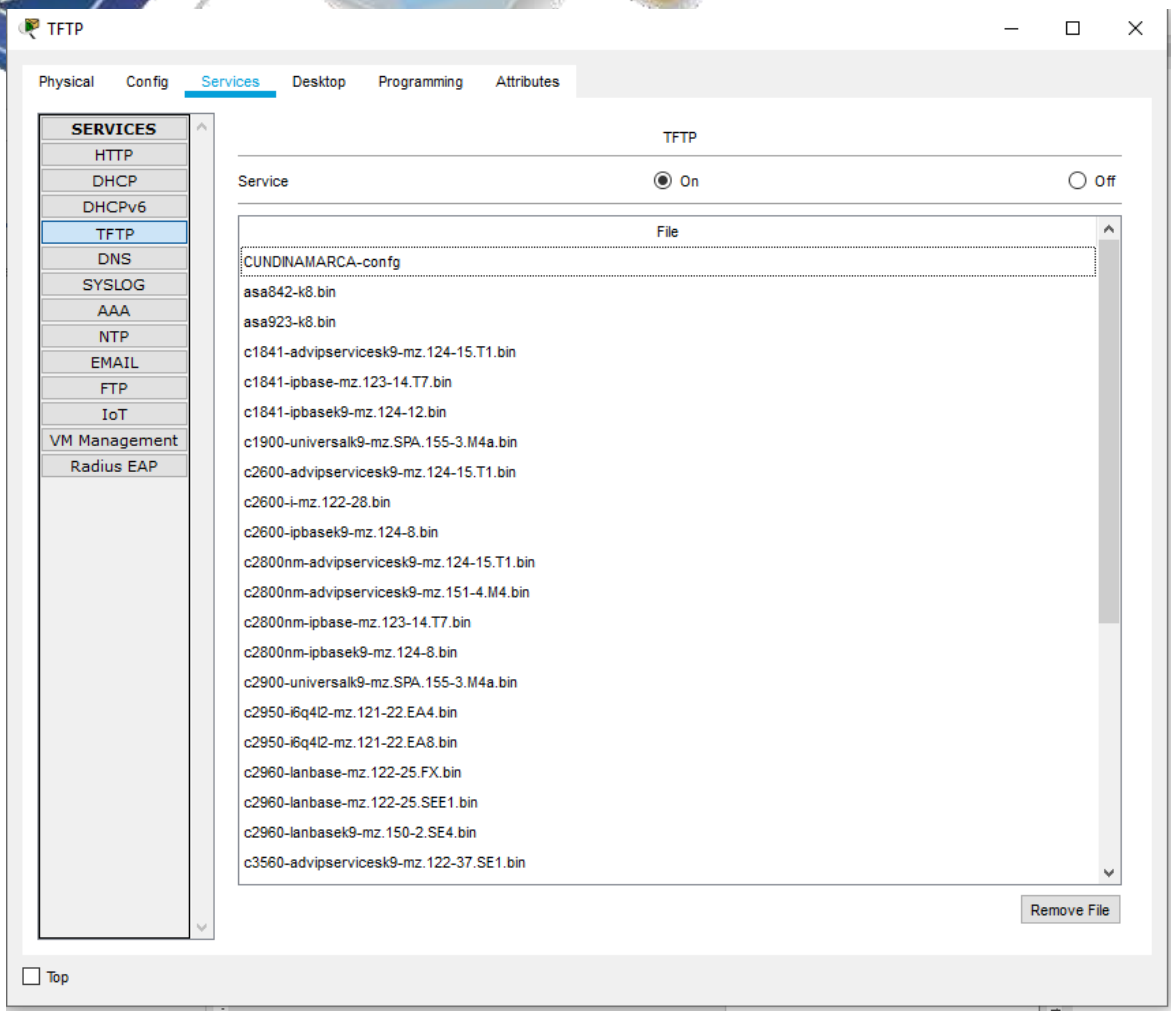

Imagen 22 habilitación de servicios TFTP

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

```
RTUNJA(config)#ip dhcp excluded-address 172.31.0.1
RTUNJA(config)#ip dhcp excluded-address 172.31.0.65
RTUNJA(config)#ip dhcp excluded-address 172.31.1.65
RTUNJA(config)#ip dhcp excluded-address 172.31.1.1
RTUNJA(config)#ip dhcp pool V10B
RTUNJA(dhcp-config)#network 172.31.0.0 255.255.255.192
RTUNJA(dhcp-config)#default-router 172.31.0.1
RTUNJA(dhcp-config)#dns-server 172.31.2.28
RTUNJA(dhcp-config)#ip dhcp pool V30B
RTUNJA(dhcp-config)#network 172.31.0.64 255.255.255.192
RTUNJA(dhcp-config)#default-router 172.31.0.65
RTUNJA(dhcp-config)#dns-server 172.31.2.28
RTUNJA(dhcp-config)#ip dhcp pool V20C
RTUNJA(dhcp-config)#network 172.31.1.64 255.255.255.192
RTUNJA(dhcp-config)#default-router 172.31.1.65
RTUNJA(dhcp-config)#dns-server 172.31.2.28
RTUNJA(dhcp-config)#ip dhcp pool V30C
RTUNJA(dhcp-config)#network 172.31.1.0 255.255.255.192
RTUNJA(dhcp-config)#default-router 172.31.1.1
RTUNJA(dhcp-config)#dns-server 172.31.2.28
RTUNJA(dhcp-config)#
```

```
RBUCARAMANGA(config)#interface f0/0.10
RBUCARAMANGA(config-subif)#ip helper-address 172.31.2.33
RBUCARAMANGA(config-subif)#interface f0/0.30
RBUCARAMANGA(config-subif)#ip helper-address 172.31.2.33
RBUCARAMANGA(config-subif)#end
RBUCARAMANGA#
RBUCARAMANGA#
```

```
RCUNDINAMARCA(config)#interface f0/0.20
RCUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
RCUNDINAMARCA(config-subif)#interface f0/0.30
RCUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
RCUNDINAMARCA(config-subif)#end
RCUNDINAMARCA#
```

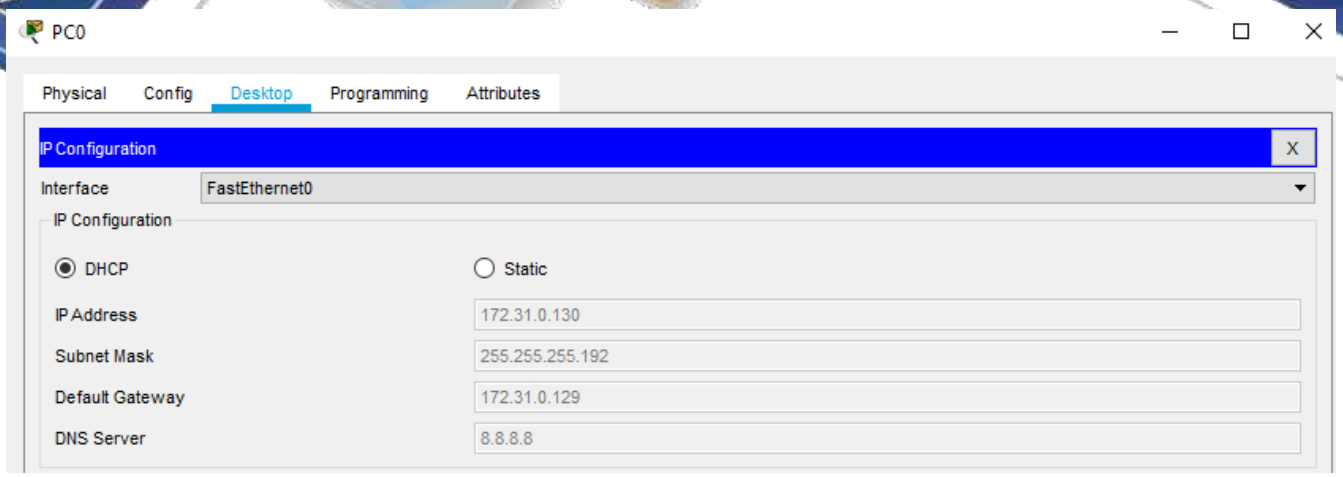

Imagen 23 Habilitación DHCP PC0

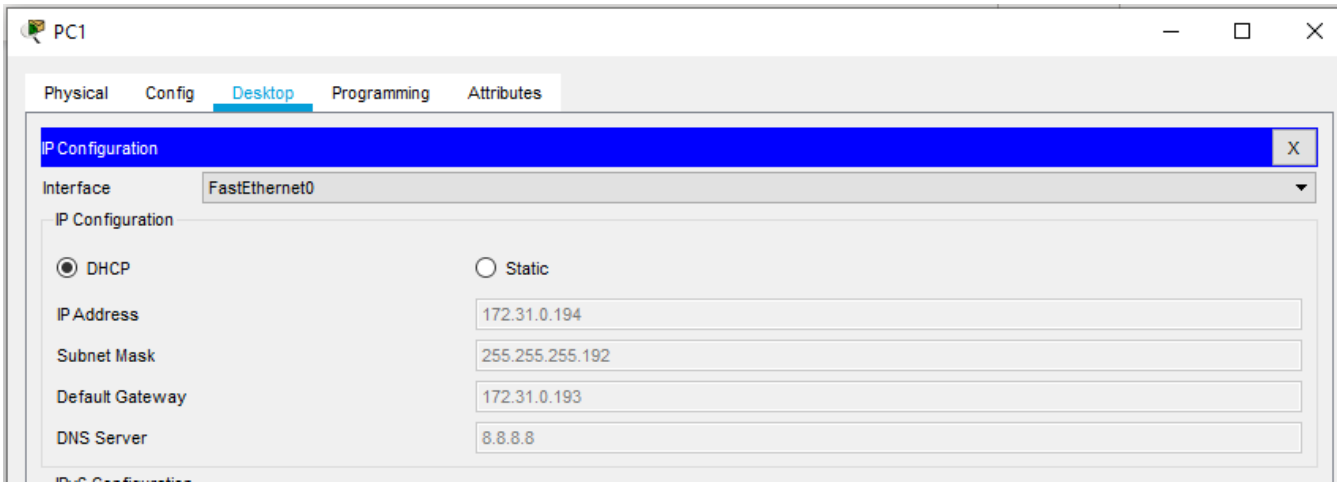

Imagen 24 Habilitación DHCP PC1

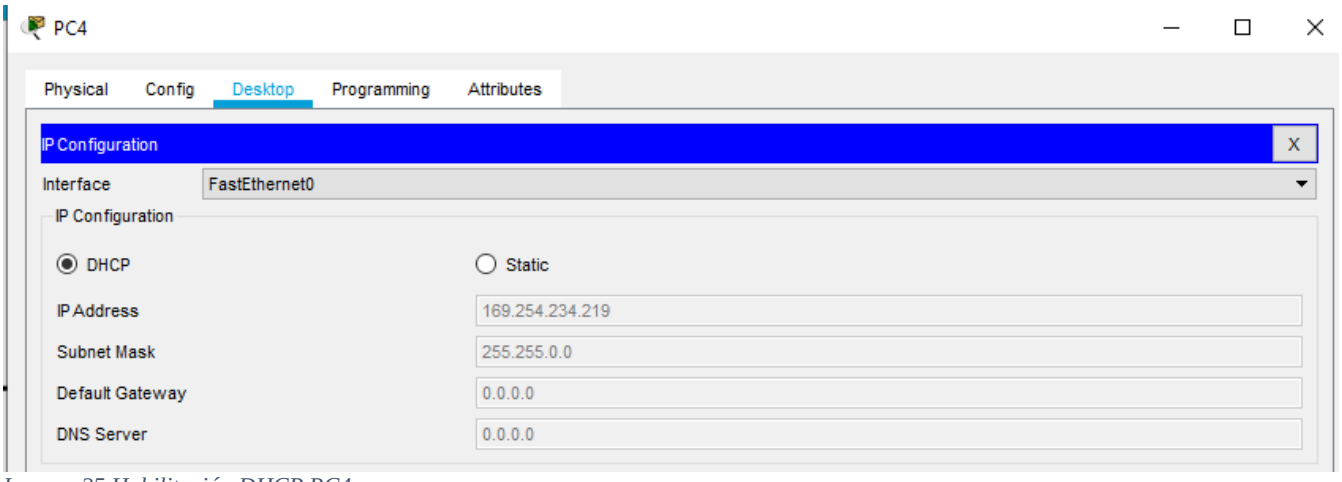

Imagen 25 Habilitación DHCP PC4

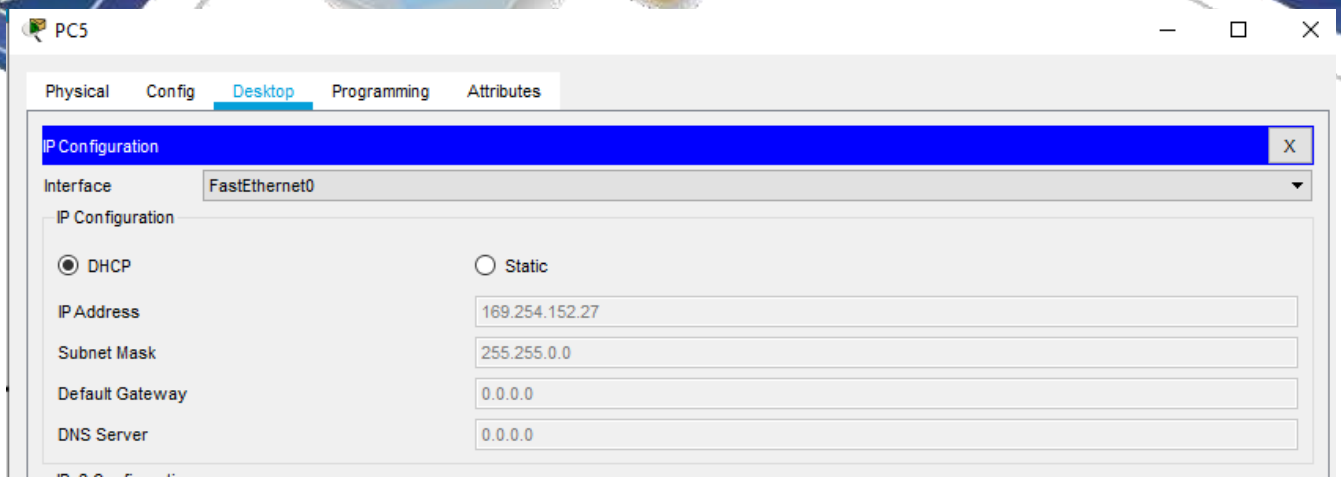

Imagen 26 Habilitación DHCP PC5

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

RTUNJA(dhcp-config)#ip nat inside source static 172.31.2.38 209.17.22.2
RTUNJA(config)#access-list 1 permit 172.0.0.0 0.255.255.255
RTUNJA(config)#ip nat inside source list 1 interfaceerface f0/1 overload
RTUNJA(config)#interface f0/1
RTUNJA(config-if)#ip nat outside
RTUNJA(config-if)#interface f0/0.1
RTUNJA(config-subif)#ip nat inside
RTUNJA(config-subif)#interface f0/0.20
RTUNJA(config-subif)#ip nat inside
RTUNJA(config-subif)#interface f0/0.30
RTUNJA(config-subif)#ip nat inside
RTUNJA(config-subif)#interface s0/0/0
RTUNJA(config-if)#ip nat inside
RTUNJA(config-if)#interface s0/0/1
RTUNJA(config-if)#ip nat inside
RTUNJA(config-if)#exit
RTUNJA(config)#ip route 0.0.0.0 0.0.0.0 209.165.220.3
RTUNJA(config)#router ospf 1
RTUNJA(config-router)#default-information originate
RTUNJA(config-router)#

RTUNJA#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

172.3.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.3.2.8/29 is directly connected, GigabitEthernet0/1
L 172.3.2.9/32 is directly connected, GigabitEthernet0/1
172.31.0.0/16 is variably subnetted, 4 subnets, 2 masks
C 172.31.2.32/30 is directly connected, Serial0/0/1
L 172.31.2.33/32 is directly connected, Serial0/0/1
C 172.31.2.36/30 is directly connected, Serial0/0/0
L 172.31.2.37/32 is directly connected, Serial0/0/0
209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.17.220.0/24 is directly connected, GigabitEthernet0/0
L 209.17.220.2/32 is directly connected, GigabitEthernet0/0

RCUNDINAMARCA#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

172.31.0.0/16 is variably subnetted, 4 subnets, 3 masks
C 172.31.2.8/29 is directly connected, GigabitEthernet0/1
L 172.31.2.9/32 is directly connected, GigabitEthernet0/1
C 172.31.2.36/30 is directly connected, Serial0/0/0
L 172.31.2.38/32 is directly connected, Serial0/0/0

RBUCARAMANGA#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

172.31.0.0/16 is variably subnetted, 4 subnets, 3 masks
C 172.31.2.0/29 is directly connected, GigabitEthernet0/0
L 172.31.2.1/32 is directly connected, GigabitEthernet0/0
C 172.31.2.32/30 is directly connected, Serial0/0/1
L 172.31.2.34/32 is directly connected, Serial0/0/1

El enrutamiento deberá tener autenticación.

```
Username: administrador
Password:
RTUNJA>enable
Password:
RTUNJA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RTUNJA(config)#interface s0/0/0
RTUNJA(config-if)#ip ospf authentication message-digest
RTUNJA(config-if)#ip ospf message-digest-key 1 md5 leon2019
RTUNJA(config-if)#interface s0/0/1
RTUNJA(config-if)#ip ospf authentication message-digest
RTUNJA(config-if)#ip ospf message-digest-key 1 md5 leon2019
RTUNJA(config-if)#
```

```
Username: administrador
Password:
RCUNDINAMARCA>enable
Password:
RCUNDINAMARCA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RCUNDINAMARCA(config)#interface s0/0/0
RCUNDINAMARCA(config-if)#ip ospf authentication message-digest
RCUNDINAMARCA(config-if)#ip ospf message-digest-key 1 md5 leon2019
RCUNDINAMARCA(config-if)#
```

```
Username: administrador
Password:
RBUCARAMANGA>enable
Password:
RBUCARAMANGA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RBUCARAMANGA(config)#line s0/0/0
^
% Invalid input detected at '^' marker.
RBUCARAMANGA(config)#interface s0/0/0
RBUCARAMANGA(config-if)#ip ospf authentication message-digest
RBUCARAMANGA(config-if)#ip ospf message-digest-key 1 md5 leon2019
RBUCARAMANGA(config-if)#
```

Se Configuran Alas Acl, De Acuerdo A Especificaciones Del Escenario 2 En El Router De Cundinamarca, La Vlan 20 No Accede A Internet Solo A La Red Interna De Tunja, La Vlan 10 De Cundinamarca Accede A Inernet Y No A La Red Interna De Tunja.

RCUNDINAMARCA(config-if)#access-list 111 deny ip 172.31.1.64 0.0.0.63 209.165.220.0 0.0.0.255
RCUNDINAMARCA(config)#access-list 111 permit ip any any
RCUNDINAMARCA(config)#interface f0/0.20
RCUNDINAMARCA(config-subif)#ip access-group 111 in
RCUNDINAMARCA(config-subif)#

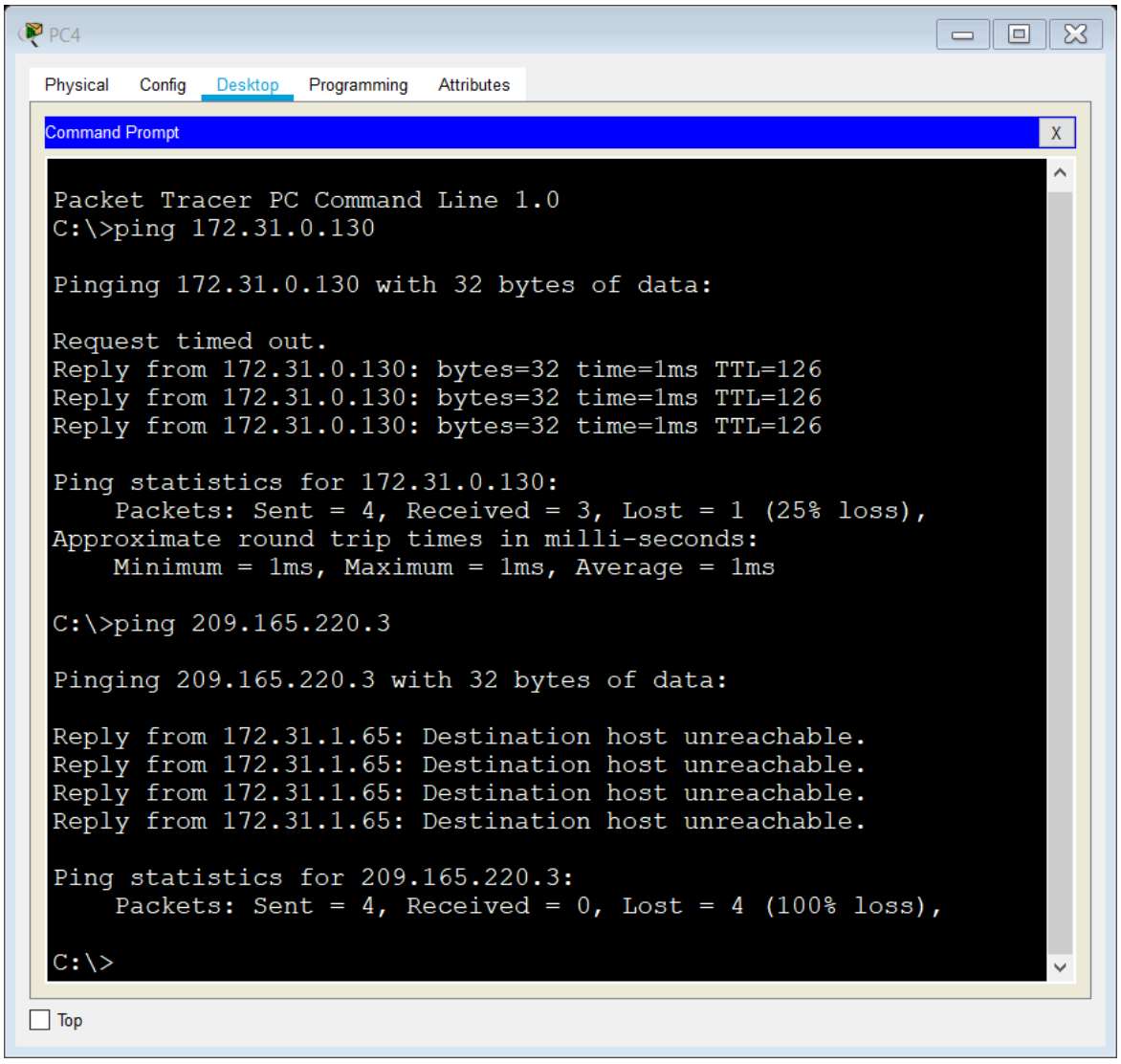

Imagen 27 Los hosts de VLAN 20 en RCUNDINAMARCA no acceden a interfaceernet, solo a la red interfaceerna de RTUNJA

Los hosts de VLAN 10 en RCUNDINAMARCA si acceden a interfaceernet y no a la red interfaceerna de RTUNJA.

RCUNDINAMARCA(config-subif)#access-list 112 permit ip 172.31.1.0 0.0.0.63 209.165.220.0 0.0.0.255
RCUNDINAMARCA(config)#access-list 112 deny ip any any
RCUNDINAMARCA(config)#interface f0/0.30
RCUNDINAMARCA(config-subif)#ip access-group 112 in
RCUNDINAMARCA(config-subif)#

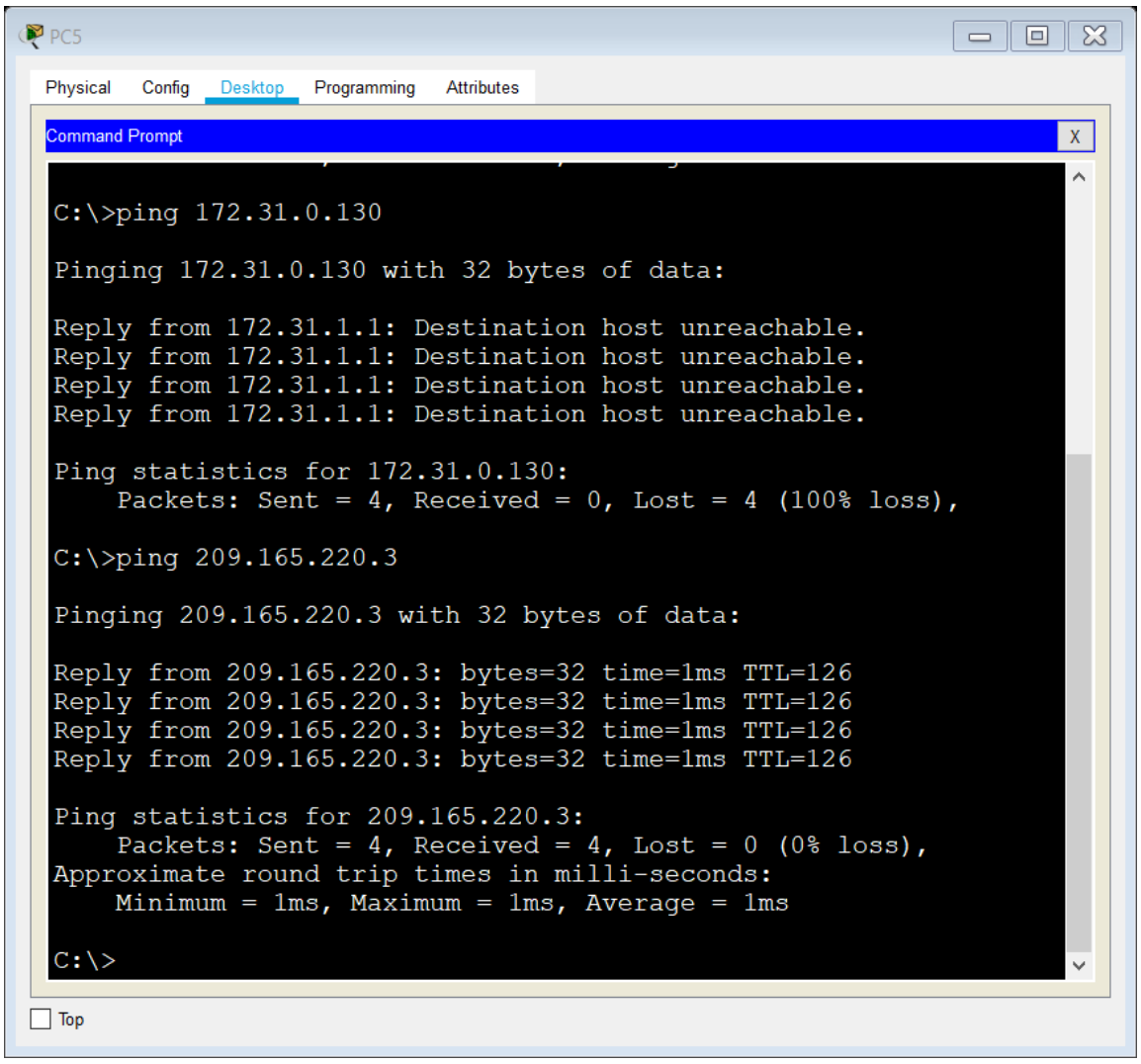

Imagen 28 Los hosts de VLAN 10 en RCUNDINAMARCA si acceden a interfaceernet y no a la red interfaceerna de RTUNJA

Los hosts de VLAN 30 en RTUNJA solo acceden a servidores web y ftp de interfaz.

```
RTUNJA(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 80
RTUNJA(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 21
RTUNJA(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 20
RTUNJA(config)#interface f0/0.30
RTUNJA(config-subif)#ip access-group 111 in
RTUNJA(config-subif)#
```

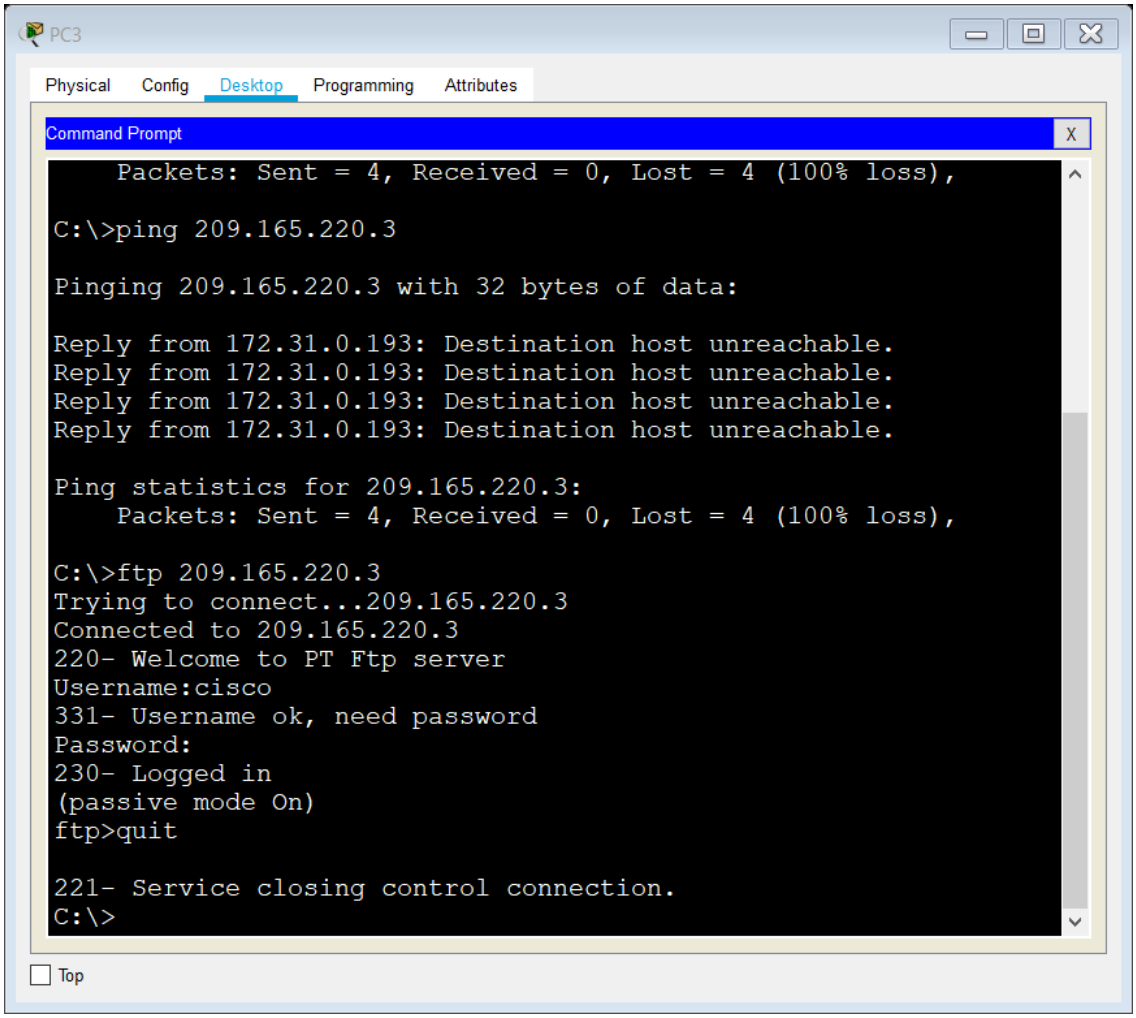

Imagen 29 Los hosts de VLAN 30 en RTUNJA solo acceden a servidores web y ftp de interfaz

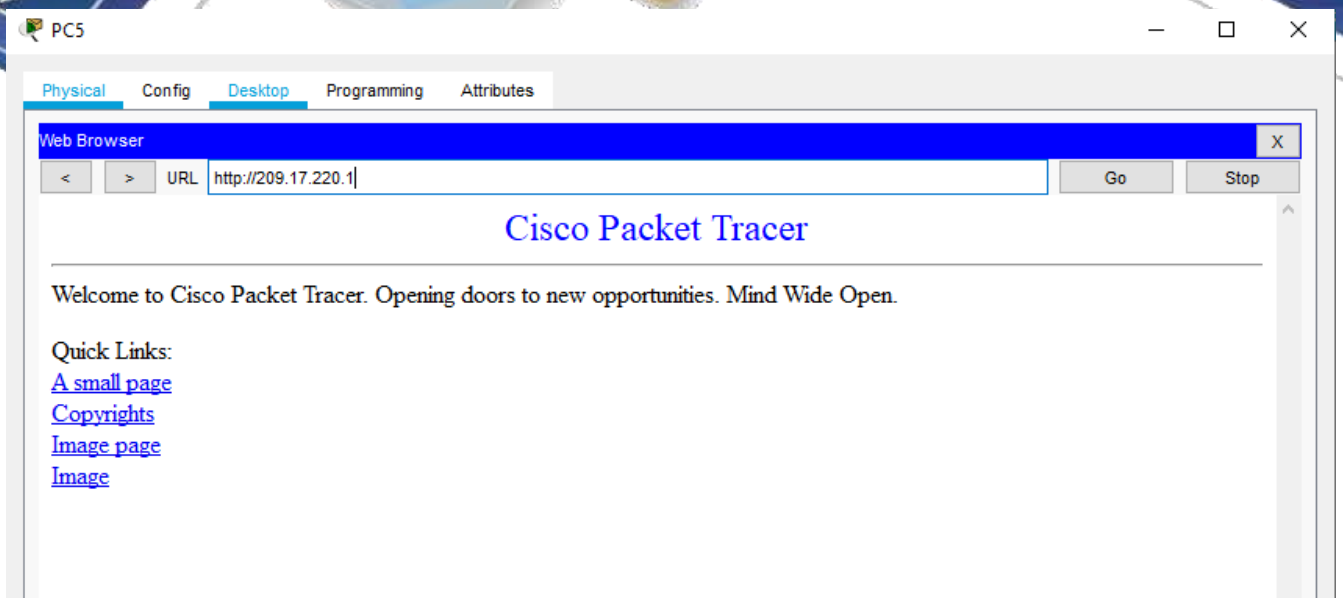

Imagen 30 Los hosts de VLAN 30 en RTUNJA solo acceden a servidores web y ftp de interfaz

Los hosts de VLAN 20 en RTUNJA solo acceden a la VLAN 20 de RCUNDINAMARCA y VLAN 10 de Bucaramanga.

RTUNJA(config-subif)#access-list 112 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
RTUNJA(config)#access-list 112 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
RTUNJA(config)#interface f0/0.20
RTUNJA(config-subif)#ip access-group 112 in
RTUNJA(config-subif)#

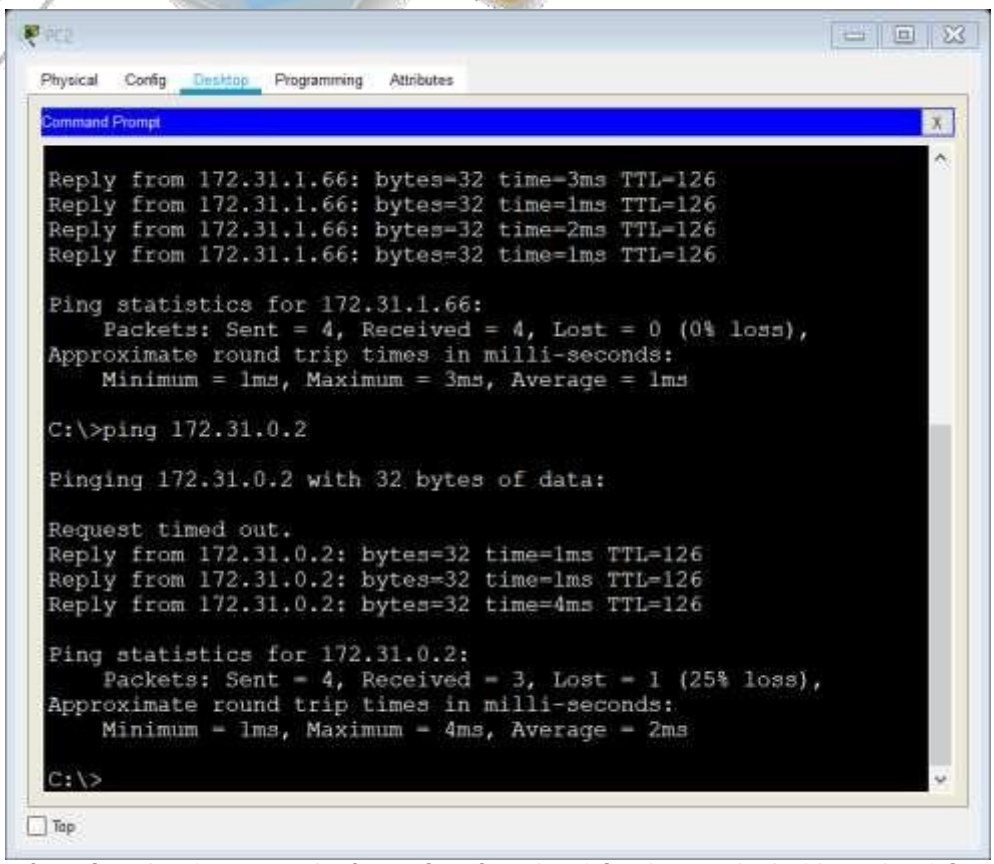

Imagen 31 Los hosts de VLAN 20 en RTUNJA solo acceden a la VLAN 20 de RCUNDINAMARCA y VLAN 10 de Bucaramanga.

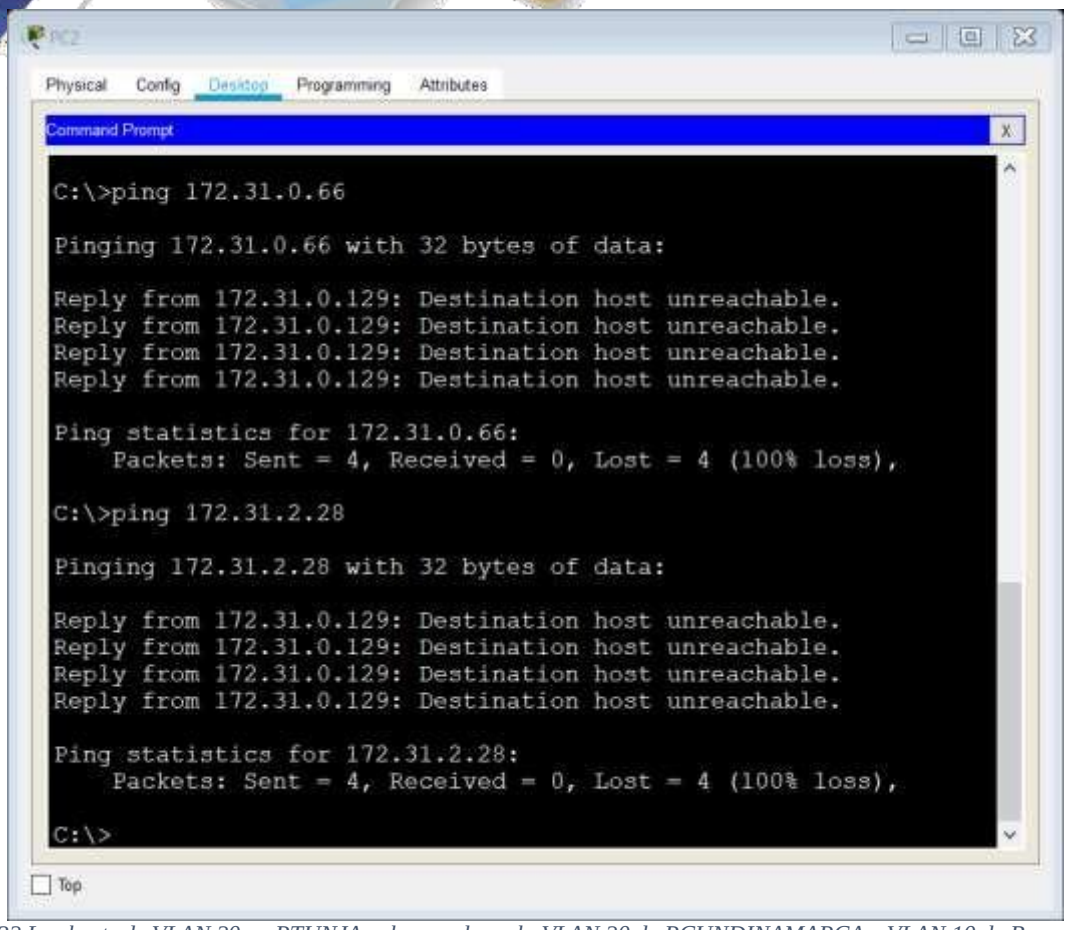

Imagen 32 Los hosts de VLAN 20 en RTUNJA solo acceden a la VLAN 20 de RCUNDINAMARCA y VLAN 10 de Bucaramanga.

Los hosts de VLAN 30 de Bucaramanga acceden a interfaceernet 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)#interface f0/0.30
BUCARAMANGA(config-subif)#ip access-group 111 in
BUCARAMANGA(config-subif)#

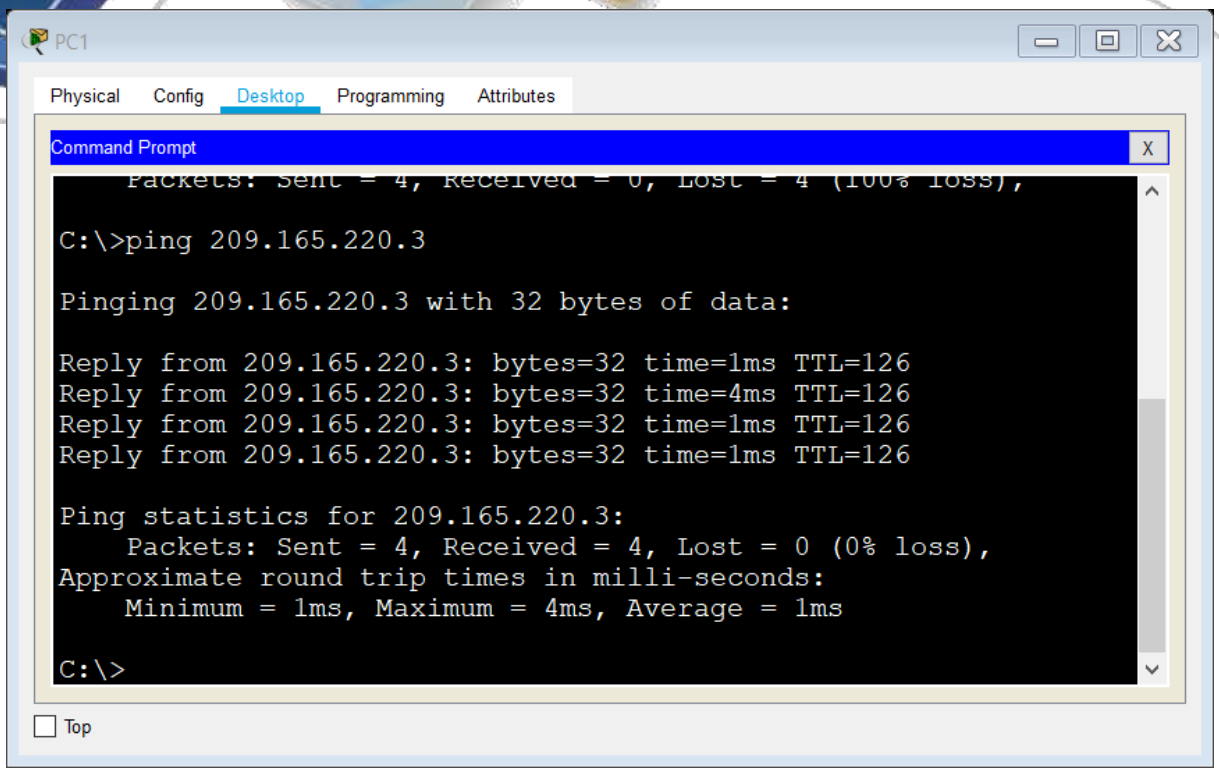

Imagen 33 Los hosts de VLAN 30 de Bucaramanga acceden a interfaceernet y a cualquier equipo de VLAN 10.

Los hosts de VLAN 10 en Bucaramanga acceden a la red de RCUNDINAMARCA (VLAN 20) y RTUNJA (VLAN 20), no interfaz.

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)#interface f0/0.10
BUCARAMANGA(config-subif)#ip access-group 112 in
BUCARAMANGA(config-subif)#

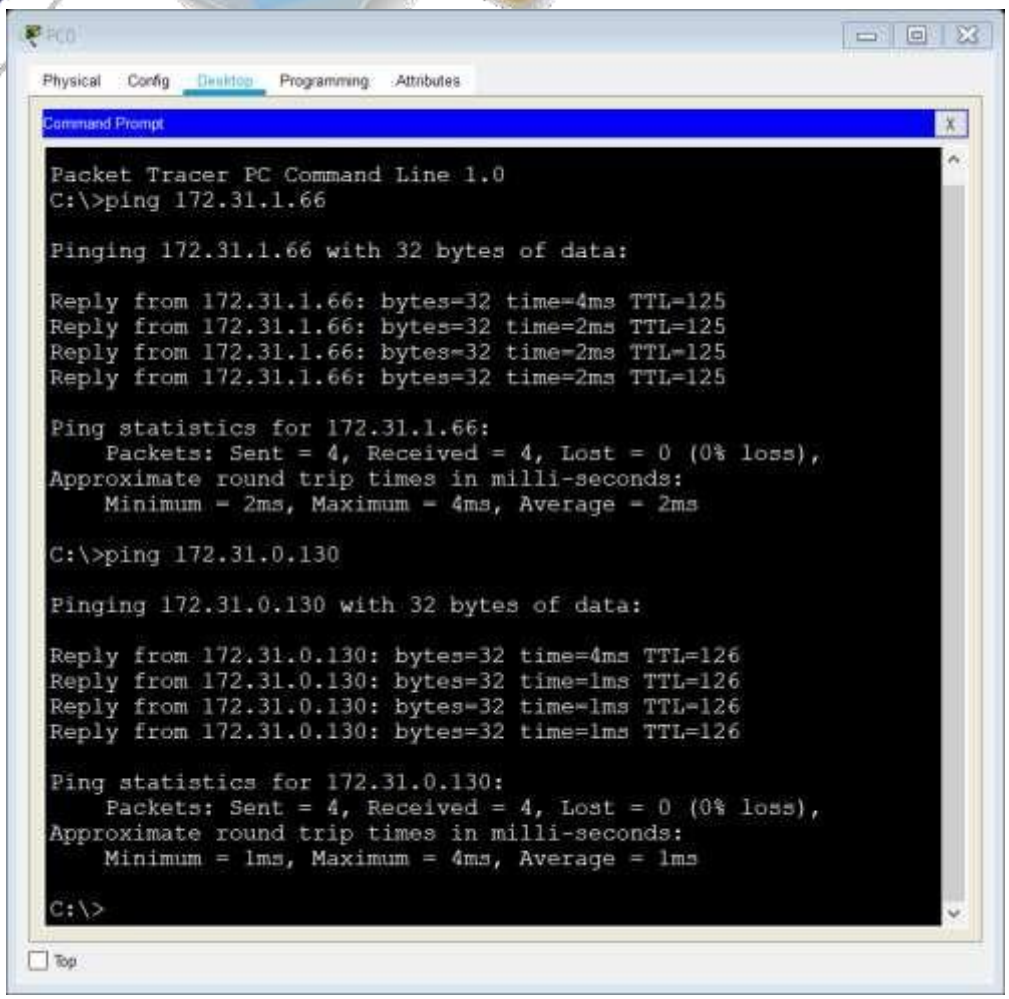

Imagen 34 Los hosts de VLAN 10 en Bucaramanga acceden a la red de RCUNDINAMARCA (VLAN 20) y RTUNJA (VLAN 20), no interfaz

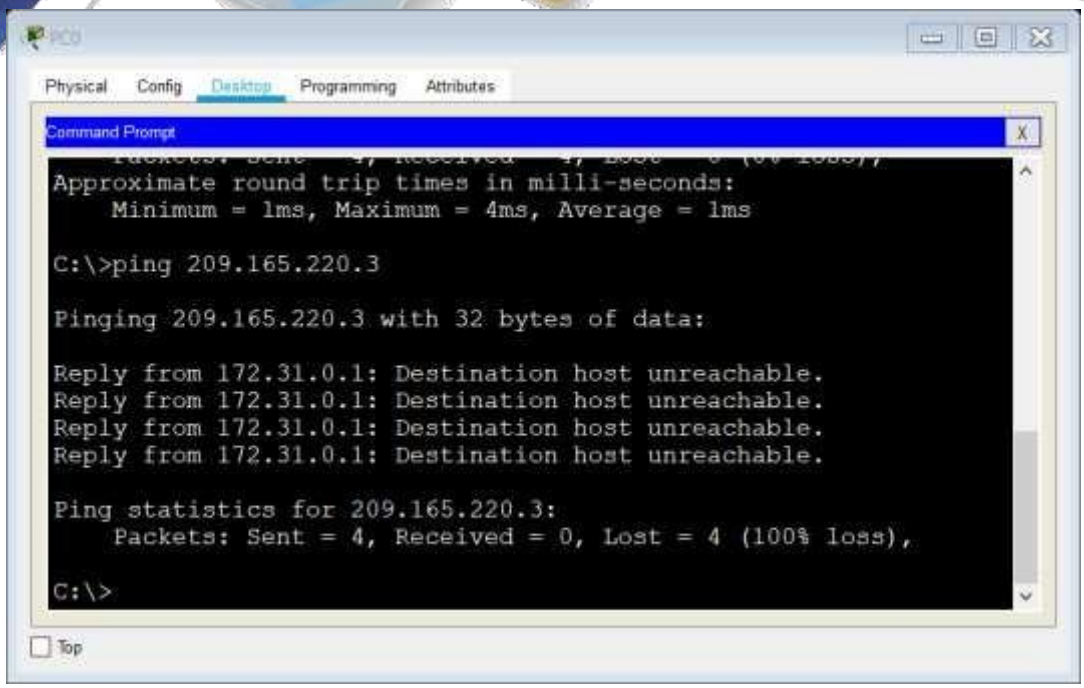

Imagen 35 Los hosts de VLAN 10 en Bucaramanga acceden a la red de RCUNDINAMARCA (VLAN 20) y RTUNJA (VLAN 20), no interfaz

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)#interface f0/0.10
BUCARAMANGA(config-subif)#ip access-group 113 out
BUCARAMANGA(config-subif)#

RTUNJA(config)#access-list 113 deny ip 172.3.2.8 0.0.0.7 172.31.0.128 0.0.0.63
RTUNJA(config)#access-list 113 deny ip 172.3.0.192 0.0.0.63 172.31.0.128 0.0.0.63
RTUNJA(config)#access-list 113 permit ip any any
RTUNJA(config)#interface f0/0.20
RTUNJA(config-subif)#ip access-group 113 out
RTUNJA(config-subif)#

RCUNDINAMARCA(config)#access-list 113 deny ip 172.31.2.8 0.0.0.7 172.31.1.64 0.0.0.63
RCUNDINAMARCA(config)#access-list 113 deny ip 172.31.1.0 0.0.0.63 172.31.1.64 0.0.0.63
RCUNDINAMARCA(config)#access-list 113 deny ip 172.31.2.24 0.0.0.7 172.31.1.64 0.0.0.63
RCUNDINAMARCA(config)#access-list 113 permit ip any any
RCUNDINAMARCA(config)#interface f0/0.20
RCUNDINAMARCA(config-subif)#ip access-group 113 out
RCUNDINAMARCA(config-subif)#

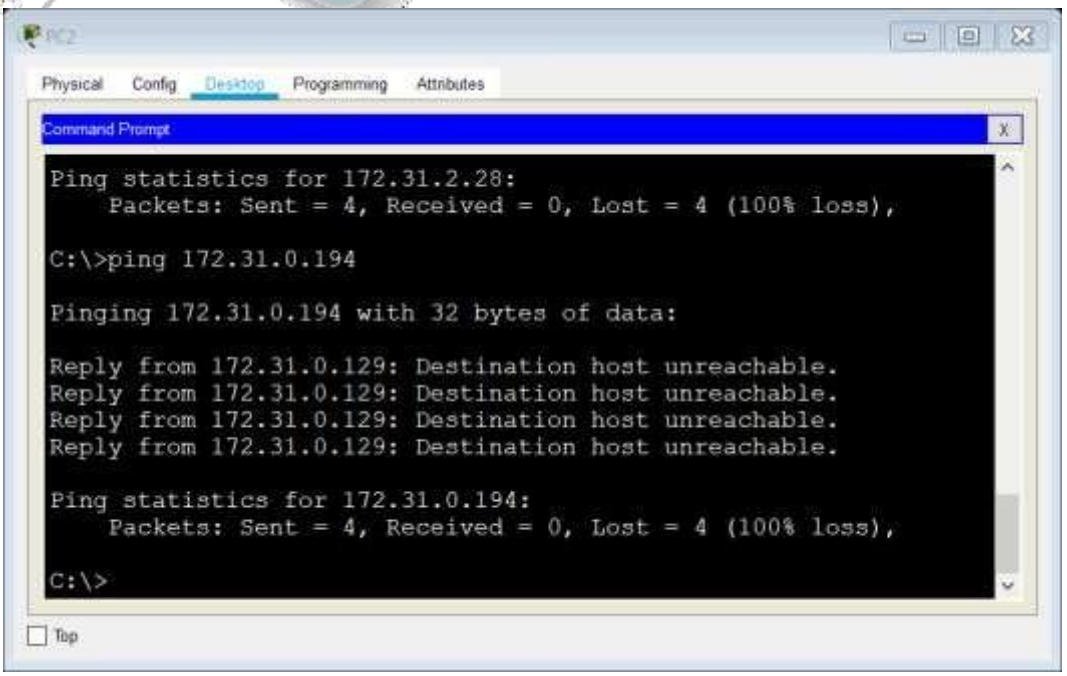

Imagen 36 Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.

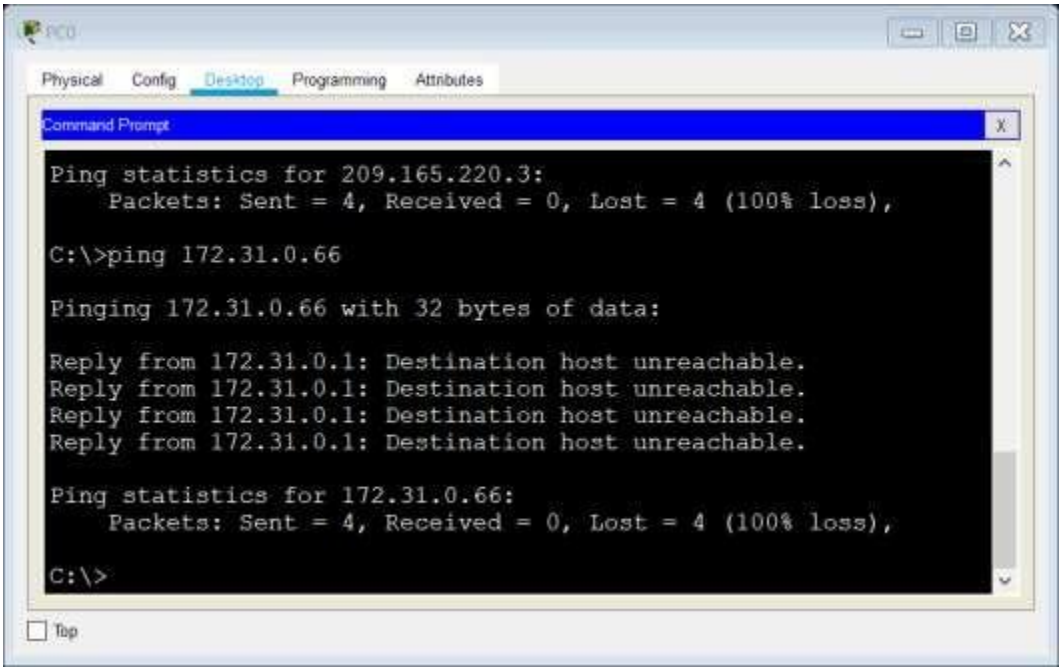

Imagen 37 Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.

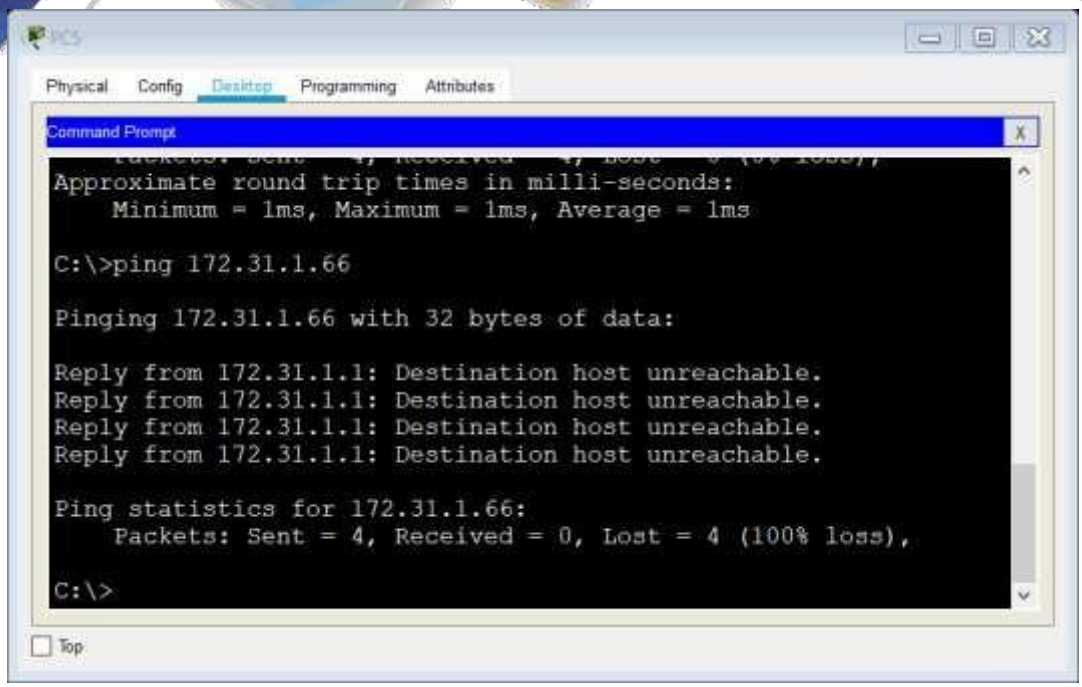

Imagen 38 Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.

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

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)#

RTUNJA(config-subif)#access-list 3 permit 172.31.2.0 0.0.0.7
RTUNJA(config)#access-list 3 permit 172.3.2.8 0.0.0.7
RTUNJA(config)#access-list 3 permit 172.31.2.8 0.0.0.7
RTUNJA(config)#line vty 0 15
RTUNJA(config-line)#access-class 3 in

RCUNDINAMARCA(config-subif)#access-list 3 permit 172.31.2.0 0.0.0.7
RCUNDINAMARCA(config)#access-list 3 permit 172.3.2.8 0.0.0.7
RCUNDINAMARCA(config)#access-list 3 permit 172.31.2.8 0.0.0.7
RCUNDINAMARCA(config)#line vty 0 15
RCUNDINAMARCA(config-line)#access-class 3 in
RCUNDINAMARCA(config-line)#

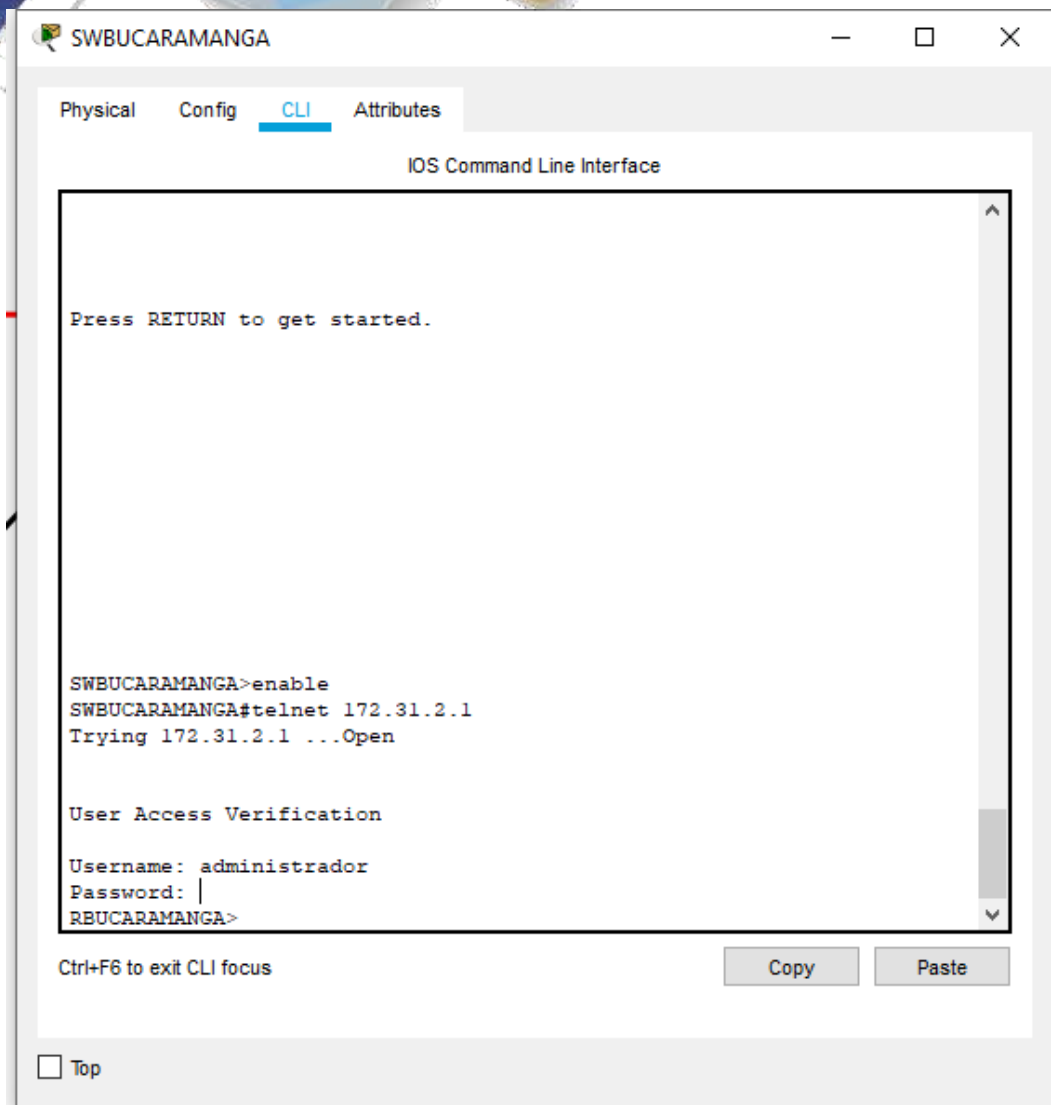

Imagen 39 Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los routers e interfaz.

Conclusiones

Las redes son una de las tecnologías que en los últimos años han avanzado a pasos agigantado y con la masificación de las TIC, es necesario comprender su estructura y funcionamiento al igual que su implementación con el propósito de poder elegir la mejor solución que se ajuste al escenario que nos encontremos al momento de planear su diseño, implementación y proyecciones.

Los parámetros de seguridad son esenciales en cualquier red ya que evita el acceso o robo de información vital de la empresa al igual que el saboteo de su red por personas inescrupulosas generando perdidas de información o pérdidas económicas.

Bibliografía

Cico Networking Academy – Ccna 1. (S.F.).

Https://Static-Course-Assets.S3.Amazonaws.Com/Itn503/Es/Index.Html.

Cico Networking Academy – Ccna 2. (S.F.). Https://Static-Course-Assets.S3.Amazonaws.Com/Rse503/Es/Index.Html.

Cisco Ccna – Configuraicón Dhcp . (S.F.). Http://Blog.Capacityacademy.Com/2014/01/09/Cisco-Ccna-Como-Configurar-Dhcp-En-Cisco-Router/.

Como Configurar Opsf En Router. (S.F.). Http://Blog.Capacityacademy.Com/2014/06/23/Cisco-Ccna-Como-Configurar-Ospf-En-Cisco-Router/.

Configuración Troncal 802.1q. (S.F.). Https://Www.Cisco.Com/C/Es_Mx/Support/Docs/Switches/Catalyst-4000-Series-Switches/24064-171.Html.