PRUEBA DE HABILIDADES PRÁCTICAS CNNA

PRESENTADO POR:
DANNY JOSÉ RÍOS PÉREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
MONTERÍA
DICIEMBRE DE 2019

PRUEBA DE HABILIDADES PRÁCTICAS CNNA

PRESENTADO POR:
DANNY JOSÉ RÍOS PÉREZ
GRUPO: 203092_26

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

TUTOR DE CURSO:
NILSON ALBEIRO FERREIRA MANZANARES

DIRECTOR DE CURSO:
JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
MONTERÍA
DICIEMBRE DE 2019

CONTENIDO

Pág.

INTRODUCCIÓN 12
OBJETIVOS 13
OBJETIVO GENERAL 13
OBJETIVOS ESPECÍFICOS 13
1. DESARROLLO DE LOS DOS ESCENARIOS 14
1.1. ESCENARIO 1 14
1.1.1. Configuración básica router 1 (Medellín) 15
1.1.2. Configuración básica router 2 (Bogotá) 16
1.1.3. Configuración básica router 3 (Cali) 17
1.1.4. Configuración básica switch 1 17
1.1.5. Configuración básica switch 2 18
1.1.6. Configuración básica switch 3 19
1.1.7. Asignación de interfaz fasthethernet y serial 20
1.1.7.1. Router Medellín 20
1.1.7.2. Router Bogotá 21
1.1.7.3. Router Cali 22
1.1.8. Verificación tabla de enrutamiento 23
1.1.8.1. Router Medellín 23
1.1.9. Diagnóstico de vecinos. 26
1.1.10. Balanceo de cargas 30
1.1.11. Configuración de enrutamiento 31
1.1.11.1. Router Medellín 31
1.1.11.2. Router Bogotá 32
1.1.11.3. Router Cali 32
1.1.12. Verificación de vecindad con los routers configurados con EIGRP 32
1.1.12.1. Router Medellín 33
1.1.12.2. Router Bogotá 33

1.1.12.3. Router Cali 34
1.1.13. Comprobación de las tablas de enrutamiento 34
1.1.13.1. Router Medellín 34
1.1.13.2. Router Bogotá 35
1.1.13.3. Router Cali 35
1.1.14. Diagnóstico de conectividad entre os puntos de la red 36
1.1.14.1. Ping desde el PC del router Cali a PC router Medellín 36
1.1.14.2. Ping desde el PC del router Cali a PC router Bogotá (Servidor) 36
1.1.15. Configuración de las listas de Control de Acceso 37
1.1.15.1. Router Medellin a Cali 37
1.1.15.2. Router Bogotá a Calí 38
1.1.15.3. Router Cali a Medellín 38
1.1.15.4. Router Cali a Bogotá 39
1.1.15.5. Router Medellín a Bogotá 39
1.1.15.6. Router Bogotá Medellín 40
1.1.16. Comprobación de la red instalada 42
1.2. ESCENARIO 2 52
1.2.1. Configuraciones router Bucaramanga 52
1.2.1.1. Básicas 52
1.2.1.2. Interfaces y seriales 53
1.2.1.3. Autenticacion AAA 54
1.2.1.4. Numero de intentos y tiempo máximo al detectar ataques 55
1.2.2. Configuraciones router Tunja 55
1.2.2.1. Básicas 55
1.2.2.2. Interfaces y seriales 55
1.2.2.3. Autenticacion AAA 57
1.2.2.4. Número de intentos y tiempo máximo al detectar ataques 57
1.2.3. Configuraciones del router Cundinamarca 58
1.2.3.1. Básicas 58
1.2.3.2. Interfaces y seriales 58

1.2.3.3. Autenticación AAA 59
1.2.3.4. Numero de intentos y tiempo máximo al detectar ataque 60
1.2.4. Configuraciones del switch Bucaramanga 60
1.2.4.1. Básicas 60
1.2.4.2. Vlans switch 61
1.2.5. Configuraciones del switch Tunja 62
1.2.5.1. Básicas 62
1.2.5.2. Vlans switch 63
1.2.6. Configuraciones switch Cundinamarca 64
1.2.6.1. Básicas 64
1.2.6.2. Vlans switch 65
1.2.7. Servidor TFTP (web interno) y almacenamiento de archivos de routers 66
1.2.7.1. Router Cundinamarca 66
1.2.7.2. Router Tunja 67
1.2.7.3. Router Bucaramanga 67
1.2.8. Proporcionando solo direcciones a los hosts de Bucaramanga y Cundinamarca 68
1.2.8.1. Router Bucaramanga 68
1.2.8.2. Router Cundinamarca 68
1.2.8.3. Router Tunja 69
1.2.9. Web server con NAT estático y equipos con NAT de sobrecarga (PAT) 70
1.2.9.1. Router Tunja 70
1.2.10. El enrutamiento deberá tener autenticación 73
1.2.10.1. Router Bucaramanga 73
1.2.10.2. Router Tunja 74
1.2.10.3. Router Cundinamarca 75
1.2.11. Listas de control de acceso 76
2. CONCLUSIONES 92
BIBLIOGRAFÍA 93

LISTA DE TABLAS

Pág

Tabla 1. Tabla de configuración 15

Tabla 2. Verificaciones listas de acceso 43

LISTA DE FIGURAS

Pág

Figura 1. Topología de la red 14
Figura 2. Topología de la red en Packet Tracer 14
Figura 3. Tabla de enrutamiento 23
Figura 4. Verificación tabla de enrutamiento (Medellín) 24
Figura 5. Tabla de enrutamiento (Bogotá) 24
Figura 6. Verificación tabla de enrutamiento (Bogotá) 25
Figura 7. Tabla de enrutamiento (Cali) 25
Figura 8. Verificación tabla de enrutamiento (Cali) 26
Figura 9. Vista vecinos (Medellín) 27
Figura 10. Verificación lista vecinos (Medellín) 27
Figura 11. Vista vecinos (Bogotá) 28
Figura 12. Verificación lista vecinos (Bogotá) 28
Figura 13. Vista vecinos (Cali) 29
Figura 14. Verificación lista vecinos (Bogotá) 29
Figura 15. Verificación balanceo de cargas (Medellín) 30
Figura 16. Verificación balanceo de cargas (Bogotá) 30
Figura 17. Verificación balanceo de cargas (Cali) 31
Figura 18. Verificación vecindad (Medellín) 33
Figura 19. Verificación vecindad (Bogotá) 33
Figura 20. Verificación vecindad (Cali) 34
Figura 21. Tabla de enrutamiento (Medellín) 34
Figura 22. Tabla de enrutamiento (Bogotá) 35
Figura 23. Tabla de enrutamiento (Cali) 35
Figura 24. Conectividad Cali – Medellín 36
Figura 25. Conectividad Cali – Bogotá 36
Figura 26. Conexión Telnet Medellín – Cali 37

Figura 27. Conexión Telnet Cali – Bogotá 38
Figura 28. Conexión Telnet Cali – Medellín 38
Figura 29. Conexión Telnet Cali – Bogotá 39
Figura 30. Conexión Telnet Medellín – Bogotá 39
Figura 31. Conexión Telnet Bogotá - Medellín 40
Figura 32. Lista ACL router Cali 41
Figura 33. Lista ACL router Bogotá 42
Figura 34. Telnet router Medellín Cal 43
Figura 35. Telnet WS1 a router Bogotá 44
Figura 36. Telnet servidor a router Cali 44
Figura 37. Telnet servidor a router Medellín 45
Figura 38. LAN del router Medellín a router Cali 45
Figura 39. LAN del router Cali a router Cali 46
Figura 40. LAN del router Medellín a router Medellín 46
Figura 41. LAN del Router Cali a router Medellín 47
Figura 42. LAN del router Cali WS_1 47
Figura 43. LAN del router Medellín WS_1 48
Figura 44. LAN del router a LAN router de Cali 48
Figura 45. LAN del router Cali a Servidor 49
Figura 46. LAN del router Medellín a Servidor 49
Figura 47. Servidor a LAN del router Medellín 50
Figura 48. Servidor a LAN del router Cali 50
Figura 49. Router Cali a LAN del router Medellín 51
Figura 50. Router Medellín a LAN del router Cali 51
Figura 51. Topología escenario 2 52
Figura 52. Verificación autenticación AAA router Bucaramanga 54
Figura 53. Verificación autenticación AAA router Tunja 57
Figura 54. Verificación autenticación AAA router Cundinamarca 60
Figura 55. Verificación vlans Switch Bucaramanga 62
Figura 56. Verificación vlans switch Tunja 64

Figura 57. Verificación vlans switch Cundinamarca 66
Figura 58. Almacenamiento de archivos TFTP 68
Figura 59. Configuración NAT router Bucaramanga 71
Figura 60. Configuración NAT router Tunja 72
Figura 61. Configuración NAT router Cundinamarca 72
Figura 62. Autenticación de enrutamiento router Bucaramanga 73
Figura 63. Autenticación de enrutamiento router Tunja 74
Figura 64. Autenticación de enrutamiento router Cundinamarca 75
Figura 65. ACL vlan 20 router Cundinamarca a red interna Tunja 76
Figura 66. ACL pc vlan 20 sin acceso a internet 77
Figura 67. ACL pc vlan 30 Cundinamarca con acceso a internet 78
Figura 68. ACL pc vlan 30 Cundinamarca a pc red de Tunja 78
Figura 69. Mensajes vlan 30 Cundinamarca a pc red de Tunja 79
Figura 70. ACL vlan 30 acceso tfp 80
Figura 71. ACL vlan 30 acceso internet 80
Figura 72. Verificación acceso a la vlan 20 y 10 81
Figura 73. acceso a vlan 20 Tunja a vlan 10 Bucaramanga 82
Figura 74. Verificación rechazo a vlan fuera del ACL 82
Figura 75. Acceso vlan 30 Bucaramanga a internet 83
Figura 76. Acceso vlan 30 a vlan 10 84
Figura 77. Acceso vlan 10 Bucaramanga a Cundinamarca y Tunja vlan 20 85
Figura 78. Internet vlan 10 Bucaramanga a Cundinamarca y Tunja vlan 20 85
Figura 79. Vlan 30 Bucaramanga a vlan 20 Tunja 87
Figura 80. vlan 30 Tunja a vlan 20 Cundinamarca 88
Figura 81. Vlan 30 Cundinamarca a vlan 30 Bucaramanga 88
Figura 82. sin acceso entre host a diferentes vlan 89
Figura 83. Verificación acceso a router Cundinamarca 90
Figura 84. Verificación acceso a router Bucaramanga 91
Figura 85. Verificación acceso a internet 91

RESUMEN

Actualmente se hace necesario la implementación de las telecomunicaciones en el sector empresarial y tener nociones sobre la administración de redes. Por tal razón es importante conocer dicho rol en cada entorno, entendiendo el funcionamiento de la información mediante las redes de información.

En esta actividad individual se relacionan conceptos de arquitectura, estructura, funciones y componentes en dos escenarios con medios y operaciones de redes introducidos para proporcionar una función específica. Como solución a la tarea se hace necesario configurar e interconectar entre sí cada dispositivo, estableciendo configuraciones básicas acorde con los parámetros establecidos para el direccionamiento IP, protocolos de enrutamiento y otros aspectos que reúnen la topología de red. Esto finalmente con el firme propósito de obtener los alcances necesarios en el desarrollo del curso CISCO CCNA, que serán mostrados a lo largo de este trabajo.

PALABRAS CLAVE: switch, redes, configuraciones, dispositivos, escenarios, protocolos.

ABSTRACT

Currently it is necessary to implement telecommunications in the business sector and have notions about network administration. For this reason it is important to know this role in each environment, understanding the operation of information through information networks.

In this individual activity, concepts of architecture, structure, functions and components in two scenarios are related to media and network operations introduced to provide a specific function. As a solution to the task it is necessary to configure and interconnect each device, establishing basic configurations according to the parameters established for IP addressing, routing protocols and other aspects that bring together the network topology. This finally with the firm intention of obtaining the necessary scopes in the development of the CISCO CCNA course, which will be shown throughout this work.

KEYWORDS: switch, networks, configurations, devices, scenarios, protocols.

INTRODUCCIÓN

El siguiente trabajo está enmarcado sobre las pruebas de habilidades practicas del DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN), donde podemos encontrar la solución de dos casos planteados como escenarios empleando los conocimientos adquiridos en cada unidad desarrollada.

Las destrezas adquiridas se integran para lograr soluciones integradas en redes LAN y WLAN con la aplicación de conceptos para lograr la configuración de direcciones IP, inicialización de dispositivos, configuración básica de routers, switches, establecimiento de seguridad, routing, Vlans, protocolo RIP, servicio de DHCP, protocolo de enrutamiento OSPF, listas de acceso, NAT, configuración de encapsulamiento, entre otros. Estas actividades han sido desarrolladas mediante el software de simulación Packet Tracer, imitando de una forma virtual los escenarios con su respectiva solución.

OBJETIVOS

OBJETIVO GENERAL

Analizar los ejercicios propuestos como escenarios para generar su solución, aplicando las habilidades obtenidas usando las herramientas y recursos necesarios consignados en las temáticas del Diplomado CISCO CCNA.

OBJETIVOS ESPECÍFICOS

- Identificar los dispositivos a utilizar para la construcción de la topología de red para cada escenario.
- Configurar los dispositivos de comunicación como routers, switch, servidores.
- Conocer y aplicar los diferentes protocolos de enrutamiento.
- Comprobar la conectividad de los dispositivos de la red.
- Implementar seguridad en los elementos que compone la red, entre otras políticas necesarias.
- Establecer los servicios de OPSFv2, protocolo dinámico de Routing, DHCP, NAT, RIP Ver2.

1. DESARROLLO DE LOS DOS ESCENARIOS

1.1. ESCENARIO 1

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

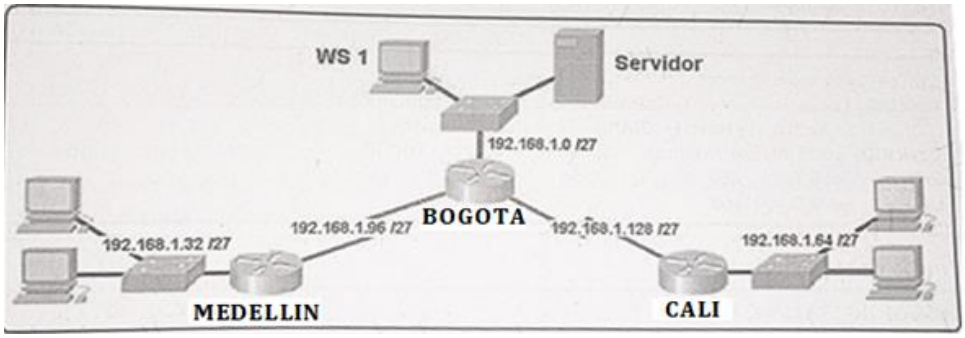

Figura 1. Topología de la red.

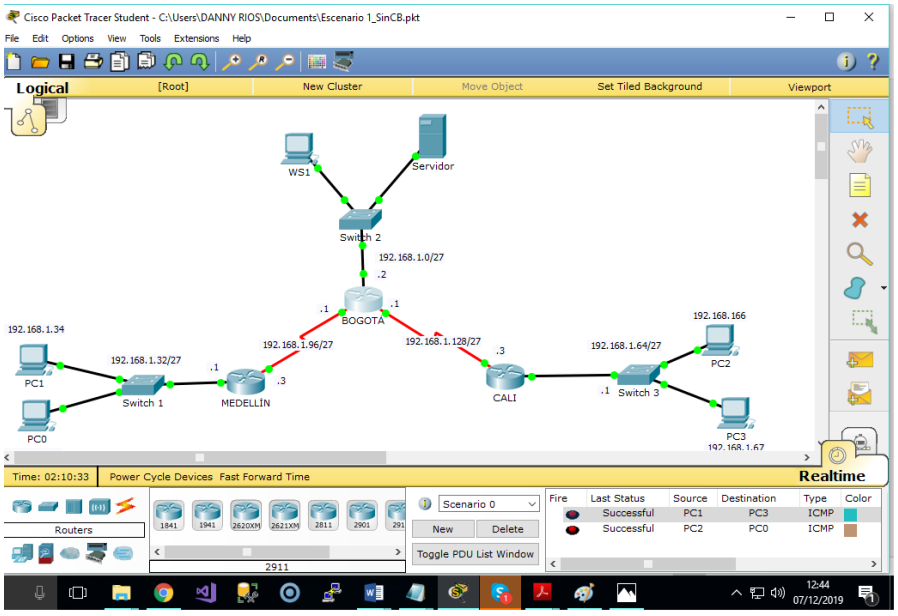

Figura 2. Topología de la red en Packet Tracer.

	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 1. Tabla de configuración.

En primer lugar se realizan las configuraciones básicas de los routers

1.1.1. Configuración básica router 1 (Medellín)

Router>enable

Router#config terminal

Router(config)#no ip domain-lookup

Router(config)#hostname R1

R1(config)#enable secret cisco

R1(config)#line console 0

R1(config-line)#password cisco

R1(config-line)#login

R1(config-line)#exit

R1(config-line)#line vty 0 4

R1(config-line)#password cisco

R1(config-line)#login

R1(config-line)#exit

R1(config)#service password-encryption

R1(config)#banner motd #Acceso solo a personal autorizado#

R3(config)#exit

R3#copy running-config startup-config

1.1.2. Configuración básica router 2 (Bogotá)

Router>enable

Router#config terminal

Router(config)#no ip domain-lookup

Router(config)#hostname R2

R2(config)#enable secret cisco

R2(config)#line console 0

R2(config-line)#password cisco

R2(config-line)#login

R2(config-line)#exit

R2(config-line)#line vty 0 4

R2(config-line)#password cisco

R2(config-line)#login

R2(config-line)#exit

R2(config)#service password-encryption

R2(config)#banner motd #Acceso solo a personal autorizado#

R3(config)#exit

R3#copy running-config startup-config

1.1.3. Configuración básica router 3 (Cali)

Router>enable

Router#config terminal

Router(config)#no ip domain-lookup

Router(config)#hostname R3

R3(config)#enable secret cisco

R3(config)#line console 0

R3(config-line)#password cisco

R3(config-line)#login

R3(config-line)#exit

R3(config-line)#line vty 0 15

R3(config-line)#password cisco

R3(config-line)#login

R3(config-line)#exit

R3(config)#service password-encryption

R3(config)#banner motd #Acceso solo a personal autorizado#

R3(config)#exit

R3#copy running-config startup-config

1.1.4. Configuración básica switch 1

Switch>enable

Switch#configure terminal

Switch(config)#hostname S1

S1(config)#enable secret cisco

S1(config)#line console 0

S1(config-line)#password cisco

S1(config-line)#login

S1(config-line)#exit

S1(config)#line vty 0 4

S1(config-line)#password cisco

S1(config-line)#login

S1(config-line)#service password-encryption

S1(config)#banner motd #Prohibido el acceso no autorizado!#

S1(config)#exit

S1#copy running-config startup-config

1.1.5. Configuración básica switch 2

Switch>enable

Switch#configure terminal

Switch(config)#hostname S2

S2(config)#enable secret cisco

S2(config)#line console 0

S2(config-line)#password cisco

S2(config-line)#login

S2(config-line)#exit

S2(config)#line vty 0 4

S2(config-line)#password cisco

S2(config-line)#login

S2(config-line)#service password-encryption

S2(config)#banner motd #Prohibido el acceso no autorizado!#

S2(config)#exit

S2#copy running-config startup-config

1.1.6. Configuración básica switch 3

Switch>enable

Switch#configure terminal

Switch(config)#hostname S3

S3(config)#enable secret cisco

S3(config)#line console 0

S3(config-line)#password cisco

S3(config-line)#login

S3(config-line)#exit

S3(config)#line vty 0 4

S3(config-line)#password cisco

S3(config-line)#login

S3(config-line)#service password-encryption

S3(config)#banner motd #Prohibido el acceso no autorizado!#

S3(config)#exit

S3#copy running-config startup-config

1.1.7. Asignación de interfaz fasthethernet y serial

En esta parte procedemos a entrar a la configuracion de la interfaz fastethernet y serial 0/0 y asignarle IP y su respectuva máscara de red.

1.1.7.1. Router Medellín

En esta parte procedemos a entrar a la configuracion de la interfaz fasethernet y serial 0/0 y asignarle IP y su respectuva máscara de red.

Router>enable

Router#configure terminal

Router(config)#interface fastethernet 0/0

Router(config-if)#ip address 192.168.1.33 255.255.255.224

Router(config-if)#no shutdown

Router(config-if)#

Router(config-if)#exit

Router(config)#interface serial 0/0

Router(config-if)#ip address 192.168.1.99 255.255.255.224

Router(config-if)#no shutdown

Router(config-if)#

Router(config-if)#exit

Router(config)#

Router>enable

Router#configure terminal

Router(config)#ip route 192.168.1.0 255.255.255.224 192.168.1.97

Router(config)#ip route 192.168.1.64 255.255.255.224 192.168.1.97

Router(config)#exit

Router#copy running-config startup-config

1.1.7.2. Router Bogotá

Router>enable

Router#configure terminal

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

Router(config)#interface fastethernet 0/0

Router(config-if)#ip address 192.168.1.1 255.255.255.224

Router(config-if)#no shutdown

Router(config-if)#

Router(config-if)#exit

Router(config)#interface serial 0/0

Router(config-if)#ip address 192.168.1.98 255.255.255.224

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#interface serial 0/1

Router(config-if)#ip address 192.168.1.130 255.255.255.224

Router(config-if)#no shutdown

Router(config-if)#exit

Router(config)#

Router>enable

Router#configure terminal

Router(config)#ip route 192.168.1.64 255.255.255.224 192.168.1.131

Router(config)#ip route 192.168.1.32 255.255.255.224 192.168.1.99

Router(config)#exit

Router#copy running-config startup-config

1.1.7.3. Router Cali

Router>enable

Router#configure terminal

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

Router(config)#interface fastethernet 0/0

Router(config-if)#ip address 192.168.1.65 255.255.255.224

Router(config-if)#no shutdown

Router(config-if)#

Router(config-if)#exit

Router(config)#interface serial 0/0

Router(config-if)#ip address 192.168.1.131 255.255.255.224

Router(config-if)#no shutdown

Router(config-if)#

Router(config-if)#exit

Router(config)#

Router(config)#ip route 192.168.1.0 255.255.255.224 192.168.1.129

Router(config)#ip route 192.168.1.32 255.255.255.224 192.168.1.129

Router(config)#exit

Router#copy running-config startup-config

1.1.8. Verificación tabla de enrutamiento

Para verificar la tabla de enrutamiento utilizamos el comando show ip route.

1.1.8.1. Router Medellín

- **Antes de configurar los routers tenemos:**

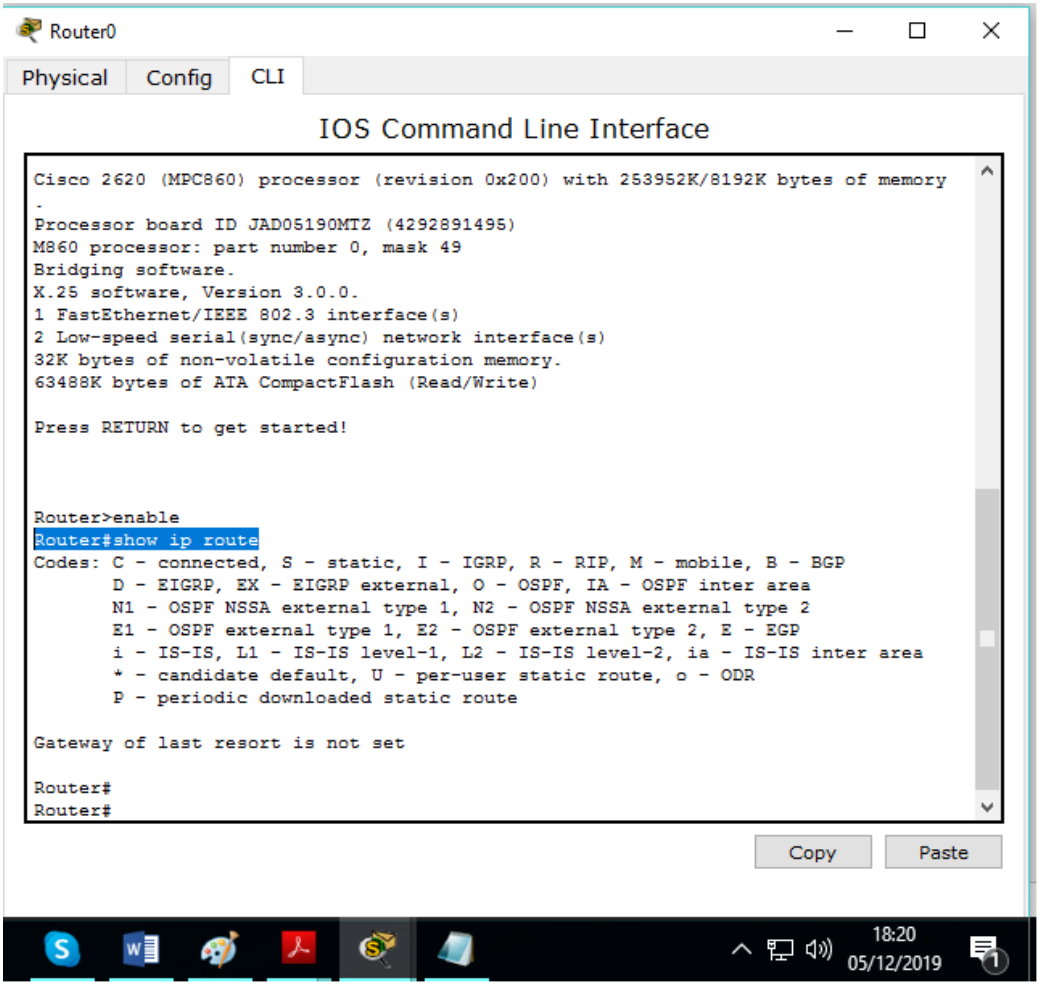

Figura 3. Tabla de enrutamiento.

➢ **Despues de la configuración:**

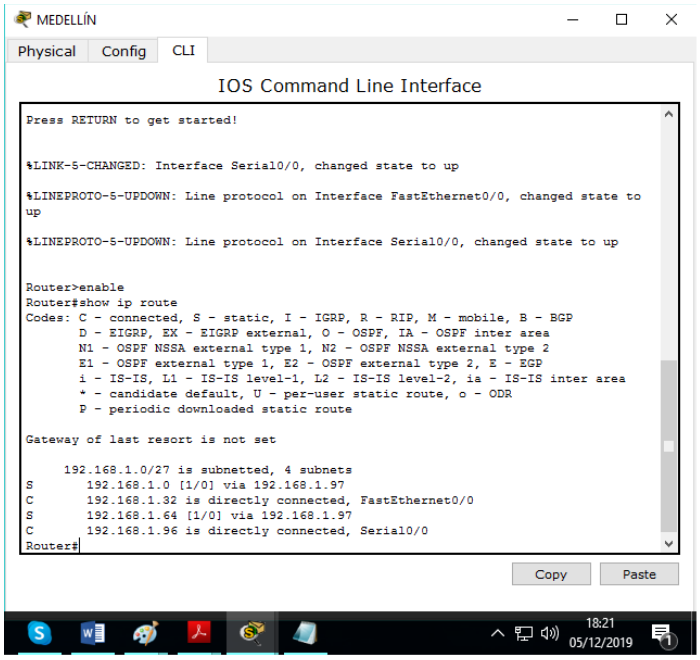

Figura 4. Verificación tabla de enrutamiento (Medellín).

➢ **Router Bogotá antes**

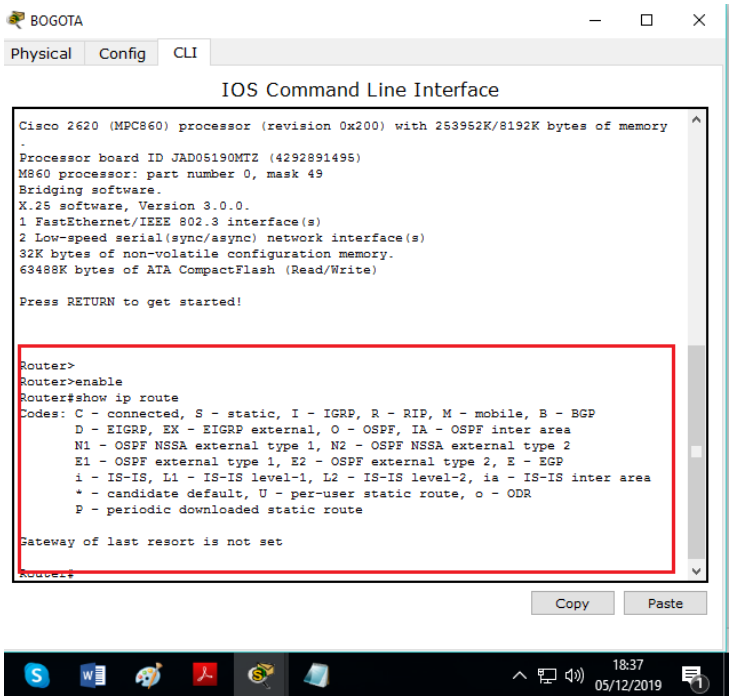

Figura 5. Tabla de enrutamiento (Bogotá).

➢ **Después:**

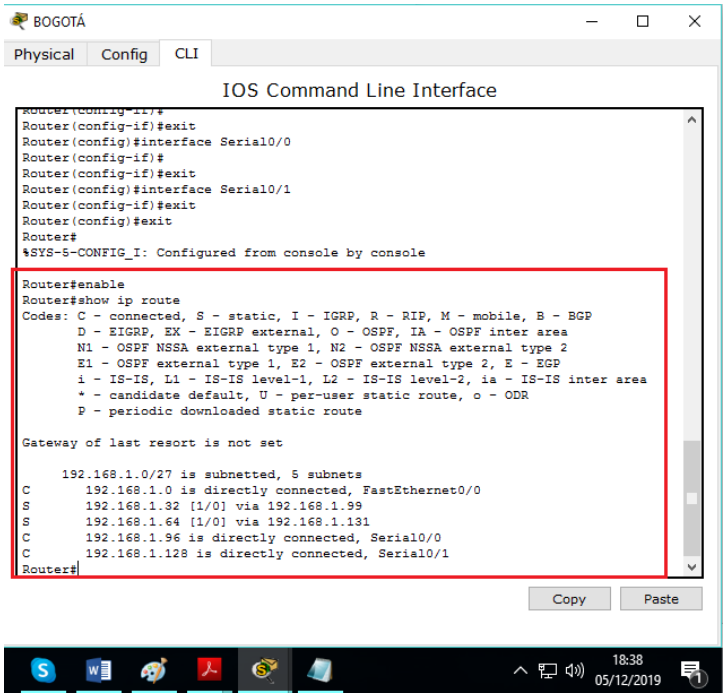

Figura 6. Verificación tabla de enrutamiento (Bogotá).

➢ **Router Cali antes**

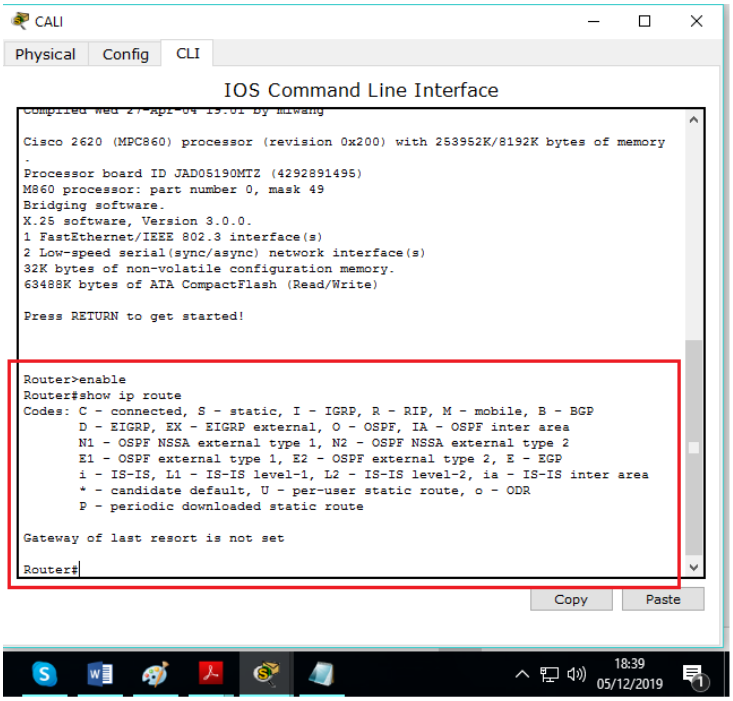

Figura 7. Tabla de enrutamiento (Cali).

- **Después**

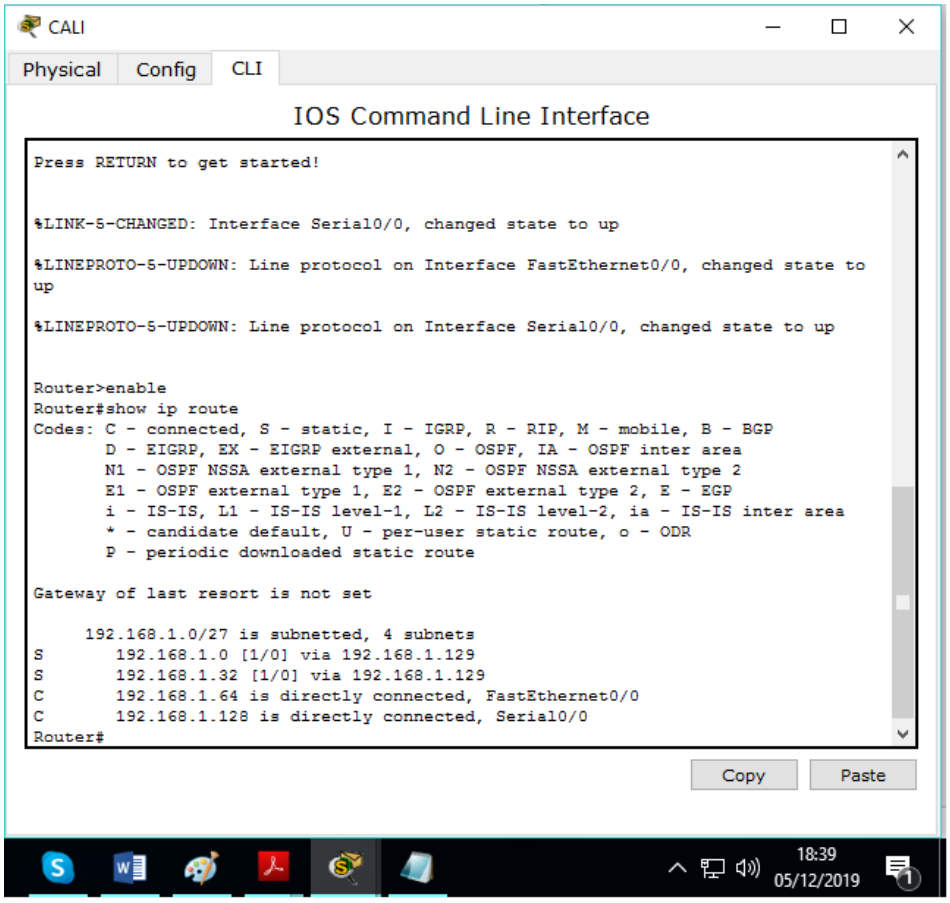

Figura 8. Verificación tabla de enrutamiento (Cali).

1.1.9. Diagnóstico de vecinos.

El comando adecuado para verificar es “cdp neighbors”, antes de esto se debe habilitar con cdp run:

- **Router Medellín (Antes)**

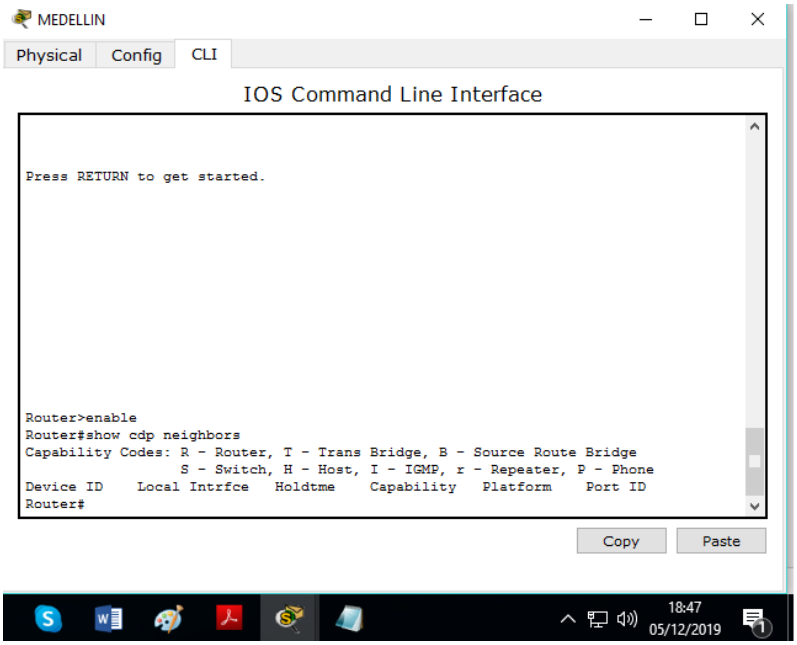

Figura 9. Vista vecinos (Medellín).

- **Router Medellín (Despúes)**

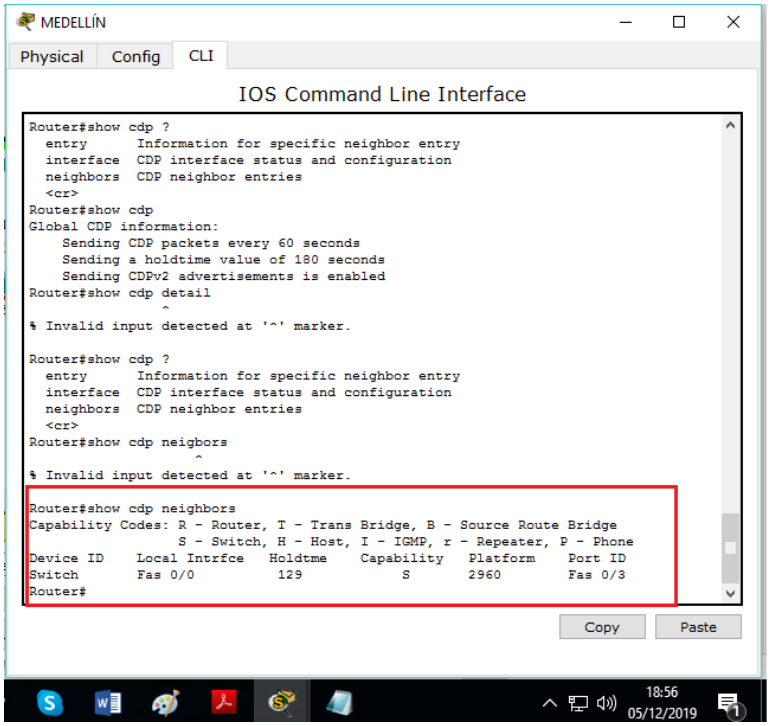

Figura 10. Verificación lista vecinos (Medellín).

- **Router Bogotá (Antes)**

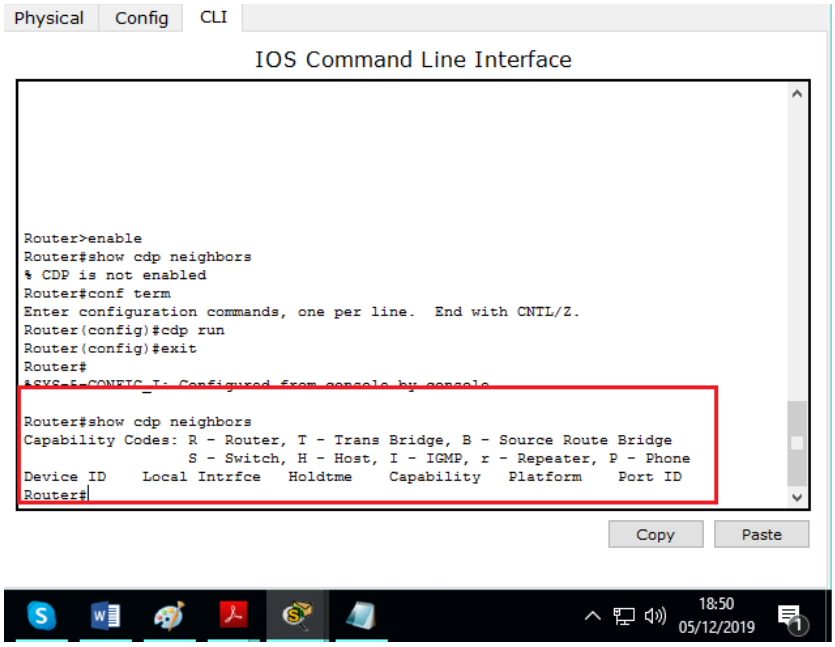

Figura 11. Vista vecinos (Bogotá).

Router Bogotá (Despúes)

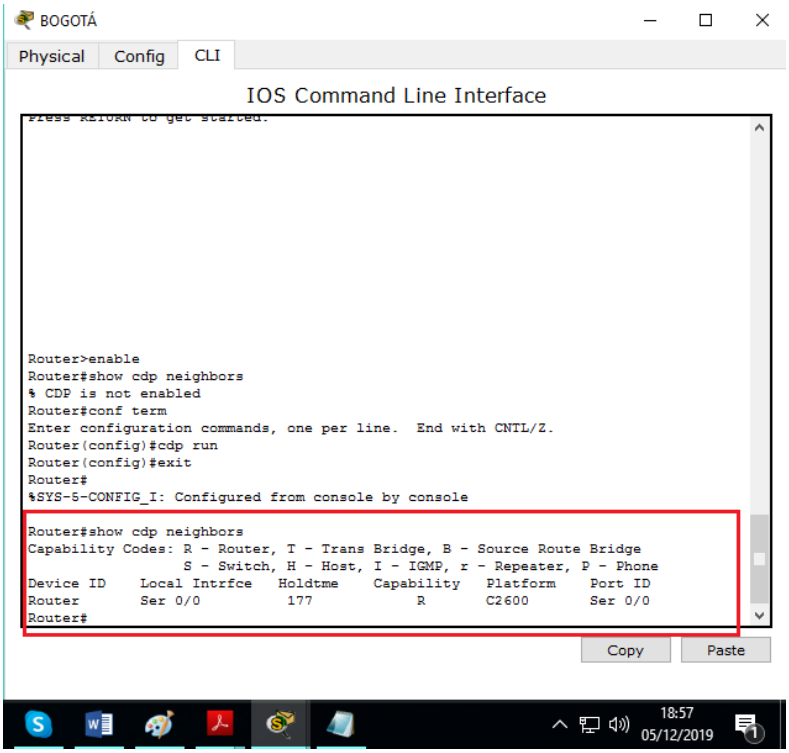

Figura 12. Verificación lista vecinos (Bogotá).

➢ **Router Cali (Antes)**

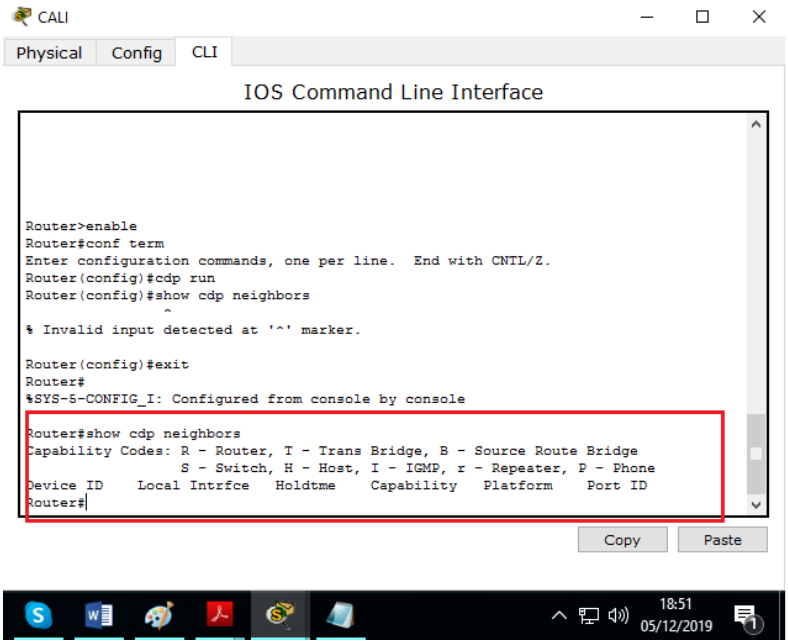

Figura 13. Vista vecinos (Cali).

➢ **Router Cali (Despúes)**

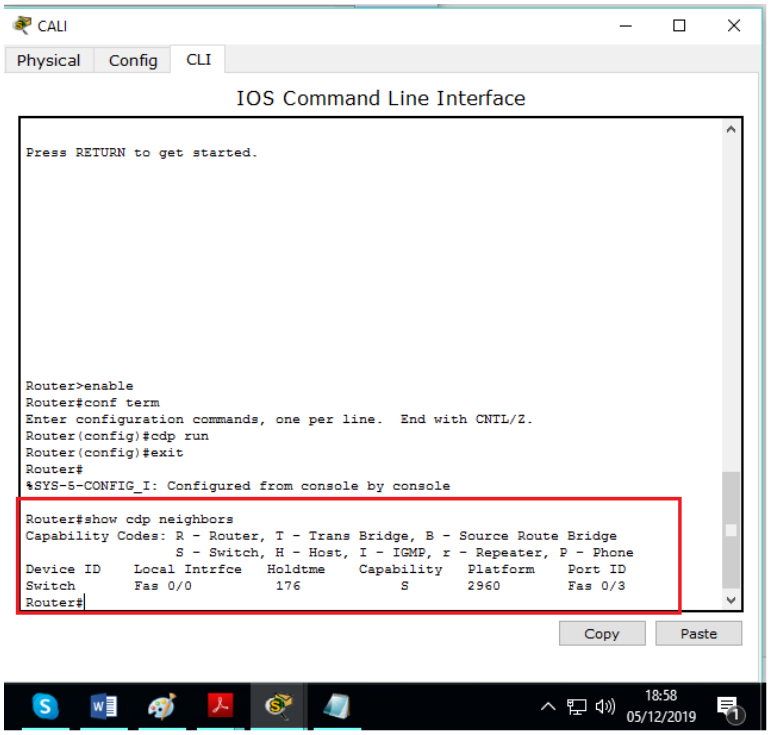

Figura 14. Verificación lista vecinos (Bogotá).

1.1.10. Balanceo de cargas

Este proceso se hace para los que poseen dos seriales conectados en el mismo Router, con diferentes opciones para llevar la carga. Para visualizar se usa el comando show ip route, que nos permite observar que no hay balanceo de carga.

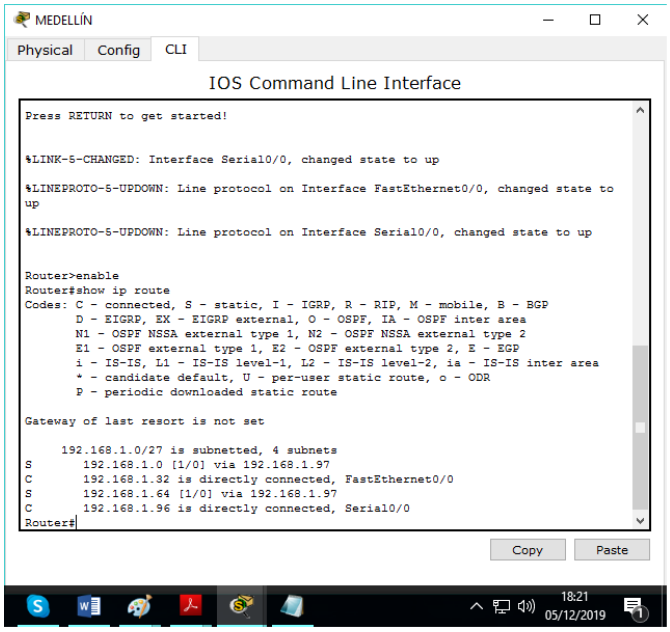

Figura 15. Verificación balanceo de cargas (Medellín).

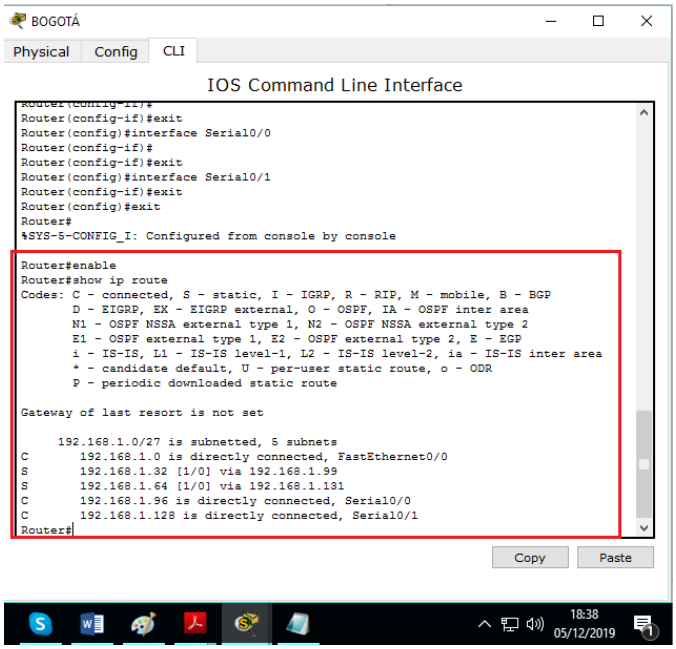

Figura 16. Verificación balanceo de cargas (Bogotá).

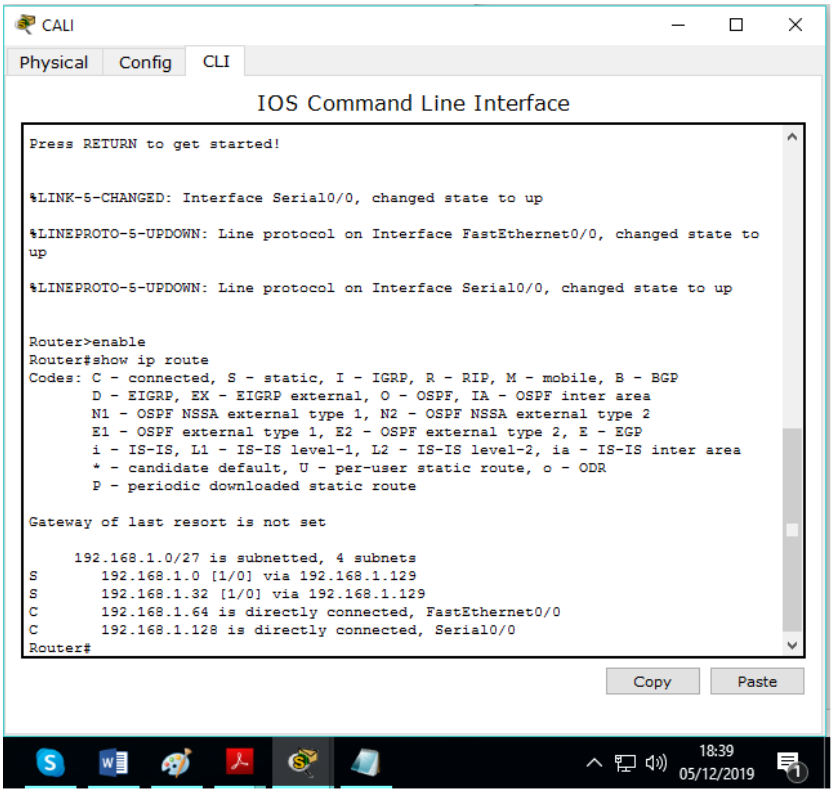

Figura 17. Verificación balanceo de cargas (Cali).

1.1.11. Configuración de enrutamiento.

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

1.1.11.1. Router Medellín

Router>enable

Router#conf term

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

Router(config)#router eigrp 200

Router(config-router)#network 192.168.1.96 0.0.0.31

Router(config-router)#network 192.168.1.32 0.0.0.31

Router(config-router)#network 192.168.1.128 0.0.0.31

Router(config-router)#

1.1.11.2. Router Bogotá

Router>enable

Router#configure term

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

Router(config)#router eigrp 200

Router(config-router)#network 192.168.1.0 0.0.0.31

Router(config-router)#network 192.168.1.96 0.0.0.31

Router(config-router)#

Router(config-router)#network 192.168.1.128 0.0.0.31

Router(config-router)#no auto-summary

Router(config-router)#

Router(config-router)#

Router#

1.1.11.3. Router Cali

Router>enable

Router#conf term

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

Router(config)#router eigrp 200

Router(config-router)#network 192.168.1.128 0.0.0.31

Router(config-router)#network 192.168.1.64 0.0.0.31

Router(config-router)#no auto-summary

1.1.12. Verificación de vecindad con los routers configurados con EIGRP.

Para esto tenemos los comandos

show ip eigrp neighbors

show ip eigrp topology

1.1.12.1. Router Medellín

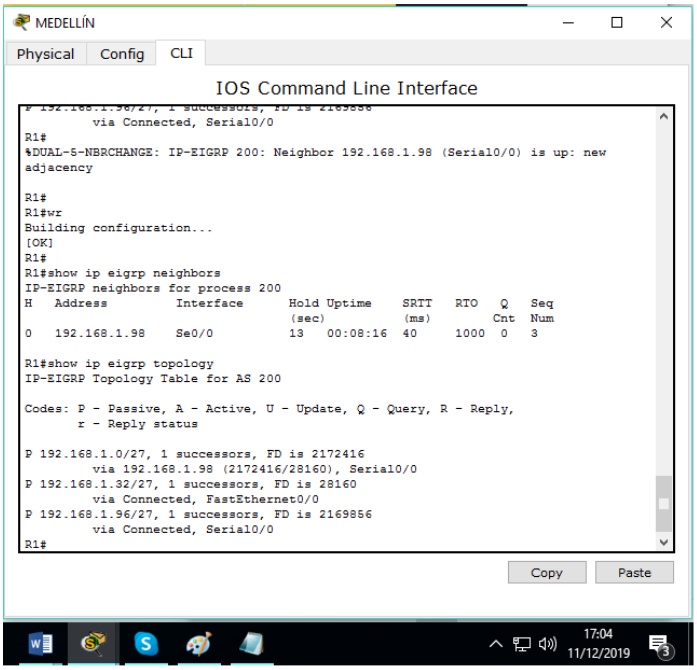

Figura 18. Verificación vecindad y EIGRP (Medellín).

1.1.12.2. Router Bogotá

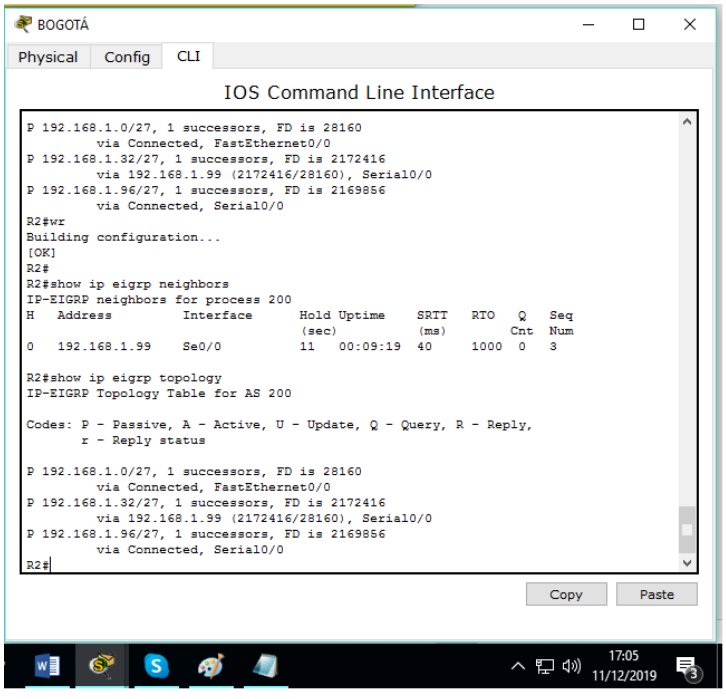

Figura 19. Verificación vecindad Y EIGRP (Bogotá).

1.1.12.3. Router Cali

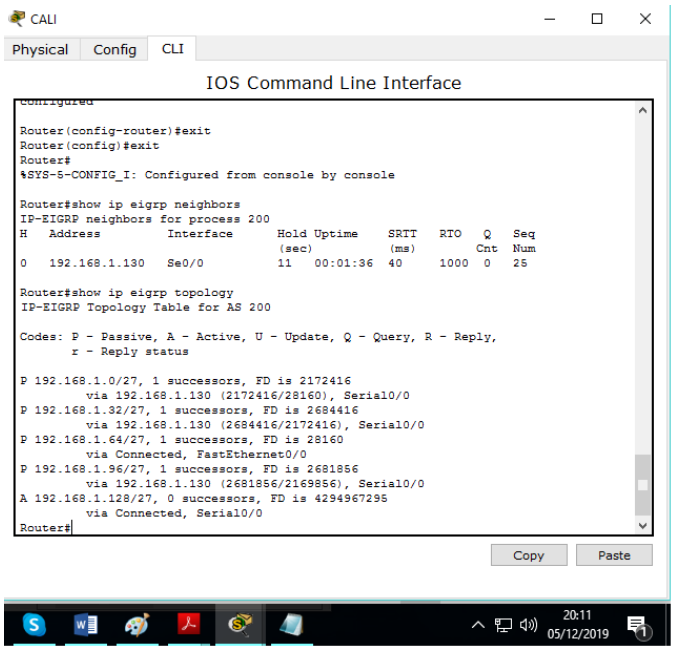

Figura 20. Verificación vecindad Y EIGRP (Cali).

1.1.13. Comprobación de las tablas de enrutamiento.

Para esto el comando indicado es show ip route

1.1.13.1. Router Medellín

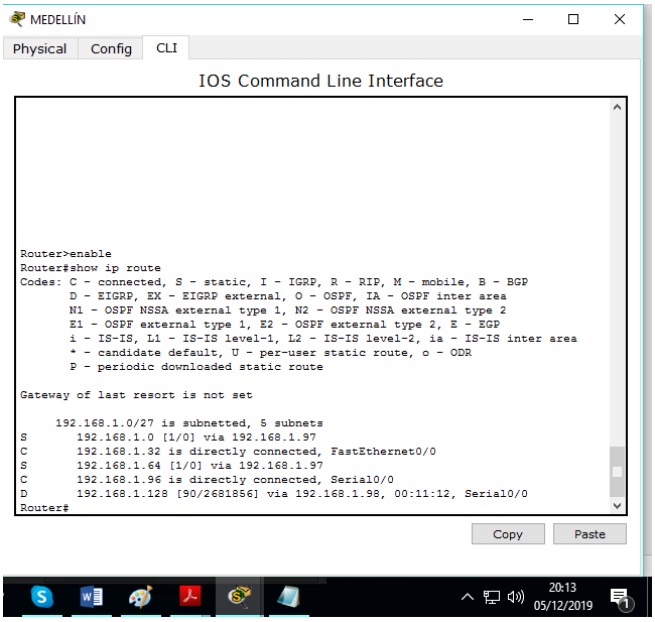

Figura 21. Tabla de enrutamiento (Medellín).

1.1.13.2. Router Bogotá

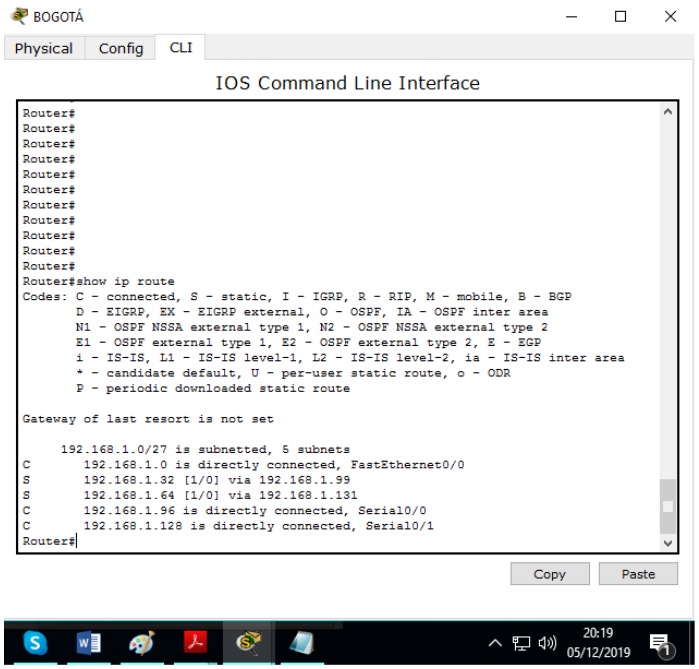

Figura 22. Tabla de enrutamiento (Bogotá).

1.1.13.3. Router Cali

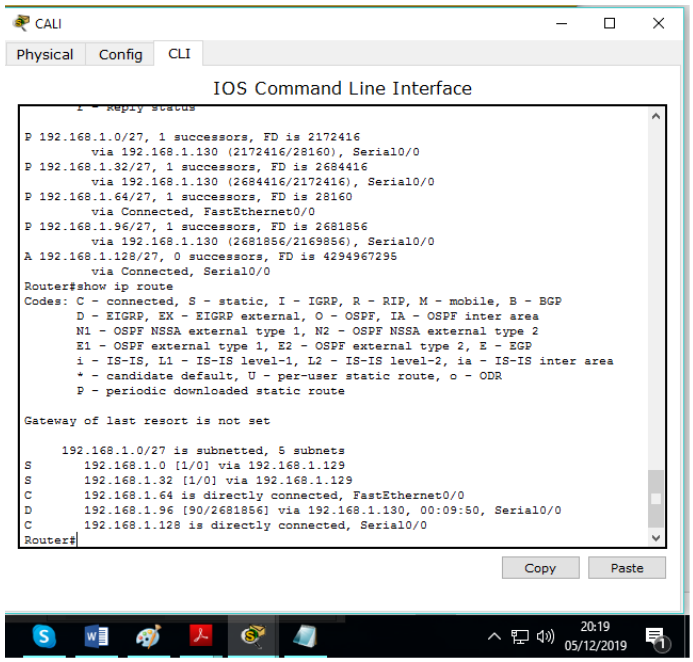

Figura 23. Tabla de enrutamiento (cali).

1.1.14. Diagnóstico de conectividad entre los puntos de la red.

1.1.14.1. Ping desde el PC del router Cali a PC router Medellín

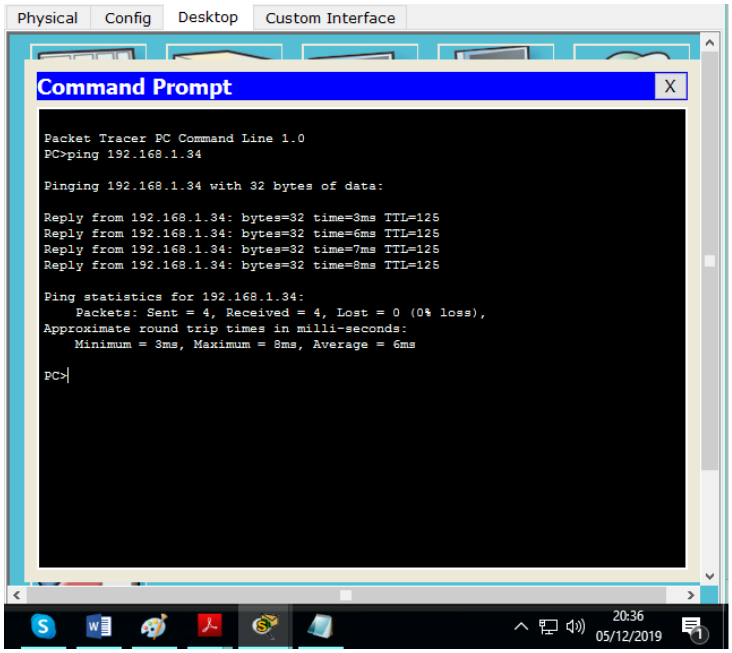

Figura 24. Conectividad Cali – Medellín.

1.1.14.2. Ping desde el PC del router Cali a PC router Bogotá (Servidor)

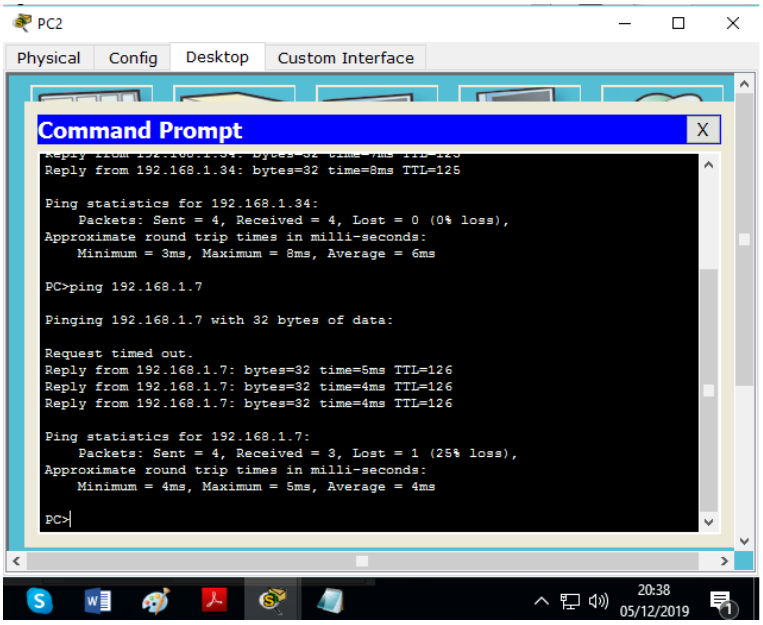

Figura 25. Conectividad Cali – Bogotá.

1.1.15. 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.

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

Como ya se había habilitado la configuración telnet con la línea vty podemos tener acceso a los routers, de igual forma podemos entrar a cualquier dispositivo de la red, por tal razón se a continuación se muestra evidencia de las conexiones.

1.1.15.1. Router Medellín a Cali

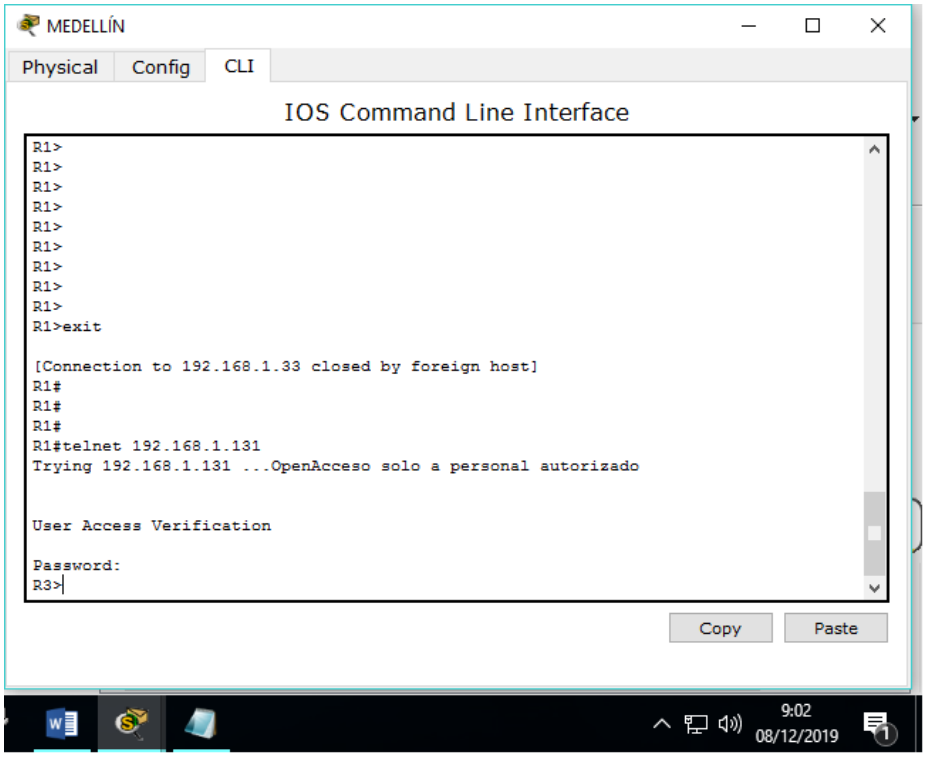

Figura 26. Conexión Telnet Medellín - Cali.

1.1.15.2. Router Bogotá a Cali

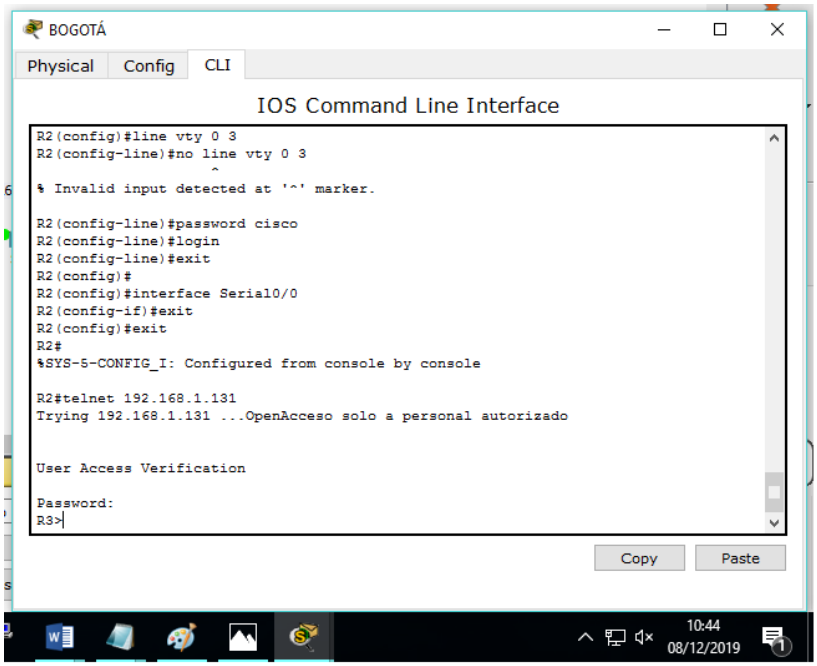

Figura 27. Conexión Telnet Cali – Bogotá.

1.1.15.3. Router Cali a Medellín

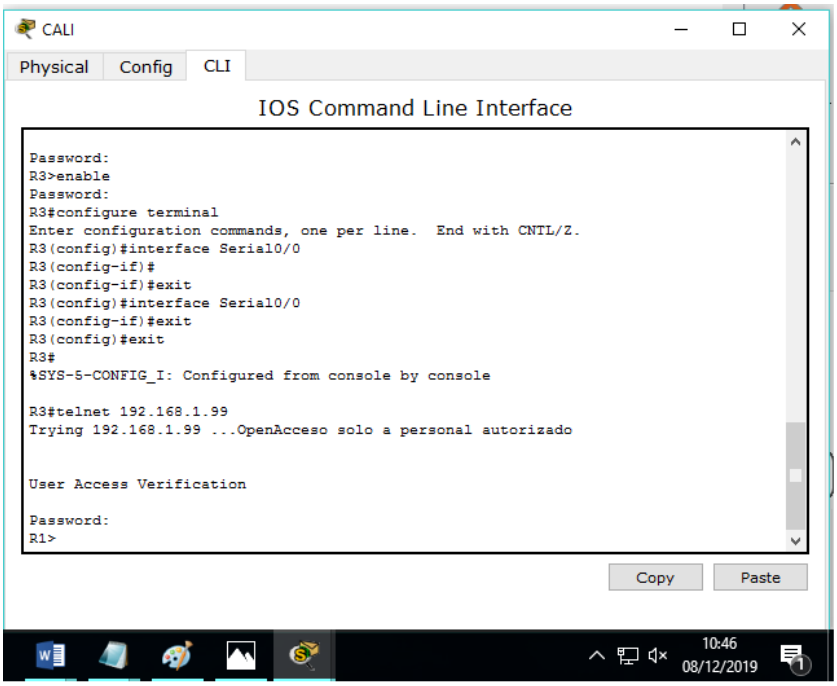

Figura 28. Conexión Telnet Cali – Medellín.

1.1.15.4. Router Cali a Bogotá

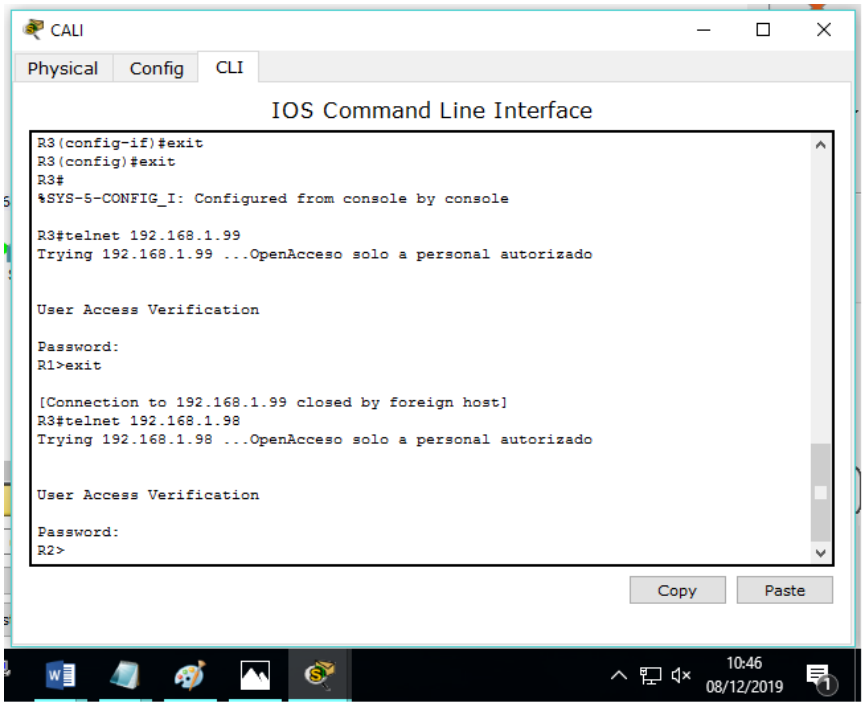

Figura 29. Conexión Telnet Cali – Bogotá.

1.1.15.5. Router Medellín a Bogotá

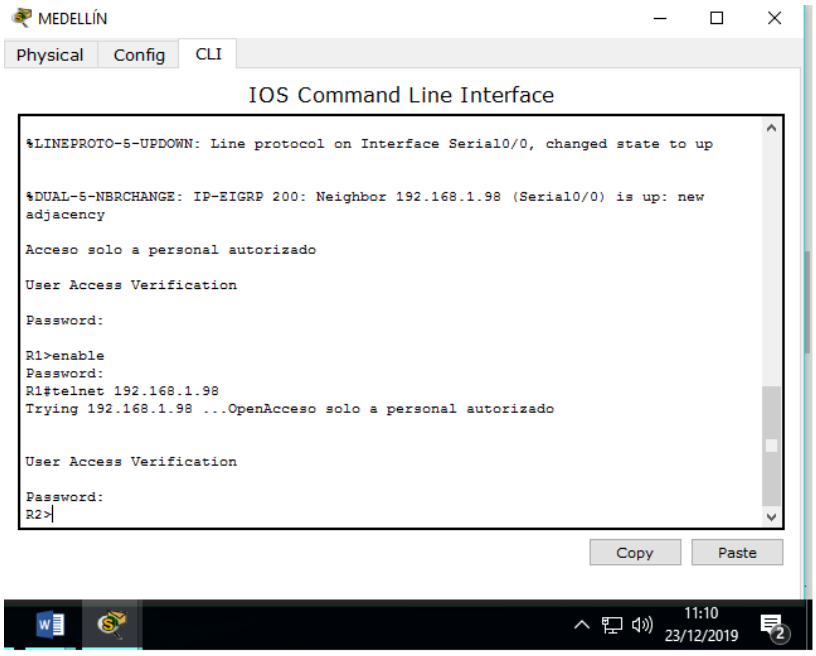

Figura 30. Conexión Telnet Medellín – Bogotá.

1.1.15.6. Router Bogotá Medellín

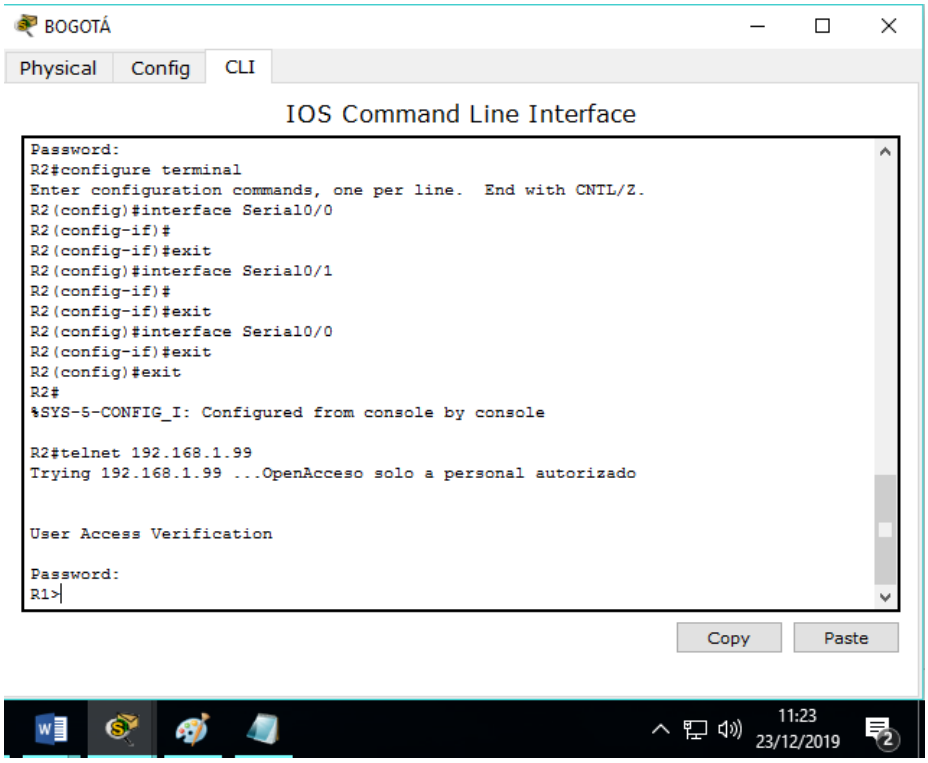

Figura 31. Conexión Telnet Bogotá - Medellín.

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.

Procedemos a realizar la configuración en el router de Bogotá:

R2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 deny 192.168.1.4
R2(config)#access-list 1 permit any
R2(config)#interface f 0/0
R2(config-if)#ip access-group 1 in
R2(config-if)#exit

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

Router Cali

R3#conf term

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

R3(config)#access-list 10 permit 192.168.1.7

R3(config)#access-list 10 deny 192.168.1.96 0.0.0.31

R3(config)#access-list 10 deny 192.168.1.4

R3(config)#int serial 0/0

R3(config-if)#ip access-group 10 in

R3(config-if)#exit

Para mostrar las listas de acceso utilizamos el comando “show access-lists” en cada router.

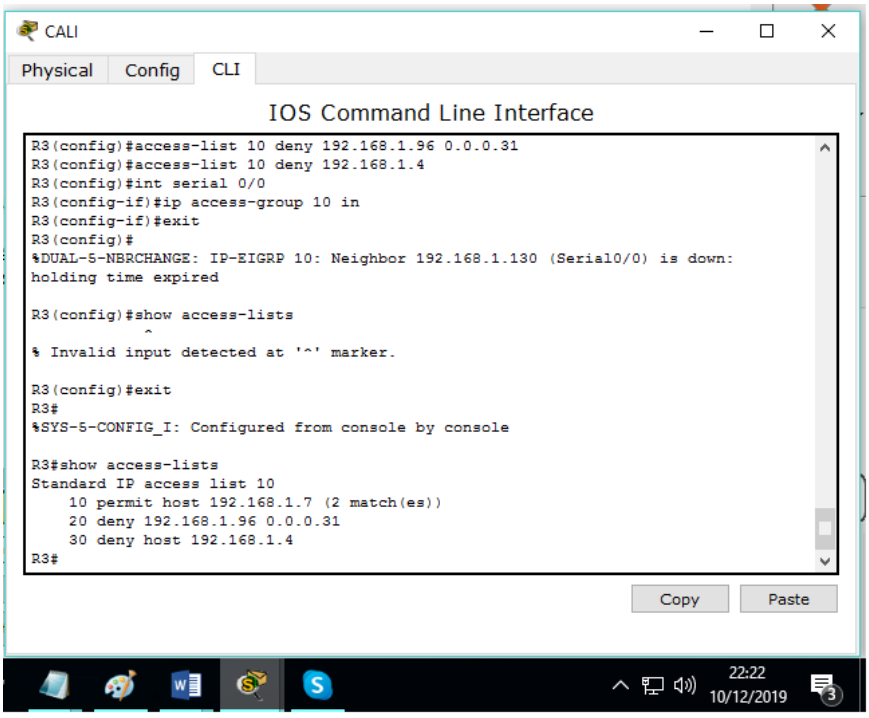

Figura 32. Lista ACL router Cali.

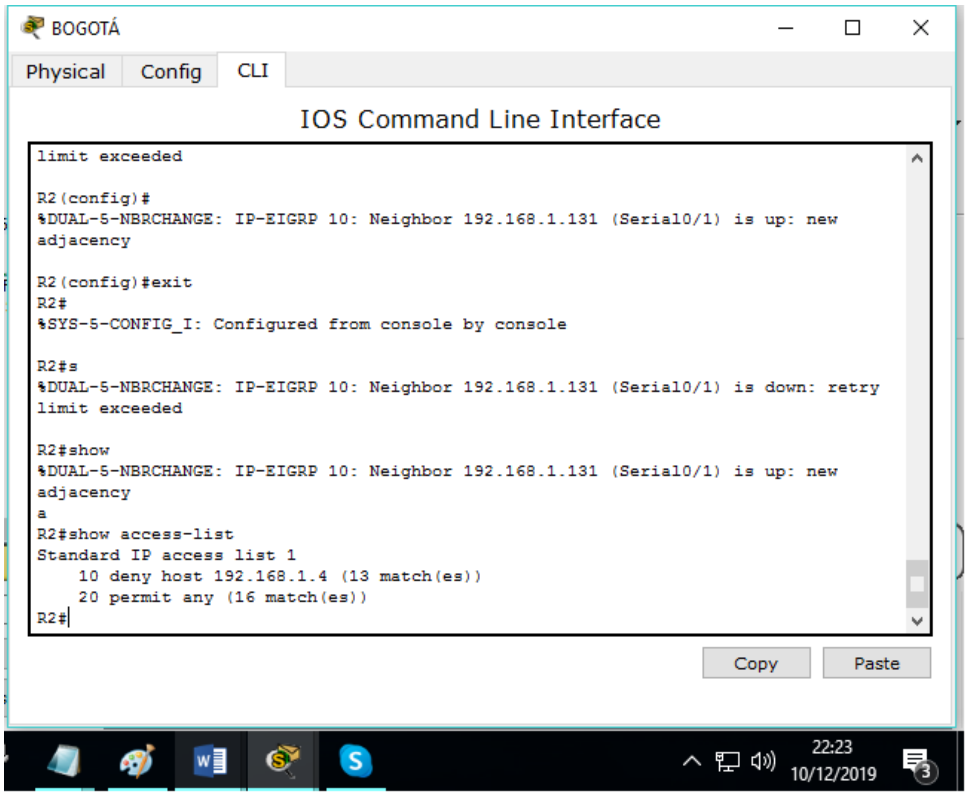

Figura 33. Lista ACL router Bogotá.

1.1.16. Comprobación de la red instalada.

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

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

	ORIGEN	DESTINO	RESULTADO
TELNET	**Router MEDELLIN**	**Router CALI**	Fallido
	WS_1	**Router BOGOTA**	Fallido
	Servidor	**Router CALI**	Exitoso
	Servidor	**Router MEDELLIN**	Exitoso
TELNET	**LAN del Router MEDELLIN**	**Router CALI**	Fallido
	LAN del Router CALI	**Router CALI**	Exitoso
	LAN del Router MEDELLIN	**Router MEDELLIN**	Exitoso

	LAN del Router CALI	**Router MEDELLIN**	Fallido
PING	**LAN del Router CALI**	**WS_1**	Fallido
	LAN del Router MEDELLIN	**WS_1**	Fallido
	LAN del Router MEDELLIN	**LAN del Router CALI**	Fallido
PING	**LAN del Router CALI**	**Servidor**	Exitoso
	LAN del Router MEDELLIN	**Servidor**	Exitoso
	Servidor	**LAN del Router MEDELLIN**	Exitoso
	Servidor	**LAN del Router CALI**	Exitoso
	Router CALI	**LAN del Router MEDELLIN**	Fallido
	Router MEDELLIN	**LAN del Router CALI**	Fallido

Tabla 2. Verificaciones listas de acceso.

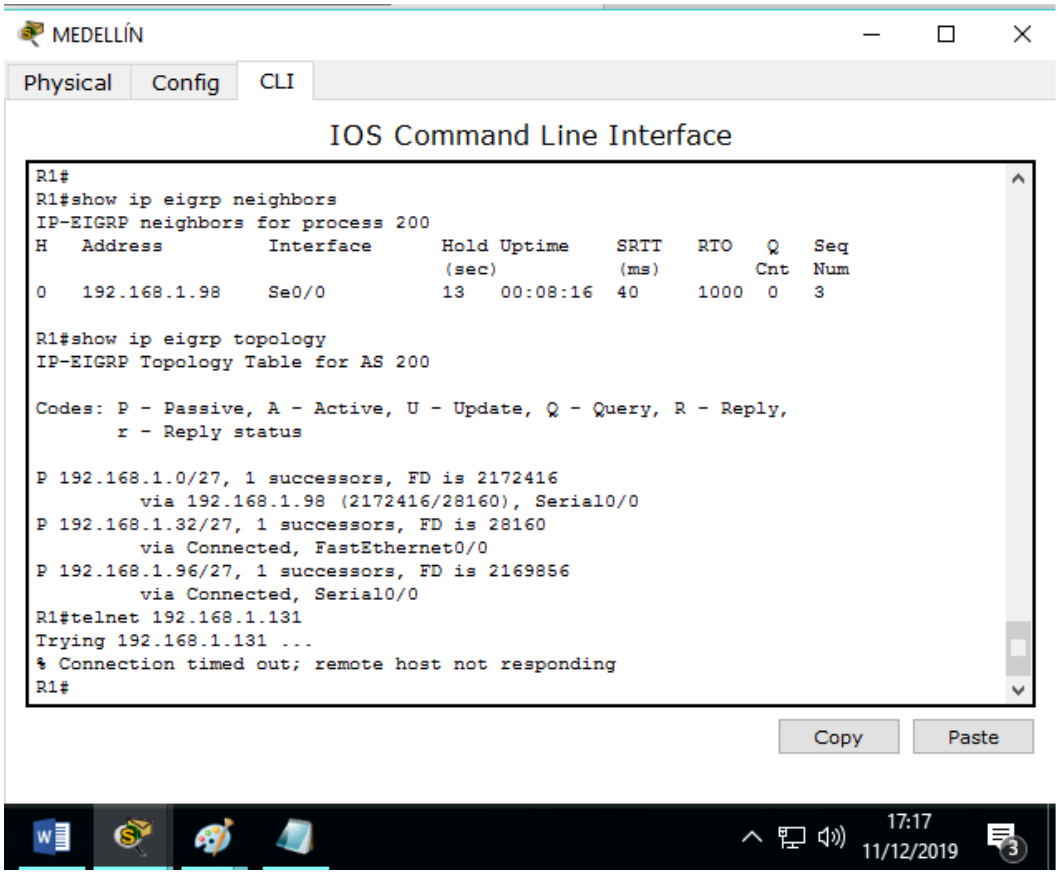

Figura 34. Telnet router Medellín Cali.

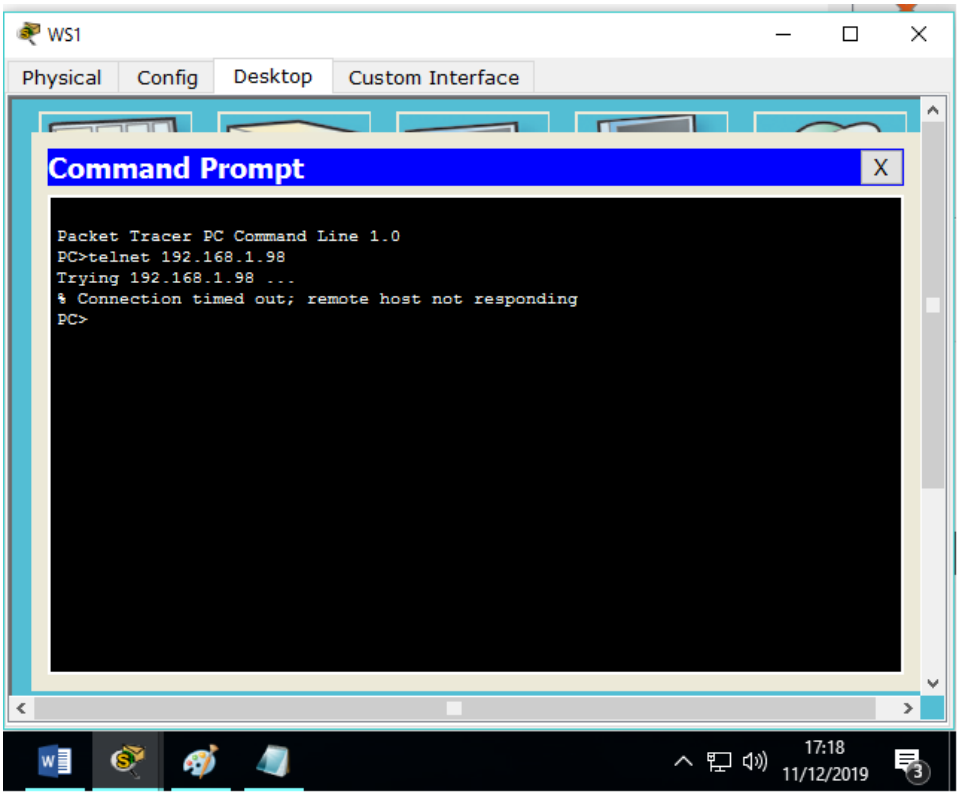

Figura 35. Telnet WS1 a router Bogotá.

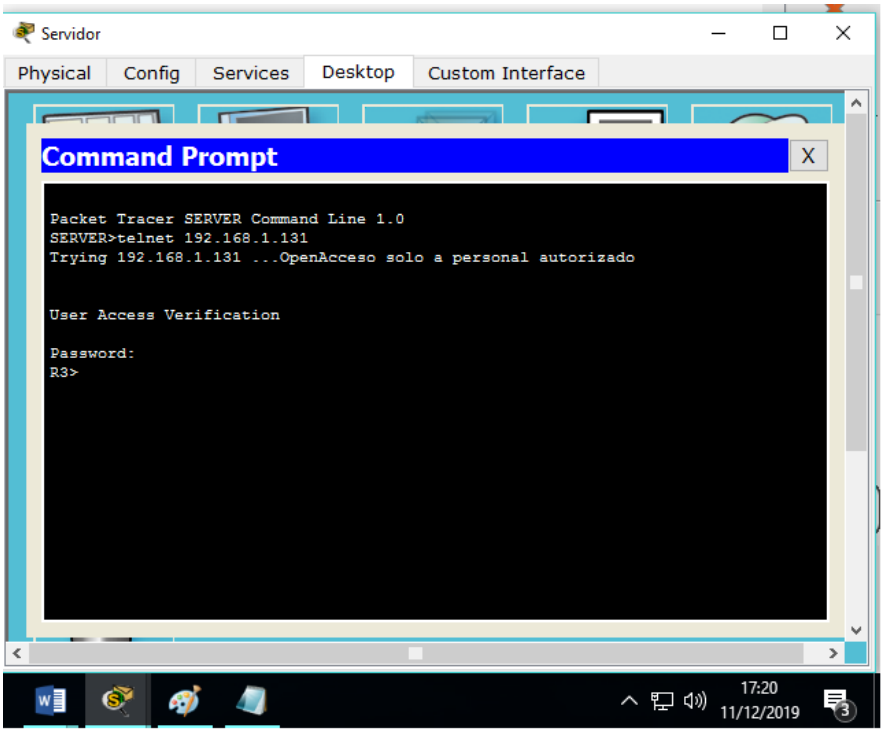

Figura 36. Telnet servidor a router Cali.

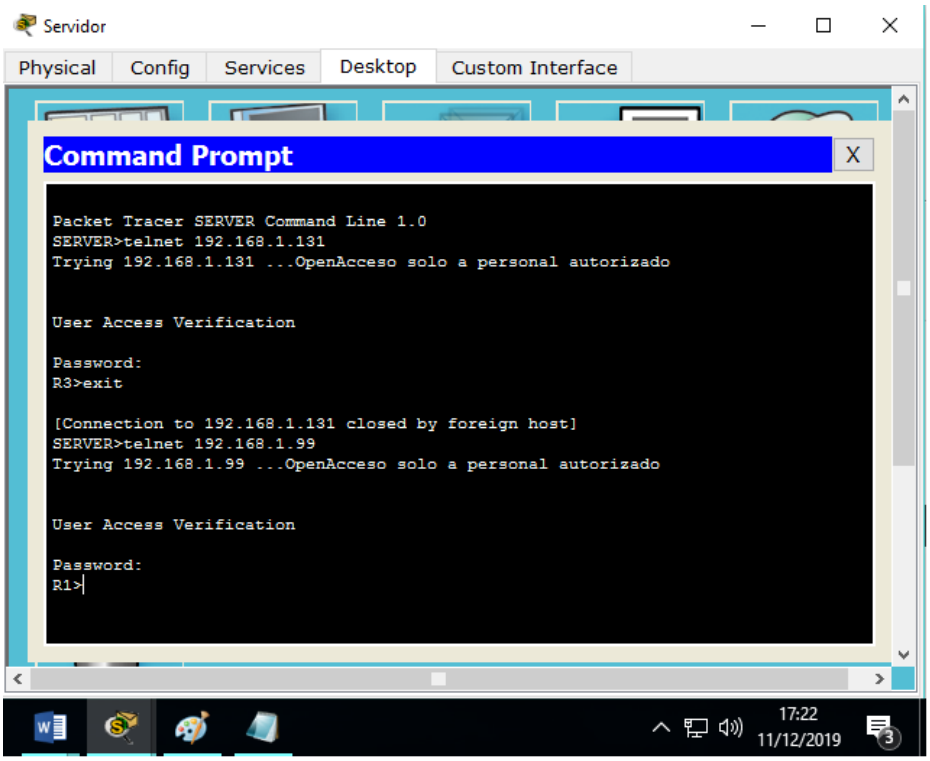

Figura 37. Telnet servidor a router Medellín.

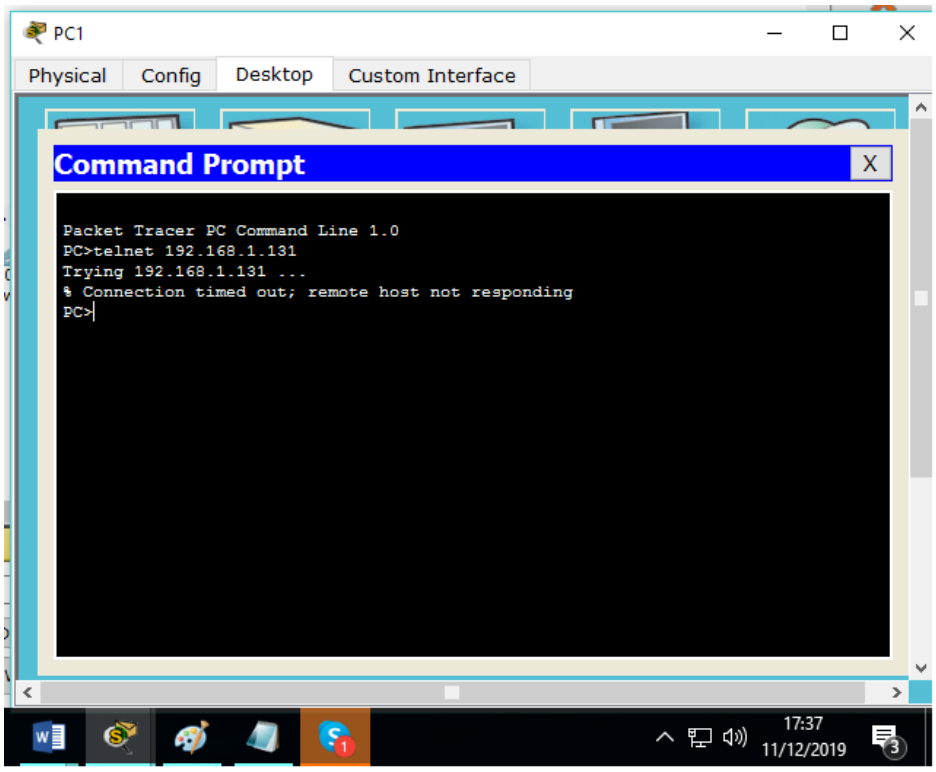

Figura 38. LAN del router Medellín a router Cali.

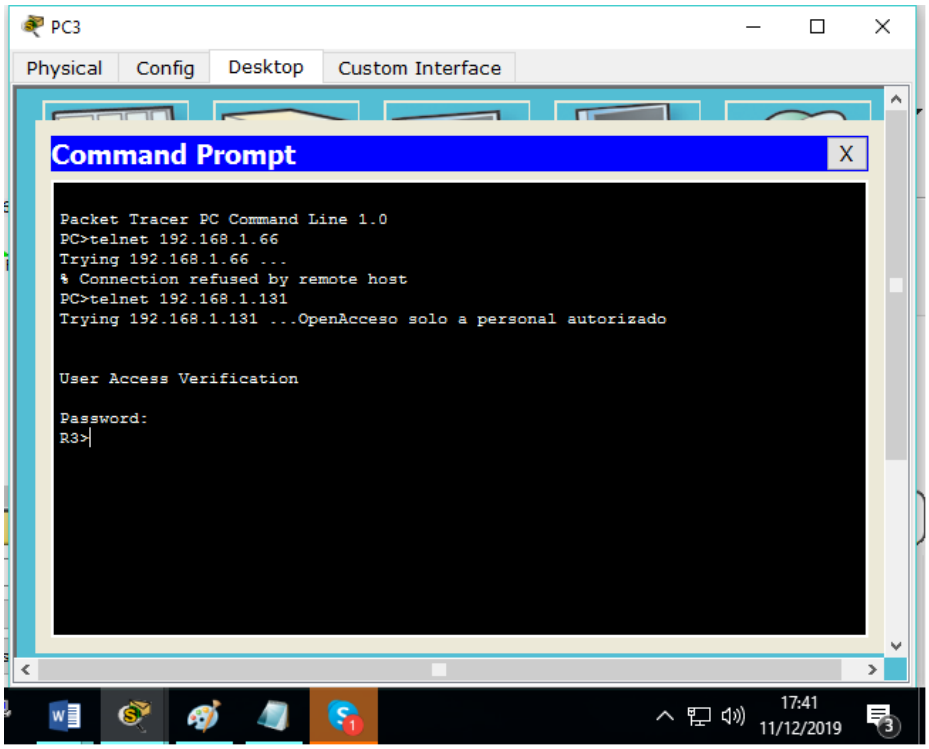

Figura 39. LAN del router Cali a router Cali.

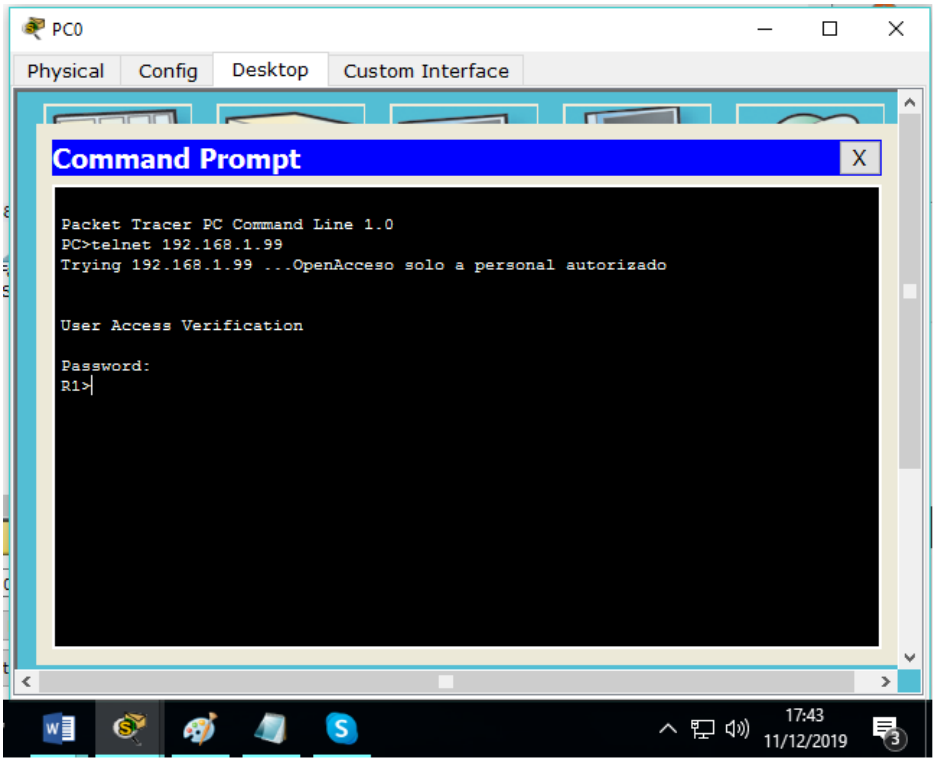

Figura 40. LAN del router Medellín a router Medellín.

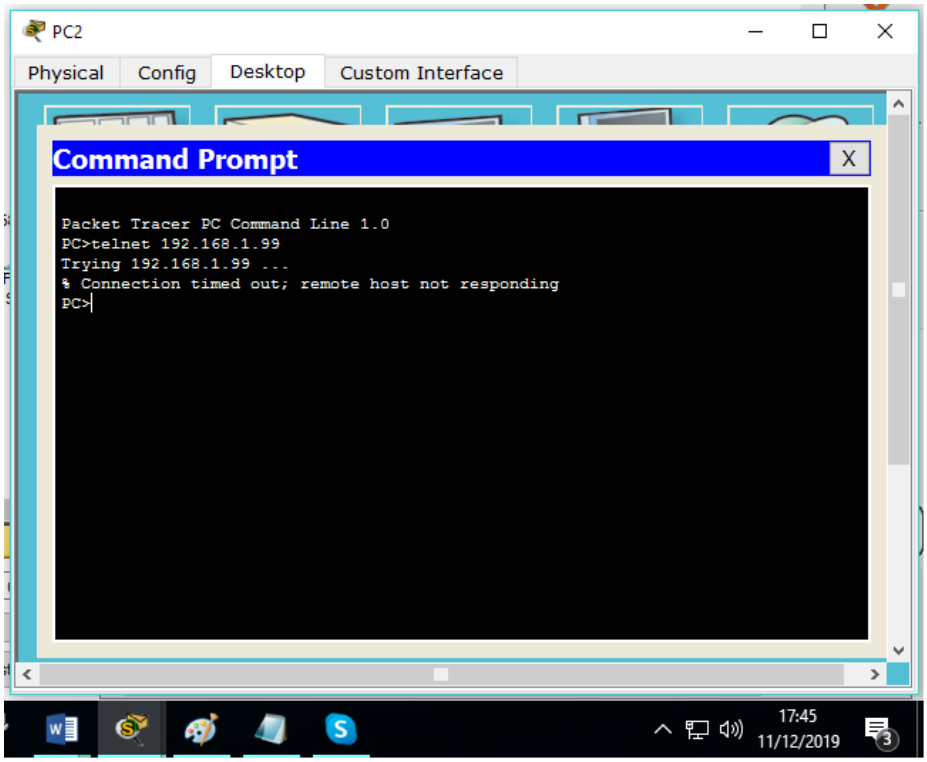

Figura 41. LAN del Router Cali a router Medellín.

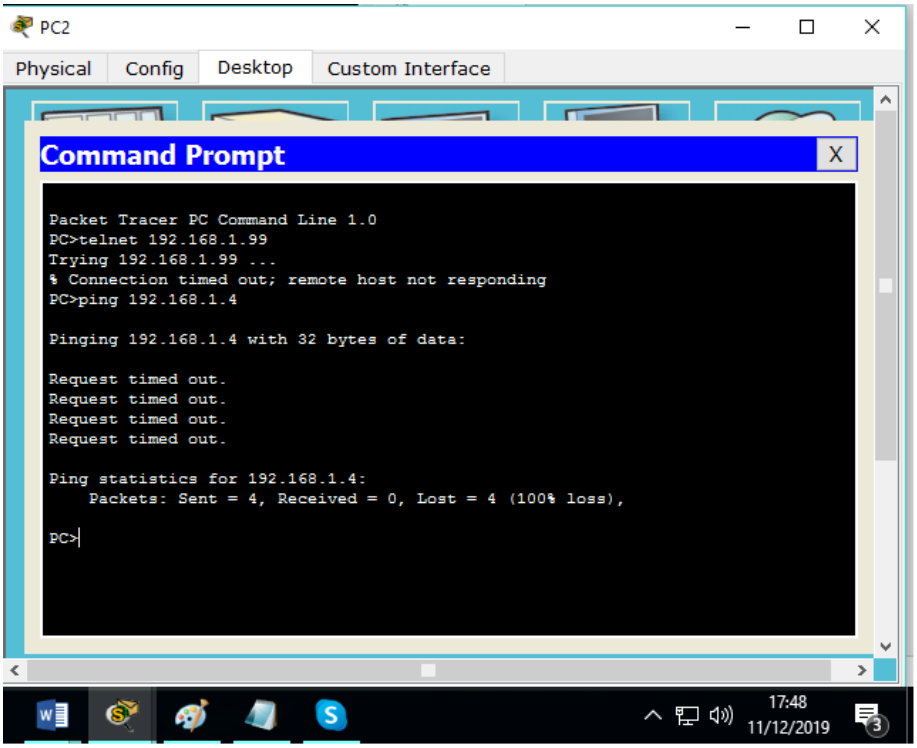

Figura 42. LAN del router Cali WS_1.

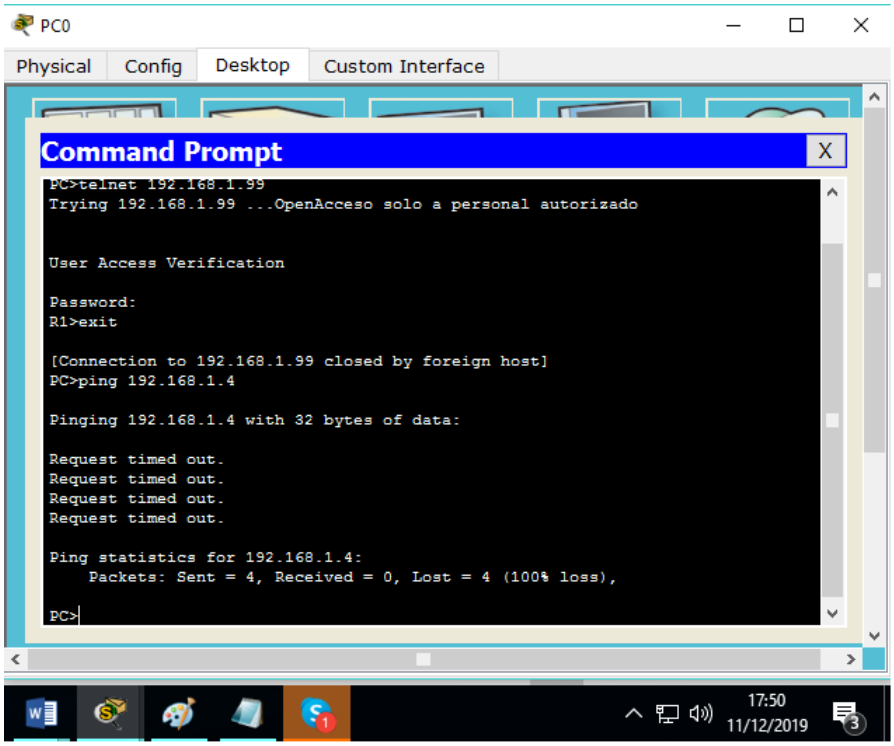

Figura 43. LAN del router Medellín WS_1.

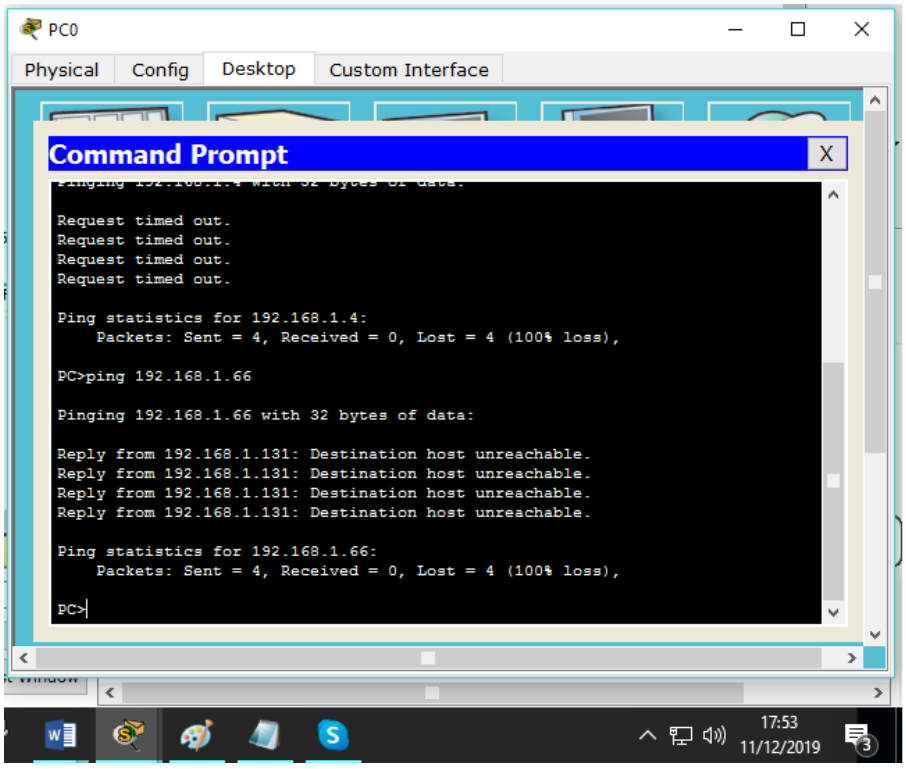

Figura 44. LAN del router a LAN router de Cali.

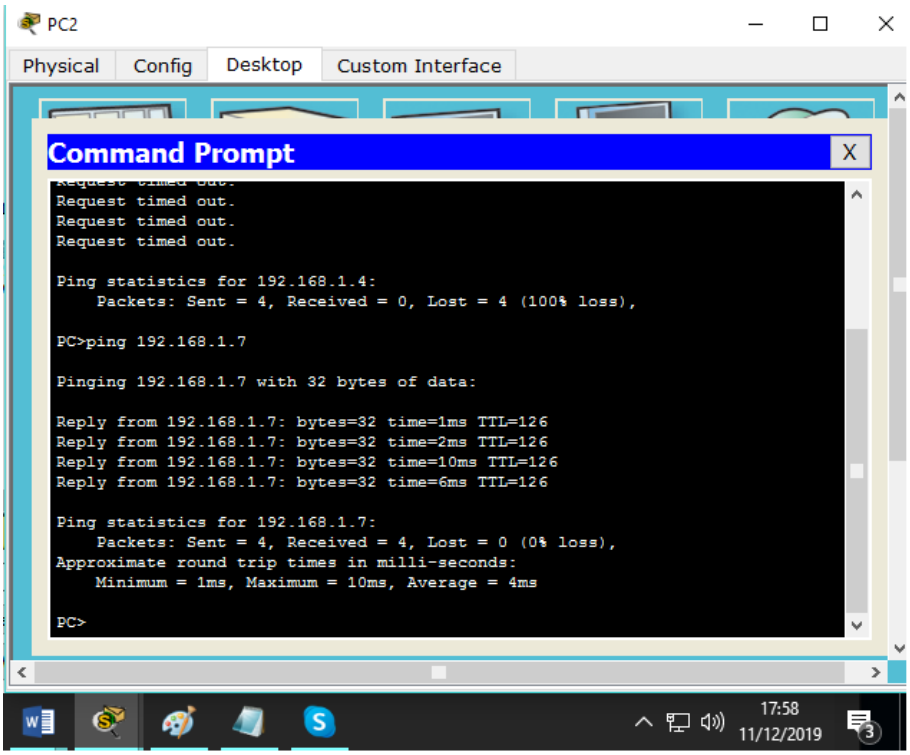

Figura 45. LAN del router Cali a Servidor.

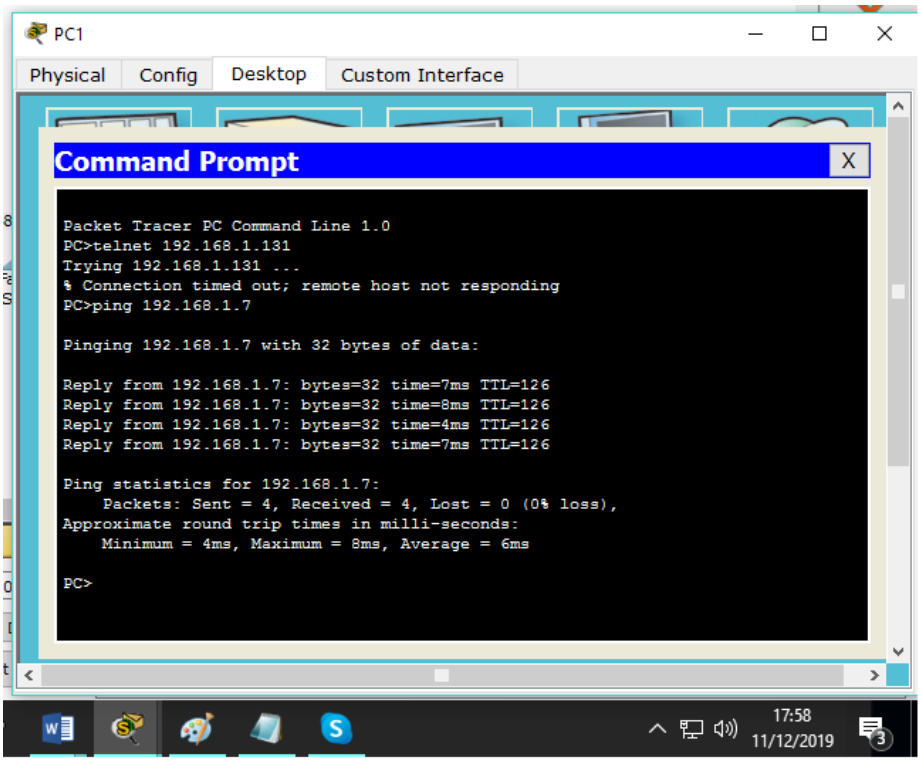

Figura 46. LAN del router Medellín a Servidor.

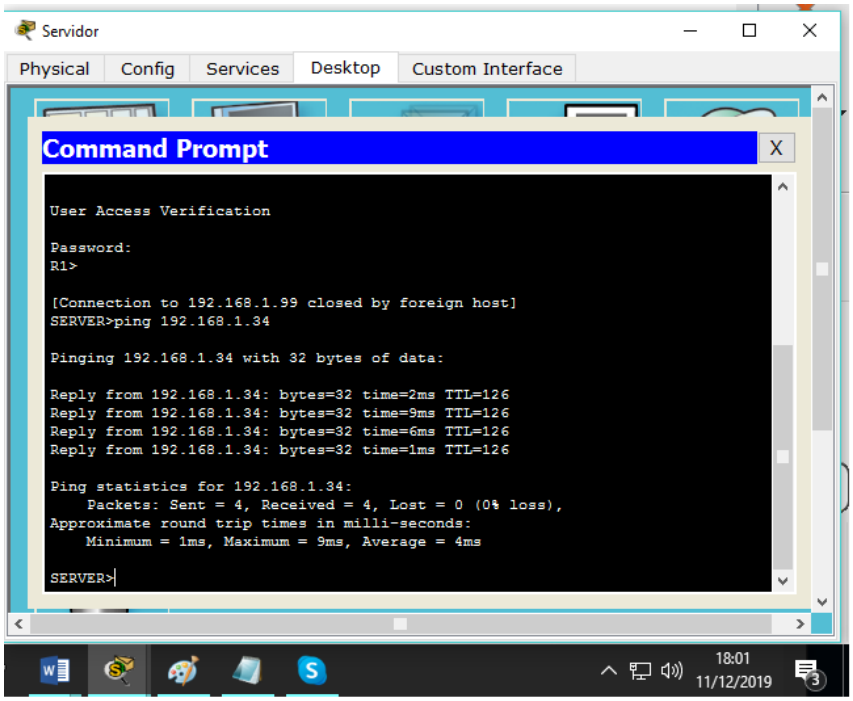

Figura 47. Servidor a LAN del router Medellín.

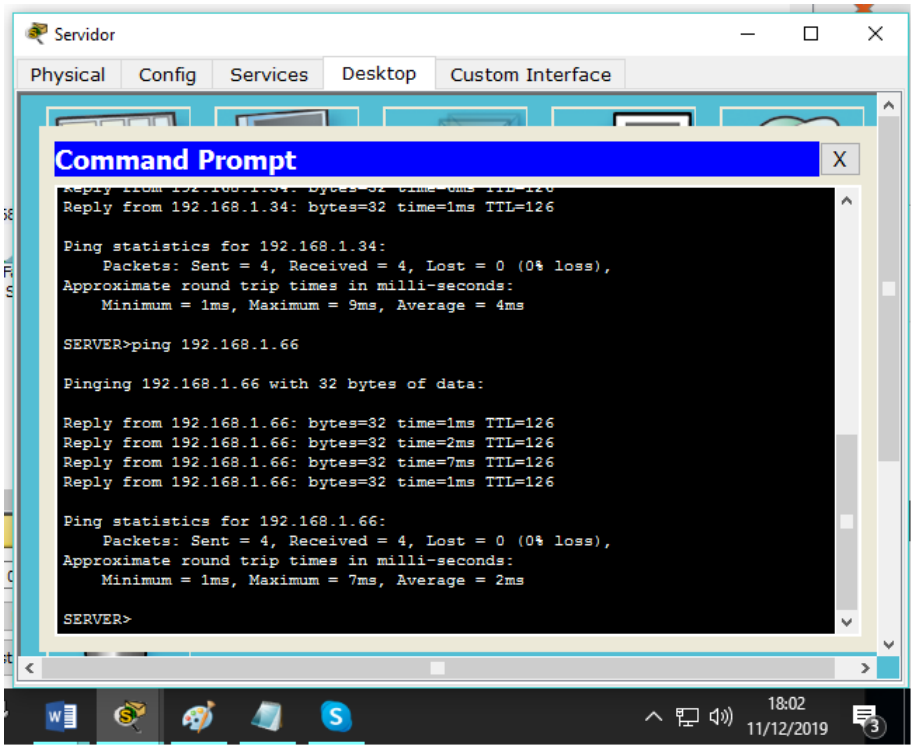

Figura 48. Servidor a LAN del router Cali.

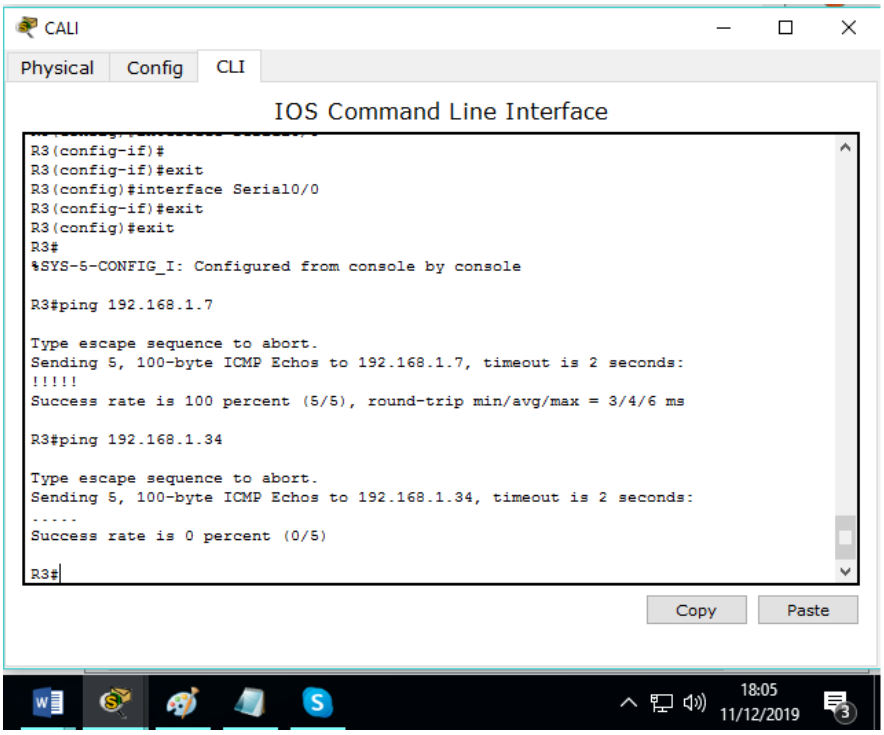

Figura 49. Router Cali a LAN del router Medellín.

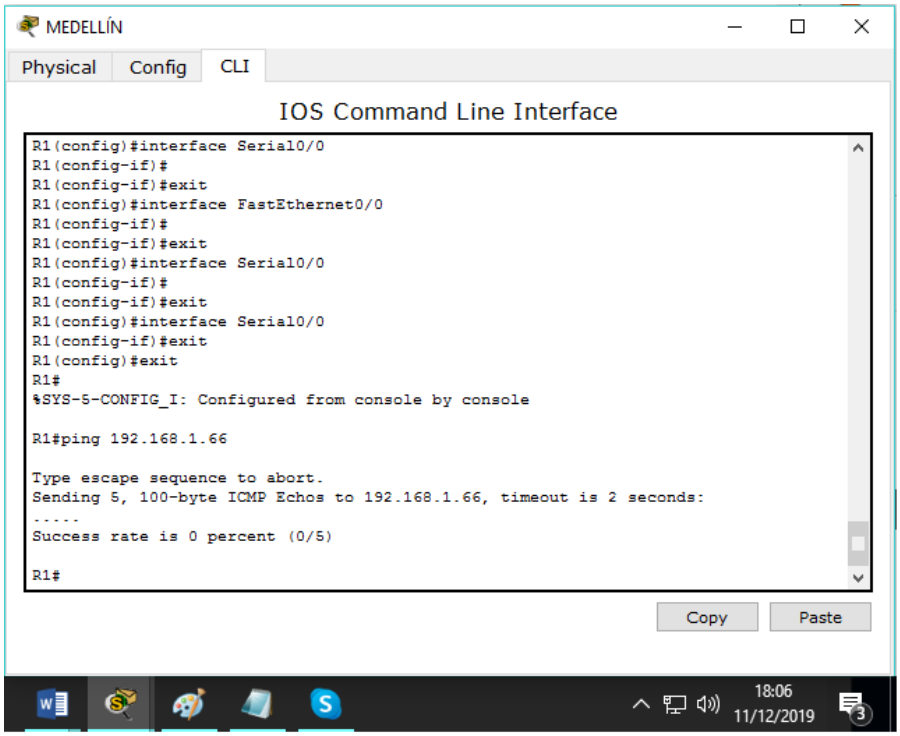

Figura 50. Router Medellín a LAN del router Cali.

1.2. ESCENARIO 2

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

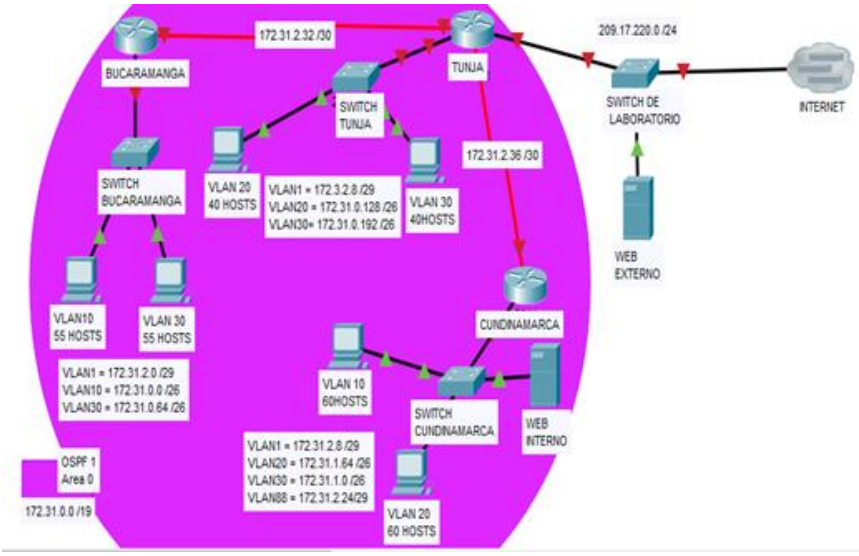

Figura 51. Topología escenario 2.

1.2.1. Configuraciones router Bucaramanga

1.2.1.1. Básicas

Router>enable

Router#config terminal

Router(config)#hostname RBucaramanga

RBucaramanga (config)#no ip domain-lookup

RBucaramanga (config)#enable secret cisco

RBucaramanga (config)#line console 0

RBucaramanga (config-line)#password cisco

RBucaramanga (config-line)#login

RBucaramanga (config)#line vty 0 4

RBucaramanga (config-line)#password cisco

RBucaramanga (config-line)#login

RBucaramanga (config-line)#exit

RBucaramanga (config)#service password-encryption

RBucaramanga (config)#banner motd #Prohibido el acceso no autorizado!#

RBucaramanga (config)#exit

RBucaramanga #copy running-config startup-config

1.2.1.2. Interfaces y seriales

RBucaramanga (config)#int serial 0/0/0

RBucaramanga (config-if)# ip add 172.31.2.34 255.255.255.252

RBucaramanga (config-if)#no shutdown

RBucaramanga (config-if)#exit

RBucaramanga(config)#int g0/0.1

RBucaramanga(config-subif)#encapsulation dot1q 1

RBucaramanga(config-subif)#ip add 172.31.2.1 255.255.255.248

RBucaramanga(config-subif)#int g0/0.10

RBucaramanga(config-subif)#encapsulation dot1q 10

RBucaramanga(config-subif)#ip add 172.31.0.1 255.255.255.192

RBucaramanga(config-subif)#int g0/0.30

RBucaramanga(config-subif)#encapsulation dot1q 30

RBucaramanga(config-subif)#ip add 172.31.0.65 255.255.255.192

RBucaramanga(config-subif)#int g0/0

RBucaramanga(config-if)#no shutdown

RBucaramanga (config-if)# int serial 0/0/0

RBucaramanga(config-if)#ip address 172.31.2.34 255.255.255.252

RBucaramanga(config-if)#no shutdown

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

1.2.1.3. Autenticación AAA

RBucaramanga(config)#username ubucaramanga secret cisco
RBucaramanga(config)#aaa new-model
RBucaramanga(config)#aaa authentication login AAA-LOGIN local
RBucaramanga(config)#line console 0
RBucaramanga(config-line)#login authentication AAA-LOGIN
RBucaramanga(config-line)#line vty 0 4
RBucaramanga(config-line)#login authentication AAA-LOGIN

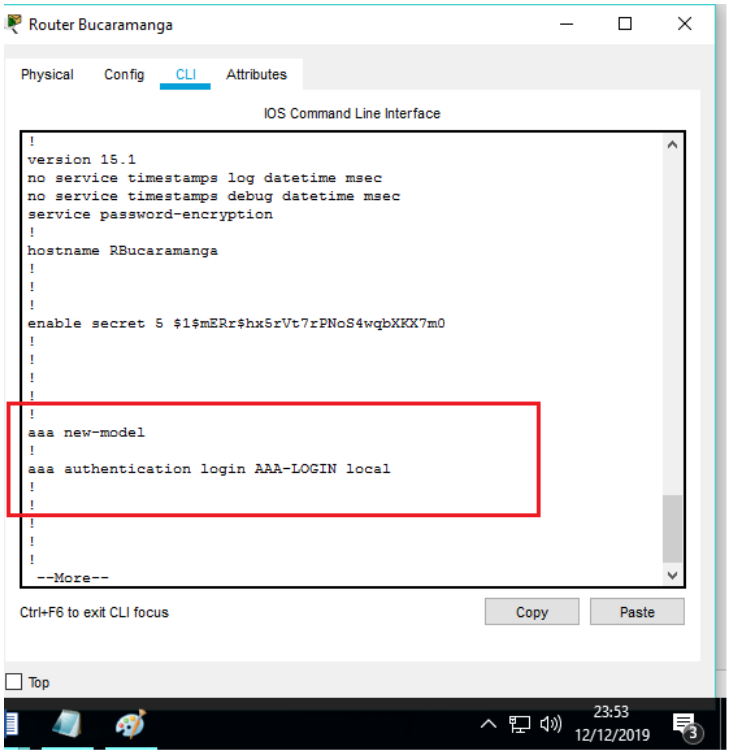

Figura 52. Verificación autenticación AAA router Bucaramanga.

1.2.1.4. Número de internos y tiempo máximo al detectar ataques.

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

1.2.2. Configuraciones router Tunja

1.2.2.1. Básicas

Router>enable
Router#config terminal
Router(config)#hostname RTunja
RTunja (config)#enable secret cisco
RTunja (config)#no ip domain-lookup
RTunja (config)#line console 0
RTunja (config-line)#password cisco
RTunja (config-line)#login
RTunja (config-line)#exit
RTunja (config)#line vty 0 4
RTunja(config-line)#password cisco
RTunja(config-line)#login
RTunja (config-line)#exit
RTunja (config)#banner motd #Prohibido el acceso no autorizado!#
RTunja (config)#exit
RTunja #copy running-config startup-config

1.2.2.2. Interfaces y seriales

RTunja (config)#int serial 0/0/0
RTunja (config-if)# ip add 172.31.2.33 255.255.255.252
RTunja (config-if)#no shutdown
RTunja (config-if)#exit

```
RTunja (config)#int serial 0/0/1
RTunja(config-if)#ip address 172.31.2.37 255.255.255.252
RTunja (config-if)#no shutdown
RTunja (config-if)#exit

RTunja(config)#int g0/0.1
RTunja(config-subif)#encapsulation dot1q 1
RTunja(config-subif)#ip address 172.3.2.9 255.255.255.248
RTunja(config-subif)#int g0/0.20
RTunja(config-subif)#encapsulation dot1q 20
RTunja(config-subif)#ip address 172.31.0.129 255.255.255.192
RTunja(config-subif)#int g0/0.30
RTunja(config-subif)#encapsulation dot1q 30
RTunja(config-subif)#ip address 172.31.0.193 255.255.255.192
RTunja(config-subif)#int g0/0
RTunja(config-if)#no shutdown
RTunja(config-if)#exit
RTunja (config)#int g0/1
RTunja(config-if)#ip address 209.165.220.1 255.255.255.0
RTunja (config-if)#no shutdown

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
```

1.2.2.3. Autenticación AAA

RTunja(config)#username utunja secret cisco

RTunja(config)#aaa new-model

RTunja(config)#aaa authentication login AAA-LOGIN local

RTunja(config)#line console 0

RTunja(config-line)#login authentication AAA-LOGIN

RTunja(config-line)#line vty 0 4

RTunja(config-line)#login authentication AAA-LOGIN

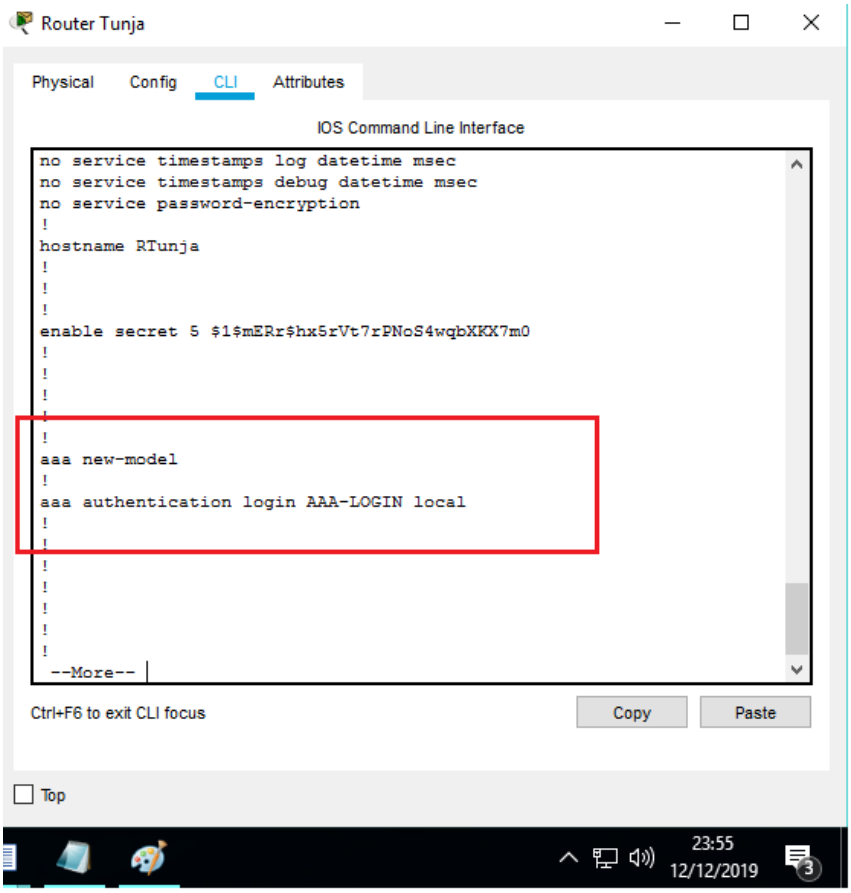

Figura 53. Verificación autenticación AAA router Tunja.

1.2.2.4. Número de intentos y tiempo máximo al detectar ataques.

RTunja(config-line)#login block-for 10 attempts 4 within 60

1.2.3. Configuraciones del router Cundinamarca

1.2.3.1. Básicas

```
Router>enable
Router#config terminal
Router(config)#hostname RCundinamarca
RCundinamarca (config)#enable secret cisco
RCundinamarca (config)#service password-encryption
RCundinamarca (config)#no ip domain-lookup
RCundinamarca (config)#line console 0
RCundinamarca (config-line)#password cisco
RCundinamarca (config-line)#login
RCundinamarca (config)#line vty 0 4
RCundinamarca (config-line)#password cisco
RCundinamarca (config-line)#login
RCundinamarca (config-line)#exit
RCundinamarca (config)#banner motd #Prohibido el acceso no autorizado!#
RCundinamarca (config)#exit
RCundinamarca #copy running-config startup-config
```

1.2.3.2. Interfaces y seriales

```
RCundinamarca(config)#int g0/0.1
RCundinamarca(config-subif)#encapsulation dot1q 1
RCundinamarca(config-subif)#ip address 172.31.2.9 255.255.255.248
RCundinamarca(config-subif)#int g0/0.20
RCundinamarca(config-subif)#encapsulation dot1q 20
RCundinamarca(config-subif)#ip address 172.31.1.65 255.255.255.192
RCundinamarca(config-subif)#int g0/0.30
RCundinamarca(config-subif)#encapsulation dot1q 30
```

```
RCundinamarca(config-subif)#ip address 172.31.1.1 255.255.255.192
RCundinamarca(config-subif)#int g0/0.88
RCundinamarca(config-subif)#encapsulation dot1q 88
RCundinamarca(config-subif)#ip address 172.31.2.25 255.255.255.248
RCundinamarca(config-subif)#int g0/0
RCundinamarca(config-if)#no shutdown
RCundinamarca(config-if)#int s0/0/0
RCundinamarca(config-if)#ip address 172.31.2.38 255.255.255.252
RCundinamarca(config-if)#no shutdown

RCundinamarca(config)#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
```

1.2.3.3. Autenticación AAA

```
RCundinamarca(config)#username ucundinamarca secret cisco
RCundinamarca(config)#aaa new-model
RCundinamarca(config)#aaa authentication login AAA-LOGIN local
RCundinamarca(config)#line console 0
RCundinamarca(config-line)#login authentication AAA-LOGIN
RCundinamarca(config-line)#line vty 0 4
RCundinamarca(config-line)#login authentication AAA-LOGIN
```

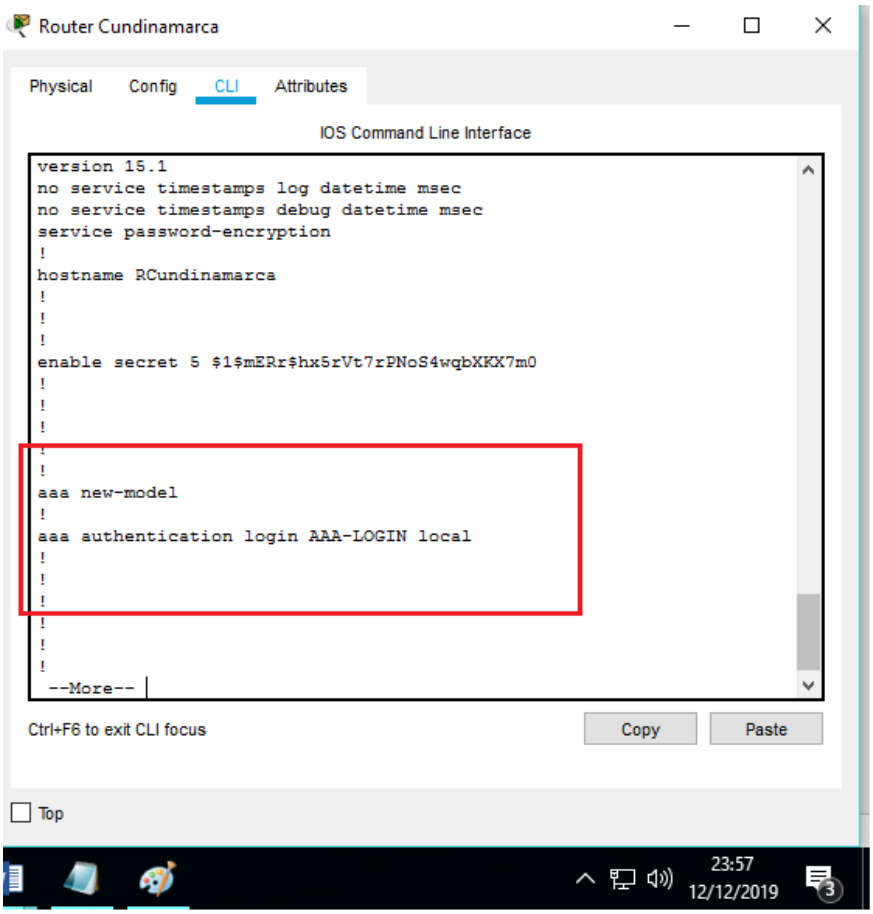

Figura 54. Verificación autenticación AAA router Cundinamarca.

1.2.3.4. Numero de intentos y tiempo máximo al detectar ataque

RCundinamarca(config-line)#login block-for 10 attempts 4 within 60

1.2.4. Configuraciones del switch Bucaramanga

1.2.4.1. Básicas

Switch>enable

Switch#conf term

Switch(config)#hostname SBucaramanga

SBucaramanga (config)#enable password cisco

SBucaramanga (config)#line console 0

SBucaramanga (config-line)# exec-timeout 6 0

SBucaramanga (config-line)# logging synchronous

SBucaramanga (config-line)#password cisco

SBucaramanga (config-line)#login

SBucaramanga (config-line)#line vty 0 15

SBucaramanga (config-line)# exec-timeout 6 0

SBucaramanga (config-line)# logging synchronous

SBucaramanga (config-line)#password cisco

SBucaramanga (config-line)#login

SBucaramanga (config-line)#exit

SBucaramanga (config)#exit

SBucaramanga #copy running-config startup-config

1.2.4.2. Vlans switch

SBucaramanga(config)#vlan 1

SBucaramanga(config-vlan)#vlan 10

SBucaramanga(config-vlan)#vlan 30

SBucaramanga(config-vlan)#int f0/10

SBucaramanga(config-if)#switchport mode access

SBucaramanga(config-if)#switchport access vlan 10

SBucaramanga(config-if)#int f0/14

SBucaramanga(config-if)#switchport mode access

SBucaramanga(config-if)#switchport access vlan 30

SBucaramanga(config-if)#int g0/1

SBucaramanga(config-if)#switchport mode trunk

SBucaramanga(config-if)#int vlan 1

SBucaramanga(config-if)#ip address 172.31.2.3 255.255.255.248

SBucaramanga(config-if)#no shutdown

SBucaramanga(config-if)#ip default-gateway 172.31.2.1

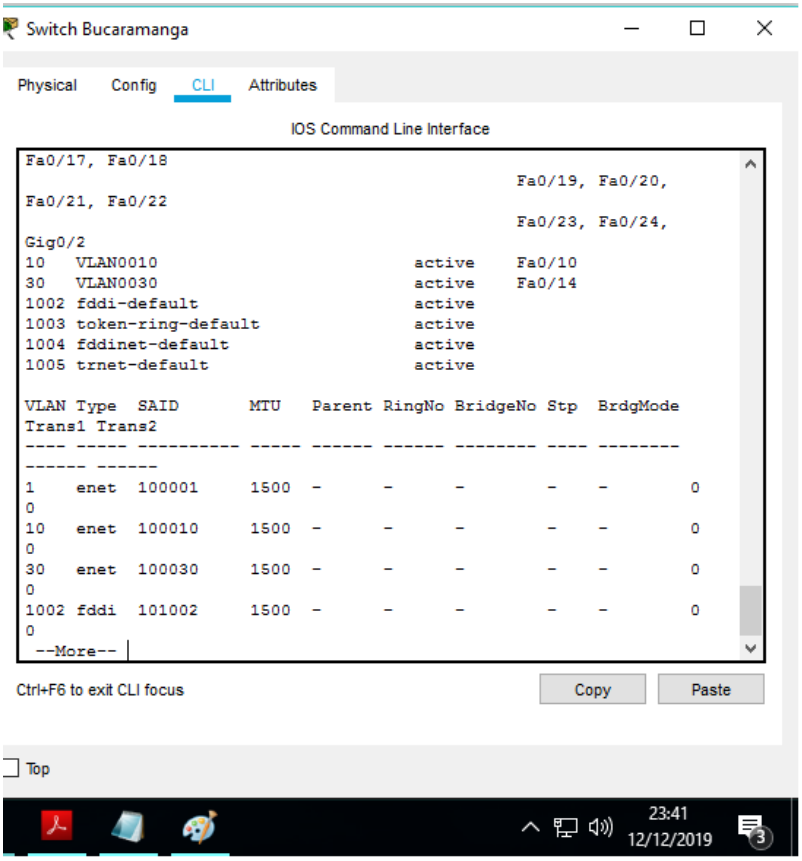

Figura 55. Verificación vlans Switch Bucaramanga.

1.2.5. Configuraciones del switch Tunja

1.2.5.1. Básicas

Switch>enable

Switch#conf term

Switch(config)#hostname STunja

STunja (config)#enable password cisco

STunja (config)#line console 0

STunja (config-line)# exec-timeout 6 0

STunja (config-line)# logging synchronous

STunja (config-line)#password cisco

STunja (config-line)#login

STunja (config-line)#line vty 0 15

STunja (config-line)# exec-timeout 6 0

STunja (config-line)# logging synchronous

STunja (config-line)#password cisco

STunja (config-line)#login

STunja (config-line)#exit

STunja (config)#exit

STunja #copy running-config startup-config

1.2.5.2. Vlans switch

STunja(config)#vlan 1

STunja(config-vlan)#vlan 20

STunja(config-vlan)#vlan 30

STunja(config-vlan)#int f0/10

STunja(config-if)#switchport mode access

STunja(config-if)#switchport access vlan 20

STunja(config-if)#int f0/14

STunja(config-if)#switchport mode access

STunja(config-if)#switchport access vlan 30

STunja(config-if)#int g0/1

STunja(config-if)#switchport mode trunk

STunja(config-if)#int vlan 1

STunja(config-if)#ip address 172.3.2.11 255.255.255.248

STunja(config-if)#no shutdown

STunja(config-if)#ip default-gateway 172.3.2.9

STunja(config-if)#exit

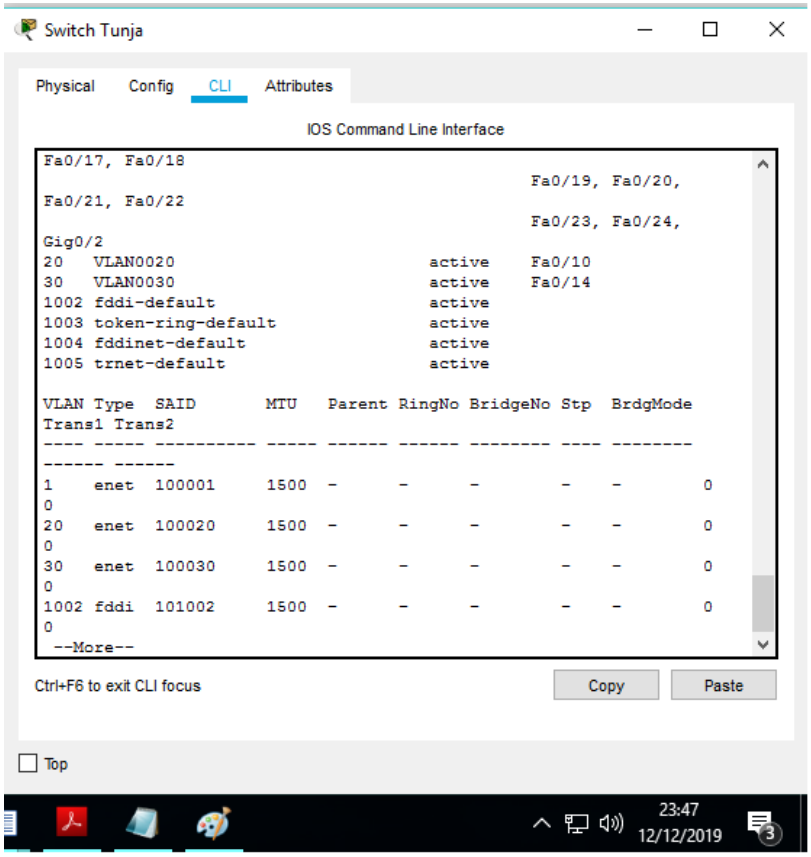

Figura 56. Verificación vlans switch Tunja.

1.2.6. Configuraciones switch Cundinamarca

1.2.6.1. Básicas

Switch>enable

Switch#conf term

Switch(config)#hostname SCundinamarca

SCundinamarca (config)#enable password cisco

SCundinamarca (config)#line console 0

SCundinamarca (config-line)# exec-timeout 6 0

SCundinamarca (config-line)# logging synchronous

SCundinamarca (config-line)#password cisco

SCundinamarca (config-line)#login

SCundinamarca (config-line)#line vty 0 15

SCundinamarca (config-line)# exec-timeout 6 0

SCundinamarca (config-line)# logging synchronous

SCundinamarca (config-line)#password cisco

SCundinamarca (config-line)#login

SCundinamarca (config-line)#exit

SCundinamarca (config)#exit

SCundinamarca #copy running-config startup-config

1.2.6.2. Vlans switch

SCundinamarca(config)#vlan 1

SCundinamarca(config-vlan)#vlan 20

SCundinamarca(config-vlan)#vlan 30

SCundinamarca(config-vlan)#vlan 88

SCundinamarca(config-vlan)#exit

SCundinamarca(config)#int f0/10

SCundinamarca(config-if)#switchport mode access

SCundinamarca(config-if)#switchport access vlan 20

SCundinamarca(config-if)#int fa0/14

SCundinamarca(config-if)#switchport mode access

SCundinamarca(config-if)#switchport access vlan 30

SCundinamarca(config-if)#int fa0/20

SCundinamarca(config-if)#switchport mode access

SCundinamarca(config-if)#switchport access vlan 88

SCundinamarca(config-if)#int g0/1

SCundinamarca(config-if)#switchport mode trunk

SCundinamarca(config-if)#int vlan 1

SCundinamarca(config-if)#ip address 172.31.2.11 255.255.255.248

SCundinamarca(config-if)#no shutdown

SCundinamarca(config-if)#ip default-gateway 172.31.2.9

SCundinamarca(config-if)#exit

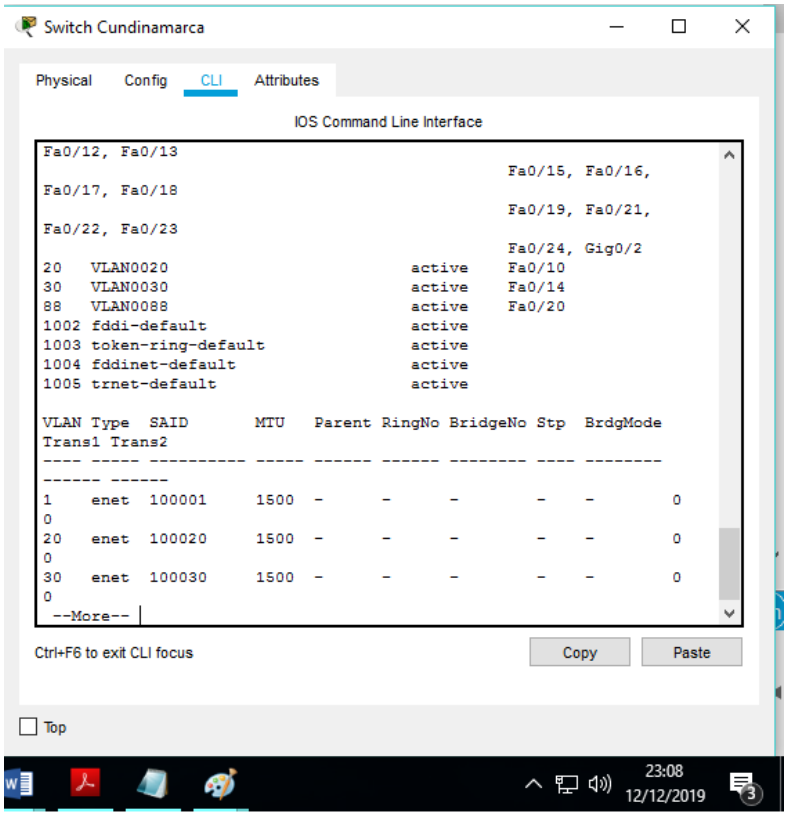

Figura 57. Verificación vlans switch Cundinamarca.

1.2.7. Servidor TFTP (web interno) y almacenamiento de archivos de routers.

Con el siguiente comando podemos copiar configuración del router al tftp server.

1.2.7.1. Router Cundinamarca

RCundinamarca#copy running-config tftp

Address or name of remote host []? 172.31.2.27

Destination filename [RCundinamarca-confg]?

Writing running-config....!!

[OK - 1747 bytes]

1747 bytes copied in 3.011 secs (580 bytes/sec)

RCundinamarca#copy running-config tftp

Address or name of remote host []? 172.31.2.27

Destination filename [RCundinamarca-confg]?

Writing running-config...!!

[OK - 1747 bytes]

1.2.7.2. Router Tunja

RTunja>enable

Password:

RTunja#copy running-config tftp

Address or name of remote host []? 172.31.2.27

Destination filename [RTunja-confg]?

Writing running-config...!!

[OK - 1634 bytes]

1634 bytes copied in 0.005 secs (326800 bytes/sec)

1.2.7.3. Router Bucaramanga

RBucaramanga>enable

Password:

RBucaramanga#copy running-config tftp

Address or name of remote host []? 172.31.2.27

Destination filename [RBucaramanga-confg]?

Writing running-config...!!

[OK - 1591 bytes]

1591 bytes copied in 0.001 secs (1591000 bytes/sec)

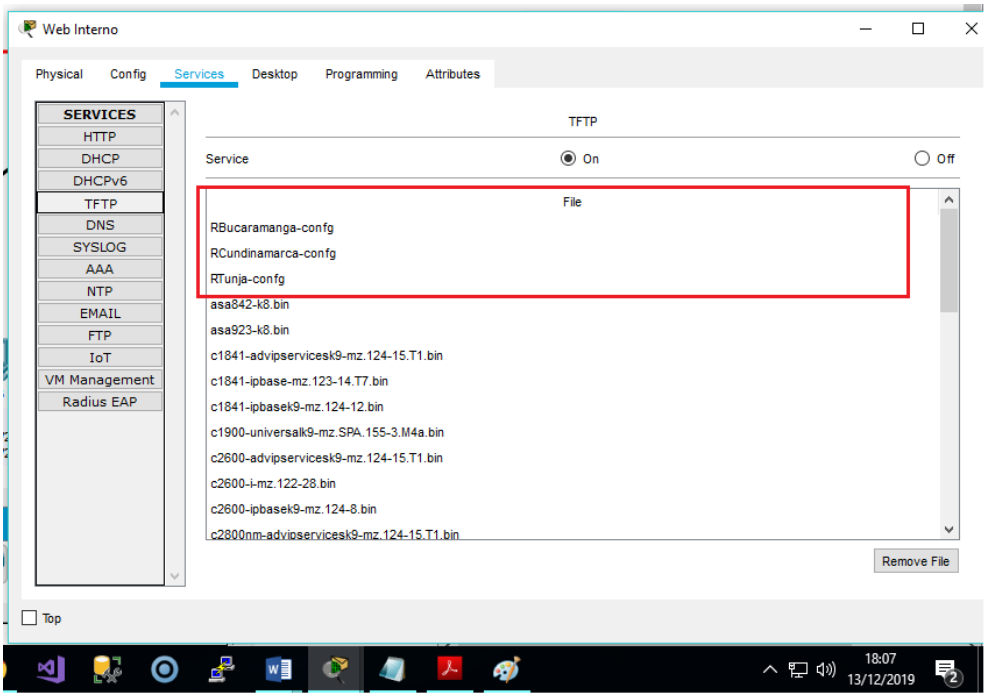

Figura 58. Almacenamiento de archivos TFTP.

1.2.8. Proporcionando solo direcciones a los hosts de Bucaramanga y Cundinamarca

1.2.8.1. Router Bucaramanga

RBucaramanga#conf term

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

RBucaramanga(config)#interface g0/0.10

RBucaramanga(config-subif)#ip helper-address 172.31.2.33

RBucaramanga(config-subif)#int g0/0.30

RBucaramanga(config-subif)#ip helper-address 172.31.2.33

RBucaramanga(config-subif)#end

1.2.8.2. Router Cundinamarca

RTunja#conf term

```
RTunja(config)#ip dhcp excluded-address 172.31.0.1 172.31.0.4
RTunja(config)#ip dhcp excluded-address 172.31.0.65 172.31.0.68
RTunja(config)#ip dhcp excluded-address 172.31.1.65 172.31.1.68
RTunja(config)#ip dhcp excluded-address 172.31.1.1 172.31.1.4
RTunja(config)#ip dhcp pool vlan10B
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 172.31.2.27
RTunja(dhcp-config)#ip dhcp pool vlan30B
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 172.31.2.27
RTunja(dhcp-config)#ip dhcp pool vlan20C
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 172.31.2.27
RTunja(dhcp-config)#ip dhcp pool vlan30C
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 172.31.2.27
RTunja(dhcp-config)#end
```

1.2.8.3. Router Tunja

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

1.2.9. Web server con NAT estático y equipos con NAT de sobrecarga (PAT).

Para este caso debemos hacer la configuración en el router de Tunja, de la siguiente forma:

1.2.9.1. Router Tunja

```
RTunja#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
RTunja(config)#ip nat inside source static 172.31.2.27 209.165.220.10
RTunja(config)#ip access-list standard NAT-ACL
RTunja(config-std-nacl)#permit 172.31.0.0 0.0.255.255
RTunja(config-std-nacl)#ip nat inside source list NAT-ACL interface g0/1 overload
RTunja(config)#int g0/1
RTunja(config-if)#ip nat outside
RTunja(config-if)#int g0/0.1
RTunja(config-subif)#ip nat inside
RTunja(config-subif)#int g0/0.20
RTunja(config-subif)#ip nat inside
RTunja(config-subif)#int g0/0.30
RTunja(config-subif)#ip nat inside
RTunja(config-subif)#int s0/0/0
RTunja(config-if)#ip nat inside
RTunja(config-if)#int s0/0/1
RTunja(config-if)#ip nat inside
RTunja(config-if)#exit
RTunja(config)#ip route 0.0.0.0 0.0.0.0 209.165.220.5
RTunja(config)#router ospf 1
RTunja(config-router)#default-information originate
RTunja(config-router)#end
RTunja#
```

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

RTunja#wr

Building configuration...

[OK]

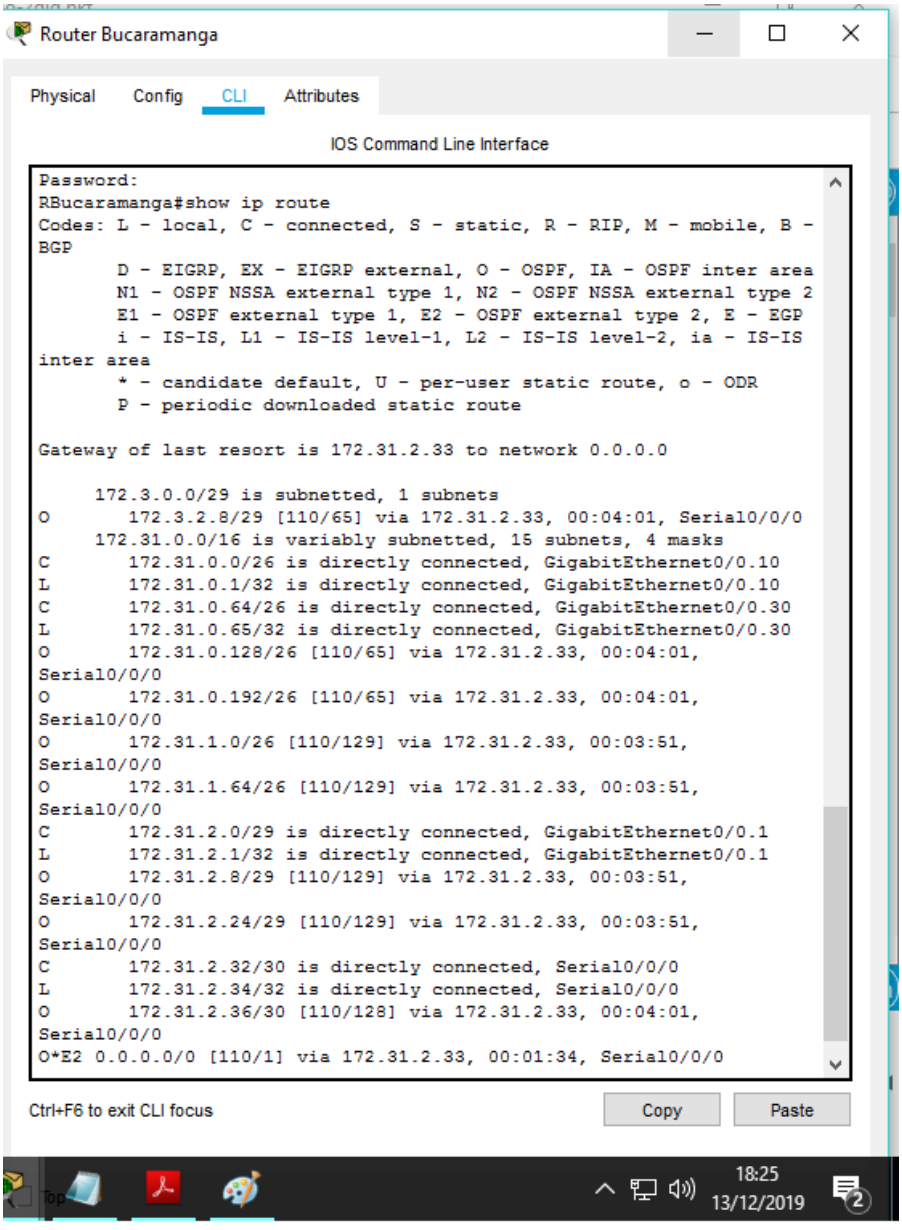

Figura 59. Configuración NAT router Bucaramanga.

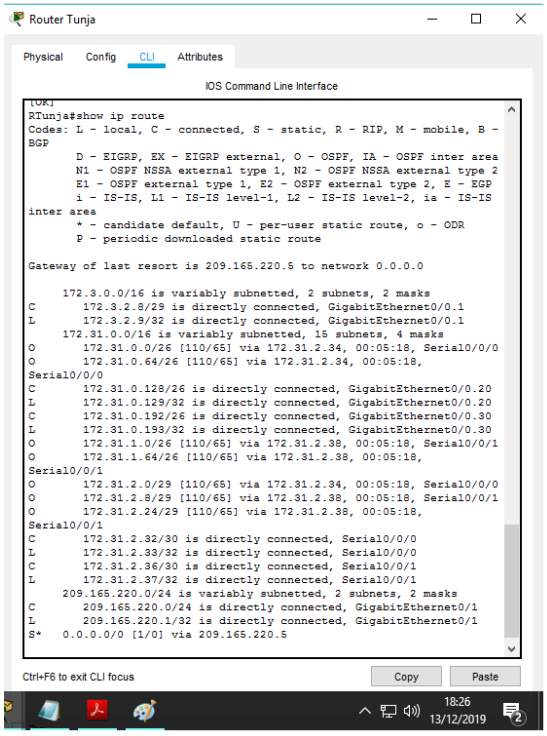

Figura 60. Configuración NAT router Tunja.

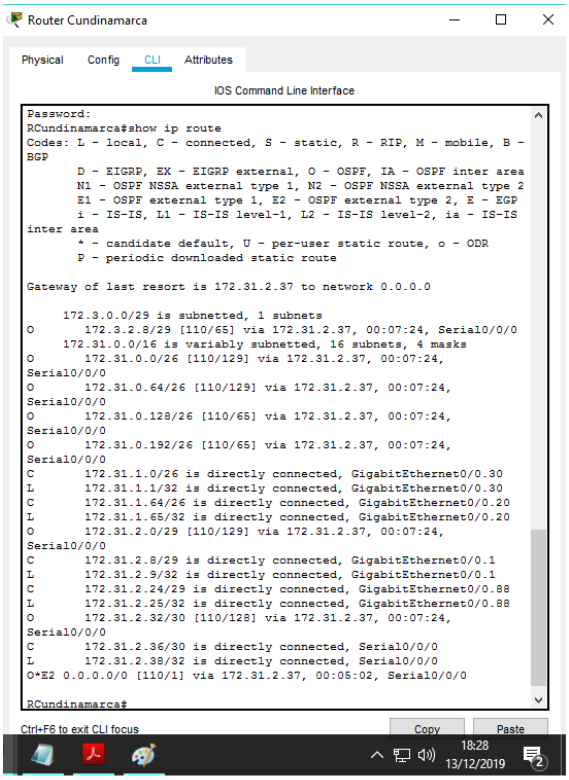

Figura 61. Configuración NAT router Cundinamarca.

1.2.10. El enrutamiento deberá tener autenticación.

1.2.10.1. Router Bucaramanga

RBucaramanga#configure terminal

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

RBucaramanga(config)#interface s0/0/0

RBucaramanga(config-if)#ip ospf authentication message-digest

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

RBucaramanga(config-if)#exit

RBucaramanga(config)#exit

RBucaramanga#

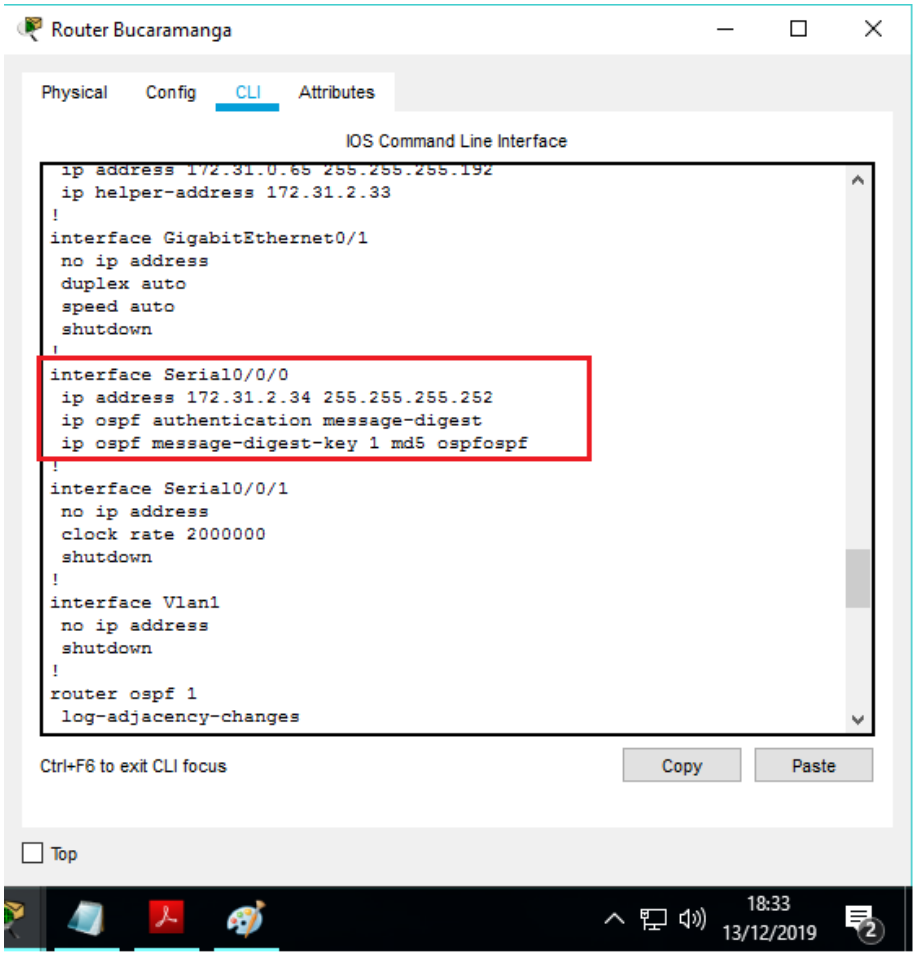

Figura 62. Autenticación de enrutamiento router Bucaramanga.

1.2.10.2. Router Tunja

RTunja#configure terminal

RTunja(config)#interface s0/0/0

RTunja(config-if)#ip ospf authentication message-digest

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

RTunja(config-if)#

00:15:10: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/0/0 from LOADING to FULL, Loading Done

interface s0/0/1

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 ospfospf

RTunja(config-if)#end

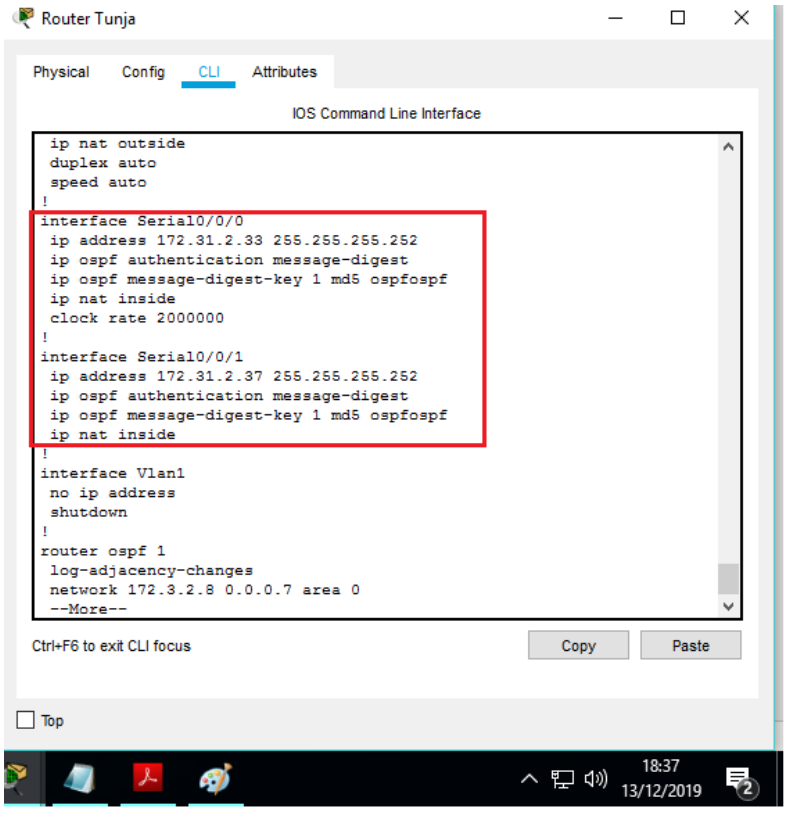

Figura 63. Autenticación de enrutamiento router Tunja.

1.2.10.3. Router Cundinamarca

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 ospfospf

RCundinamarca(config-if)#end

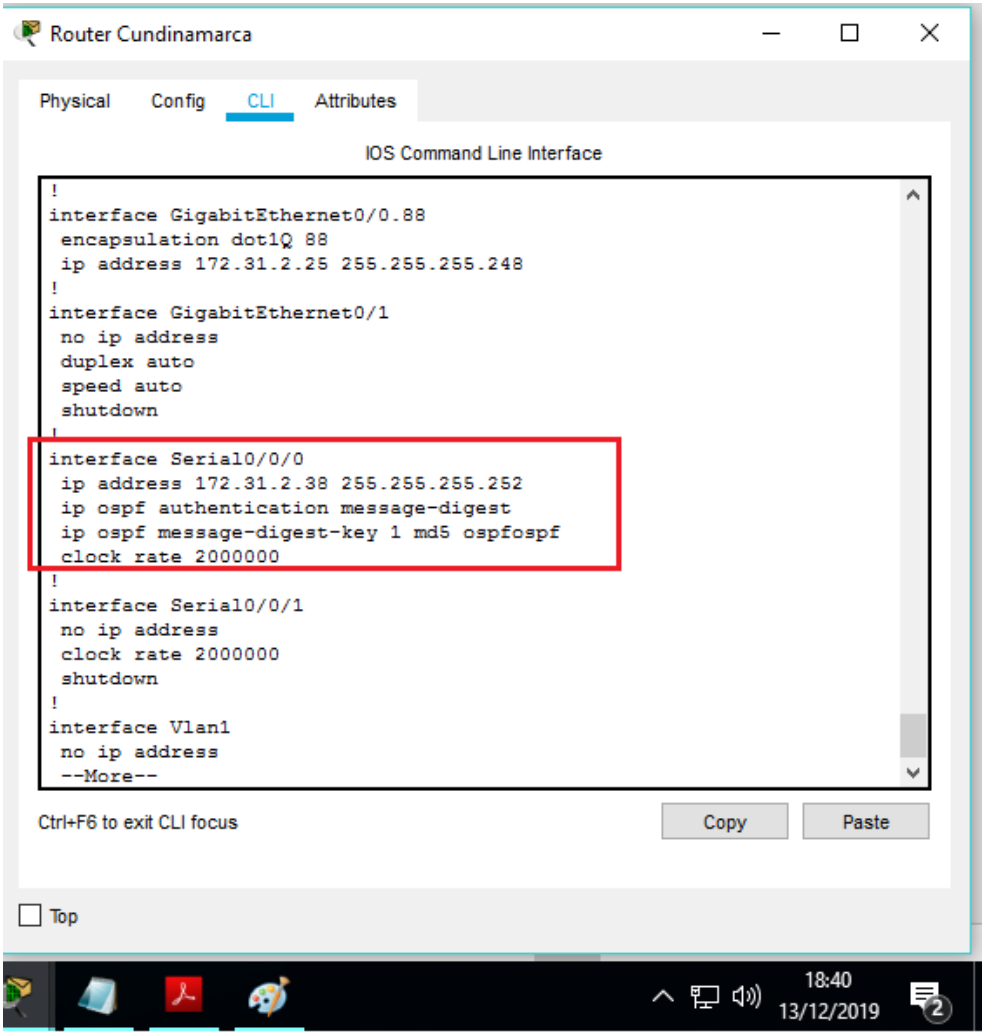

Figura 64. Autenticación de enrutamiento router Cundinamarca.

1.2.11. Listas de control de acceso:

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

Configuración que debe realizarse en el router Cundinamarca.

RCundinamarca#conf term

RCundinamarca(config)#access-list 152 deny ip 172.31.1.64 0.0.0.63 209.165.220.0 0.0.0.255

RCundinamarca(config)#access-list 152 permit udp any any eq bootps

RCundinamarca(config)#access-list 152 permit ip any any

RCundinamarca(config)#int g0/0.20

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

RCundinamarca(config-subif)#end

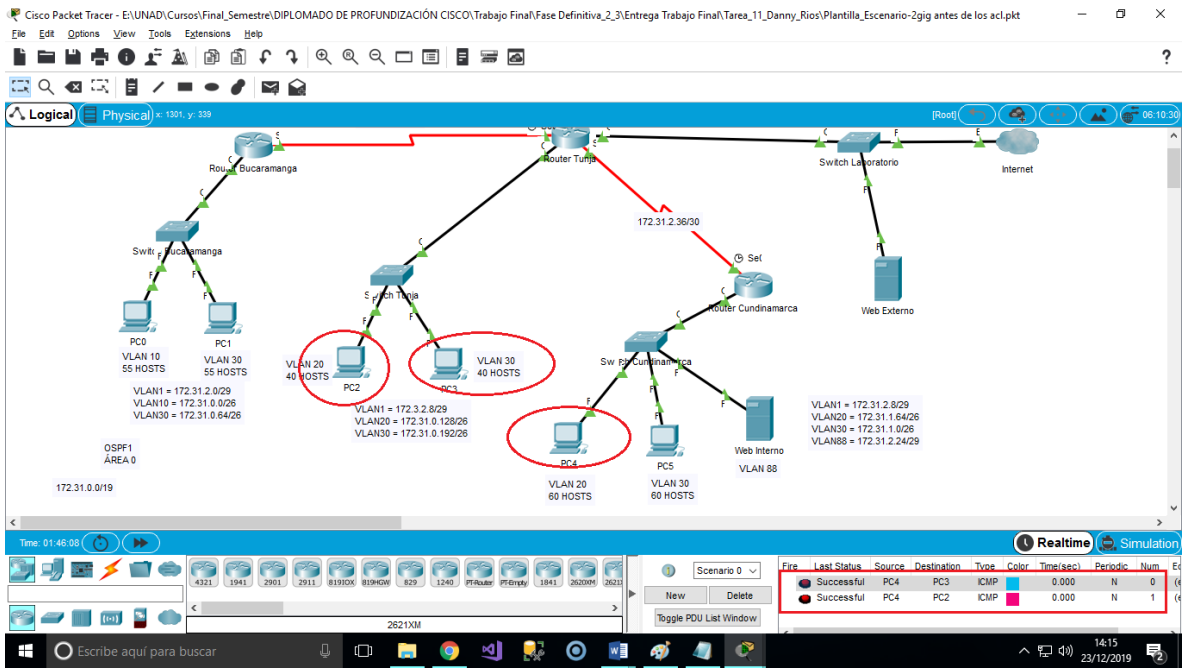

Figura 65. ACL vlan 20 router Cundinamarca a red interna Tunja.

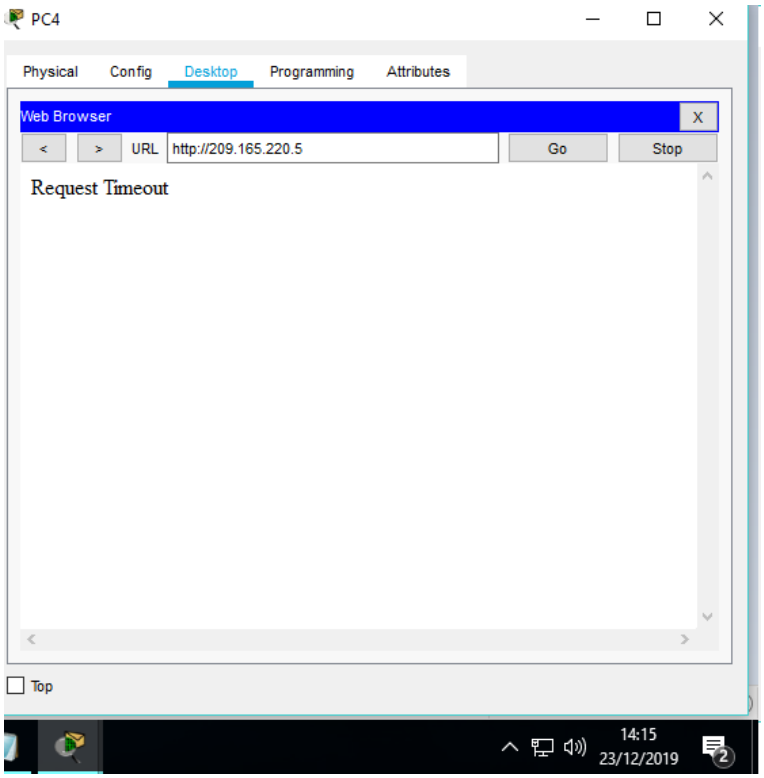

Figura 66. ACL pc vlan 20 sin acceso a internet.

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

Configuración que debe realizarse en el router Cundinamarca.

RCundinamarca#conf term

RCundinamarca(config)#access-list 153 permit tcp 172.31.1.0 0.0.0.63 host 209.165.220.5 eq 80

RCundinamarca(config)#access-list 153 deny ip any any

RCundinamarca(config)#int g0/0.30

RCundinamarca(config-subif)#ip access-group 153 in

RCundinamarca(config-subif)#end

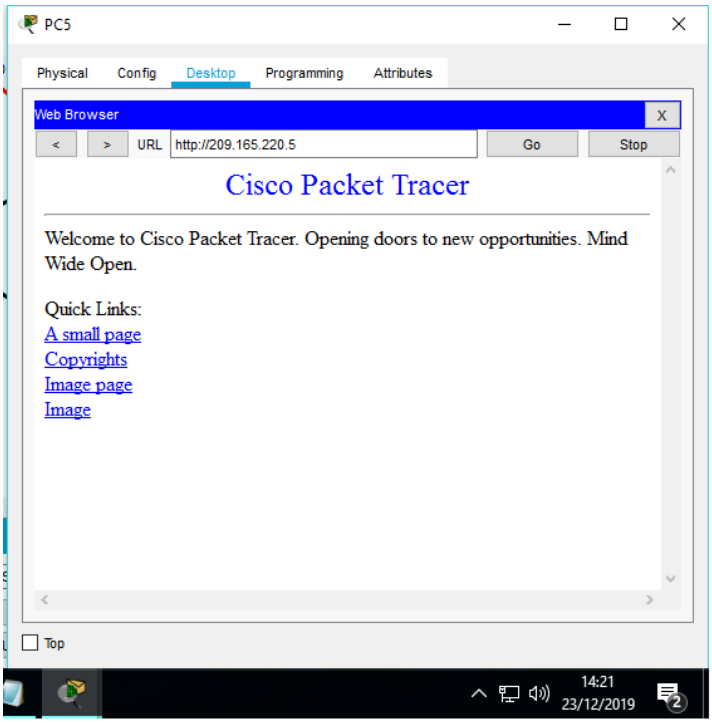

Figura 67. ACL pc vlan 30 Cundinamarca con acceso a internet.

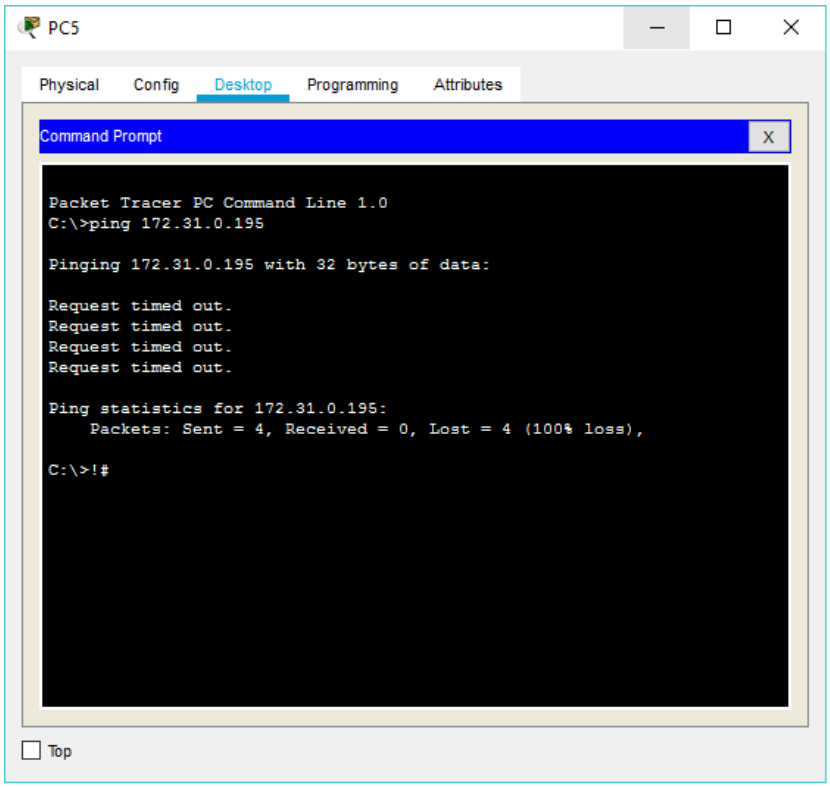

Figura 68. ACL pc vlan 30 Cundinamarca a pc red de Tunja.

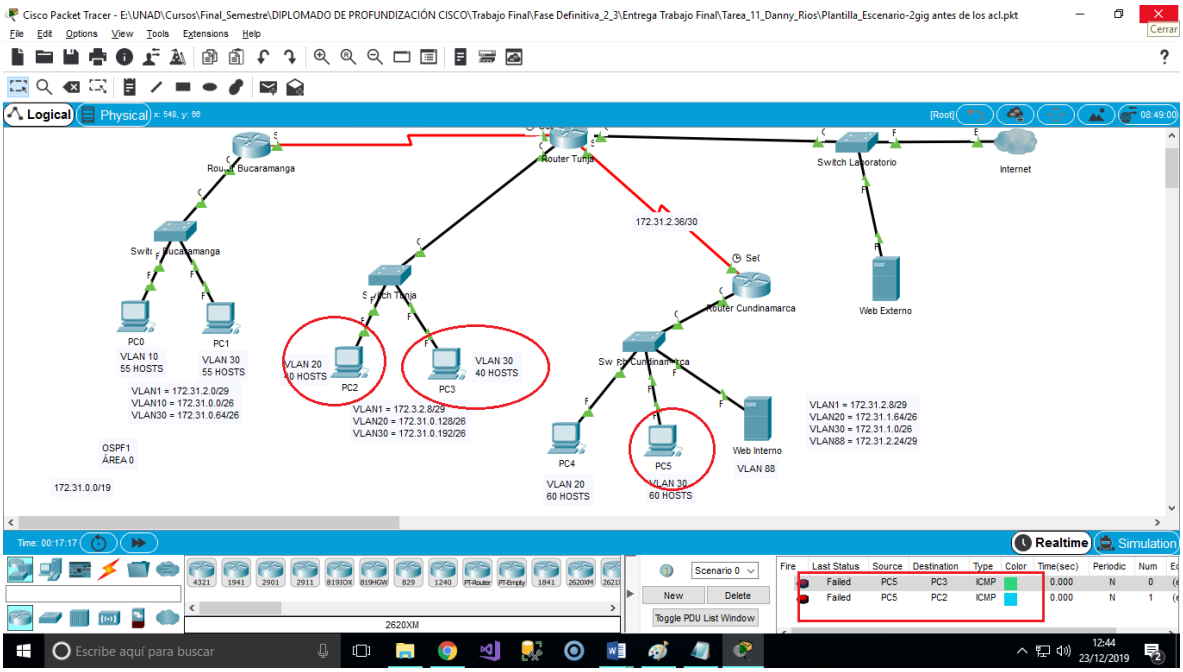

Figura 69. Mensajes vlan 30 Cundinamarca a pc red de Tunja.

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

Configuración que debe realizarse en el router Tunja.

RTunja#configure terminal

RTunja(config)#access-list 152 permit tcp 172.31.0.192 0.0.0.63 209.165.220.5 0.0.0.255 eq 80

RTunja(config)#access-list 152 permit tcp 172.31.0.192 0.0.0.63 209.165.220.5 0.0.0.255 eq 21

RTunja(config)#int g0/0.30

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

RTunja(config-subif)#end

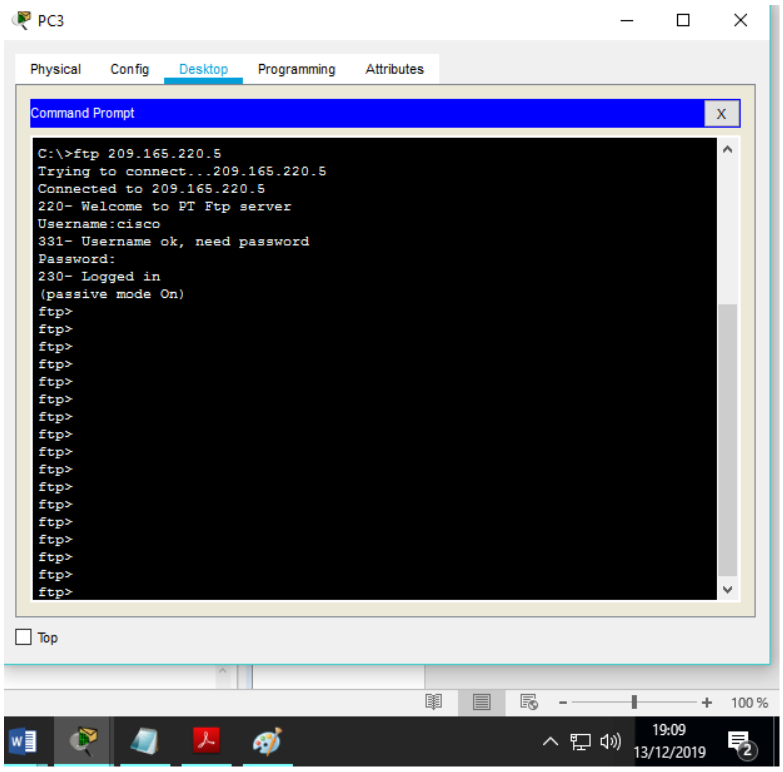

Figura 70. ACL vlan 30 acceso tfp.

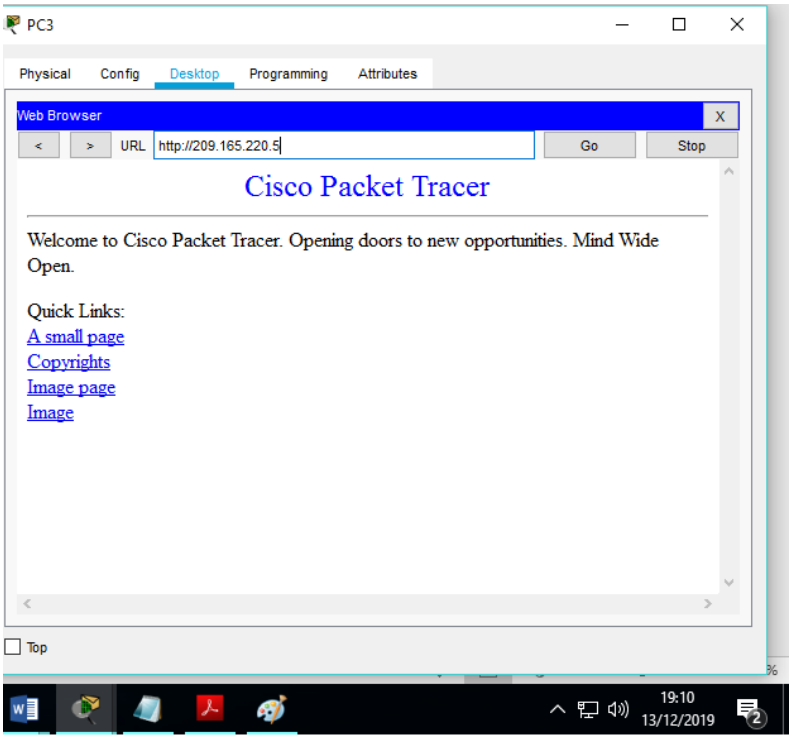

Figura 71. ACL vlan 30 acceso internet.

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

Configuración que debe realizarse en el router Tunja.

RTunja#conf term

RTunja(config)#access-list 153 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63

RTunja(config)#access-list 153 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63

RTunja(config)#int g0/0.20

RTunja(config-subif)#ip access-group 153 in

RTunja(config-subif)#end

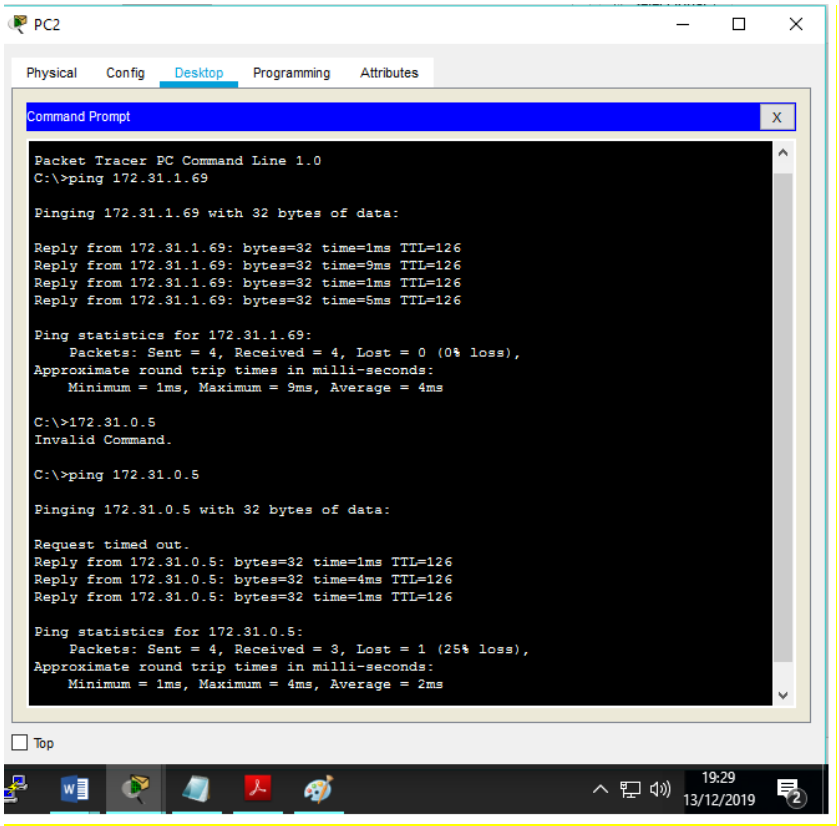

Figura 72. Verificación acceso a la vlan 20 y 10

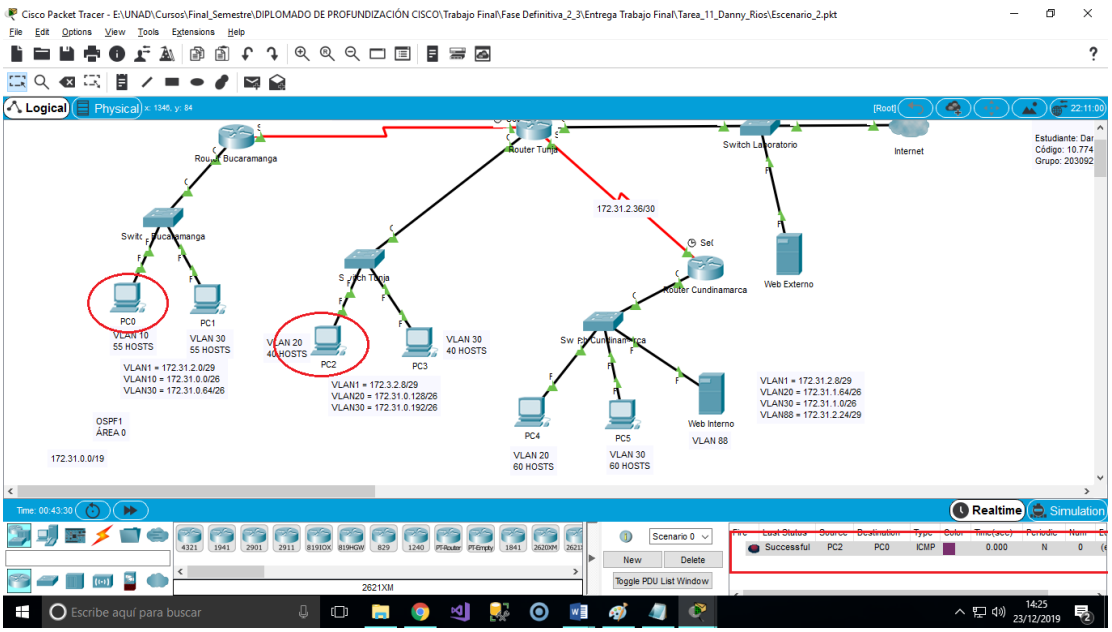

Figura 73. acceso a vlan 20 Tunja a vlan 10 Bucaramanga.

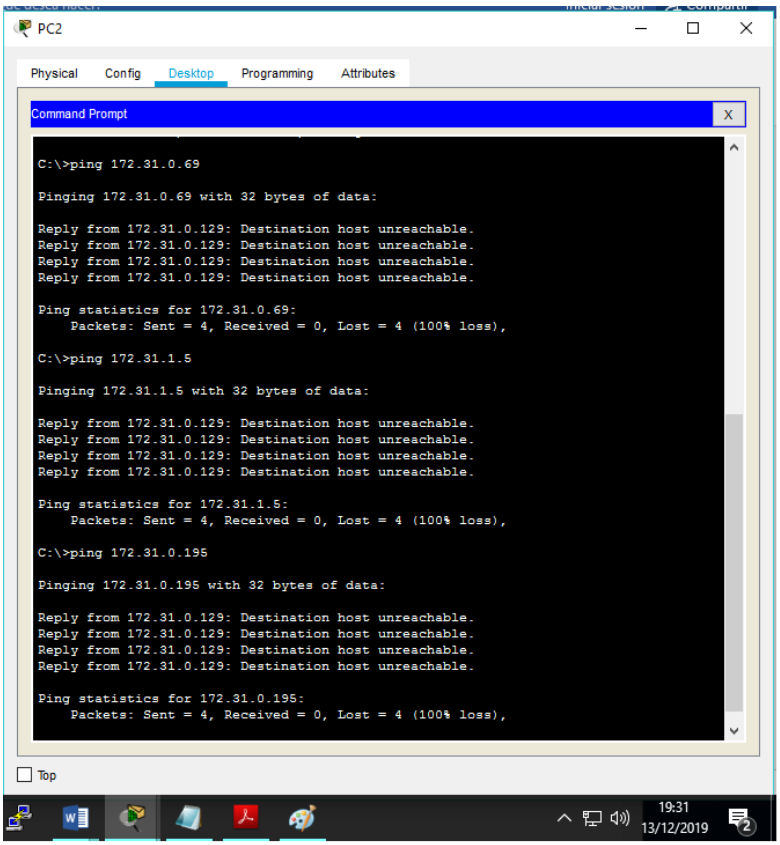

Figura 74. Verificación rechazo a vlan fuera del ACL

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

Configuración que debe realizarse en el router Bucaramanga.

RBucaramanga#configure terminal
RBucaramanga(config)#access-list 152 permit tcp 172.31.0.64 0.0.0.63 host 209.165.220.5 eq 80
RBucaramanga(config)#int g0/0.30
RBucaramanga(config-subif)#ip access-group 152 in
RBucaramanga(config-subif)#end
RBUCARAMANGA(config)#access-list 153 permit ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.0.63
RBUCARAMANGA(config)#access-list 153 deny ip any any
RBUCARAMANGA(config)# int g0/0.30
RBUCARAMANGA(config-subif)#ip access-group 153 in

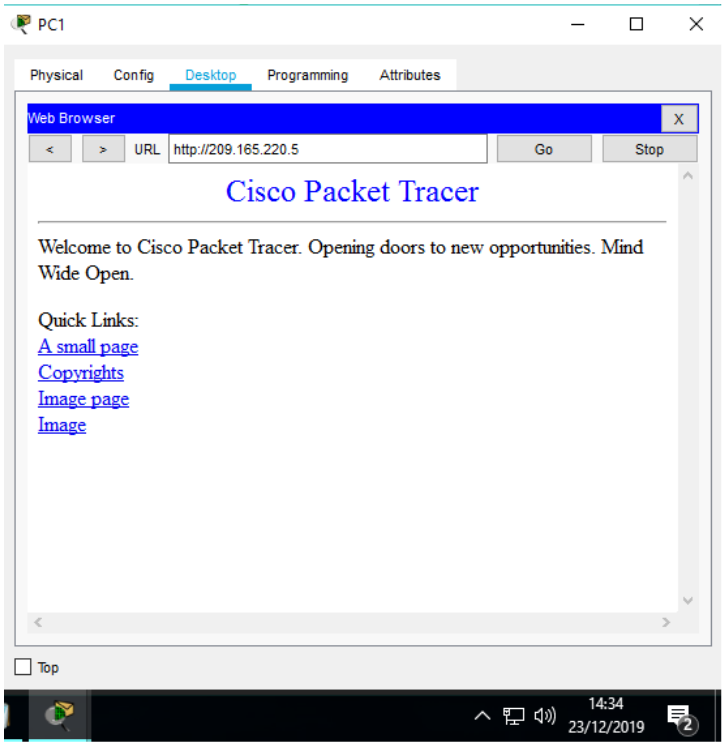

Figura 75. Acceso vlan 30 Bucaramanga a internet.

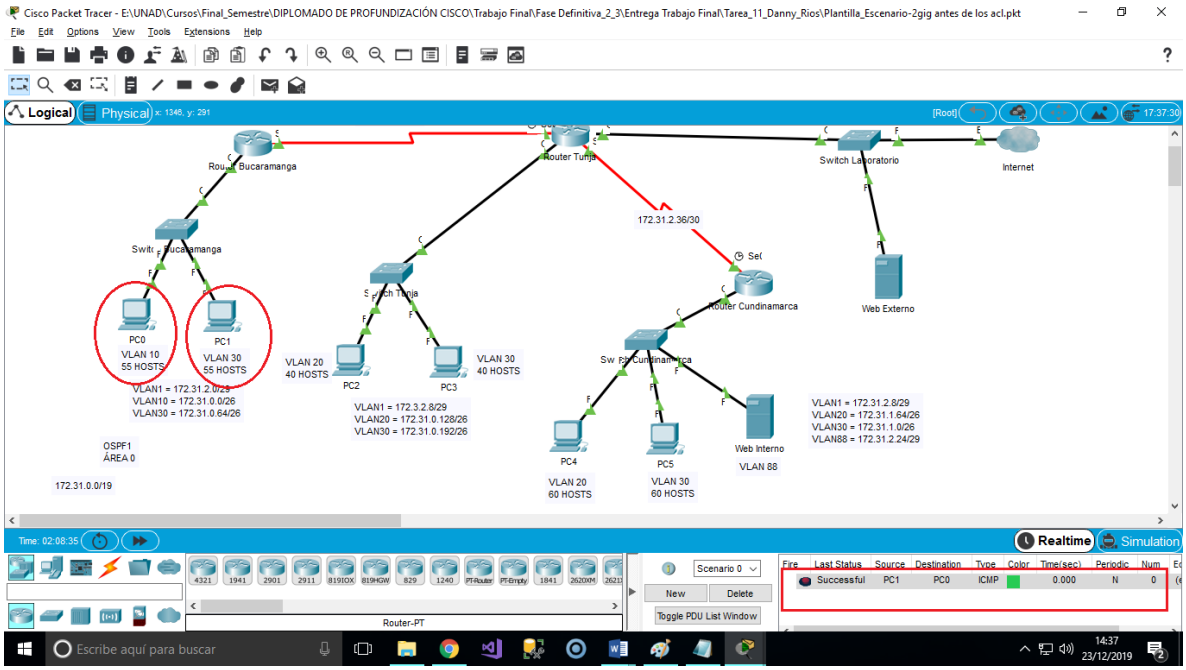

Figura 76. Acceso vlan 30 a vlan 10.

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

Configuración que debe realizarse en el router Bucaramanga.

RBucaramanga#conf term

RBucaramanga(config)#access-list 152 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63

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

RBucaramanga(config)#int g0/0.10

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

RBucaramanga(config-subif)#end

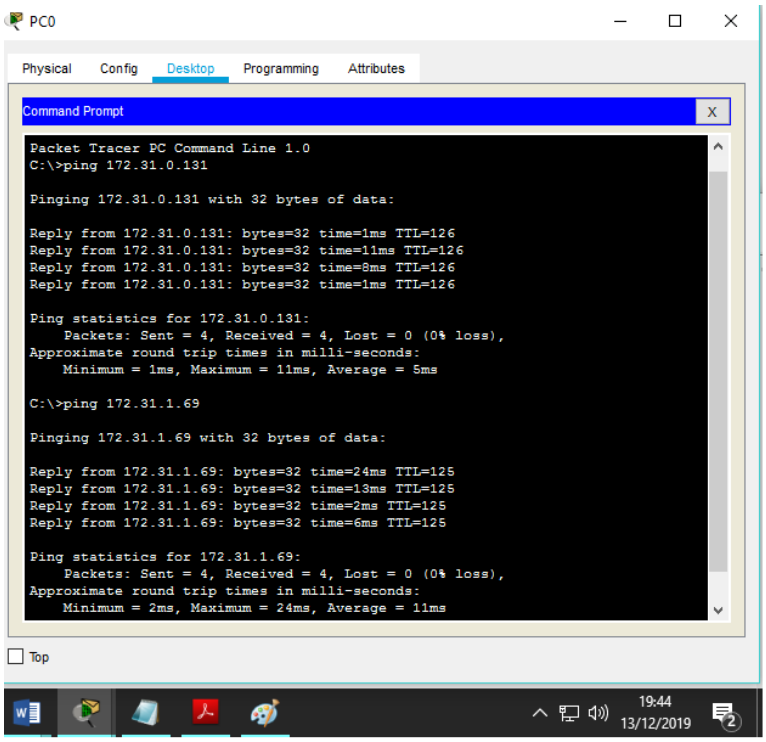

Figura 77. Acceso vlan 10 Bucaramanga a Cundinamarca y Tunja vlan 20.

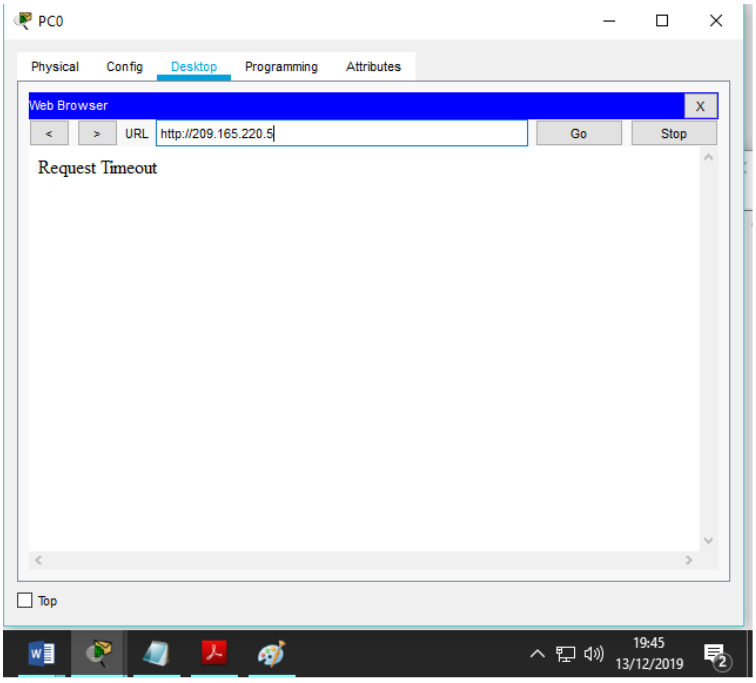

Figura 78. Internet vlan 10 Bucaramanga a Cundinamarca y Tunja vlan 20.

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

Configuración que debe realizarse en:

- ✓ **Router Bucaramanga**

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

- ✓ **Router Tunja**

```
RTunja#configure terminal
RTunja(config)#access-list 153 deny ip 172.3.2.8 0.0.0.7 172.31.0.128 0.0.0.63
RTunja(config)#access-list 153 deny ip 172.3.0.192 0.0.0.63 172.31.0.128 0.0.0.63
RTunja(config)#access-list 153 permit ip any any
RTunja(config)#int g0/0.20
RTunja(config-subif)#ip access-group 153 out
RTunja(config-subif)#end
```

✓ **Router Cundinamarca**

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

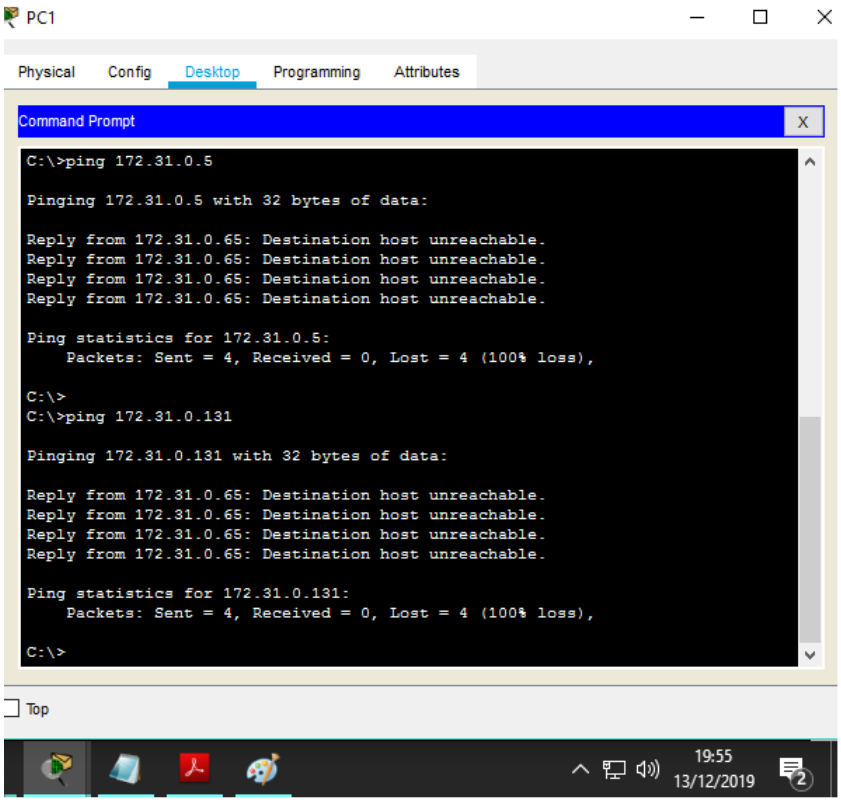

Figura 79. Vlan 30 Bucaramanga a vlan 20 Tunja

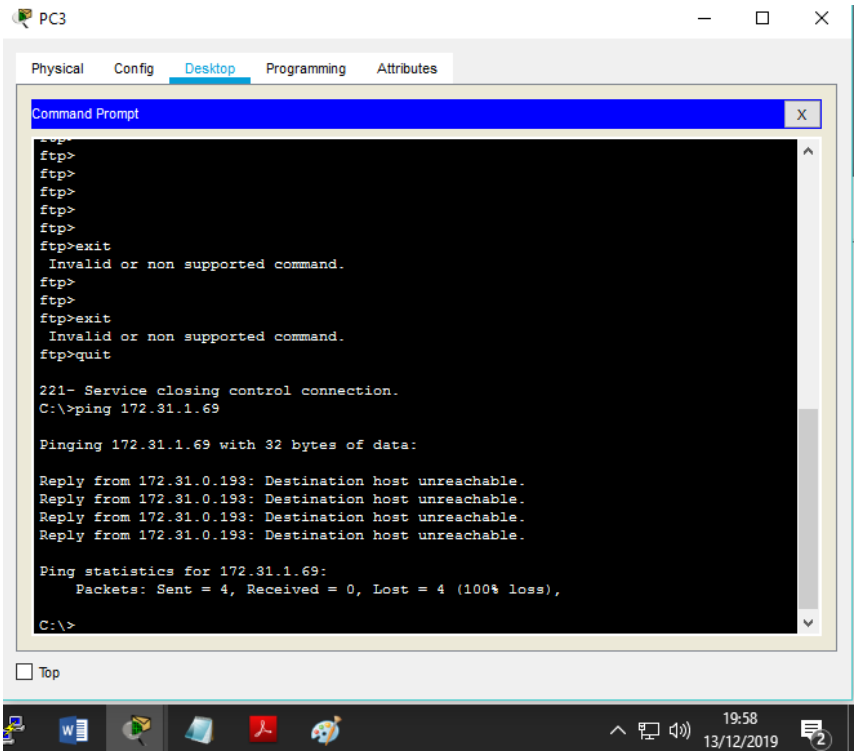

Figura 80. vlan 30 Tunja a vlan 20 Cundinamarca.

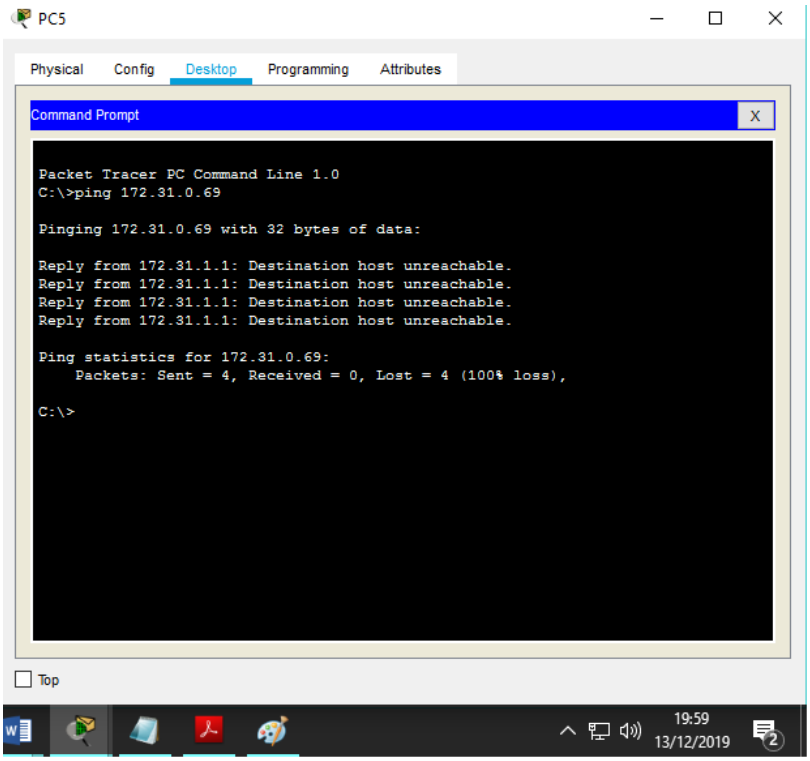

Figura 81. Vlan 30 Cundinamarca a vlan 30 Bucaramanga

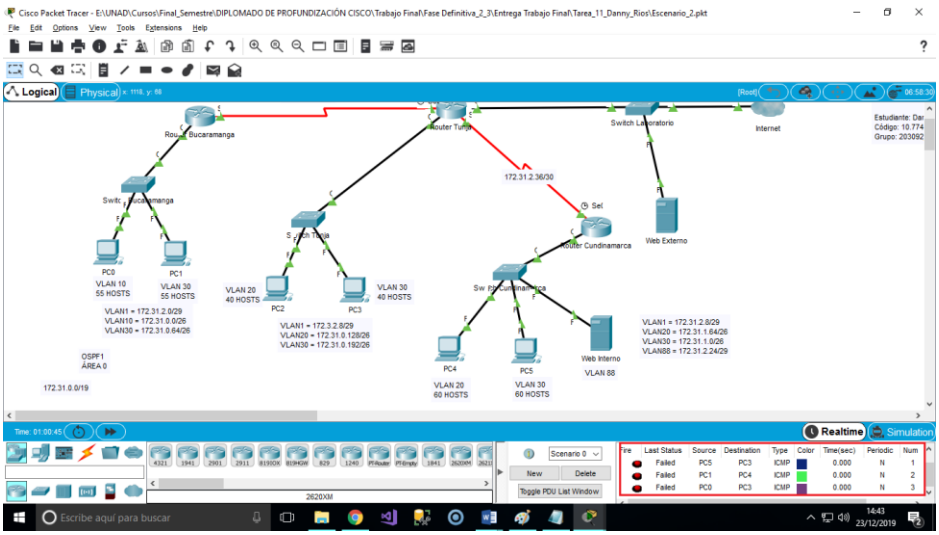

Figura 82. sin acceso entre host a diferentes vlan.

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

Configuración que debe realizarse en:

✓ **Router Bucaramanga**

RBucaramanga#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RBucaramanga(config)#access-list 9 permit 172.31.2.0 0.0.0.7
RBucaramanga(config)#access-list 9 permit 172.3.2.8 0.0.0.7
RBucaramanga(config)#access-list 9 permit 172.31.2.8 0.0.0.7
RBucaramanga(config)#line vty 0 4
RBucaramanga(config-line)#access-class 9 in
RBucaramanga(config-line)#end

✓ **Router Tunja**

RTunja#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

RTunja(config)#access-list 9 permit 172.31.2.0 0.0.0.7

RTunja(config)#access-list 9 permit 172.3.2.8 0.0.0.7

RTunja(config)#access-list 9 permit 172.31.2.8 0.0.0.7

RTunja(config)#line vty 0 4

RTunja(config-line)#access-class 9 in

RTunja(config-line)#end

- ✓ **Router Cundinamarca**

RCundinamarca#configure terminal

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

RCundinamarca(config)#access-list 9 permit 172.31.2.0 0.0.0.7

RCundinamarca(config)#access-list 9 permit 172.3.2.8 0.0.0.7

RCundinamarca(config)#access-list 9 permit 172.31.2.8 0.0.0.7

RCundinamarca(config)#line vty 0 4

RCundinamarca(config-line)#access-class 9 in

RCundinamarca(config-line)#end

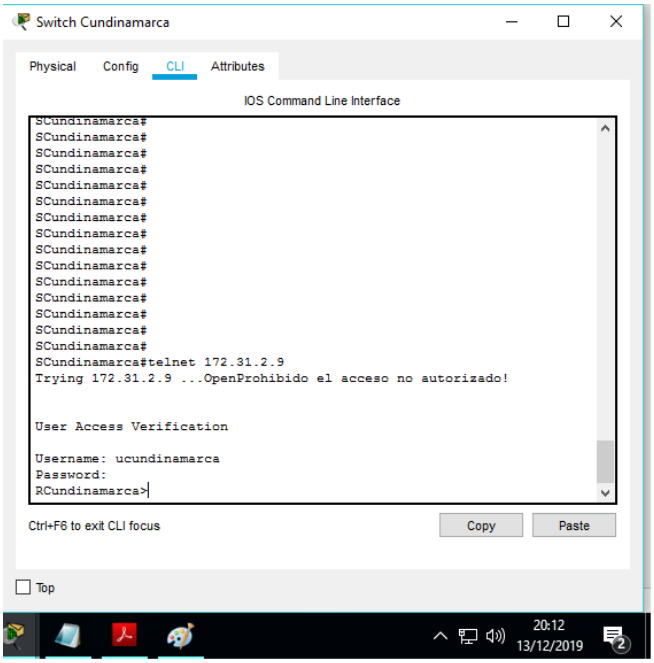

Figura 83. Verificación acceso a router Cundinamarca.

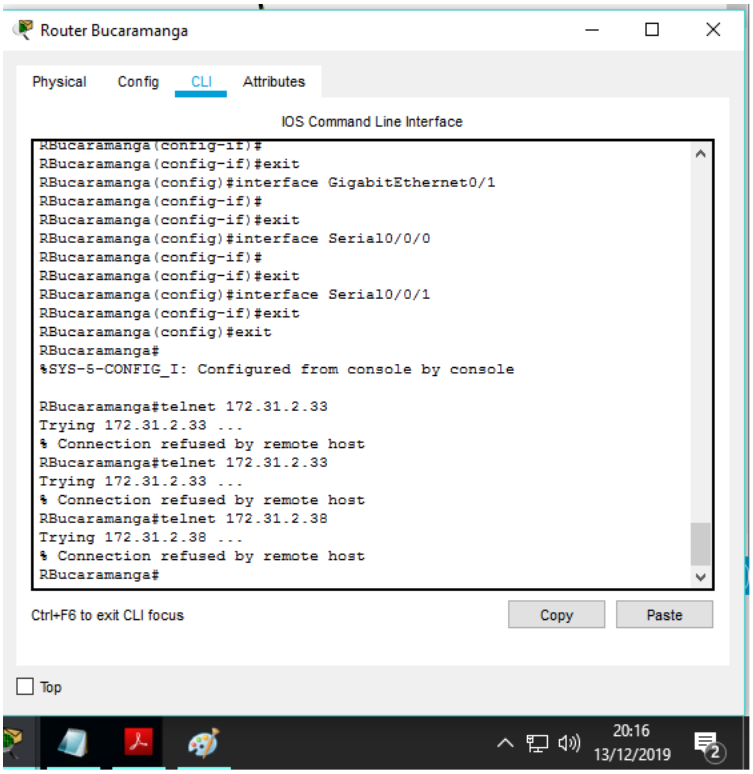

Figura 84. Verificación acceso a router Bucaramanga.

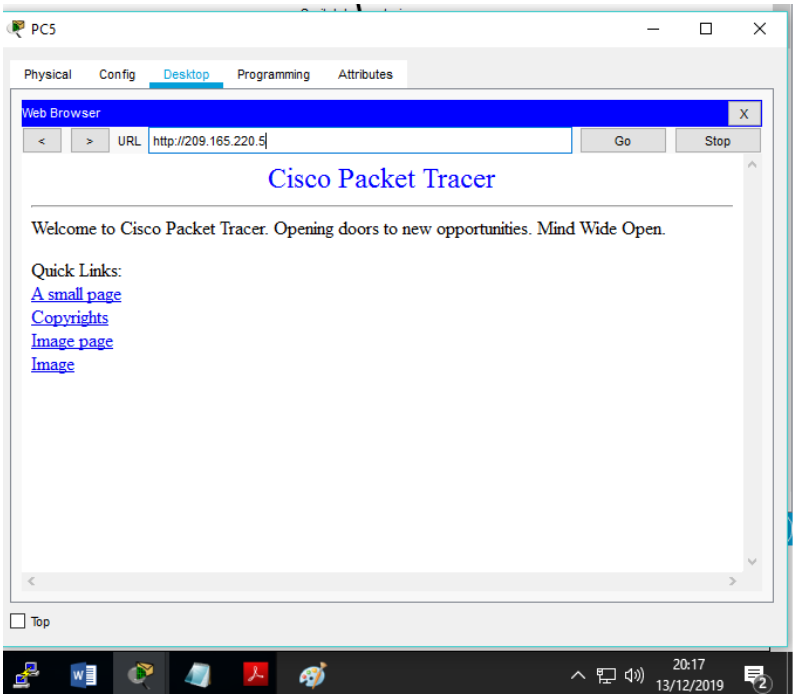

Figura 85. Verificación acceso a internet.

CONCLUSIONES

Mediante el desarrollo de los escenarios propuestos como actividad final se generaron diversos conocimientos para realizar tareas que permiten una adecuada administración de redes, ingresando los comandos y configuraciones necesarios que establecen acciones y controles, de los cuales podemos mencionar:

- Se comprendieron y usaron los protocolos de routing disponibles ante la necesidad de la red.
- El uso de las configuraciones básicas de los dispositivos como switches y routers.
- La implementación de los distintos protocolos DHCP que permiten en un equipo obtener su configuración en forma dinámica.
- La aplicación y análisis de la configuración de dispositivos de red para el óptimo funcionamiento de la misma.
- Se aplicaron los conceptos para establecer la conectividad IPv4 usando direcciones IP
- Se validaron los principales conceptos de enrutamiento, comenzando por el protocolo RIP y OSPF.
- El análisis y ejecución de las instrucciones para las ACL estándar y extendidas en los dispositivos.
- El establecimiento de VLAN, que permiten organizar y distribuir terminales generando un buen tráfico en la red.
- Se identificaron las funciones, incluyendo la configuración y aplicación de DHCPv4.
- Se trabajó con el protocolo NAT para traducir IPs Privadas a IPs públicas, aprovechando recursos públicos, proporcionando un entorno seguro.
- El uso de NAT dinámica / estática como característica que traduce conexiones TCP y UDP realizadas por un host y un puerto en una red externa a otra dirección y puerto de la red interna.

BIBLIOGRAFÍA

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

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

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

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

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

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

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