Diplomado De Profundización Cisco (Diseño e implementación de soluciones integradas LAN / WAN)

Paso 11 - Prueba De Habilidades Prácticas CCNA Trabajo Final

Presentado Por:

Oscar Darío Castro Rosero

Tutor:

Nilson Albeiro Ferreira Manzanares

Universidad Nacional Abierta Y A Distancia - Unad

Escuela De Ciencias Básicas De La Tecnología E Ingeniería

Programa De Ingeniería De Sistemas

CEAD – San Juan de Pasto

2020

Tabla de Contenido.

Lista de figuras.

Lista de tablas.

Resumen

Gracias a la evolución de los medios tecnológicos es necesario que como futuros profesionales seamos capaces de dar solución integral a problemas con aplicabilidad real, por esto hacemos parte activa del desarrollo del diplomado de profundización en Cisco CCNA por medio de la sustentación escrita de la resolución de escenarios complejos. Para su ejecución se utilizaron las versiones 6.1.1. y 7.2.2 de Packet Tracer aprovechando comandos compatibles y específicos para cada escenario.

Abstract

Thanks to the evolution of the technological means, it is necessary that as future professionals we be able to provide a comprehensive solution to problems with real applicability, for this reason we are an active part of the development of the deepening diploma in Cisco CCNA through the written support of the resolution of complex scenarios For its execution, versions 6.1.1 were used. and 7.2.2 of Packet Tracer taking advantage of compatible and specific commands for each scenario.

Introducción

El presente informe tiene como finalidad demostrar la ejecución practica de todos los conocimientos adquiridos durante el periodo académico establecido para el desarrollo del Diplomado de profundización de Cisco CCNA.

En este documento se plasman las evidencias que sustentan la simulación de dos escenarios diferentes en cuanto al manejo de redes, subredes, vlan además de protocolos de seguridad y enrutamiento que hacen más dinámica la transmisión de paquetes.

Objetivos

Objetivo general:
Realizar y desarrollar los escenarios propuestos como prueba de habilidades practicas del Diplomado de Profundización CCNA demostrando todos los conocimientos adquiridos durante este periodo académico.

Objetivos específicos:

- Analizar caso de uso propuesto.
- Establecer elementos para la configuración de una red.
- Estructurar la topología de red.
- Proponer estrategias para hacer eficaz la transmisión de datos.
- Parametrizar cada dispositivo de la red.
- Aplicar protocolos de seguridad para la conexión de dispositivos.
- Identificar las tablas de direccionamiento entre vecinos.
- Configurar acceso remoto vía Telnet.
- Crear listas de control de acceso entre componentes de la red.
- Realizar pruebas de transmisión de datos.

Desarrollo de escenarios

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.

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.

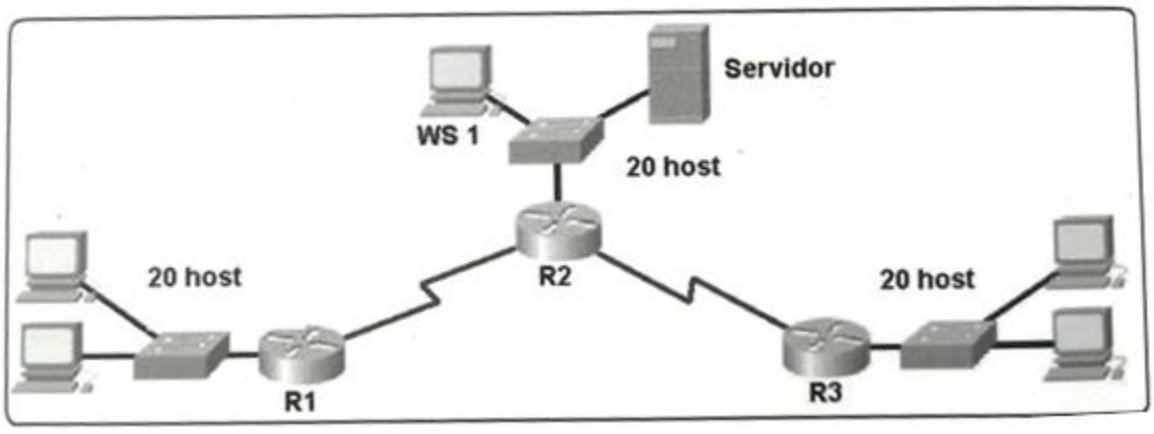

Figura 1.Diseño de red escenario 1.

Topología de red:

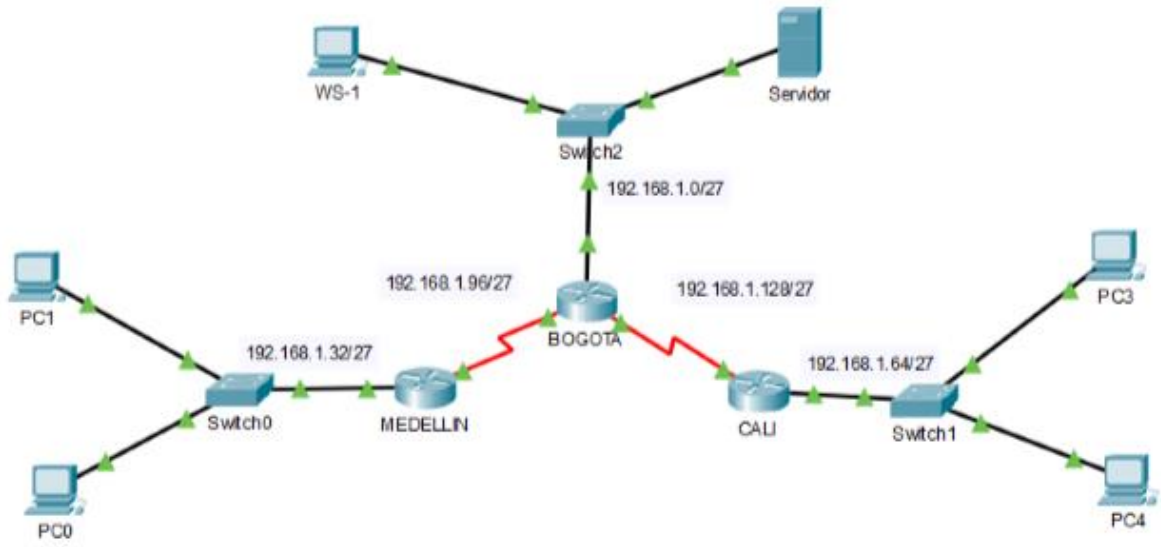

Figura 2.Topología de red escenario 1.

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

ROUTER MEDELLIN
Enable
Configure terminal
Hostname MEDELLIN
Enable secret class
Line vty 0 15
Password cisco
Exit
Line console 0
Password cisco
Exit
Service password-encryption
interface serial 0/0/0

ip address 192.168.1.99 255.255.255.224
exit
interface fastEthernet 0/0
ip address 192.168.1.33 255.255.255.224

ROUTER BOGOTA

Enable
Configure terminal
Hostname BOGOTA
Enable secret class
Line vty 0 15
Password cisco
Exit
Line console 0
Password cisco
Exit
Service password-encryption
interface serial 0/0/0
ip address 192.168.1.98 255.255.255.224
exit
interface serial 0/0/1
ip address 192.168.1.130 255.255.255.224
exit
interface fastEthernet 0/0
ip address 192.168.1.1 255.255.255.224

ROUTER CALI

Enable
Configure terminal
Hostname CALI
Enable secret class
Line vty 0 15
Password cisco
Exit
Line console 0
Password cisco
Exit
Service password-encryption
interface serial 0/0/0

ip address 192.168.1.131 255.255.255.224
exit
interface fastEthernet 0/0
ip address 192.168.1.65 255.255.255.224

- Realizar la conexión fisica de los equipos con base en la topología de red

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

Parte 1: Asignación de direcciones IP:

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

Parte 2: Configuración Básica.

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

Tabla 1.Direccionamiento

	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

b. Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

Enrutamiento:

ROUTER MEDELLIN:

Ip route 192.168.1.32 255.255.255.224 192.168.1.99
Ip route 192.168.1.64 255.255.255.224 192.168.1.99
Ip route 192.168.1.64 255.255.255.224 192.168.1.131

ROUTER BOGOTA:

Ip route 192.168.1.32 255.255.255.224 192.168.1.99
Ip route 192.168.1.64 255.255.255.224 192.168.1.99
Ip route 192.168.1.64 255.255.255.224 192.168.1.131

ROUTER CALI:

Ip route 192.168.1.32 255.255.255.224 192.168.1.130
Ip route 192.168.1.96 255.255.255.224 192.168.1.130
Ip route 192.168.1.0 255.255.255.224 192.168.1.130

c. Verificar el balanceo de carga que presentan los routers.
d. Realizar un diagnóstico de vecinos uando el comando cdp.

ROUTER MEDELLIN:

Enable

Show cdp neighbors

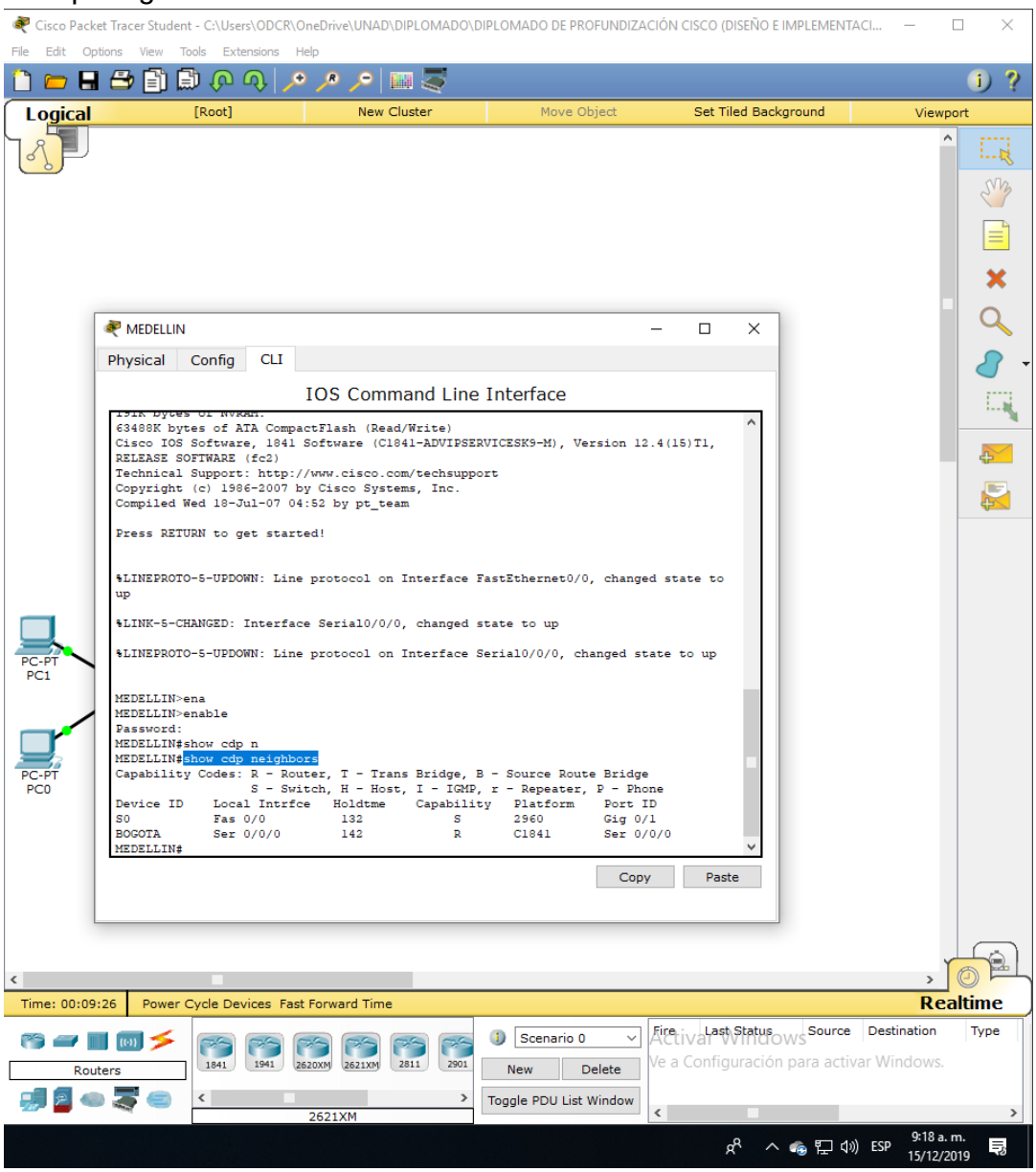

Figura 3.CDP Router Medellín.

ROUTER BOGOTA:

Enable

Show cdp neighbors

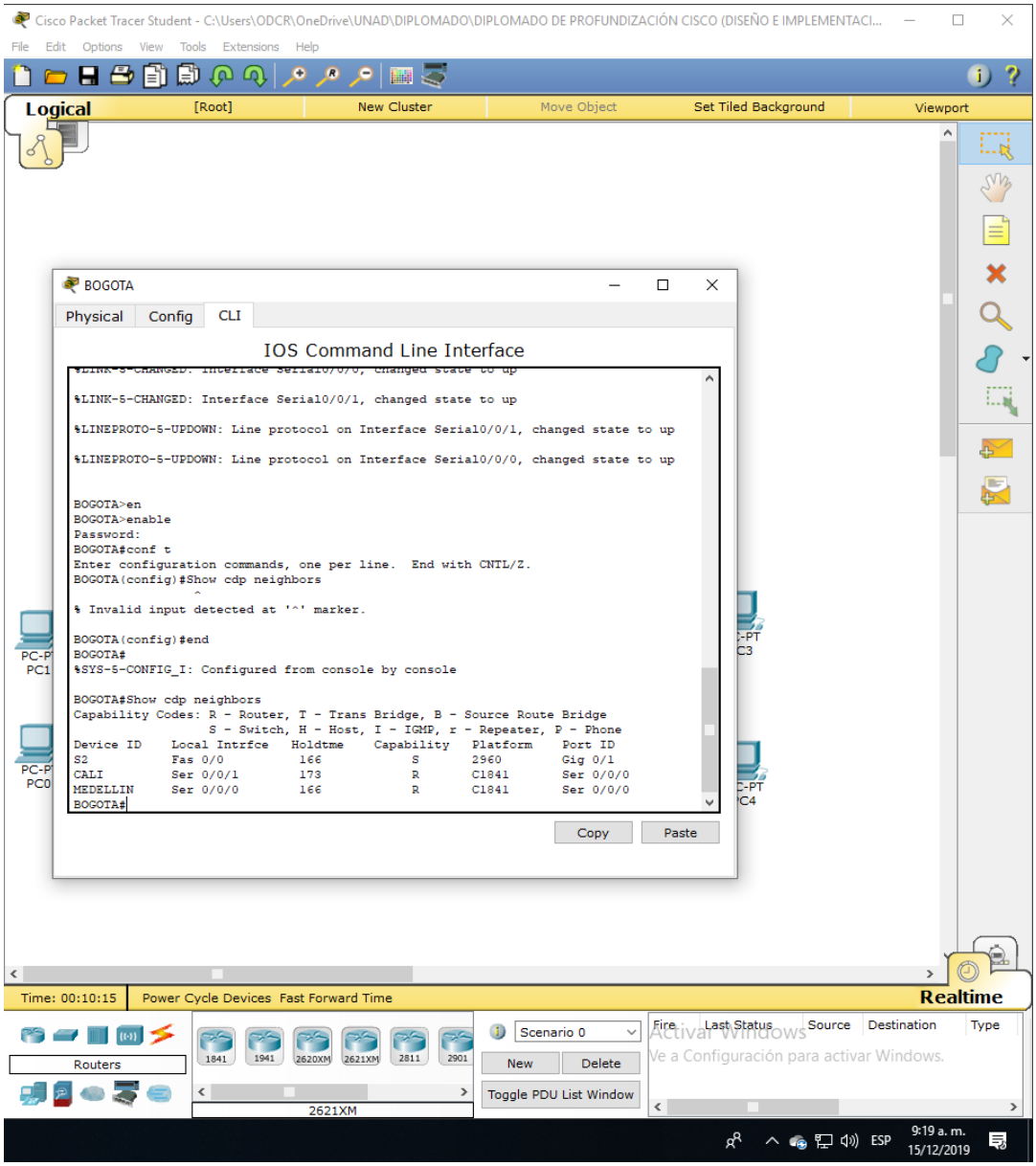

Figura 4.CDP Router Bogotá.

ROUTER CALI:

Enable

Show cdp neighbors

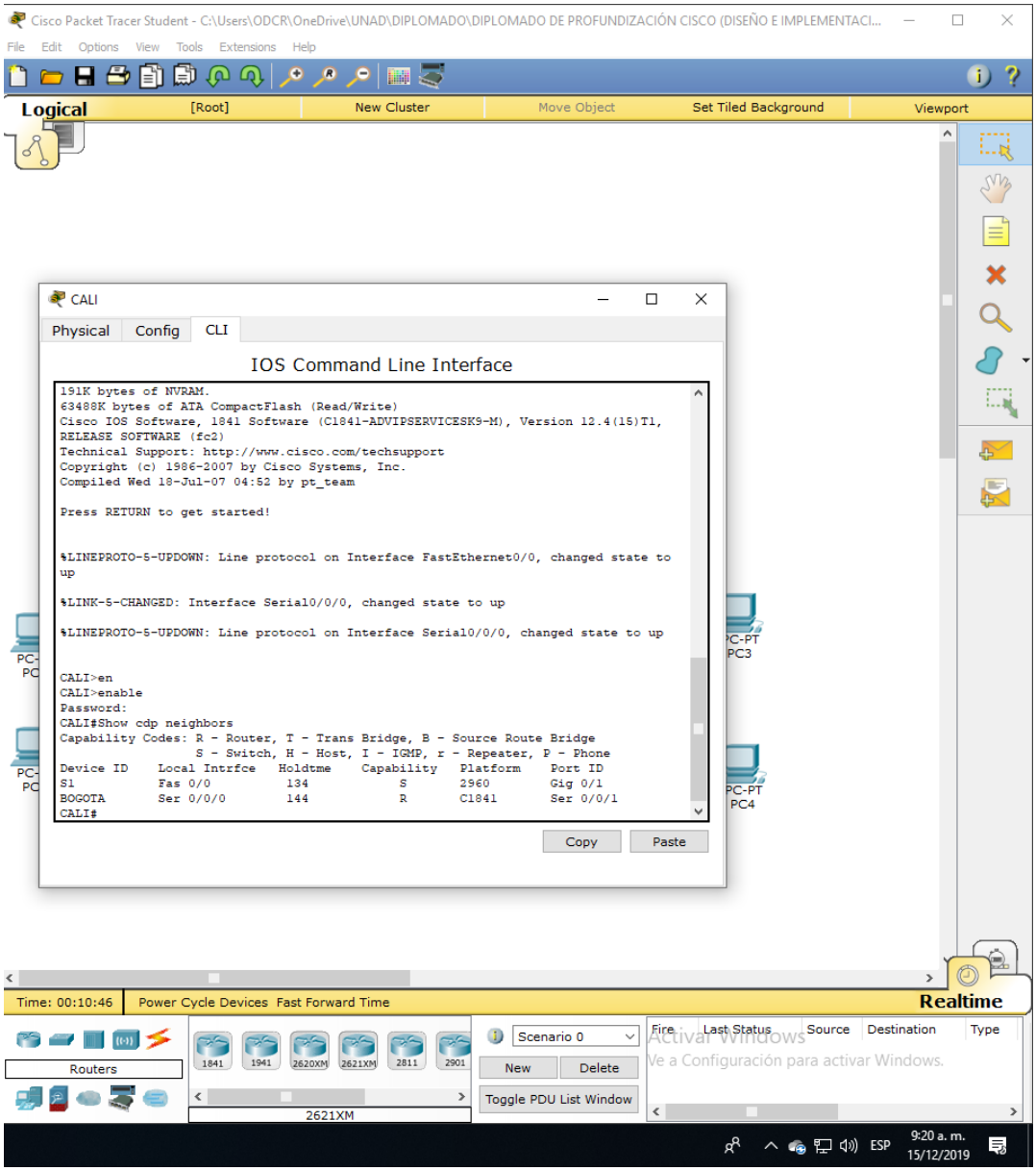

Figura 5.CDP Router Cali.

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

PC0:
Ping 192.168.1.67 (PC3)

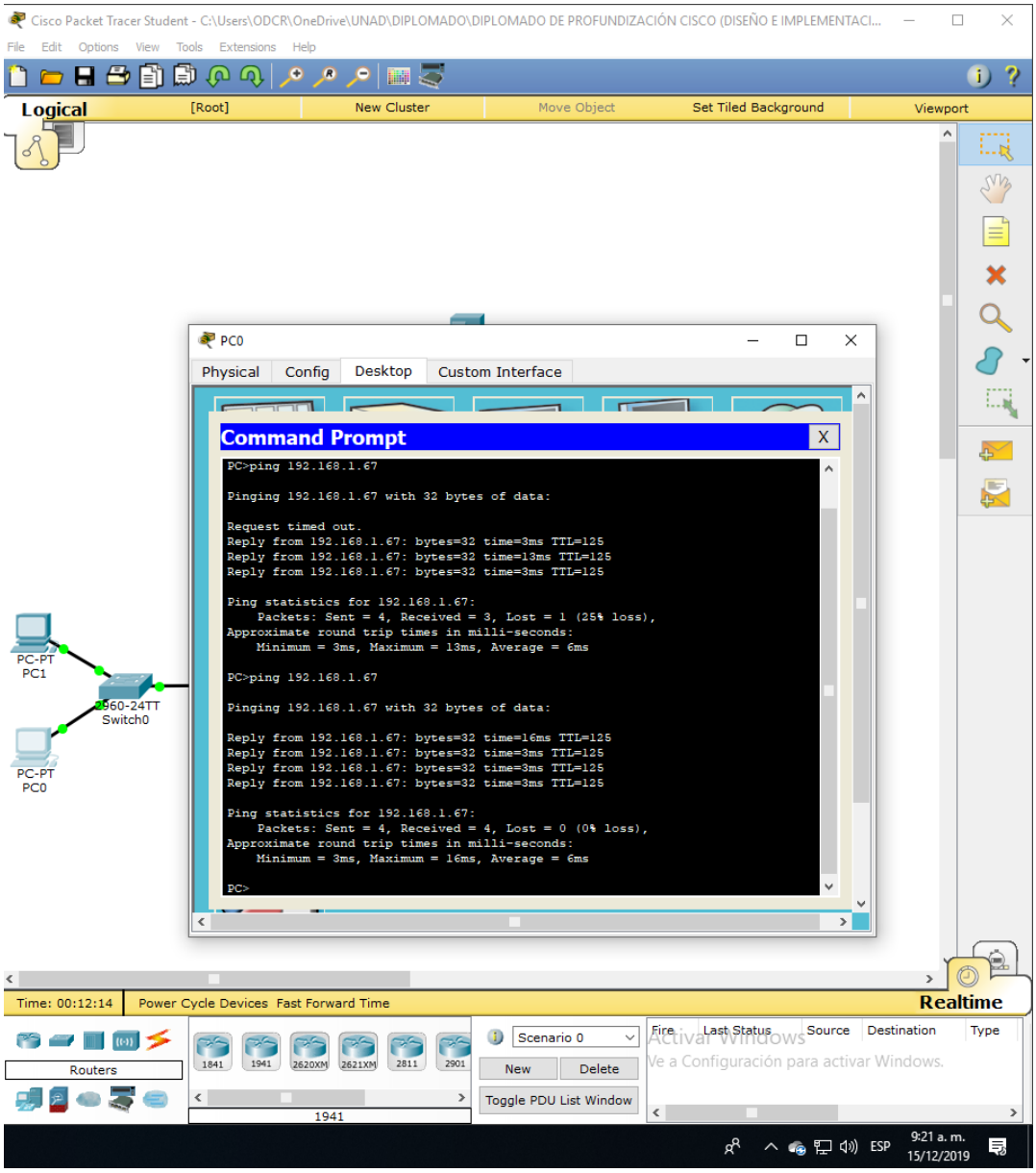

Figura 6.Prueba de Conectividad a PC3.

Ping 192.168.1.3 (WS-1)

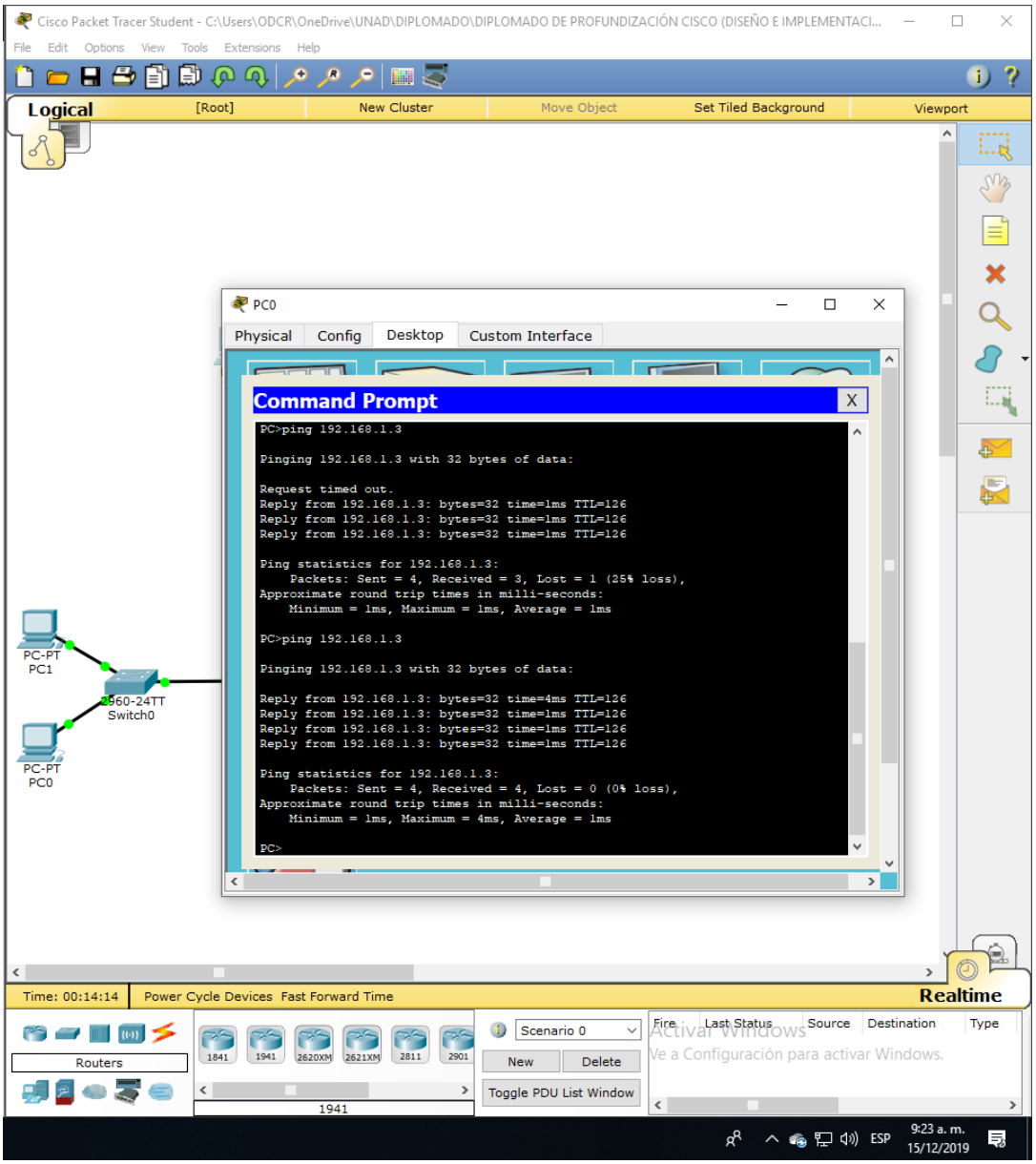

Figura 7.Prueba de Conectividad a WS-1.

PC4:
Ping 192.168.1.4 (Servidor)

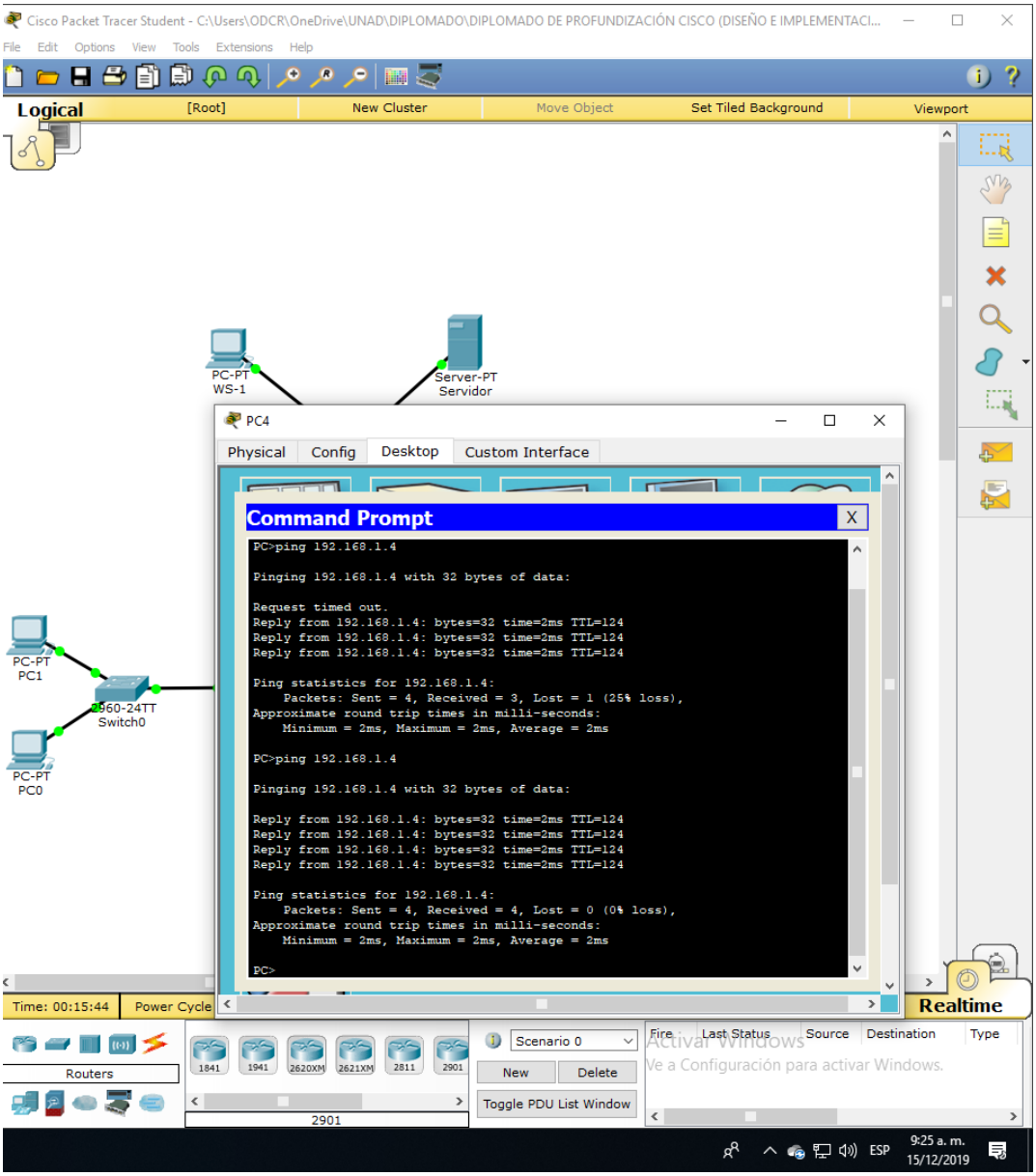

Figura 8.Prueba de Conectividad a Servidor.

Parte 3: Configuración de Enrutamiento.

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

ROUTER MEDELLIN:

Enable
Configure terminal
Router eigrp 200
Network 192.168.1.0

ROUTER BOGOTA:

Enable
Configure terminal
Router eigrp 200
Network 192.168.1.0

ROUTER CALI:

Enable
Configure terminal
Router eigrp 200
Network 192.168.1.0

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

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

ROUTER MEDELLIN:

Show ip route

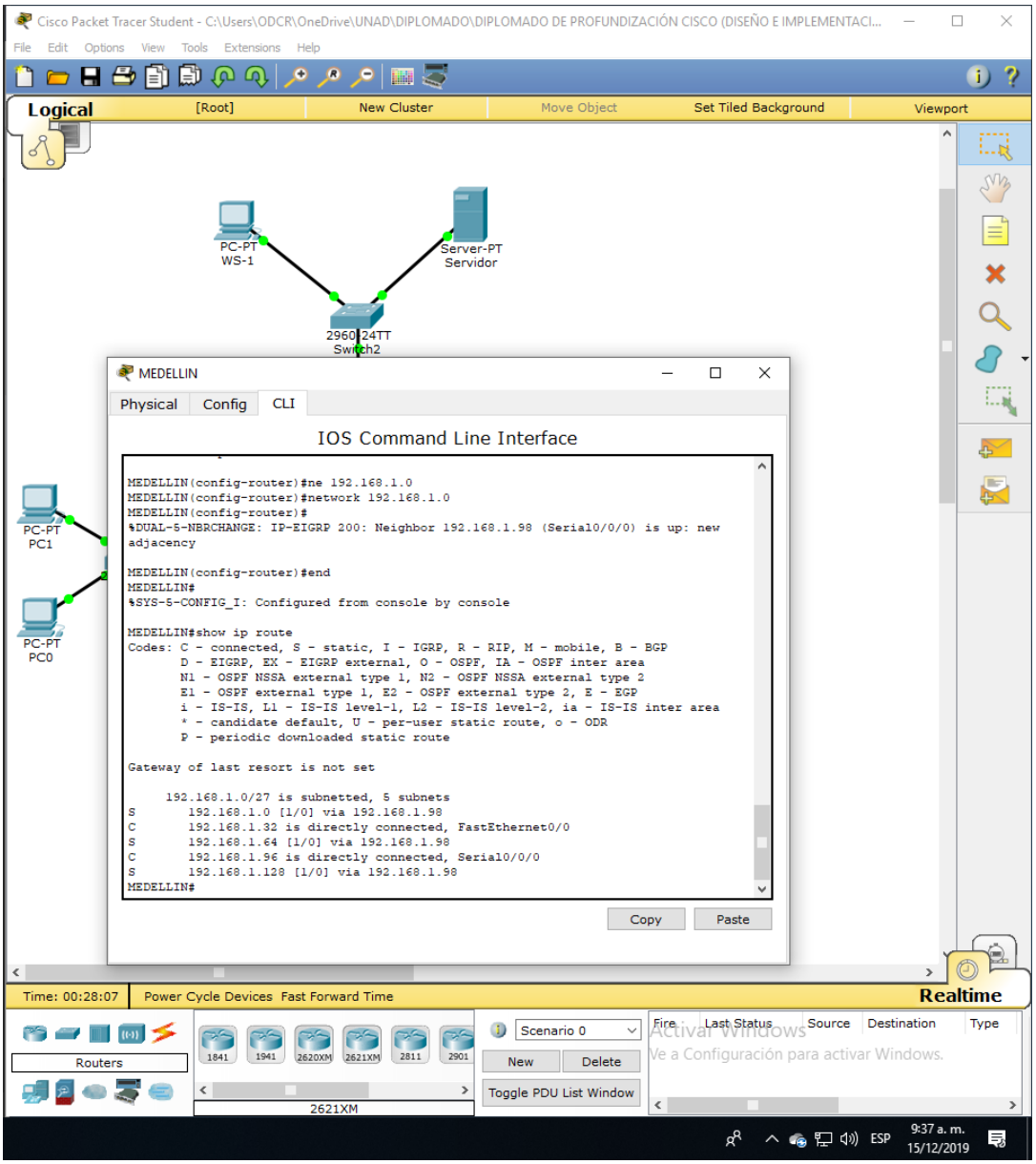

Figura 9.Tabla de direccionamiento Router Medellín.

ROUTER BOGOTA:

Show ip route

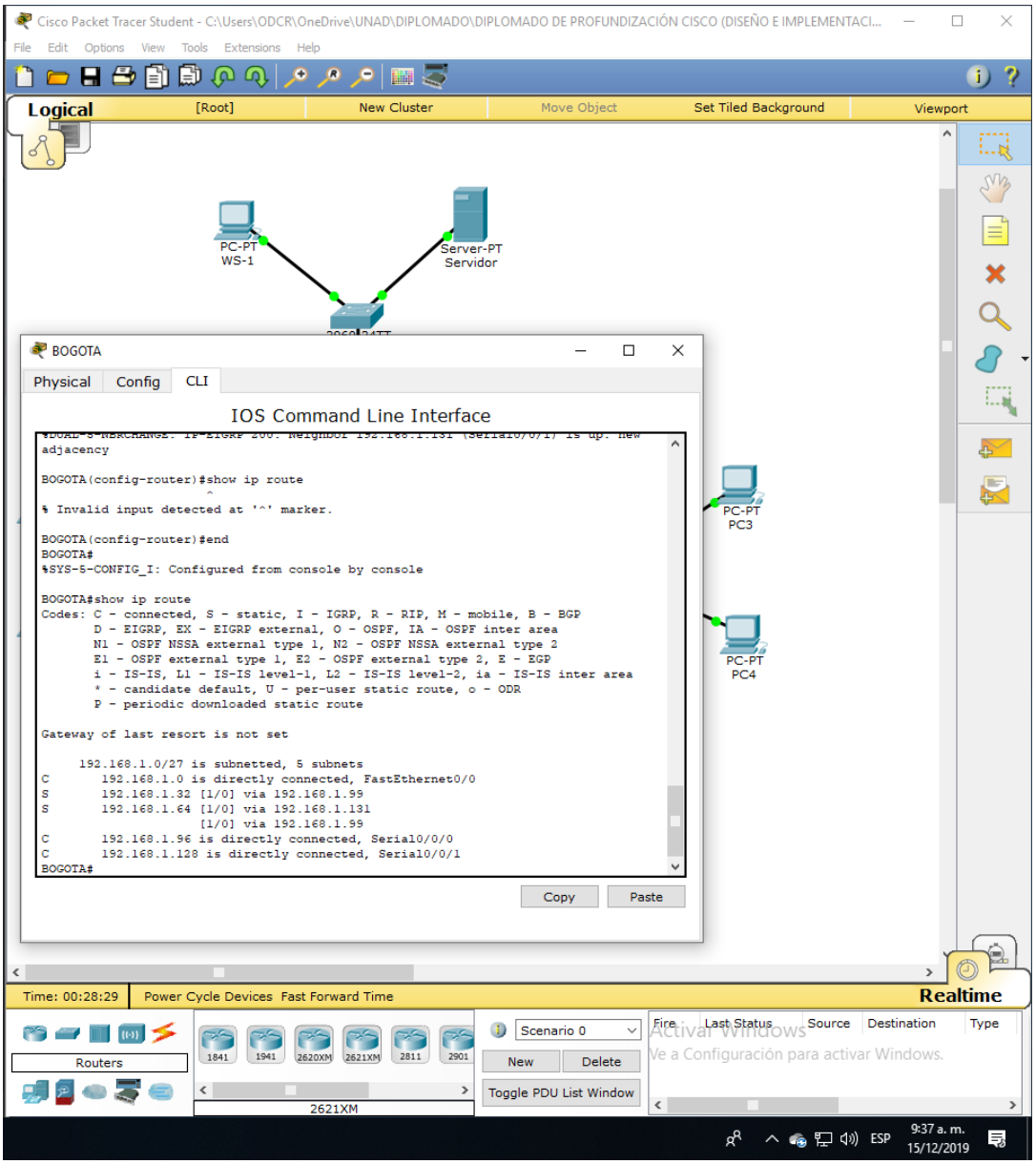

Figura 10.Tabla de direccionamiento Router Bogotá.

ROUTER CALI:
Show ip route

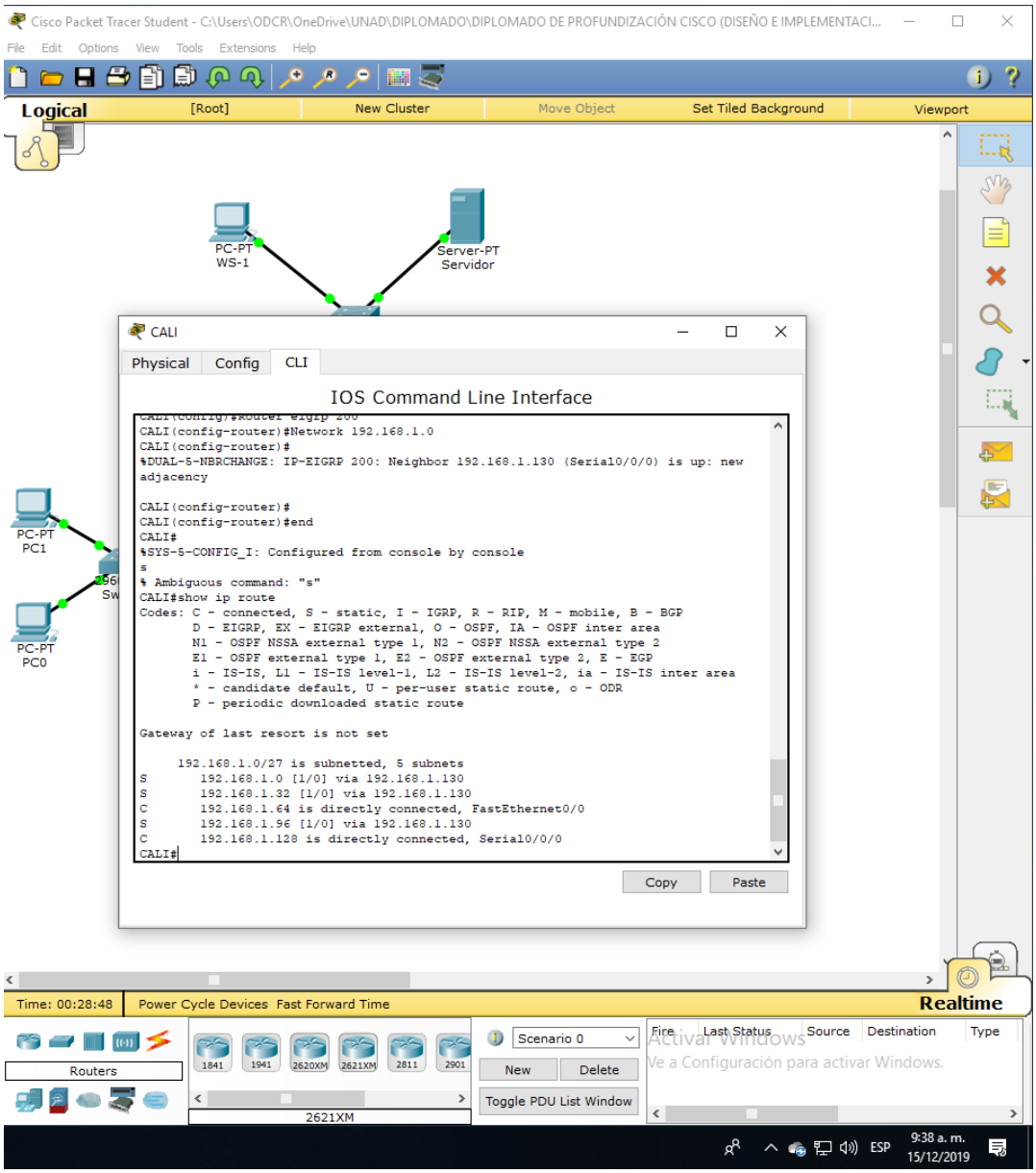

Figura 11.Tabla de direccionamiento Router Cali.

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

PC4 (HOST ROUTER CALI) a PC0(HOST ROUTER MEDELLIN)

Ping 192.168.1.34

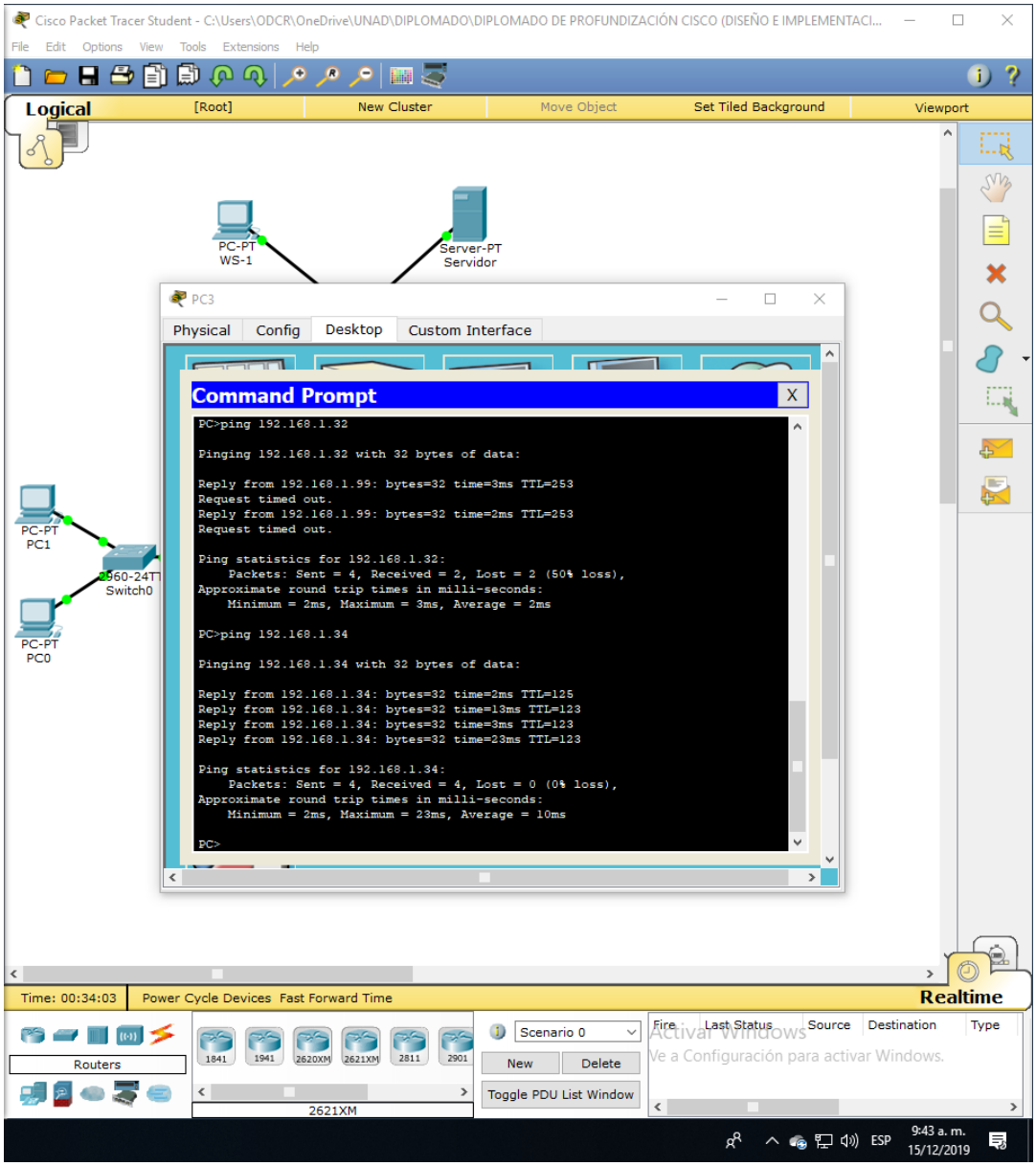

Figura 12.Ping PC0

PC4 (HOST ROUTER CALI) a Servidor (HOST ROUTER BOGOTA)
Ping 192.168.1.4

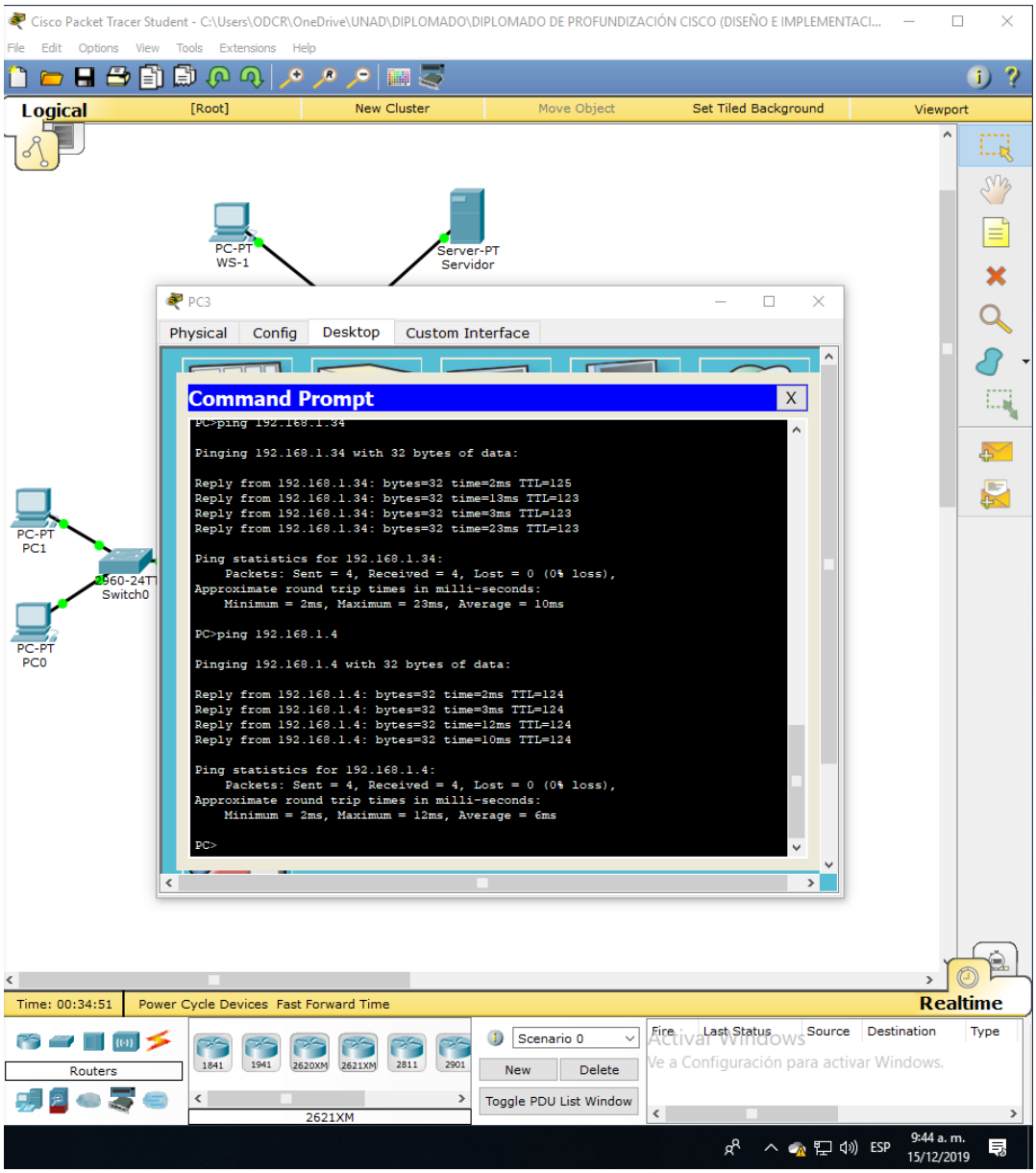

Figura 13.Ping a Servidor

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:

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

ROUTER MEDELLIN

Enable
Configure terminal
Line vty 0 15
Password cisco
Exit

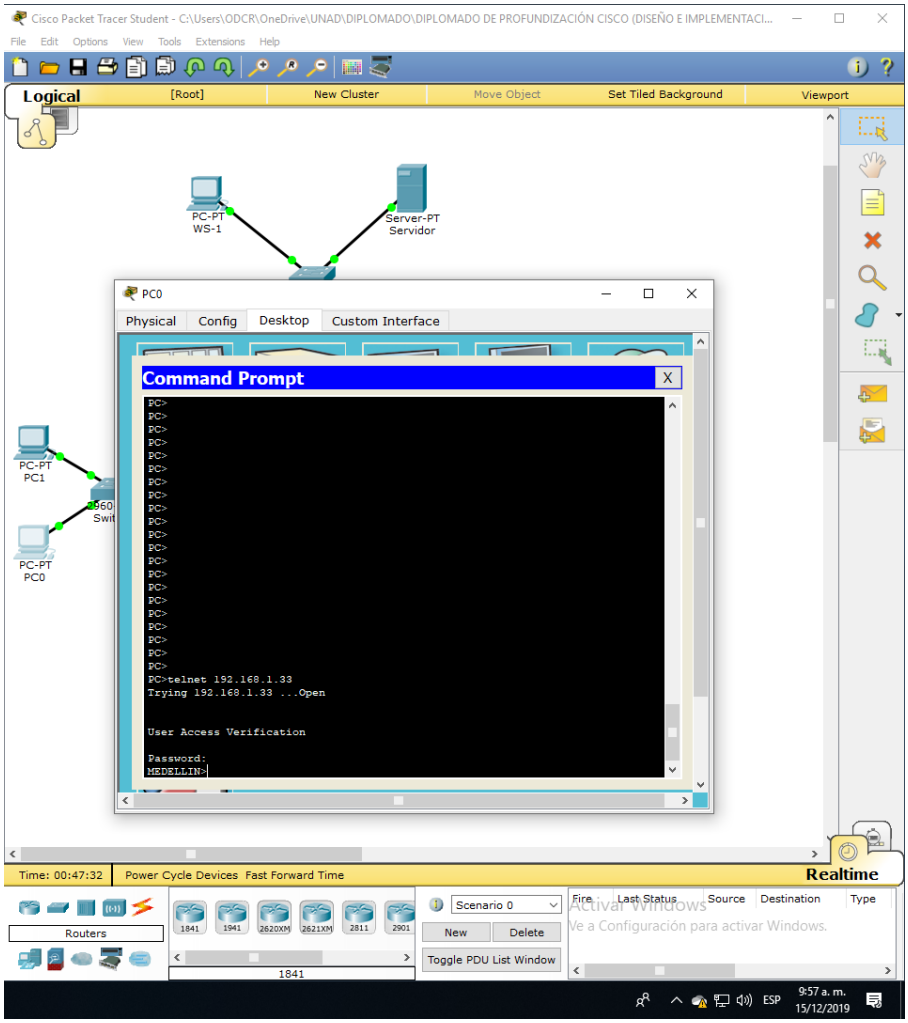

Figura 14.Habilitacion Telnet Router Medellín.

ROUTER BOGOTA

Enable
Configure terminal
Line vty 0 15
Password cisco
Exit

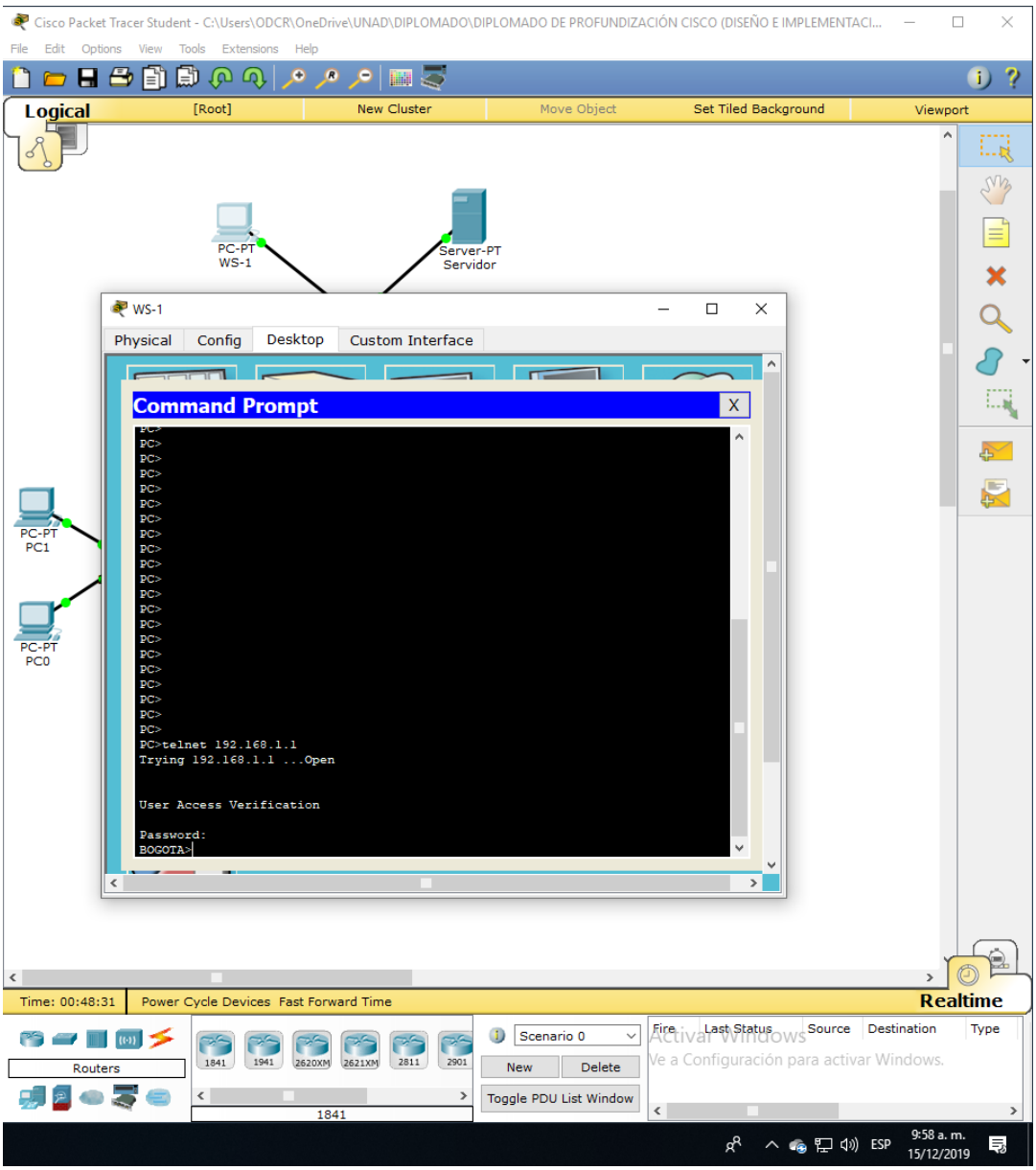

Figura 15.Habilitacion Telnet Router Bogotá

ROUTER CALI

Enable
Configure terminal
Line vty 0 15
Password cisco
exit

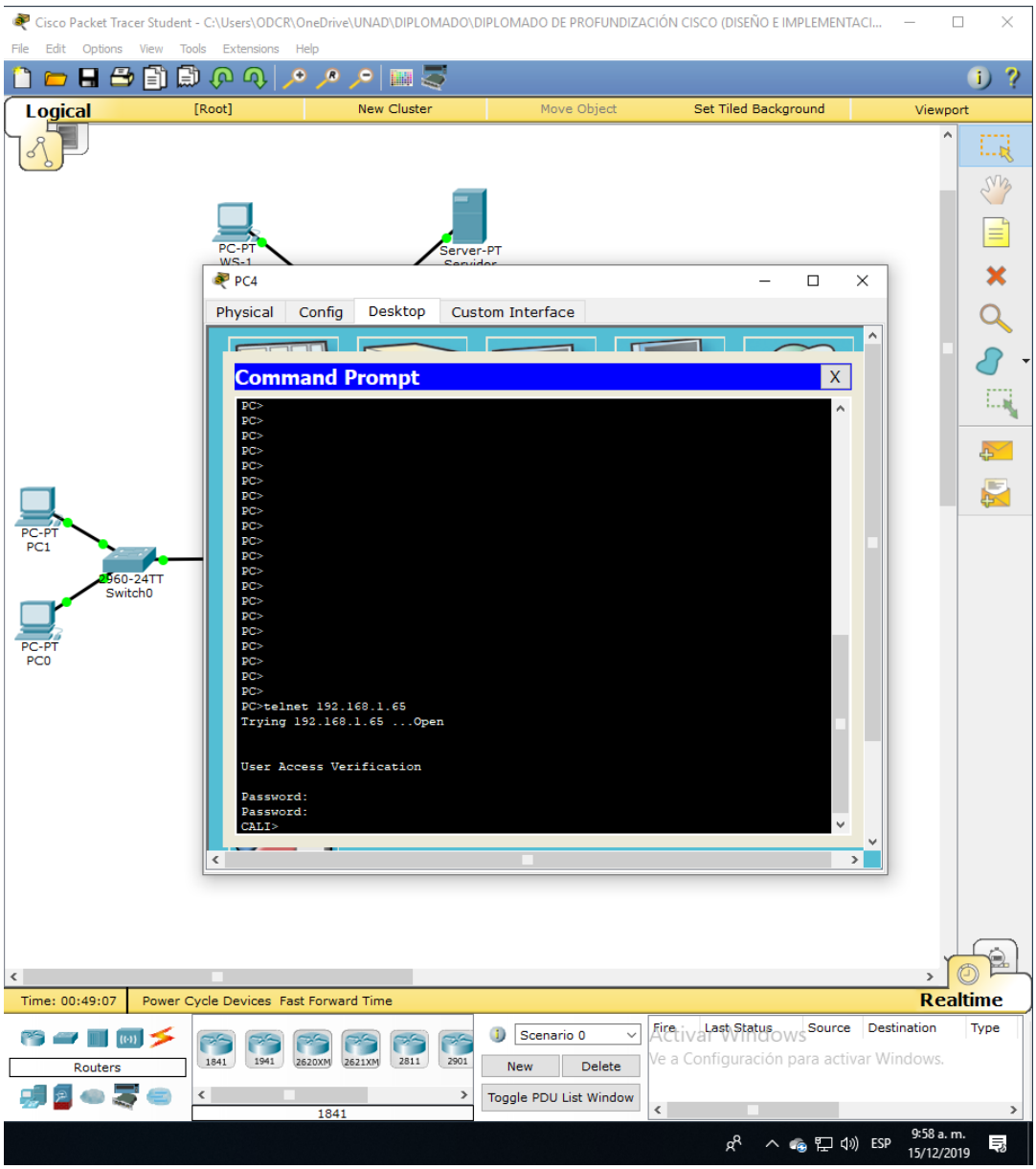

Figura 16.Habilitacion Telnet Router Cali.

a. El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.
b. Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor.

Parte 5: 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.

Tabla 2.Pruebas funcionales.

	ORIGEN	DESTINO	RESULTADO
TELNET	**Router MEDELLIN**	Router CALI	CONEXION
	WS_1	Router BOGOTA	DESCONEXION
	Servidor	Router CALI	CONEXIÓN
	Servidor	Router MEDELLIN	CONEXION
TELNET	**LAN del Router MEDELLIN**	Router CALI	DESCONEXION
	LAN del Router CALI	Router CALI	DESCONEXION
	LAN del Router MEDELLIN	Router MEDELLIN	DESCONEXION
	LAN del Router CALI	Router MEDELLIN	DESCONEXION
PING	**LAN del Router CALI**	WS_1	DESCONEXION
	LAN del Router MEDELLIN	WS_1	DESCONEXION
	LAN del Router MEDELLIN	LAN del Router CALI	DESCONEXIÓN
PING	**LAN del Router CALI**	Servidor	CONEXIÓN
	LAN del Router MEDELLIN	Servidor	CONEXIÓN
	Servidor	LAN del Router MEDELLIN	CONEXIÓN
	Servidor	LAN del Router CALI	CONEXIÓN
	Router CALI	LAN del Router MEDELLIN	DESCONEXION
	Router MEDELLIN	LAN del Router CALI	CONEXION

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.

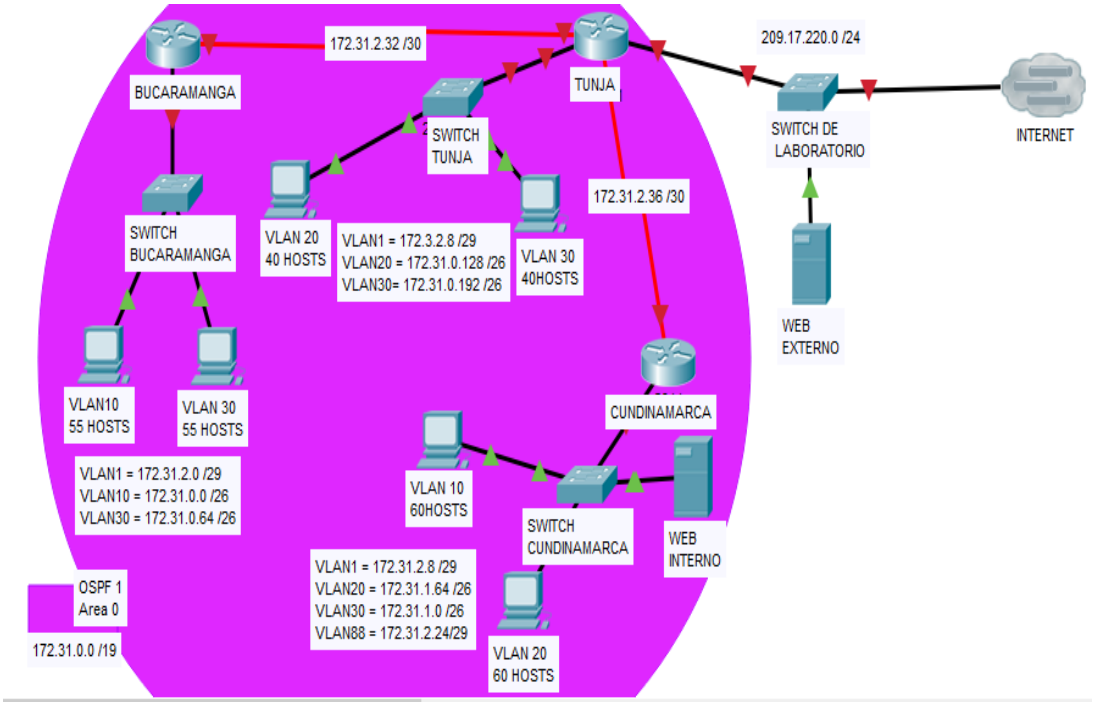

Figura 17.Diseño de red escenario 2.

Topología de red

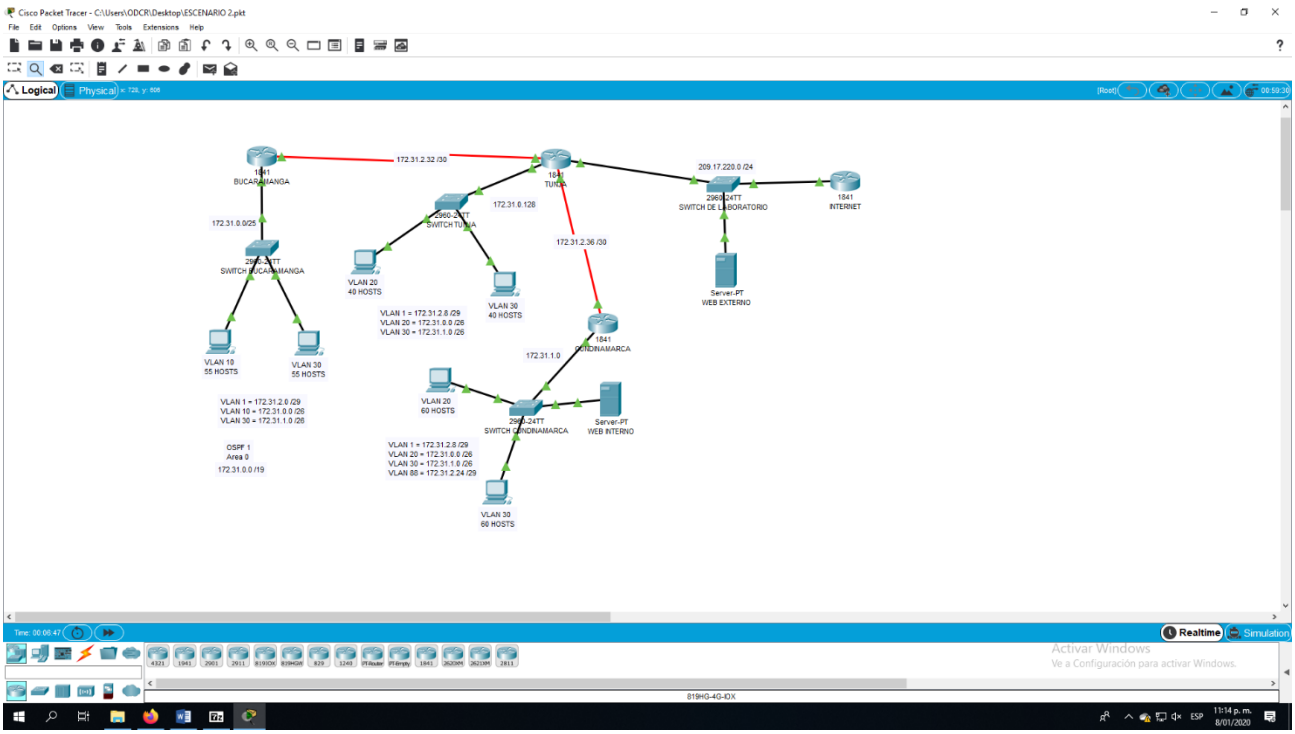

Figura 18.Topología de red escenario 2.

Desarrollo

Los siguientes son los requerimientos necesarios:

Parte 1: Configuración básica

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.

ROUTER CUNDINAMARCA

Enable
Configure terminal

Hostname CUNDINAMARCA

no ip domain-lookup

enable secret class

username CISCO password CLASS

aaa new-model

aaa authentication login LOCAL local

line console 0

password cisco

login authentication LOCAL

exec-timeout 5 0

line vty 0 15

login authentication LOCAL

password cisco

exec-timeout 5 0

exit

banner motd #

Prohibido el acceso a personal no autorizado#

service password-encryption

login block-for 300 attempt 3 within 60

exit

copy running-config startup-config

int s0/0/0

ip address 172.31.2.38 255.255.255.252

no shutdown

int fa0/1

ip address 172.31.1.1 255.255.255.128

no shutdown

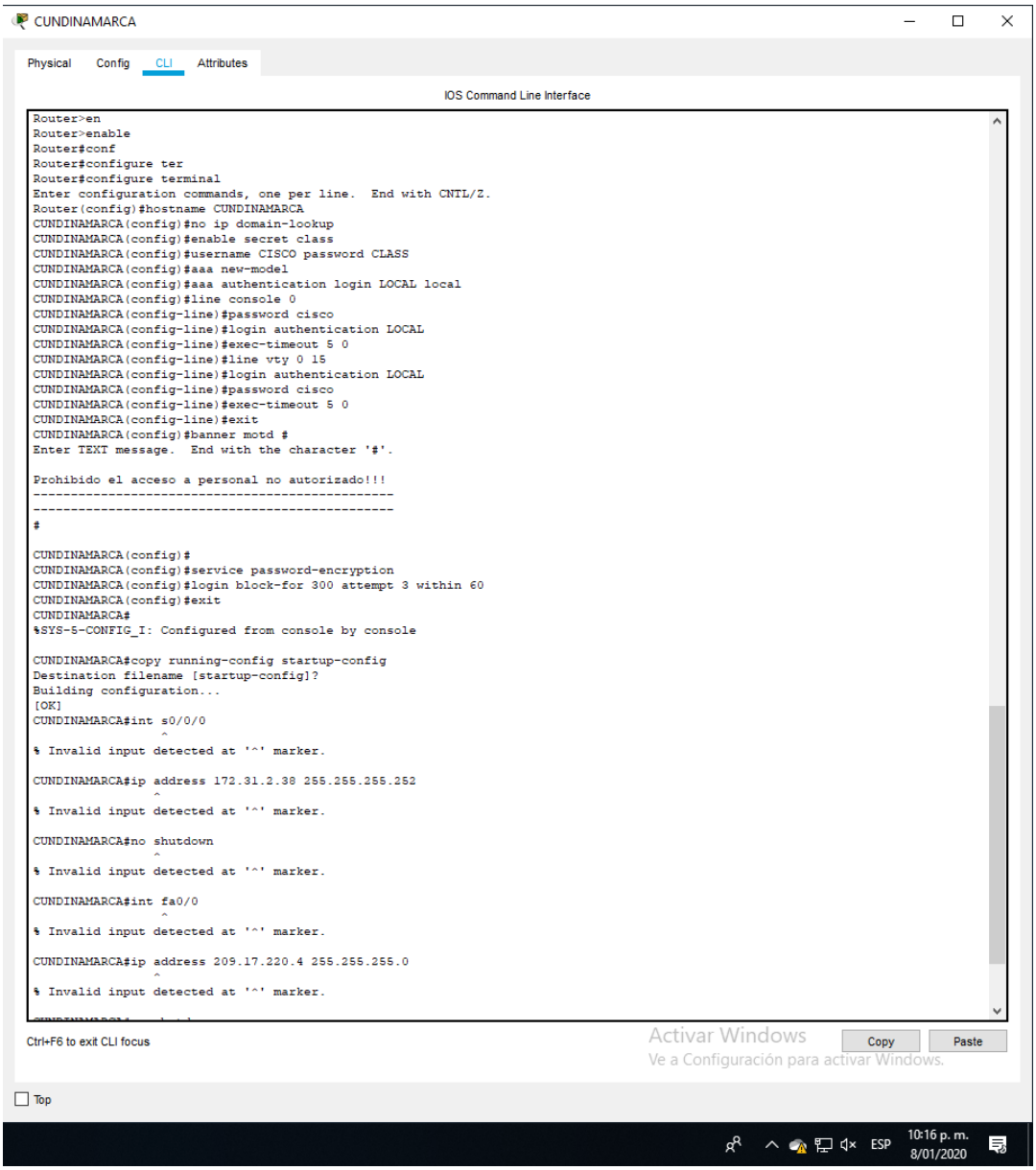

Figura 19. Configuración básica router CUNDINAMARCA.

ROUTER TUNJA

Enable
Configure terminal

Hostname TUNJA

no ip domain-lookup

enable secret class

```
username CISCO password CLASS
aaa new-model
aaa authentication login LOCAL local
line console 0
password cisco
login authentication LOCAL
line vty 0 15
login authentication LOCAL
password cisco
exit
int fa0/0
ip address 209.17.220.4 255.255.255.0
no shutdown
banner motd #
Prohibido el acceso a personal no autorizado #
service password-encryption
line console 0
exec-timeout 5 0
line vty 0 15
exec-timeout 5 0
exit
login block-for 300 attempt 3 within 60
exit
copy running-config startup-config
```

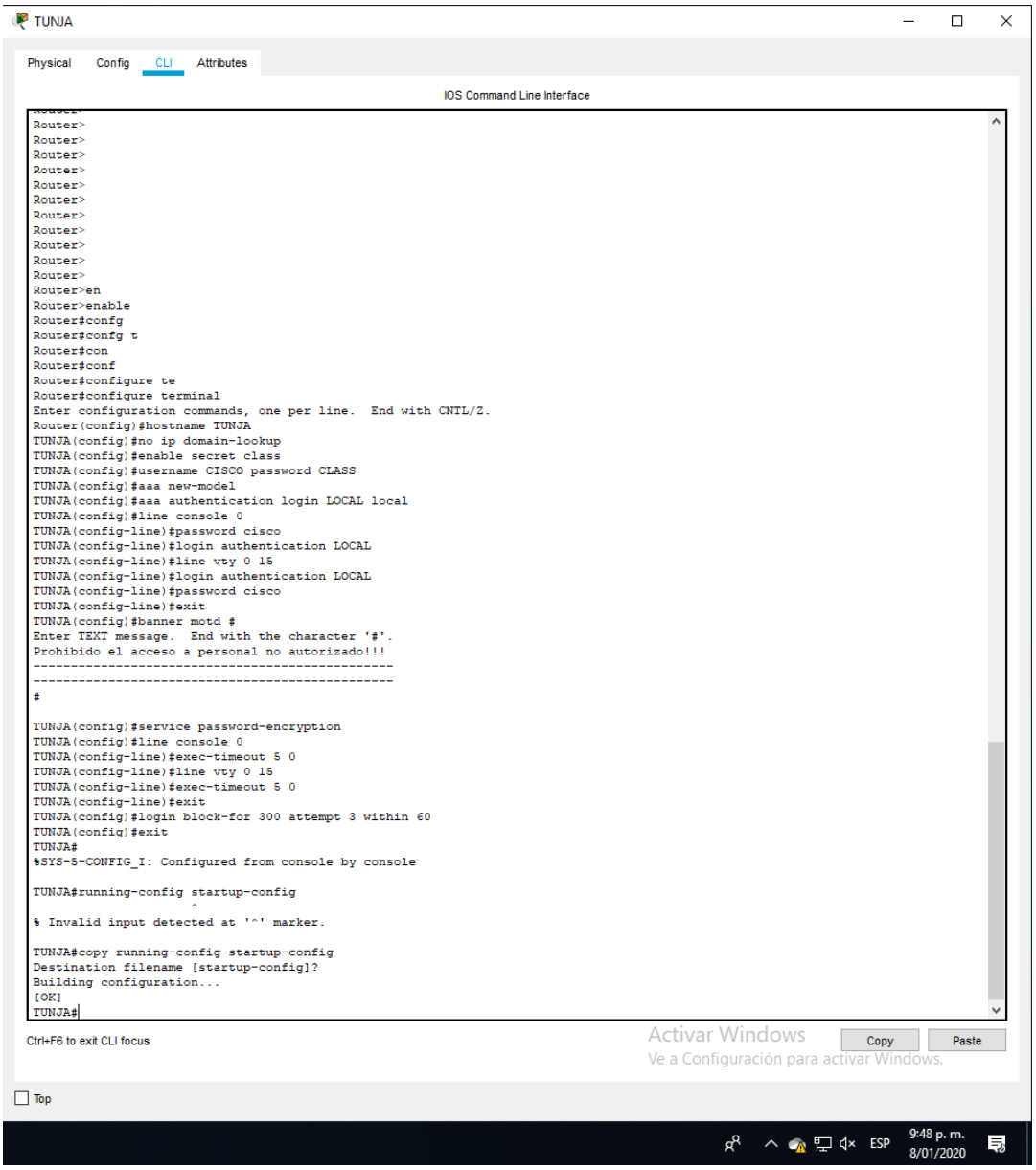

Figura 20. Configuración básica router TUNJA 1.

int fa0/0

no ip address 209.17.220.3 255.255.255.0

ip address 209.17.220.1 255.255.255.0

exit

int fa0/0

ip address 172.31.0.129 255.255.255.128
no shutdown

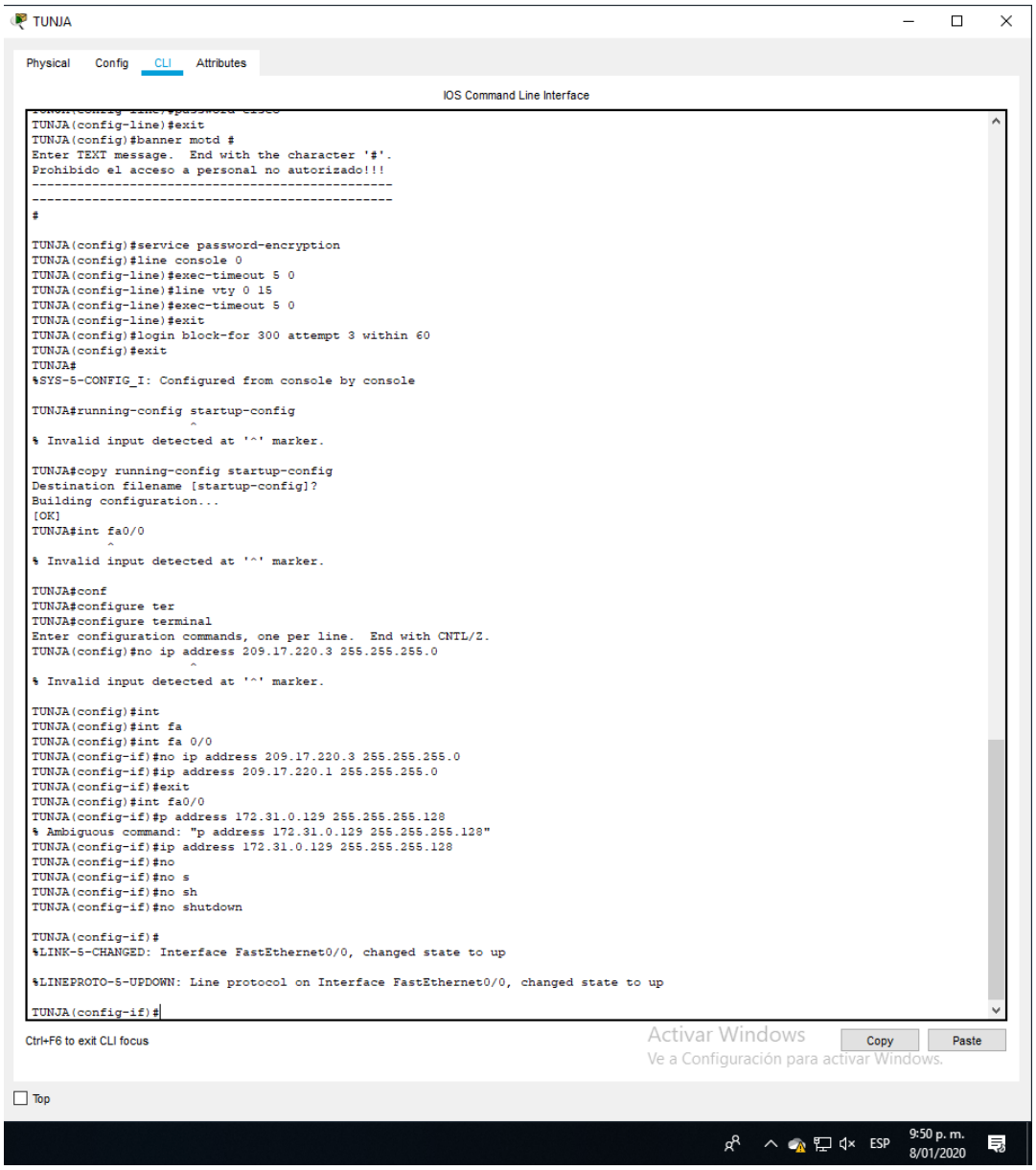

Figura 21. Configuración básica router TUNJA 2.

ROUTER BUCARAMANGA

```
Enable
Configure terminal
Hostname BUCARAMANGA
no ip domain-lookup
enable secret class
username CISCO password CLASS
aaa new-model
aaa authentication login LOCAL local
line console 0
password cisco
login authentication LOCAL
exec-timeout 5 0
line vty 0 15
password cisco
login authentication LOCAL
exec-timeout 5 0
exit
banner motd #
Prohibido el acceso a personal no autorizado#
service password-encryption
login block-for 300 attempt 3 within 60
exit
copy running-config startup-config
int s0/0/0
ip address 172.31.2.34 255.255.255.252
no shutdown
int fa0/0
```

ip address 172.31.0.129 255.255.255.128
no shutdown

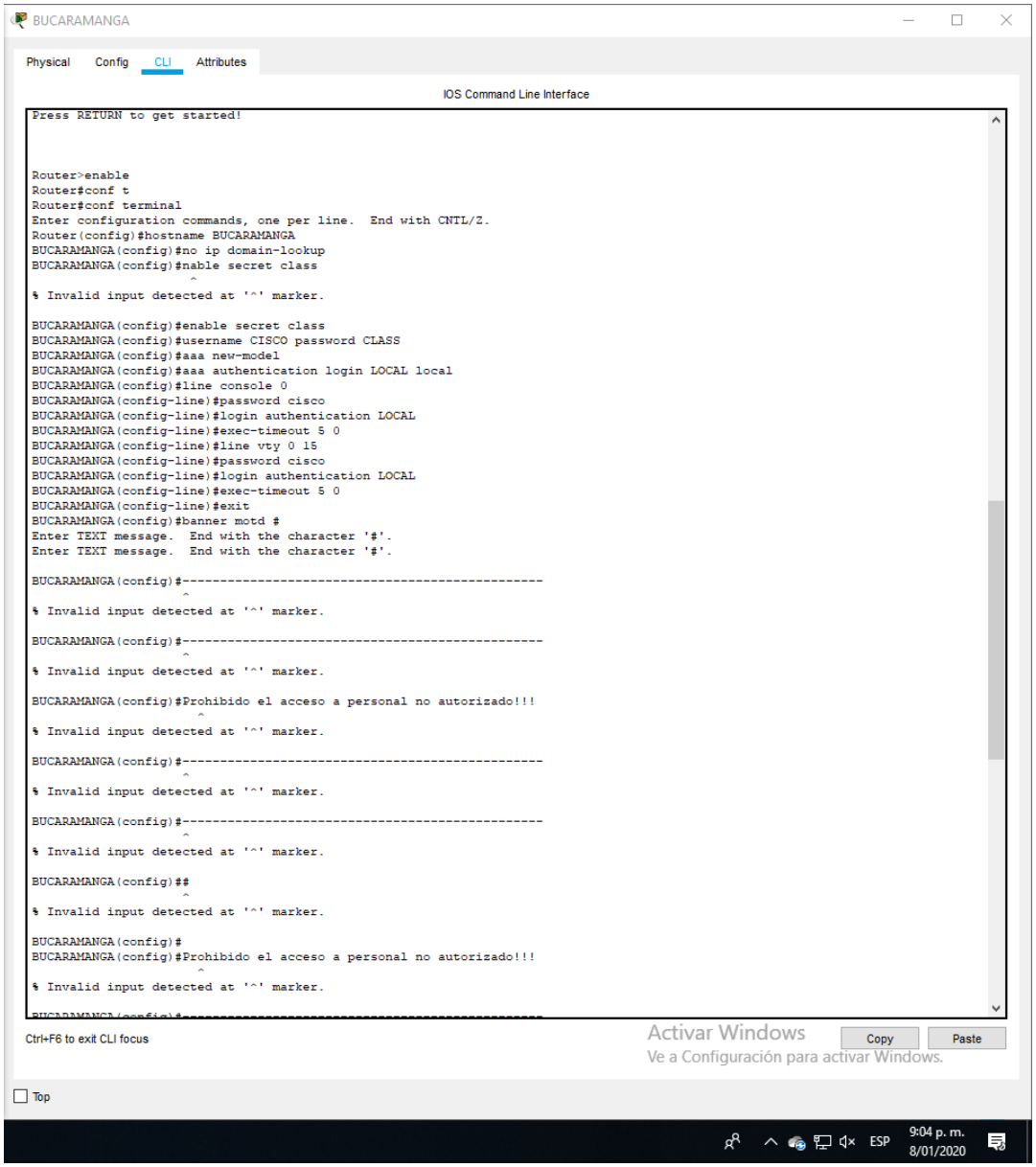

Figura 22. Configuración básica router BUCARAMANGA 1.

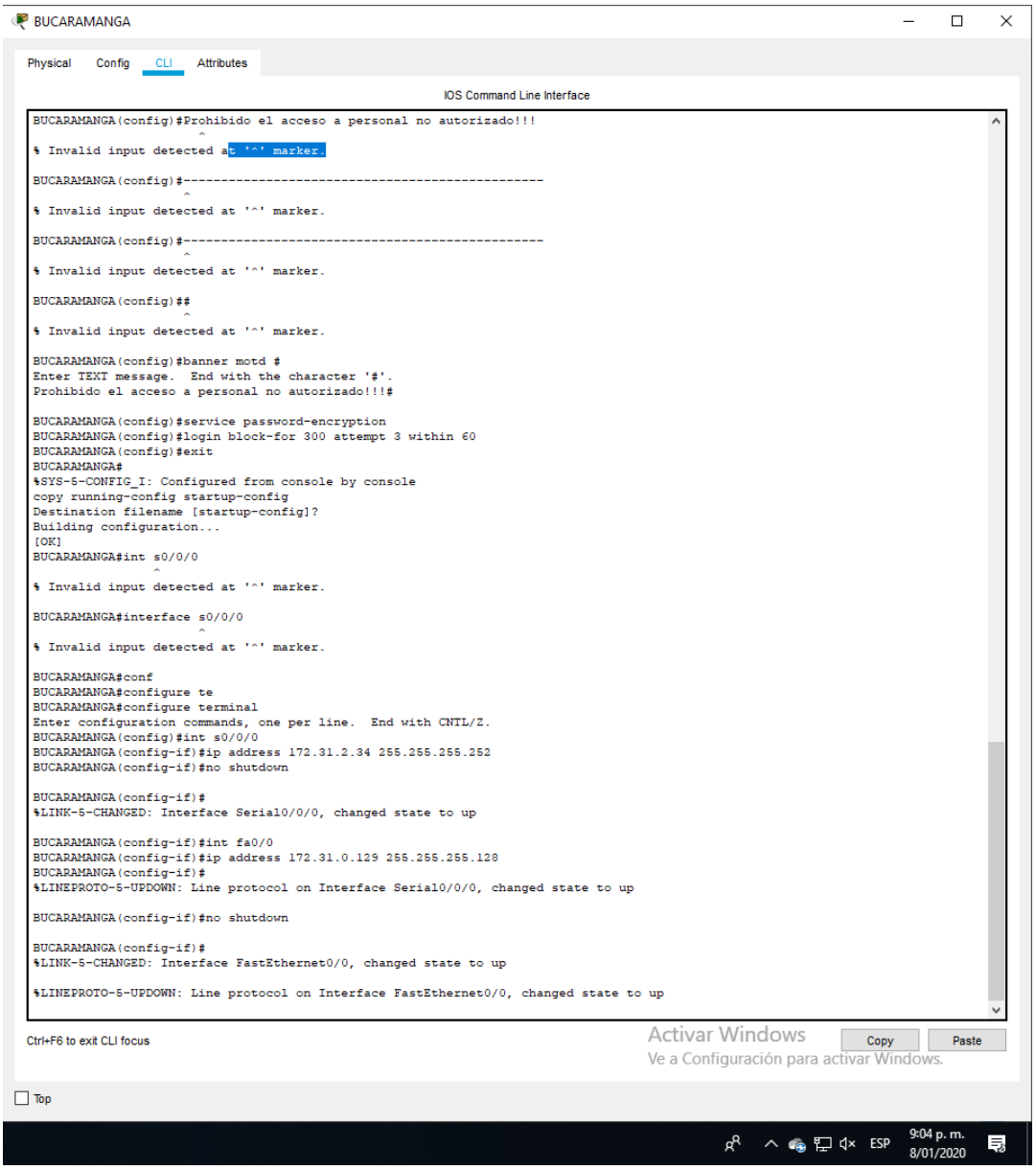

Figura 23. Configuración básica router BUCARAMANGA 2.

Parte 2: Creación servidores TFTP y almacenamiento de archivos

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

ROUTER CUNDINAMARCA

show flash

copy flash tftp

Figura 24. Activación servidor TFTP router CUNDINAMARCA.

ROUTER TUNJA

show flash

copy flash tftp

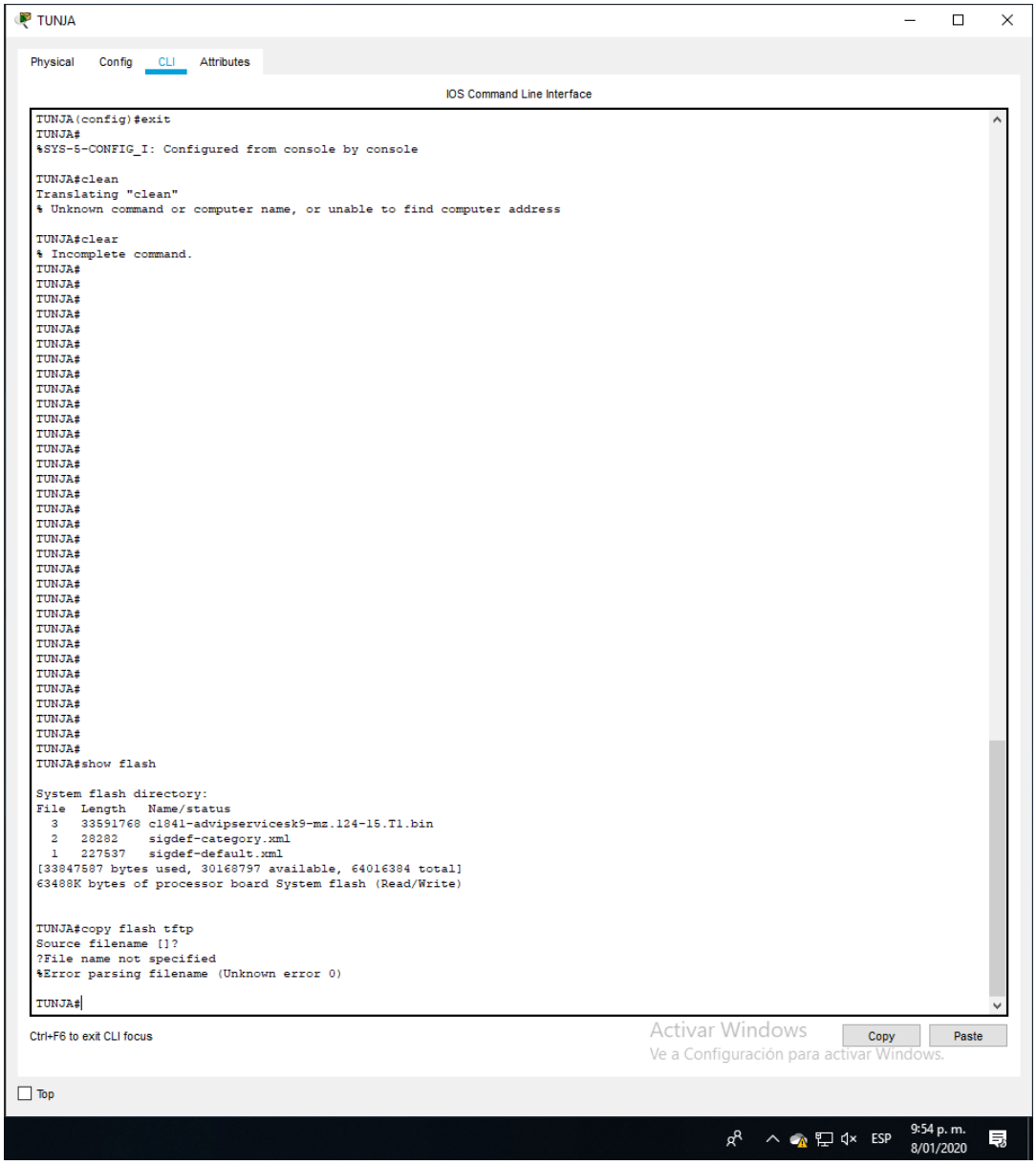

Figura 25. Activación servidor TFTP router TUNJA.

ROUTER BUCARAMANGA

show flash
copy flash tftp

Figura 26. Activación servidor TFTP router BUCARAMANGA.

Parte 3: Creación de NAT y enrutamiento

- El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).
- El enrutamiento deberá tener autenticación.
- Listas de control de acceso

ROUTER CUNDINAMARCA

```
nat pool NATCUND 172.31.2.37 172.31.2.38 netmask 255.255.255.252
access-list 1 permit 172.31.1.0 0.0.0.63
ip nat inside source list 1 pool NATCUND overload
access-list 2 permit 172.31.0.0 0.0.0.63
ip nat inside source list 2 pool NATCUND overload
int fa0/0
ip nat inside
int s0/0/0
ip nat outside
```

Figura 27.Asignación NAT router CUNDINAMARCA.

ROUTER TUNJA

ip nat inside source static 209.17.220.4 172.31.2.33

int fa0/0

ip nat inside

int s0/0/0

ip nat outside

ip nat pool NATPOOL 172.31.2.33 172.31.2.34 netmask 255.255.255.252

access-list 1 permit 172.31.0.0 0.0.0.63

access-list 2 permit 172.31.1.0 0.0.0.63

ip nat inside source list 1 pool NATPOOL overload

ip nat inside source list 2 pool NATPOOL overload

int fa0/1

ip nat inside

int s0/0/0

ip nat outside

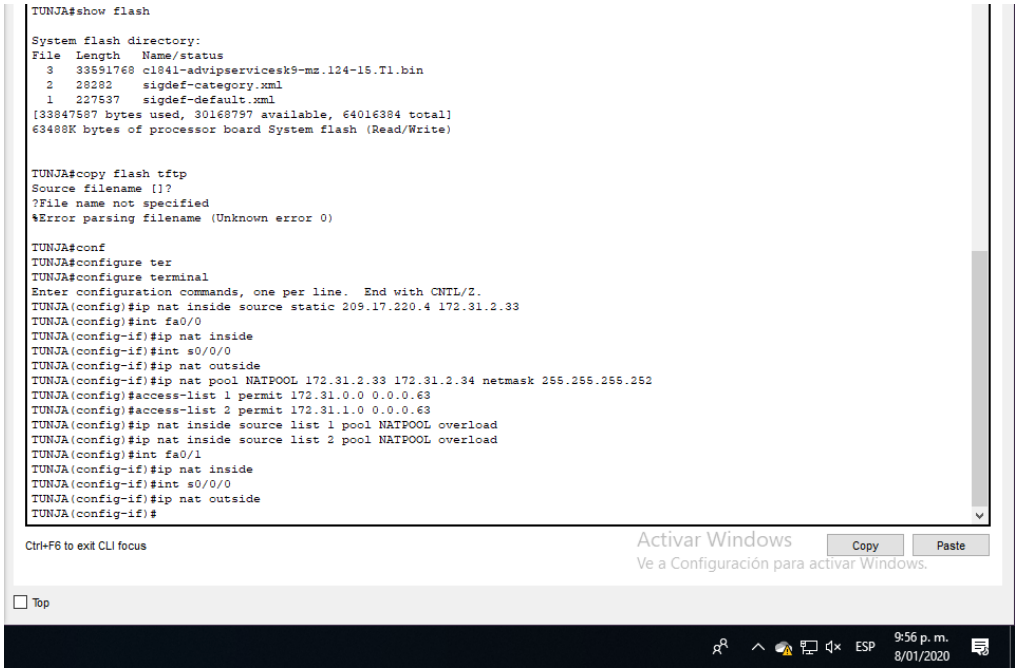

Figura 28.Asignacin NAT router TUNJA.

ROUTER BUCARAMANGA

ip nat pool NATBUC 172.31.2.33 172.31.2.34 netmask 255.255.255.252

access-list 1 permit 172.31.0.0 0.0.0.63

access-list 2 permit 172.31.1.0 0.0.0.63

ip nat inside source list 1 pool NATBUC overload

ip nat inside source list 2 pool NATBUC overload

int fa0/0

ip nat inside

int s0/0/0

ip nat outside

Figura 29.Asignación NAT router BUCARAMANGA.

Parte 4: Asignación de máscaras de red variable

- VLSM: utilizar la dirección 172.31.0.0 /18 para el direccionamiento.

Parte 5: Creación de listas de acceso

ROUTER CUNDINAMARCA

access-list 100 deny ip host 172.31.0.1 200.17.220.2 0.0.0.255
access-list 100 permit ip host 172.31.0.1 172.31.0.20 0.0.0.63
access-list 100 permit ip host 172.31.0.1 172.31.1.15 0.0.0.63
int fa0/0
ip access-group 100 out
no shutdown
access-list 102 permit ip host 172.31.0.2 200.17.220.2 0.0.0.255
access-list 102 deny ip host 172.31.0.2 172.31.0.20 0.0.0.63
access-list 102 deny ip host 172.31.0.2 172.31.1.15 0.0.0.63
int fa0/0
ip access-group 102 out
no shutdown

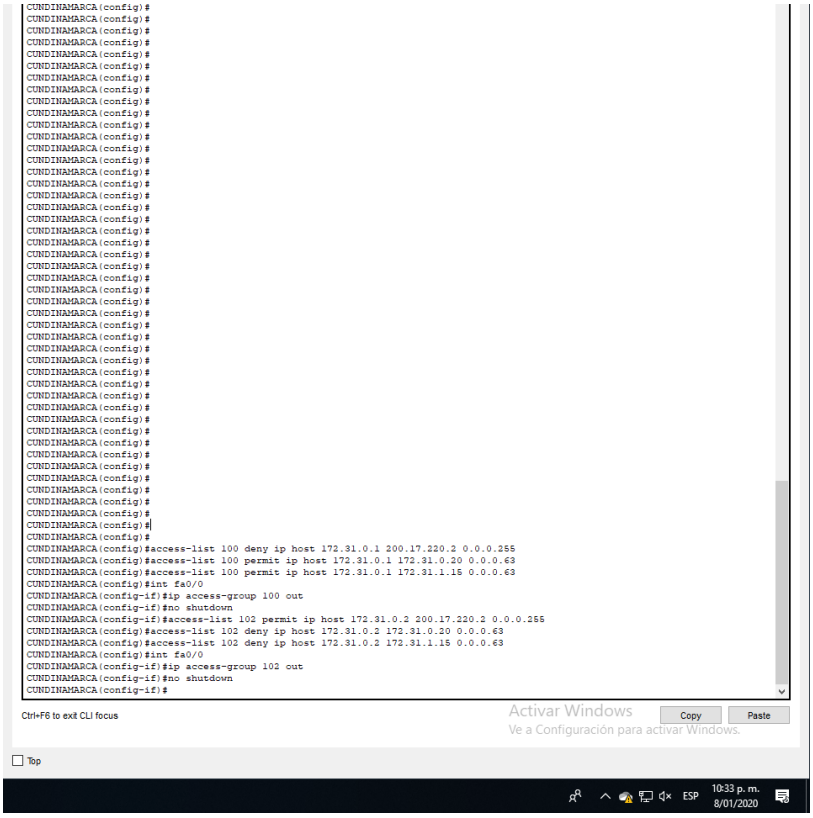

Figura 30.Creación de listas de acceso router CUNDINAMARCA.

ROUTER TUNJA

access-list 100 permit ip host 172.31.1.15 200.17.220.4 0.0.0.255
access-list 100 permit tcp host 172.31.1.15 200.17.220.2 0.0.0.255
int fa0/1
ip access-group 100 out
no shutdown
access-list 101 permit ip host 172.31.0.20 172.31.0.2 0.0.0.63
access-list 101 permit ip host 172.31.0.20 172.31.0.5 0.0.0.63
int fa0/1
ip access-group 101 out
no shutdown

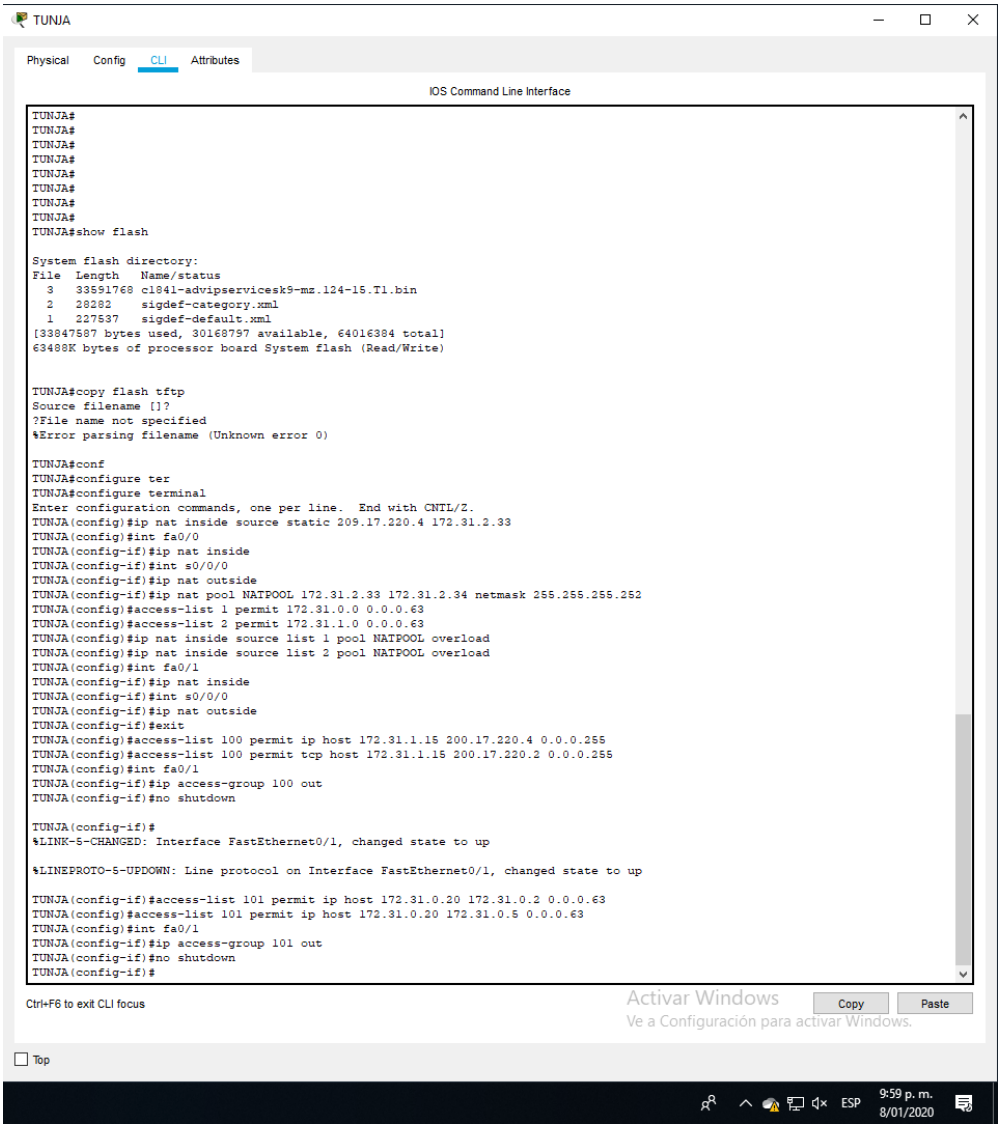

Figura 31.Creación de listas de acceso router TUNJA.

ROUTER BUCARAMANGA

access-list 100 permit ip host 172.31.1.5 200.17.220.2 0.0.0.255
access-list 100 permit ip host 172.31.1.5 172.31.0.0 0.0.0.63
int fa0/0
ip access-group 100 out
no shutdown
access-list 101 deny ip host 172.31.0.5 200.17.220.2 0.0.0.255
access-list 101 permit ip host 172.31.0.5 172.31.0.20 0.0.0.63
access-list 101 permit ip host 172.31.0.5 172.31.0.2 0.0.0.63
int fa0/0
ip access-group 101 out
no shutdown

Figura 32.Creación de listas de acceso router BUCARAMANGA.

Parte 6: Creación y asignación de VLAN

- 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.

SWITCH CUNDINAMARCA

```
Enable
Configure terminal
vlan 10
exit
vlan 20
exit
vlan 30
exit
vlan 88
exit
int range fa0/15-19
switchport mode access
switchport access vlan 20
exit
int range fa0/20-24
switchport mode access
switchport access vlan 10
exit
```

do wr

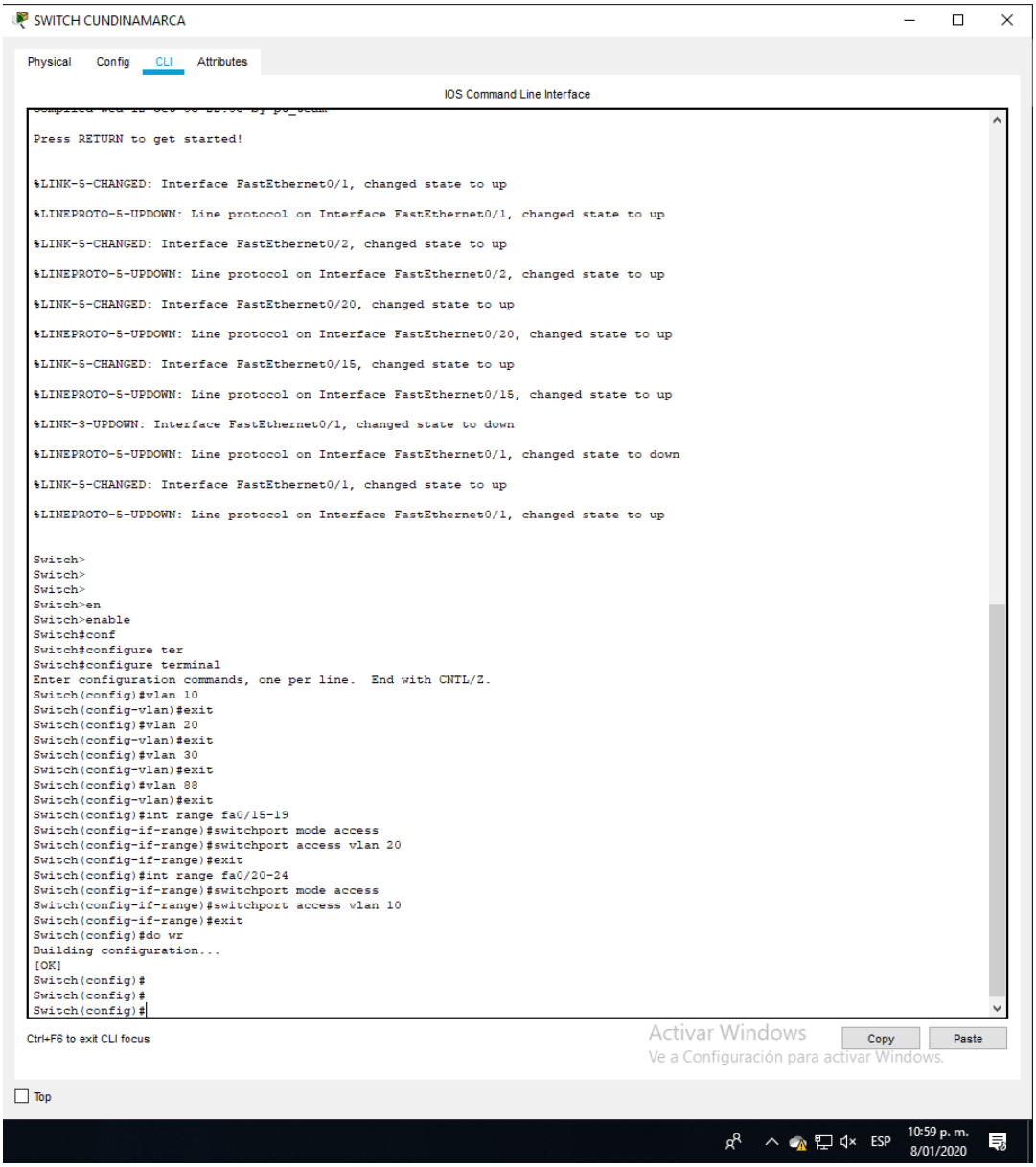

Figura 33.Creación VLAN switch CUNDINAMARCA.

ROUTER CUNDINAMARCA

Enable
Configure terminal
int fa0/0.20
encapsulation dot1Q 20

ip address 172.31.0.1 255.255.255.192
no shutdown
int fa0/0.30
encapsulation dot1Q 30
ip address 172.31.1.1 255.255.255.192
no shutdown

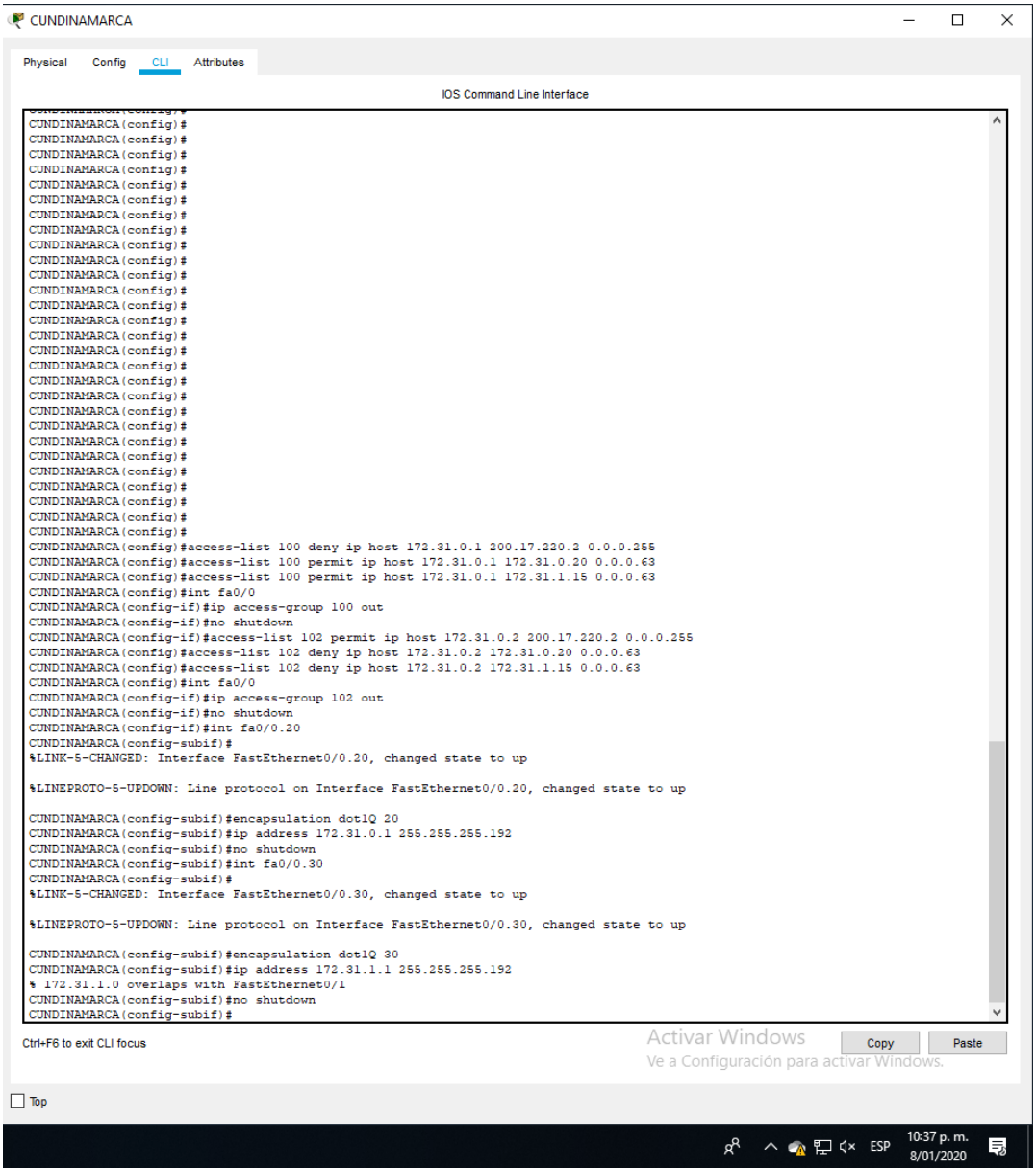

Figura 34.Encapsulación router CUNDINAMARCA.

router ospf 1
network 172.31.2.36 0.0.0.3 area 0
network 172.31.1.0 0.0.0.127 area 0
exit
int s0/0/0
ip ospf authentication-key cisco
ip ospf authentication

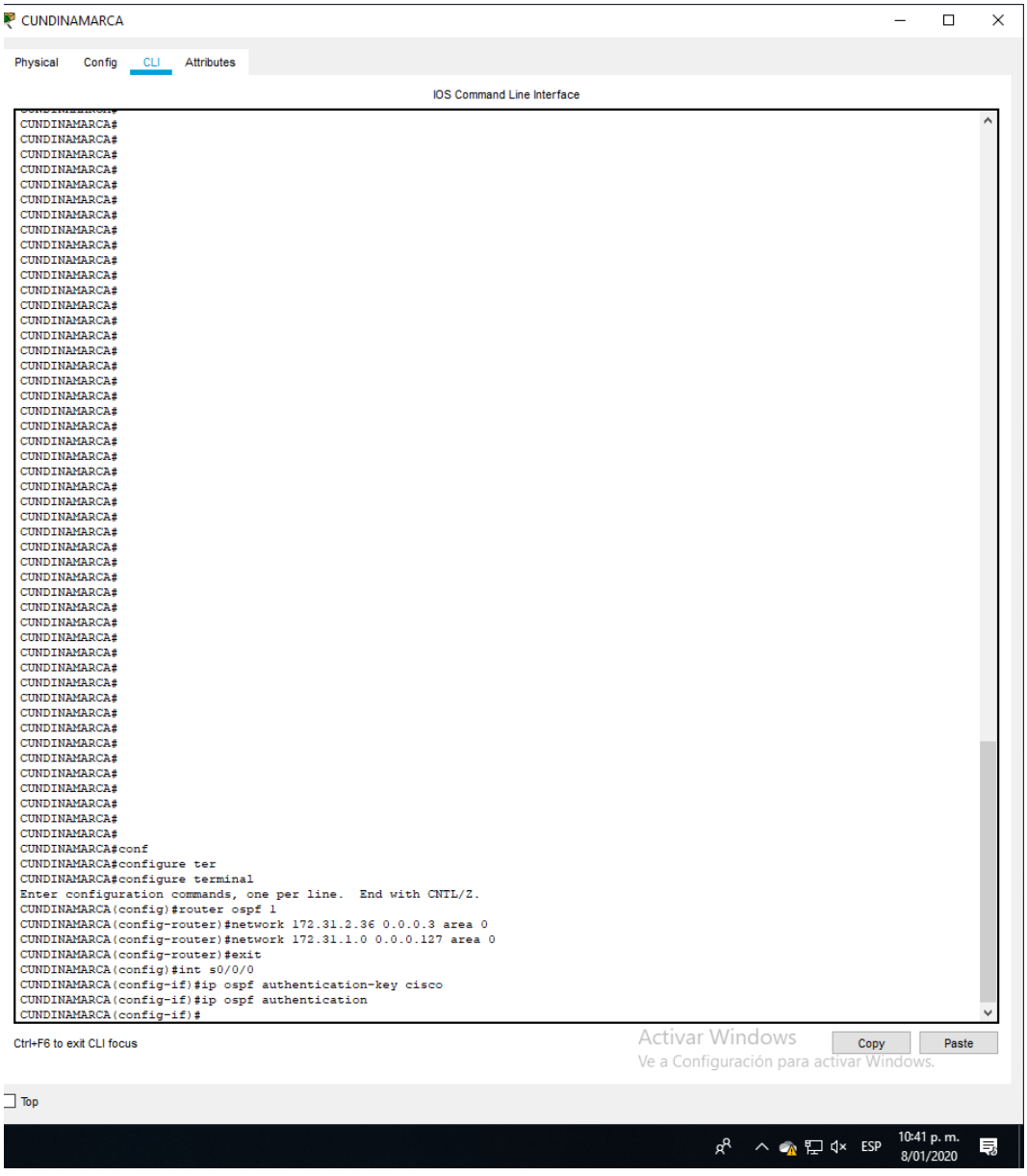

Figura 35.Enrutamiento OSPF router CUNDINAMARCA.

SWITCH TUNJA

Enable
Configure terminal
vlan 20
exit
vlan 30
exit
int range fa0/5-10
switchport mode access
switchport access vlan 20
exit
int range fa0/15-20
switchport mode access
switchport access vlan 30
do wr

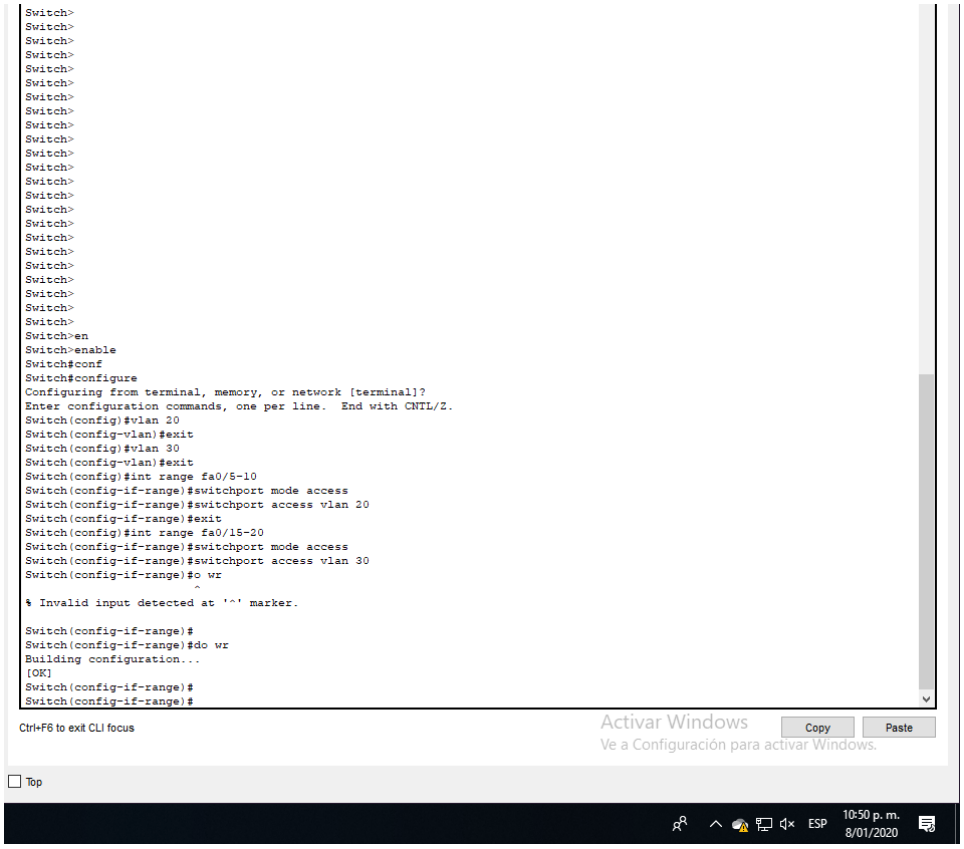

Figura 36.Creación VLAN switch TUNJA.

ROUTER TUNJA

Enable
Configure terminal
int fa0/1.20
encapsulation dot1Q 20
ip address 172.31.0.1 255.255.255.192
no shutdown
int fa0/1.30
encapsulation dot1Q 30
ip address 172.31.1.1 255.255.255.192
no shutdown

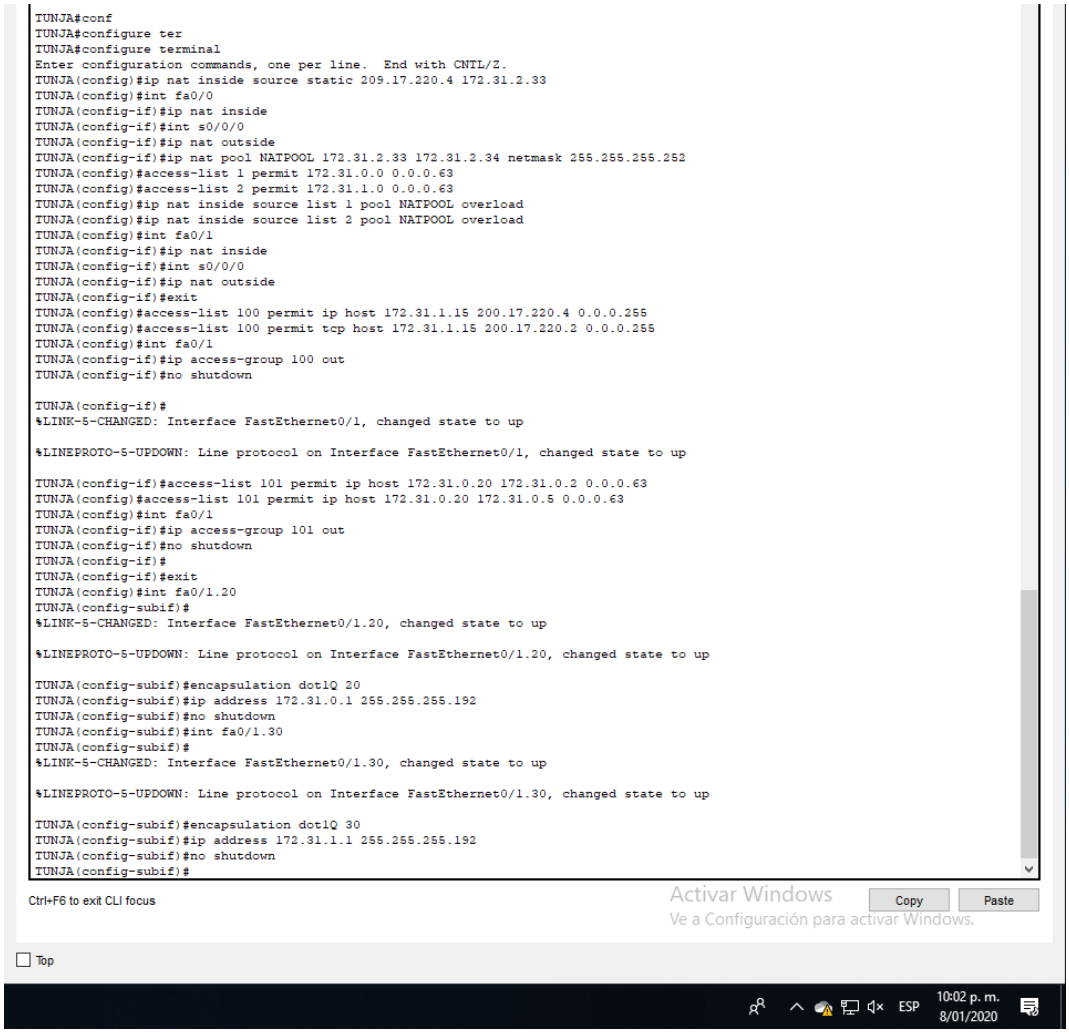

Figura 37.Encapsulación router TUNJA.

router ospf 1
network 172.31.2.32 0.0.0.3 area 0
network 172.31.2.36 0.0.0.3 area 0
network 209.17.220.0 0.0.0.255 area 0
exit
int s0/0/0
ip ospf authentication-key cisco
ip ospf authentication
int s0/0/1
ip ospf authentication-key cisco
ip ospf authentication
exit

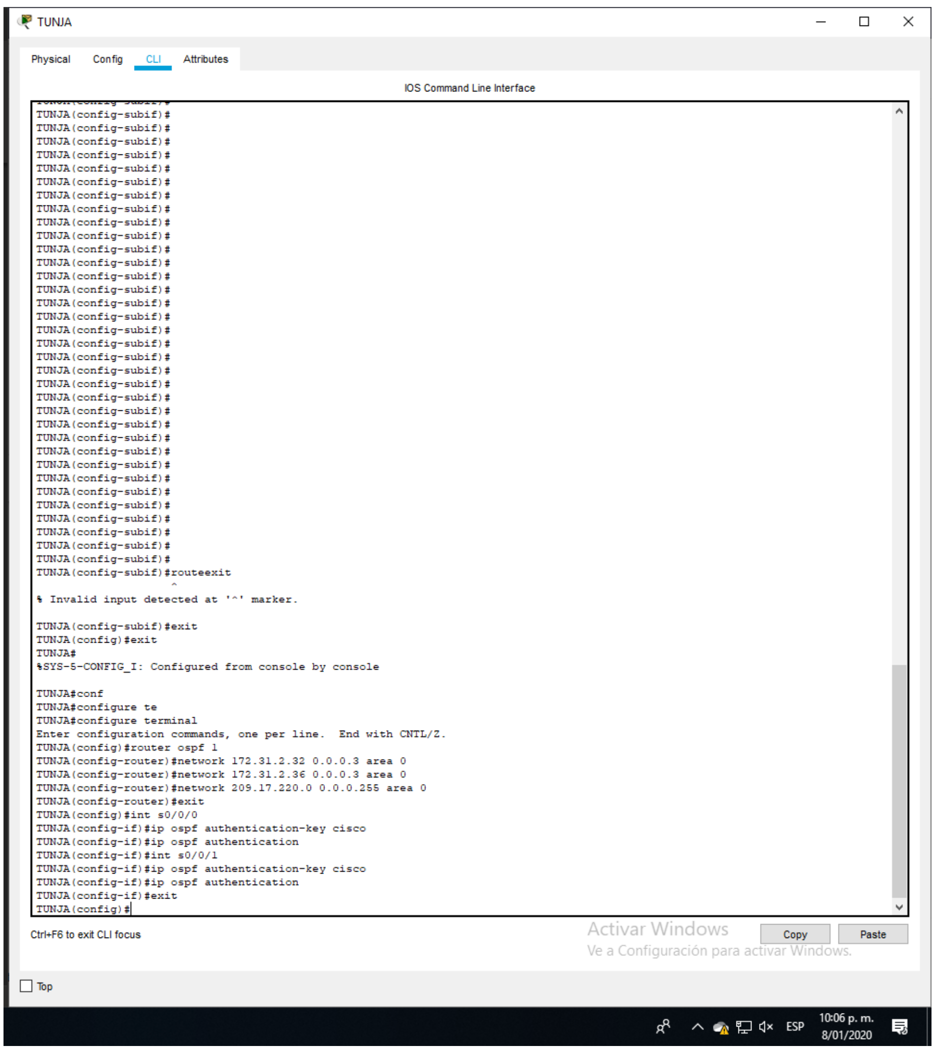

Figura 38.Enrutamiento OSPF router TUNJA.

SWITCH BUCARAMANGA

Enable
Configure terminal
vlan 10
exit
vlan 30
exit
int range fa0/2-5
switchport access vlan 10
do write
exit
int range fa0/20-24
switchport access vlan 30
switchport mode access
switchport access vlan 30
exit
int range fa0/2-4
switchport mode access
switchport access vlan 10
exit

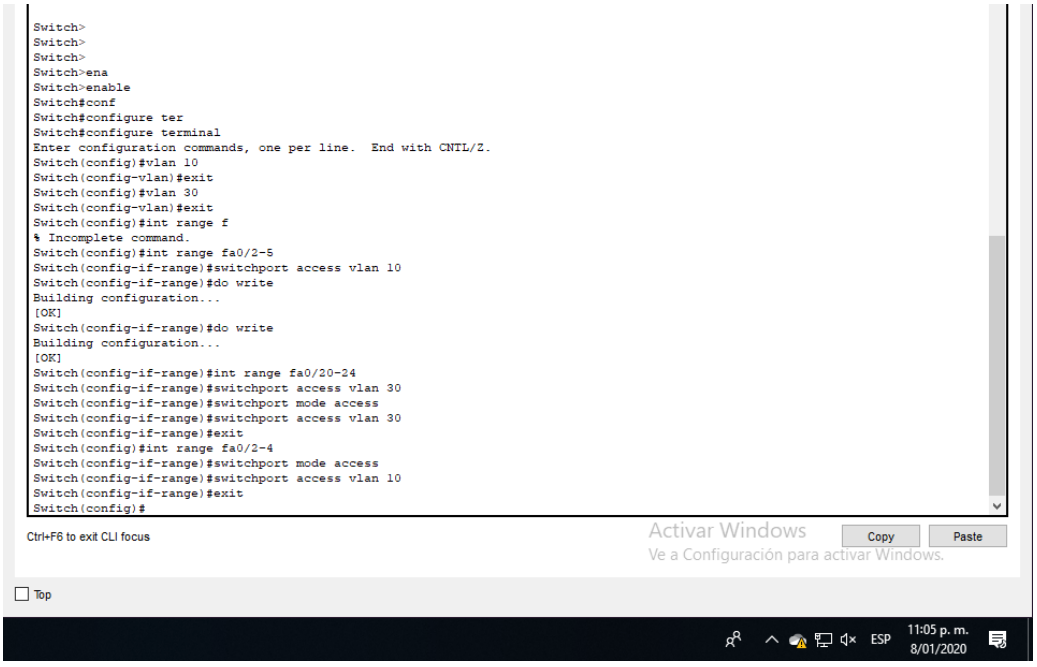

Figura 39.Creación VLAN switch BUCARAMANGA.

ROUTER BUCARAMANGA

```
Enable
Configure terminal
int fa0/0.10
encapsulation dot1Q 10
ip address 172.31.0.1 255.255.255.192
no shutdown
int fa0/0.30
encapsulation dot1Q 30
ip address 172.31.1.1 255.255.255.192
no shutdown
router ospf 1

network 172.31.2.32 0.0.0.3 area 0

network 172.31.0.0 0.0.0.127 area 0

exit

int s0/0/0

ip ospf authentication-key cisco

ip ospf authentication
```

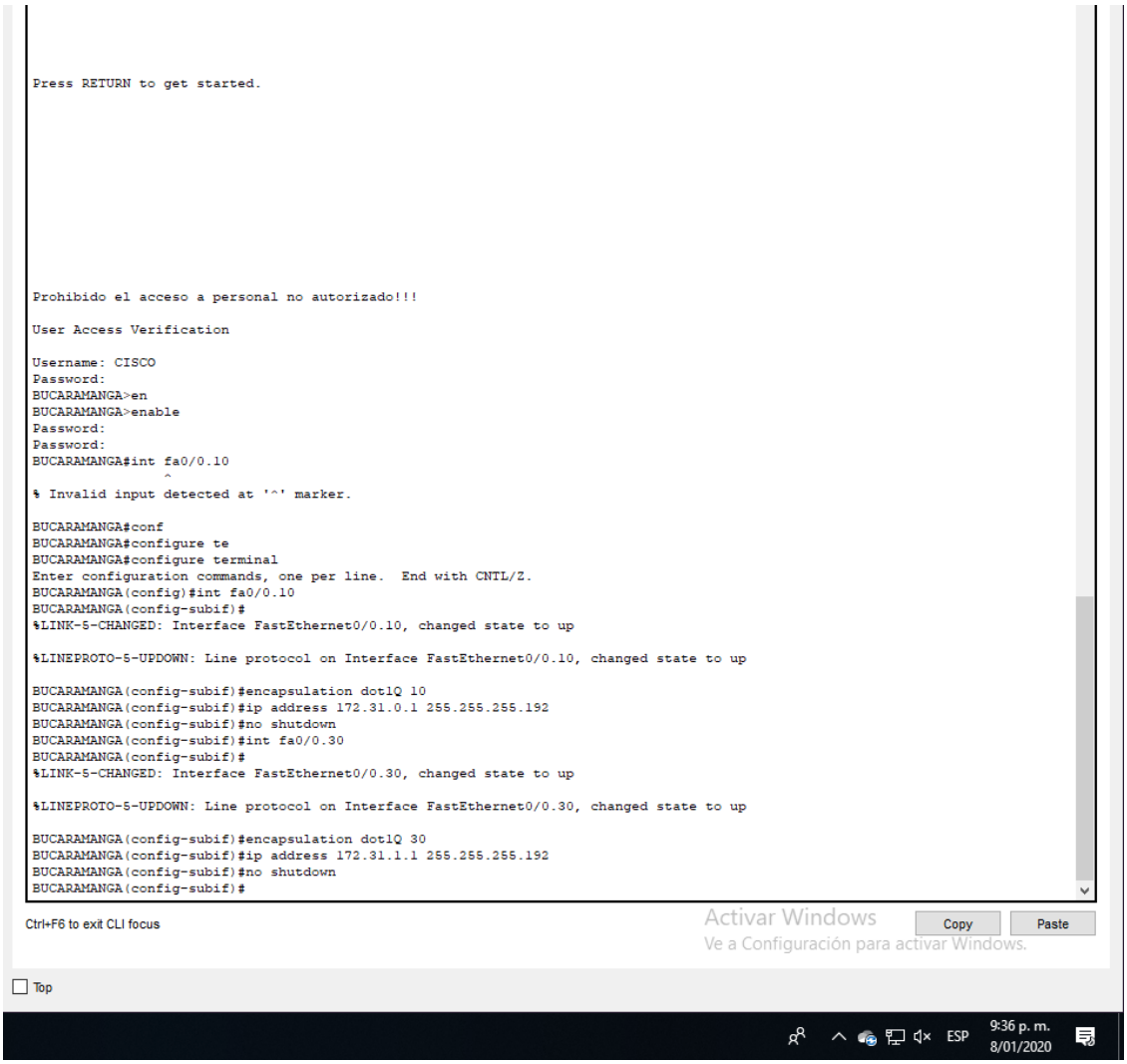

Figura 40.Encapsulación router BUCARAMANGA.

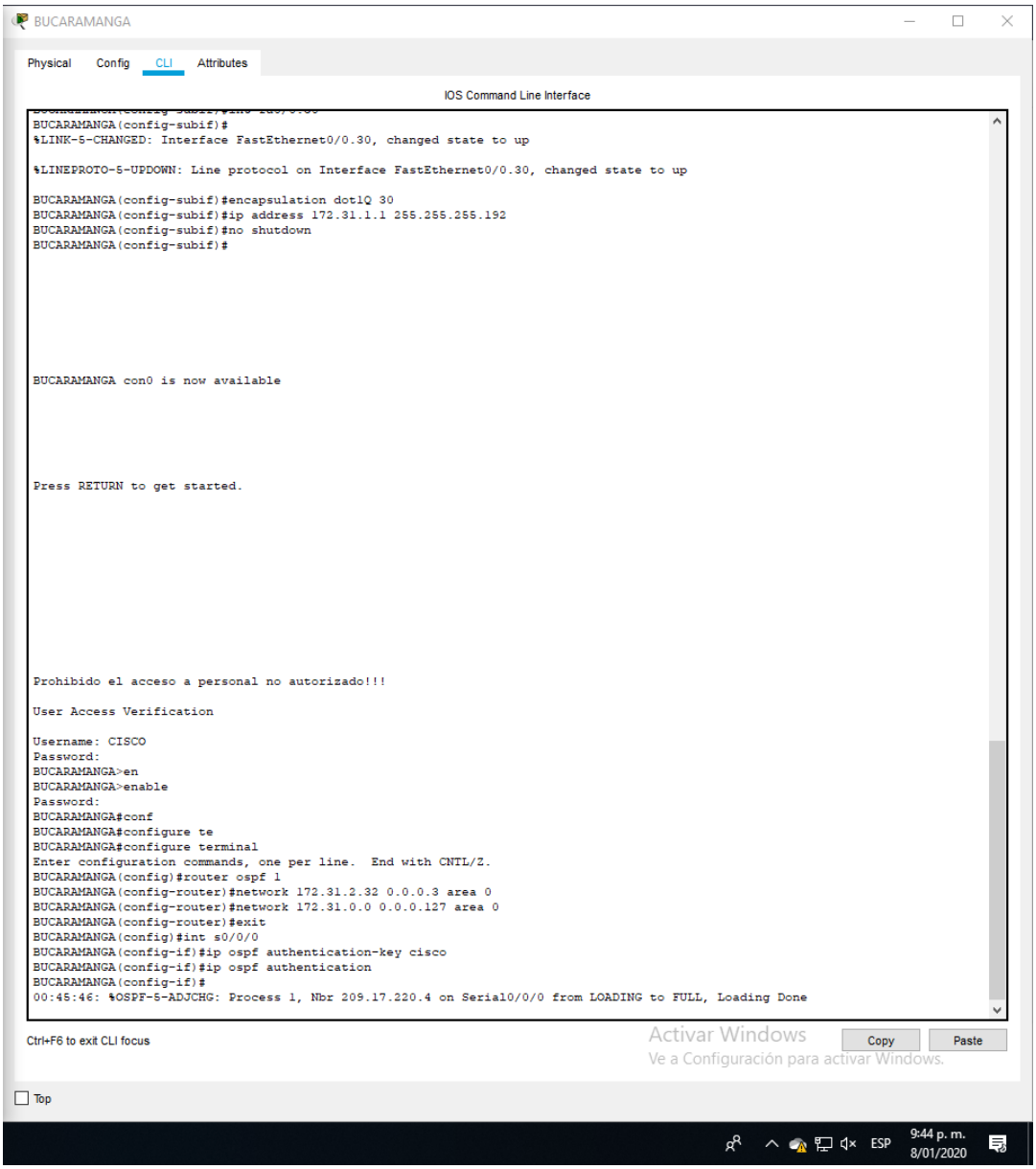

Figura 41.Enrutamiento OSPF router BUCARAMANGA.

Aspectos a tener en cuenta

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

Conclusiones

Gracias a los conocimientos aportados en el presente curso se logran aplicar en su mayor parte las técnicas de enrutamiento adecuadas para dar solución a los escenarios propuestos.

Se procedió a sustentar todos y cada uno de los pasos y procesos requeridos para la realización de la actividad, tales como validación de comandos y capturas de pantalla.

La prueba de habilidades prácticas se presenta como una gran oportunidad para definir y aplicar los principios de redes y telecomunicaciones previo a su montaje en sistemas reales y físicos.

Bibliografía

- Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3L74BZ3bpMiXRx0
- Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf
- Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de http://mr-telecomunicaciones.com/wp-content/uploads/2018/09/wendellodom.pdf
- Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3GQVfFFrjnEGFFU