

**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.

Resumen	8
Abstract	9
Introducción	5
Objetivos	6
Objetivo general:.....	6
Objetivos específicos:.....	6
Desarrollo de escenarios	7
Escenario 1	7
Topología de red	7
Desarrollo	8
Parte 1: Asignación de direcciones IP:.....	10
Parte 2: Configuración Básica.	10
Enrutamiento:	11
Parte 3: Configuración de Enrutamiento.....	18
Parte 4: Configuración de las listas de Control de Acceso.	23
Parte 5: Comprobación de la red instalada.	27
Escenario 2	28
Topología de red	29
Desarrollo	29
Parte 1: Configuración básica	29
Parte 2: Creación servidores TFTP y almacenamiento de archivos	38
Parte 3: Creación de NAT y enrutamiento.....	41
Parte 4: Asignación de máscaras de red variable	45
Parte 5: Creación de listas de acceso	45
Parte 6: Creación y asignación de VLAN	48
Conclusiones	60
Bibliografía	61

Lista de figuras.

Figura 1.Diseño de red escenario 1.	7
Figura 2.Topología de red escenario 1.	8
Figura 3.CDP Router Medellín.	12
Figura 4.CDP Router Bogotá.	13
Figura 5.CDP Router Cali.	14
Figura 6.Prueba de Conectividad a PC3.	15
Figura 7.Prueba de Conectividad a WS-1.	16
Figura 8.Prueba de Conectividad a Servidor.	17
Figura 9.Tabla de direccionamiento Router Medellín.	19
Figura 10.Tabla de direccionamiento Router Bogotá.	20
Figura 11.Tabla de direccionamiento Router Cali.	21
Figura 12.Ping PC0.	22
Figura 13.Ping a Servidor	23
Figura 14.Habilitacion Telnet Router Medellín.	24
Figura 15.Habilitacion Telnet Router Bogotá	25
Figura 16.Habilitacion Telnet Router Cali.	26
Figura 17.Diseño de red escenario 2.	28
Figura 18.Topología de red escenario 2.	29
Figura 19. Configuración básica router CUNDINAMARCA.	31
Figura 20. Configuración básica router TUNJA 1.	33
Figura 21. Configuración básica router TUNJA 2.	34
Figura 22. Configuración básica router BUCARAMANGA 1.	36
Figura 23. Configuración básica router BUCARAMANGA 2.	37
Figura 24. Activación servidor TFTP router CUNDINAMARCA.	38
Figura 25. Activación servidor TFTP router TUNJA.	39
Figura 26. Activación servidor TFTP router BUCARAMANGA.	40
Figura 27.Asignación NAT router CUNDINAMARCA.	42
Figura 28.Asignacin NAT router TUNJA.	43
Figura 29.Asignación NAT router BUCARAMANGA.	44
Figura 30.Creación de listas de acceso router CUNDINAMARCA.	45
Figura 31.Creación de listas de acceso router TUNJA.	46
Figura 32.Creación de listas de acceso router BUCARAMANGA.	47
Figura 33.Creación VLAN switch CUNDINAMARCA.	49
Figura 34.Encapsulación router CUNDINAMARCA.	50
Figura 35.Enrutamiento OSPF router CUNDINAMARCA.	51
Figura 36.Creación VLAN switch TUNJA.	52

Figura 37.Encapsulación router TUNJA.....53
Figura 38.Enrutamiento OSPF router TUNJA.54
Figura 39.Creación VLAN switch BUCARAMANGA.55
Figura 40.Encapsulación router BUCARAMANGA.57
Figura 41.Enrutamiento OSPF router BUCARAMANGA.58

Lista de tablas.

Tabla 1.Direccionamiento	10
Tabla 2.Pruebas funcionales.....	27

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 práctica 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 prácticas 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.

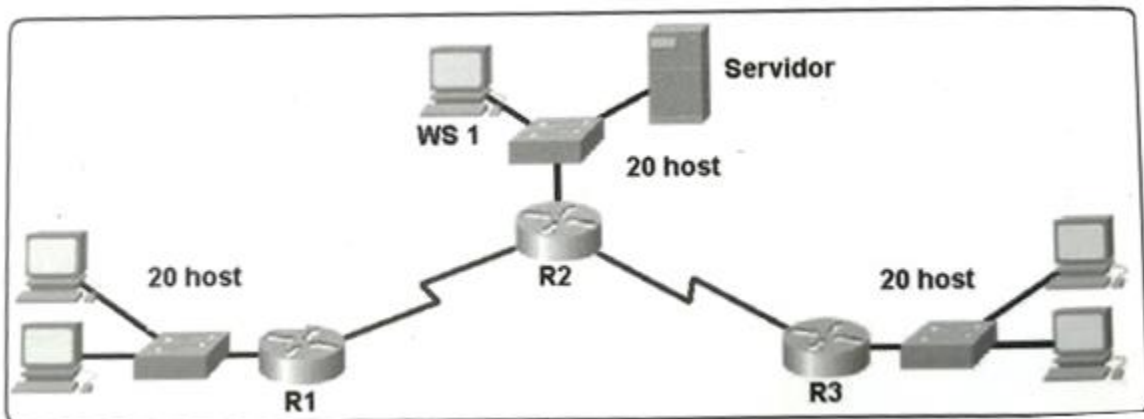


Figura 1. Diseño de red escenario 1.

Topología de red:

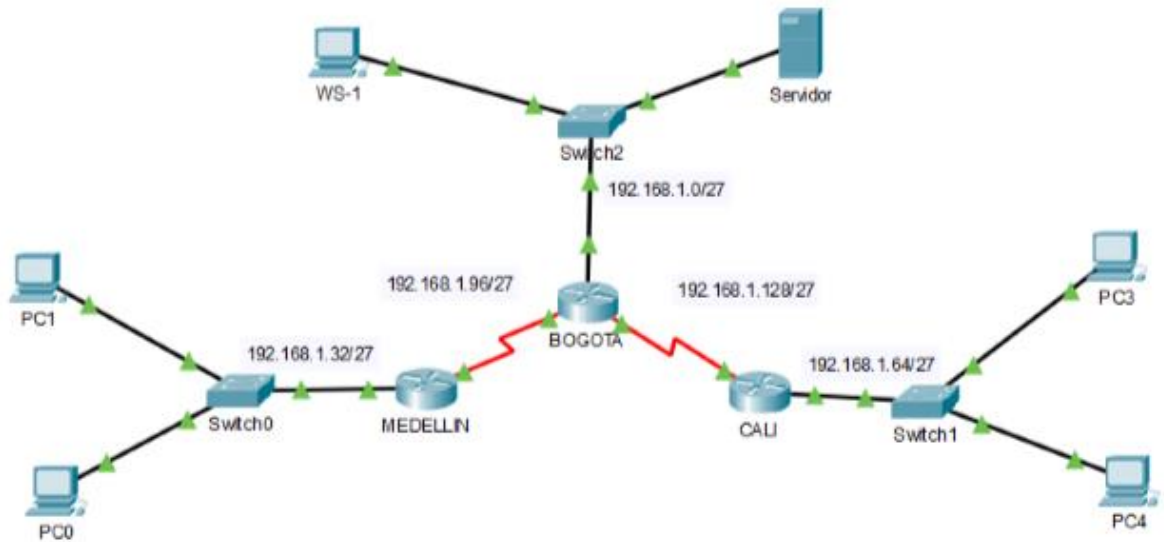


Figura 2. Topología de red escenario 1.

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 física 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:

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

Parte 2: Configuración Básica.

- 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 Sistema Autónomo	Eigrp 200	Eigrp 200	Eigrp 200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

- 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:

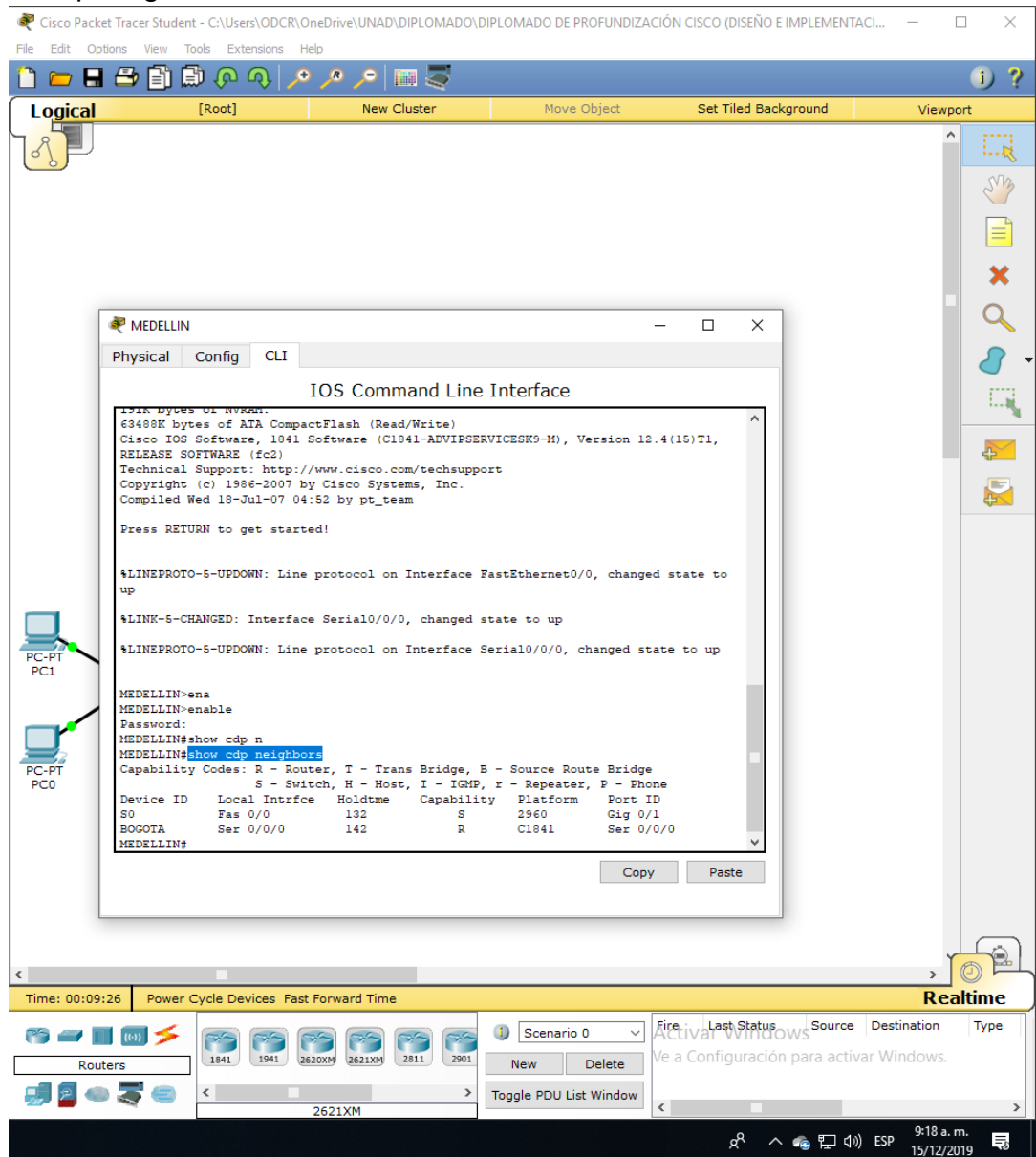
```
Ip route 192.168.1.32 255.255.255.224 192.168.1.130  
Ip route 192.168.1.96 255.255.255.224 192.168.1.130  
Ip route 192.168.1.0 255.255.255.224 192.168.1.130
```

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

ROUTER MEDELLIN:

Enable

Show cdp neighbors



The screenshot shows the Cisco Packet Tracer interface. The main window displays the 'Logical' view of a network. A central window titled 'MEDELLIN' shows the 'CLI' (Command Line Interface) of the router. The CLI output is as follows:

```
MEDELLIN>ena
MEDELLIN>enable
Password:
MEDELLIN#show cdp n
MEDELLIN#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID      Local Intrfce  Holdtime   Capability  Platform  Port ID
S0              Fas 0/0       132        S           2960      Gig 0/1
BOGOTA         Ser 0/0/0     142        R           C1841     Ser 0/0/0
MEDELLIN#
```

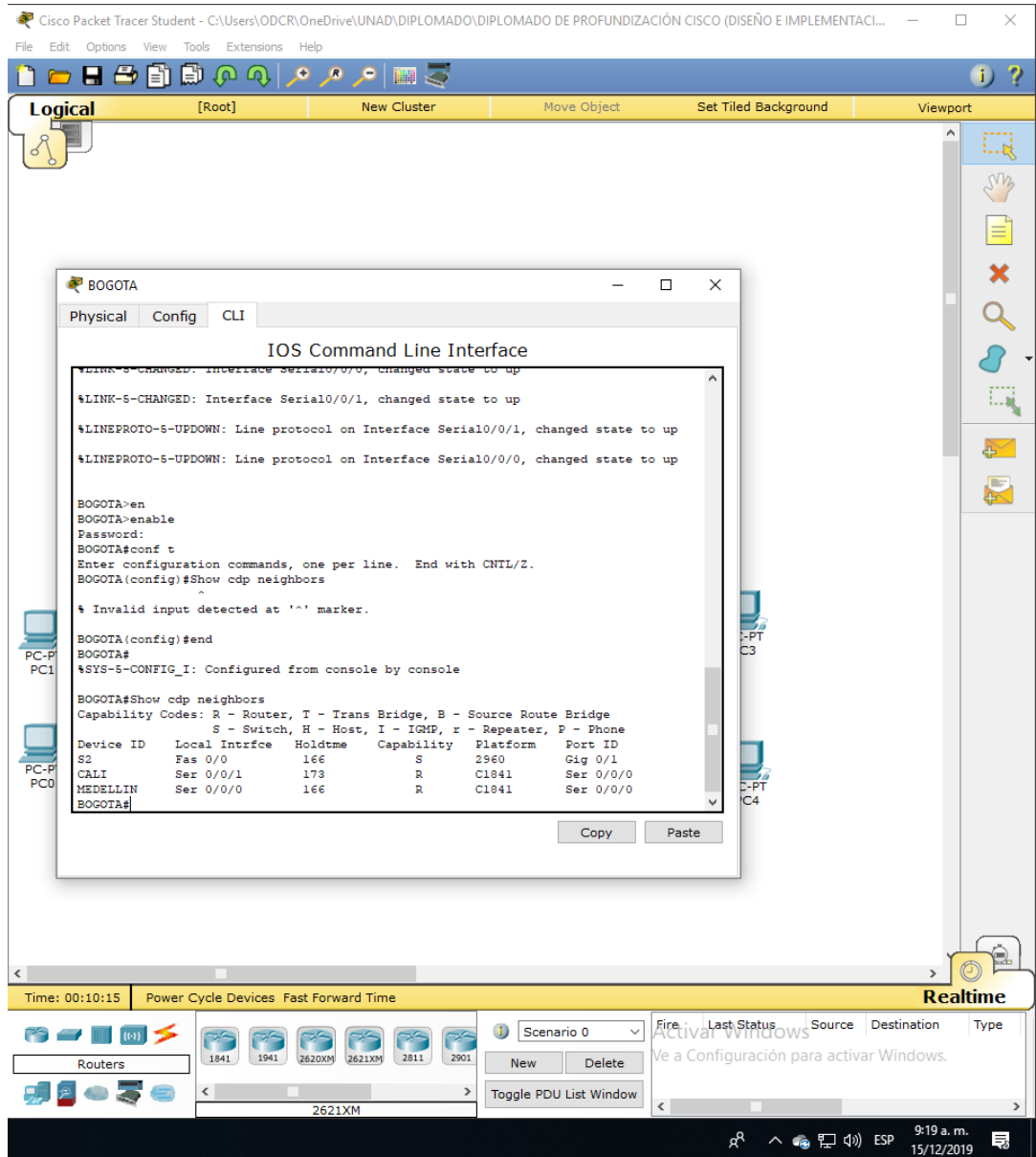
The bottom of the interface shows the 'Realtime' view with a 'Routers' panel containing icons for various router models (1841, 1941, 2620XM, 2621XM, 2811, 2901) and a 'Scenario 0' dropdown menu. A 'Toggle PDU List Window' button is also visible.

Figura 3.CDP Router Medellín.

ROUTER BOGOTA:

Enable

Show cdp neighbors



The screenshot shows the Cisco Packet Tracer Student interface. The main window displays the CLI for Router Bogota. The CLI output shows the configuration of interfaces and the execution of the 'show cdp neighbors' command, displaying a table of neighboring devices.

```
BOGOTA>en
BOGOTA>enable
Password:
BOGOTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA (config)#show cdp neighbors
% Invalid input detected at '^' marker.
BOGOTA (config)#end
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console
BOGOTA#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID      Local Intrfce   Holdtme    Capability   Platform   Port ID
S2             Fas 0/0/0      166        S            2960      Gig 0/1
CALI           Ser 0/0/1      173        R            Cl841     Ser 0/0/0
HEDELLIN      Ser 0/0/0      166        R            Cl841     Ser 0/0/0
BOGOTA#
```

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
S2	Fas 0/0/0	166	S	2960	Gig 0/1
CALI	Ser 0/0/1	173	R	Cl841	Ser 0/0/0
HEDELLIN	Ser 0/0/0	166	R	Cl841	Ser 0/0/0

Figura 4.CDP Router Bogotá.

ROUTER CALI:

Enable
Show cdp neighbors

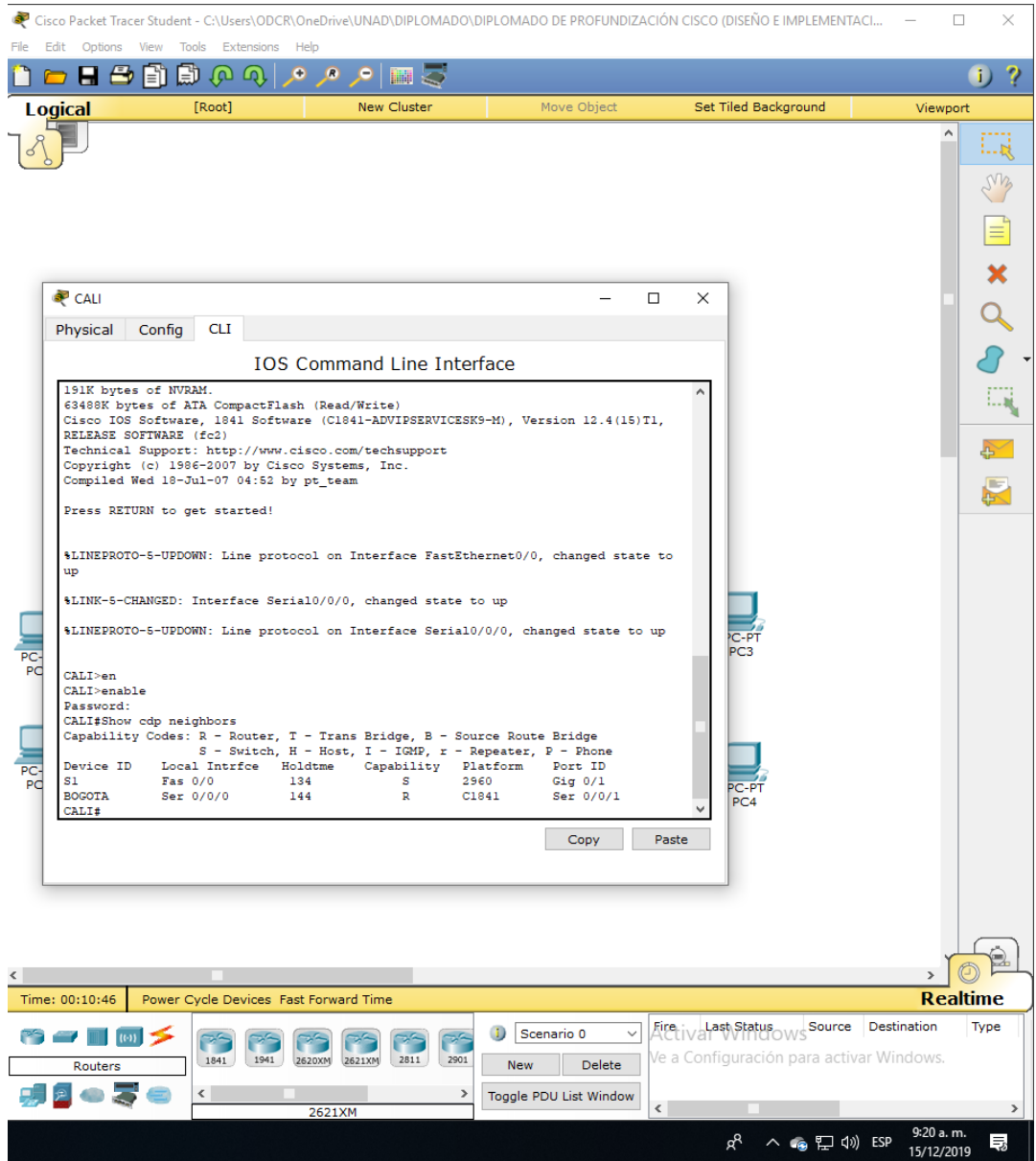


Figura 5.CDP Router Cali.

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

PC0:

Ping 192.168.1.67 (PC3)

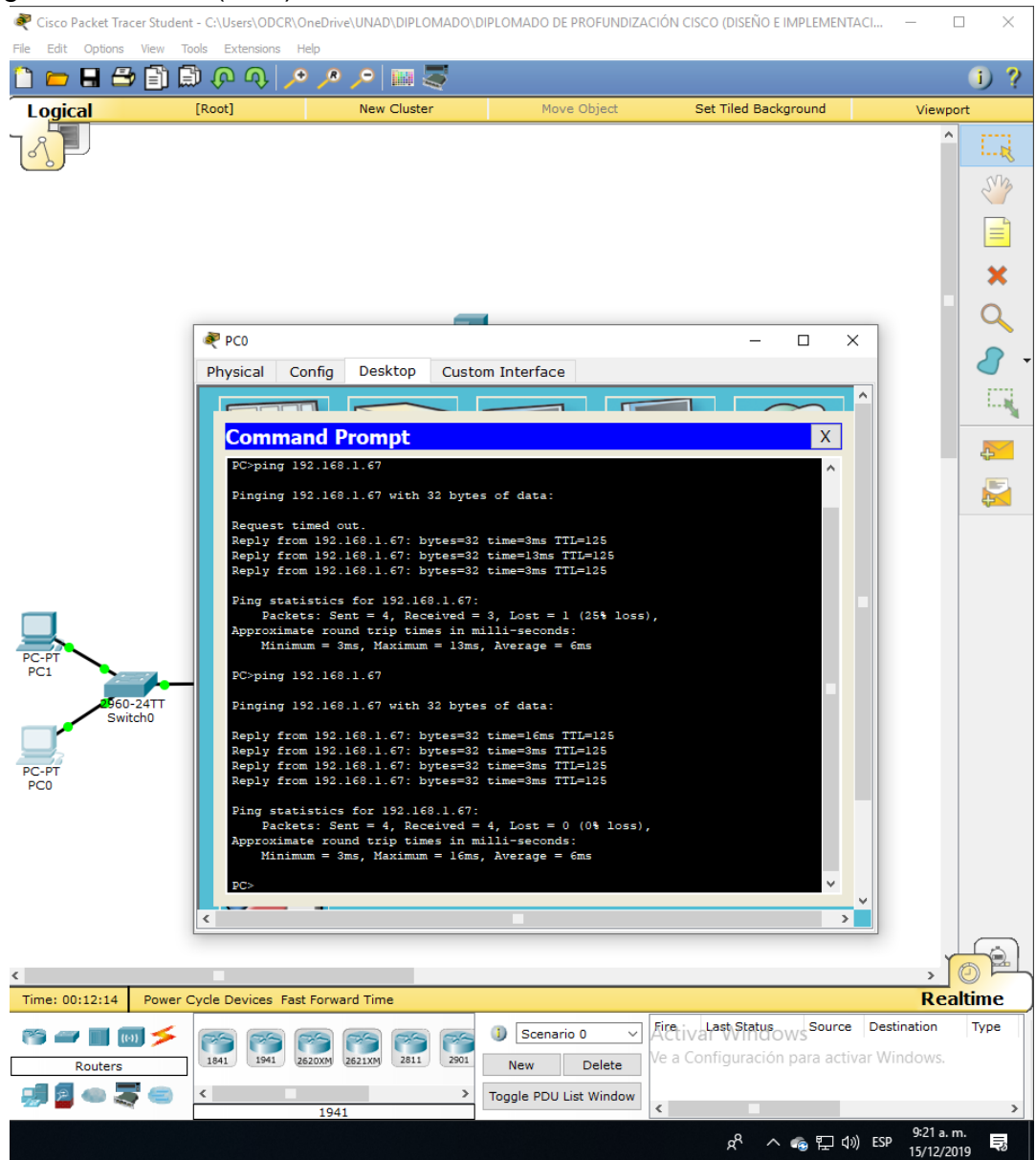


Figura 6. Prueba de Conectividad a PC3.

Ping 192.168.1.3 (WS-1)

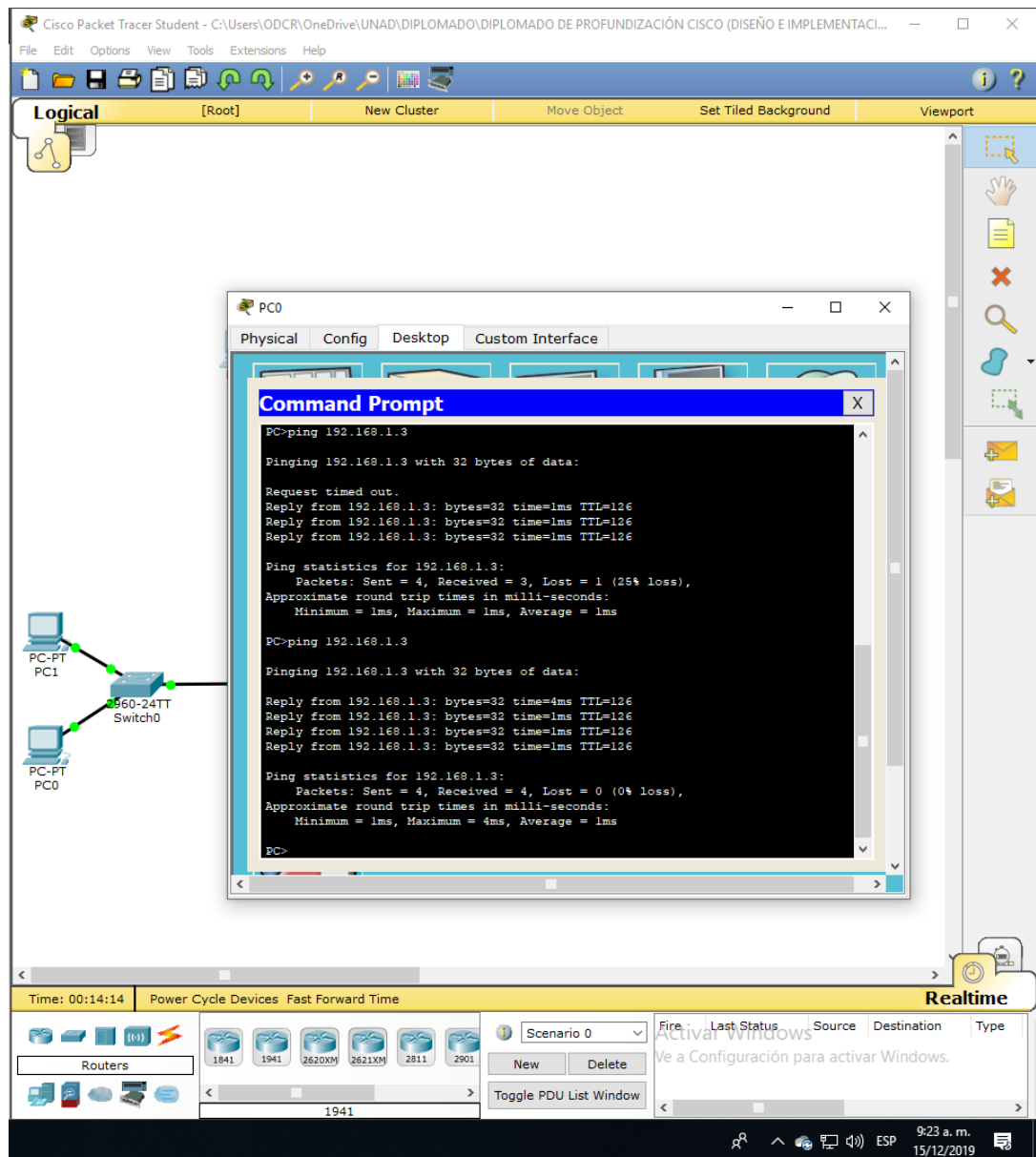


Figura 7. Prueba de Conectividad a WS-1.

PC4:
Ping 192.168.1.4 (Servidor)

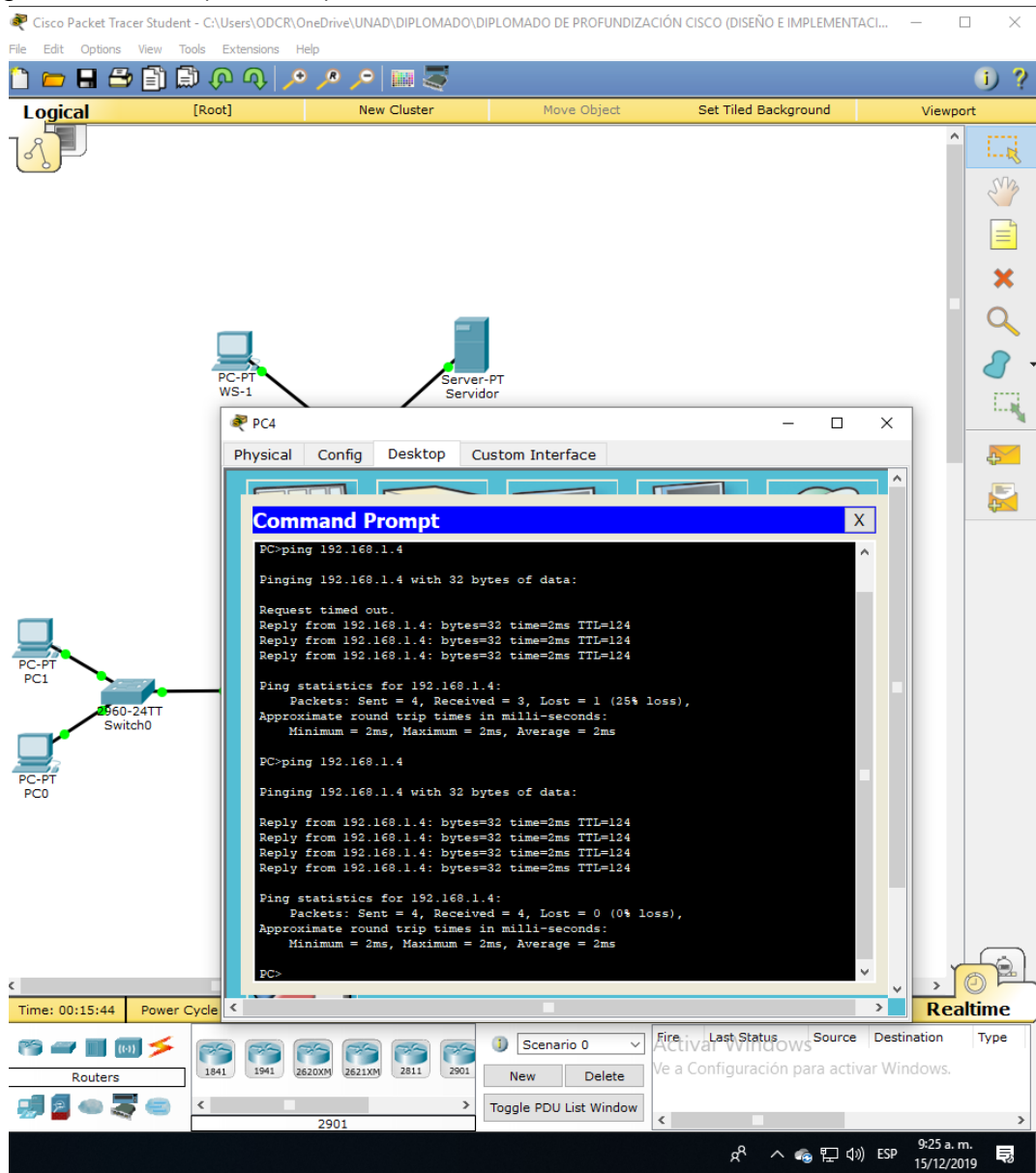


Figura 8. Prueba de Conectividad a Servidor.

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

The screenshot shows the Cisco Packet Tracer interface with a network diagram and a CLI window for Router Medellín. The network diagram includes a central 2960 24TT Switch2 connected to PC-PT WS-1, Server-PT Servidor, PC-PT PC1, and PC-PT PC0. The CLI window shows the following configuration and routing table output:

```

MEDELLIN(config-router)#ne 192.168.1.0
MEDELLIN(config-router)#network 192.168.1.0
MEDELLIN(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.98 (Serial10/0/0) is up: new adjacency
MEDELLIN(config-router)#end
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console

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

Gateway of last resort is not set

 192.168.1.0/27 is subnetted, 5 subnets
S    192.168.1.0 [1/0] via 192.168.1.98
C    192.168.1.32 is directly connected, FastEthernet0/0
S    192.168.1.64 [1/0] via 192.168.1.98
C    192.168.1.96 is directly connected, Serial10/0/0
S    192.168.1.128 [1/0] via 192.168.1.98
MEDELLIN#
  
```

The bottom of the interface shows the 'Realtime' section with a 'Routers' table:

Router Model	IP Address	Status			
1841	1941	2620XM	2621XM	2811	2901
2621XM					

Figura 9. Tabla de direccionamiento Router Medellín.

ROUTER BOGOTA: Show ip route

The screenshot shows the Cisco Packet Tracer interface with a logical network diagram. A router named 'BOGOTA' is connected to a PC-PT WS-1 and a Server-PT Servidor. A configuration window for the router is open, showing the CLI output of the 'show ip route' command.

```

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

Gateway of last resort is not set

 192.168.1.0/27 is subnetted, 5 subnets
 C    192.168.1.0 is directly connected, FastEthernet0/0
 S    192.168.1.32 [1/0] via 192.168.1.99
 S    192.168.1.64 [1/0] via 192.168.1.131
      [1/0] via 192.168.1.99
 C    192.168.1.96 is directly connected, Serial0/0/0
 C    192.168.1.128 is directly connected, Serial0/0/1
BOGOTA#
  
```

The interface also shows a 'Realtime' panel at the bottom with a 'Routers' list containing models 1841, 1941, 2620XM, 2621XM, 2811, and 2901. The current router selected is 2621XM.

Figura 10. Tabla de direccionamiento Router Bogotá.

ROUTER CALI: Show ip route

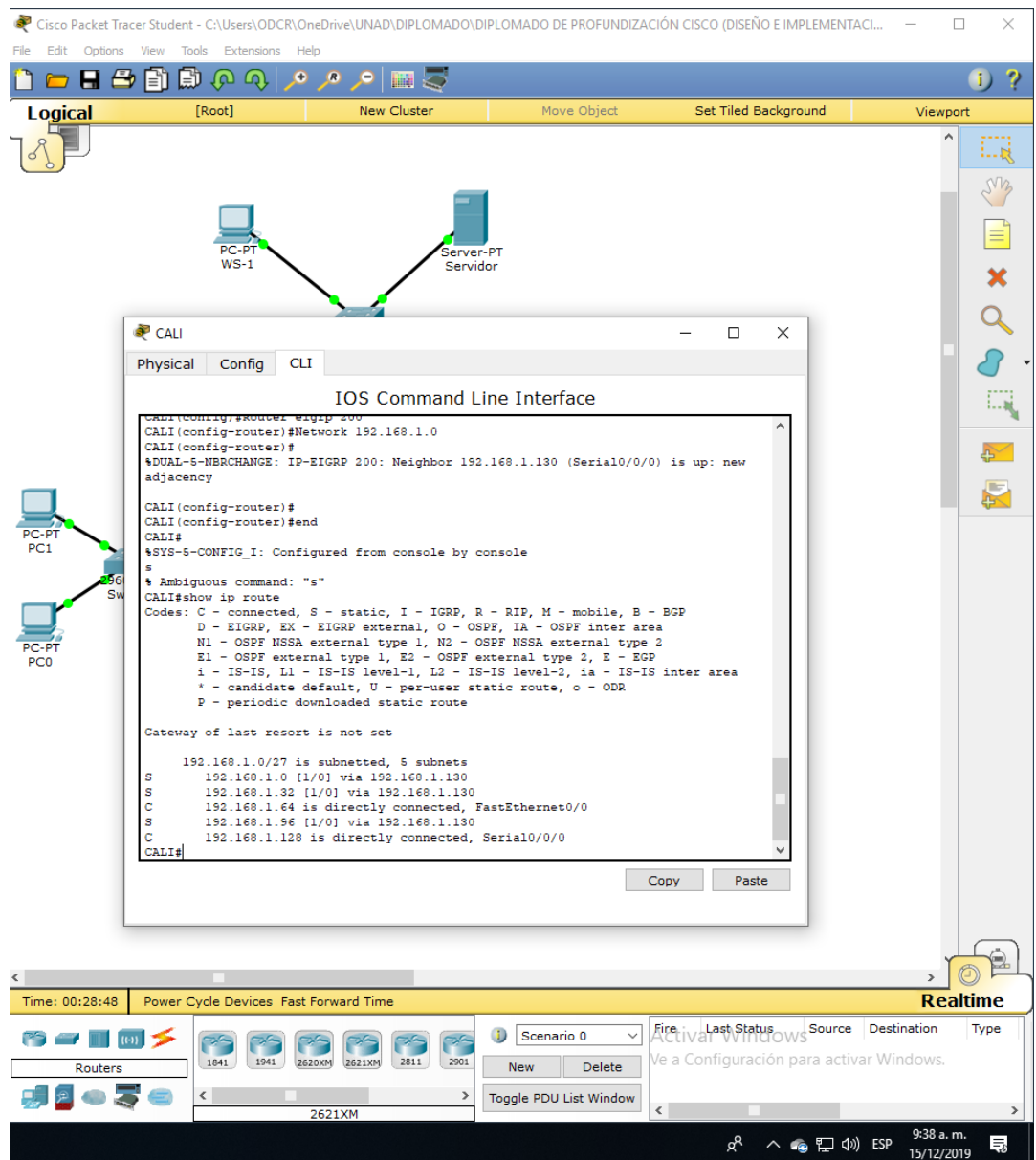


Figura 11. Tabla de direccionamiento Router Cali.

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

The screenshot shows the Cisco Packet Tracer interface. In the background, a network diagram is visible with a central switch labeled '2660-24T Switch0' connected to several devices: 'PC-PT WS-1', 'Server-PT Servidor', 'PC-PT PC1', and 'PC-PT PC0'. A 'Command Prompt' window is open in the foreground, showing the following output:

```
PC>ping 192.168.1.32
Pinging 192.168.1.32 with 32 bytes of data:
Reply from 192.168.1.99: bytes=32 time=3ms TTL=253
Request timed out.
Reply from 192.168.1.99: bytes=32 time=2ms TTL=253
Request timed out.

Ping statistics for 192.168.1.32:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

PC>ping 192.168.1.34
Pinging 192.168.1.34 with 32 bytes of data:
Reply from 192.168.1.34: bytes=32 time=2ms TTL=125
Reply from 192.168.1.34: bytes=32 time=13ms TTL=123
Reply from 192.168.1.34: bytes=32 time=3ms TTL=123
Reply from 192.168.1.34: bytes=32 time=23ms TTL=123

Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 23ms, Average = 10ms

PC>
```

The interface also shows a 'Routers' panel with various router models (1841, 1941, 2620XM, 2621XM, 2811, 2901) and a 'Realtime' panel with a table for active windows.

Figura 12. Ping PC0

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

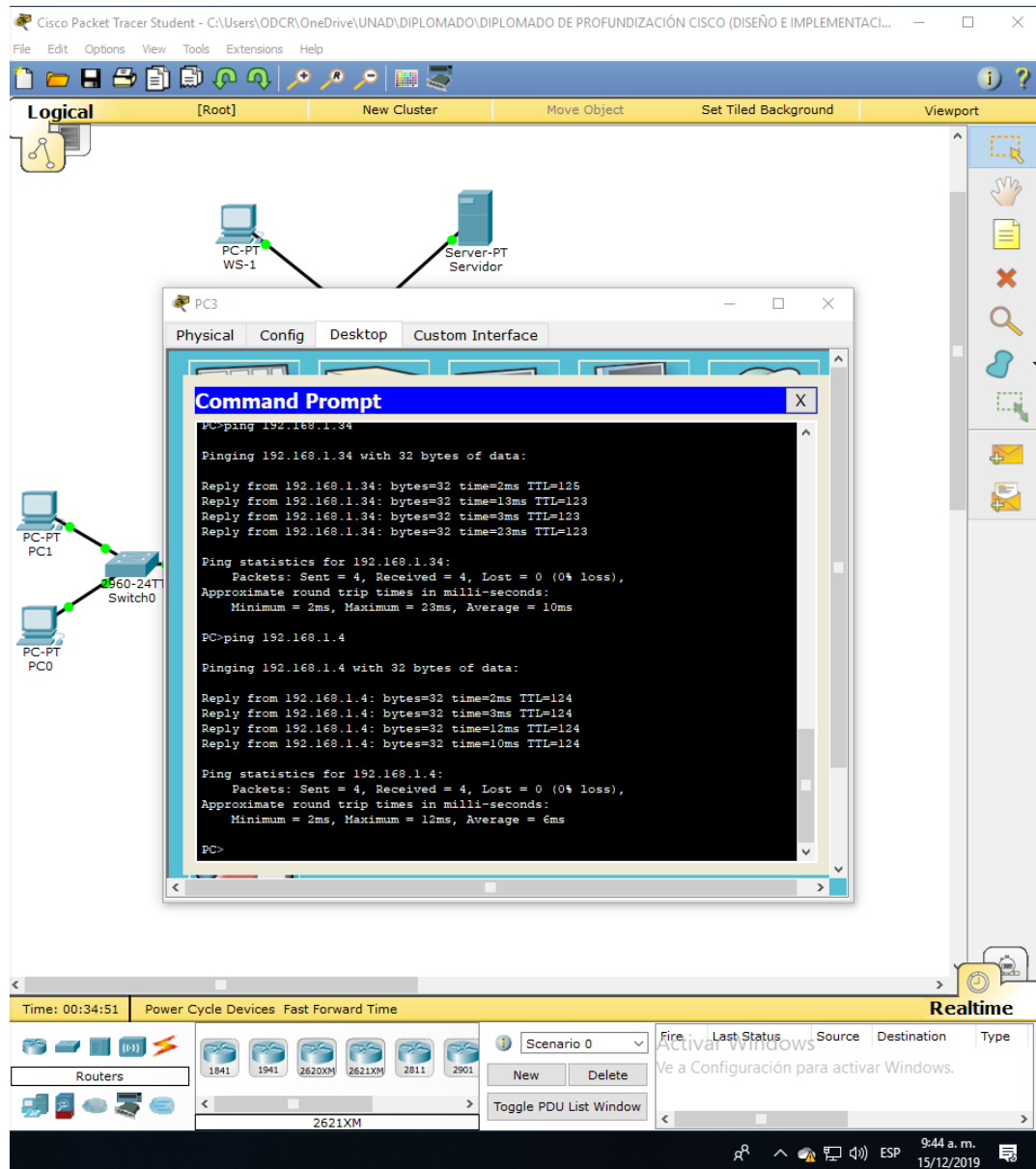


Figura 13. Ping a Servidor

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.

ROUTER BOGOTA

Enable
Configure terminal
Line vty 0 15
Password cisco
Exit

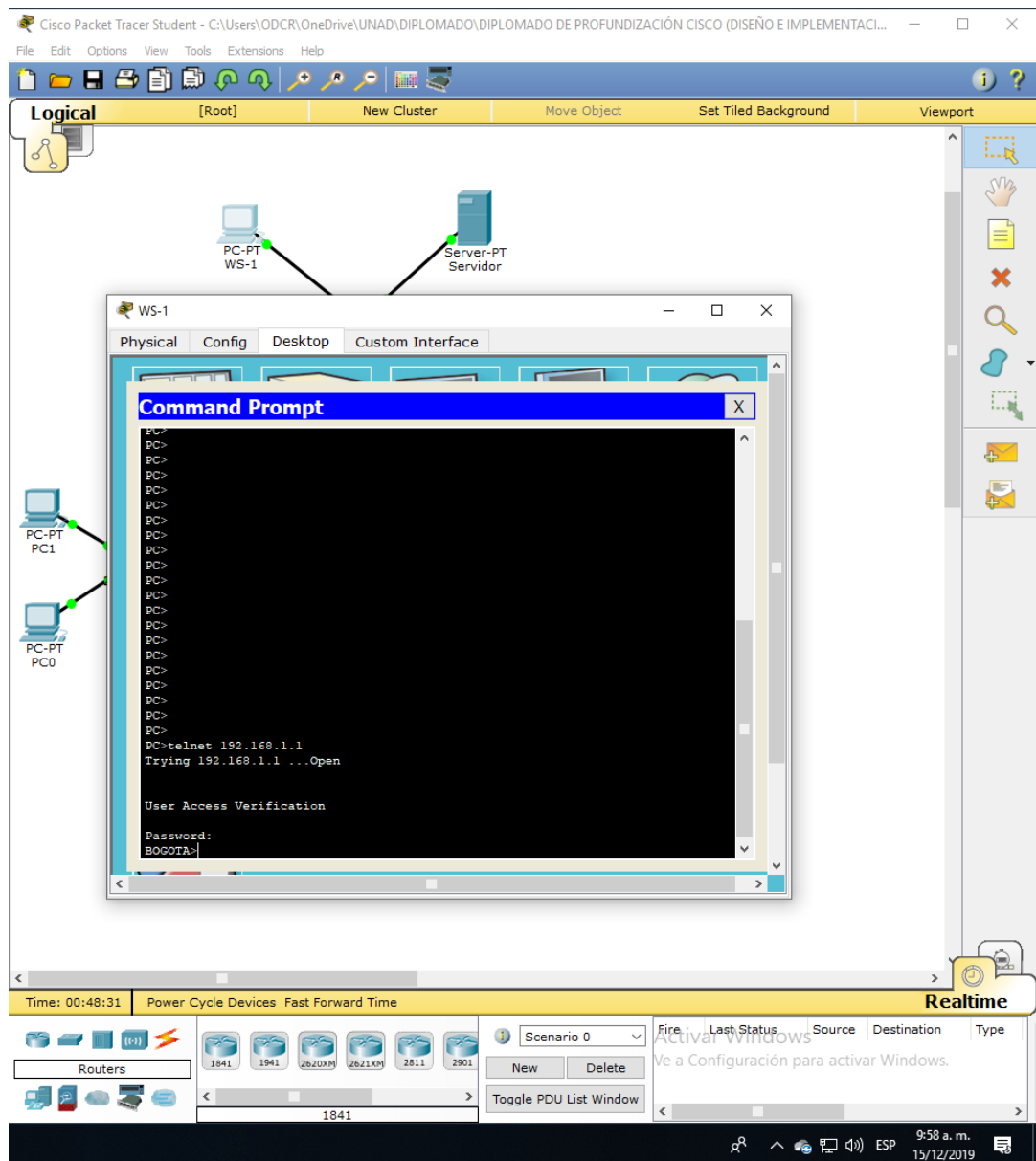


Figura 15. Habilitación Telnet Router Bogotá

ROUTER CALI

Enable
Configure terminal
Line vty 0 15
Password cisco
exit

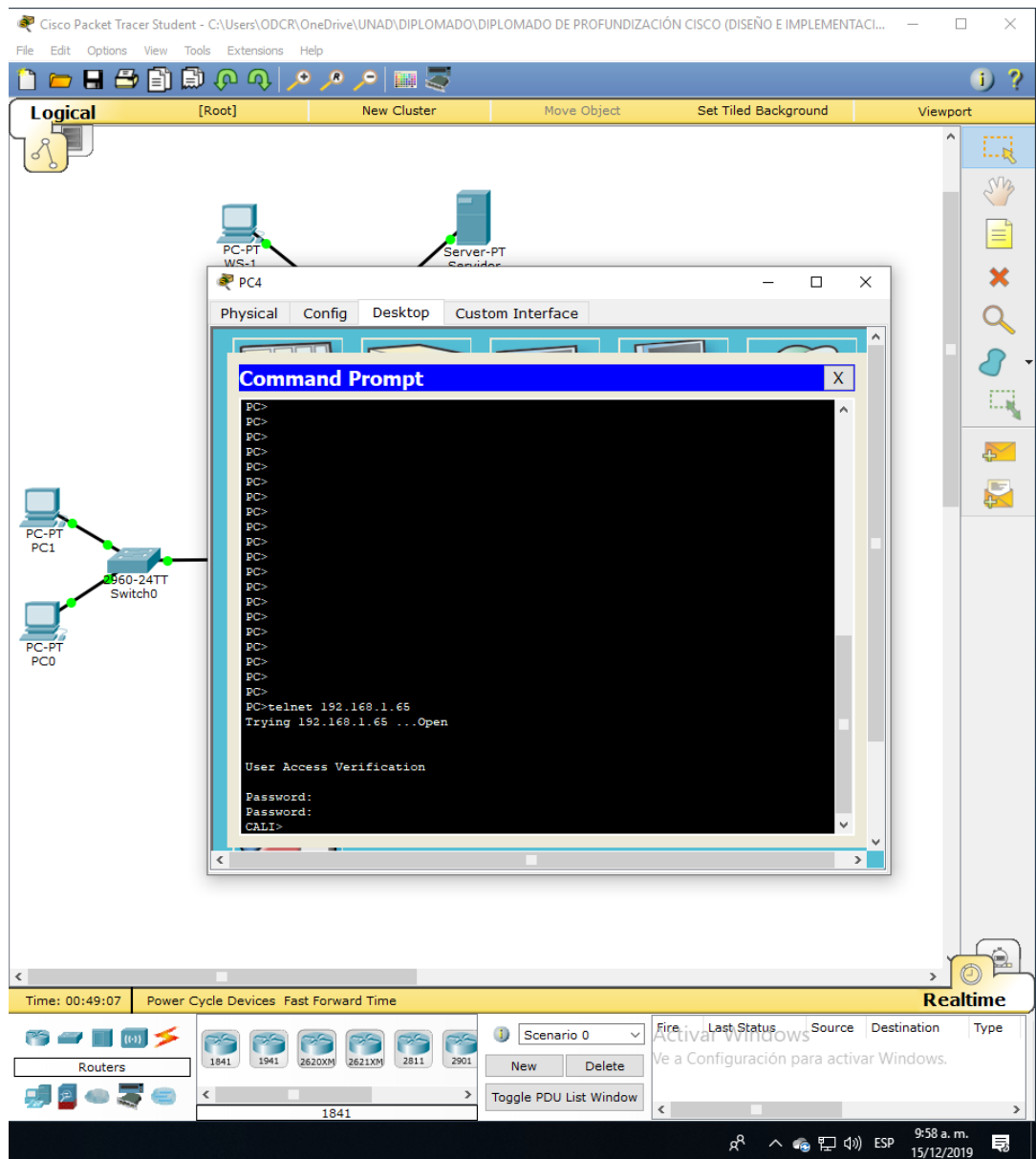


Figura 16.Habilitacion Telnet Router Cali.

- 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.

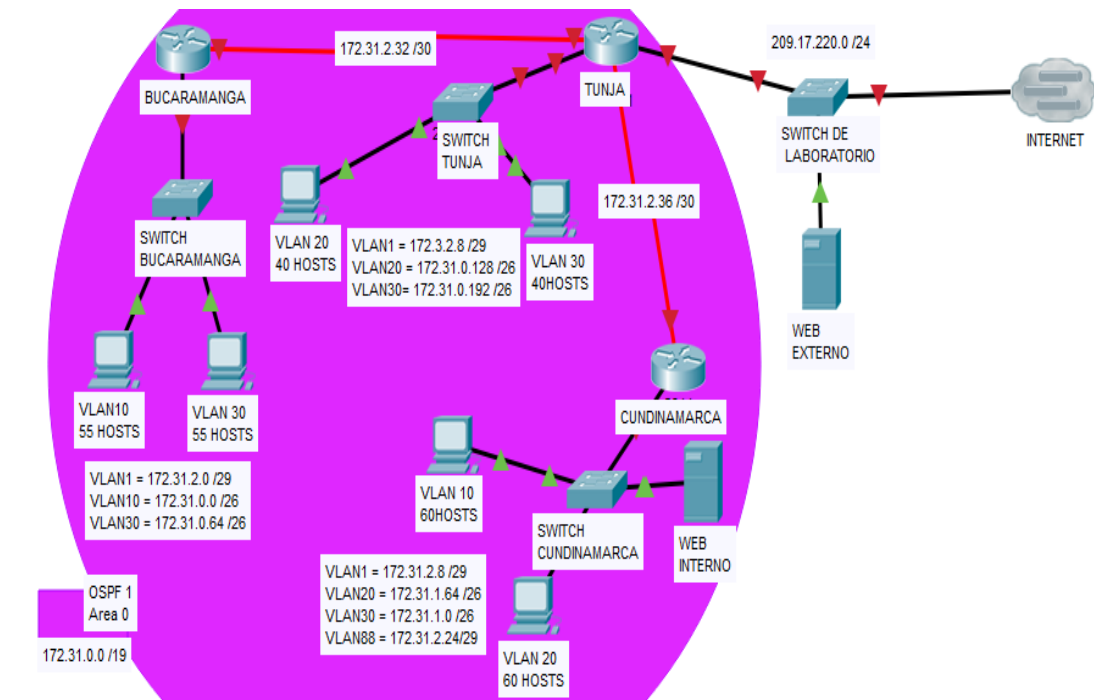


Figura 17. Diseño de red escenario 2.

Topología de red

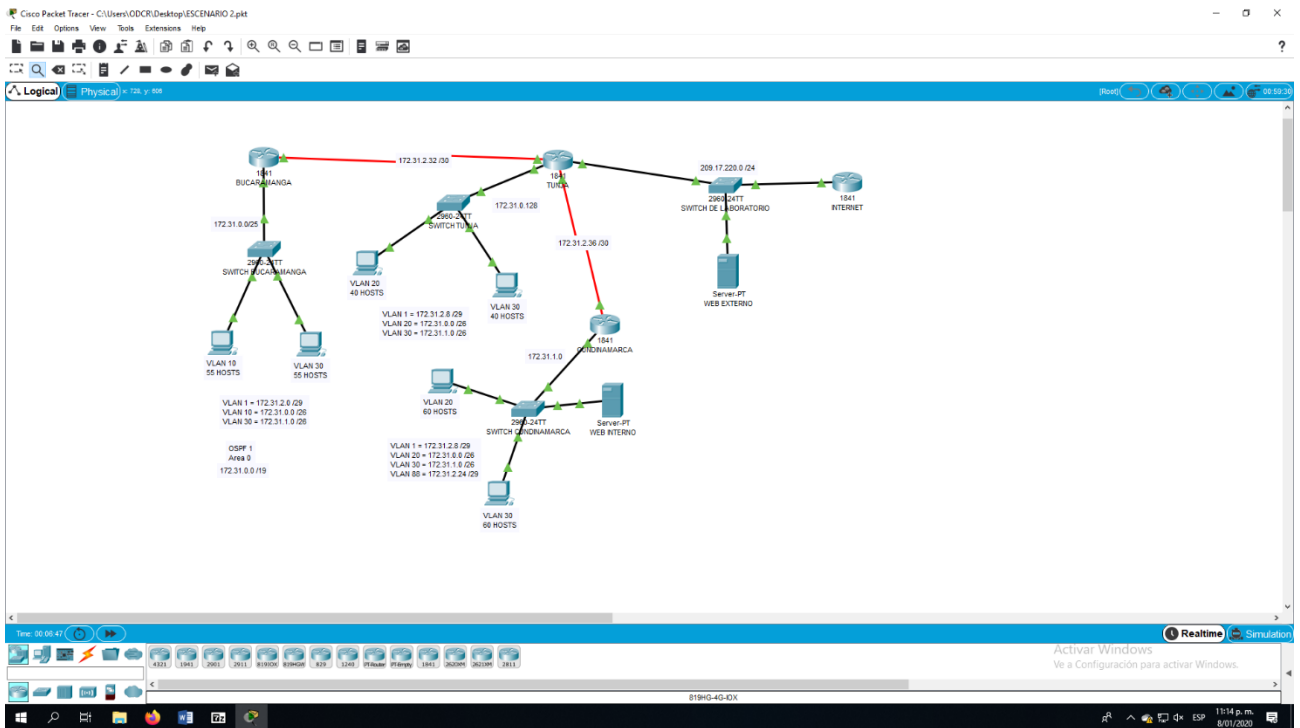


Figura 18. Topología de red escenario 2.

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
```

```
Router>en
Router>enable
Router#conf
Router#configure ter
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router (config)#hostname CUNDINAMARCA
CUNDINAMARCA (config)#no ip domain-lookup
CUNDINAMARCA (config)#enable secret class
CUNDINAMARCA (config)#username CISCO password CLASS
CUNDINAMARCA (config)#aaa new-model
CUNDINAMARCA (config)#aaa authentication login LOCAL local
CUNDINAMARCA (config)#line console 0
CUNDINAMARCA (config-line)#password cisco
CUNDINAMARCA (config-line)#login authentication LOCAL
CUNDINAMARCA (config-line)#exec-timeout 5 0
CUNDINAMARCA (config-line)#line vty 0 15
CUNDINAMARCA (config-line)#login authentication LOCAL
CUNDINAMARCA (config-line)#password cisco
CUNDINAMARCA (config-line)#exec-timeout 5 0
CUNDINAMARCA (config-line)#exit
CUNDINAMARCA (config)#banner motd #
Enter TEXT message. End with the character '#'.

Prohibido el acceso a personal no autorizado!!!
-----
#
CUNDINAMARCA (config)#
CUNDINAMARCA (config)#service password-encryption
CUNDINAMARCA (config)#login block-for 300 attempt 3 within 60
CUNDINAMARCA (config)#exit
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console

CUNDINAMARCA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CUNDINAMARCA#int s0/0/0
^
% Invalid input detected at '^' marker.

CUNDINAMARCA#ip address 172.31.2.38 255.255.255.252
^
% Invalid input detected at '^' marker.

CUNDINAMARCA#no shutdown
^
% Invalid input detected at '^' marker.

CUNDINAMARCA#int fa0/0
^
% Invalid input detected at '^' marker.

CUNDINAMARCA#ip address 209.17.220.4 255.255.255.0
^
% Invalid input detected at '^' marker.
```

Activar Windows
Ve a Configuración para activar Windows.

Copy Paste

Ctrl+F6 to exit CLI focus

Top

10:16 p. m.
8/01/2020

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
```

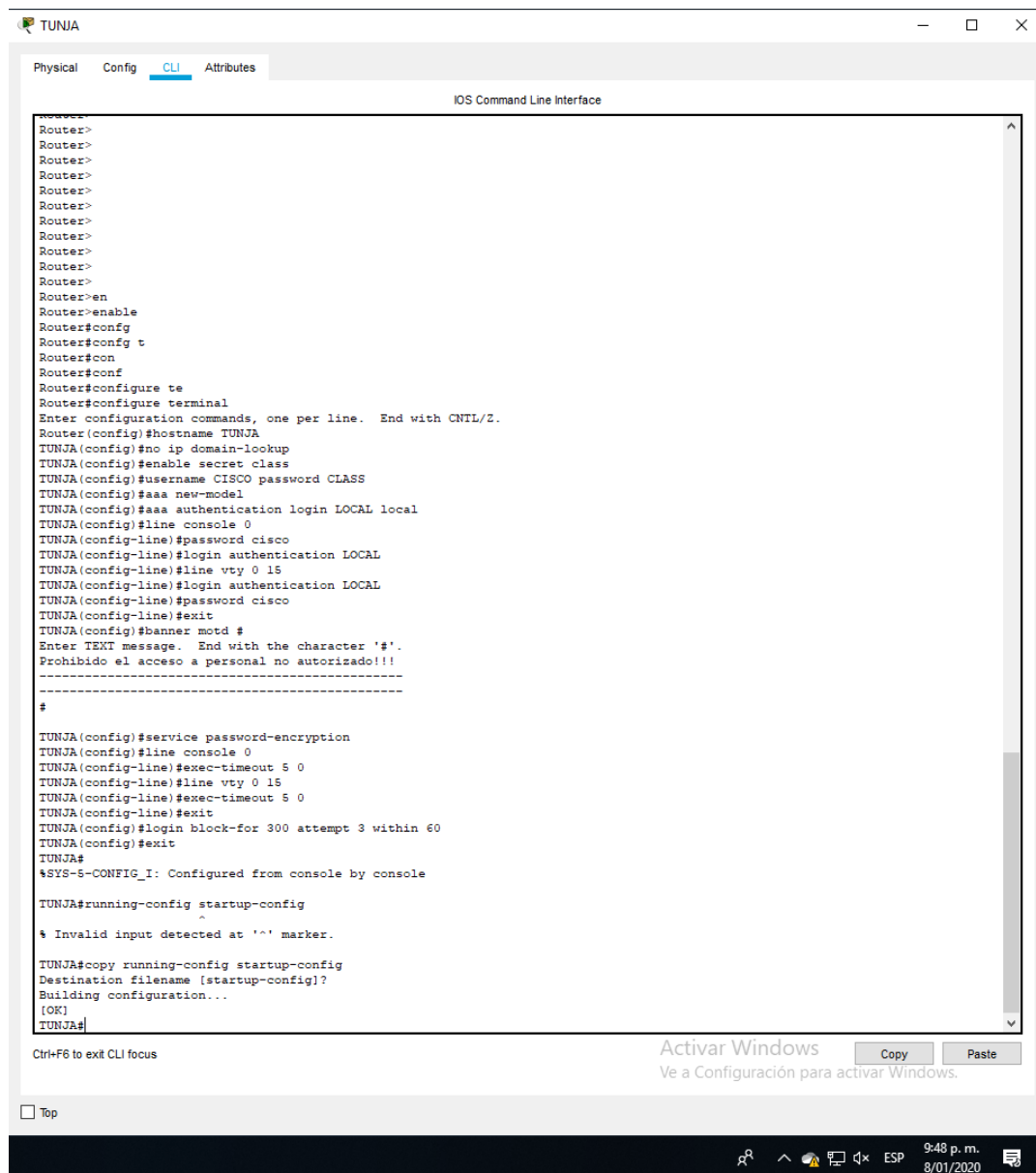


Figura 20. Configuración básica router TUNJA 1.

```

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

```

```

TUNJA(config-line)#password 123456
TUNJA(config-line)#exit
TUNJA(config)#banner motd #
Enter TEXT message. End with the character '#'.
Prohibido el acceso a personal no autorizado!!!
-----
#
TUNJA(config)#service password-encryption
TUNJA(config)#line console 0
TUNJA(config-line)#exec-timeout 5 0
TUNJA(config-line)#line vty 0 15
TUNJA(config-line)#exec-timeout 5 0
TUNJA(config-line)#exit
TUNJA(config)#login block-for 300 attempt 3 within 60
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console

TUNJA#running-config startup-config
^
% Invalid input detected at '^' marker.

TUNJA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
TUNJA#int fa0/0
^
% Invalid input detected at '^' marker.

TUNJA#conf
TUNJA#configure ter
TUNJA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#no ip address 209.17.220.3 255.255.255.0
^
% Invalid input detected at '^' marker.

TUNJA(config)#int
TUNJA(config)#int fa
TUNJA(config)#int fa 0/0
TUNJA(config-if)#no ip address 209.17.220.3 255.255.255.0
TUNJA(config-if)#ip address 209.17.220.1 255.255.255.0
TUNJA(config-if)#exit
TUNJA(config)#int fa0/0
TUNJA(config-if)#ip address 172.31.0.129 255.255.255.128
% Ambiguous command: "p address 172.31.0.129 255.255.255.128"
TUNJA(config-if)#ip address 172.31.0.129 255.255.255.128
TUNJA(config-if)#no
TUNJA(config-if)#no s
TUNJA(config-if)#no sh
TUNJA(config-if)#no shutdown

TUNJA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

TUNJA(config-if)#

```

Activar Windows
Ve a Configuración para activar Windows.

Copy Paste

Ctrl+F6 to exit CLI focus

Top

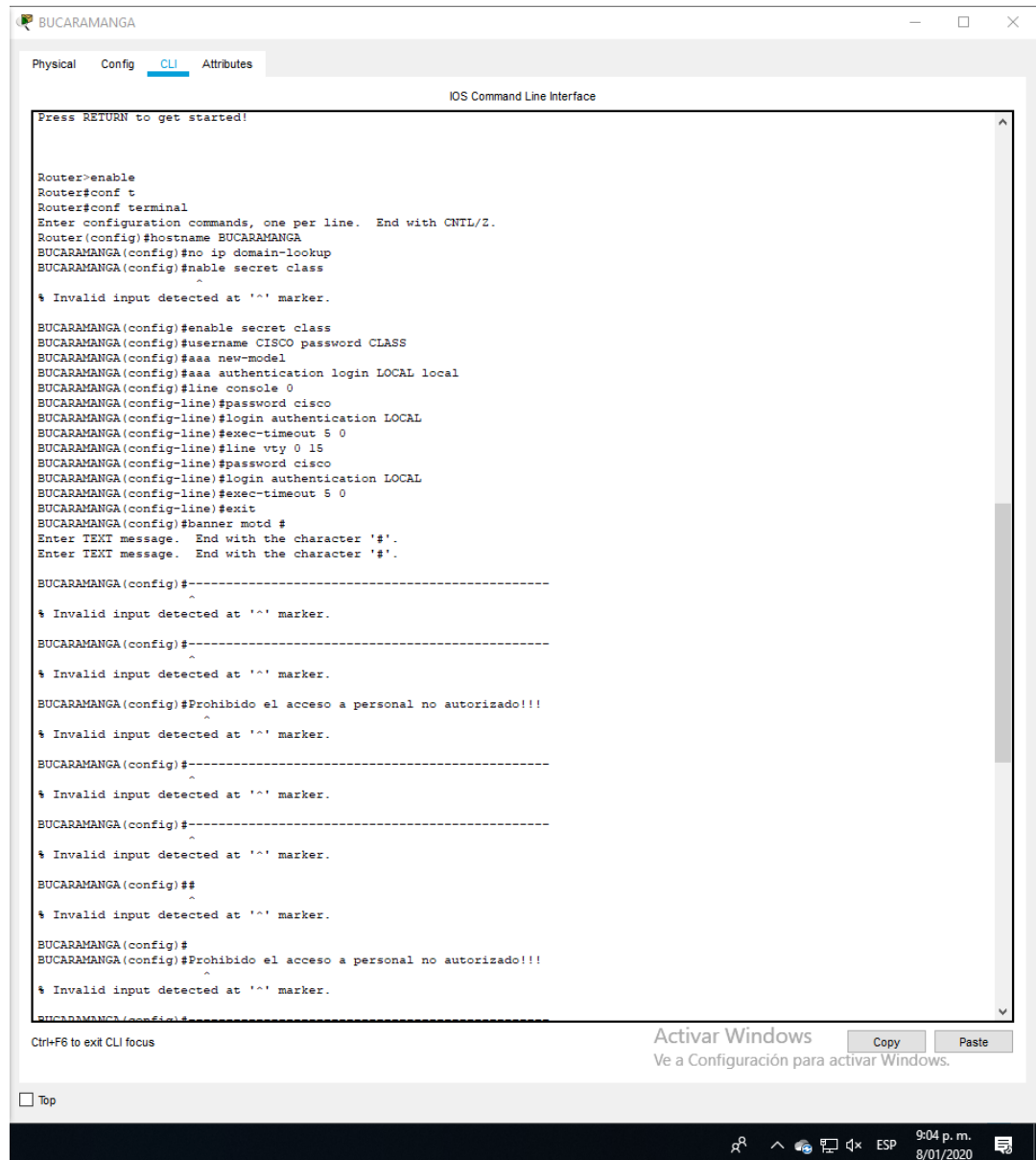
9:50 p. m.
8/01/2020

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



```
Press RETURN to get started!

Router>enable
Router#conf t
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router (config)#hostname BUCARAMANGA
BUCARAMANGA(config)#no ip domain-lookup
BUCARAMANGA(config)#enable secret class
^
% Invalid input detected at '^' marker.

BUCARAMANGA(config)#enable secret class
BUCARAMANGA(config)#username CISCO password CLASS
BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#aaa authentication login LOCAL local
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#password cisco
BUCARAMANGA(config-line)#login authentication LOCAL
BUCARAMANGA(config-line)#exec-timeout 5 0
BUCARAMANGA(config-line)#line vty 0 15
BUCARAMANGA(config-line)#password cisco
BUCARAMANGA(config-line)#login authentication LOCAL
BUCARAMANGA(config-line)#exec-timeout 5 0
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#banner motd #
Enter TEXT message. End with the character '#'.
Enter TEXT message. End with the character '#'.

BUCARAMANGA(config)#-----
^
% Invalid input detected at '^' marker.

BUCARAMANGA(config)#-----
^
% Invalid input detected at '^' marker.

BUCARAMANGA(config)#Prohibido el acceso a personal no autorizado!!!
^
% Invalid input detected at '^' marker.

BUCARAMANGA(config)#-----
^
% Invalid input detected at '^' marker.

BUCARAMANGA(config)#-----
^
% Invalid input detected at '^' marker.

BUCARAMANGA(config)##
^
% Invalid input detected at '^' marker.

BUCARAMANGA(config)#
BUCARAMANGA(config)#Prohibido el acceso a personal no autorizado!!!
^
% Invalid input detected at '^' marker.

BUCARAMANGA(config)#
```

Activar Windows
Ve a Configuración para activar Windows.

Copy Paste

Ctrl+F6 to exit CLI focus

Top

9:04 p. m.
8/01/2020

Figura 22. Configuración básica router BUCARAMANGA 1.

```
BUCARAMANGA
Physical Config CLI Attributes
IOS Command Line Interface
BUCARAMANGA(config)#Prohibido el acceso a personal no autorizado!!!
^
% Invalid input detected at '^' marker.
BUCARAMANGA(config)#-----
^
% Invalid input detected at '^' marker.
BUCARAMANGA(config)#-----
^
% Invalid input detected at '^' marker.
BUCARAMANGA(config)##
^
% Invalid input detected at '^' marker.
BUCARAMANGA(config)#banner motd #
Enter TEXT message. End with the character '#'.
Prohibido el acceso a personal no autorizado!!!#
BUCARAMANGA(config)#service password-encryption
BUCARAMANGA(config)#login block-for 300 attempt 3 within 60
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
BUCARAMANGA#int s0/0/0
^
% Invalid input detected at '^' marker.
BUCARAMANGA#interface s0/0/0
^
% Invalid input detected at '^' marker.
BUCARAMANGA#conf
BUCARAMANGA#configure te
BUCARAMANGA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#int s0/0/0
BUCARAMANGA(config-if)#ip address 172.31.2.34 255.255.255.252
BUCARAMANGA(config-if)#no shutdown
BUCARAMANGA(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
BUCARAMANGA(config-if)#int fa0/0
BUCARAMANGA(config-if)#ip address 172.31.0.129 255.255.255.128
BUCARAMANGA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
BUCARAMANGA(config-if)#no shutdown
BUCARAMANGA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Ctrl+F6 to exit CLI focus
Activar Windows
Ve a Configuración para activar Windows.
Copy Paste
Top
9:04 p. m.
8/01/2020
```

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

```
CUNDINAMARCA con0 is now available

Press RETURN to get started.

Prohibido el acceso a personal no autorizado!!!
-----

User Access Verification
Username:
Username: CISCO
Password:
CUNDINAMARCA>enab
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#show flash

System flash directory:
File Length Name/status
 3 33591768 c1841-advipservicesk9-mz.124-15.T1.bin
 2 28282 sigdef-category.xml
 1 227537 sigdef-default.xml
[33847587 bytes used, 30168797 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)

CUNDINAMARCA#copy flash tftp
Source filename []?
?File name not specified
*Error parsing filename (Unknown error 0)

CUNDINAMARCA#
```

Figura 24. Activación servidor TFTP router CUNDINAMARCA.

ROUTER BUCARAMANGA

show flash
copy flash tftp



```
BUCARAMANGA con0 is now available

Press RETURN to get started.

Prohibido el acceso a personal no autorizado!!!

User Access Verification

Username: CISCO
Password:
BUCARAMANGA>ena
BUCARAMANGA>enable
Password:
Password:
? Bad secrets

BUCARAMANGA>en
BUCARAMANGA>enable
Password:
BUCARAMANGA#show
BUCARAMANGA#show f
BUCARAMANGA#show flash

System flash directory:
File Length Name/status
 3 33591768 c1841-advipservicesk9-mz.124-15.T1.bin
 2 28282 sigdef-category.xml
 1 227537 sigdef-default.xml
[33847587 bytes used, 30168797 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)

BUCARAMANGA#copy flash tftp
Source filename []?
```

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

```

```

TUNJA#show flash
System flash directory:
File Length Name/status
 3 33591768 c1941-advipsservicesk9-mz.124-15.T1.bin
 2 28282 sigdef-category.xml
 1 227537 sigdef-default.xml
[33847587 bytes used, 30168797 available, 64016384 total]
63498K bytes of processor board System flash (Read/Write)

TUNJA#copy flash tftp
Source filename []?
?File name not specified
%Error parsing filename (Unknown error 0)

TUNJA#conf
TUNJA#configure ter
TUNJA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA (config)#ip nat inside source static 209.17.220.4 172.31.2.33
TUNJA (config)#int fa0/0
TUNJA (config-if)#ip nat inside
TUNJA (config-if)#int s0/0/0
TUNJA (config-if)#ip nat outside
TUNJA (config-if)#ip nat pool NATPOOL 172.31.2.33 172.31.2.34 netmask 255.255.255.252
TUNJA (config)#access-list 1 permit 172.31.0.0 0.0.0.63
TUNJA (config)#access-list 2 permit 172.31.1.0 0.0.0.63
TUNJA (config)#ip nat inside source list 1 pool NATPOOL overload
TUNJA (config)#ip nat inside source list 2 pool NATPOOL overload
TUNJA (config)#int fa0/1
TUNJA (config-if)#ip nat inside
TUNJA (config-if)#int s0/0/0
TUNJA (config-if)#ip nat outside
TUNJA (config-if)#

```

Figura 28. Asignación 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
```

```
BUCARAMANGA#
BUCARAMANGA#
BUCARAMANGA con0 is now available
|
Press RETURN to get started.

Prohibido el acceso a personal no autorizado!!!
User Access Verification

Username: cisco
Password:
% Login invalid

Username: CISCO
Password:
BUCARAMANGA#en
BUCARAMANGA#enable
Password:
BUCARAMANGA#ip nat pool NATBUC 172.31.2.33 172.31.2.34 netmask 255.255.255.252
^
% Invalid input detected at '^' marker.

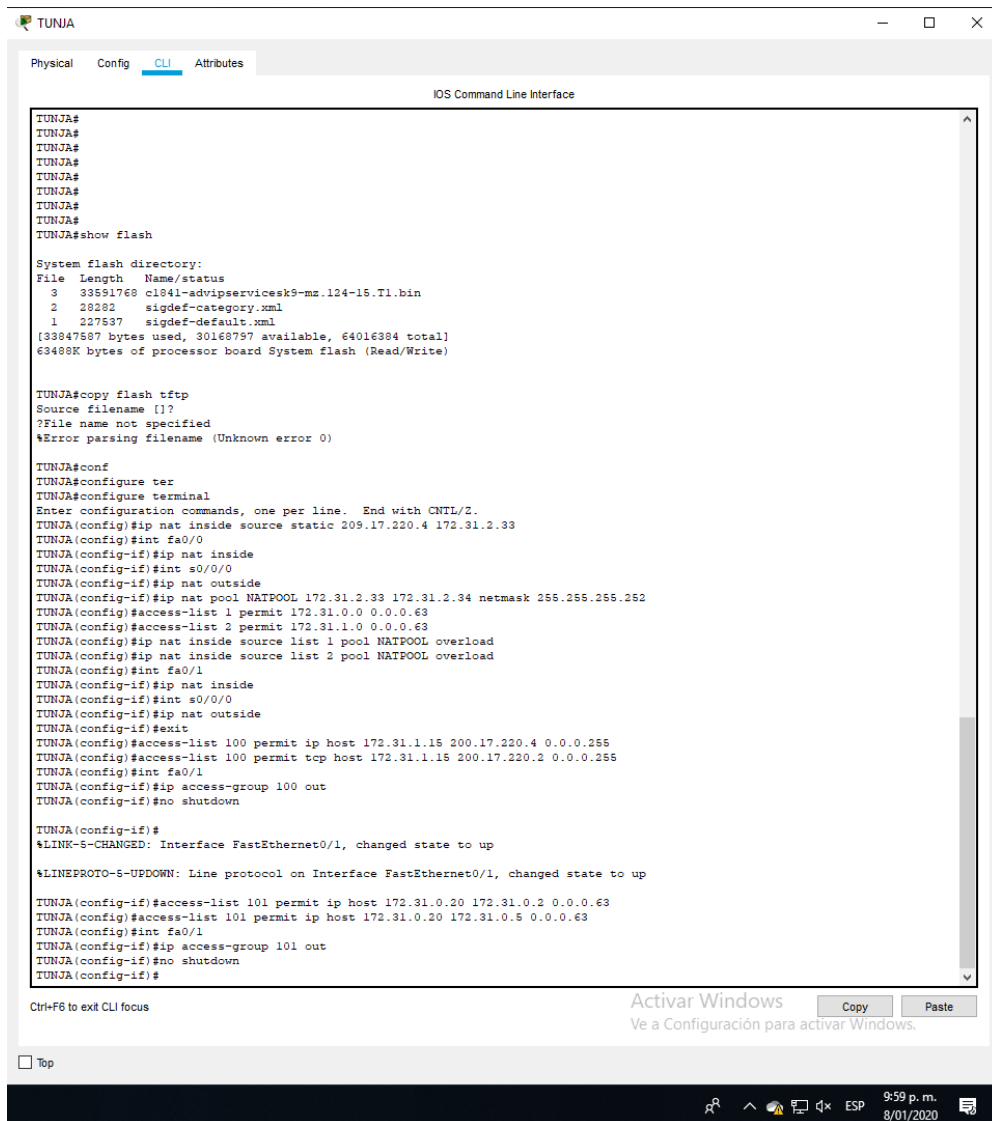
BUCARAMANGA#conf
BUCARAMANGA#configure t
BUCARAMANGA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#ip nat pool NATBUC 172.31.2.33 172.31.2.34 netmask 255.255.255.252
BUCARAMANGA(config)#access-list 1 permit 172.31.0.0 0.0.0.63
BUCARAMANGA(config)#access-list 2 permit 172.31.1.0 0.0.0.63
BUCARAMANGA(config)#ip nat inside source list 1 pool NATBUC overload
BUCARAMANGA(config)#ip nat inside source list 2 pool NATBUC overload
BUCARAMANGA(config)#int fa0/0
BUCARAMANGA(config-if)#ip nat inside
BUCARAMANGA(config-if)#int s0/0/0
BUCARAMANGA(config-if)#ip nat outside
BUCARAMANGA(config-if)#
```

Figura 29. Asignación NAT router BUCARAMANGA.

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
```



The screenshot shows the TUNJA router's CLI interface with the following commands and output:

```
TUNJA#
TUNJA#
TUNJA#
TUNJA#
TUNJA#
TUNJA#
TUNJA#show flash

System flash directory:
File Length Name/status
 3 33591768 cl84l-advipervicesk9-mz.124-15.Tl.bin
 2 26282 sigdef-category.xml
 1 227537 sigdef-default.xml
[33847587 bytes used, 30168797 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)

TUNJA#copy flash tftp
Source filename []?
?File name not specified
%Error parsing filename (Unknown error 0)

TUNJA#conf
TUNJA#configure ter
TUNJA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#ip nat inside source static 209.17.220.4 172.31.2.33
TUNJA(config)#int fa0/0
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#int s0/0/0
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#ip nat pool NATPOOL 172.31.2.33 172.31.2.34 netmask 255.255.255.252
TUNJA(config)#access-list 1 permit 172.31.0.0 0.0.0.63
TUNJA(config)#access-list 2 permit 172.31.1.0 0.0.0.63
TUNJA(config)#ip nat inside source list 1 pool NATPOOL overload
TUNJA(config)#ip nat inside source list 2 pool NATPOOL overload
TUNJA(config)#int fa0/1
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#int s0/0/0
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#exit
TUNJA(config)#access-list 100 permit ip host 172.31.1.15 200.17.220.4 0.0.0.255
TUNJA(config)#access-list 100 permit tcp host 172.31.1.15 200.17.220.2 0.0.0.255
TUNJA(config)#int fa0/1
TUNJA(config-if)#ip access-group 100 out
TUNJA(config-if)#no shutdown

TUNJA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

TUNJA(config-if)#access-list 101 permit ip host 172.31.0.20 172.31.0.2 0.0.0.63
TUNJA(config)#access-list 101 permit ip host 172.31.0.20 172.31.0.5 0.0.0.63
TUNJA(config)#int fa0/1
TUNJA(config-if)#ip access-group 101 out
TUNJA(config-if)#no shutdown
TUNJA(config-if)#
```

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
```

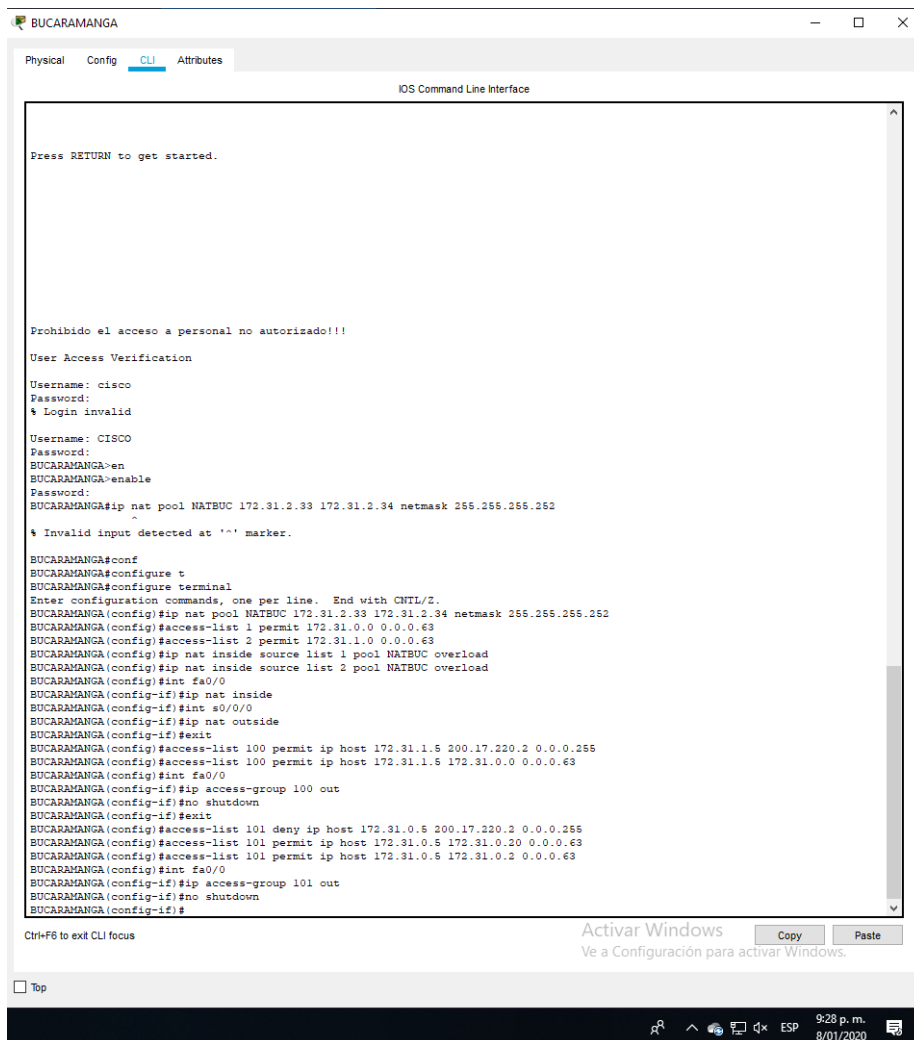
```
access-list 101 permit ip host 172.31.0.5 172.31.0.20 0.0.0.63
```

```
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
```



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

Press RETURN to get started.

Prohibido el acceso a personal no autorizado!!!

User Access Verification
Username: cisco
Password:
* Login invalid
Username: CISCO
Password:
BUCARAMANGA>en
BUCARAMANGA#enable
Password:
BUCARAMANGA#ip nat pool NATBUC 172.31.2.33 172.31.2.34 netmask 255.255.255.252
^
* Invalid input detected at '^' marker.

BUCARAMANGA#conf
BUCARAMANGA#configure t
BUCARAMANGA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#ip nat pool NATBUC 172.31.2.33 172.31.2.34 netmask 255.255.255.252
BUCARAMANGA(config)#access-list 1 permit 172.31.0.0 0.0.0.63
BUCARAMANGA(config)#access-list 2 permit 172.31.1.0 0.0.0.63
BUCARAMANGA(config)#ip nat inside source list 1 pool NATBUC overload
BUCARAMANGA(config)#ip nat inside source list 2 pool NATBUC overload
BUCARAMANGA(config)#int fa0/0
BUCARAMANGA(config-if)#ip nat inside
BUCARAMANGA(config-if)#int s0/0/0
BUCARAMANGA(config-if)#ip nat outside
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#access-list 100 permit ip host 172.31.1.5 200.17.220.2 0.0.0.255
BUCARAMANGA(config)#access-list 100 permit ip host 172.31.1.5 172.31.0.0 0.0.0.63
BUCARAMANGA(config)#int fa0/0
BUCARAMANGA(config-if)#ip access-group 100 out
BUCARAMANGA(config-if)#no shutdown
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#access-list 101 deny ip host 172.31.0.5 200.17.220.2 0.0.0.255
BUCARAMANGA(config)#access-list 101 permit ip host 172.31.0.5 172.31.0.20 0.0.0.63
BUCARAMANGA(config)#access-list 101 permit ip host 172.31.0.5 172.31.0.2 0.0.0.63
BUCARAMANGA(config)#int fa0/0
BUCARAMANGA(config-if)#ip access-group 101 out
BUCARAMANGA(config-if)#no shutdown
BUCARAMANGA(config-if)#
BUCARAMANGA(config-if)#
```

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 acceso 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

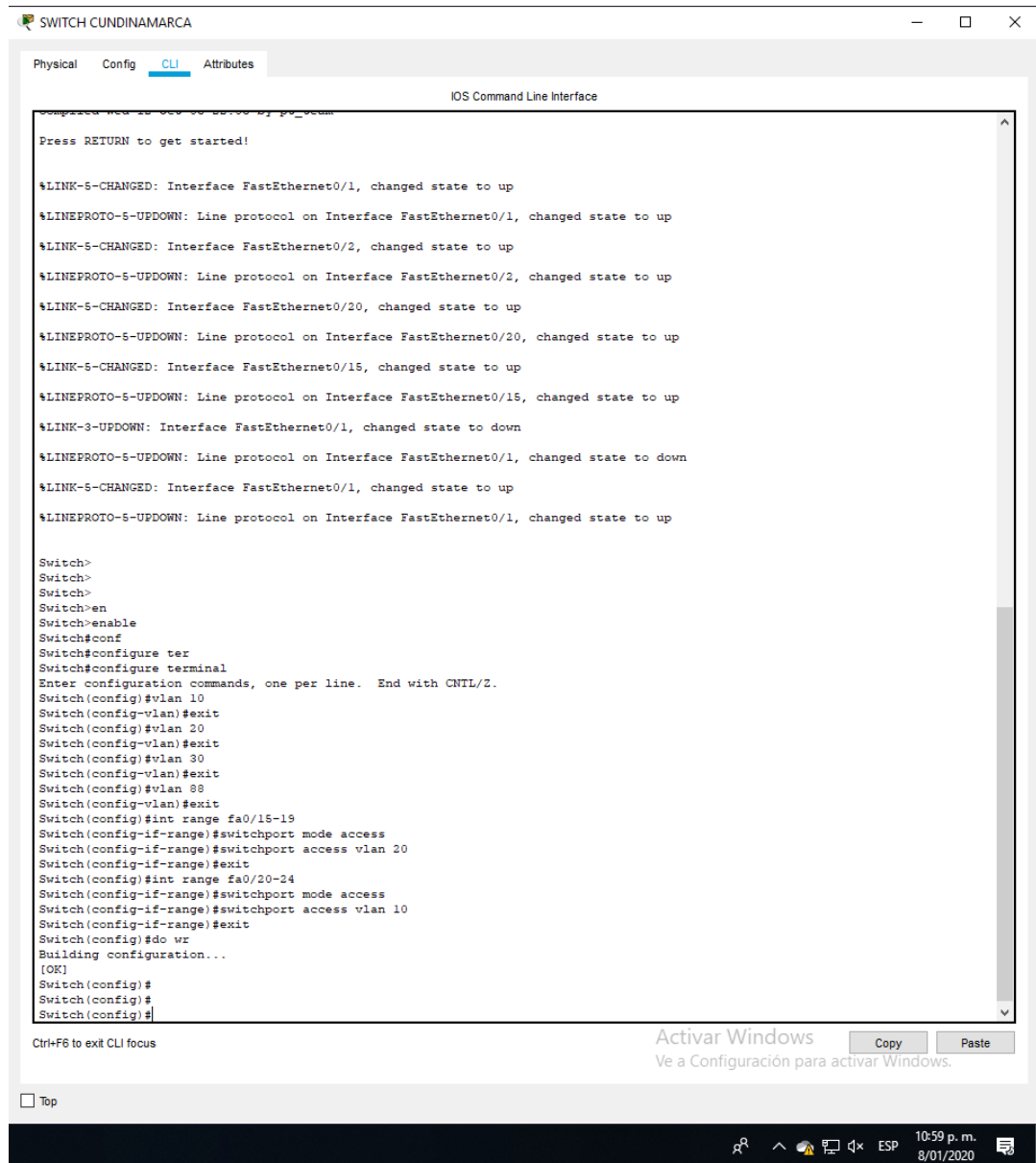


Figura 33.Creación VLAN switch CUNDINAMARCA.

ROUTER CUNDINAMARCA

```
Enable
Configure terminal
int fa0/0.20
encapsulation dot1Q 20
```


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
```

```
TUNJA#conf
TUNJA#configure ter
TUNJA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#ip nat inside source static 209.17.220.4 172.31.2.33
TUNJA(config)#int fa0/0
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#int s0/0/0
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#ip nat pool NATPOOL 172.31.2.33 172.31.2.34 netmask 255.255.255.252
TUNJA(config)#access-list 1 permit 172.31.0.0 0.0.0.63
TUNJA(config)#access-list 2 permit 172.31.1.0 0.0.0.63
TUNJA(config)#ip nat inside source list 1 pool NATPOOL overload
TUNJA(config)#ip nat inside source list 2 pool NATPOOL overload
TUNJA(config)#int fa0/1
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#int s0/0/0
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#exit
TUNJA(config)#access-list 100 permit ip host 172.31.1.15 200.17.220.4 0.0.0.255
TUNJA(config)#access-list 100 permit tcp host 172.31.1.15 200.17.220.2 0.0.0.255
TUNJA(config)#int fa0/1
TUNJA(config-if)#ip access-group 100 out
TUNJA(config-if)#no shutdown
TUNJA(config-if)#

TUNJA(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

TUNJA(config-if)#access-list 101 permit ip host 172.31.0.20 172.31.0.2 0.0.0.63
TUNJA(config)#access-list 101 permit ip host 172.31.0.20 172.31.0.5 0.0.0.63
TUNJA(config)#int fa0/1
TUNJA(config-if)#ip access-group 101 out
TUNJA(config-if)#no shutdown
TUNJA(config-if)#
TUNJA(config-if)#exit
TUNJA(config)#int fa0/1.20
TUNJA(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/1.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1.20, changed state to up

TUNJA(config-subif)#encapsulation dot1Q 20
TUNJA(config-subif)#ip address 172.31.0.1 255.255.255.192
TUNJA(config-subif)#no shutdown
TUNJA(config-subif)#int fa0/1.30
TUNJA(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/1.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1.30, changed state to up

TUNJA(config-subif)#encapsulation dot1Q 30
TUNJA(config-subif)#ip address 172.31.1.1 255.255.255.192
TUNJA(config-subif)#no shutdown
TUNJA(config-subif)#
```

Activar Windows
Ve a Configuración para activar Windows.

Copy Paste

Ctrl+F6 to exit CLI focus

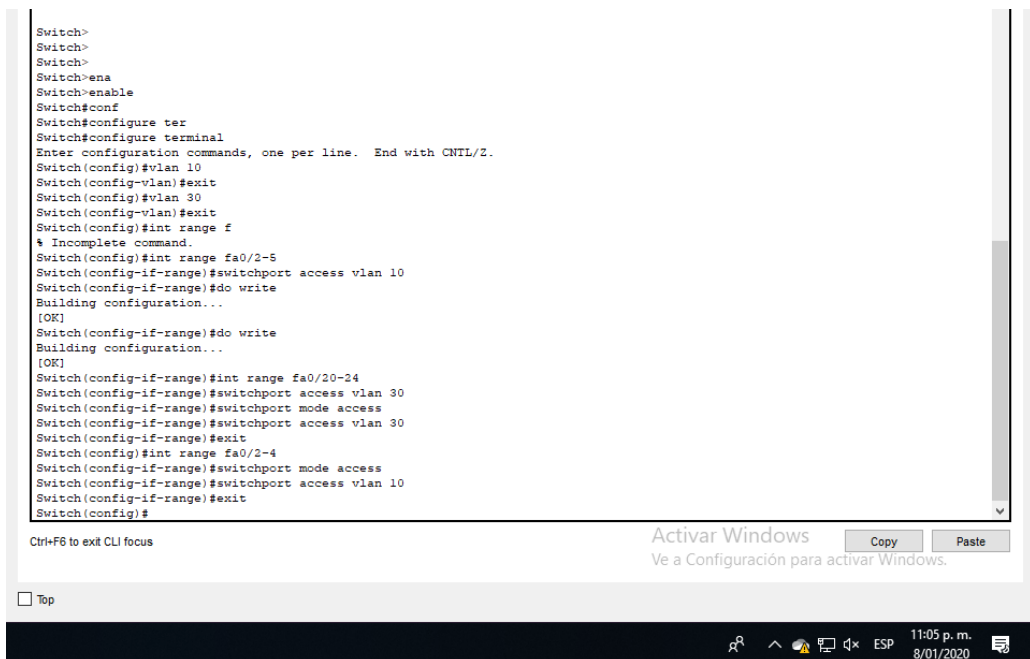
Top

10:02 p. m.
8/01/2020

Figura 37. Encapsulación 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
```



```
Switch>
Switch>
Switch>
Switch>ena
Switch#enable
Switch#conf
Switch#configure ter
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#exit
Switch(config)#int range f
* Incomplete command.
Switch(config)#int range fa0/2-5
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#do write
Building configuration...
[OK]
Switch(config-if-range)#do write
Building configuration...
[OK]
Switch(config-if-range)#int range fa0/20-24
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
Switch(config)#int range fa0/2-4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#
```

Activar Windows
Ve a Configuración para activar Windows.

Copy Paste

Ctrl+F6 to exit CLI focus

Top

11:05 p. m.
8/01/2020

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
```

```
Press RETURN to get started.

Prohibido el acceso a personal no autorizado!!!

User Access Verification

Username: CISCO
Password:
BUCARAMANGA>en
BUCARAMANGA>enable
Password:
Password:
BUCARAMANGA#int fa0/0.10
^
% Invalid input detected at '^' marker.

BUCARAMANGA#conf
BUCARAMANGA(config)#configure te
BUCARAMANGA(config)#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#int fa0/0.10
BUCARAMANGA(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed state to up

BUCARAMANGA(config-subif)#encapsulation dot1Q 10
BUCARAMANGA(config-subif)#ip address 172.31.0.1 255.255.255.192
BUCARAMANGA(config-subif)#no shutdown
BUCARAMANGA(config-subif)#int fa0/0.30
BUCARAMANGA(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up

BUCARAMANGA(config-subif)#encapsulation dot1Q 30
BUCARAMANGA(config-subif)#ip address 172.31.1.1 255.255.255.192
BUCARAMANGA(config-subif)#no shutdown
BUCARAMANGA(config-subif)#
```

Activar Windows
Ve a Configuración para activar Windows.

Copy Paste

Ctrl+F6 to exit CLI focus

Top

9:36 p. m.
8/01/2020

Figura 40. Encapsulación router BUCARAMANGA.

```
BUCARAMANGA (config-subif)#  
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up  
  
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up  
  
BUCARAMANGA (config-subif)#encapsulation dot1Q 30  
BUCARAMANGA (config-subif)#ip address 172.31.1.1 255.255.255.192  
BUCARAMANGA (config-subif)#no shutdown  
BUCARAMANGA (config-subif)#  
  
BUCARAMANGA con0 is now available  
  
Press RETURN to get started.  
  
Prohibido el acceso a personal no autorizado!!!  
User Access Verification  
Username: CISCO  
Password:  
BUCARAMANGA>en  
BUCARAMANGA>enable  
Password:  
BUCARAMANGA#conf  
BUCARAMANGA#configure te  
BUCARAMANGA#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
BUCARAMANGA (config)#router ospf 1  
BUCARAMANGA (config-router)#network 172.31.2.32 0.0.0.3 area 0  
BUCARAMANGA (config-router)#network 172.31.0.0 0.0.0.127 area 0  
BUCARAMANGA (config-router)#exit  
BUCARAMANGA (config)#int s0/0/0  
BUCARAMANGA (config-if)#ip ospf authentication-key cisco  
BUCARAMANGA (config-if)#ip ospf authentication  
BUCARAMANGA (config-if)#  
00:45:46: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.4 on Serial0/0/0 from LOADING to FULL, Loading Done
```

Activar Windows
Ve a Configuración para activar Windows.

Copy Paste

Ctrl+F6 to exit CLI focus

Top

9:44 p. m.
8/01/2020

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!AmlJYei-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!AmlJYei-NT1Im3GQVfFFrjnEGFFU>