

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

Presentado por:  
Gustavo Adolfo Osorio

Presentado a:  
NILSON ALBEIRO FERREIRA MANZANARES  
Ingeniero de sistemas magister en educación  
Grupo: 203092\_33

Universidad Nacional Abierta y a Distancia  
Ingeniería de sistemas  
Diplomado de cisco CCNA  
UNAD  
Diciembre de 2019

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

GUSTAVO ADOLFO OSORIO

Universidad Nacional Abierta y a Distancia  
Ingeniería de sistemas  
Diplomado de cisco CCNA  
UNAD  
Diciembre de 2019

Nota de aceptación

---

---

---

---

---

---

---

Firma del presidente del jurado

---

Firma del jurado

---

Firma del jurado

**Dos quebradas, 12 de diciembre de 2019**

## **DEDICATORIA**

Este libro está dedicado a mi bella esposa, Maryuris y mi hermoso hijo, Juan Pablo, a mi madre, María Belén y mi padre, Gilberto. Por su inmensa comprensión, su apoyo incondicional, el gran amor y una enorme empatía, son siempre la fuerza que me impulsa a seguir adelante en mi vida.

## **AGRADECIMIENTOS**

Me gustaría agradecer a todo mis inolvidables compañeros de curso por su excelente apoyo, por los aciertos y desaciertos. Pero siempre con el objetivo de hacer las cosas lo mejor posible generando un aprendizaje de alta calidad. Gracias también al personal de la UNAD por su excelente apoyo y recomendación, especialmente al Ing. Nilson Albeiro Ferreira Manzanares, por impulsarme a mejorar constantemente, revisando hasta el último detalle para que realizara todo al 100%.

## TABLA DE CONTENIDO

### Contenido

Resumen .....	10
Abstract.....	10
Introducción .....	11
objetivos.....	12
Objetivo general .....	12
Objetivos especificos.....	12
<b>Descripción de escenarios propuestos para la prueba de habilidades .....</b>	<b>13</b>
<b>Escenario 1.....</b>	<b>13</b>
Desarrollo .....	14
Parte 1: Asignación de direcciones IP. ....	17
Parte 2: Configuración Básica. ....	17
Parte 3: Configuración de Enrutamiento.....	22
Parte 4: Configuración de las listas de Control de Acceso. ....	27
Parte 5: Comprobación de la red instalada.....	35
<b>Escenario 2.....</b>	<b>39</b>
Desarrollo .....	40
Parte 1: Configuración básica. ....	40
Configuración de los router.....	40
parte 2: Configuración avanzada.....	45
Autenticación local con AAA.....	45
Cifrado de contraseñas.....	46
Máximo de internos para acceder al router y máximo tiempo de acceso al detectar ataques. ....	46
Establecer un servidor TFTP que almacene todos los archivos necesarios de los routers.....	47
El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca. ....	49
El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).....	51
El enrutamiento deberá tener autenticación. ....	52
Listas de control de acceso: .....	60

Habilitar VLAN en cada switch y permitir su enrutamiento. ....70  
Conclusiones .....74  
Bibliografía.....75

## TABLA DE ILUSTRACIONES

Ilustración 1. Escenario 1 .....	13
Ilustración 2. Configuración Host de Routers Medellín, Bogotá y Cali .....	14
Ilustración 3. Conexión física de los equipos con base en la topología de red escenario 1.....	17
Ilustración 4. Router MEDELLIN Comando “show ip route” .....	20
Ilustración 5. Router BOGOTA Comando “show ip route” .....	20
Ilustración 6. Router CALI Comando “show ip route” .....	20
Ilustración 7. Vecinos Router BOGOTA comando “show cdp neighbors” .....	21
Ilustración 8. Vecinos Router CALI comando “show cdp neighbors”.....	21
Ilustración 9. Vecinos Router MEDELLIN comando “show cdp neighbors” .....	21
Ilustración 10. Prueba de conectividad en cada tramo de la ruta usando Ping. ....	22
Ilustración 11. Vecinos Router CALI comando “show ip eigrp neighbors” .....	24
Ilustración 12. Vecinos Router BOGOTA comando “show ip eigrp neighbors” .....	24
Ilustración 13. Vecinos Router MEDELLIN comando “show ip eigrp neighbors” .....	24
Ilustración 14. Router CALI Comando “show ip route” .....	25
Ilustración 15. Router BOGOTA Comando “show ip route” .....	25
Ilustración 16. Router CALI Comando “show ip route” .....	25
Ilustración 17. Ping desde Servidor a PC1, PC2 y PC3.....	26
Ilustración 18. Ping desde el host PC4 del Router CALI hacia el host PC1 de la red MEDELLIN y al Servidor	26
Ilustración 19. Ilustración 19. Ping desde Servidor a Router Cali. ....	27
Ilustración 20. Ping desde Servidor a PC4, Router Medellín Y Router Bogotá.....	27
Ilustración 21. Ping PC3 a PC4, PC1 y PC2 .....	28
Ilustración 22. Ping PC3 a Router Cali, Router Bogotá y Router Medellín. ....	28
Ilustración 23. Ping PC4 a Router Cali, Route Medellín y Router Bogotá.....	29
Ilustración 24. Ping PC4 a PC3, PC1 y PC2 .....	29
Ilustración 25. Ping de PC1 a Router Cali, Router Medellín y Router Bogotá. ....	30
Ilustración 26. Ping de PC1 a PC2, PC3, PC4. ....	30
Ilustración 28. Ping PC1 a Servidor .....	31
Ilustración 27. Ping PC2 a Servidor .....	31
Ilustración 29. Ping PC4 a Servidor .....	32
Ilustración 30. Ping PC3 a Servidor .....	32
Ilustración 31. Ping de PC2 a Router Cali, Router Medellín y Router Bogotá. ....	33
Ilustración 32. Ping de PC2 a PC1, PC3, PC4. ....	33
Ilustración 33. Ping desde el host PC1 del Router MEDELLIN hacia el Router BOGOTA y CALI. ....	36
Ilustración 34. Ping desde el host PC1 del Router MEDELLIN hacia host PC4 de la red CALI y al WS1 y Servidor. ....	37
Ilustración 35. Ping desde el Servidor hacia PC1 de la red MEDELLIN, al PC4 de la red CALI y al WS1 .....	37
Ilustración 36. Escenario 2.....	39
Ilustración 37. Conexión física de los equipos con base en la topología de red escenario 2.....	40
Ilustración 38. Configuración Ip Servidor Tftp .....	47
Ilustración 39. Activación del servicio TFTP en el servidor interno.. ....	48
Ilustración 40. Archivos Backup almacenados en el servidor TFTP .....	49
Ilustración 41. DHCP host de Bucaramanga Vlan30 .....	56
Ilustración 42. DHCP host de Bucaramanga Vlan10 .....	56
Ilustración 43. DHCP host de Cundinamarca Vlan30.....	57
Ilustración 44. DHCP host de Cundinamarca Vlan20.....	57
Ilustración 45. Comunicación de host de Router Bucaramanga Vlan10 a red Tunja y Vlan20 red Cundinamarca.....	58

Ilustración 46. Comunicación de host de Router Bucaramanga Vlan10 a red Bucaramanda y Servidor Web .....	58
Ilustración 48. Comunicación de host de Router Cundinamarca Vlan30 a red Cundinamarca.....	59
Ilustración 47. Comunicación de host de Router Cundinamarca Vlan30 a red Bucaramanga y Servidor FTP. ....	59
Ilustración 49. Comunicación de host de Router Cundinamarca Vlan30 a Servidor FTP y Servidor Web.....	60
Ilustración 50. Verificacion control de acceso Vlan20 Cundinamarca solo a la red interna de Tunja.....	61
Ilustración 51. Verificacion control de acceso Vlan10 Cundinamarca si acceden a internet y no a la red interna de Tunja.....	61
Ilustración 52. Verificacion control de acceso hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet (servidor web).....	62
Ilustración 53. Verificacion control de acceso hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de interne (servidor ftp). ....	63
Ilustración 54. Verificacion control de acceso hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.....	63
Ilustración 55. Verificacion control de acceso hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10. ....	64
Ilustración 56. Verificacion control de acceso hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.....	65
Ilustración 57. Verificacion control de acceso hosts de VLAN 10 Bucaramanga no pueden acceder los host VLAN 30 en Bucaramanga .....	66
Ilustración 58. Verificacion control de acceso hosts de VLAN 20 Tunja no pueden acceder los host VLAN 30 en Tunja .....	67
Ilustración 59. Verificacion control de acceso hosts de VLAN 30 Bucaramanga no pueden acceder los host VLAN 10 en Bucaramanga .....	67
Ilustración 60. Verificacion control de acceso hosts de VLAN 30 Tunja no pueden acceder los host VLAN 20 en Tunja .....	68
Ilustración 61. Verificacion control de acceso hosts de VLAN 20 Cundinamarca no pueden acceder los host VLAN 30 en Cundinamarca .....	68
Ilustración 62. Verificacion control de acceso hosts de VLAN 30 Cundinamarca no pueden acceder los host VLAN 20 en Cundinamarca .....	69
Ilustración 63. Verificacion control de acceso los hosts de las VLAN administrativas y de la VLAN de servidores tienen acceso a los routers e internet (VLAN Bucaramanga no tienen acceso a los routers e internet).....	70
Ilustración 64. Verificacion control de acceso los hosts de las VLAN administrativas y de la VLAN de servidores tienen acceso a los routers e internet (VLAN Cundinamarca tienen acceso a los routers e internet).....	70

## RESUMEN

El contenido de la prueba de habilidades CCNA describe el enrutamiento en redes de LAN y WAN, que es la base para la configuración de redes básicas. Este trabajo se basa principalmente en el enrutamiento estático y dinámico.

También trata de la configuración de enrutadores y conmutadores, que son los principales elementos para el enrutamiento.

La parte práctica de la prueba de habilidades CCNA sustenta el conocimiento para el primer y segundo módulo de Cisco CCNA, explorando los protocolos y conceptos de enrutamiento como RIP, VLSM, EIGRP y OSPF.

Palabras clave: enrutamiento, RIP, VLSM, EIGRP, OSPF

## ABSTRACT

The content of the CCNA skills test describes routing on LAN and WAN networks, which is the basis for basic network configuration. This work is mainly based on static and dynamic routing.

It also deals with the configuration of routers and switches, which are the main elements for routing.

The practical part of the CCNA skills test supports knowledge for the first and second Cisco CCNA module, exploring routing protocols and concepts such as RIP, VLSM, EIGRP and OSPF.

Keywords: routing, RIP, VLSM, EIGRP, OSPF

## INTRODUCCIÓN

Por medio del presente trabajo se da solución a la prueba de habilidades CCNA, que forma parte de las actividades evaluativas del Diplomado de Profundización CCNA. La cual pone a prueba las habilidades adquiridas a lo largo del diplomado.

El desarrollo de la actividad practica muestra la arquitectura y funciones de las redes LAN y WAN. Los principios y la estructura del direccionamiento IP y los fundamentos del estándar de redes de área local Ethernet, lo cual proporcionar una base del conocimiento adquirido.

Finalmente se construye una red Ethernet usando routers y switches, empleando los comandos de la interfaz de línea de comandos (CLI) de Cisco para realizar las configuraciones básicas de los dispositivos, utilizando herramientas de red para verificar instrucciones de red y analizar el tráfico de datos

Se realiza las configuraciones básicas para los routers y switches y se implementan esquemas de direccionamiento IP. Describiendo los dispositivos y servicios utilizados para soportar las comunicaciones en una la red LAN y WAN. En las cuales se observa el papel de las capas de protocolo red. Comprendiendo así la importancia de los esquemas de direccionamiento IP, tras aplicar máscaras de subred y direccionamiento IP para cumplir con los requisitos del protocolo IPv4.

## OBJETIVOS

### OBJETIVO GENERAL

Adquirir habilidades prácticas con la configuración de ROUTERS, SWITCHS, VLAN, direccionamiento IP, enrutamiento, protocolos DHCP, EIGRP y OSPF con lista de control de acceso.

### OBJETIVOS ESPECIFICOS

- Trazar cableado red LAN y WAN basados en el estándar de redes de área local Ethernet.
- Configurar los ROUTERS y SWITCHS.
- efectuar el direccionamiento IP, enrutamiento y subredes.
- Configurar los protocolos de enrutamiento estático y enrutamiento dinámico.
- Configurar listas de control de acceso, LAN virtuales (VLAN), DHCP y el enmascaramiento de IP o Network Address Translation (NAT).

## Descripción de escenarios propuestos para la prueba de habilidades

### Escenario 1

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

### Topología de red

Los requerimientos solicitados son los siguientes:

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

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

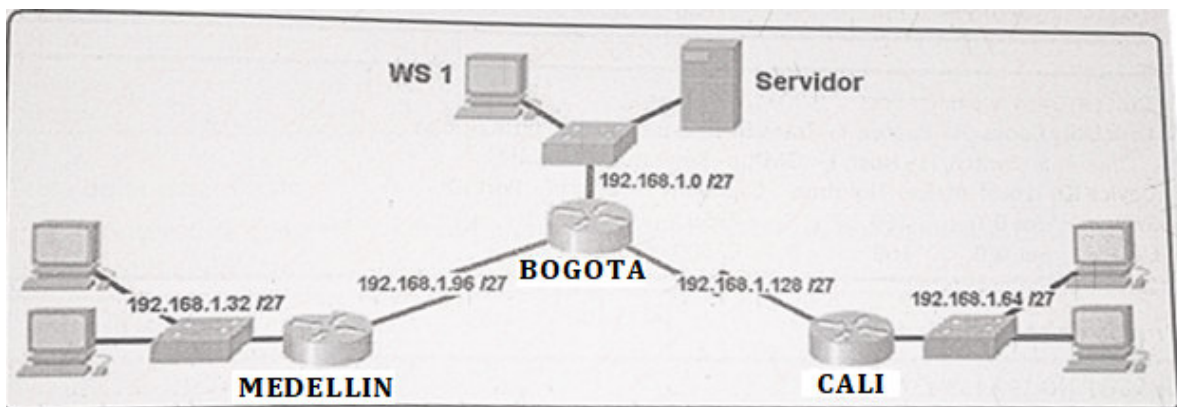
Parte 3: La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.

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

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

Parte 6: Configuración final.

Ilustración 1. Escenario 1

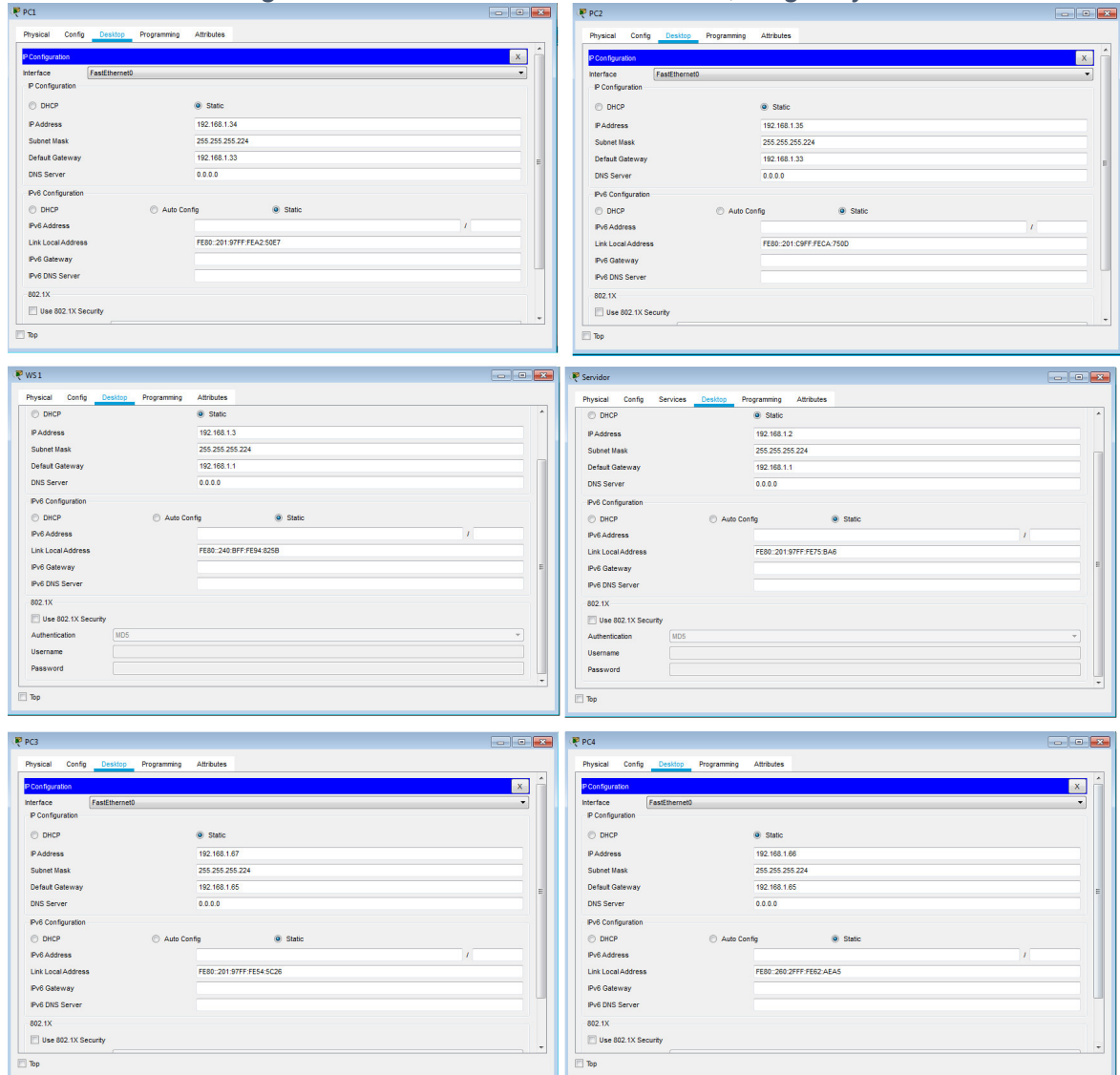


## DESARROLLO

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).

*Ilustración 2. Configuración Host de Routers Medellín, Bogotá y Cali*



Para los 3 enrutadores se debe agregar módulos de puertos Seriales para este caso se utilizara la Tarjeta Cisco HWIC-2T.

## Router MEDELLIN

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN
MEDELLIN(config)#enable secret cisco
MEDELLIN(config)#service password-encryption
MEDELLIN(config)#banner motd "Prohibido el Acceso no Autorizado"
MEDELLIN(config)#line console 0
MEDELLIN(config-line)#password class
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
MEDELLIN(config)#line vty 0 15
MEDELLIN(config-line)#password class
MEDELLIN(config-line)#login
MEDELLIN(config-line)#end
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN#
MEDELLIN#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
MEDELLIN#
```

## **Router BOGOTA**

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA
BOGOTA(config)#enable secret cisco
BOGOTA(config)#service password-encryption
BOGOTA(config)#banner motd "Prohibido el Acceso no Autorizado"
BOGOTA(config)#line console 0
BOGOTA(config-line)#password class
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#line vty 0 15
BOGOTA(config-line)#password class
BOGOTA(config-line)#login
```

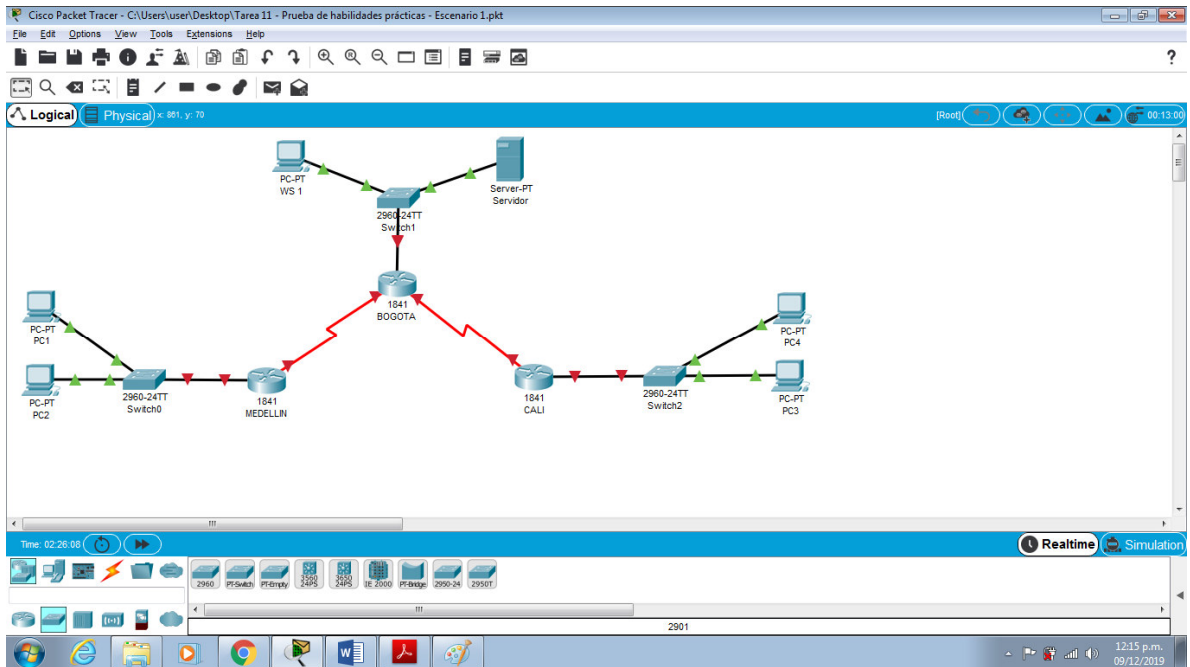
```
BOGOTA(config-line)#end
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console
BOGOTA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
BOGOTA#
```

## **Router CALI**

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CALI
CALI(config)#enable secret cisco
CALI(config)#service password-encryption
CALI(config)#banner motd "Prohibido el Acceso no Autorizado"
CALI(config)#line console 0
CALI(config-line)#password class
CALI(config-line)#login
CALI(config-line)#exit
CALI(config)#line vty 0 15
CALI(config-line)#password class
CALI(config-line)#login
CALI(config-line)#end
CALI#
%SYS-5-CONFIG_I: Configured from console by console
CALI#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CALI#
```

**Realizar la conexión física de los equipos con base en la topología de red**

Ilustración 3. Conexión física de los equipos con base en la topología de red escenario 1



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 crecimiento futuro de la red corporativa.
- b. Asignar una dirección IP a la red. **192.168.1.0**

### Parte 2: Configuración Básica.

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

	R1	R2	R3
Nombre de Host	<b>MEDELLIN</b>	<b>BOGOTA</b>	<b>CALI</b>
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	<b>Eigrp</b>	<b>Eigrp</b>	<b>Eigrp</b>
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

### Router MEDELLIN

MEDELLIN#**configure terminal**

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

MEDELLIN(config)#**interface Serial0/0/0**

MEDELLIN(config-if)#**ip address 192.168.1.99 255.255.255.224**

MEDELLIN(config-if)#**clock rate 56000**

MEDELLIN(config-if)#**no shutdown**

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

MEDELLIN(config-if)#**exit**

MEDELLIN(config)#**exit**

MEDELLIN#

%SYS-5-CONFIG\_I: Configured from console by console

MEDELLIN#

MEDELLIN#**configure terminal**

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

MEDELLIN(config)#**interface FastEthernet 0/0**

MEDELLIN(config-if)#**ip address 192.168.1.33 255.255.255.224**

MEDELLIN(config-if)#**no shutdown**

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

MEDELLIN(config-if)#**exit**

MEDELLIN(config)#**exit**

MEDELLIN#

%SYS-5-CONFIG\_I: Configured from console by console

MEDELLIN#

## Router BOGOTA

BOGOTA #**configure terminal**

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

BOGOTA (config)#**interface Serial0/0/0**

BOGOTA (config-if)#**ip address 192.168.1.98 255.255.255.224**

BOGOTA (config-if)#**no shutdown**

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down

BOGOTA (config-if)#**exit**

BOGOTA (config)#**exit**

BOGOTA #

%SYS-5-CONFIG\_I: Configured from console by console

BOGOTA #

BOGOTA #**configure terminal**

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

BOGOTA (config)#**interface Serial0/0/1**

BOGOTA (config-if)#**ip address 192.168.1.130 255.255.255.224**

BOGOTA (config-if)#**clock rate 56000**

```
BOGOTA (config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
BOGOTA (config-if)#exit
BOGOTA (config)#exit
BOGOTA #
%SYS-5-CONFIG_I: Configured from console by console
BOGOTA #
BOGOTA #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA (config)#interface FastEthernet 0/0
BOGOTA (config-if)#ip address 192.168.1.1 255.255.255.224
BOGOTA (config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
BOGOTA (config-if)#exit
BOGOTA (config)#exit
BOGOTA #
%SYS-5-CONFIG_I: Configured from console by console
BOGOTA #
```

## Router CALI

```
CALI#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI (config)#interface Serial0/0/0
CALI (config-if)#ip address 192.168.1.131 255.255.255.224
CALI (config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
CALI (config-if)#exit
CALI (config)#exit
CALI #
%SYS-5-CONFIG_I: Configured from console by console
CALI #
CALI #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI (config)#interface FastEthernet 0/0
CALI (config-if)#ip address 192.168.1.65 255.255.255.224
CALI (config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
CALI (config-if)#exit
CALI (config)#exit
CALI #
```

%SYS-5-CONFIG\_I: Configured from console by console  
CALI #

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.

*Ilustración 4. Router MEDELLIN Comando “show ip route”*

```
MEDELLIN#
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, 2 subnets
C       192.168.1.32 is directly connected, FastEthernet0/0
C       192.168.1.96 is directly connected, Serial0/0/0

MEDELLIN#
MEDELLIN#
MEDELLIN#

Ctrl+F6 to exit CLI focus
```

*Ilustración 5. Router BOGOTA Comando “show ip route”*

```
BOGOTA#
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, 3 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0
C       192.168.1.96 is directly connected, Serial0/0/0
C       192.168.1.128 is directly connected, Serial0/0/1

BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#

Ctrl+F6 to exit CLI focus
```

*Ilustración 6. Router CALI Comando “show ip route”*

```
CALI#
CALI#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, 2 subnets
C       192.168.1.64 is directly connected, FastEthernet0/0
C       192.168.1.128 is directly connected, Serial0/0/0

CALI#
CALI#
CALI#
CALI#
CALI#
CALI#
CALI#
CALI#
CALI#
CALI#

Ctrl+F6 to exit CLI focus
```

c. Verificar el balanceo de carga que presentan los routers.





```
Password:
BOGOTA#
BOGOTA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#router eigrp 200
BOGOTA(config-router)#network 192.168.1.0 0.0.0.31
BOGOTA(config-router)#network 192.168.1.128 0.0.0.31
BOGOTA(config-router)#network 192.168.1.96 0.0.0.31
BOGOTA(config-router)#no auto-summary
BOGOTA(config-router)#end
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console
BOGOTA#
Router CALI
```

```
BOGOTA>enable
Password:
CALI#
CALI #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI (config)#router eigrp 200
CALI (config-router)#network 192.168.1.128 0.0.0.31
CALI(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.130 (Serial0/0/0) is
up: new adjacency
CALI (config-router)#network 192.168.1.64 0.0.0.31
CALI (config-router)#no auto-summary
CALI(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.130 (Serial0/0/0)
resync: summary configured
CALI (config-router)#end
CALI #
%SYS-5-CONFIG_I: Configured from console by console
CALI #
```

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



Ilustración 14. Router CALI Comando “show ip route”

```
-----
CALI#
CALI#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
D   192.168.1.0 [90/2172416] via 192.168.1.130, 00:13:37, Serial0/0/0
D   192.168.1.32 [90/2684416] via 192.168.1.130, 00:13:37, Serial0/0/0
C   192.168.1.64 is directly connected, FastEthernet0/0
D   192.168.1.96 [90/2681856] via 192.168.1.130, 00:13:37, Serial0/0/0
C   192.168.1.128 is directly connected, Serial0/0/0

CALI#
CALI#
CALI#
CALI#
CALI#
CALI#
CALI#
CALI#
CALI#
CALI#
Ctrl+F6 to exit CLI focus
```

Ilustración 16. Router BOGOTA Comando “show ip route”

```
-----
BOGOTA#
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
D   192.168.1.32 [90/2172416] via 192.168.1.99, 00:13:52, Serial0/0/0
D   192.168.1.64 [90/2172416] via 192.168.1.131, 00:10:23, Serial0/0/1
C   192.168.1.96 is directly connected, Serial0/0/0
C   192.168.1.128 is directly connected, Serial0/0/1

BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
BOGOTA#
Ctrl+F6 to exit CLI focus
```

Ilustración 15. Router MEDELLIN Comando “show ip route”

```
-----
MEDELLIN#
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
D   192.168.1.0 [90/2172416] via 192.168.1.98, 00:13:12, Serial0/0/0
C   192.168.1.32 is directly connected, FastEthernet0/0
D   192.168.1.64 [90/2684416] via 192.168.1.98, 00:09:49, Serial0/0/0
C   192.168.1.96 is directly connected, Serial0/0/0
D   192.168.1.128 [90/2681856] via 192.168.1.98, 00:13:12, Serial0/0/0

MEDELLIN#
MEDELLIN#
MEDELLIN#
MEDELLIN#
MEDELLIN#
MEDELLIN#
MEDELLIN#
MEDELLIN#
MEDELLIN#
MEDELLIN#
Ctrl+F6 to exit CLI focus
```

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.

Ilustración 17. Ping desde Servidor a PC1, PC2 y PC3.

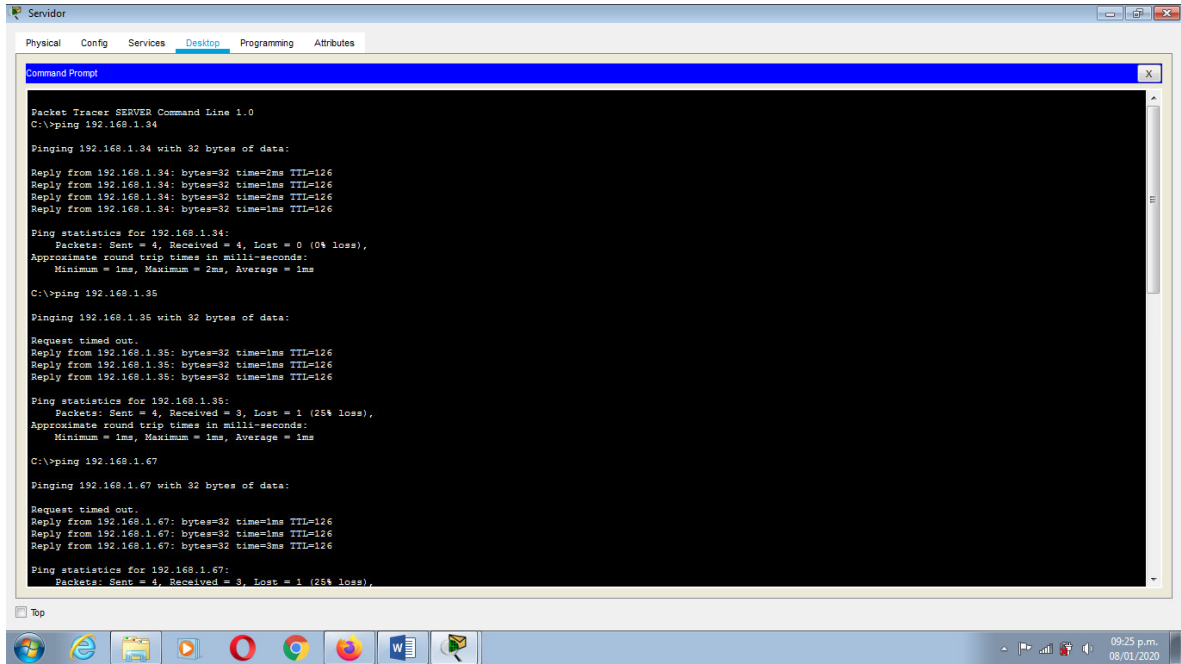


Ilustración 18. Ping desde el host PC4 del Router CALI hacia el host PC1 de la red MEDELLIN y al Servidor

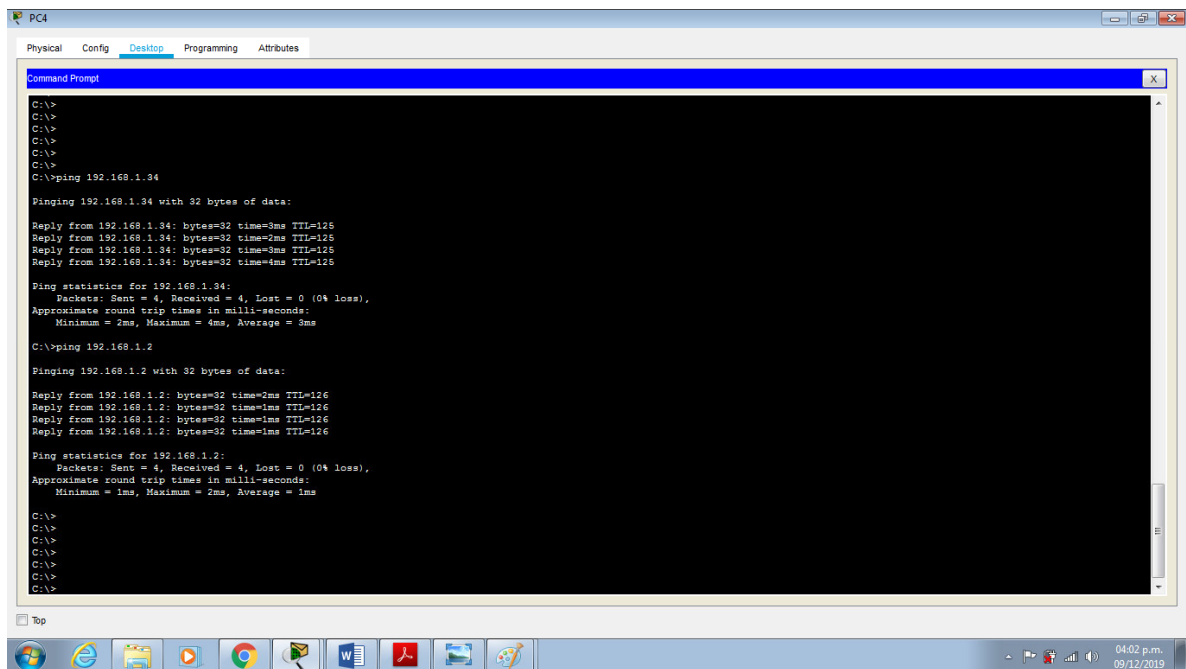


Ilustración 20. Ilustración 19. Ping desde Servidor a Router Cali.

```
Serveror
Physical Config Services Desktop Programming Attributes
Command Prompt
Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms
C:\>ping 192.168.1.66
Pinging 192.168.1.66 with 32 bytes of data:
Reply from 192.168.1.66: bytes=32 time=1ms TTL=126
Reply from 192.168.1.66: bytes=32 time=2ms TTL=126
Reply from 192.168.1.66: bytes=32 time=1ms TTL=126
Reply from 192.168.1.66: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\>ping 192.168.1.33
Pinging 192.168.1.33 with 32 bytes of data:
Reply from 192.168.1.33: bytes=32 time=5ms TTL=254
Reply from 192.168.1.33: bytes=32 time=1ms TTL=254
Reply from 192.168.1.33: bytes=32 time=1ms TTL=254
Reply from 192.168.1.33: bytes=32 time=1ms TTL=254
Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>
```

Ilustración 19. Ping desde Servidor a PC4, Router Medellin Y Router Bogota.

```
Serveror
Physical Config Services Desktop Programming Attributes
Command Prompt
Pinging 192.168.1.33 with 32 bytes of data:
Reply from 192.168.1.33: bytes=32 time=5ms TTL=254
Reply from 192.168.1.33: bytes=32 time=1ms TTL=254
Reply from 192.168.1.33: bytes=32 time=1ms TTL=254
Reply from 192.168.1.33: bytes=32 time=1ms TTL=254
Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 192.168.1.65
Pinging 192.168.1.65 with 32 bytes of data:
Reply from 192.168.1.65: bytes=32 time=7ms TTL=254
Reply from 192.168.1.65: bytes=32 time=1ms TTL=254
Reply from 192.168.1.65: bytes=32 time=1ms TTL=254
Reply from 192.168.1.65: bytes=32 time=1ms TTL=254
Ping statistics for 192.168.1.65:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 7ms, Average = 2ms
C:\>
```

Ilustración 22. Ping PC3 a PC4, PC1 y PC2

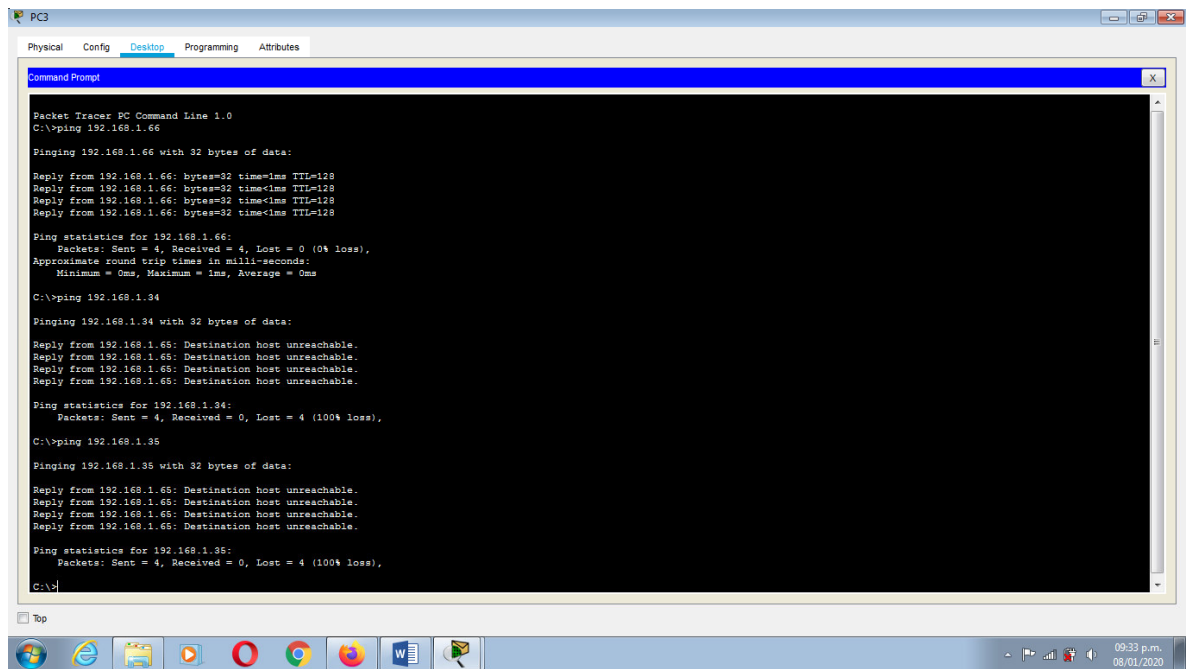


Ilustración 21. Ping PC3 a Router Cali, Router Bogota y Router Medellin.

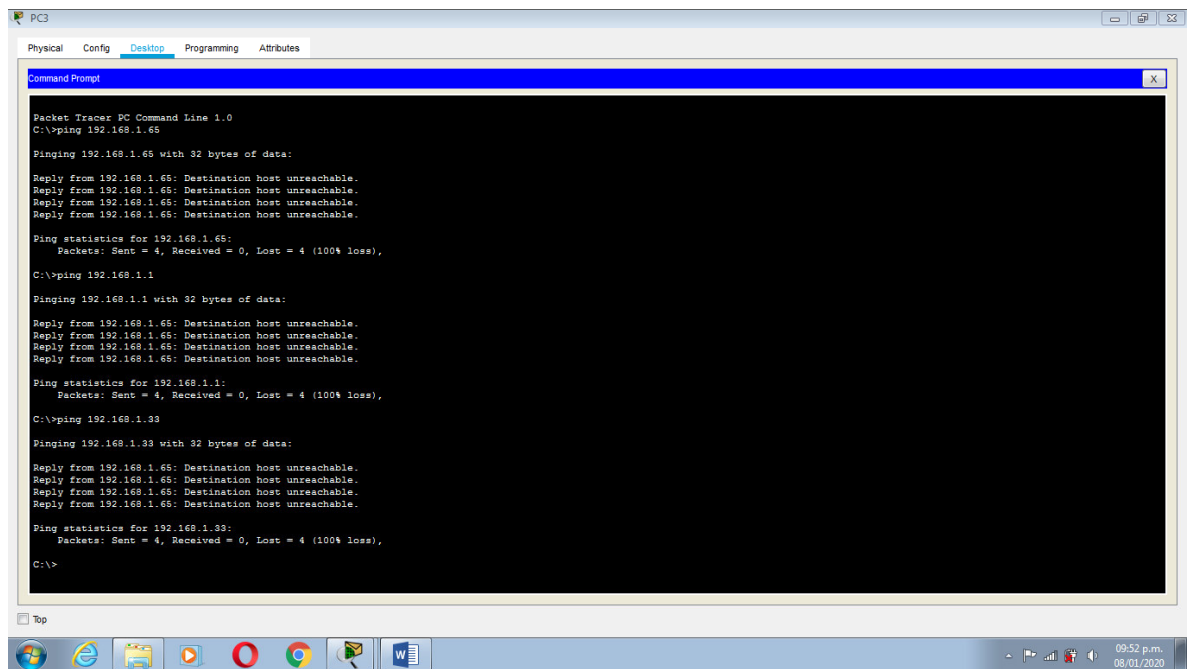


Ilustración 24. Ping PC4 a Router Cali, Route Medellin y Router Bogota.

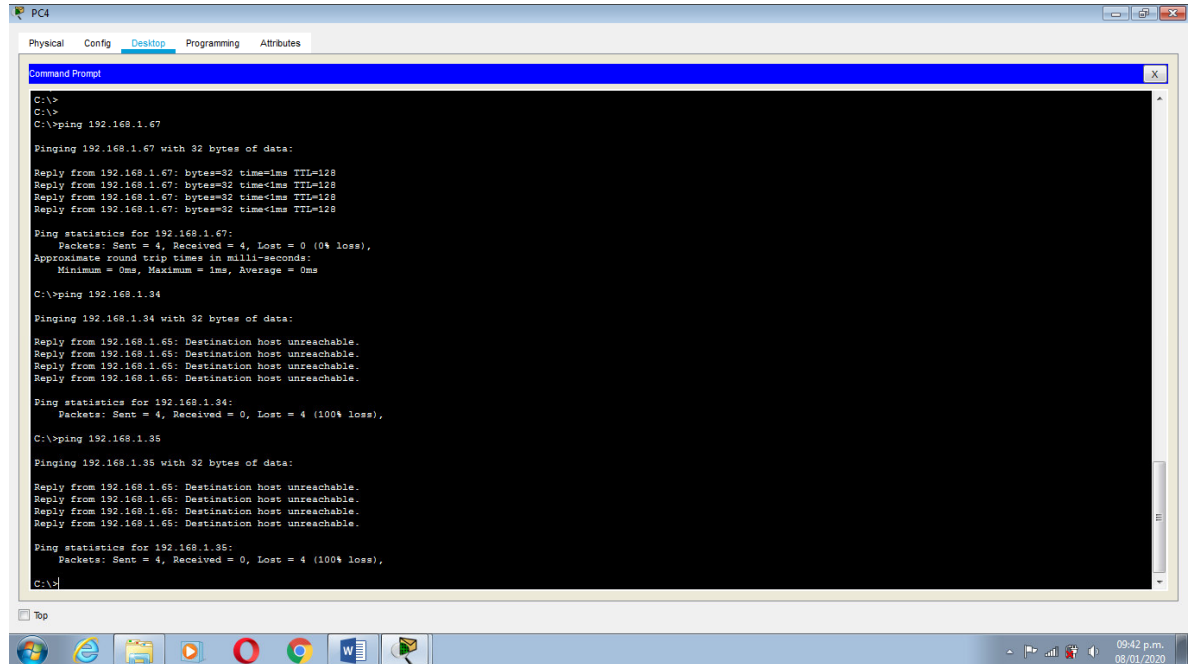


Ilustración 23. Ping PC4 a PC3, PC1 y PC2

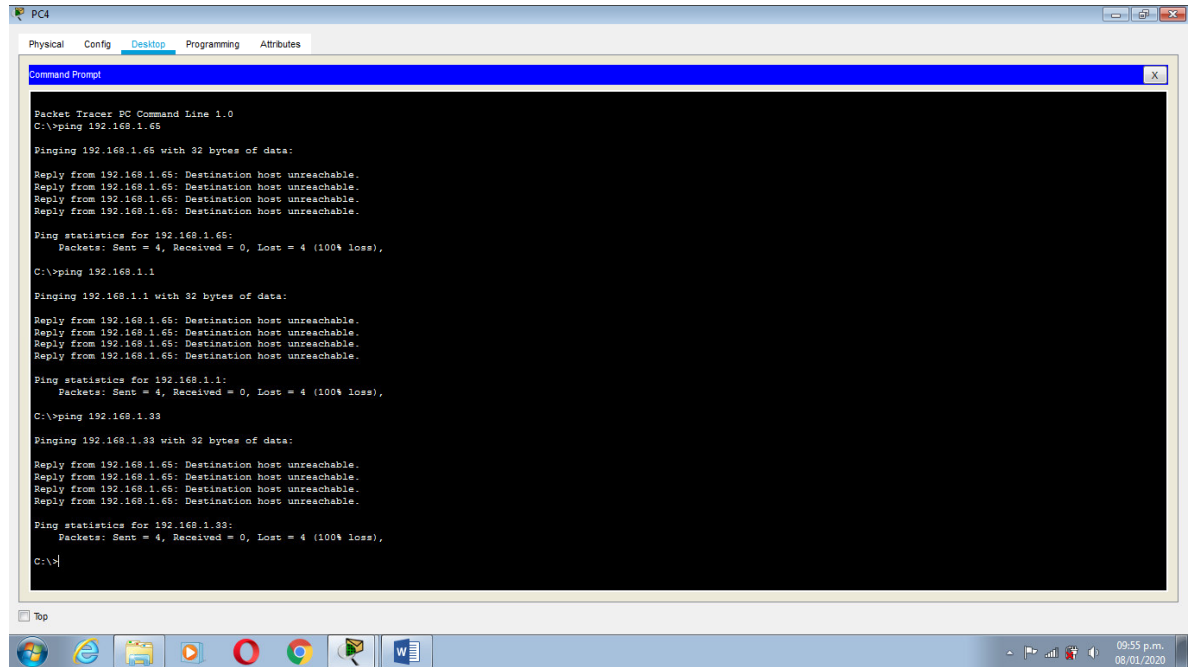


Ilustración 26. Ping de PC1 a Router Cali, Router Medellin y Router Bogota.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.65

Pinging 192.168.1.65 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.65:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Ilustración 25. Ping de PC1 a PC2, PC3, PC4.

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:
Reply from 192.168.1.35: bytes=32 time=1ms TTL=128
Reply from 192.168.1.35: bytes=32 time=1ms TTL=128
Reply from 192.168.1.35: bytes=32 time=1ms TTL=128
Reply from 192.168.1.35: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.67

Pinging 192.168.1.67 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.67:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

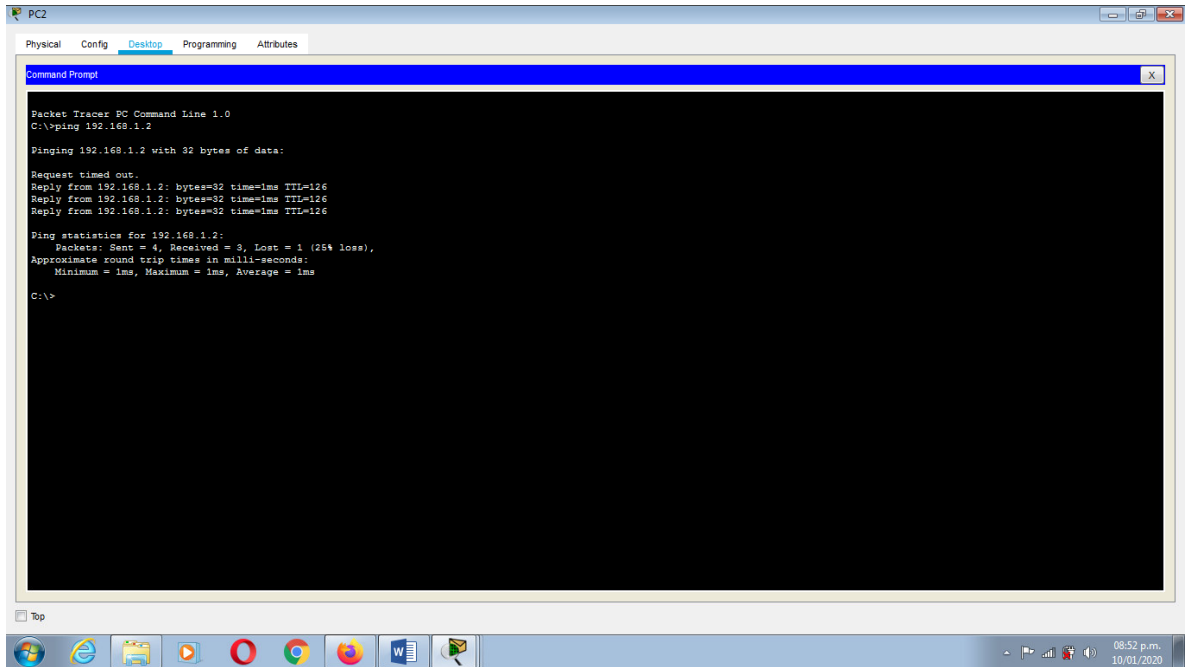
C:\>ping 192.168.1.66

Pinging 192.168.1.66 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Ilustración 28. Ping PC2 a Servidor



The screenshot shows a Packet Tracer PC Command Line window for PC2. The command prompt displays the following output:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

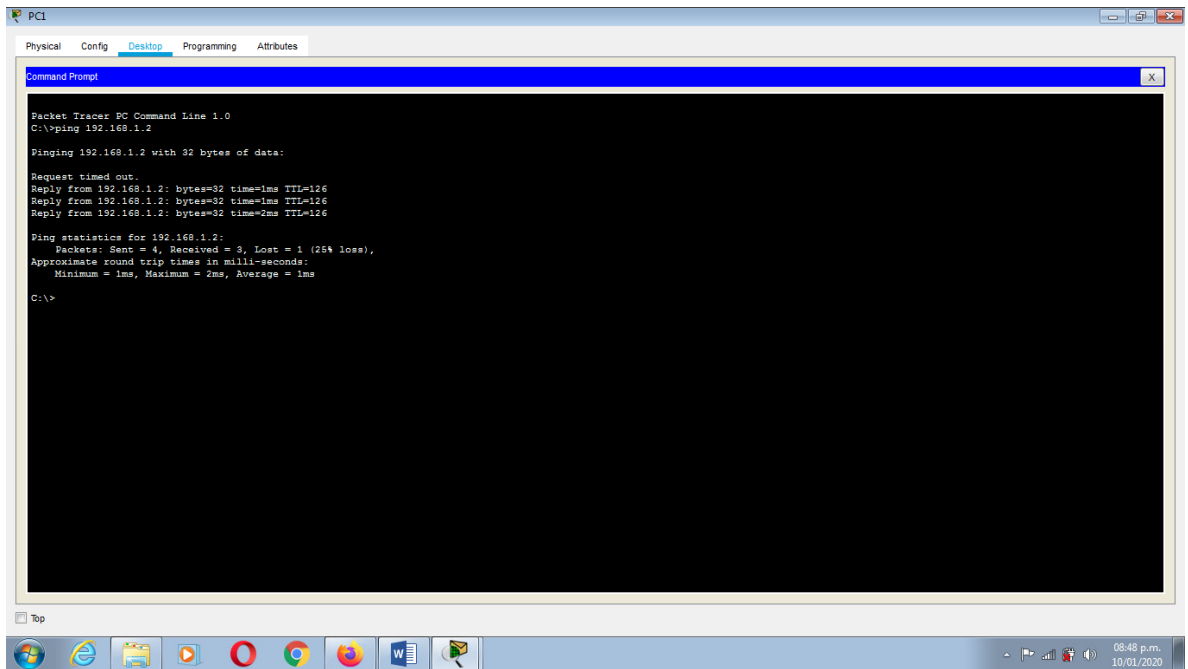
Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>
```

Ilustración 27. Ping PC1 a Servidor



The screenshot shows a Packet Tracer PC Command Line window for PC1. The command prompt displays the following output:

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

Ilustración 29. Ping PC4 a Servidor

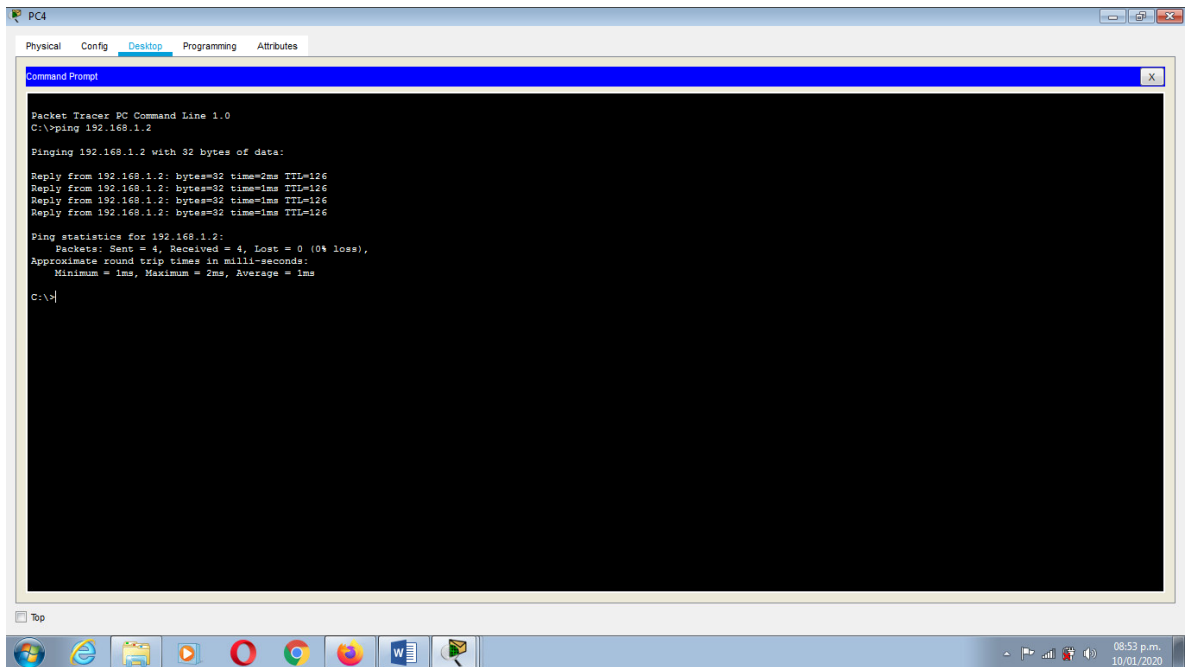


Ilustración 30. Ping PC3 a Servidor

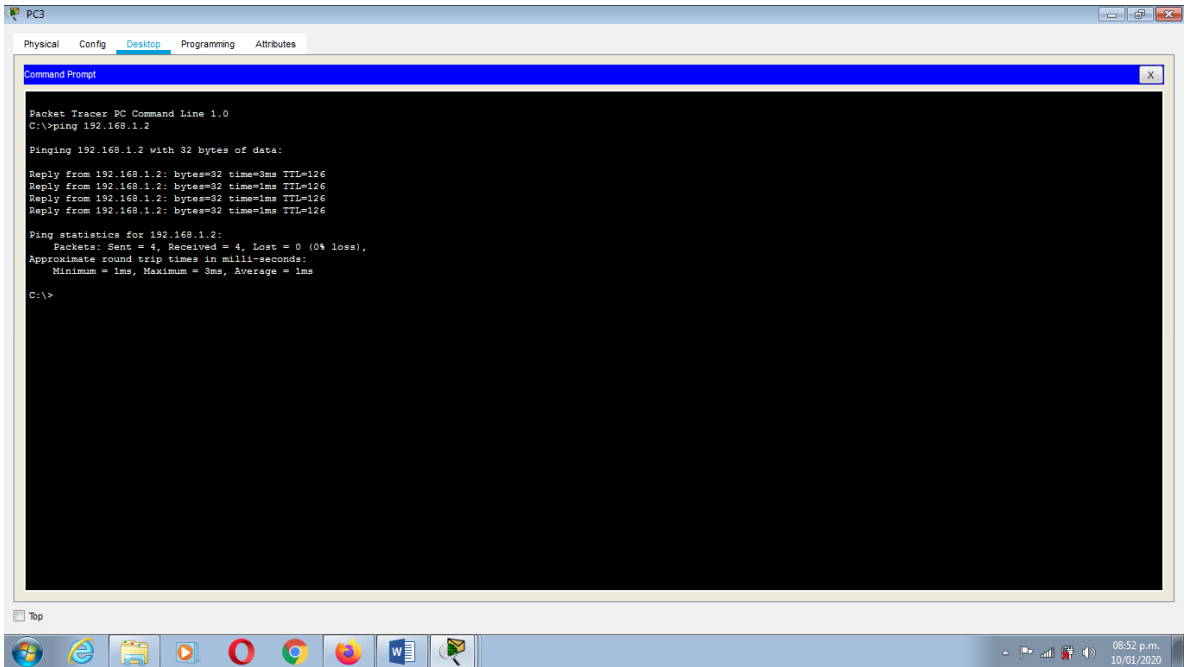


Ilustración 31. Ping de PC2 a Router Cali, Router Medellin y Router Bogota.

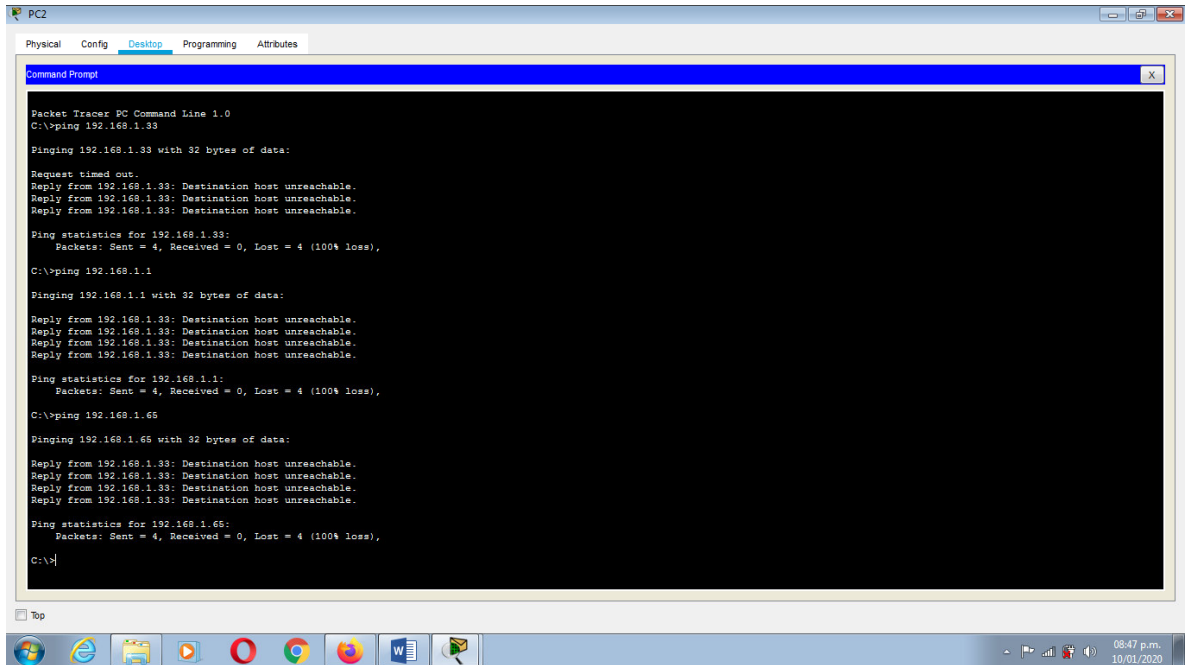
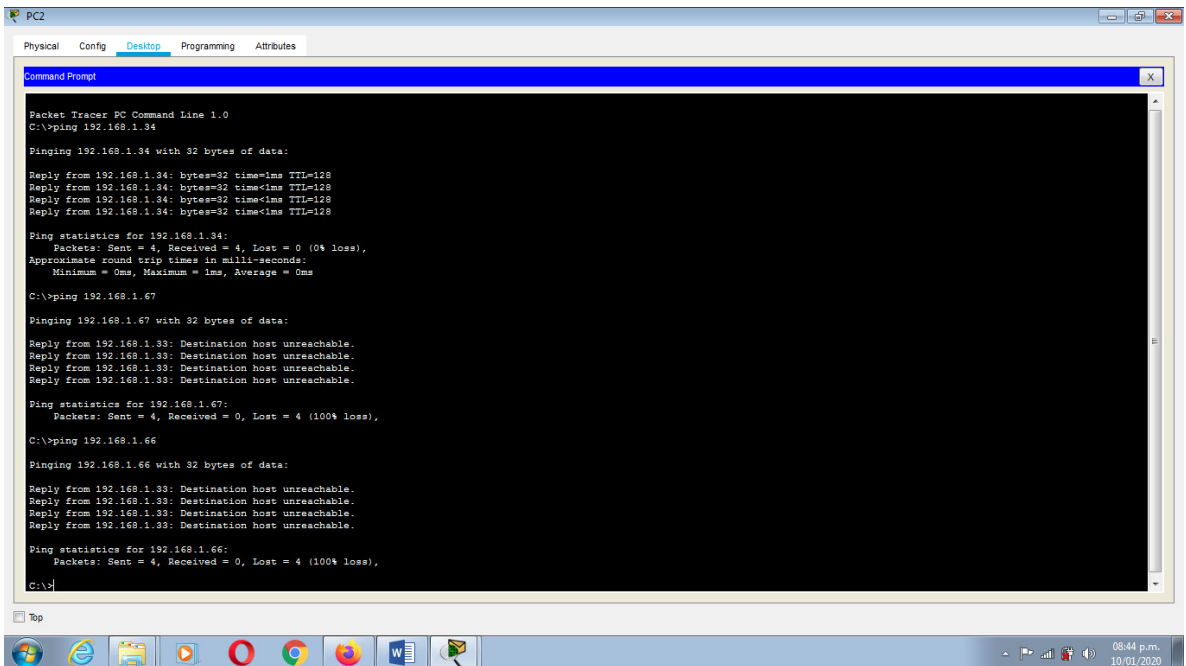


Ilustración 32. Ping de PC2 a PC1, PC3, PC4.



## Parte 4: Configuración de las listas de Control de Acceso

En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo. El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers. Las condiciones para crear las ACL son las siguientes:

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

```
MEDELLIN>enable
Password:
MEDELLIN#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 host
192.168.1.2
MEDELLIN(config)#access-list 110 permit icmp any any echo-reply
MEDELLIN(config)#access-list 110 deny ip any any
MEDELLIN(config)#int FastEthernet0/0
MEDELLIN(config-if)#ip access-group 110 in
MEDELLIN(config-if)#exit
MEDELLIN(config)#exit
MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN#
```

### **Router CALI**

```
CALI>enable
Password:
CALI #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI (config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.2
CALI (config)#access-list 110 permit icmp any any echo-reply
CALI (config)#access-list 110 deny ip any any
CALI (config)#int FastEthernet0/0
CALI (config-if)#ip access-group 110 in
```

```
CALI (config-if)#exit
CALI (config)#exit
CALI #
%SYS-5-CONFIG_I: Configured from console by console
CALI #
```

Se ha permitido acceso a la red 192.168.1.0 y al servidor 192.168.1.2, luego se ha permitido a cualquier tráfico para el protocolo ICMP y Respuesta de Eco, en seguida se ha denegado a cualquier otro tráfico IP. A continuación se asoció la ACL a la interfaz FastEthernet0/0. Por último le indicamos el sentido (entrada)

### **Router BOGOTA**

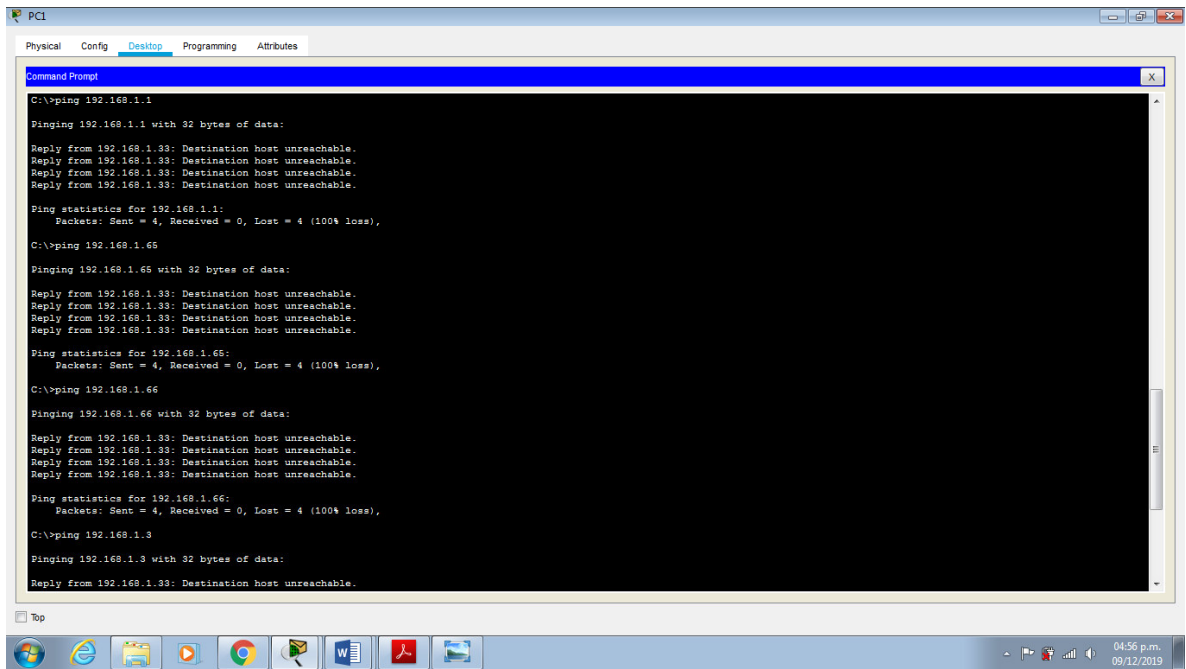
```
BOGOTA>enable
Password:
BOGOTA #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA (config)#access-list 110 permit ip 192.168.1.0 0.0.0.255 host
192.168.1.2
BOGOTA (config)# access-list 110 deny ip any any
BOGOTA (config)#int FastEthernet0/0
BOGOTA (config-if)# ip access-group 110 out
BOGOTA (config-if)#exit
BOGOTA (config)#exit
BOGOTA #
%SYS-5-CONFIG_I: Configured from console by console
BOGOTA #
```

Se ha permitido al host 192.168.1.0 y host 192.168.1.2, luego se ha denegado a cualquier tráfico IP. A continuación se asoció la ACL a la interfaz FastEthernet0/0. Por último le indicamos el sentido (salida)

### **Parte 5: Comprobación de la red instalada.**

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

*Ilustración 33. Ping desde el host PC1 del Router MEDELLIN hacia el Router BOGOTA y CALI.*



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.65
Pinging 192.168.1.65 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.65:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.66
Pinging 192.168.1.66 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.
```

Ilustración 34. Ping desde el host PC1 del Router MEDELLIN hacia host PC4 de la red CALI y al WS1 y Servidor.

```
Command Prompt
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.1.66
Pinging 192.168.1.66 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=2ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=5ms TTL=126
Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms
C:\>
```

Solo se obtiene respuesta desde el servidor 192.168.1.2

Ilustración 35. Ping desde el Servidor hacia PC1 de la red MEDELLIN, al PC4 de la red CALI y al WS1

```
Command Prompt
C:\>ping 192.168.1.34
Pinging 192.168.1.34 with 32 bytes of data:
Reply from 192.168.1.34: bytes=32 time=5ms TTL=126
Reply from 192.168.1.34: bytes=32 time=3ms TTL=126
Reply from 192.168.1.34: bytes=32 time=1ms TTL=126
Reply from 192.168.1.34: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms
C:\>ping 192.168.1.66
Pinging 192.168.1.66 with 32 bytes of data:
Reply from 192.168.1.66: bytes=32 time=5ms TTL=126
Reply from 192.168.1.66: bytes=32 time=1ms TTL=126
Reply from 192.168.1.66: bytes=32 time=1ms TTL=126
Reply from 192.168.1.66: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms
C:\>ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Se obtiene respuesta positiva de todos los equipos

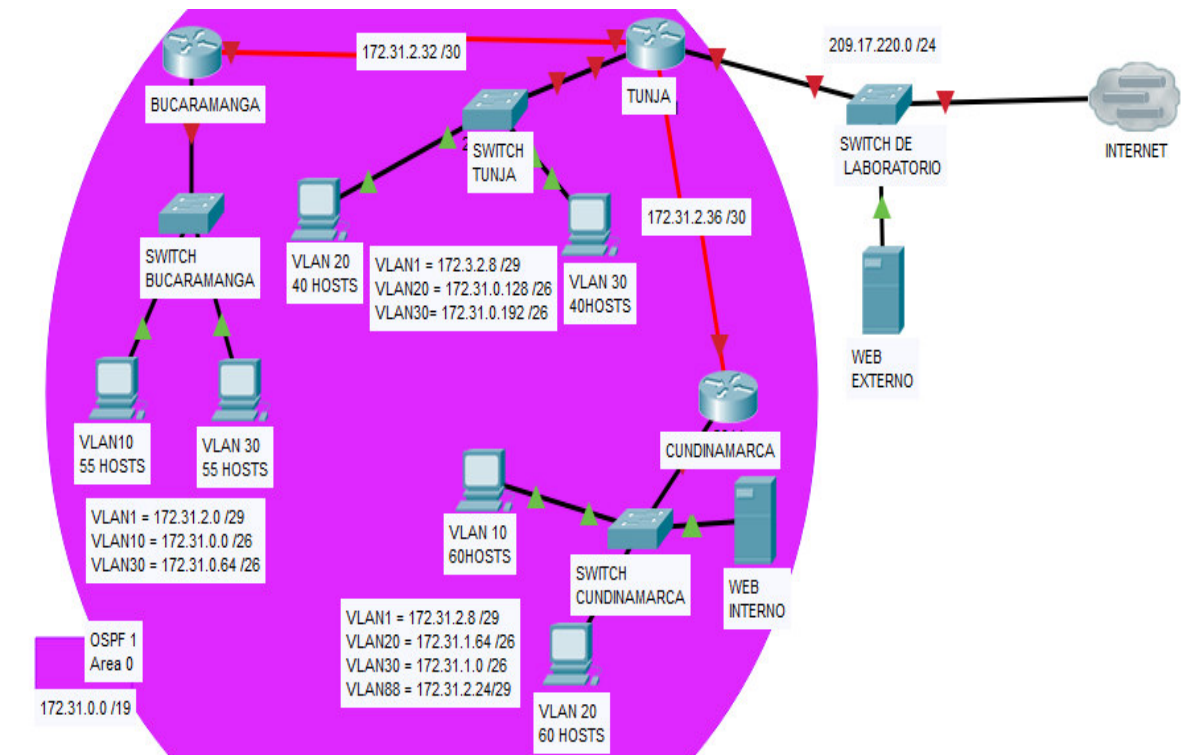
b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red.

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	CONEXIÓN EXITOSA
	WS_1	Router BOGOTA	CONEXIÓN EXITOSA
	Servidor	Router CALI	CONEXIÓN EXITOSA
	Servidor	Router MEDELLIN	CONEXIÓN EXITOSA
TELNET	LAN del Router MEDELLIN	Router CALI	CONNECTION TIMED OUT
	LAN del Router CALI	Router CALI	CONNECTION TIMED OUT
	LAN del Router MEDELLIN	Router MEDELLIN	CONNECTION TIMED OUT
	LAN del Router CALI	Router MEDELLIN	CONNECTION TIMED OUT
PING	LAN del Router CALI	WS_1	DESTINATION HOST UNREACHABLE
	LAN del Router MEDELLIN	WS_1	DESTINATION HOST UNREACHABLE
	LAN del Router MEDELLIN	LAN del Router CALI	DESTINATION HOST UNREACHABLE
PING	LAN del Router CALI	Servidor	REPLY FROM 192.168.1.2
	LAN del Router MEDELLIN	Servidor	REPLY FROM 192.168.1.2
	Servidor	LAN del Router MEDELLIN	REPLY FROM 192.168.1.34
	Servidor	LAN del Router CALI	REPLY FROM 192.168.1.66
	Router CALI	LAN del Router MEDELLIN	SUCCESS RATE IS 100 PERCENT (5/5)
	Router MEDELLIN	LAN del Router CALI	SUCCESS RATE IS 100 PERCENT (5/5)

## 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.

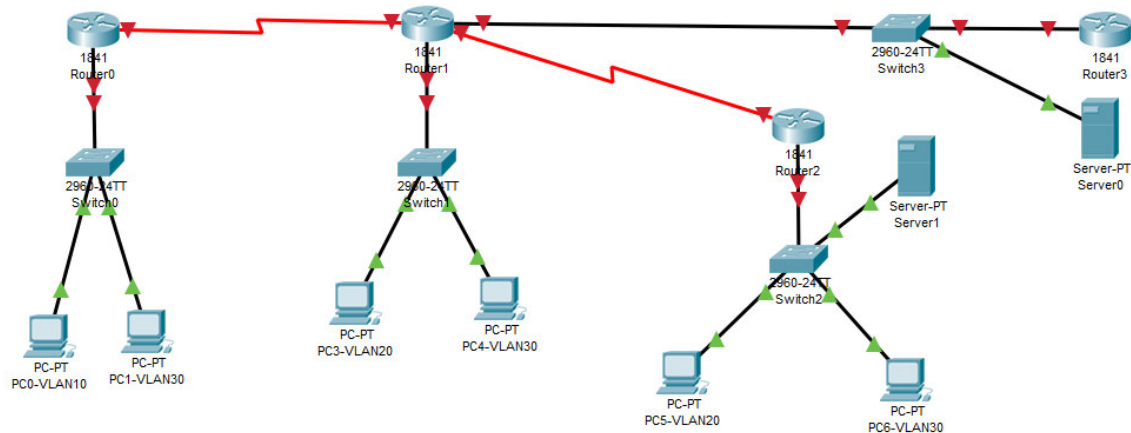
Ilustración 36. Escenario 2.



## DESARROLLO

### PARTE 1: CONFIGURACIÓN BÁSICA.

Ilustración 37. Conexión física de los equipos con base en la topología de red escenario 2



### Configuración de los router

#### Router BUCARAMANGA

Would you like to enter the initial configuration dialog? [yes/no]: **no**  
Press RETURN to get started!

Router>

Router>**enable**

Router#**configure terminal**

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

Router(config)#**hostname BUCARAMANGA**

BUCARAMANGA(config)#**no ip domain-lookup**

BUCARAMANGA (config)#**banner motd "Prohibido el Acceso no Autorizado"**

BUCARAMANGA (config)# **enable secret class**

BUCARAMANGA (config)#**line console 0**

BUCARAMANGA (config-line)#**password cisco**

BUCARAMANGA (config-line)#**login**

BUCARAMANGA(config-line)#**logging synchronous**

BUCARAMANGA (config-line)#**exit**

BUCARAMANGA (config)#**line vty 0 15**

BUCARAMANGA (config-line)#**password cisco**

BUCARAMANGA (config-line)#**login**

BUCARAMANGA(config-line)#**logging synchronous**

BUCARAMANGA (config-line)#**end**

BUCARAMANGA #

%SYS-5-CONFIG\_I: Configured from console by console

BUCARAMANGA> **enable**

```

BUCARAMANGA # configure terminal
BUCARAMANGA (config)#interface FastEthernet0/0.1
BUCARAMANGA(config-subif)#encapsulation dot1Q 1
BUCARAMANGA(config-subif)#ip address 172.31.2.1 255.255.255.248
BUCARAMANGA(config-subif)#interface FastEthernet0/0.10
BUCARAMANGA(config-subif)#encapsulation dot1Q 10
BUCARAMANGA(config-subif)#ip address 172.31.0.1 255.255.255.192
BUCARAMANGA(config-subif)#interface FastEthernet0/0.30
BUCARAMANGA(config-subif)#encapsulation dot1Q 30
BUCARAMANGA(config-subif)#ip address 172.31.0.65 255.255.255.192
BUCARAMANGA(config-if)#interface FastEthernet0/0
BUCARAMANGA(config-if)#no shutdown
BUCARAMANGA(config-if)#interface Serial0/0/0
BUCARAMANGA(config-if)#ip address 172.31.2.34 255.255.255.252
BUCARAMANGA (config-if)#no shutdown
BUCARAMANGA(config-if)#end
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#copy running-config startup-config
Destination filename [startup-config]? [Intro]
Building configuration...
[OK]
BUCARAMANGA #

```

## **Router TUNJA**

```

Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname TUNJA
TUNJA (config)#no ip domain-lookup
TUNJA (config)#banner motd "Prohibido el Acceso no Autorizado"
TUNJA (config)# enable secret class
TUNJA (config)#line console 0
TUNJA (config-line)#password cisco
TUNJA (config-line)#login
TUNJA(config-line)#logging synchronous
TUNJA (config-line)#exit
TUNJA (config)#line vty 0 15
TUNJA (config-line)#password cisco
TUNJA (config-line)#login
TUNJA(config-line)#logging synchronous

```

```

TUNJA (config-line)#end
TUNJA #
%SYS-5-CONFIG_I: Configured from console by console
TUNJA # configure terminal
TUNJA (config)#interface FastEthernet0/1
TUNJA (config-if)# ip address 200.17.220.1 255.255.255.0
TUNJA (config-if)# no shutdown
TUNJA (config-if)#exit
TUNJA (config)# exit
TUNJA (config)#interface Serial0/0/0
TUNJA (config-if)# ip address 172.31.2.33 255.255.255.252
TUNJA (config-if)# clock rate 56000
TUNJA (config-if)# no shutdown
TUNJA (config-if)#exit
TUNJA (config)#
TUNJA (config)#interface Serial0/0/1
TUNJA (config-if)# ip address 172.31.2.37 255.255.255.252
TUNJA (config-if)# clock rate 56000
TUNJA (config-if)# no shutdown
TUNJA (config-if)# exit
TUNJA (config)# exit
TUNJA #configure terminal
Enter configuration commands, one per line. End with CNTL/Z
TUNJA (config)# interface FastEthernet0/0.1
TUNJA (config-subif)#encapsulation dot1q 1
TUNJA (config-subif)# ip address 172.31.2.9 255.255.255.248
TUNJA (config-subif)#end
TUNJA #
%SYS-5-CONFIG_I: Configured from console by console
TUNJA #
TUNJA #configure terminal
Enter configuration commands, one per line. End with CNTL/Z
TUNJA (config)# interface FastEthernet0/0.20
TUNJA(config-subif)#encapsulation dot1q 20
TUNJA (config-subif)# ip address 172.31.0.129 255.255.255.192
TUNJA (config-subif)#end
TUNJA #
%SYS-5-CONFIG_I: Configured from console by console
TUNJA #
TUNJA #configure terminal
Enter configuration commands, one per line. End with CNTL/Z
TUNJA (config)# interface FastEthernet0/0.30
TUNJA(config-subif)#encapsulation dot1q 30
TUNJA (config-subif)#ip address 172.31.0.193 255.255.255.192
TUNJA (config-subif)#exit

```

```
TUNJA(config-if)# exit
TUNJA(config)# interface FastEthernet0/0
TUNJA(config-if)#no shutdown
TUNJA(config-if)#end
TUNJA#
```

```
TUNJA #
%SYS-5-CONFIG_I: Configured from console by console
TUNJA #
TUNJA #copy running-config startup-config
Destination filename [startup-config]? [Intro]
Building configuration...
[OK]
TUNJA #
```

## **Router CUNDINAMARCA**

Would you like to enter the initial configuration dialog? [yes/no]: **no**  
Press RETURN to get started!

```
Router>
```

```
Router>enable
```

```
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)#banner motd "Prohibido el Acceso no Autorizado"
```

```
CUNDINAMARCA (config)# enable secret class
```

```
CUNDINAMARCA (config)#line console 0
```

```
CUNDINAMARCA (config-line)#password cisco
```

```
CUNDINAMARCA (config-line)#login
```

```
CUNDINAMARCA(config-line)#logging synchronous
```

```
CUNDINAMARCA (config-line)#exit
```

```
CUNDINAMARCA (config)#line vty 0 15
```

```
CUNDINAMARCA (config-line)#password cisco
```

```
CUNDINAMARCA (config-line)#login
```

```
CUNDINAMARCA(config-line)#logging synchronous
```

```
CUNDINAMARCA (config-line)#end
```

```
CUNDINAMARCA #
```

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

```
CUNDINAMARCA # configure terminal
```

```
CUNDINAMARCA (config)#interface Serial0/0/0
```

```
CUNDINAMARCA (config-if)# ip address 172.31.2.38 255.255.255.252
```

```
CUNDINAMARCA (config-if)# no shutdown
```

```
CUNDINAMARCA (config-if)#exit
```

```
CUNDINAMARCA (config)# exit
```

```
CUNDINAMARCA #copy running-config startup-config
Destination filename [startup-config]? [Intro]
Building configuration...
[OK]
```

## Router ISP

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#no ip domain-lookup
ISP(config)#banner motd "Prohibido el Acceso no Autorizado"
ISP(config)# enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#logging synchronous
ISP(config-line)#exit
ISP(config)#line vty 0 15
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#logging synchronous
ISP(config-line)#end
ISP#
%SYS-5-CONFIG_I: Configured from console by console
ISP # configure terminal
ISP (config)# interface FastEthernet0/0
ISP (config-if)# ip address 200.17.220.254 255.255.255.0
ISP (config-if)# no shutdown
ISP (config-if)# exit
ISP (config)#
Enter configuration commands, one per line. End with CNTL/Z.
ISP (config)#ip route 172.31.0.0 255.255.224.0 200.17.220.200
ISP (config)# exit
ISP #copy running-config startup-config
Destination filename [startup-config]? [Intro]
Building configuration...
[OK]
```

## PARTE 2: CONFIGURACIÓN AVANZADA

### Autenticación local con AAA.

Se Habilita AAA (Authentication, Authorization and Accounting), se crea una lista de autenticación que se almacena en forma local la base de datos del usuario y se le señala al Router, que a los usuarios les corresponde autenticarse a partir de la lista recién establecida para conectarse. Se asignan usuario sin privilegios y un usuario con el máximo de privilegios “15”.

### Router BUCARAMANGA

```
BUCARAMANGA>enable
```

```
Password:
```

```
BUCARAMANGA#configure terminal
```

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

```
BUCARAMANGA(config)#username admin privilege 15 password 0 admin
```

```
BUCARAMANGA(config)#aaa new-model
```

```
BUCARAMANGA(config)#aaa authentication login LOCAL_AUTH local
```

```
BUCARAMANGA(config)#line console 0
```

```
BUCARAMANGA(config-line)#login authentication LOCAL_AUTH
```

```
BUCARAMANGA(config-line)#line vty 0 15
```

```
BUCARAMANGA(config-line)#login authentication LOCAL_AUTH
```

```
BUCARAMANGA(config-line)#exit
```

### Router TUNJA

```
TUNJA>enable
```

```
Password:
```

```
TUNJA #configure terminal
```

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

```
TUNJA(config)#username admin privilege 15 password 0 admin
```

```
TUNJA(config)#aaa new-model
```

```
TUNJA(config)#aaa authentication login LOCAL_AUTH local
```

```
TUNJA(config)#line console 0
```

```
TUNJA(config-line)#login authentication LOCAL_AUTH
```

```
TUNJA(config-line)#line vty 0 15
```

```
TUNJA(config-line)#login authentication LOCAL_AUTH
```

```
TUNJA(config-line)#exit
```

### Router CUNDINAMARCA

```
CUNDINAMARCA >enable
```

```
Password:
```

**CUNDINAMARCA #configure terminal**

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

**CUNDINAMARCA(config)# username admin privilege 15 password 0 admin**

**CUNDINAMARCA(config)#aaa new-model**

**CUNDINAMARCA(config)#aaa authentication login LOCAL\_AUTH local**

**CUNDINAMARCA(config)#line console 0**

**CUNDINAMARCA(config-line)#login authentication LOCAL\_AUTH**

**CUNDINAMARCA(config-line)#line vty 0 15**

**CUNDINAMARCA(config-line)#login authentication LOCAL\_AUTH**

**CUNDINAMARCA(config-line)#exit**

**Cifrado de contraseñas.**

**Router BUCARAMANGA**

**BUCARAMANGA>enable**

Password:

**BUCARAMANGA #configure terminal**

**BUCARAMANGA(config)#service password-encryption**

**Router TUNJA**

**TUNJA>enable**

Password:

**TUNJA #configure terminal**

**TUNJA (config)#service password-encryption**

**Router CUNDINAMARCA**

**CUNDINAMARCA>enable**

Password:

**CUNDINAMARCA #configure terminal**

**CUNDINAMARCA (config)#service password-encryption**

**Máximo de internos para acceder al router y máximo tiempo de acceso al detectar ataques.**

En el comando “block-for 60”, si fallan los intentos de inicio de sesión, se bloquea por 60 segundos antes de permitir el acceso nuevamente. Se utiliza el comando “attempts 2 within 30” solo permite realizar dos intentos de inicio de sesión en 30 segundos.

**Router BUCARAMANGA**

**BUCARAMANGA>enable**

Password:

**BUCARAMANGA #configure terminal**

**BUCARAMANGA(config)#login block-for 60 attempts 2 within 30**

## Router TUNJA

TUNJA>enable

Password:

TUNJA #configure terminal

TUNJA (config)#login block-for 60 attempts 2 within 30

## Router CUNDINAMARCA

CUNDINAMARCA >enable

Password:

CUNDINAMARCA #configure terminal

CUNDINAMARCA (config)#login block-for 60 attempts 2 within 30

El comando “security authentication failure rate” no es soportado por Packetracer. Este bloquea los intentos de conexión durante un tiempo determinado, limitando los intentos de conexión por fuerza bruta.

**Establecer un servidor TFTP que almacene todos los archivos necesarios de los routers.**

*Ilustración 38. Configuración Ip Servidor Tftp*

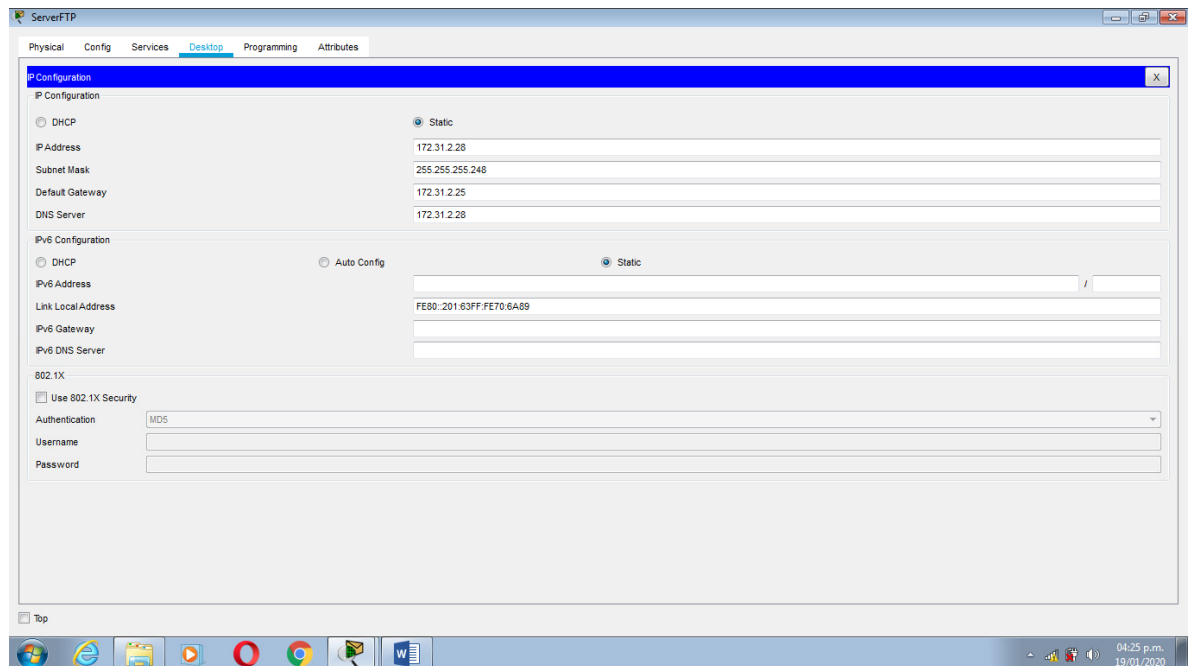
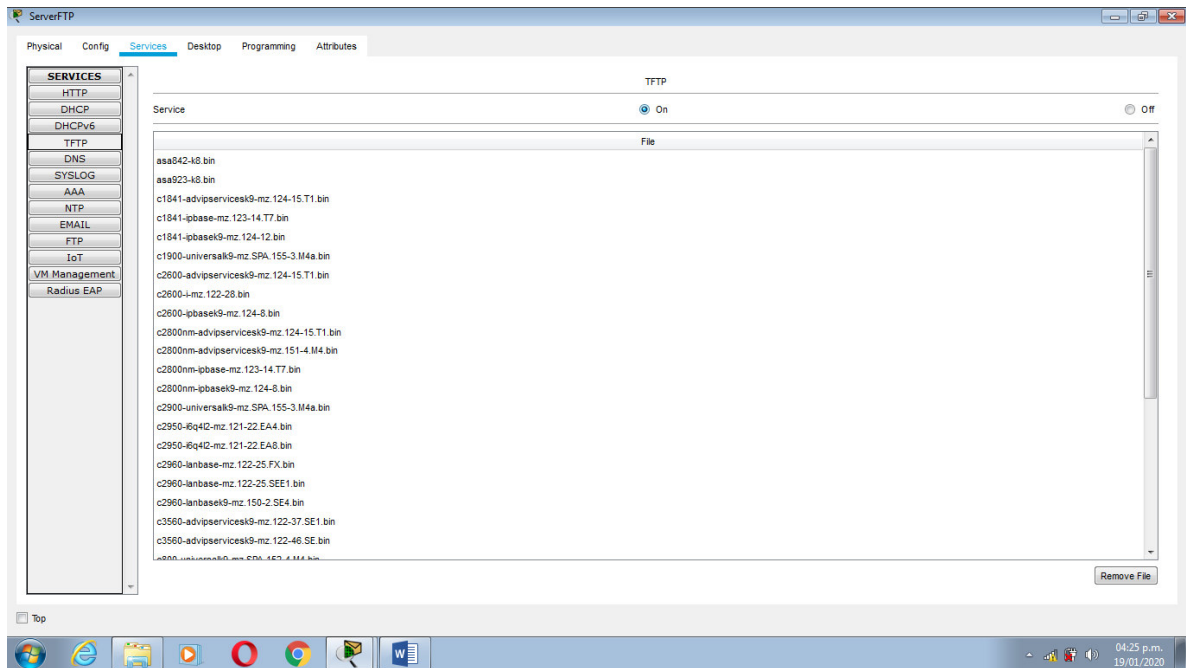


Ilustración 39. Activación del servicio TFTP en el servidor interno..



## Copia de seguridad del Router BUCARAMANGA TFTP

```
BUCARAMANGA>enable
Password:
BUCARAMANGA#
BUCARAMANGA#copy running-config tftp
Address or name of remote host []? 172.31.2.28
Destination filename [BUCARAMANGA-config]? backup_R-bucaramanga
Writing running-config....!!
[OK - 1920 bytes]
1920 bytes copied in 3.023 secs (635 bytes/sec)
BUCARAMANGA#
```

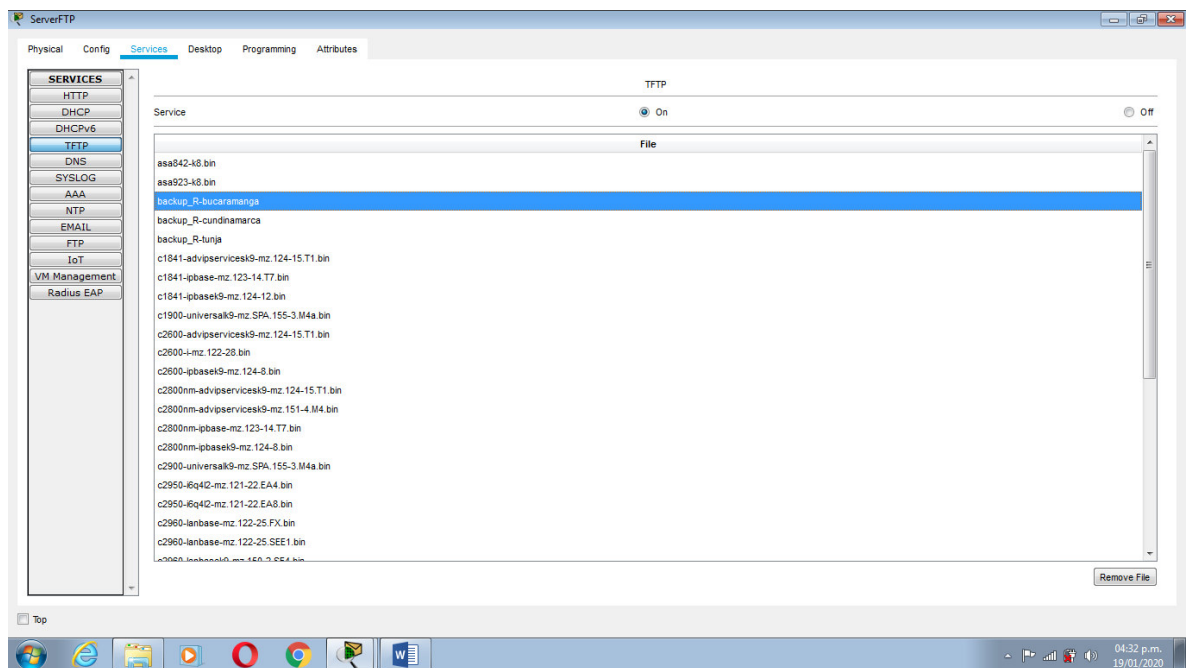
## Copia de seguridad del Router TUNJA TFTP

```
TUNJA >enable
TUNJA#
TUNJA#copy running-config tftp
Address or name of remote host []? 172.31.2.28
Destination filename [TUNJA-config]? backup_R-tunja
Writing running-config...!!
[OK - 2980 bytes]
2980 bytes copied in 0.004 secs (745000 bytes/sec)
TUNJA#
```

## Copia de seguridad del Router CUNDINAMARCA TFTP

```
TUNJA >enable
CUNDINAMARCA#
CUNDINAMARCA#
CUNDINAMARCA#copy running-config tftp
Address or name of remote host []? 172.31.2.28
Destination filename [CUNDINAMARCA-config]? backup_R-cundinamarca
Writing running-config...!!
[OK - 2076 bytes]
2076 bytes copied in 0 secs
CUNDINAMARCA#
```

Ilustración 40. Archivos Backup almacenados en el servidor TFTP



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

## Router TUNJA

Excluimos las direcciones IP que no deseamos que el servidor le proporcione a los clientes

```
TUNJA >enable
Password:
TUNJA #configure terminal
```

```
TUNJA(config)#ip dhcp excluded-address 172.31.0.1
TUNJA(config)# ip dhcp excluded-address 172.31.0.65
TUNJA(config)# ip dhcp excluded-address 172.31.1.65
TUNJA(config)# ip dhcp excluded-address 172.31.1.1
TUNJA(config)#exit
TUNJA#
```

Creamos los pool, de acuerdo a las redes que queremos

```
TUNJA(config)#ip dhcp pool B-10
TUNJA(dhcp-config)#network 172.31.0.0 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.0.1
TUNJA(dhcp-config)#dns-server 172.31.2.28
TUNJA(dhcp-config)#exit
```

```
TUNJA(config)#ip dhcp pool B-30
TUNJA(dhcp-config)#network 172.31.0.64 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.0.65
TUNJA(dhcp-config)#dns-server 172.31.2.28
TUNJA(dhcp-config)#exit
```

```
TUNJA(config)#ip dhcp pool C-20
TUNJA(dhcp-config)#network 172.31.1.64 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.1.65
TUNJA(dhcp-config)#dns-server 172.31.2.28
TUNJA(dhcp-config)#exit
```

```
TUNJA(config)#ip dhcp pool C-30
TUNJA(dhcp-config)#network 172.31.1.0 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.1.1
TUNJA(dhcp-config)#dns-server 172.31.2.28
TUNJA(dhcp-config)#exit
```

Se agrega IP Helper para el Router BUCARAMANGA y el Router CUNDINAMARCA, porque el DHCP se encuentra fuera de la red.

### **Router BUCARAMANGA**

```
BUCARAMANGA(config)#interface FastEthernet0/0.10
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.33
BUCARAMANGA(config-subif)#exit
BUCARAMANGA(config) interface FastEthernet0/0.30
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.33
BUCARAMANGA(config-subif)#end
BUCARAMANGA#
```

### **Router CUNDINAMARCA**

```

CUNDINAMARCA> enable
CUNDINAMARCA # configure terminal
CUNDINAMARCA (config)# interface FastEthernet0/0.20
CUNDINAMARCA (config-if)# ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#end
CUNDINAMARCA#
CUNDINAMARCA#enable
CUNDINAMARCA # configure terminal
CUNDINAMARCA(config)# interface FastEthernet0/0.30
CUNDINAMARCA (config-if)# ip helper-address 172.31.2.37
CUNDINAMARCA (config-subif)#end
CUNDINAMARCA #

```

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

### **Router TUNJA**

```

TUNJA > enable
TUNJA # configure terminal
TUNJA(config)# ip nat inside source static 172.31.2.28 200.17.220.4
TUNJA(config)# access-list 1 permit 172.31.0.0 0.0.31.255
TUNJA(config)# ip nat inside source list 1 interface FastEthernet0/1 overload
TUNJA(config)#ip route 0.0.0.0 0.0.0.0 200.17.220.3
TUNJA(config)#router ospf 1
TUNJA(config-router)#default-information originate
TUNJA(config-router)#
%SYS-5-CONFIG_: Configured from console by console
TUNJA#

```

Establecer dominios inside y outside de la configuración NAT

```

TUNJA(config-if)# interface FastEthernet0/1
TUNJA(config-if)# ip nat outside
TUNJA(config-if)#exit
TUNJA(config)#
TUNJA(config)# interface FastEthernet0/0.1
TUNJA(config-if)# ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#
TUNJA(config)# interface FastEthernet0/0.20
TUNJA(config-if)# ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#

```

```

TUNJA(config)# interface FastEthernet0/0.30
TUNJA(config-if)# ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#
TUNJA(config-if)# interface Serial0/0/0
TUNJA(config-if)# ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#
TUNJA(config-if)# interface Serial0/0/1
TUNJA(config-if)# ip nat inside
TUNJA(config-if)# exit
TUNJA(config)# exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console
TUNJA#

```

**El enrutamiento deberá tener autenticación.**

Activación de OSPF y autenticación MD5 para las interfaces seriales y enrutamiento OSPF en cada uno de los routers

### **Router BUCARAMANGA**

```

BUCARAMANGA#
BUCARAMANGA # configure terminal
BUCARAMANGA (config)# router ospf 1
BUCARAMANGA (config-router)#area 0 authentication message-digest
BUCARAMANGA (config-router)#network 172.31.0.0 0.0.0.63 area 0
BUCARAMANGA (config-router)#network 172.31.0.64 0.0.0.63 area 0
BUCARAMANGA (config-router)#network 172.31.2.0 0.0.0.7 area 0
BUCARAMANGA (config-router)#network 172.31.2.32 0.0.0.3 area 0
BUCARAMANGA (config-router)#exit
BUCARAMANGA (config)#exit
BUCARAMANGA #

```

```

BUCARAMANGA > enable
BUCARAMANGA # configure terminal
BUCARAMANGA (config)# interface serial0/0/0
BUCARAMANGA(config-if)#ip ospf authentication message-digest
BUCARAMANGA(config-if)#ip ospf message-digest-key 1 md5 cisco
BUCARAMANGA (config-if)# exit
BUCARAMANGA(config)#exit
BUCARAMANGA #
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA #

```

## Router TUNJA

```
TUNJA (config)# router ospf 1
TUNJA (config-router)#area 0 authentication message-digest
TUNJA (config-router)#network 172.31.2.8 0.0.0.7 area 0
TUNJA (config-router)#network 172.31.0.128 0.0.0.63 area 0
TUNJA (config-router)#network 172.31.0.192 0.0.0.63 area 0
TUNJA (config-router)#network 172.31.2.32 0.0.0.3 area 0
TUNJA (config-router)#network 172.31.2.36 0.0.0.3 area 0
TUNJA (config-router)#default-information originate
TUNJA (config-router)#exit
TUNJA (config)#exit
TUNJA #
%SYS-5-CONFIG_I: Configured from console by console
TUNJA #
```

```
TUNJA > enable
TUNJA # configure terminal
TUNJA (config)# interface serial0/0/0
TUNJA (config-if)#ip ospf authentication message-digest
TUNJA (config-if)#ip ospf message-digest-key 1 md5 cisco
TUNJA (config-if)# exit
TUNJA (config)# interface serial0/0/1
TUNJA (config-if)#ip ospf authentication message-digest
TUNJA (config-if)#ip ospf message-digest-key 1 md5 cisco
TUNJA (config-if)# exit
```

## Router CUNDINAMARCA

```
CUNDINAMARCA > enable
CUNDINAMARCA # configure terminal
CUNDINAMARCA (config)# interface serial0/0/0
CUNDINAMARCA (config-if)#ip ospf authentication message-digest
CUNDINAMARCA (config-if)#ip ospf message-digest-key 1 md5 cisco
CUNDINAMARCA (config-if)# exit
CUNDINAMARCA (config)# router ospf 1
CUNDINAMARCA (config-router)#area 0 authentication message-digest
CUNDINAMARCA (config-router)#exit
CUNDINAMARCA (config)#exit
CUNDINAMARCA #
%SYS-5-CONFIG_I: Configured from console by console
CUNDINAMARCA #
```

```

CUNDINAMARCA # configure terminal
CUNDINAMARCA (config)# router ospf 1
CUNDINAMARCA (config-router)#area 0 authentication message-digest
CUNDINAMARCA (config-router)#network 172.31.1.0 0.0.0.63 area 0
CUNDINAMARCA (config-router)#network 172.31.1.64 0.0.0.63 area 0
CUNDINAMARCA (config-router)#network 172.31.2.16 0.0.0.7 area 0
CUNDINAMARCA (config-router)#network 172.31.2.36 0.0.0.3 area 0
CUNDINAMARCA (config-router)#network 172.31.2.24 0.0.0.7 area 0
CUNDINAMARCA (config-router)#exit
CUNDINAMARCA (config)#exit
CUNDINAMARCA #
CUNDINAMARCA #configure terminal
Enter configuration commands, one per line. End with CNTL/Z
CUNDINAMARCA (config)# interface FastEthernet0/0.1
CUNDINAMARCA (config-subif)#encapsulation dot1q 1 native
CUNDINAMARCA (config-subif)# ip address 172.31.2.17 255.255.255.248
CUNDINAMARCA (config-subif)#end
CUNDINAMARCA #
%SYS-5-CONFIG_I: Configured from console by console
CUNDINAMARCA #
CUNDINAMARCA #configure terminal
Enter configuration commands, one per line. End with CNTL/Z
CUNDINAMARCA (config)# interface FastEthernet0/0.20
CUNDINAMARCA (config-subif)#encapsulation dot1q 20
CUNDINAMARCA (config-subif)# ip address 172.31.1.65 255.255.255.192
CUNDINAMARCA (config-subif)#end
CUNDINAMARCA #
%SYS-5-CONFIG_I: Configured from console by console
CUNDINAMARCA #
CUNDINAMARCA #configure terminal
Enter configuration commands, one per line. End with CNTL/Z
CUNDINAMARCA (config)# interface FastEthernet0/0.30
CUNDINAMARCA (config-subif)#encapsulation dot1q 30
CUNDINAMARCA (config-subif)# ip address 172.31.1.1 255.255.255.192
CUNDINAMARCA (config-subif)#end
CUNDINAMARCA #
%SYS-5-CONFIG_I: Configured from console by console
CUNDINAMARCA #
CUNDINAMARCA #
CUNDINAMARCA #configure terminal
Enter configuration commands, one per line. End with CNTL/Z
CUNDINAMARCA (config)# interface FastEthernet0/0.88
CUNDINAMARCA (config-subif)#encapsulation dot1q 88
CUNDINAMARCA (config-subif)# ip address 172.31.2.25 255.255.255.248
CUNDINAMARCA (config-subif)#end

```

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

## **EI DHCP no proporciona direcciones a los hosts de Tunja**

### **PC3-VLAN20-TUNJA**

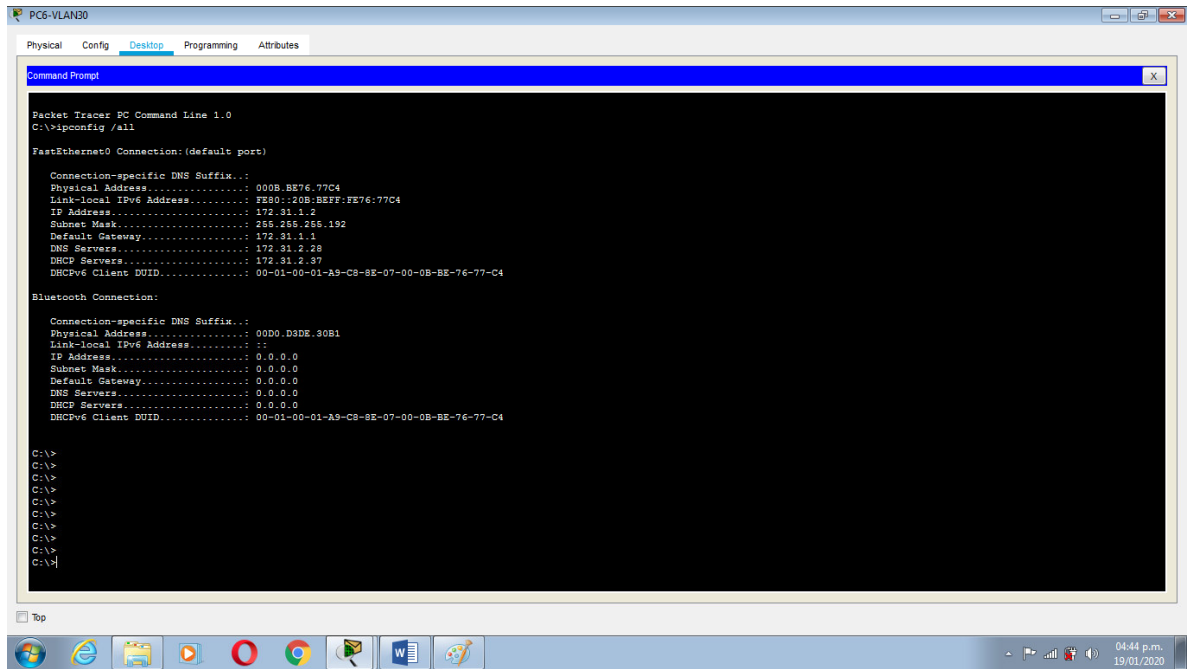
```
Packet Tracer PC Command Line 1.0
C:\>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::201:C9FF:FE62:3842
Autoconfiguration IP Address....: 169.254.56.66
Subnet Mask.....: 255.255.0.0
Default Gateway.....: 0.0.0.0
Bluetooth Connection:
Link-local IPv6 Address.....: ::
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0
C:\>
```

### **PC4-VLAN30-TUNJA**

```
Packet Tracer PC Command Line 1.0
C:\>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::290:21FF:FE6A:B869
Autoconfiguration IP Address....: 169.254.184.105
Subnet Mask.....: 255.255.0.0
Default Gateway.....: 0.0.0.0
Bluetooth Connection:
Link-local IPv6 Address.....: ::
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0
C:\>
```



Ilustración 43. DHCP host de Cundinamarca Vlan30



The screenshot shows a Packet Tracer PC configuration window for 'PCS-VLAN30'. The 'Config' tab is active, displaying a 'Command Prompt' window. The command prompt shows the output of the 'ipconfig /all' command, detailing network configuration for both FastEthernet0 and Bluetooth connections. The FastEthernet0 configuration includes a physical address of 000B.BE76.77C4, a link-local IPv6 address of FE80::20B:BEFF:FE76:77C4, an IP address of 172.31.1.2, a subnet mask of 255.255.255.192, a default gateway of 172.31.1.1, DNS servers at 172.31.2.28, and DHCP servers at 172.31.2.27. The Bluetooth connection is disabled and has default settings. The taskbar at the bottom shows the system tray with the date and time: 04:44 p.m., 19/01/2020.

```
Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

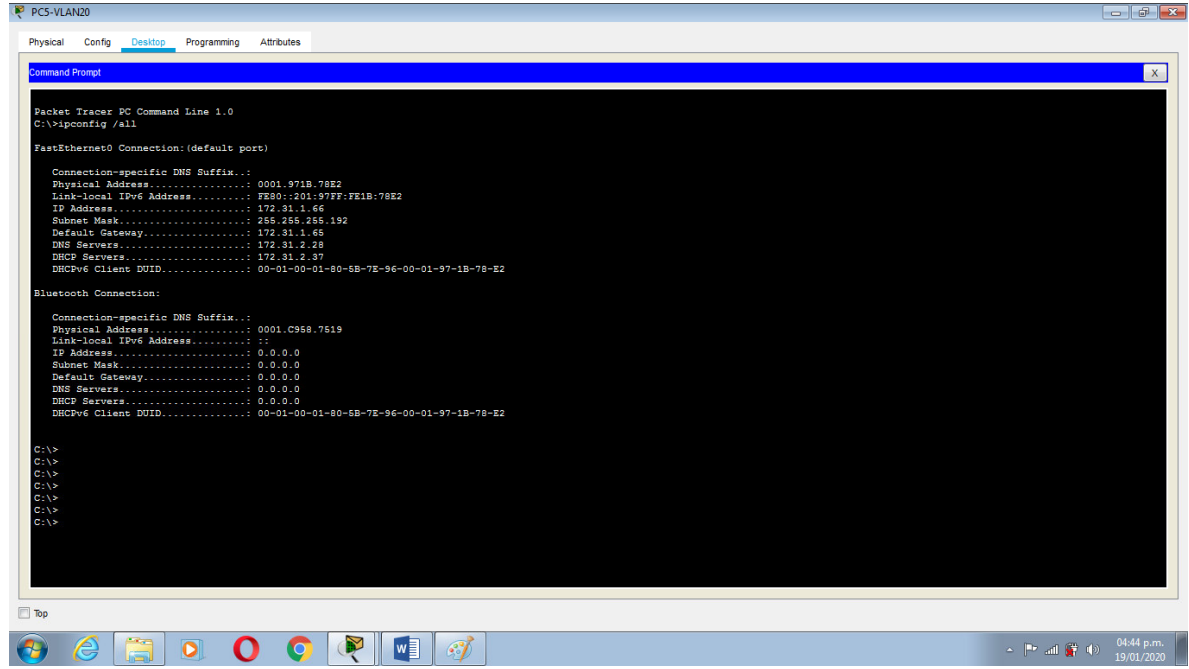
Connection-specific DNS Suffix...:
Physical Address. . . . .: 000B.BE76.77C4
Link-local IPv6 Address. . . . .: FE80::20B:BEFF:FE76:77C4
IP Address. . . . .: 172.31.1.2
Subnet Mask. . . . .: 255.255.255.192
Default Gateway. . . . .: 172.31.1.1
DNS Servers. . . . .: 172.31.2.28
DHCP Servers. . . . .: 172.31.2.27
DHCPv6 Client DUID. . . . .: 00-01-00-01-A9-C8-8E-07-00-0B-BE-76-77-C4

Bluetooth Connection:

Connection-specific DNS Suffix...:
Physical Address. . . . .: 00D0.D3DE.30B1
Link-local IPv6 Address. . . . .: ::
IP Address. . . . .: 0.0.0.0
Subnet Mask. . . . .: 0.0.0.0
Default Gateway. . . . .: 0.0.0.0
DNS Servers. . . . .: 0.0.0.0
DHCP Servers. . . . .: 0.0.0.0
DHCPv6 Client DUID. . . . .: 00-01-00-01-A9-C8-8E-07-00-0B-BE-76-77-C4

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
```

Ilustración 44. DHCP host de Cundinamarca Vlan20



The screenshot shows a Packet Tracer PC configuration window for 'PCS-VLAN20'. The 'Config' tab is active, displaying a 'Command Prompt' window. The command prompt shows the output of the 'ipconfig /all' command, detailing network configuration for both FastEthernet0 and Bluetooth connections. The FastEthernet0 configuration includes a physical address of 0001.971B.78E2, a link-local IPv6 address of FE80::201:97FF:FE1B:78E2, an IP address of 172.31.1.66, a subnet mask of 255.255.255.192, a default gateway of 172.31.1.66, DNS servers at 172.31.2.28, and DHCP servers at 172.31.2.37. The Bluetooth connection is disabled and has default settings. The taskbar at the bottom shows the system tray with the date and time: 04:44 p.m., 19/01/2020.

```
Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Physical Address. . . . .: 0001.971B.78E2
Link-local IPv6 Address. . . . .: FE80::201:97FF:FE1B:78E2
IP Address. . . . .: 172.31.1.66
Subnet Mask. . . . .: 255.255.255.192
Default Gateway. . . . .: 172.31.1.66
DNS Servers. . . . .: 172.31.2.28
DHCP Servers. . . . .: 172.31.2.37
DHCPv6 Client DUID. . . . .: 00-01-00-01-80-5B-7E-96-00-01-97-1B-78-E2

Bluetooth Connection:

Connection-specific DNS Suffix...:
Physical Address. . . . .: 0001.C959.7519
Link-local IPv6 Address. . . . .: ::
IP Address. . . . .: 0.0.0.0
Subnet Mask. . . . .: 0.0.0.0
Default Gateway. . . . .: 0.0.0.0
DNS Servers. . . . .: 0.0.0.0
DHCP Servers. . . . .: 0.0.0.0
DHCPv6 Client DUID. . . . .: 00-01-00-01-80-5B-7E-96-00-01-97-1B-78-E2

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
```

Ilustración 45. Comunicación de host de Router Bucaramanga Vlan10 a red Tunja y Vlan20 red Cundinamarca

```
PCO-VLAN10
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.31.0.130
Pinging 172.31.0.130 with 32 bytes of data:
Reply from 172.31.0.130: bytes=32 time=5ms TTL=126
Reply from 172.31.0.130: bytes=32 time=1ms TTL=126
Reply from 172.31.0.130: bytes=32 time=1ms TTL=126
Reply from 172.31.0.130: bytes=32 time=1ms TTL=126
Ping statistics for 172.31.0.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms
C:\>ping 172.31.0.194
Pinging 172.31.0.194 with 32 bytes of data:
Reply from 172.31.0.194: bytes=32 time=1ms TTL=126
Reply from 172.31.0.194: bytes=32 time=1ms TTL=126
Reply from 172.31.0.194: bytes=32 time=1ms TTL=126
Reply from 172.31.0.194: bytes=32 time=1ms TTL=126
Ping statistics for 172.31.0.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\>ping 172.31.1.66
Pinging 172.31.1.66 with 32 bytes of data:
Reply from 172.31.1.66: bytes=32 time=3ms TTL=125
Reply from 172.31.1.66: bytes=32 time=3ms TTL=125
Reply from 172.31.1.66: bytes=32 time=3ms TTL=125
Reply from 172.31.1.66: bytes=32 time=3ms TTL=125
Ping statistics for 172.31.1.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 5ms, Average = 3ms
```

Ilustración 46. Comunicación de host de Router Bucaramanga Vlan10 a red Bucaramanda y Servidor Web

```
PCO-VLAN10
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.31.1.2
Pinging 172.31.1.2 with 32 bytes of data:
Request timed out.
Reply from 172.31.1.2: bytes=32 time=2ms TTL=125
Reply from 172.31.1.2: bytes=32 time=2ms TTL=125
Reply from 172.31.1.2: bytes=32 time=7ms TTL=125
Ping statistics for 172.31.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 7ms, Average = 5ms
C:\>ping 172.31.2.28
Pinging 172.31.2.28 with 32 bytes of data:
Reply from 172.31.2.28: bytes=32 time=8ms TTL=125
Reply from 172.31.2.28: bytes=32 time=2ms TTL=125
Reply from 172.31.2.28: bytes=32 time=2ms TTL=125
Reply from 172.31.2.28: bytes=32 time=5ms TTL=125
Ping statistics for 172.31.2.28:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 8ms, Average = 4ms
C:\>ping 209.17.220.3
Pinging 209.17.220.3 with 32 bytes of data:
Reply from 209.17.220.3: bytes=32 time=2ms TTL=126
Reply from 209.17.220.3: bytes=32 time=1ms TTL=126
Reply from 209.17.220.3: bytes=32 time=2ms TTL=126
Reply from 209.17.220.3: bytes=32 time=1ms TTL=126
Ping statistics for 209.17.220.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Ilustración 48. Comunicación de host de Router Cundinamarca Vlan30 a red Bucaramanga y Servidor FTP.

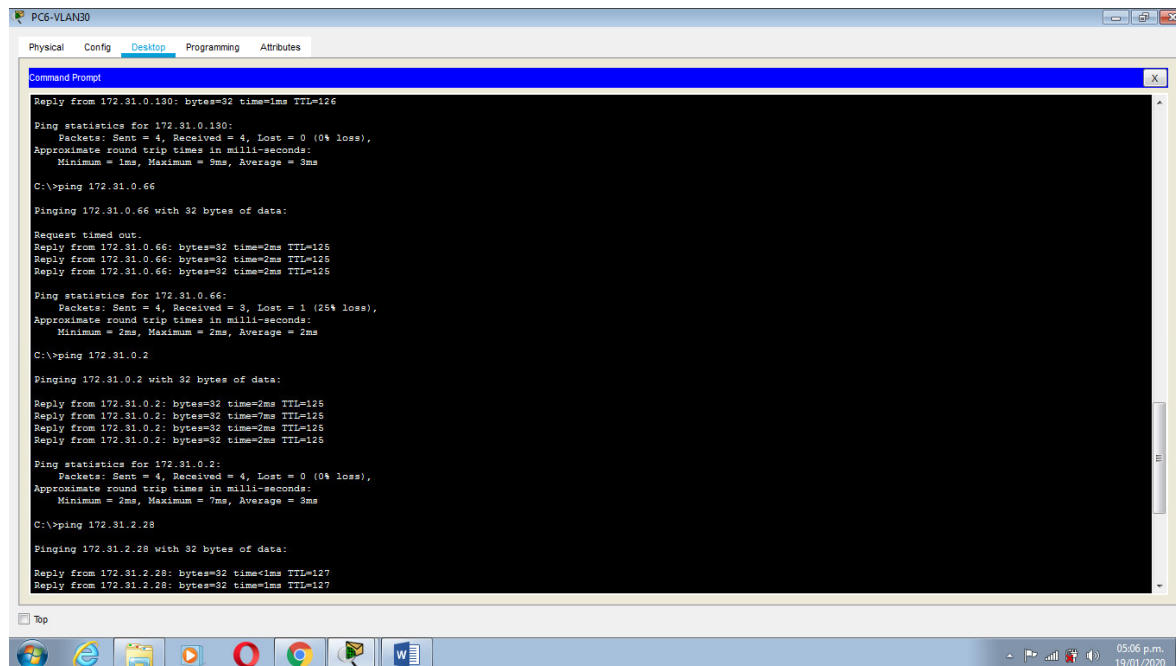


Ilustración 47. Comunicación de host de Router Cundinamarca Vlan30 a red Cundinamarca.

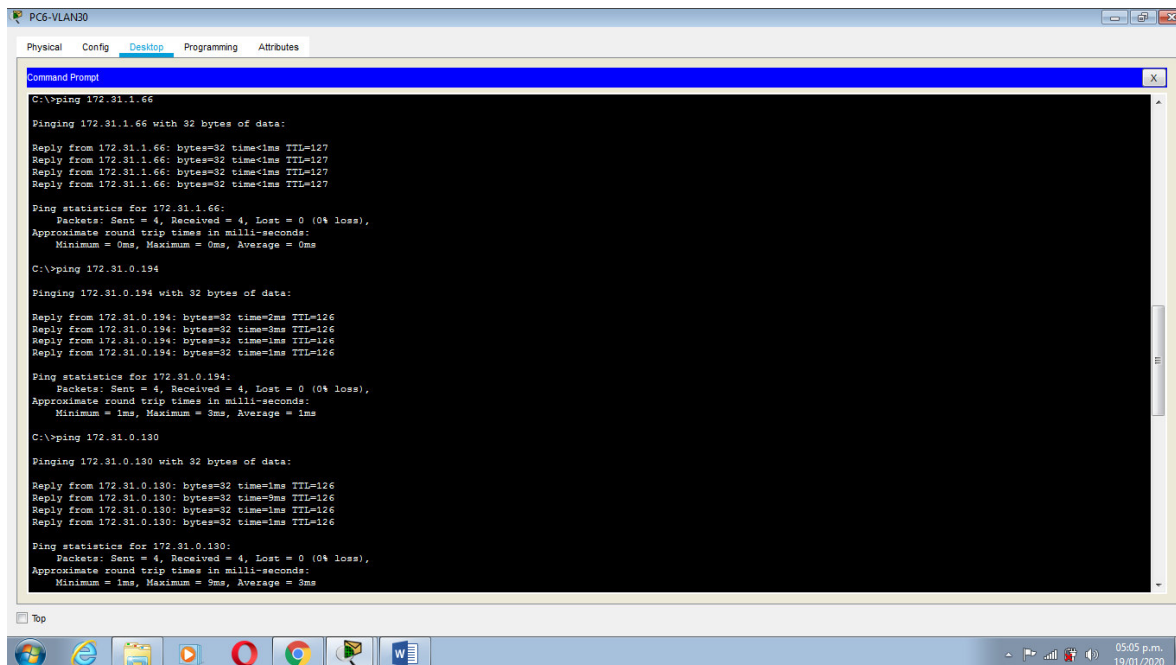
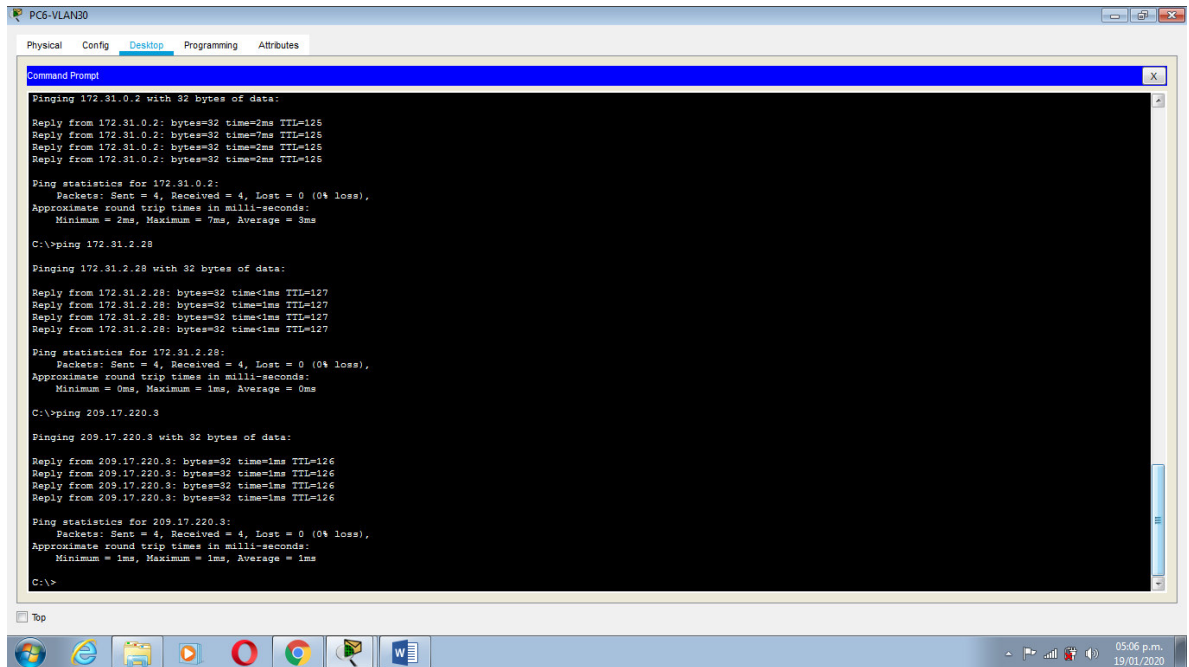


Ilustración 49. Comunicación de host de Router Cundinamarca Vlan30 a Servidor FTP y Servidor Web.



## Listas de control de acceso:

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

```
CUNDINAMARCA(config)#access-list 100 deny ip 172.31.1.64 0.0.0.63 200.17.220.0 0.0.0.255
```

```
CUNDINAMARCA(config)#access-list 100 permit ip any any
```

```
CUNDINAMARCA(config)#interface FastEthernet0/0.20
```

```
CUNDINAMARCA(config-subif)#ip access-group 100 in
```

```
CUNDINAMARCA(config-subif)#
```



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

```
TUNJA(config)#access-list 100 permit tcp 172.31.0.192 0.0.0.63 200.17.220.0
0.0.0.255 eq 80
TUNJA(config)#access-list 100 permit tcp 172.31.0.192 0.0.0.63 200.17.220.0
0.0.0.255 eq 21
TUNJA(config)#access-list 100 permit tcp 172.31.0.192 0.0.0.63 200.17.220.0
0.0.0.255 eq 20
TUNJA(config)#interface FastEthernet0/0.30
TUNJA(config-subif)#ip access-group 100 in
TUNJA(config-subif)#
```

*Ilustración 52. Verificación control de acceso hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet (servidor web).*

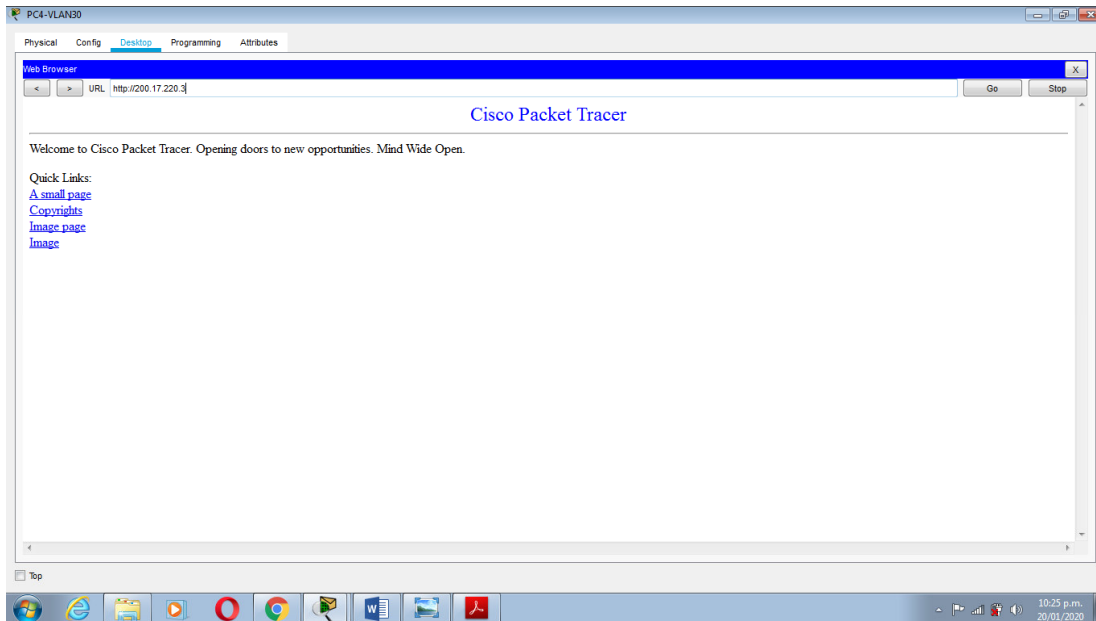
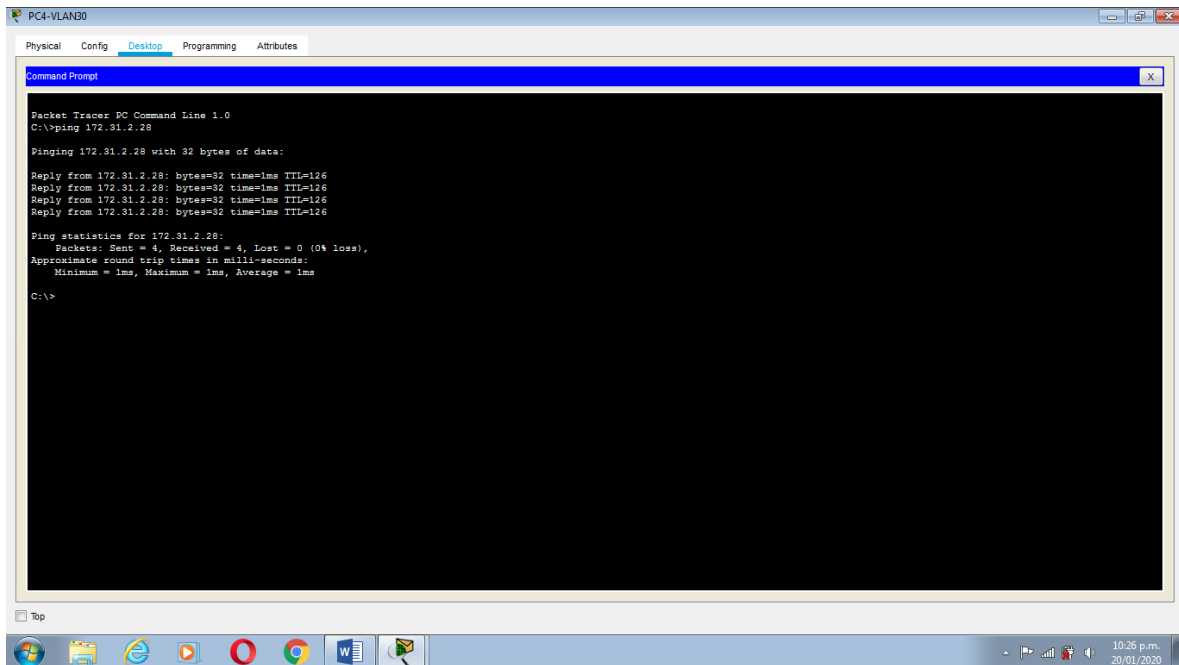
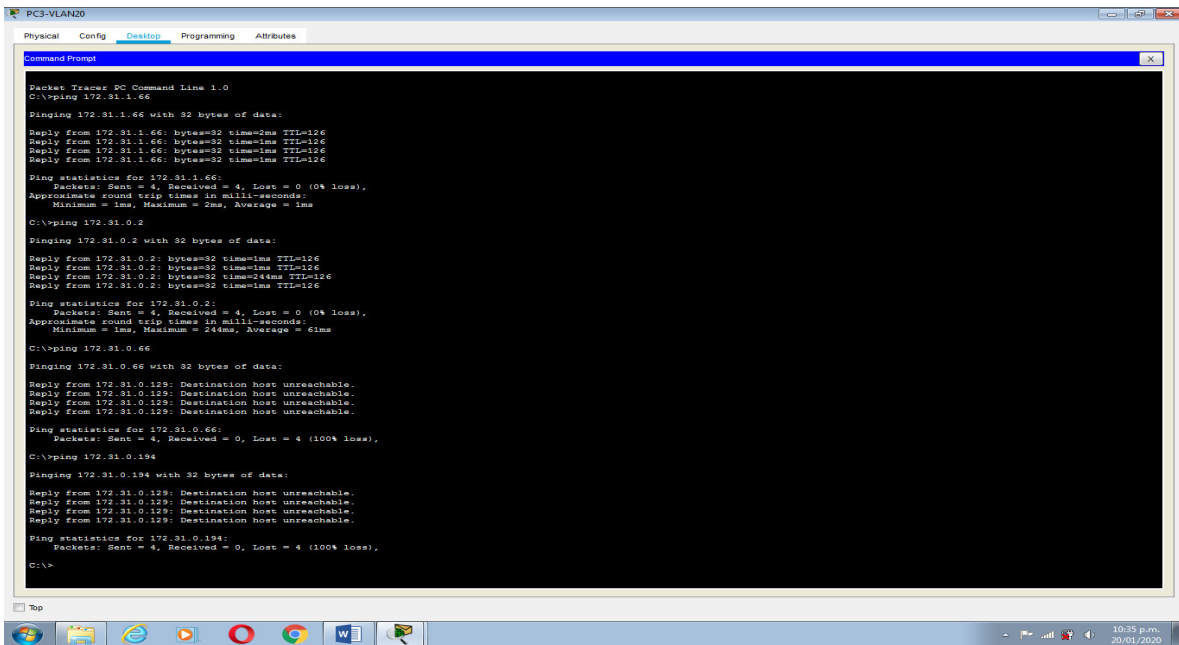


Ilustración 53. Verificación control de acceso hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de interne (servidor ftp).



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

Ilustración 54. Verificación control de acceso hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.



```

TUNJA(config-subif)#access-list 102 permit ip 172.31.0.128 0.0.0.63 172.31.1.64
0.0.0.63
TUNJA(config)#access-list 102 permit ip 172.31.0.128 0.0.0.63 172.31.0.0
0.0.0.63
TUNJA(config)#interface FastEthernet0/0.20
TUNJA(config-subif)#ip access-group 102 in

```

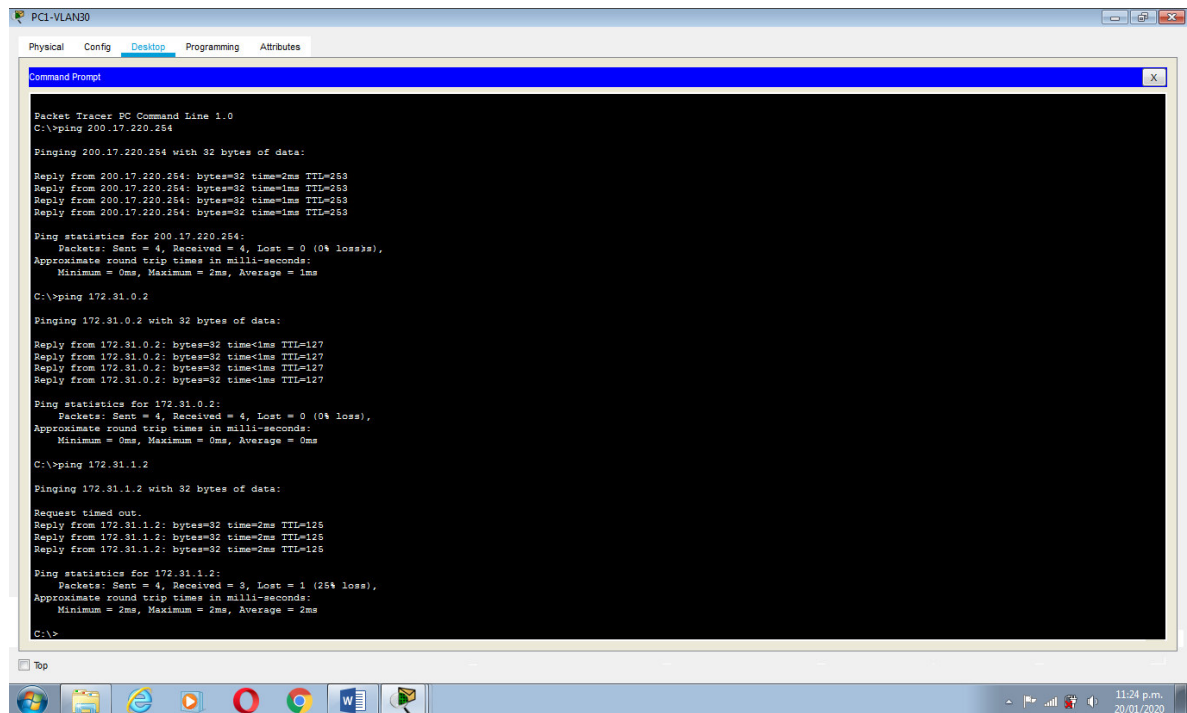
- Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.

```

BUCARAMANGA(config)#access-list 101 permit ip 172.31.0.64 0.0.0.63
200.17.220.0 0.0.0.255
BUCARAMANGA(config)#interface FastEthernet0/0.30
BUCARAMANGA(config-subif)#ip access-group 101 in
BUCARAMANGA(config-subif)#end
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#

```

*Ilustración 55. Verificación control de acceso hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.*



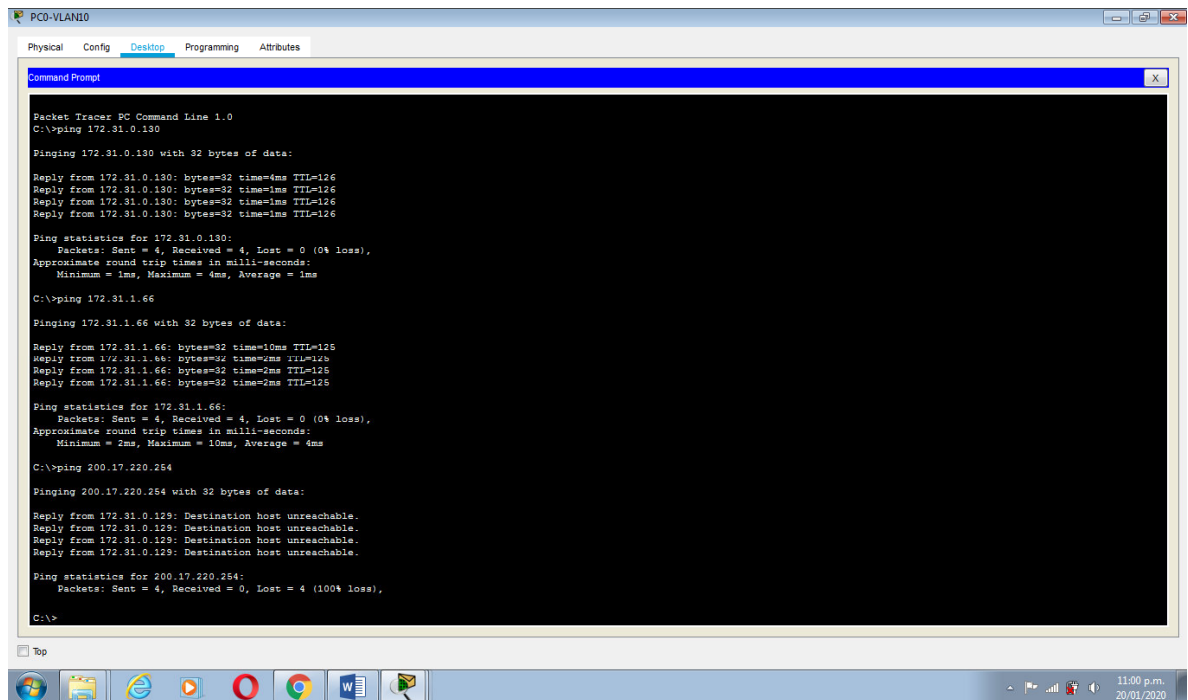
- Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.

```

BUCARAMANGA(config)#access-list 102 permit ip 172.31.0.0 0.0.0.63
172.31.1.64 0.0.0.63
BUCARAMANGA(config)#access-list 102 permit ip 172.31.0.0 0.0.0.63
172.31.0.128 0.0.0.63
BUCARAMANGA(config)#interface FastEthernet0/0.10
BUCARAMANGA(config-subif)#ip access-group 102 in
BUCARAMANGA(config-subif)#end
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
BUCARAMANGA#

```

*Ilustración 56. Verificación control de acceso 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.

```

BUCARAMANGA(config)#access-list 103 deny ip 172.31.2.0 0.0.0.7
172.31.0.0 0.0.0.63
BUCARAMANGA(config)#access-list 103 deny ip 172.31.0.64 0.0.0.63
172.31.0.0 0.0.0.63
BUCARAMANGA(config)#access-list 103 permit ip any any
BUCARAMANGA(config)#interface FastEthernet0/0.10
BUCARAMANGA(config-subif)#ip access-group 103 out
BUCARAMANGA(config-subif)#end
BUCARAMANGA#

```









Ilustración 64. Verificación control de acceso los hosts de las VLAN administrativas y de la VLAN de servidores tienen acceso a los routers e internet (VLAN Bucaramanga no tienen acceso a los routers e internet)

```
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 200.17.220.1 with 32 bytes of data:
Reply from 172.31.0.65: Destination host unreachable.
Reply from 172.31.0.65: Destination host unreachable.
Reply from 172.31.0.65: Destination host unreachable.
Reply from 172.31.0.65: Destination host unreachable.
Ping statistics for 200.17.220.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 172.31.2.34
Pinging 172.31.2.34 with 32 bytes of data:
Reply from 172.31.0.65: Destination host unreachable.
Reply from 172.31.0.65: Destination host unreachable.
Reply from 172.31.0.65: Destination host unreachable.
Reply from 172.31.0.65: Destination host unreachable.
Ping statistics for 172.31.2.34:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 172.31.2.38
Pinging 172.31.2.38 with 32 bytes of data:
Reply from 172.31.0.65: Destination host unreachable.
Reply from 172.31.0.65: Destination host unreachable.
Reply from 172.31.0.65: Destination host unreachable.
Reply from 172.31.0.65: Destination host unreachable.
Ping statistics for 172.31.2.38:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 200.17.220.254
Pinging 200.17.220.254 with 32 bytes of data:
Reply from 172.31.0.65: Destination host unreachable.
Reply from 172.31.0.65: Destination host unreachable.
```

Ilustración 63. Verificación control de acceso los hosts de las VLAN administrativas y de la VLAN de servidores tienen acceso a los routers e internet (VLAN Cundinamarca tienen acceso a los routers e internet)

```
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 172.31.2.34
Pinging 172.31.2.34 with 32 bytes of data:
Reply from 172.31.2.34: bytes=32 time=2ms TTL=253
Reply from 172.31.2.34: bytes=32 time=2ms TTL=253
Reply from 172.31.2.34: bytes=32 time=4ms TTL=253
Reply from 172.31.2.34: bytes=32 time=2ms TTL=253
Ping statistics for 172.31.2.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 2ms
C:\>ping 172.31.2.38
Pinging 172.31.2.38 with 32 bytes of data:
Reply from 172.31.2.38: bytes=32 time=1ms TTL=254
Reply from 172.31.2.38: bytes=32 time=1ms TTL=254
Reply from 172.31.2.38: bytes=32 time=4ms TTL=254
Reply from 172.31.2.38: bytes=32 time=1ms TTL=254
Ping statistics for 172.31.2.38:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 1ms
C:\>ping 172.31.2.38
Pinging 172.31.2.38 with 32 bytes of data:
Reply from 172.31.2.38: bytes=32 time<1ms TTL=255
Reply from 172.31.2.38: bytes=32 time<1ms TTL=255
Reply from 172.31.2.38: bytes=32 time<1ms TTL=255
Reply from 172.31.2.38: bytes=32 time<1ms TTL=255
Ping statistics for 172.31.2.38:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

**Habilitar VLAN en cada switch y permitir su enrutamiento.**

## SWITCH BUCARAMANGA

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SB
SB(config)#enable password class
SB(config)#line console 0
SB(config-line)#password cisco
SB(config-line)#login
SB(config-line)#line vty 0 15
SB(config-line)#password cisco
SB(config-line)#login
SB(config-line)#exit
SB(config)#line console 0
SB(config-line)#logging synchronous
SB(config)#vlan 1
SB(config-vlan)#vlan 10
SB(config-vlan)#vlan 30
SB(config-vlan)# interface FastEthernet 0/10
SB(config-if)#switchport mode access
SB(config-if)#switchport access vlan 10
SB(config-if)# interface FastEthernet 0/24
SB(config-if)#switchport mode access
SB(config-if)#switchport access vlan 30
SB(config-if)# interface FastEthernet 0/1
SB(config-if)#switchport mode trunk
SB(config-if)#int vlan 1
SB(config-if)#ip address 172.31.2.3 255.255.255.248
SB(config-if)#no shutdown
SB(config-if)#ip default-gateway 172.31.2.1
```

## SWITCH TUNJA

```
Switch(config)#
Switch>enable
Switch(config)#configure terminal
Switch(config)#no ip domain-lookup
Switch(config)#hostname ST
ST(config)#enable password class
ST(config)#line console 0
ST(config-line)#password cisco
ST(config-line)#login
ST(config-line)#line vty 0 15
ST(config-line)#password cisco
```

```
ST(config-line)#login
ST(config-line)#exit
ST(config)#line console 0
ST(config-line)#logging synchronous
ST(config)#vlan 1
ST(config-vlan)#vlan 20
ST(config-vlan)#vlan 30
ST(config-vlan)#interface FastEthernet0/20
ST(config-if)#switchport mode access
ST(config-if)#switchport access vlan 20
ST(config-if)#interface FastEthernet0/24
ST(config-if)#switchport mode access
ST(config-if)#switchport access vlan 30
ST(config-if)#interface FastEthernet0/1
ST(config-if)#switchport mode trunk
ST(config-if)#int vlan 1
ST(config-if)#ip address 172.3.2.11 255.255.255.248
ST(config-if)#no shutdown
ST(config-if)#ip default-gateway 172.31.2.9
```

## **SWITCH CUNDINAMARCA**

```
Switch>enable
Switch(config)#configure terminal
Switch(config)#no ip domain-lookup
Switch(config)#hostname SC
SC(config)#enable password class
SC(config)#line console 0
SC(config-line)#password cisco
SC(config-line)#login
SC(config-line)#line vty 0 15
SC(config-line)#password cisco
SC(config-line)#login
SC(config-line)#exit
SC(config)#line console 0
SC(config-line)#logging synchronous
SC(config)#vlan 1
SC(config-vlan)#vlan 20
SC(config-vlan)#vlan 30
SC(config-vlan)#vlan 88
SC(config-vlan)#exit
SC(config)# interface FastEthernet0/10
SC(config-if)#switchport mode access
SC(config-if)#switchport access vlan 20
SC(config-if)# interface FastEthernet0/20
```

```
SC(config-if)#switchport mode access
SC(config-if)#switchport access vlan 30
SC(config-if)# interface FastEthernet0/24
SC(config-if)#switchport mode access
SC(config-if)#switchport access vlan 88
SC(config-if)# interface FastEthernet0/1
SC(config-if)#switchport mode trunk
SC(config-if)#int vlan 1
SC(config-if)#ip address 172.31.2.11 255.255.255.248
SC(config-if)#no shutdown
SC(config-if)#ip default-gateway 172.31.2.9
```

## CONCLUSIONES

Se logró da solución a los dos casos propuestos, comprendiendo así las configuraciones básicas del enrutamiento estático y dinámico, el funcionamiento de los protocolos RIP, VLSM, EIGRP y OSPF. Comprendiendo también el funcionamiento de los enrutadores y conmutadores en las redes locales bajo el estándar Ethernet.

El manejo de casos de estudios nos permite enfrentarnos a una situación real, esto nos permite poner en prácticas todo el conocimiento adquirido a fin de resolver los problemas plantados preparándonos de esta forma para el mundo real en donde este escenario será el pan de cada día en nuestras labores profesionales como administradores de red.

El software PACKET TRACERT es una excelente herramienta, la cual me ha permitido el diseño e implementación de las redes simulando diversos ambientes. Poniendo en práctica todo el conocimiento adquirido y realizándolo de tal forma que simula a la perfección el comportamiento de los equipos físicos reales. Tan cual como si se estuviera en frente de los equipos de red.

## BIBLIOGRAFÍA

CISCO. (2017, 5 septiembre). Enhanced Interior Gateway Routing Protocol. Recuperado 13 diciembre, 2019, de <https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html>

Cisco Systems, Inc.. (s.f.). Configuración básica de seguridad. Recuperado 13 diciembre, 2019, de [https://www.academia.edu/24211601/Configuración\\_básica\\_de\\_seguridad](https://www.academia.edu/24211601/Configuración_básica_de_seguridad)

CISCO. (2017, 26 julio). Configuring Basic AAA on an Access Server. Recuperado 13 diciembre, 2019, de <https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html>

CISCO. (2017, 26 septiembre). AAA Authentication login default local group tacacs+ CLI Explained. Recuperado 13 diciembre, 2019, de <https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/200606-aaa-authentication-login-default-local.html>

MIKROWAYS. (2010, 6 junio). Tipos de NAT y configuración en Cisco. Recuperado 13 diciembre, 2019, de <https://www.mikroways.net/2010/06/06/tipos-de-nat-y-configuracion-en-cisco/>