PRUEBA DE HABILIDADES PRÁCTICAS CCNA

WILLIAM GEOVANNY NAVARRO CAÑON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA DE SISTEMAS

2019

PRUEBA DE HABILIDADES PRÁCTICAS CCNA

WILLIAM GEOVANNY NAVARRO CAÑON

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

TUTOR

NILSON ALBEIRO FERREIRA MANZANARES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA DE SISTEMAS

2019

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Presidente del Jurado

Jurado

Jurado

DEDICATORIA

Le dedico a mi familia que me ha apoyado y a las personas más cercanas que me han impulsado a para cumplir mis metas y poder ir cumpliendo los objetivos que tengo propuestos en lo académico y en lo personal enseñándome cuales son los valores que debo tener y mis responsabilidades.

AGRADECIMIENTO

Agradezco a cada de una de las personas que me he encontrado en el camino para poder desarrollar un conocimiento académico, a todos los compañeros con los que participe en cada curso y a los tutores que me dieron lineamientos para elaborar y llevar a cabo cada uno de los cursos obteniendo el conocimiento necesario e incrementando mis habilidades y aptitudes académicas.

CONTENIDO

LISTA DE TABLAS

TABLA DE FIGURAS

RESUMEN

Durante el desarrollo del Diplomado de profundización CISCO se vinieron desarrollando diferentes tipos de laboratorios sobre casos puntuales que necesitaban solución y para ello se usaron herramientas como el software Packet Tracert y laboratorios en línea preparados por CISCO con equipos conectados a la red para realizar las simulaciones de configuración en equipos reales.

Se pretende entonces que el estudiante desarrolle las habilidades y el conocimiento para realizar el montaje de una red, configurando los diferentes dispositivos y equipos necesarios como routers, switches y equipos de cómputo; para la actividad final se necesita dar solución a dos escenarios propuestos, realizando las configuraciones pertinentes y haciendo uso del software de Packet Tracert para realizar la simulación del montaje de la red con sus diferentes equipos y configuraciones.

ABSTRACT

During the development of the CISCO deepening Diploma, different types of laboratories were developed on specific cases that needed solution and for this purpose tools such as Packet Tracert software and online laboratories prepared by CISCO with equipment connected to the network were used to perform the simulations of configuration in real equipment.

It is then intended that the student develop the skills and knowledge to perform the assembly of a network, configuring the different devices and equipment necessary as routers, switches and computer equipment; For the final activity it is necessary to solve two proposed scenarios, making the relevant configurations and using the Packet Tracert software to perform the simulation of the network assembly with its different equipment and configurations.

INTRODUCCIÓN

Para la culminación del diplomado de profundización CISCO se pretende desarrollar dos ejercicios con los conocimientos adquiridos durante los cursos vistos en las plataformas de CISCO, se requiere entonces aplicar diferentes configuraciones en routers, switches y PCs; se necesita también realizar la configuración de redes LAN/WAN y realizar todo esto en un software para la simulación como Packet Tracert.

PRUEBA DE HABILIDADES PRÁCTICAS CCNA

Escenario 1

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

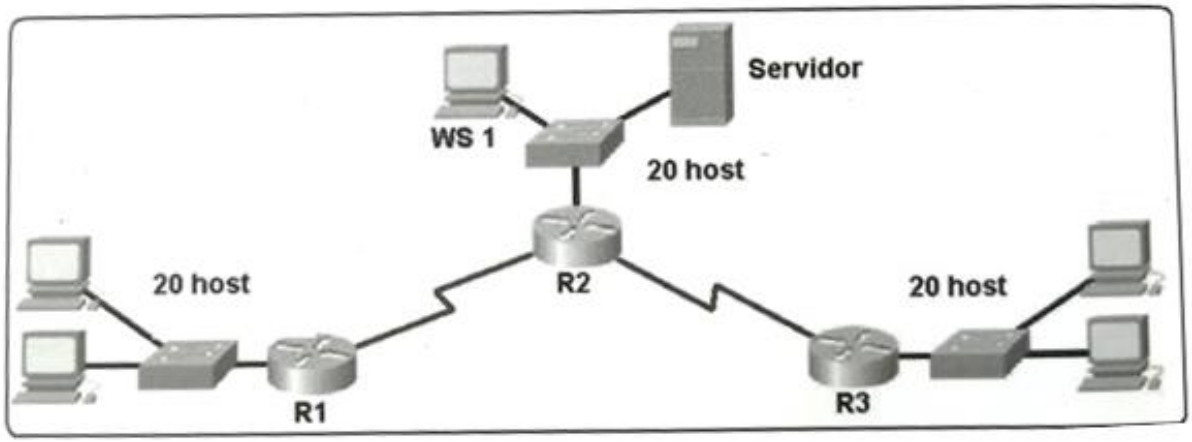


Figura 1 – Topología Escenario 1

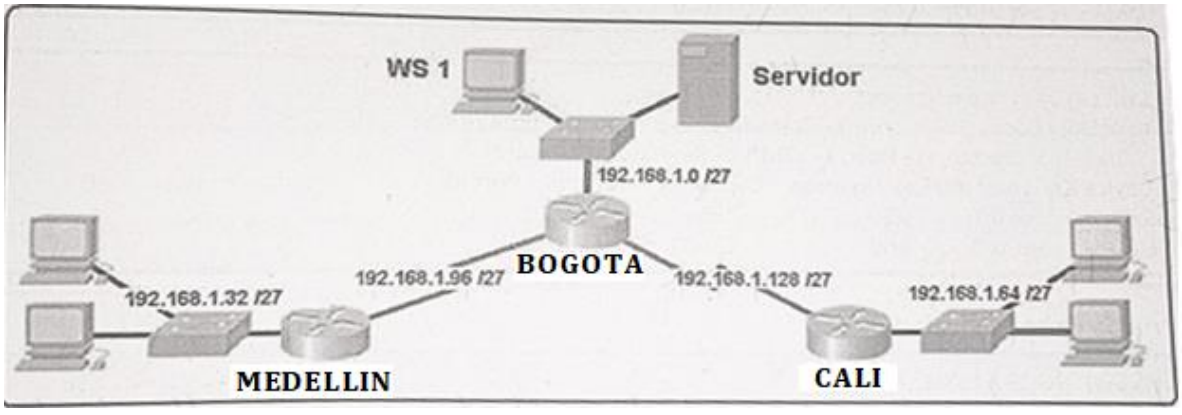


Figura 2 – Topología Escenario 1

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

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

Configuración Routers

- **Router Medellín**

  #en
  #config t
  #no ip domain-lookup
  #enable secret cisco
  #line con 0
  #password class
  #exit
  #line vty 0 15
  #password class
  #login
  #exit
  #service password-encryption
  #exit
  #copy running-config startup-config

- **Router Bogotá**

  #en
  #config t
  #no ip domain-lookup
  #enable secret cisco
  #line con 0
  #password class
  #exit
  #line vty 0 15
  #password class
  #login
  #exit
  #service password-encryption

#exit
#copy running-config startup-config

- **Router Cali**
-
- #en
- #config t
- #no ip domain-lookup
- #enable secret cisco
- #line con 0
- #password class
- #exit
- #line vty 0 15
- #password class
- #login
- #exit
- #service password-encryption
- #exit
- #copy running-config startup-config

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.

N° sub red	Dirección subred	Broadcast	Netmask
1	192.168.1.0	192.168.1.31	255.255.255.224
2	192.168.1.32	192.168.1.63	255.255.255.224
3	192.168.1.64	192.168.1.95	255.255.255.224
4	192.168.1.96	192.168.1.127	255.255.255.224
5	192.168.1.128	192.168.1.159	255.255.255.224
6	192.168.1.160	192.168.1.191	255.255.255.224
7	192.168.1.192	192.168.1.223	255.255.255.224
8	192.168.1.224	192.168.1.255	255.255.255.224

Tabla 1 – Subneteo Red

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.

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

	R1	R2	R3
Nombre de Host	**MEDELLIN**	**BOGOTA**	**CALI**
Dirección de Ip en interfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/1		192.168.1.130	
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	**Eigrp**	**Eigrp**	**Eigrp**
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

Tabla 2 – Asignación IP

- **Asignación IP Router Medellín**

```
#en
#config t
#int fa0/0
#ip add 192.168.1.33 255.255.255.224
#no shut
#exit
#int s1/0
#ip add 192.168.199 255.255.255.224
```

#no shut
#end

- **Asignación IP Router Cali**

#en
#config t
#int fa0/0
#ip add 192.168.1.65 255.255.255.224
#no shut
#exit
#int s1/0
#ip add 192.168.131 255.255.255.224
#no shut
#end

- **Asignación IP Router Bogota**

#en
#config t
#int fa2/0
#ip add 192.168.1.1 255.255.255.224
#no shut
#exit
#int s0/0
#ip add 192.168.1.98 255.255.255.224
#no shut
#exit
#int s1/0
#ip add 192.168.1.130 255.255.255.224
#no shut
#end

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.

#show ip route

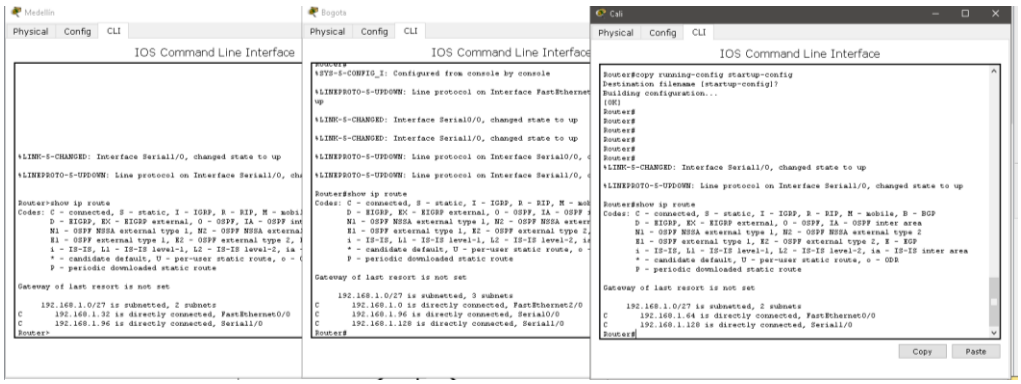


Figura 3 – Tabla de enrutamiento

c. Verificar el balanceo de carga que presentan los routers

#show ip route

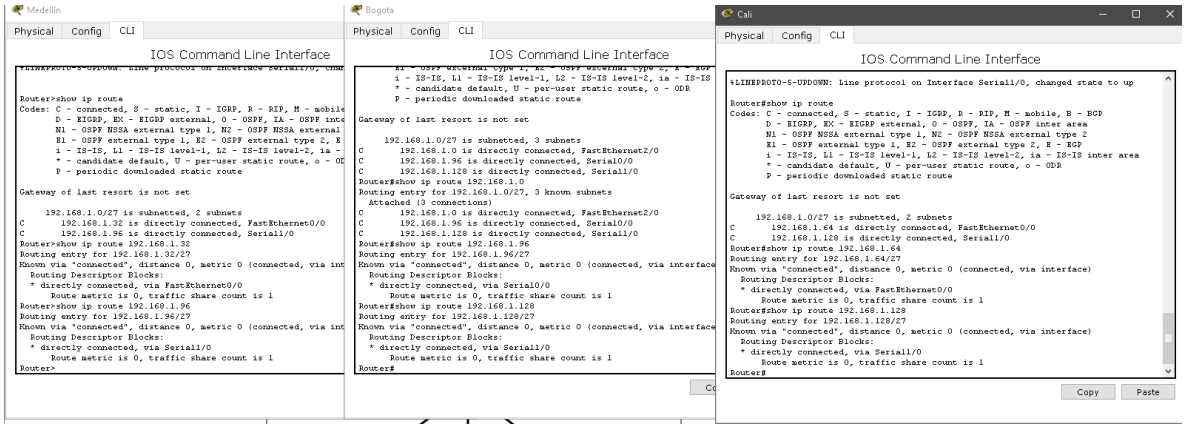


Figura 4 – Balanceo de enrutamiento

d. Realizar un diagnóstico de vecinos usando el comando cdp.

#sh cdp neighbors

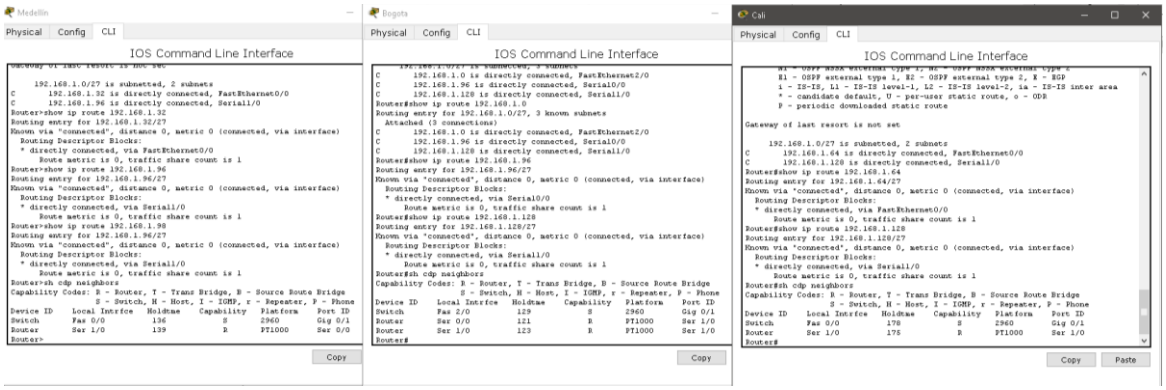


Figura 5 – Diagnostico de Vecinos.

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

>ping 192.168.1.99

>ping 192.168.1.131

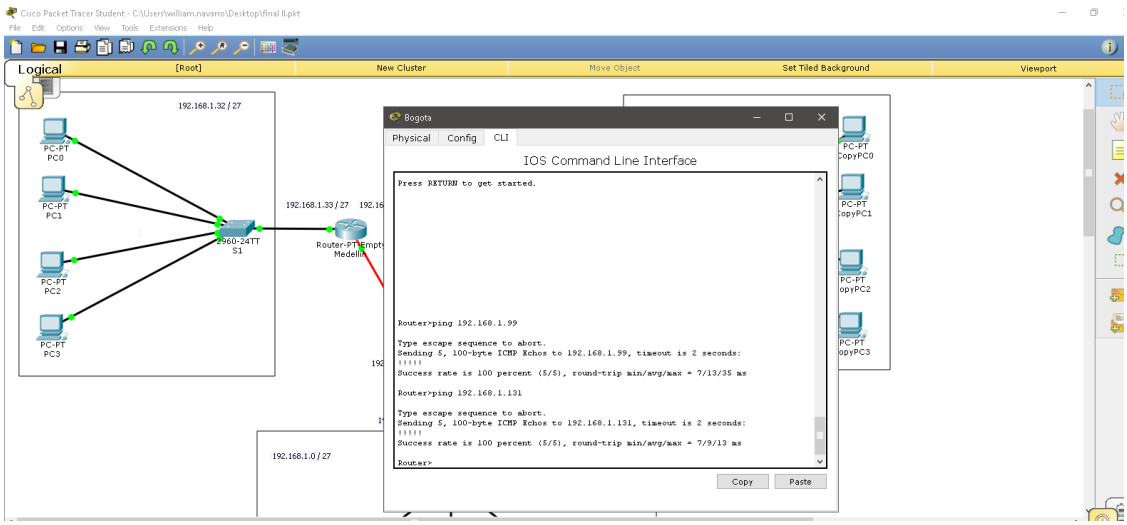


Figura 6 – Verificación de ping

Parte 3: Configuración de Enrutamiento.

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

- **Enrutamiento router Medellín**

#en

#config t

#router eigrp 200

#network 192.168.1.32 0.0.0.31

#network 192.168.1.96 0.0.0.31

#no auto-summary

- **Enrutamiento router Cali**

#en

#config t

#router eigrp 200

#network 192.168.1.64 0.0.0.31

#network 192.168.1.128 0.0.0.31

#no auto-summary

- **Enrutamiento router Medellín**

#en

#config t

#router eigrp 200

#network 192.168.1.96 0.0.0.31

#network 192.168.1.128 0.0.0.31

#network 192.168.1.0 0.0.0.31

#no auto-summary

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

#sh ip eigrp neighbors

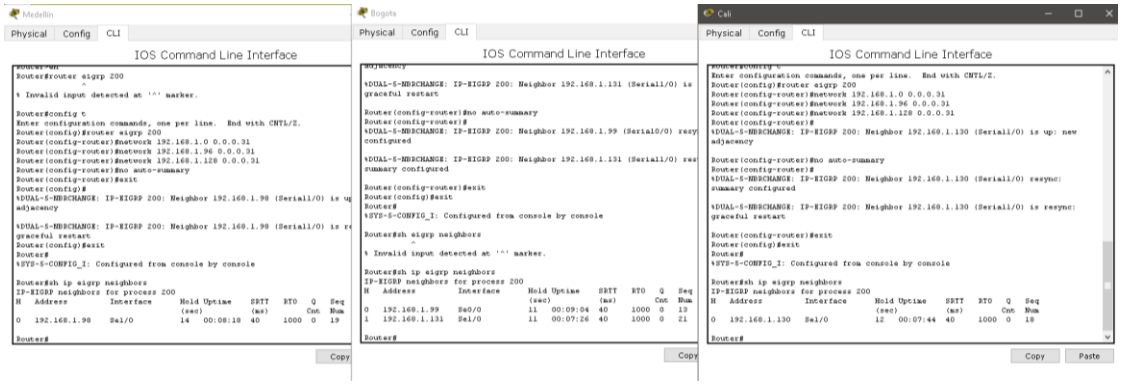


Figura 7 – Vecindad de routers

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

#sh ip route

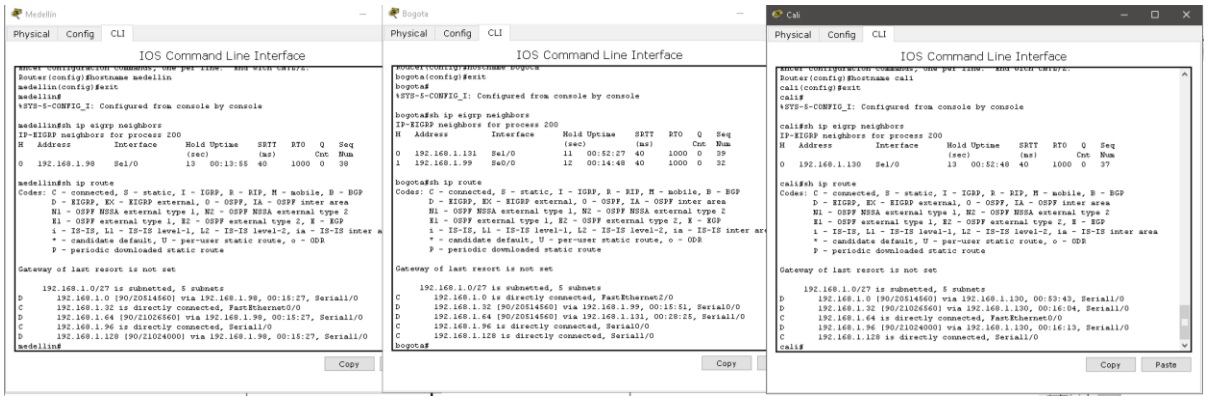


Figura 8 – Tablas de enrutamiento

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.

- Ping a host red de Medellín.

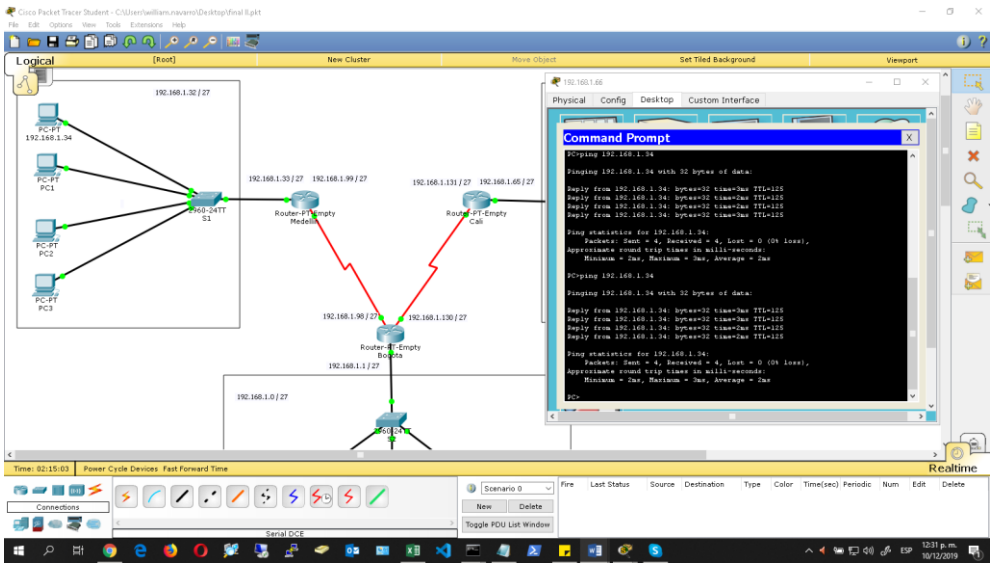


Figura 9 – ping host Medellín

- Ping a host servidor Bogot

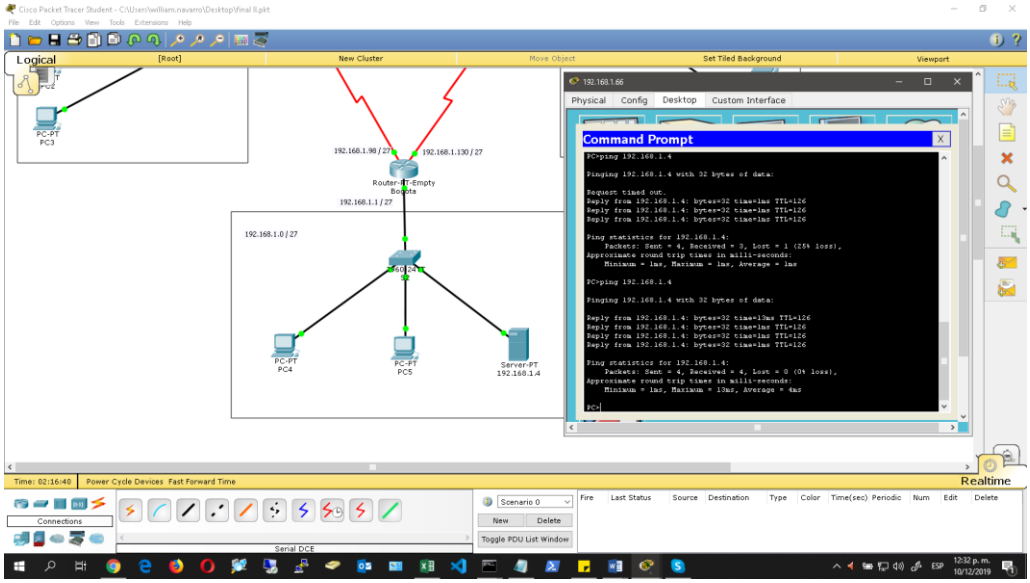


Figura 10 – Ping host Bogotá

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.

- Configuración Telnet Medellin
  #en
  #config t
  #line vty 0 4
  #password class
  #login
  #exit

- Configuración Telnet Bogota
  #en
  #config t
  #line vty 0 4
  #password class
  #login
  #exit

- Configuración Telnet Cali
  #en
  #config t
  #line vty 0 4
  #password class
  #login
  #exit

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.

- **Configuración Router Medellín y Cali**

#access-list 110 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.2

#access-list 110 permit icmp any any echo-reply

#access-list 110 deny ip any any

#int fastO/O

#ip access-group 110 in

- **Configuración Router Bogota**

#access-list 110 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.2

#access-list 110 deny ip any any

#int fastO/O

#ip access-group 110 out

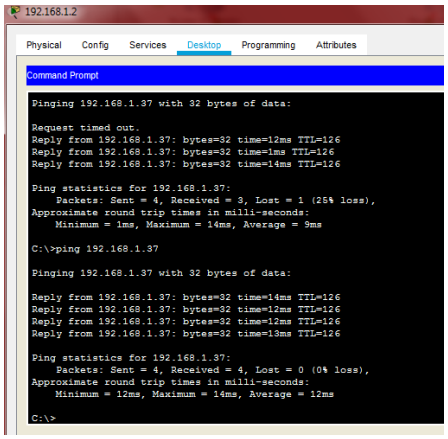


Figura 11 – Ping pc Medellín

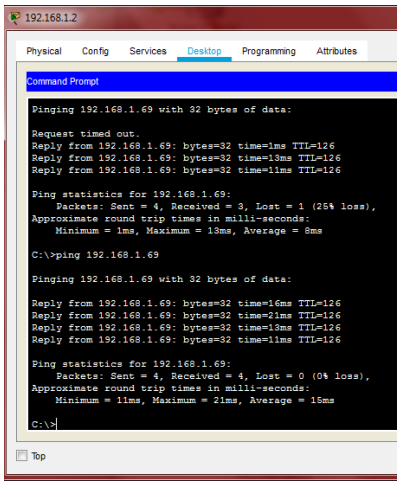


Figura 12 -Ping pc Cali

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.

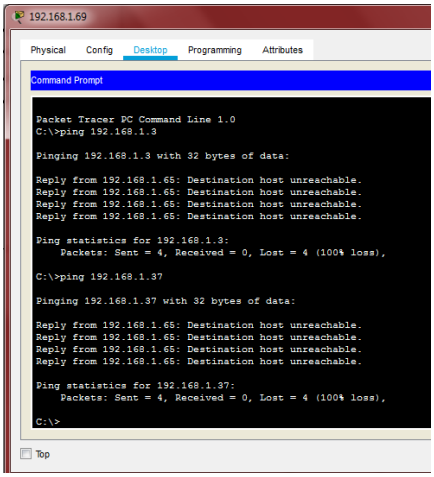


Figura 13 – ping Cali a Servidor

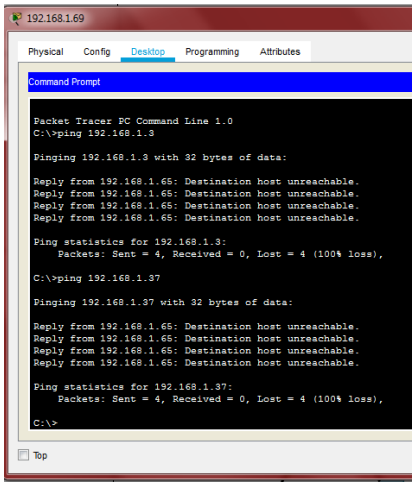


Figura 14 – ping Cali a Medellín

Parte 5: Comprobación de la red instalada.

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

-Router Medellín

#show access-list
Extended IP access list 110
10 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.2
20 permit icmp any any echo-reply
30 deny ip any any

-Router Bogota

#show access-list
Extended IP access list 110
10 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.2
20 deny ip any any

-Router Cali

#show access-list
Extended IP access list 110
10 permit ip 192.168.1.0 0.0.0.255 host 192.168.1.2
20 permit icmp any any echo-reply
30 deny ip any any

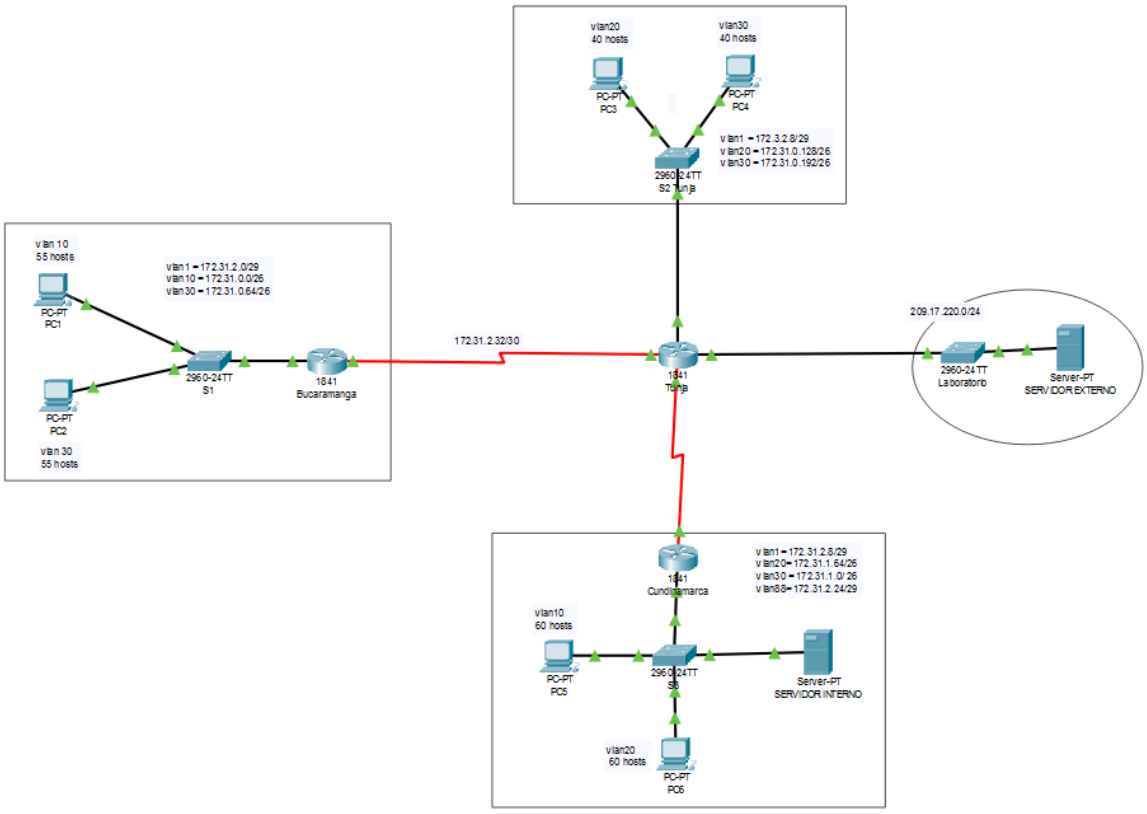
b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.

	ORIGEN	DESTINO	RESULTADO
TELNET	**Router MEDELLIN**	**Router CALI**	Permitido
	WS_1	**Router BOGOTA**	Permitido
	Servidor	**Router CALI**	Permitido
	Servidor	**Router MEDELLIN**	Permitido
TELNET	**LAN del Router MEDELLIN**	**Router CALI**	Denegado
	LAN del Router CALI	**Router CALI**	Denegado
	LAN del Router MEDELLIN	**Router MEDELLIN**	Denegado
	LAN del Router CALI	**Router MEDELLIN**	Denegado
PING	**LAN del Router CALI**	**WS_1**	Denegado
	LAN del Router MEDELLIN	**WS_1**	Denegado
	LAN del Router MEDELLIN	**LAN del Router CALI**	Denegado
PING	**LAN del Router CALI**	**Servidor**	Permitido
	LAN del Router MEDELLIN	**Servidor**	Permitido
	Servidor	**LAN del Router MEDELLIN**	Permitido
	Servidor	**LAN del Router CALI**	Permitido
	Router CALI	**LAN del Router MEDELLIN**	Permitido
	Router MEDELLIN	**LAN del Router CALI**	Permitidos

Tabla 3 – Comprobaciones escenario 1

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.



Desarrollo

Los siguientes son los requerimientos necesarios:

- Todos los routers deberán tener los siguiente:

- Configuración básica.

- **Configuración Router Bucaramanga**

#conf term

#hostname bucaramanga

#no ip domain-lookup

#banner motd “Solo personal autorizado”

#enable secret consola

#line console 0

#password cisco

#login

#logging synchronous

#line vty 0 15

#password cisco

#login

#logging synchronous

#int f0/0.1

#encapsulation dot1q 1

#ip address 172.31.2.1 255.255.255.248

#int f0/0.10

#encapsulation dot1q 10

#ip address 172.31.0.1 255.255.255.192

#int f0/0.30

#encapsulation dot1q 30

#ip address 172.31.0.65 255.255.255.192

#int f0/0

#no shutdown

#int s0/0/0

#ip address 172.31.2.34 255.255.255.252

#no shutdown

#router ospf 1

#network 172.31.0.0 0.0.0.63 area 0

#network 172.31.0.64 0.0.0.63 area 0

#network 172.31.2.0 0.0.0.7 area 0

#network 172.31.2.32 0.0.0.3 area 0

#end

- **Configuración Router Tunja**

>en

#conf term

#hostname tunja

#no ip domain-lookup

#banner motd “Solo personal autorizado”

#enable secret cisco

#line console 0

#password consola

#login

#logging synchronous

#line vty 0 15

#password cisco

#login

#logging synchronous

#int f0/0.1

#encapsulation dot1q 1

#ip address 172.3.2.9 255.255.255.248

#int f0/0.20

#encapsulation dot1q 20

#ip address 172.31.0.129 255.255.255.192

#int f0/0.30

#encapsulation dot1q 30

#ip address 172.31.0.193 255.255.255.192

#int f0/0

#no shutdown

#int s0/0/0

#ip address 172.31.2.33 255.255.255.252

#no shutdown

#int s0/0/1

#ip address 172.31.2.37 255.255.255.252

#no shutdown

#int f0/1

#ip address 209.165.220.1 255.255.255.0

#no shutdown

#router ospf 1

#network 172.3.2.8 0.0.0.7 area 0

#network 172.31.0.128 0.0.0.63 area 0

#network 172.31.0.192 0.0.0.63 area 0

#network 172.31.2.32 0.0.0.3 area 0

#network 172.31.2.36 0.0.0.3 area 0

#end

- **Configuración Router Cundinamarca**

>en

#conf term

#hostname cundinamarca

#no ip domain-lookup

#banner motd “Solo personal autorizado”

#enable secret consola

#line console 0

#password cisco123

#login

#logging synchronous

#line vty 0 15

#password consola

#login

#logging synchronous

#int f0/0.1

#encapsulation dot1q 1

#ip address 172.31.2.9 255.255.255.248

#int f0/0.20

#encapsulation dot1q 20

#ip address 172.31.1.65 255.255.255.192

#int f0/0.30

#encapsulation dot1q 30

#ip address 172.31.1.1 255.255.255.192

#int f0/0.88

#encapsulation dot1q 88

#ip address 172.31.2.25 255.255.255.248

#int f0/0

#no shutdown

#int s0/0/0

#ip address 172.31.2.38 255.255.255.252

#no shutdown

#router ospf 1

#network 172.31.1.0 0.0.0.63 area 0

#network 172.31.1.64 0.0.0.63 area 0

#network 172.31.2.8 0.0.0.7 area 0

#network 172.31.2.24 0.0.0.7 area 0

#network 172.31.2.36 0.0.0.3 area 0

#end

- **Configuración Switch Bucaramanga**

>en

#conf term

#hostname S1

#vlan 1

#vlan 10

#vlan 30

#int f0/20

#switchport mode access

#switchport access vlan 10

#int f0/24

#switchport mode access

#switchport access vlan 30

#int f0/1

#switchport mode trunk

#int vlan 1

#ip address 172.31.2.3 255.255.255.248

#no shutdown

#ip default-gateway 172.31.2.1

- **Configuración Switch Tunja**

>en

#conf term

#hostname SWTUNJA

#vlan 1

#vlan 20

#vlan 30

#int f0/20

#switchport mode access

#switchport access vlan 20

#int f0/24

#switchport mode access

#switchport access vlan 30

#int f0/1

#switchport mode trunk

#int vlan 1

#ip address 172.3.2.11 255.255.255.248

#no shutdown

#ip default-gateway 172.3.2.9

- **Configuración Switch Cundinamarca**

>en

#conf term

#hostname SWCUNDINAMARCA

#vlan 1

#vlan 20

#vlan 30

#vlan 88

#exit

#int f0/20

#switchport mode access

#switchport access vlan 20

#int f0/24

#switchport mode access

#switchport access vlan 30

#int f0/10

#switchport mode access

#switchport access vlan 88

#int f0/1

#switchport mode trunk

#int vlan 1

#ip address 172.31.2.11 255.255.255.248

#no shutdown

#ip default-gateway 172.31.2.9

- **Autenticación AAA Bucaramanga**

#username admin secret cisco

#aaa new-model

#aaa authentication login AUTH local

#line console 0

#login authentication AUTH

#line vty 0 15

#login authentication AUTH

#service password-encryption

- **Autenticación AAA Tunja**

#username admin secret cisco

#aaa new-model

#aaa authentication login AUTH local

#line console 0

#login authentication AUTH

#line vty 0 15

#login authentication AUTH

#service password-encryption

- **Autenticación AAA Cundinamarca**

#username admin secret cisco

#aaa new-model

#aaa authentication login AUTH local

#line console 0

#login authentication AUTH

#line vty 0 15

#login authentication AUTH

#service password-encryption

- **Intentos de acceso al router**

Bucaramanga

#login block-for 5 attempts 4 within 60

Tunja

#login block-for 5 attempts 4 within 60

Cundinamarca

#login block-for 5 attempts 4 within 60

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

Bucaramanga

#login block-for 5 attempts 4 within 60

Tunja

#login block-for 5 attempts 4 within 60

Cundinamarca

#login block-for 5 attempts 4 within 60

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

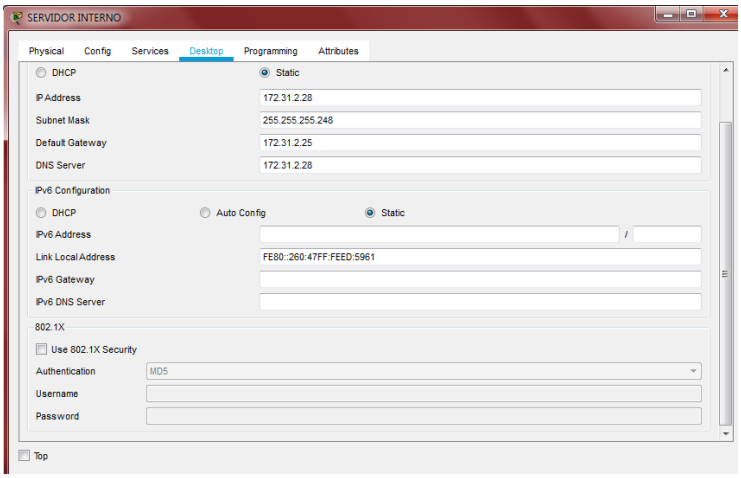


Figura 15 -Servidor Interno

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

- **Router Tunja**

#ip dhcp excluded-address 172.31.0.1

#ip dhcp excluded-address 172.31.0.65

#ip dhcp excluded-address 172.31.1.65

#ip dhcp excluded-address 172.31.1.1

#ip dhcp pool V10B

#network 172.31.0.0 255.255.255.192

#default-router 172.31.0.1

#dns-server 172.31.2.28

#ip dhcp pool V30B

#network 172.31.0.64 255.255.255.192

#default-router 172.31.0.65

#dns-server 172.31.2.28

#ip dhcp pool V20C

#network 172.31.1.64 255.255.255.192

#default-router 172.31.1.65

#dns-server 172.31.2.28

#ip dhcp pool V30C

#network 172.31.1.0 255.255.255.192

#default-router 172.31.1.1

#dns-server 172.31.2.28

- **Router Bucaramanga**

#int f0/0.10

#ip helper-address 172.31.2.33

#int f0/0.30

#ip helper-address 172.31.2.33

#end

- **Router Cundinamarca**

#int f0/0.20

#ip helper-address 172.31.2.37

#int f0/0.30

#ip helper-address 172.31.2.37

#end

- **Pc Bucaramanga**

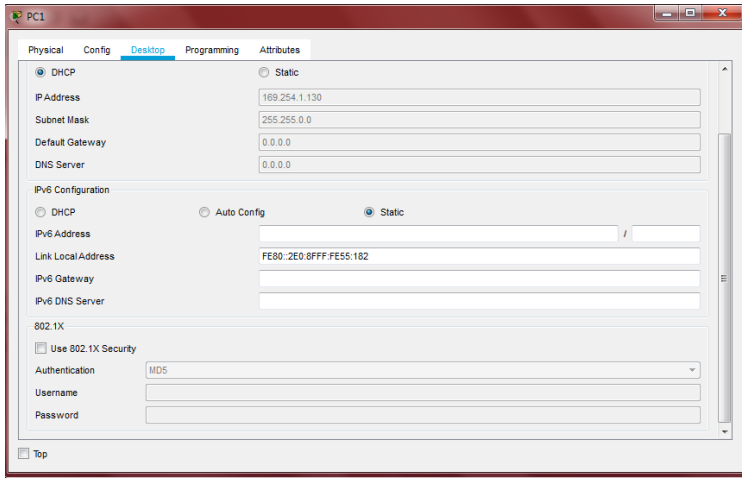


Figura 16 – Configuración Pc Bucaramanga

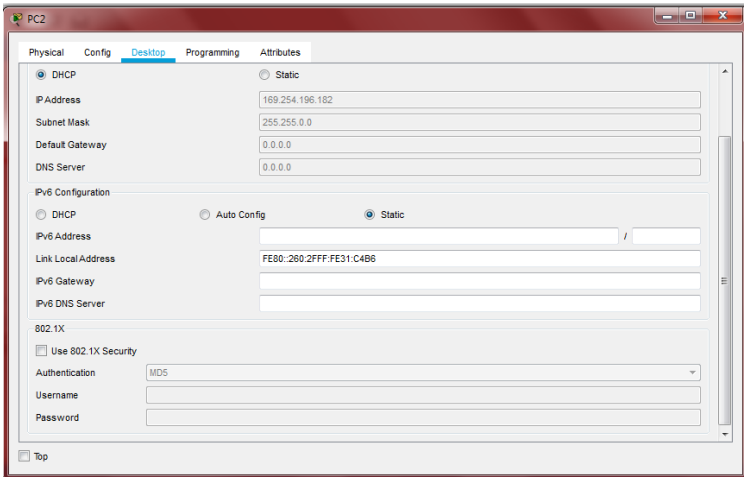


Figura 17 – Configuración Pc Bucaramanga

- **Pc Tunja**

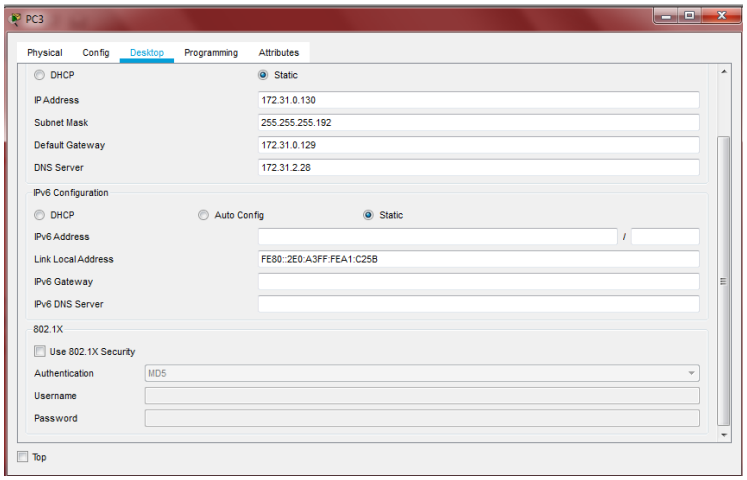


Figura 18 – configuración Pc Tunja

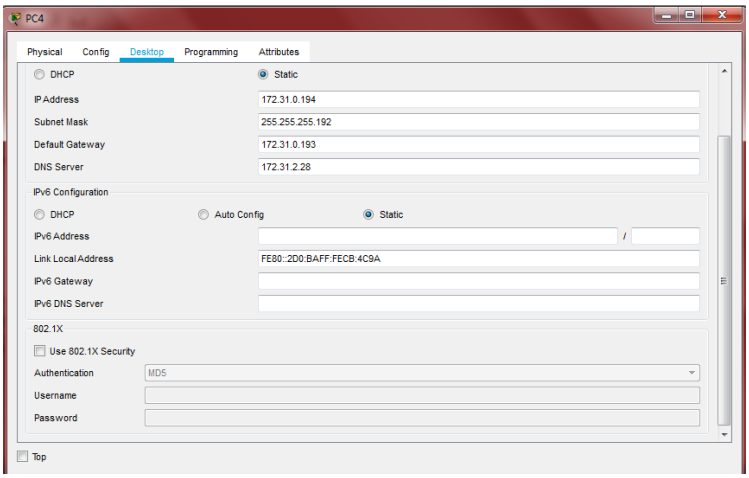


Figura 19 – Configuración Pc Tunja

- **Pc Cundinamarca**

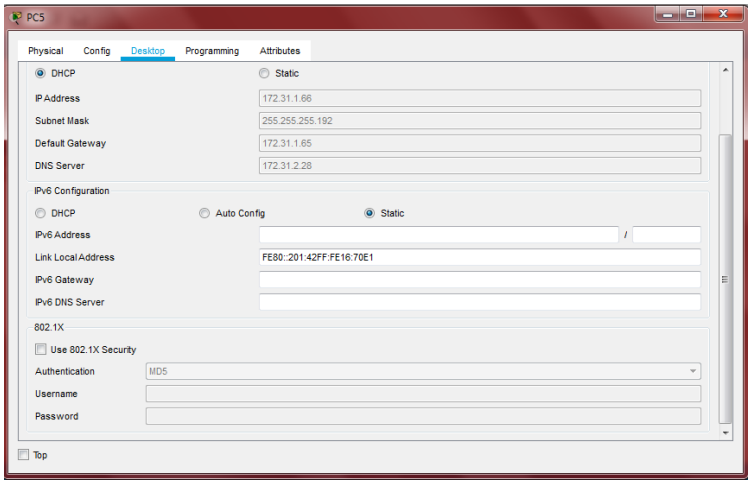


Figura 20 – Configuración Pc Cundinamarca

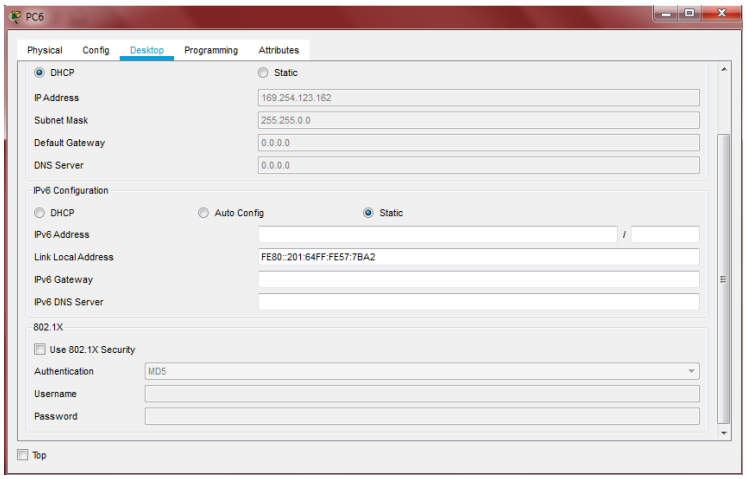


Figura 21 – Configuración Pc Cundinamarca

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

- **Tunja**

#ip nat inside source static 172.31.2.28 209.165.220.4

#access-list 1 permit 172.0.0.0 0.255.255.255

#ip nat inside source list 1 interface f0/1 overload

#int f0/1

#ip nat outside

#int f0/0.1

#ip nat inside

#int f0/0.20

#ip nat inside

#int f0/0.30

#ip nat inside

#int s0/0/0

#ip nat inside

#int s0/0/1

#ip nat inside

#exit

#ip route 0.0.0.0 0.0.0.0 209.165.220.3

#router ospf 1

#default-information originate

#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 209.165.220.3 to network 0.0.0.0
172.3.0.0/29 is subnetted, 1 subnets
C 172.3.2.8 is directly connected, FastEthernet0/0.1
172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks
O 172.31.0.0/26 [110/65] via 172.31.2.34, 00:24:49, Serial0/0/0
O 172.31.0.64/26 [110/65] via 172.31.2.34, 00:24:49, Serial0/0/0
C 172.31.0.128/26 is directly connected, FastEthernet0/0.20
C 172.31.0.192/26 is directly connected, FastEthernet0/0.30
O 172.31.1.0/26 [110/65] via 172.31.2.38, 00:23:33, Serial0/0/1
O 172.31.1.64/26 [110/65] via 172.31.2.38, 00:23:33, Serial0/0/1
O 172.31.2.0/29 [110/65] via 172.31.2.34, 00:24:49, Serial0/0/0
O 172.31.2.8/29 [110/65] via 172.31.2.38, 00:23:33, Serial0/0/1
O 172.31.2.24/29 [110/65] via 172.31.2.38, 00:23:33, Serial0/0/1
C 172.31.2.32/30 is directly connected, Serial0/0/0
C 172.31.2.36/30 is directly connected, Serial0/0/1
C 209.165.220.0/24 is directly connected, FastEthernet0/1
S* 0.0.0.0/0 [1/0] via 209.165.220.3

- **Bucaramanga**

#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 172.31.2.33 to network 0.0.0.0

172.3.0.0/29 is subnetted, 1 subnets

O 172.3.2.8 [110/65] via 172.31.2.33, 00:25:08, Serial0/0/0

172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks

C 172.31.0.0/26 is directly connected, FastEthernet0/0.10

C 172.31.0.64/26 is directly connected, FastEthernet0/0.30

O 172.31.0.128/26 [110/65] via 172.31.2.33, 00:25:08, Serial0/0/0

O 172.31.0.192/26 [110/65] via 172.31.2.33, 00:25:08, Serial0/0/0

O 172.31.1.0/26 [110/129] via 172.31.2.33, 00:23:42, Serial0/0/0

O 172.31.1.64/26 [110/129] via 172.31.2.33, 00:23:42, Serial0/0/0

C 172.31.2.0/29 is directly connected, FastEthernet0/0.1

O 172.31.2.8/29 [110/129] via 172.31.2.33, 00:23:42, Serial0/0/0

O 172.31.2.24/29 [110/129] via 172.31.2.33, 00:23:42, Serial0/0/0

C 172.31.2.32/30 is directly connected, Serial0/0/0

O 172.31.2.36/30 [110/128] via 172.31.2.33, 00:24:02, Serial0/0/0

O*E2 0.0.0.0/0 [110/1] via 172.31.2.33, 00:02:01, Serial0/0/0

- **Cundinamarca**

#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 172.31.2.37 to network 0.0.0.0

172.3.0.0/29 is subnetted, 1 subnets

O 172.3.2.8 [110/65] via 172.31.2.37, 00:24:15, Serial0/0/0

172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks

O 172.31.0.0/26 [110/129] via 172.31.2.37, 00:24:15, Serial0/0/0

O 172.31.0.64/26 [110/129] via 172.31.2.37, 00:24:15, Serial0/0/0

O 172.31.0.128/26 [110/65] via 172.31.2.37, 00:24:15, Serial0/0/0

O 172.31.0.192/26 [110/65] via 172.31.2.37, 00:24:15, Serial0/0/0

C 172.31.1.0/26 is directly connected, FastEthernet0/0.30

C 172.31.1.64/26 is directly connected, FastEthernet0/0.20

O 172.31.2.0/29 [110/129] via 172.31.2.37, 00:24:15, Serial0/0/0

C 172.31.2.8/29 is directly connected, FastEthernet0/0.1

C 172.31.2.24/29 is directly connected, FastEthernet0/0.88

O 172.31.2.32/30 [110/128] via 172.31.2.37, 00:24:15, Serial0/0/0

C 172.31.2.36/30 is directly connected, Serial0/0/0

O*E2 0.0.0.0/0 [110/1] via 172.31.2.37, 00:02:24, Serial0/0/0

- **Tunja**

#show ip nat translation

Pro Inside global Inside local Outside local Outside global

icmp 209.165.220.1:1 172.31.1.2:1 209.165.220.3:1 209.165.220.3:1

icmp 209.165.220.1:2 172.31.1.2:2 209.165.220.3:2 209.165.220.3:2

icmp 209.165.220.1:3 172.31.1.2:3 209.165.220.3:3 209.165.220.3:3

icmp 209.165.220.1:4 172.31.1.2:4 209.165.220.3:4 209.165.220.3:4

--- 209.165.220.4 172.31.2.28 --- ---

El enrutamiento deberá tener autenticación.

- **Bucaramanga**

#conf t

#int s0/0/0

#ip ospf authentication message-digest

#ip ospf message-digest-key 1 md5 cisco123

- **Cundinamarca**

#int s0/0/0

#ip ospf authentication message-digest

#ip ospf message-digest-key 1 md5 cisco123

- **Tunja**

#conf t

#int s0/0/0

#ip ospf authentication message-digest

#ip ospf message-digest-key 1 md5 cisco123

#int s0/0/1

#ip ospf authentication message-digest

#ip ospf message-digest-key 1 md5 cisco123

Listas de control de acceso:

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

- **CUNDINAMARCA**

#access-list 111 deny ip 172.31.1.64 0.0.0.63 209.165.220.0 0.0.0.255

#access-list 111 permit ip any any

#int f0/0.20

#ip access-group 111 in

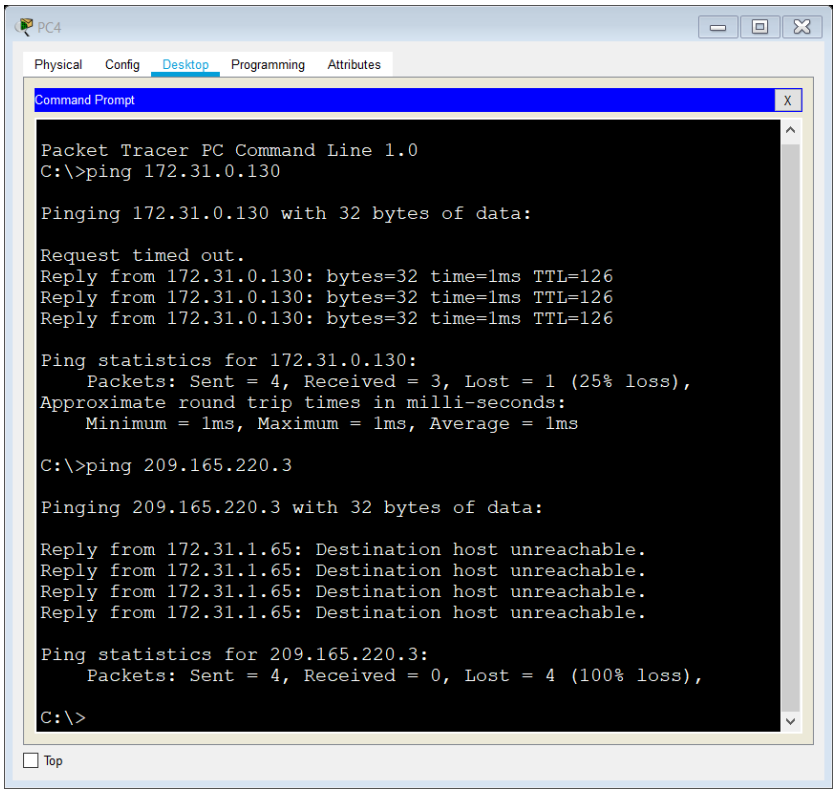


Figura 22 – Ping

Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.

- **Cundinamarca**

#access-list 112 permit ip 172.31.1.0 0.0.0.63 209.165.220.0 0.0.0.255

#access-list 112 deny ip any any

#int f0/0.30

#ip access-group 112 in

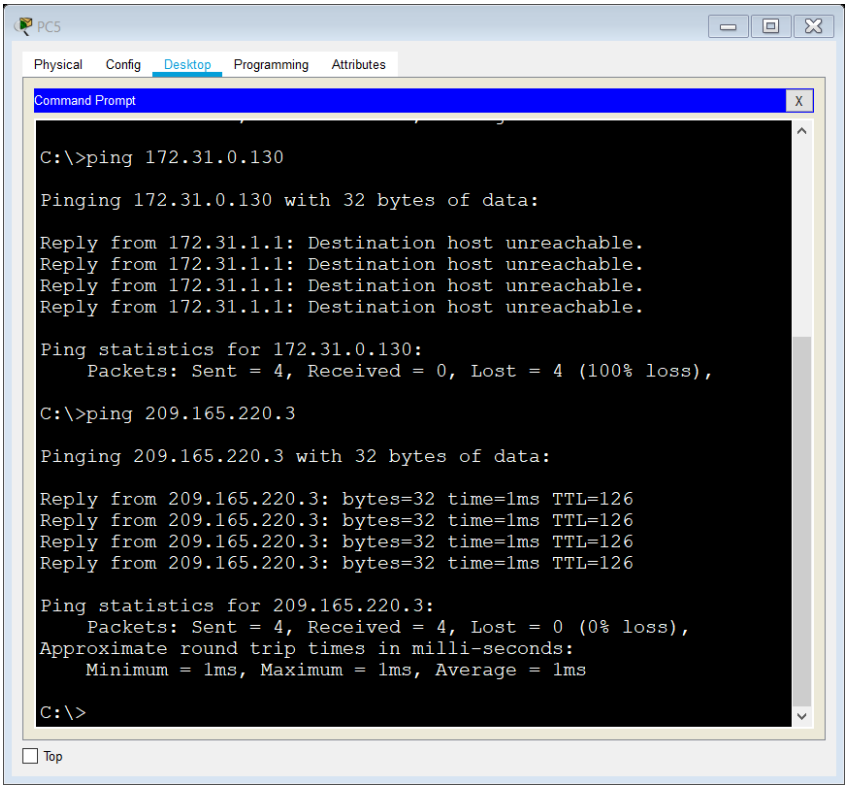


Figura 23 – Ping

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

- **Tunja**

#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 80

#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 21

#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 20

#int f0/0.30

#ip access-group 111 in

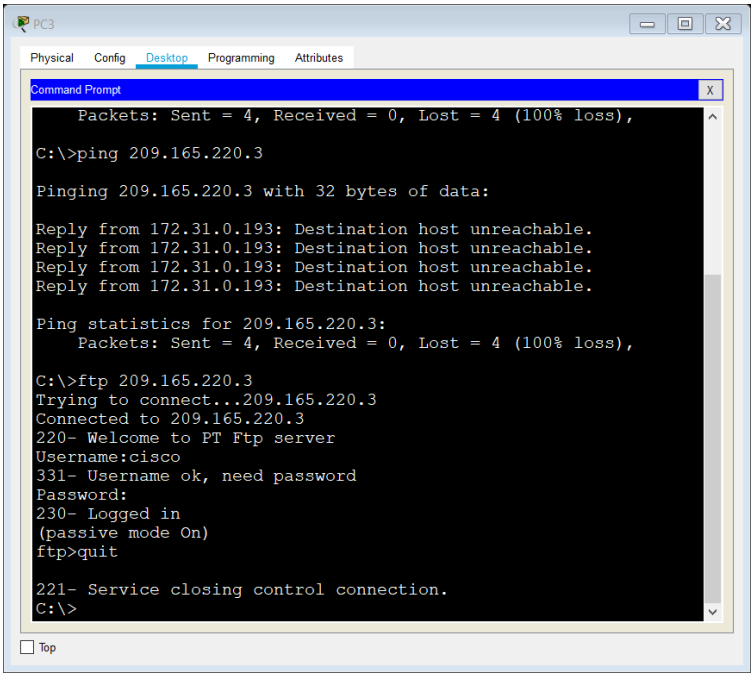


Figura 24 – Ping

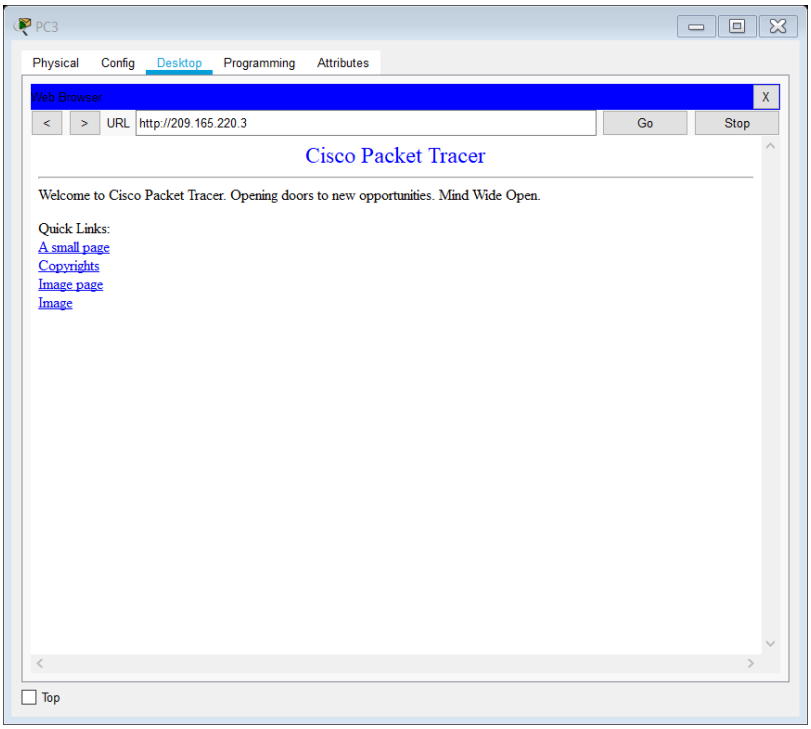


Figura 25 – Pagina Server

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

- **TUNJA**

#access-list 112 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63

#access-list 112 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63

#int f0/0.20

#ip access-group 112 in

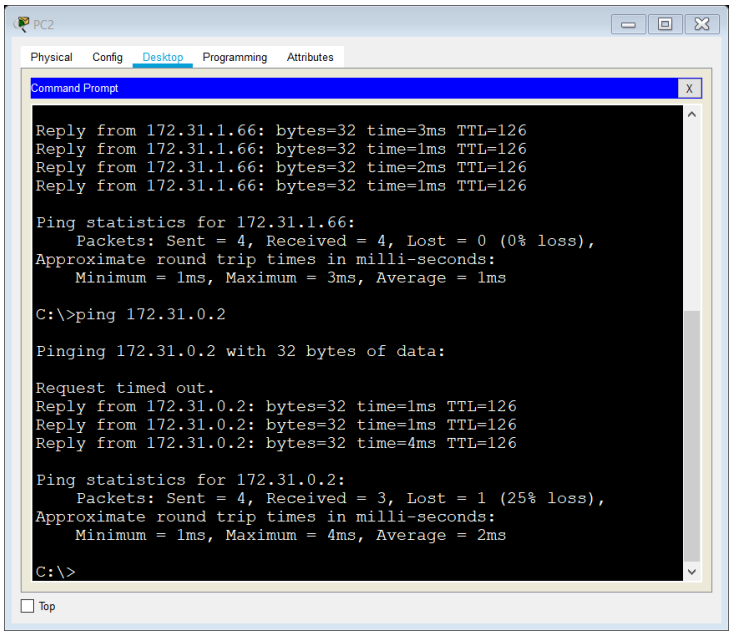


Figura 26 - Ping

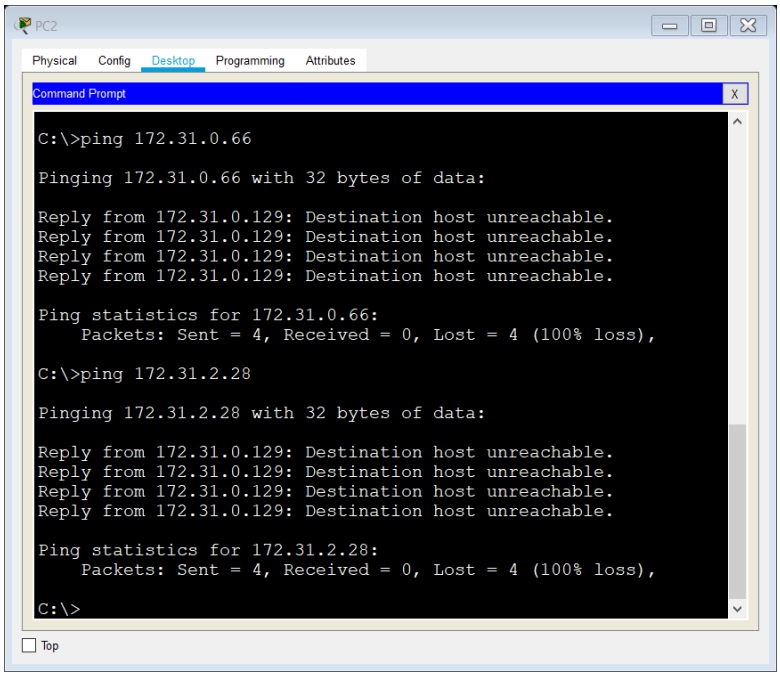


Figura 27 - Ping

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

- **Bucaramanga**

#access-list 111 permit ip 172.31.0.64 0.0.0.63 209.165.220.0 0.0.0.255

#int f0/0.30

#ip access-group 111 in

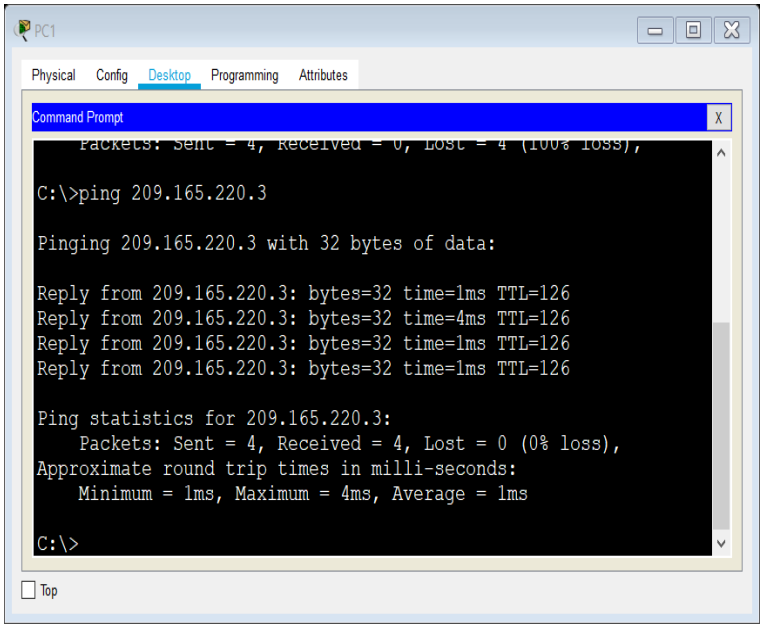


Figura 28 - Ping

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

- **Bucaramanga**

#access-list 112 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63

#access-list 112 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63

#int f0/0.10

#ip access-group 112 in

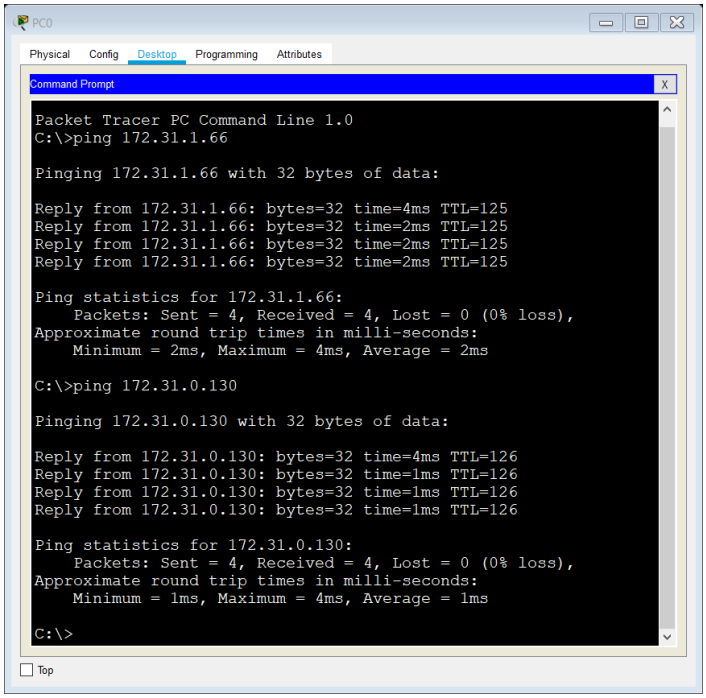


Figura 29 - ping

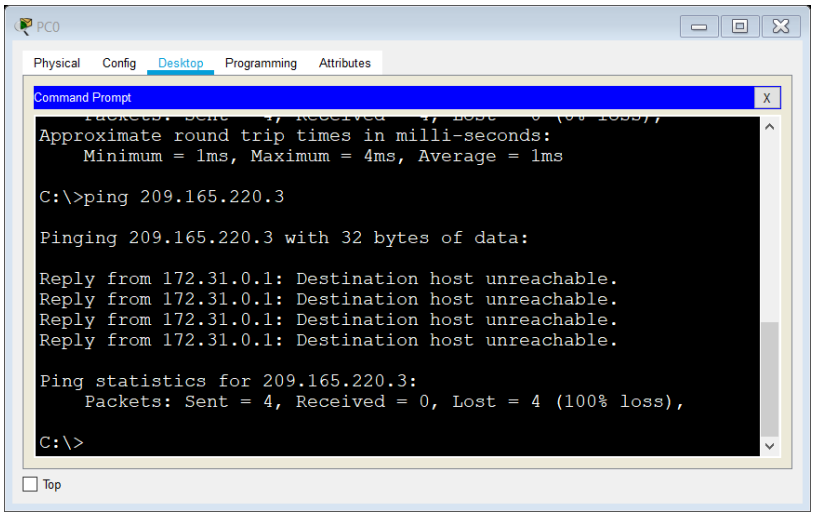


Figura 30 – Ping

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

- **Bucaramanga**

#access-list 113 deny ip 172.31.2.0 0.0.0.7 172.31.0.0 0.0.0.63

#access-list 113 deny ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.0.63

#access-list 113 permit ip any any

#int f0/0.10

#ip access-group 113 out

- **Tunja**

#access-list 113 deny ip 172.3.2.8 0.0.0.7 172.31.0.128 0.0.0.63

#access-list 113 deny ip 172.3.0.192 0.0.0.63 172.31.0.128 0.0.0.63

#access-list 113 permit ip any any

#int f0/0.20

#ip access-group 113 out

- **Cundinamarca**

#access-list 113 deny ip 172.31.2.8 0.0.0.7 172.31.1.64 0.0.0.63

#access-list 113 deny ip 172.31.1.0 0.0.0.63 172.31.1.64 0.0.0.63

#access-list 113 deny ip 172.31.2.24 0.0.0.7 172.31.1.64 0.0.0.63

#access-list 113 permit ip any any

#int f0/0.20

#ip access-group 113 out

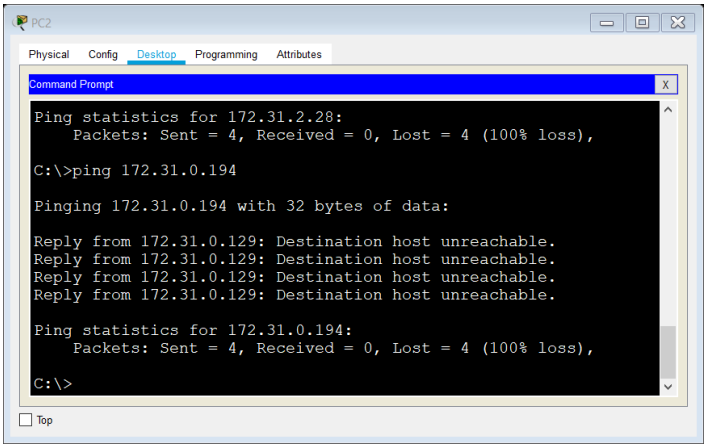


Figura 31 – Ping

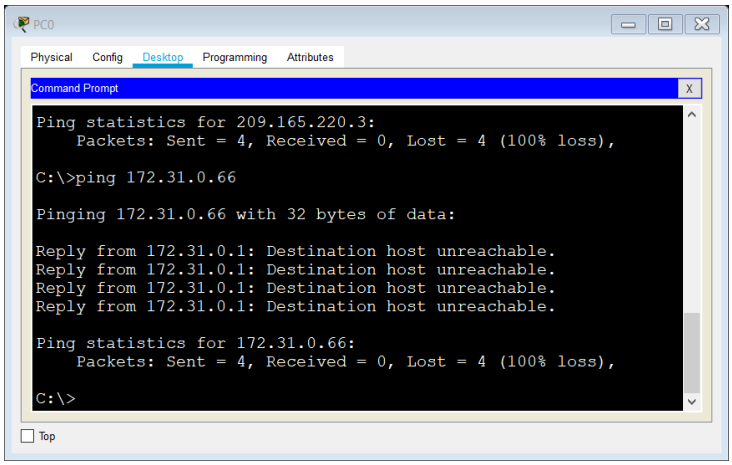


Figura 32 - Ping

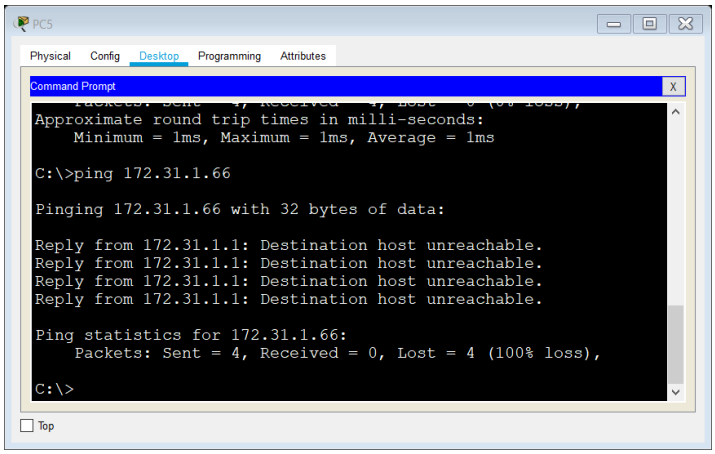


Figura 33 - Ping

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

- **Bucaramanga**

#access-list 3 permit 172.31.2.0 0.0.0.7

#access-list 3 permit 172.3.2.8 0.0.0.7

#access-list 3 permit 172.31.2.8 0.0.0.7

#line vty 0 15

#access-class 3 in

- **Tunja**

#access-list 3 permit 172.31.2.0 0.0.0.7

#access-list 3 permit 172.3.2.8 0.0.0.7

#access-list 3 permit 172.31.2.8 0.0.0.7

#line vty 0 15

#access-class 3 in

- **Cundinamarca**

#access-list 3 permit 172.31.2.0 0.0.0.7

#access-list 3 permit 172.3.2.8 0.0.0.7

#access-list 3 permit 172.31.2.8 0.0.0.7

#line vty 0 15

#access-class 3 in

CONCLUSIONES

Con el desarrollo de los escenarios propuestos se pudo colocar en práctica el conocimiento adquirido durante el diplomado de profundización CISCO, permitiendo al estudiante identificar sus habilidades que durante este fue adquiriendo para identificar las soluciones óptimas y adecuadas para la resolución de problemas reales.

El uso de una configuración adecuada y los equipos que se usen para el montaje de una red puede facilitar la comunicación de varias partes permitiendo que allá una estabilidad en las comunicaciones y así esto puede asegurar la integridad y la seguridad de los datos.

BIBLIOGRAFIA

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

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

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

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

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

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

Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3L74BZ3bpMiXRx0

Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de

http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf

Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de http://mr-telecomunicaciones.com/wp-content/uploads/2018/09/wendellodom.pdf

Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1Im3GQVfFFrjnEGFFU

CISCO. (2014). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1