EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

David Alfonso Vega Palacio

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA ESCUELA DE CIENCIAS BASICAS Y TECNOLOGÍAS 2019

EVALUACIÓN – PRUEBA DE HABILIDADES PRACTICAS CCNA

David Alfonso Vega Palacio

GRUPO 26

DIPLOMADO DE PROFUNDIZACIÓN CISCO
DISEÑO E IMPLEMENTACION DE SOLUCIONES INTEGRADAS LAN / WLAN

TUTOR
NILSON ALBEIRO FERREIRA MANZANARES

DIRECTOR
JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS Y TECNOLOGIAS
2019

Resumen

La importancia de las telecomunicaciones en el mundo moderno es tema vital para el desarrollo humano, es por ello que entender como fluye la información entre la sociedad y mas específicamente en las organizaciones es de vital importantica y reto para el ingeniero de sistemas.

Es por ello que entendiendo las líneas anteriores la Universidad Abierta y a Distancia UNAD en colaboración con CISCO Networking Academy, ha desarrollado el diplomado: "CISCO diseño e implementación de redes LAN-WAN", en donde permite desarrollar habilidades a través de sus modulos de aprendizajes contextos que se vera enfrentado el futuro egresado de la rama, como trabajo final se dispone de un trabajo practico que demuestran dichas habilidades adquiridas a lo largo del curso.

Abstract

The importance of telecommunications in the modern world is a vital issue for human development, which is why understanding how information flows between society and more specifically in organizations is vitally important and challenging for the systems engineer.

That is why, understanding the previous lines, UNAD Open and Distance University in collaboration with CISCO Networking Academy, has developed the diploma: "CISCO design and implementation of LAN-WAN networks", where it allows to develop skills through its modules of learning contexts that will face the future graduate of the branch, as a final work there is a practical work that demonstrates these acquired skills along the course.

Índice

Contenido

EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA 1
Abstract 4
Índice 5
Introducción 7
1. Escenario 1 8
1.1 Topologia de red en Packet Tracert 8
1.2 Tabla de configuracion basica en la red 9
1.3 Configuracion Inicial de dispositivos 9
1.4 Configuracion Interfaz y Seriales 12
1.5 Verificacion de tabla de enturnamientos en los routers 15
1.6 Verificacion balance de cargas en los routers 17
1.7 Verificacion de vecinos usando el comando cdp 18
1.8 Asignacion de enturnamiento EIGRP 20
1.9 Verificacion de vencindad EIGRP en los routers 21
1.10 Comprovacion en las tablas de enturnamientos 22
1.11 Diagnostico de comprobacion de puntos de la red 24
1.12 Configuración lists de control de Acceso 25
1.13 Comprobación de la red instalada. 28
2. Escenario 2 29
2.1 Comprobación de la red instalada. 29
2.1.1 Topología. 30
2.1.2 Router Bucaramanga 30
2.1.3 Router Bucaramanga Interfaces y seriales 31
2.1.4 Switch Bucaramanga 31
S1(config)#do write 31
2.1.5 Switch Bucaramanga Vlan 31
2.1.6 Router Tunja 32
2.1.7 Router Tunja Interfaces y seriales 33

2.1.7 Switch Tunja 33
2.1.8 Switch Tunja Vlan 34
2.1.9 Router Cundinamaca 34
2.1.10 Router Cundinamarca Interfaces y seriales 35
2.1.11 Switch Cundinamarca 35
2.1.12 Switch Cundinamarca Vlan 36
2.2 Servidor TFTP 37
2.3 Servicio DHCP en los routers 38
2.3.1 Router Bucaramanga 38
2.3.2 Router Cundinamarca 38
2.4 NAT 39
2.4 Enrutamiento autenticación 40
2.5 Listas de control de acceso: 41
Conclusiones 44
Bibliografía 45

Introducción

El presente trabajo académico es la demostración del aprendizaje practico adquirido a lo largo del diplomado “CISCO diseño e implementación de redes LAN-WAN” impartido por la Universidad abierta y a distancia UNAD, en donde se presentan dos escenarios hipotéticos para la aplicación practica de dichos conocimientos.

1. Escenario 1

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

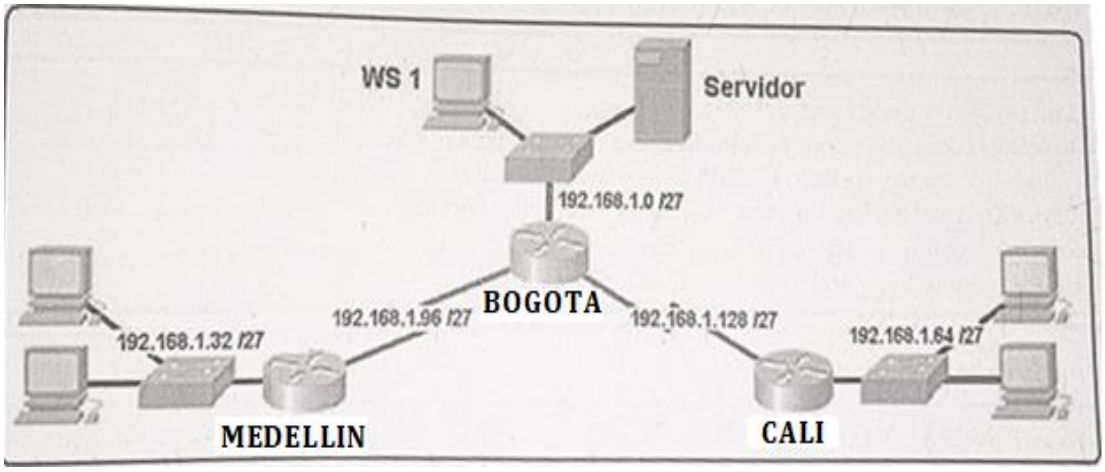

Figura 1. Imagen topología de red inicial

1.1 Topologia de red en Packet Tracert

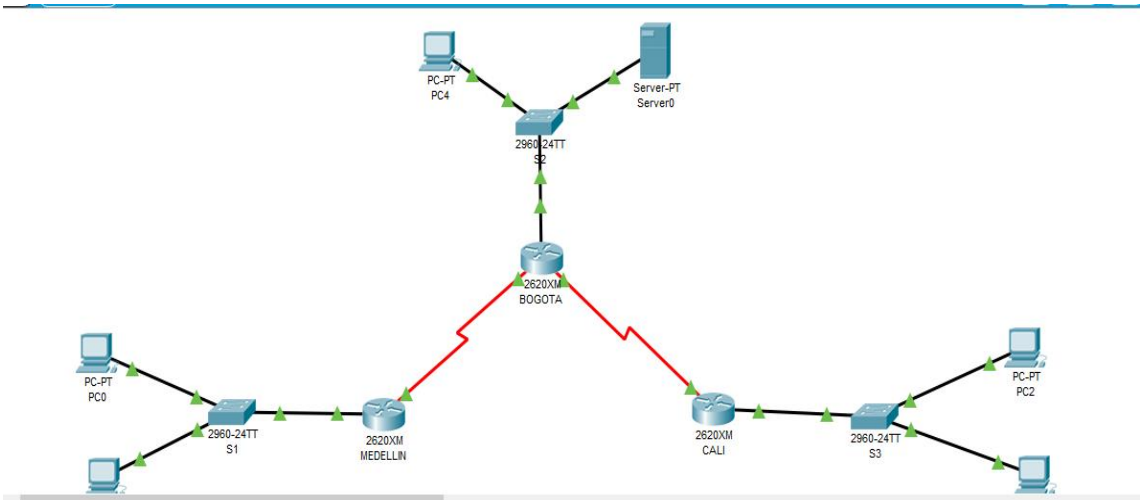

Figura 2. Imagen topología de red en packet tracert

1.2 Tabla de configuracion basica en la red

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

Tabla 1. Tabla de configuración de dispositivos

1.3 Configuracion Inicial de dispositivos

1.3.1 Router Bogota

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#no ip domain-lookup
Router(config)#hostname BOGOTA
BOGOTA(config)#enable secret cisco
BOGOTA(config)#line console 0
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#line vty 0 4
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#service password-encryption
BOGOTA(config)#banner motd #Acceso denegado#
BOGOTA(config)#exit
BOGOTA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

1.3.2 Router Medellín

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname MEDELLIN
MEDELLIN(config)#enable secret cisco
MEDELLIN(config)#line console 0
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
MEDELLIN(config)#line vty 0 4
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
MEDELLIN(config)#service password-encryption
MEDELLIN(config)#banner motd #Acceso denegado#
MEDELLIN(config)#exit
MEDELLIN#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

1.3.3 Router Cali

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname CALI
CALI(config)#enable secret cisco
CALI(config)#line console 0
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#exit
CALI(config)#line vty 0 15
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#exit
CALI(config)#service password-encryption
CALI(config)#banner motd #Acceso no autorizado#
CALI(config)#exit
CALI#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

1.3.4 Switch S1

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret cisco
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd #Acceso denegado#
S1(config)#exit
S1#copy running-config startup-config
Destination filename [startup-config]?
    Building configuration...
```

1.3.5 Switch S2

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#enable secret cisco
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#line vty 0 4
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#service password-encryption
S2(config)#banner motd #Acceso no autorizado#
S2(config)#exit
S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

1.3.6 Switch S3

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#enable secret cisco
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#service password-encryption
S3(config)#banner motd #Acceso no autorizado#
S3(config)#exit
S3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

1.4 Configuracion Interfaz y Seriales

Se realiza configuracion de las interfaces y seriales según tabla dispuesto en el esenario 1.

1.4.1 Router Medellín

```
Acceso denegado
User Access Verification
Password:
MEDELLIN>enable
Password:
MEDELLIN#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#interface fastethernet 0/0
MEDELLIN(config-if)#
MEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.224
MEDELLIN(config-if)#no shutdown
MEDELLIN(config-if)#
```

```
MEDELLIN(config-if)#exit
MEDELLIN(config)#interface serial 0/0
MEDELLIN(config-if)#ip address 192.168.1.99 255.255.255.224
MEDELLIN(config-if)#no shutdown
MEDELLIN(config-if)#
MEDELLIN(config-if)#exit
MEDELLIN(config)#ip route 192.168.1.0 255.255.255.224 192.168.1.97
MEDELLIN(config)#ip route 192.168.1.64 255.255.255.224 192.168.1.97
MEDELLIN(config)#exit
MEDELLIN#copy running-config startup-config
```

1.4.2 Router Bogotá

```
Acceso denegado
User Access Verification
Password:
BOGOTA>enable
Password:
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
BOGOTA(config-if)#
BOGOTA(config-if)#exit
BOGOTA(config)#interface serial 0/0
BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#exit
BOGOTA(config)#interface serial 0/1
BOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#exit
BOGOTA(config)#ip route 192.168.1.64 255.255.255.224 192.168.1.131
BOGOTA(config)#ip route 192.168.1.32 255.255.255.224 192.168.1.99
BOGOTA(config)#exit
BOGOTA#copy running-config startup-config
```

1.4.3 Router Cali

```
Acceso no autorizado
User Access Verification
Password:
CALI>enable
Password:
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
CALI(config-if)#exit
CALI(config)#interface serial 0/0
CALI(config-if)#ip address 192.168.1.131 255.255.255.224
CALI(config-if)#no shutdown
CALI(config-if)#exit
CALI(config)#
CALI(config)#ip route 192.168.1.0 255.255.255.224 192.168.1.129
CALI(config)#ip route 192.168.1.32 255.255.255.224 192.168.1.129
CALI(config)#exit
CALI#copy running-config startup-config
```

1.5 Verificacion de tabla de enturnamientos en los routers

Se procede a la verificacion de los routers en su tabla de enturnamiento

1.5.1 Router Medellín

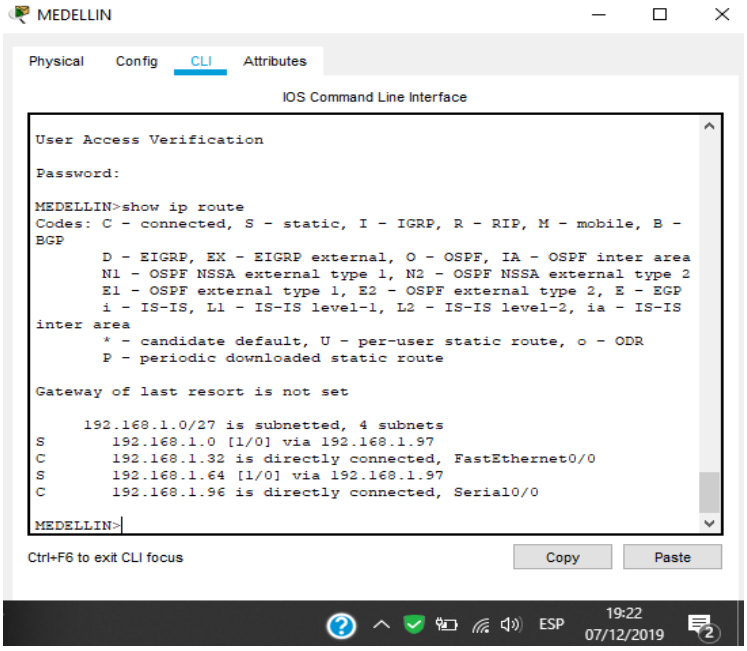

Figura 3. Imagen router Medellín

1.5.2 Router Bogotá

Figura 4. Imagen router Bogotá

1.5.3 Router Cali

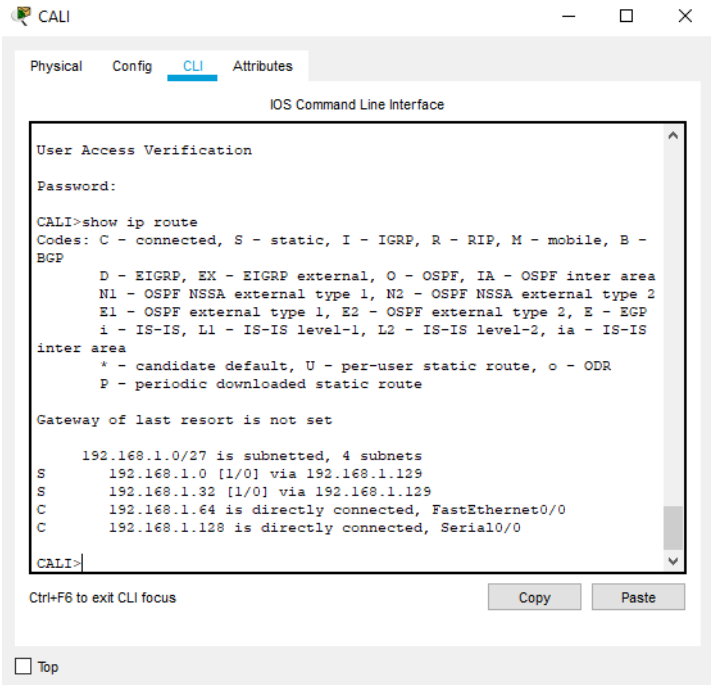

Figura 5. Imagen router Cali

1.6 Verificacion balance de cargas en los routers

El balance de carga se designa mediante el comando ip route, y es dado para los routers que tienen dos seriales conectados.

1.6.1 Router Medellin

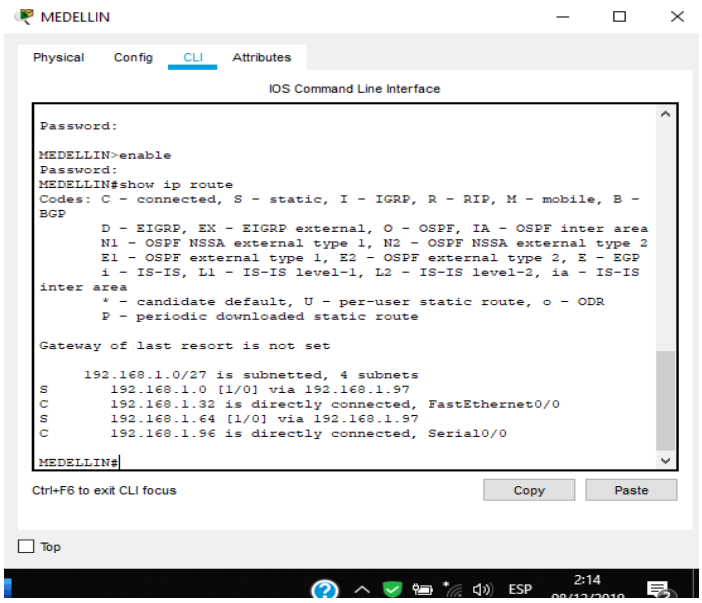

Figura 6. Imagen router Medellin

1.6.2 Router Bogotá

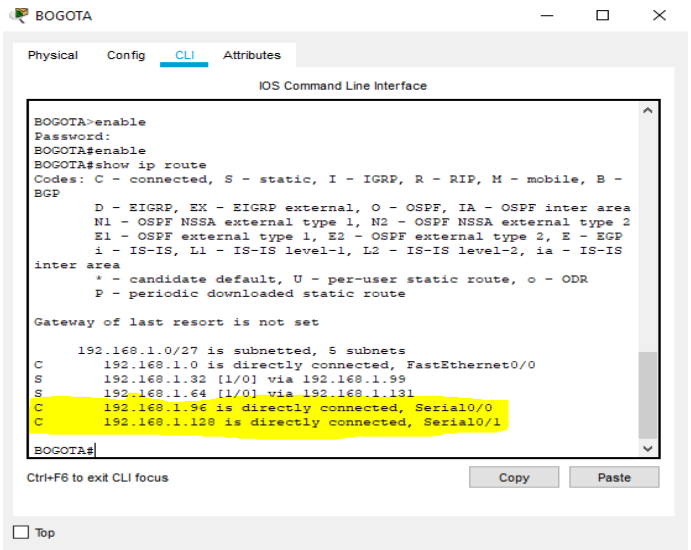

Figura 6. Imagen router Bogotá

1.6.3 Router Cali

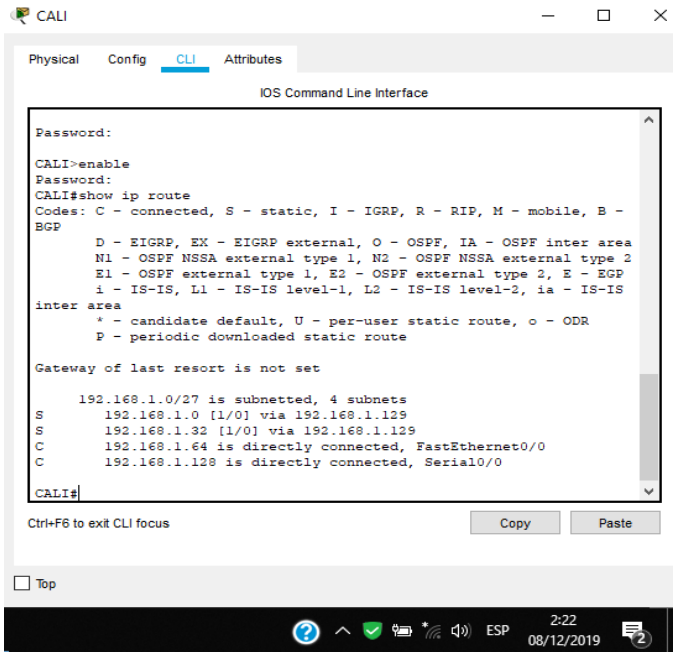

Figura 7. Imagen router Cali

1.7 Verificacion de vecinos usando el comando cdp

La verificacion de vecinos se utiliza bajo el comando show cdp neighbors, en cada uno de los routers

1.7.1 Router Medellín

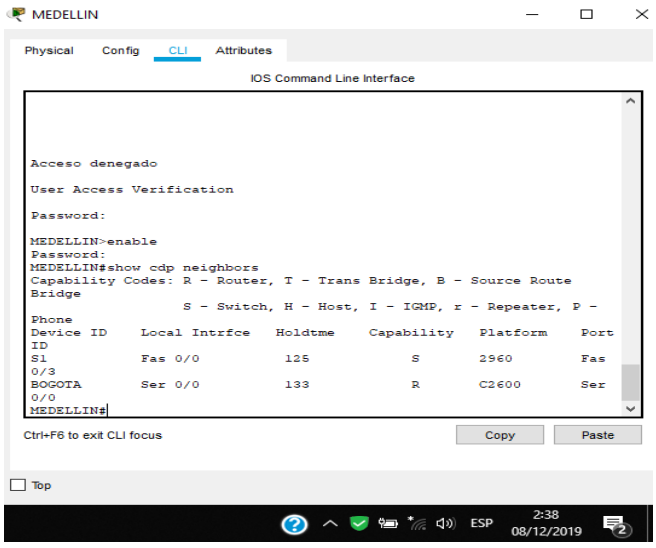

Figura 7. Imagen router Medellin

1.7.2 Router Bogotá

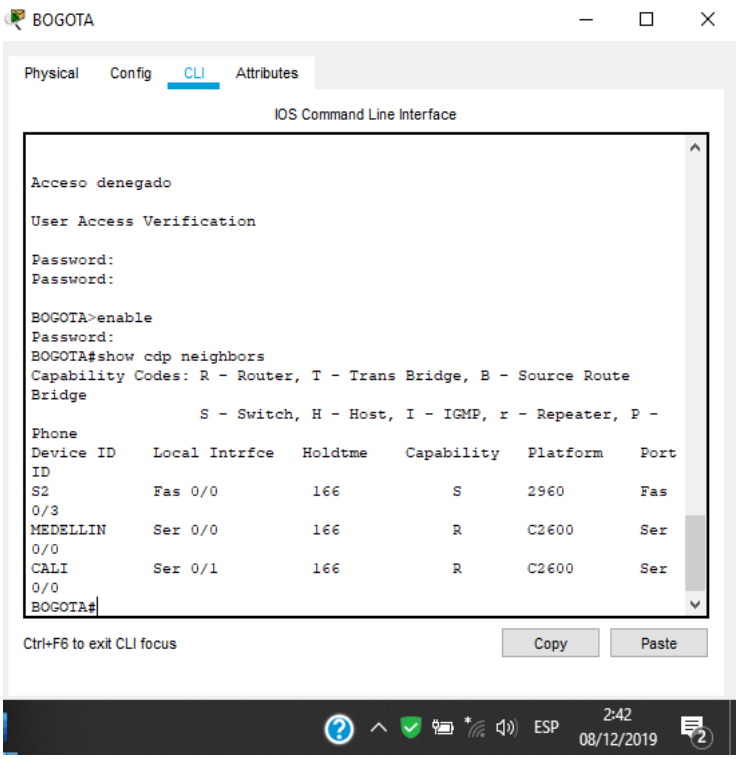

Figura 8. Imagen router Bogotá

1.7.3 Router Cali

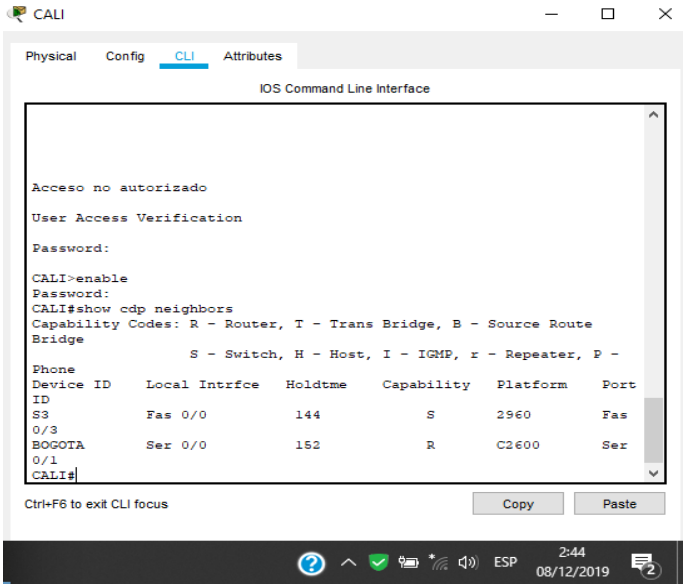

Figura 9. Imagen router Cali

1.8 Asignacion de enturnamiento EIGRP

Se realiza la asignacion de enturnamiento EIGRP a los routers considerando el direccionamiento diseñado.

1.8.1 Router Medellin

```
MEDELLIN>enable
MEDELLIN#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#router eigrp 10
MEDELLIN(config-router)#network 192.168.1.96 0.0.0.31
MEDELLIN(config-router)#network 192.168.1.32 0.0.0.31
MEDELLIN(config-router)#network 192.168.1.128 0.0.0.31
MEDELLIN(config-router)#
```

1.8.2 Router Bogotá

```
BOGOTA>enable
Password:
BOGOTA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#router eigrp 10
BOGOTA(config-router)#network 192.168.1.0 0.0.0.31
BOGOTA(config-router)#network 192.168.1.96 0.0.0.31
BOGOTA(config-router)#
BOGOTA(config-router)#network 192.168.1.128 0.0.0.31
BOGOTA(config-router)#no auto-summary
BOGOTA(config-router)#exit
```

1.8.3 Router Cali

```
CALI>enable
CALI#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#router eigrp 10
CALI(config-router)#network 192.168.1.128 0.0.0.31
CALI(config-router)#network 192.168.1.64 0.0.0.31
CALI(config-router)#no auto-summary
CALI(config-router)#exit
```

1.9 Verificacion de vencindad EIGRP en los routers

Se realiza la verificacion de vencidad dada por los comandos show ip eigrp neighbors y show ip eigrp topology

1.9.1 Router Medellin

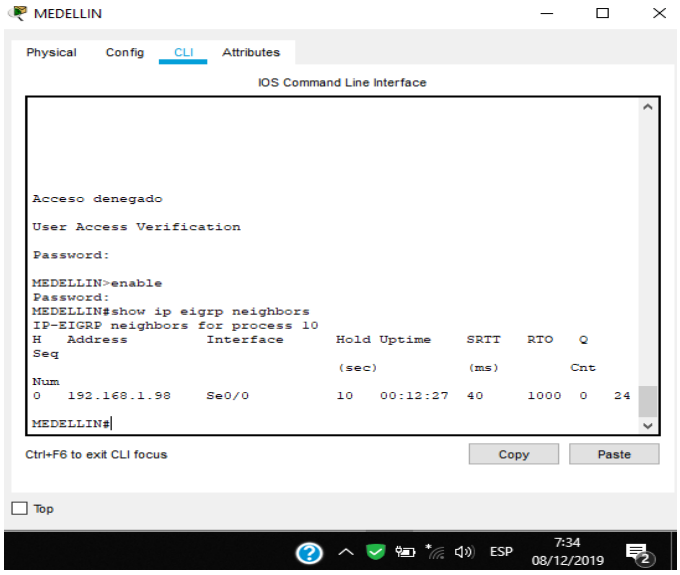

Figura 10. Imagen router Medellin

1.9.2 Router Bogotá

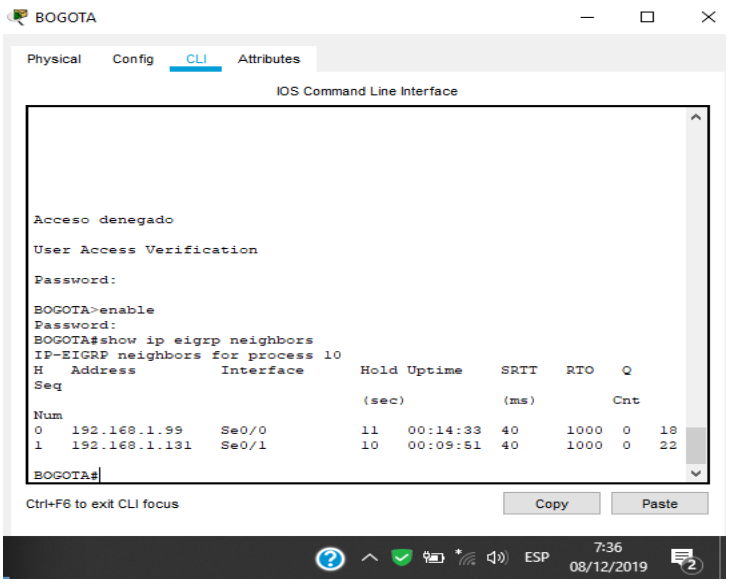

Figura 11. Imagen router Bogotá

1.9.3 Router Cali

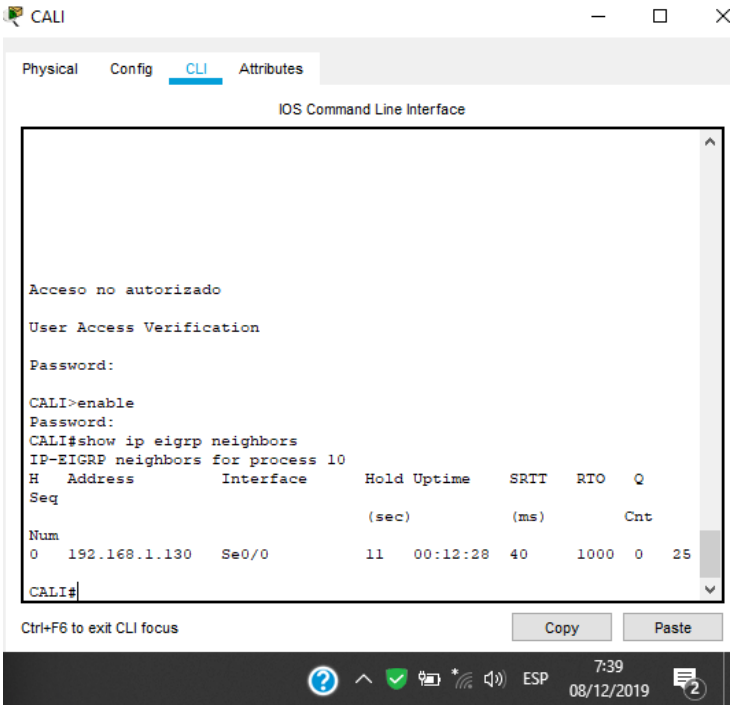

Figura 12. Imagen router Cali

1.10 Comprovacion en las tablas de enturnamientos

Se comprueba mendiante el comando show ip route

1.10.1 Router Medellin

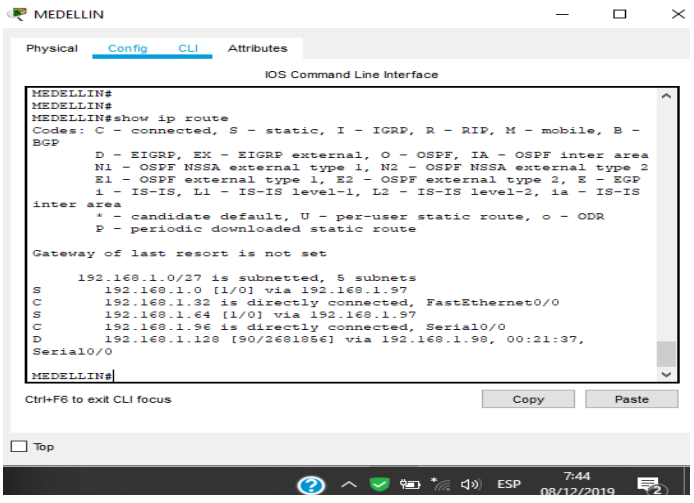

Figura 13. Imagen router Medellin

1.10.2 Router Bogotá

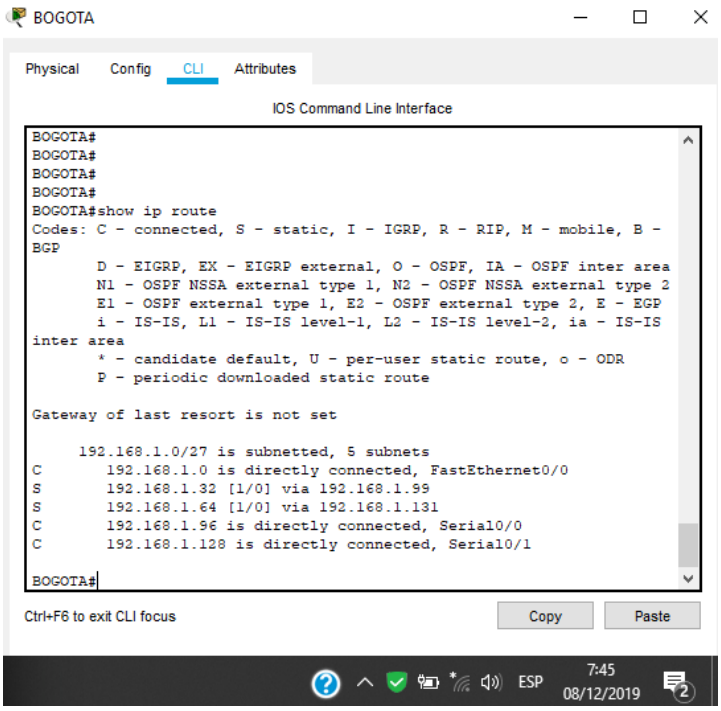

Figura 14. Imagen router Bogotá

1.10.3 Router Cali

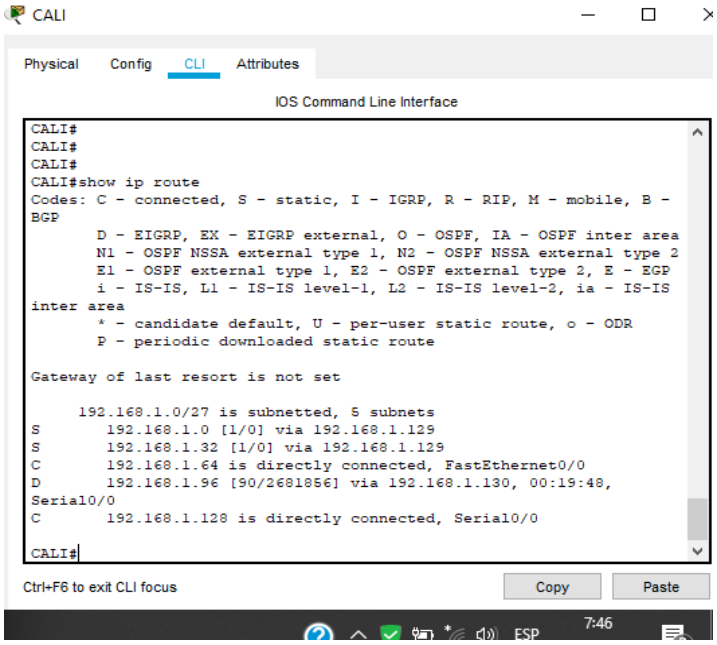

Figura 15. Imagen router Cali

1.11 Diagnostico de comprobacion de puntos de la red

Se realiza comprovacion de diagnostico mediante el comando ping para verificar los puntos de red del esenario.

1.11.1 Host lan Cali a router Medellin

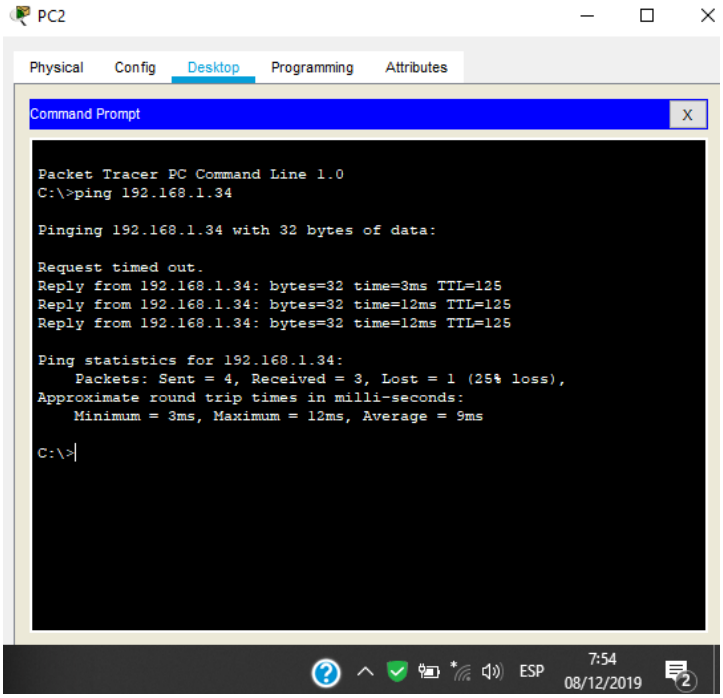

Figura 16. Imagen ping lan cali router medellin

1.11.2 Host lan Cali a Servidor

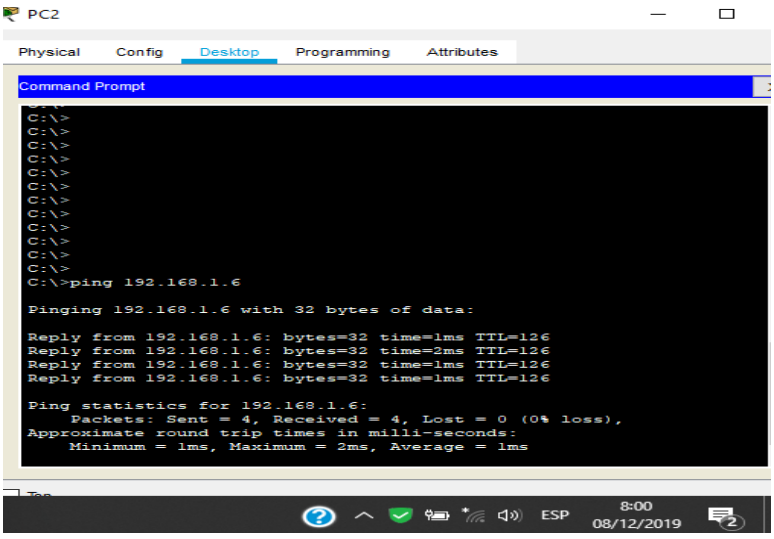

Figura 16. Imagen ping host lan cali a servidor

1.12 Configuración lists 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:

Configuración de habilitación para establecer conexiones Telnet.

En la configuracion inicial de cada routes se establecio la configuracion necesaria para la habilitacion de la conexiónes Telnet.

1.12.1 Router Medellín

```
MEDELLIN(config)#line vty 0 4
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
```

1.12.2 Router Bogotá

```
BOGOTA(config)#line vty 0 4
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
```

1.12.3 Router Cali

```
CALI(config)#line vty 0 15
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#exit
```

1.12.4 Conexión Telnet entre routers Medellin-Bogota

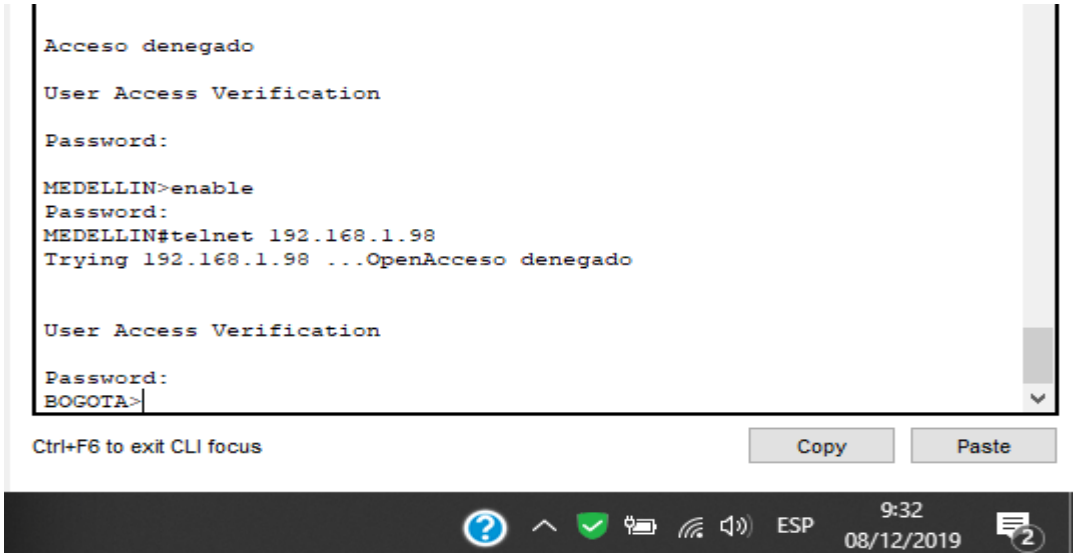

Figura 17. Imagen router Medellin

1.12.5 Conexión Telnet entre routers Cali-Bogota

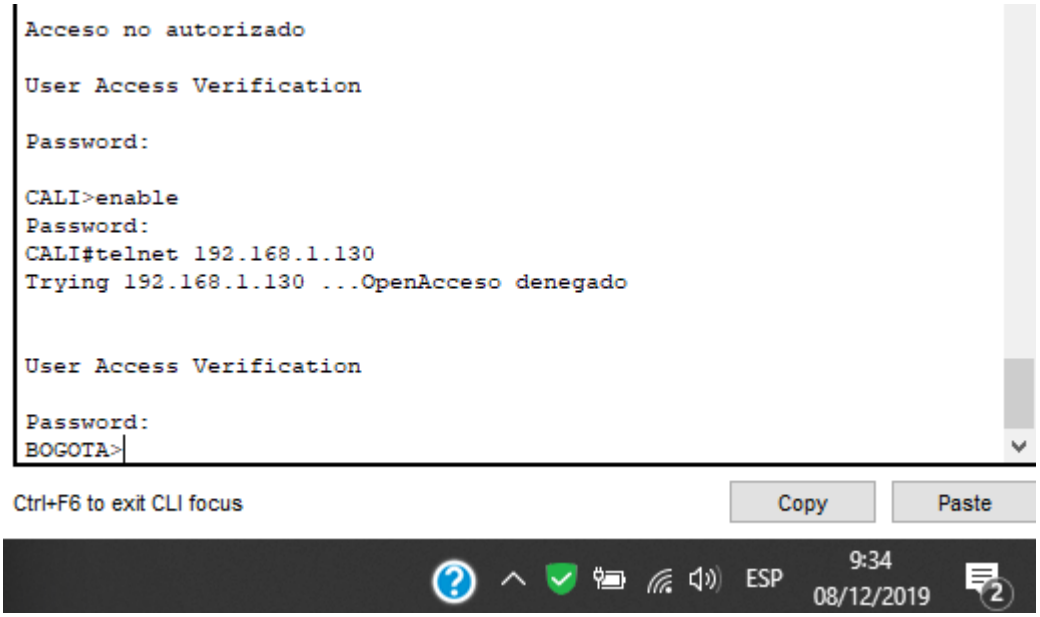

Figura 18. Imagen router Cali

1.12.6 Conexión Telnet entre routers Bogota- Medellin/Cali

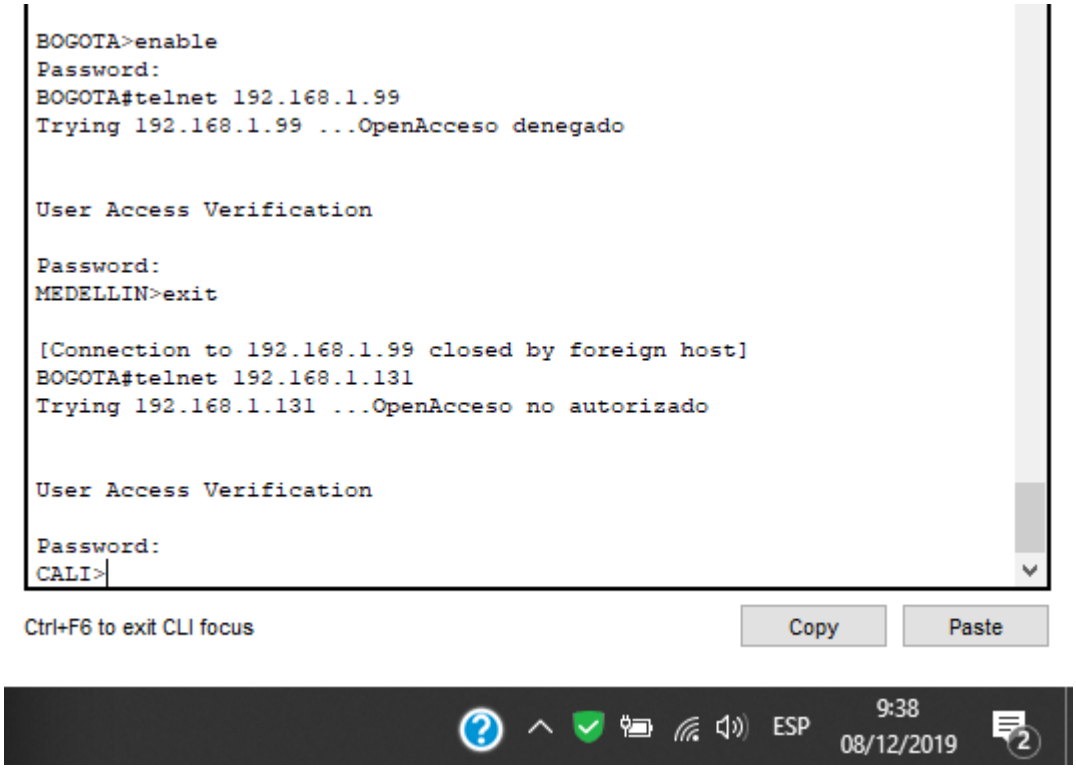

Figura 19. Imagen router Medellin

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.

BOGOTA(config)#access-list 1 permit 192.168.1.6 0.0.0.224
BOGOTA(config)#access-list 1 deny any
BOGOTA(config)#int se0/0
BOGOTA(config-if)#ip access-group 1 out
BOGOTA(config-if)#exit
BOGOTA(config)#int se0/1
BOGOTA(config-if)#ip access-group 1 out
BOGOTA(config-if)#exit

a. 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.

```
MEDELLIN#conf t
MEDELLIN(config)#access-list 111 permit ip 192.168.1.32 0.0.0.31 host
192.168.1.6
MEDELLIN(config)#int fa0/0
MEDELLIN(config-if)#ip access-group 111 in
MEDELLIN(config-if)#exit
MEDELLIN(config)#
```

```
CALI(config)#access-list 111 permit ip 192.168.1.64 0.0.0.31 host 192.168.1.6
CALI(config)#int fa0/0
CALI(config-if)#ip access-group 111 in
CALI(config-if)#exit
CALI(config)#
```

1.13 Comprobación de la red instalada.

a. Se debe probar que la configuración de las listas de acceso fue exitosa.
b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	Exitoso
	WS_1	Router BOGOTA	Falla
	Servidor	Router CALI	Exitoso
	Servidor	Router MEDELLIN	Exitoso
TELNET	AN del Router MEDELLIN	Router CALI	Exitoso
	LAN del Router CALI	Router CALI	Exitoso
	AN del Router MEDELLIN	Router MEDELLIN	Exitoso
	LAN del Router CALI	Router MEDELLIN	Exitoso
PING	LAN del Router CALI	WS_1	Falla
	AN del Router MEDELLIN	WS_1	Falla
	AN del Router MEDELLIN	LAN del Router CALI	Falla
PING	LAN del Router CALI	Servidor	Exitoso
	AN del Router MEDELLIN	Servidor	Exitoso
	Servidor	AN del Router MEDELLIN	Exitoso
	Servidor	LAN del Router CALI	Exitoso
	Router CALI	AN del Router MEDELLIN	Falla
	Router MEDELLIN	LAN del Router CALI	Falla

2. Escenario 2

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

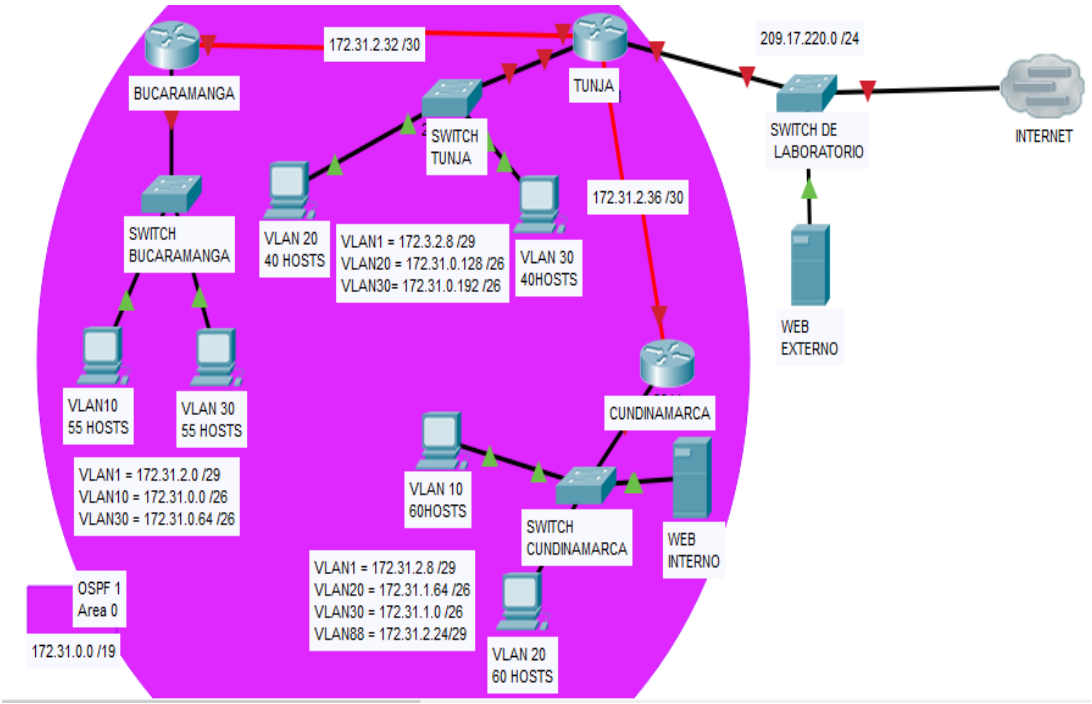

Figura 20. Imagen esquema escenario 2

2.1 Comprobación de la red instalada.

Los siguientes son los requerimientos necesarios:

Todos los routers deberán tener los siguiente:

- Configuración básica.
- Autenticación local con AAA.
- Cifrado de contraseñas.
- Un máximo de internos para acceder al router.
- Máximo tiempo de acceso al detectar ataques.

2.1.1 Topología.

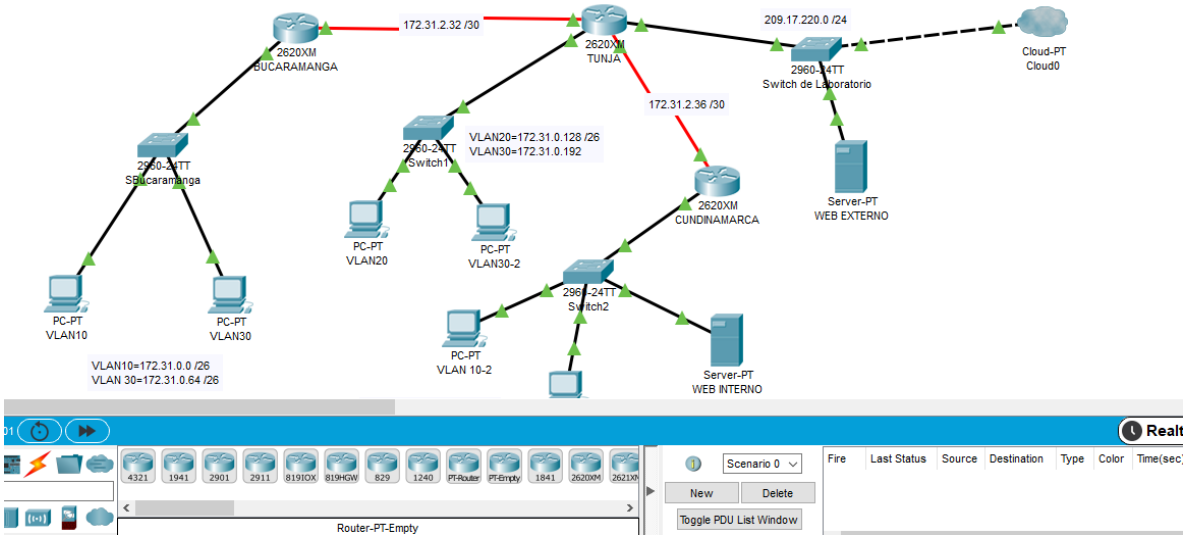

Figura 21. Imagen topología

2.1.2 Router Bucaramanga

```
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)#aaa authentication login local enable
BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#aaa authentication login AUTH local
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#login authentication AUTH
BUCARAMANGA(config-line)#line vty 0 15
BUCARAMANGA(config-line)#login authentication AUTH
BUCARAMANGA(config)#username cisco secret cisco
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#service password-encryption
BUCARAMANGA(config)#exit
BUCARAMANGA#copy running-config startup-config
```

2.1.3 Router Bucaramanga Interfaces y seriales

```
BUCARAMANGA(config)#interface fastEthernet 0/0
BUCARAMANGA(config-if)#no shutdown
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#int se0/0
BUCARAMANGA(config-if)#ip add 172.31.2.33 255.255.255.252
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#ip route 172.31.0.192 255.255.255.192 172.31.2.34
BUCARAMANGA(config)#ip route 172.31.0.128 255.255.255.192 172.31.2.34
BUCARAMANGA(config)#ip route 172.31.2.8 255.255.255.248 172.31.2.34
BUCARAMANGA(config)#ip route 172.31.1.64 255.255.255.192 172.31.2.34
```

2.1.4 Switch Bucaramanga

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret cisco
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#no ip domain-lookup
S1(config)#do write
```

2.1.5 Switch Bucaramanga Vlan

```
S1(config)#vlan ?
S1(config)#vlan 10
S1(config-vlan)#vlan 30
S1(config-vlan)#exit
S1(config)#interface vlan10
S1(config)#interface vlan30
S1(config)#interface fa0/1
S1(config-if)#switchport mode access
```

```
S1(config-if)#switchport access vlan 10
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#interface fa0/2
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30


S1(config-if)#no shutdown
S1(config-if)#do write
S1(config)#int fa0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
```

2.1.6 Router Tunja

```
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)#aaa authentication login local enable
TUNJA(config)#aaa new-model
TUNJA(config)#aaa authentication login AUTH local
TUNJA(config)#line console 0
TUNJA(config-line)#login authentication AUTH
TUNJA(config-line)#line vty 0 15
TUNJA(config-line)#login authentication AUTH
TUNJA(config-line)#username cisco secret cisco
TUNJA(config-line)#exit
TUNJA(config)#service password-encryption
TUNJA(config)#exit
TUNJA#copy running-config startup-config
```

2.1.7 Router Tunja Interfaces y seriales

```
TUNJA(config)#interface serial 0/0
TUNJA(config-if)#ip address 172.31.2.34 255.255.255.252
TUNJA(config-if)#Ip ospf message-digest-key 1 md5 7 network
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#no shutdown
TUNJA(config-if)#exit

TUNJA(config)#int fa0/0
TUNJA(config-if)#no shutdown
TUNJA(config-if)#exit

TUNJA(config)#int se0/1
TUNJA(config-if)#ip add 172.31.2.37 255.255.255.252
TUNJA(config-if)#no shutdown
TUNJA(config-if)#exit


TUNJA(config)#ip route 172.31.0.64 255.255.255.192 172.31.2.33
TUNJA(config)#ip route 172.31.0.0 255.255.255.192 172.31.2.33
TUNJA(config)#ip route 172.31.2.8 255.255.255.248 172.31.2.38
TUNJA(config)#ip route 172.31.1.64 255.255.255.192 172.31.2.38
TUNJA(config)#ip route 172.31.2.24 255.255.255.248 172.31.2.38
```

2.1.7 Switch Tunja

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#enable secret cisco
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#line vty 0 15
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#service password-encryption
S2(config)#no ip domain-lookup
```

S2(config)#do write

2.1.8 Switch Tunja Vlan

S2(config)#vlan 20
S2(config-vlan)#vlan 30
S2(config-vlan)#exit
S2(config)#interface vlan 20
S2(config-if)#interface vlan 30
S2(config-if)#interface fa0/01
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 20
S2(config-if)#no shutdown
S2(config-if)#exit
S2(config)#interface fa0/2
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 30
S2(config-if)#no shutdown
S2(config-if)#do write

S2(config)#int fa0/3
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 1

2.1.9 Router Cundinamaca

Router>enable
Router#configure terminal
Router(config)#hostname CUNDINAMARCA
CUNDINAMARCA(config)#no ip domain-lookup
CUNDINAMARCA(config)#aaa authentication login local enable

CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#aaa authentication login AUTH local
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#login authentication AUTH
CUNDINAMARCA(config-line)#line vty 0 15
CUNDINAMARCA(config-line)#login authentication AUTH
CUNDINAMARCA(config-line)#username cisco secret cisco
CUNDINAMARCA(config)#service password-encryption
CUNDINAMARCA(config)#exit

```
CUNDINAMARCA#copy running-config startup-config
```

2.1.10 Router Cundinamarca Interfaces y seriales

```
CUNDINAMARCA(config)#int se0/0
CUNDINAMARCA(config-if)#ip add 172.31.2.38 255.255.255.252
CUNDINAMARCA(config-if)#no shutdown
CUNDINAMARCA(config-line)#exit


CUNDINAMARCA(config)#int fa0/0
CUNDINAMARCA(config-if)#no shutdown
CUNDINAMARCA(config-line)#exit

CUNDINAMARCA(config)#ip route 172.31.0.128 255.255.255.192 172.31.2.37
CUNDINAMARCA(config)#ip route 172.31.0.192 255.255.255.192 172.31.2.37
CUNDINAMARCA(config)#ip route 172.31.0.0 255.255.255.192 172.31.2.37
CUNDINAMARCA(config)#ip route 172.31.0.64 255.255.255.192 172.31.2.37
```

2.1.11 Switch Cundinamarca

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname S3
S3(config)#enable secret cisco
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#no ip domain-lookup
S3(config)#do write
```

2.1.12 Switch Cundinamarca Vlan

```
S3#enable
S3#configure terminal
S3(config)#vlan 10
S3(config-vlan)#exit
S3(config)#vlan 20
S3(config-vlan)#exit
S3(config)#vlan 88
S3(config-vlan)#exit
S3(config)#int vlan 10
S3(config-if)#int vlan 20
S3(config)#int vlan88

S3(config-if)#int fa0/1
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 10
S3(config-if)#no shutdown
S3(config-if)#exit

S3(config)# int fa0/2
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 20
S3(config-if)#no shutdown
S3(config-if)#exit

S3(config)#int fa0/3
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 88
S3(config-if)#no shutdown
S3(config-if)#exit

S3(config)#int fa0/4
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#exit
S3(config)#do write
```

2.2 Servidor TFTP

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

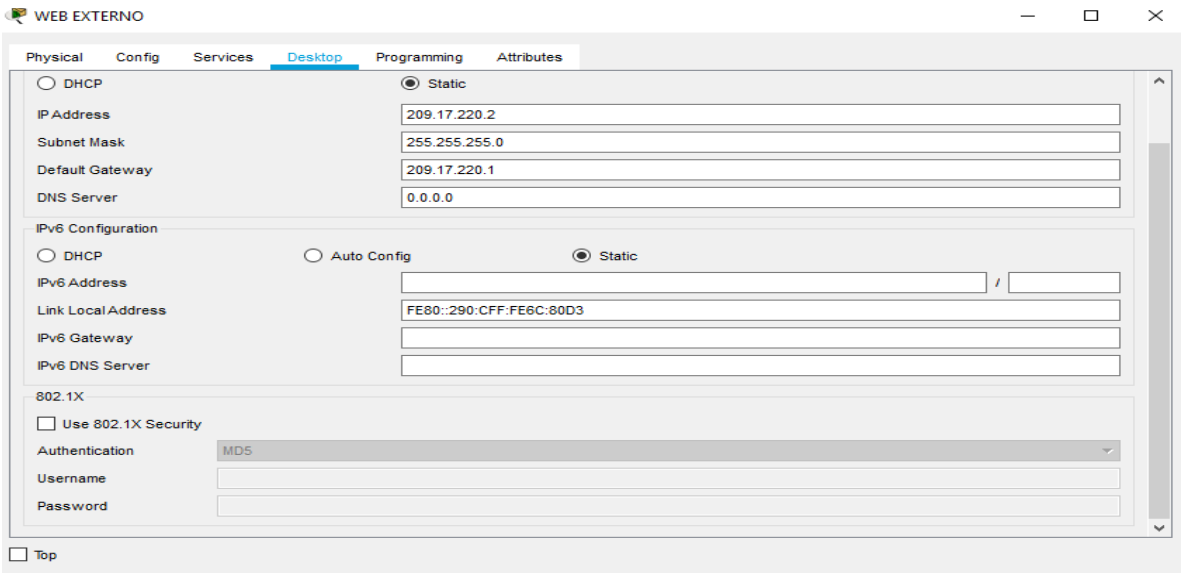

Figura 22. Imagen servidor TFTP

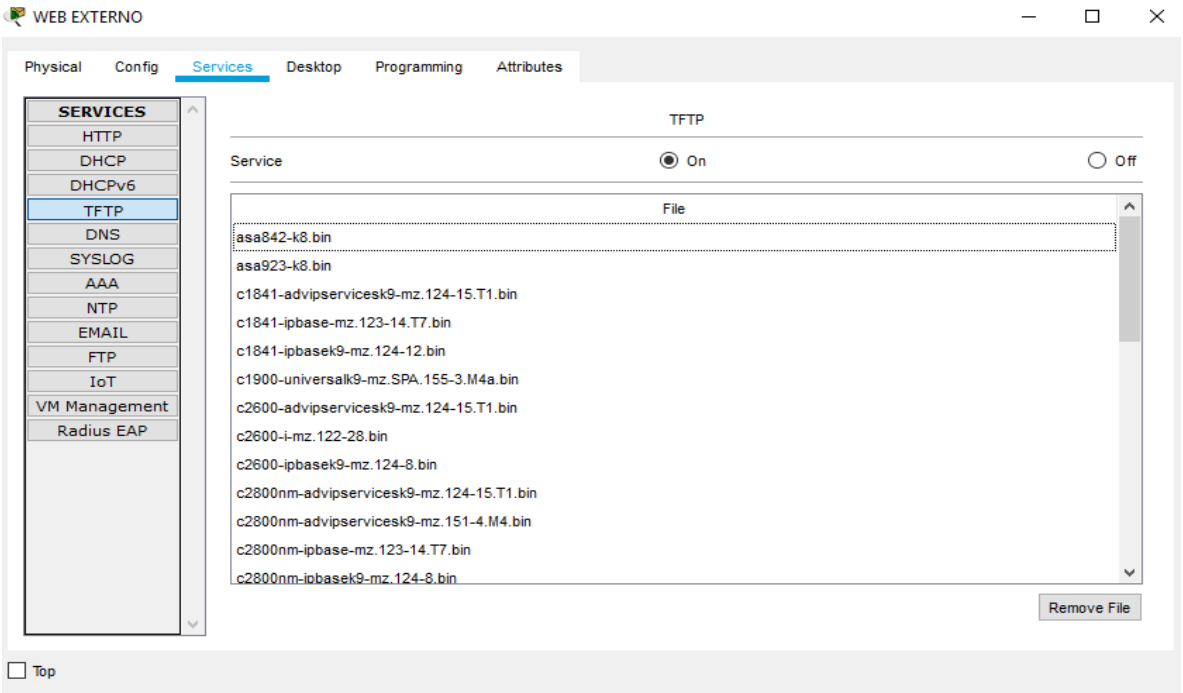

Figura 23. Imagen servidor TFTP

2.3 Servicio DHCP en los routers

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

2.3.1 Router Bucaramanga

```
BUCARAMANGA(config)#ip dhcp pool upvn10
BUCARAMANGA(dhcp-config)#network 172.31.0.0 255.255.255.192
BUCARAMANGA(dhcp-config)#default-router 172.31.0.1
BUCARAMANGA(dhcp-config)#option 150 ip 172.31.0.1
BUCARAMANGA(dhcp-config)#exit

BUCARAMANGA(config)#ip dhcp pool upvn30
BUCARAMANGA(dhcp-config)#network 172.31.0.64 255.255.255.192
BUCARAMANGA(dhcp-config)#default-router 172.31.0.65
BUCARAMANGA(dhcp-config)#option 150 ip 172.31.0.65
BUCARAMANGA(dhcp-config)#exit

BUCARAMANGA(config)#interface fa0/0.10
BUCARAMANGA(config-subif)#
BUCARAMANGA(config-subif)#encapsulation dot1q 10
BUCARAMANGA(config-subif)#ip add 172.31.0.1 255.255.255.192
BUCARAMANGA(config-subif)#exit

BUCARAMANGA(config)#interface fa0/0.30
BUCARAMANGA(config-subif)#encapsulation dot1q 30
BUCARAMANGA(config-subif)#ip add 172.31.0.65 255.255.255.192
BUCARAMANGA(config-subif)#exit


BUCARAMANGA(config)#router ospf 1
BUCARAMANGA(config-router)#network 172.31.0.0 0.0.0.255 area 0
BUCARAMANGA(config-router)#router-id 1.1.1.1
```

2.3.2 Router Cundinamarca

```
CUNDINAMARCA(config)#ip dhcp pool upvn10
CUNDINAMARCA(dhcp-config)#network 172.31.2.8 255.255.255.248
```

```
CUNDINAMARCA(dhcp-config)#default-router 172.31.2.9
CUNDINAMARCA(dhcp-config)#option 150 ip 172.31.2.9
CUNDINAMARCA(dhcp-config)#exit

CUNDINAMARCA(config)#ip dhcp pool upvn20
CUNDINAMARCA(dhcp-config)#network 172.31.1.64 255.255.255.192
CUNDINAMARCA(dhcp-config)#default-router 172.31.1.65
CUNDINAMARCA(dhcp-config)#option 150 ip 172.31.1.65
CUNDINAMARCA(dhcp-config)#exit

CUNDINAMARCA(config)#interface fa0/0.10
CUNDINAMARCA(config-subif)#encapsulation dot1q 10
CUNDINAMARCA(config-subif)#ip add 172.31.2.9 255.255.255.248
CUNDINAMARCA(config-subif)#exit

CUNDINAMARCA(config)#interface fa0/0.20
CUNDINAMARCA(config-subif)#encapsulation dot1q 20
CUNDINAMARCA(config-subif)#ip add 172.31.1.65 255.255.255.192
CUNDINAMARCA(config-subif)#exit

CUNDINAMARCA(config)#int fa0/0.88
CUNDINAMARCA(config-subif)#encapsulation dot1q 88
CUNDINAMARCA(config-subif)#ip address 172.31.2.25 255.255.255.248
CUNDINAMARCA(config-subif)#exit


CUNDINAMARCA(config)#router ospf 1
CUNDINAMARCA(config-router)#network 172.31.1.0 0.0.0.255 area 0
CUNDINAMARCA(config-router)#network 172.31.2.0 0.0.0.255 area 0
CUNDINAMARCA(config-router)#router-id 1.1.1.1
CUNDINAMARCA(config-router)#exit
```

2.4 NAT

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

```
TUNJA(config)#ip nat inside source static 172.31.2.28 209.165.220.4
TUNJA(config)#access-list 1 permit 172.0.0.0 0.255.255.255
TUNJA(config)#ip nat inside source list 1 interface fa1/0 overload
TUNJA(config)#int fa1/0
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#int f0/0.20
```

```
TUNJA(config-subif)#ip nat inside
TUNJA(config-subif)#int f0/0.30
TUNJA(config-subif)#ip nat inside
TUNJA(config-subif)#int se0/0
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#int se0/1
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#ip route 0.0.0.0 0.0.0.0 209.165.220.3
TUNJA(config)#router ospf 1
TUNJA(config-router)#default-information originate
```

2.4 Enrutamiento autenticación

El enrutamiento deberá tener autenticación.

```
BUCARAMANGA(config)#int se0/0
BUCARAMANGA(config-if)#ip ospf authentication message-digest
BUCARAMANGA(config-if)#ip ospf message-digest-key 1 md5 cisco
```

```
CUNDINAMARCA(config)#int se0/0
CUNDINAMARCA(config-if)#ip ospf authentication message-digest
CUNDINAMARCA(config-if)#ip ospf message-digest-key 1 md5 cisco
```

```
TUNJA(config)#int se0/0
TUNJA(config-if)#ip ospf authentication message-digest
TUNJA(config-if)#ip ospf message-digest-key 1 md5 cisco
TUNJA(config-if)#int se0/1
TUNJA(config-if)#ip ospf authentication message-digest
TUNJA(config-if)#ip ospf message-digest-key 1 md5 cisco
```

2.5 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-if)#access-list 111 deny ip 172.31.1.64 0.0.0.63 209.165.220.0 0.0.0.255
CUNDINAMARCA(config)#access-list 111 permit ip any any
CUNDINAMARCA(config)#int f0/0.20
```

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

```
CUNDINAMARCA(config)#access-list 112 permit ip 172.31.1.0 0.0.0.63 209.165.220.0 0.0.0.255
CUNDINAMARCA(config)#access-list 112 deny ip any any
CUNDINAMARCA(config)#int f0/0.10
CUNDINAMARCA(config-subif)#ip access-group 112 in
```

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

```
TUNJA(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 80
TUNJA(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 21
TUNJA(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 20
TUNJA(config)#int f0/0.30
TUNJA(config-subif)#ip access-group 111 in
```

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

```
TUNJA(config)#access-list 112 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
TUNJA(config)#access-list 112 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
TUNJA(config)#int f0/0.20
TUNJA(config-subif)#ip access-group 112 in
```

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

```
BUCARAMANGA(config)#access-list 111 permit ip 172.31.0.64 0.0.0.63 209.165.220.0 0.0.0.255
BUCARAMANGA(config)#int f0/0.30
BUCARAMANGA(config-subif)#ip access-group 111 in
```

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 112 permit ip 172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63
BUCARAMANGA(config)#access-list 112 permit ip 172.31.0.0 0.0.0.63 172.31.0.128 0.0.0.63
BUCARAMANGA(config)#int f0/0.10
BUCARAMANGA(config-subif)#ip access-group 112 in
```

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

```
BUCARAMANGA(config)#access-list 113 deny ip 172.31.2.0 0.0.0.7 172.31.0.0 0.0.0.63
BUCARAMANGA(config)#access-list 113 deny ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.0.63
BUCARAMANGA(config)#access-list 113 permit ip any any
BUCARAMANGA(config)#int f0/0.10
BUCARAMANGA(config-subif)#ip access-group 113 out
```

```
CUNDINAMARCA(config)#access-list 113 deny ip 172.31.2.8 0.0.0.7 172.31.1.64 0.0.0.63
CUNDINAMARCA(config)#access-list 113 deny ip 172.31.1.0 0.0.0.63 172.31.1.64 0.0.0.63
CUNDINAMARCA(config)#access-list 113 deny ip 172.31.2.24 0.0.0.7 172.31.1.64 0.0.0.63
CUNDINAMARCA(config)#access-list 113 permit ip any any
CUNDINAMARCA(config)#int f0/0.20
CUNDINAMARCA(config-subif)#ip access-group 113 out
```

```
TUNJA(config)#access-list 113 deny ip 172.3.2.8 0.0.0.7 172.31.0.128 0.0.0.63
TUNJA(config)#access-list 113 deny ip 172.3.0.192 0.0.0.63 172.31.0.128 0.0.0.63
TUNJA(config)#access-list 113 permit ip any any
TUNJA(config)#int f0/0.20
TUNJA(config-subif)#ip access-group 113 out
```

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

```
BUCARAMANGA(config)#access-list 3 permit 172.31.2.0 0.0.0.7
BUCARAMANGA(config)#access-list 3 permit 172.3.2.8 0.0.0.7
BUCARAMANGA(config)#access-list 3 permit 172.31.2.8 0.0.0.7
BUCARAMANGA(config)#line vty 0 15
BUCARAMANGA(config-line)#access-class 3 in
```

```
CUNDINAMARCA(config)#access-list 3 permit 172.31.2.0 0.0.0.7
CUNDINAMARCA(config)#access-list 3 permit 172.3.2.8 0.0.0.7
CUNDINAMARCA(config)#access-list 3 permit 172.31.2.8 0.0.0.7
CUNDINAMARCA(config)#line vty 0 15
CUNDINAMARCA(config-line)#access-class 3 in
```

```
TUNJA(config)#access-list 3 permit 172.31.2.0 0.0.0.7
TUNJA(config)#access-list 3 permit 172.3.2.8 0.0.0.7
TUNJA(config)#access-list 3 permit 172.31.2.8 0.0.0.7
TUNJA(config)#line vty 0 15
TUNJA(config-line)#access-class 3 in
```

ARCHIVOS APK

https://drive.google.com/file/d/1VzQeYtnBUnx9BbxgyYL1UVyRZYGfpKFX/view?usp=sharing

Conclusiones

En el desarrollo de la actividad anterior se puso en practicas habilidades adquiridas durante el desarrollo del diplomado sumado a un amplio numero de tareas en el desarrollo de cada uno de los puntos propuestos, se ejecutan funciones tales como la verificación de conexión, configuración básica de dispositivos, enrutamientos estáticos entre muchas otras que fortalecen las habilidades practicas como futuros egresados de la ingeniería de sistemas aplicado en el campo de las telecomunicaciones.

Bibliografía

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

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://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxilary%20materials/Cisco-ICND2.pdf

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

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