PRUEBA DE HABILIDADES PRÁCTICAS CNN

LUZ DARY GÓMEZ SABY

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS EN TECNOLOGÍA E INGENIERÍA

COLOMBIA

2020

PRUEBA DE HABILIDADES PRÁCTICAS CNN

Luz Dary Gómez Saby
Grupo–2 03092_26

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

TUTOR
NILSON ALBEIRO FERREIRA MANZANARES

DIRECTOR
JUAN CARLOS VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS EN TECNOLOGÍA E INGENIERÍA

COLOMBIA
2020

CONTENIDO

Resumen

En la actualidad los sistemas de información son una herramienta muy poderosa puesto que generan efectividad y mayor productividad a las organizaciones y en general a la sociedad tanto en la vida diaria y aun más en el sector académico financiero y en en todos los escenarios de la vida.

El presente trabajo centra su contenido en el desarrollo de dos escenarios en el contexto de redes de comunicaciones bajo la supervicion de la UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD), en colaboración con CISCO Networking Academy, el cual brinda dar un pespectiva de la conectividad de información entre diferentes ciudades las cuales comparten y administran información tanto local como global.

Abstract

At present, information systems are a very powerful tool since they generate effectiveness and greater productivity for organizations and society in general both in daily life and even more in the financial academic sector and in all life scenarios. .

The present work focuses its content on the development of two scenarios in the context of communications networks under the supervision of the UNIVERSIDAD NACIONAL ABIERTA YA DISTANCIA (UNAD), in collaboration with CISCO Networking Academy, which provides a perspective of the connectivity of information between different cities which share and manage both local and global information.

Introducción

La importancia de la tecnología y los medios de comunicación en el mundo actual es cada vez mayor, razón por la cual las diferentes empresas e instituciones deben cada día hacer uso de diferentes medios que le permitan estar intercomunicados de manera ágil, segura y eficaz.

En este caso, para el desarrollo de este trabajo final del curso, se nos presenta una empresa con sedes en diferentes ciudades y haciendo uso de los diferentes conocimientos adquiridos durante el curso se realiza la configuración de la red, de manera que permita la interconexión de los diferentes dispositivos tecnológicos pertenecientes a cada una de las sucursales, configuración de red que fue realizada de acuerdo a los requerimientos y parámetros solicitados y establecidos para la implementación de esta.

Con el desarrollo de este trabajo final se evidencia la aprehensión de diferentes conceptos y conocimientos adquiridos durante el curso, lo cual permite, por medio de la práctica, identificar posibles fortalezas o debilidades en los diferentes temas desarrollados y aplicados y que serán de gran utilidad dentro de las diferentes labores profesionales del estudiante.

OBJETIVOS

GENERAL

Realizar la configuración de la red propuesta en el caso teniendo en cuenta las especificaciones y parámetros establecidos para esta, aplicando los conocimientos adquiridos en el Diplomado De Profundización CISCO, para dar solución al problema que se nos plantea.

OBJETIVOS ESPECIFICOS

- ✓ Realizar la conexión y respectiva configuración de Routers y Switches en una red, mediante la aplicación de comandos del IOS de Cisco.

- ✓ Identificar los conceptos principales y protocolos de enrutamiento, reconociendo las diversas características de cada topología.

- ✓ Adquirir y aplicar los conocimientos principales del programa Packet tracert y Smart Lab en la configuración de redes de comunicaciones, implementando comandos de la plataforma CISCO.

- ✓ Comprobar la adecuada configuración de cada dispositivo en la red mediante instrucciones ping y tracert.

- ✓ Implementar en el diseño de la red de acuerdo a los lineamientos del problema presentado.

- ✓ Realizar el reconocimiento de Vla, la respectiva configuración, direccionamiento de red y mascara de direccionamiento.

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.

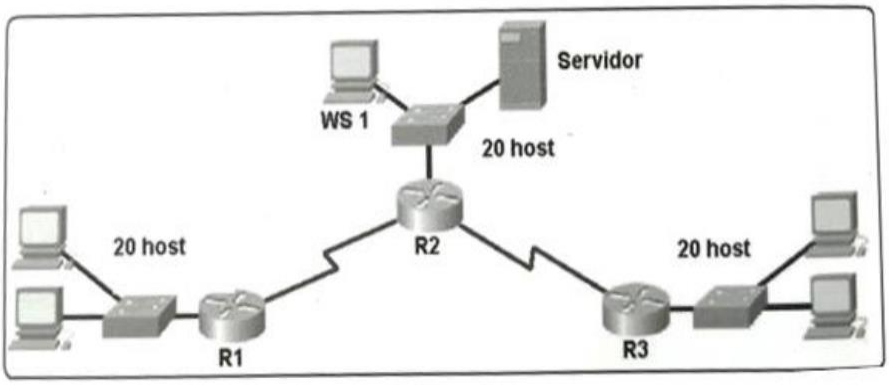
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

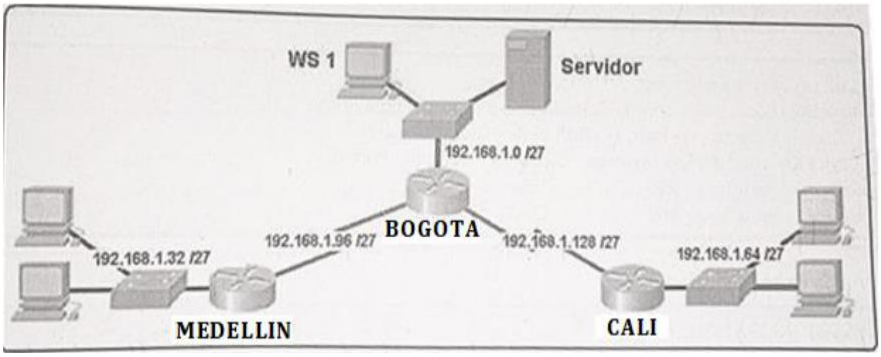
Parte 3: La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.

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.





1 SUBNETEO

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

	Address:	Netmask: Mascara de red	Host mínimo	Host máximo	Network:	Broadcast:	host
1	192.168.1.1	255.255.255.224=27	192.168.1. 1	192.168.1. 30	192.168.1.0/27	192.168.1. 31	30
2	192.168.1. 33	255.255.255.224=27	192.168.1.33	192.168.1. 62	192.168.1.32/27	192.168.1.63	30
3	192.168.1.65	255.255.255.224=27	192.168.1. 65	192.168.1. 94	192.168.1.64/27	192.168.1. 95	30
4	192.168.1. 96	255.255.255.224=27	192.168.1. 97	192.168.1.126	192.168.1.96/27	192.168.1. 127	30
5	192.168.1. 128	255.255.255.224=27	192.168.1. 129	192.168.1. 158	192.168.1.128/27	192.168.1. 159	30
6	192.168.1.60	255.255.255.224=27	192.168.1. 161	192.168.1. 190	192.168.1.160/27	192.168.1. 191	30
7	192.168.1. 192	255.255.255.224=27	192.168.1.193	192.168.1. 222	192.168.1.192/27	192.168.1. 223	30
8	192.168.1.2.24	255.255.255.224=27	192.168.1. 225	192.168.1. 254	192.168.1.224/27	192.168.1. 255	30

1.1 Asignar una dirección IP a la red.

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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)#banner motd #NO ESTAS AUTORIZADO#
BOGOTA(config)#exit
BOGOTA#
%SYS-5-CONFIG_I: Configured from console by console
Exit
```

```
Router>en
Router#conf t
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 #PERSNAL AUTORIZADO UNAD#
MEDELLIN(config)#exit
MEDELLIN#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

SWICH

Switch#conf t

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

Switch(config)#hostname Sw1

Sw1(config)#enable secret cisco

Sw1(config)#line console 0

Sw1(config-line)#password cisco

Sw1(config-line)#login

Sw1(config-line)#exit

Sw1(config)#line vty 0 4

Sw1(config-line)#password cisco

Sw1(config-line)#login

Sw1(config-line)#service password-encryption

Sw1(config)#banner motd #PERSONAL AUTORIZADO#

Sw1(config)#exit

Sw1#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Sw1#

Switch>enable

Switch#conf t

```
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Sw2
Sw2(config)#enable secret cisco
Sw2(config)#line console 0
Sw2(config-line)#password cisco
Sw2(config-line)#login
Sw2(config-line)#exit
Sw2(config)#line vty 0 4
Sw2(config-line)#password cisco
Sw2(config-line)#login
Sw2(config-line)#service password-encryption
Sw2(config)#banner motd #SOLO PERSONAL AUTORIZADO#
Sw2(config)#exit
Sw2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
Switch>ena
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Sw3
Sw3(config)#enable secret cisco
Sw3(config)#line console 0
Sw3(config-line)#password cisco
Sw3(config-line)#login
Sw3(config-line)#exit
Sw3(config)#line vty 0 4
Sw3(config-line)#password cisco
```

Sw3(config-line)#login

Sw3(config-line)#service password-encryption

Sw3(config)#banner motd #PERSONAL AUTORIZADO#

Sw3#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Sw3#

Configuracion Interfaz y Seriales

BOGOTA#enable
BOGOTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#interface g0/0
BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224
BOGOTA(config-if)#no sh
BOGOTA(config-if)#exit
BOGOTA(config)#interface s0/1/0
BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224
BOGOTA(config-if)#no sh
BOGOTA(config-if)#exit
BOGOTA(config)#interface s0/1/1
BOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224
BOGOTA(config-if)#no sh
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

MEDELLIN#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#interface g0/0
MEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.224
MEDELLIN(config-if)#no sh
MEDELLIN(config-if)#exit

```
MEDELLIN(config)#interface s0/1/0
MEDELLIN(config-if)#ip address 192.168.1.99 255.255.255.224
MEDELLIN(config-if)#no sh
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
Destination filename [startup-config]?
Building configuration...
[OK]
MEDELLIN#
```

```
CALI>enable
Password:
CALI#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#interface g0/0
CALI(config-if)#ip address 192.168.1.65 255.255.255.224
CALI(config-if)#no sh
CALI(config-if)#interface s0/1/0
CALI(config-if)#ip address 192.168.1.131 255.255.255.224
CALI(config-if)#no sh
CALI(config-if)#exit
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
Destination filename [startup-config]?
Building configuration...
[OK]
CALI#
```

1.2 CONFIGURACIÓN BÁSICA.

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

b.	R1	R2	R3
Nombre de Host	**MEDELLIN**	**BOGOTA**	**CALI**
Dirección de Ip en interfaz Serial 0/1/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/1/1		192.168.1.130	
Dirección de Ip en interfaz GigabitEthernet 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

1.2.1 Verificar la tabla de enrutamiento. En cada uno de los routers para comprobar las redes y sus rutas.

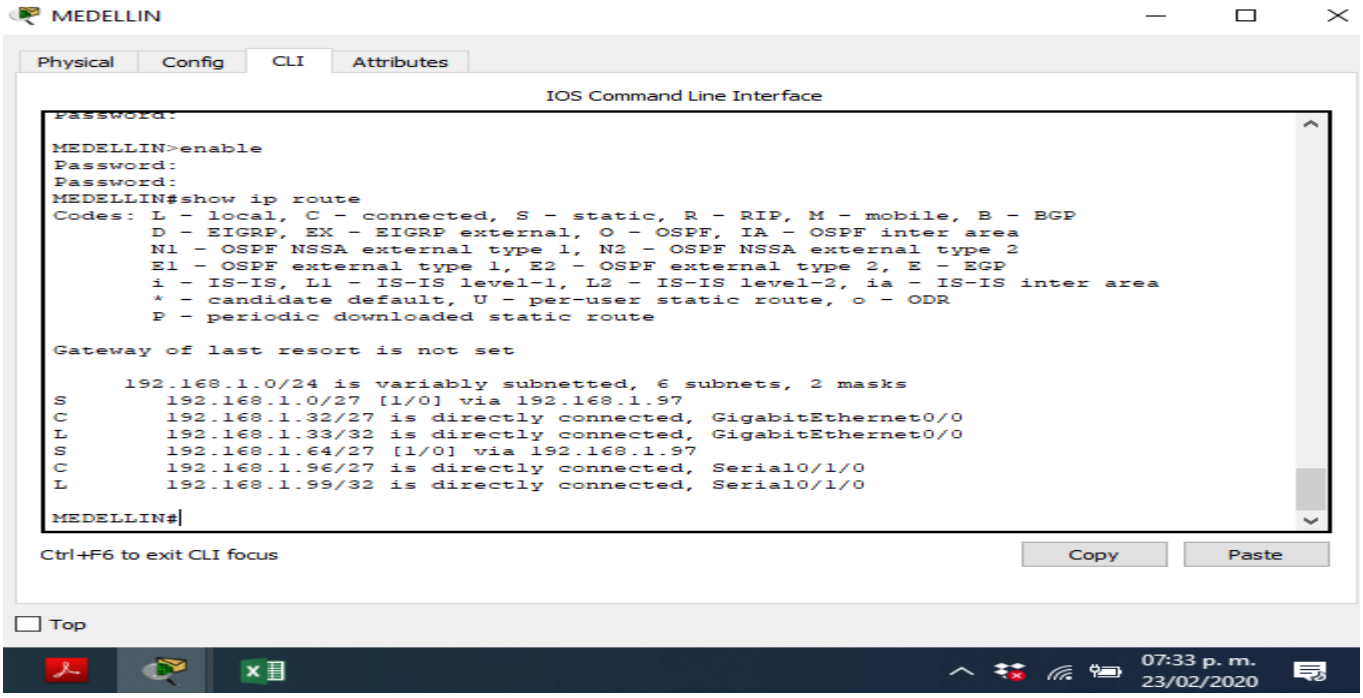


Figura 1. Imagen router Medellin

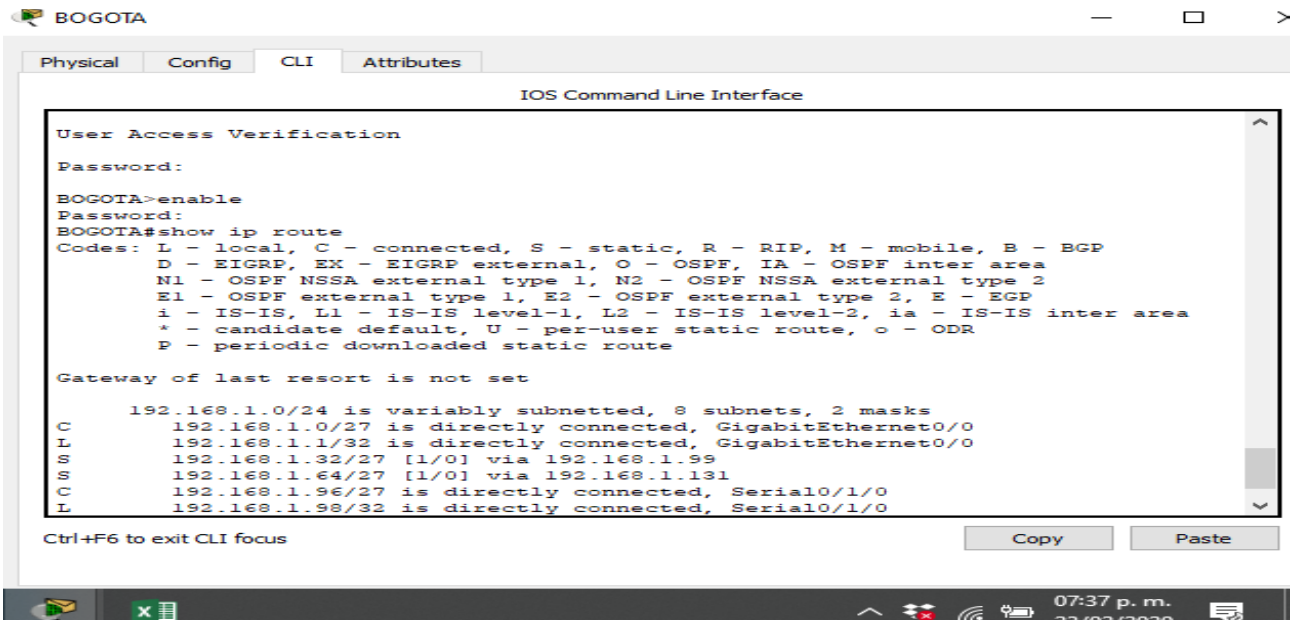


Figura 2. Imagen router Bogotá

Figura 3. Imagen router Cali

1.2.2 Verificacion balanceo de cargas

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

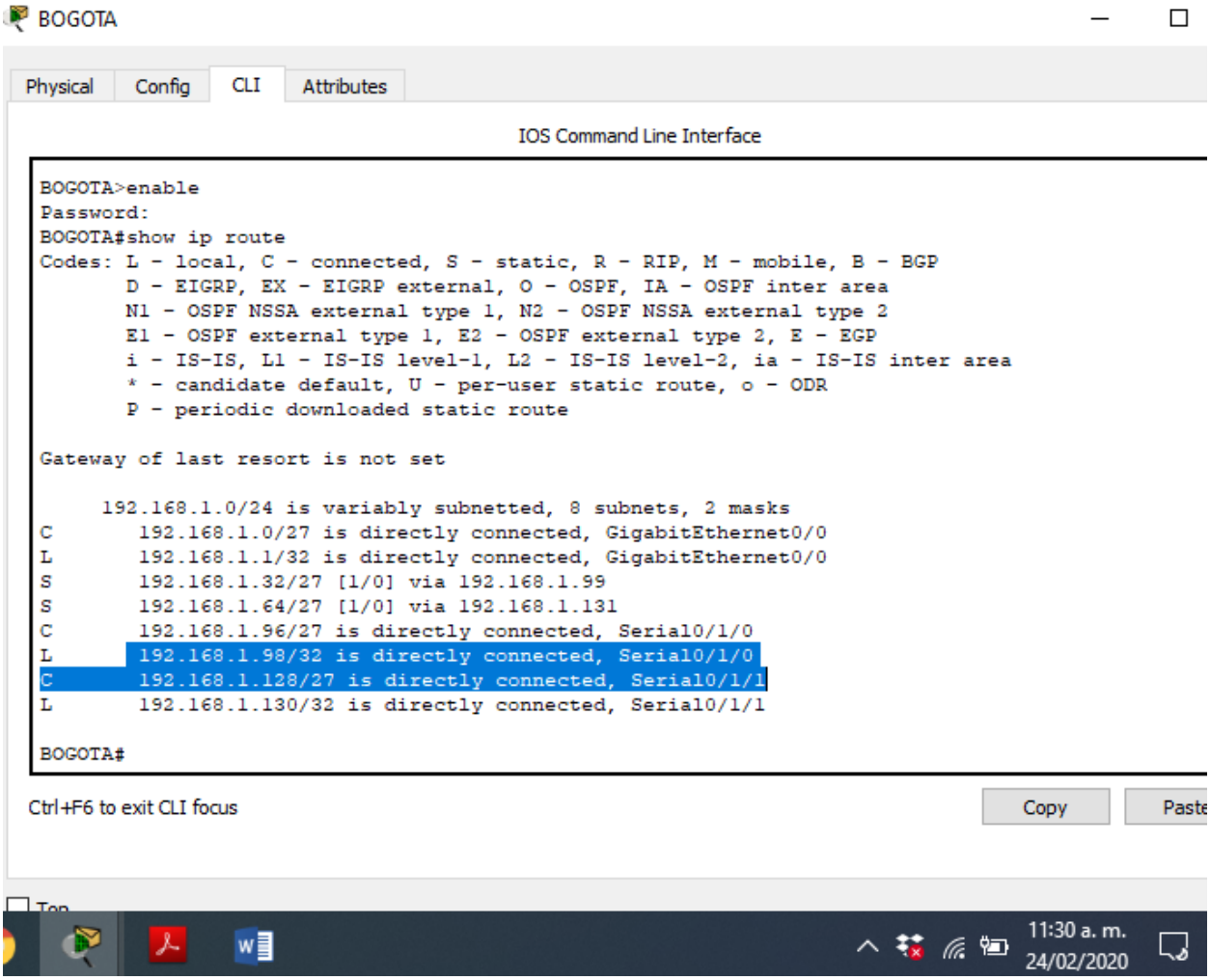


Figura 4. Imagen router Bogota

1.2.3 Diagnóstico de vecinos

Usando el comando cdp y show cdp neighbors

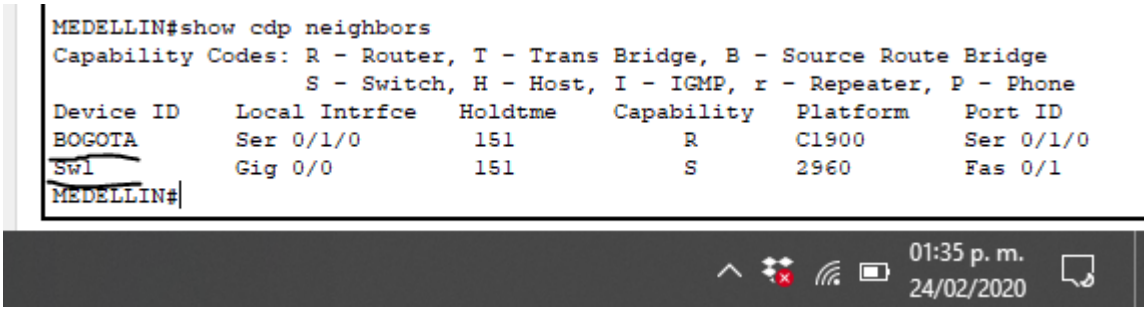


Figura 5. Red MEDELLIN muestra dos vecinos; router bogota y el Switch1

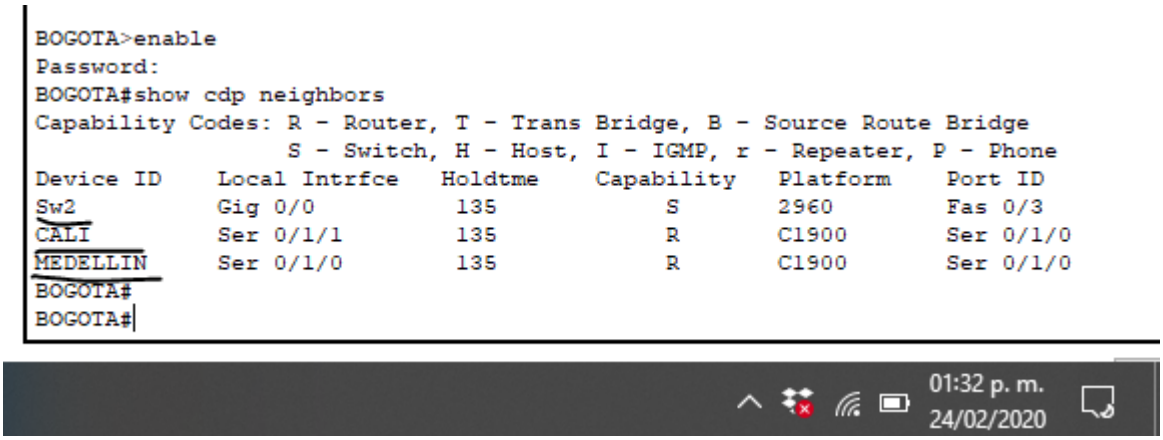


Figura 6. Red de bogota tiene tres vecinos; router Medellin, Router Cali y el Switch2

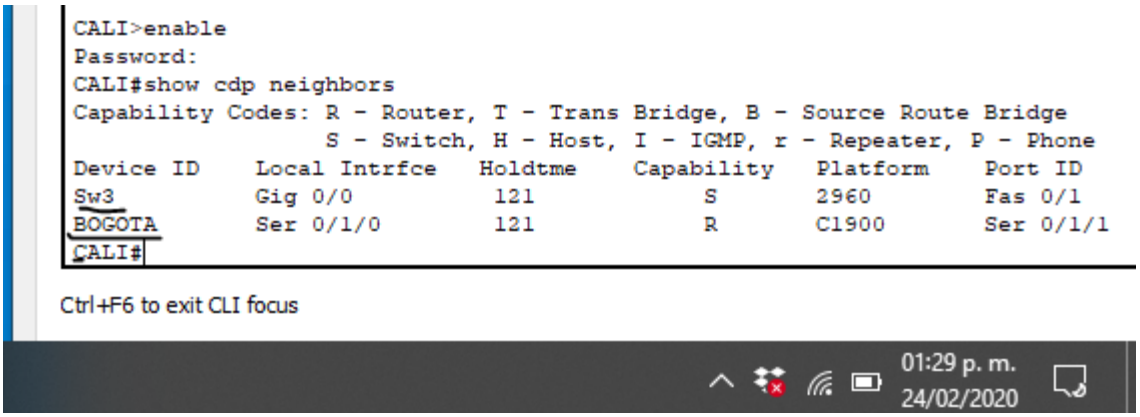


Figura 7. La red cali tiene dos vecinos router Bogota y el Switch3

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

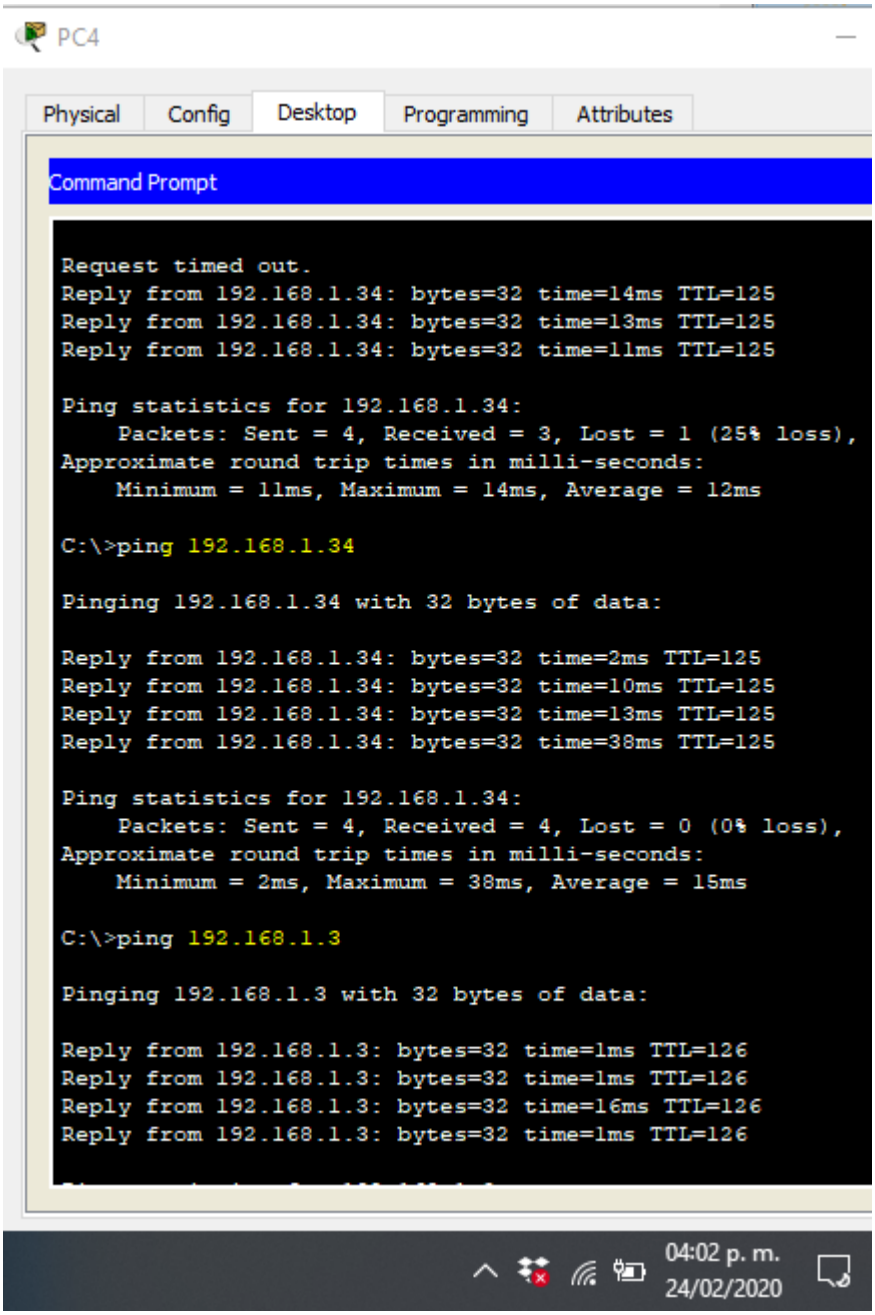


Figura 8. Ping mostrando conectividad entre las redes.

1.3. CONFIGURACIÓN DE ENRUTAMIENTO.

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

```
MEDELLIN>enable
Password:
MEDELLIN#conf t
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)#exit
MEDELLIN(config)#
```

```
BOGOTA>enable
Password:
BOGOTA#conf t
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)#network 192.168.1.128 0.0.0.31
BOGOTA(config-router)#no auto-summary
BOGOTA(config-router)#exit
BOGOTA(config)#
```

```
CALI>enable
Password:
CALI#conf t
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)#no auto-summary
CALI(config-router)#exit
```

1.3.2 Verificarificacion de vecinos con EIGRP.

Verificacion de vencindad EIGRP en los routers con los comandos show ip eigrp neighbors y show ip eigrp topology

```
MEDELLIN#show ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt Num
0   192.168.1.98    Se0/1/0         13   01:41:54  40     1000  0   7

MEDELLIN#
```

Figura 9. router Medellin tiene de vecinos al router de Bogota

```
BOGOTA>
BOGOTA>enable
Password:
Password:
BOGOTA#show ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt Num
0   192.168.1.99    Se0/1/0         13   02:03:21  40     1000  0   7
1   192.168.1.131   Se0/1/1         12   01:56:34  40     1000  0   8

BOGOTA#
```

Ctrl+F6 to exit CLI focus Copy Past

Figura 10. Router bogota TIENE de vecinos El router de medellin y cali

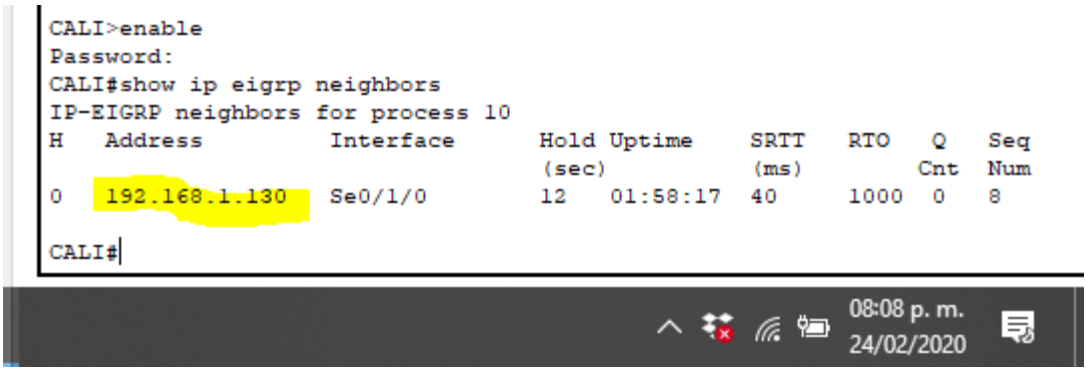


Figura 11. Router CALI tiene de vesino a router de bogota

1.3.3 VERIFICACION DE RUTAS ESTABLECIDAS

Comando show ip route

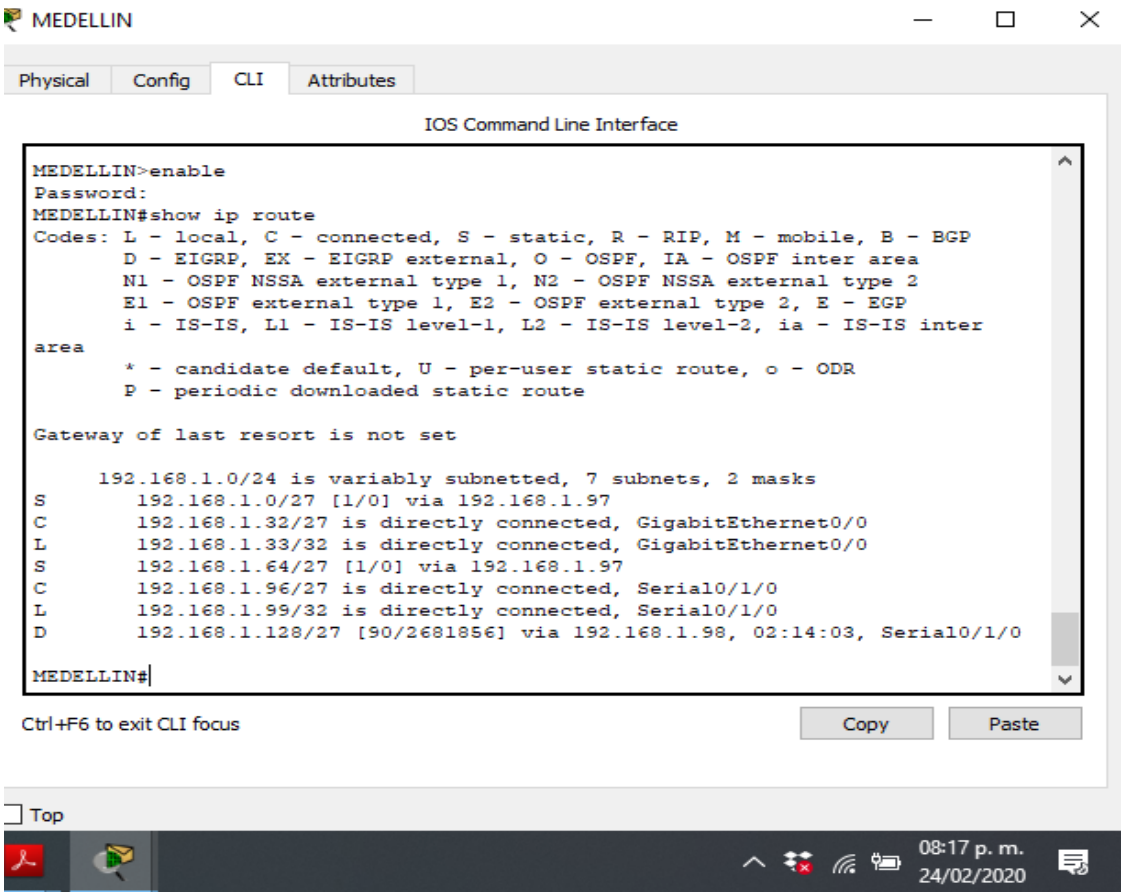


Figura 12. Imagen router Medellin

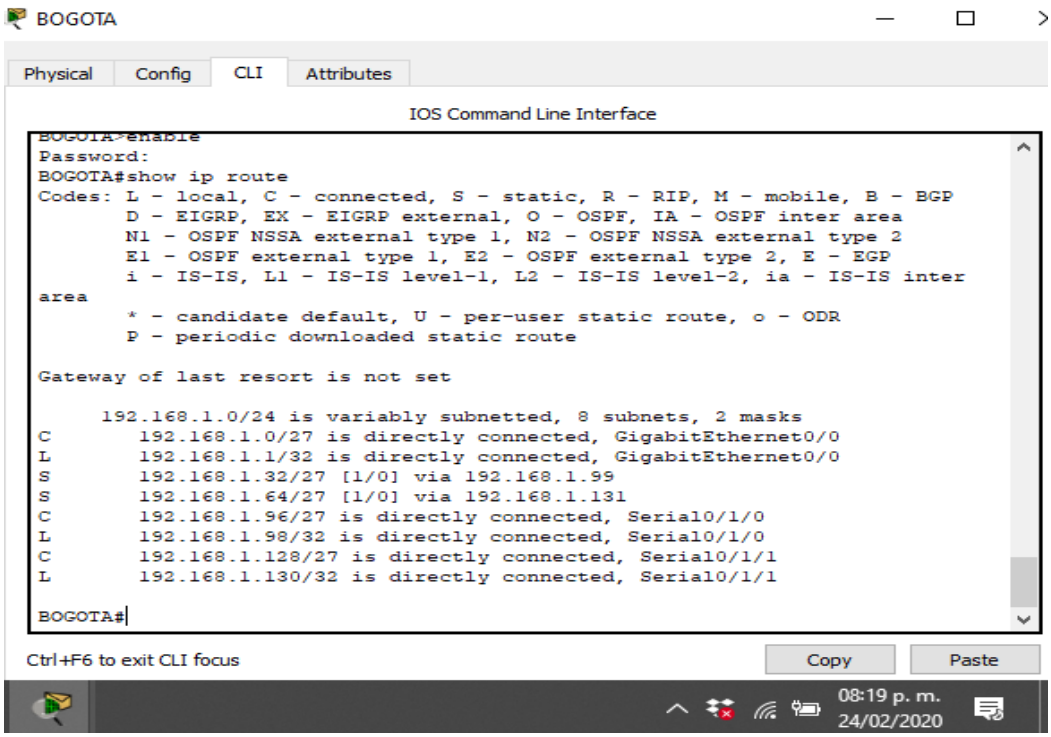


Figura 13. Imagen router Bogotá

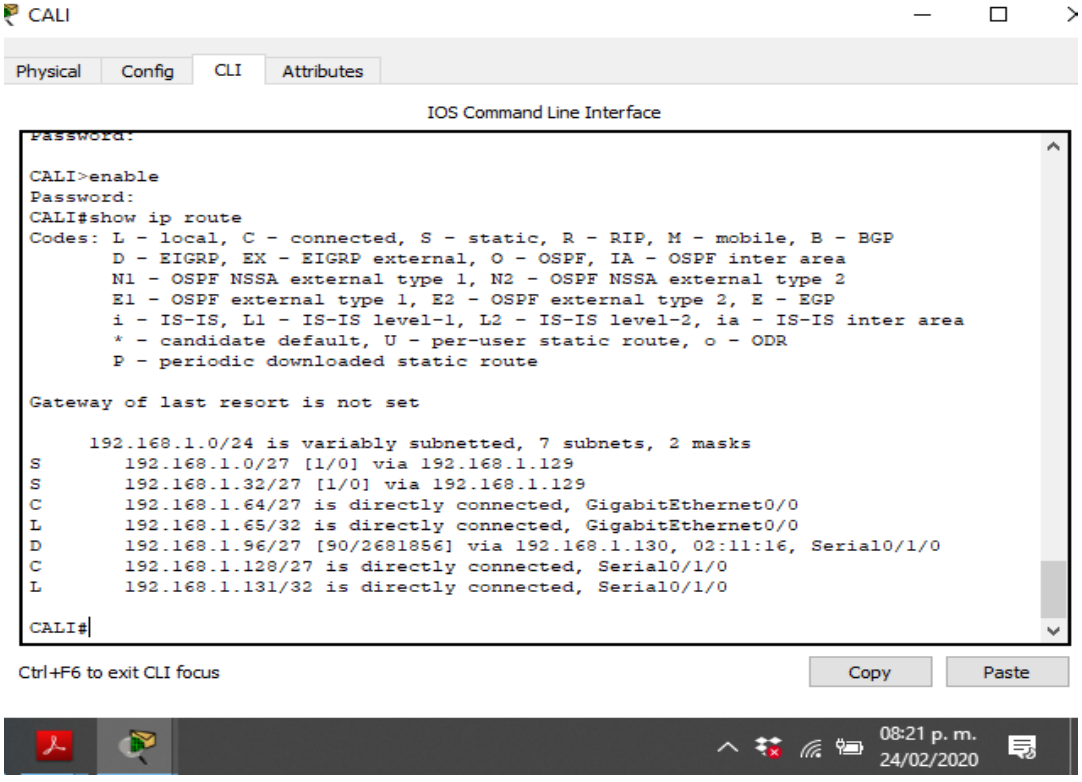


Figura 14. Imagen router Cali

1.3.4 DIAGNOSTICO DE REDES LAN

Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se pueda 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.

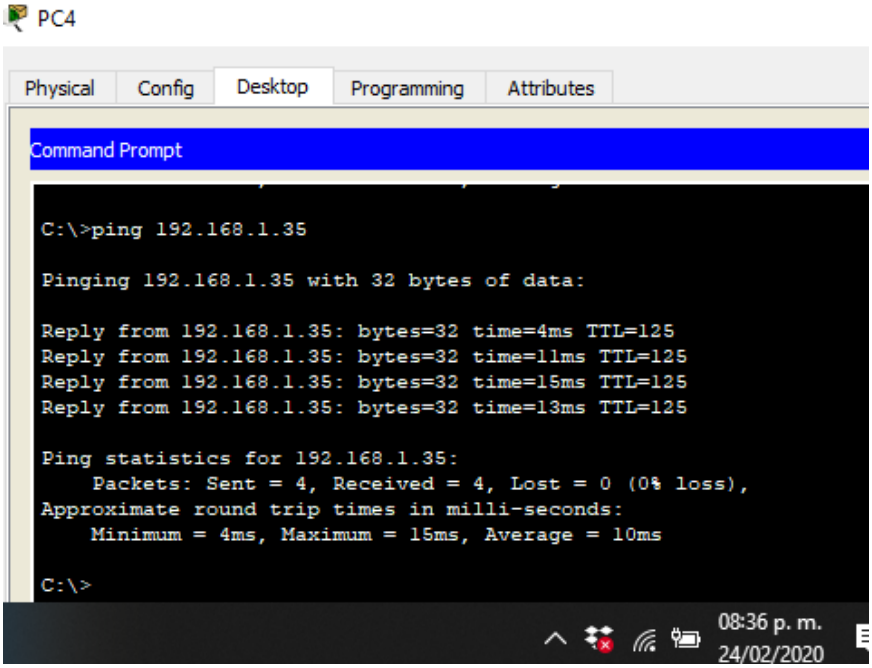


Figura 15. Ping de cali a la lan de Medellin

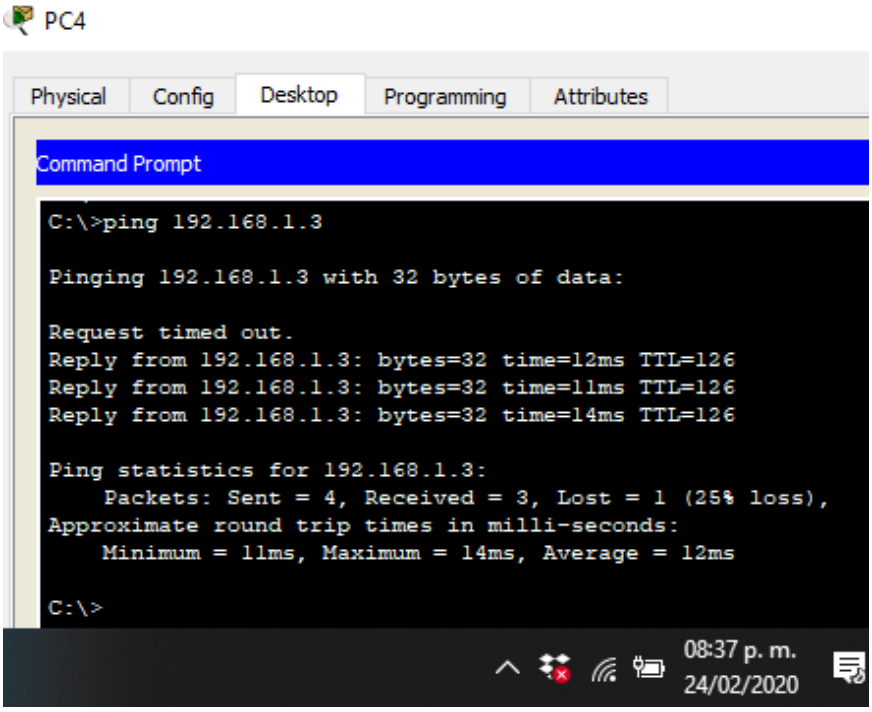


Figura 16. Ping de cali al servidor

1.4. 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:

1.4.1 CONEXIONES TELNET

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

```
MEDELLIN#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#line vty 0 4
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
```

```
BOGOTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#line vty 0 4
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#
```

```
CALI#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#line vty 0 15
CALI(config-line)#password cisco
CALI(config-line)#login
CALI(config-line)#exit
CALI(config)#
```

Conexión Telnet Medellin-Bogota

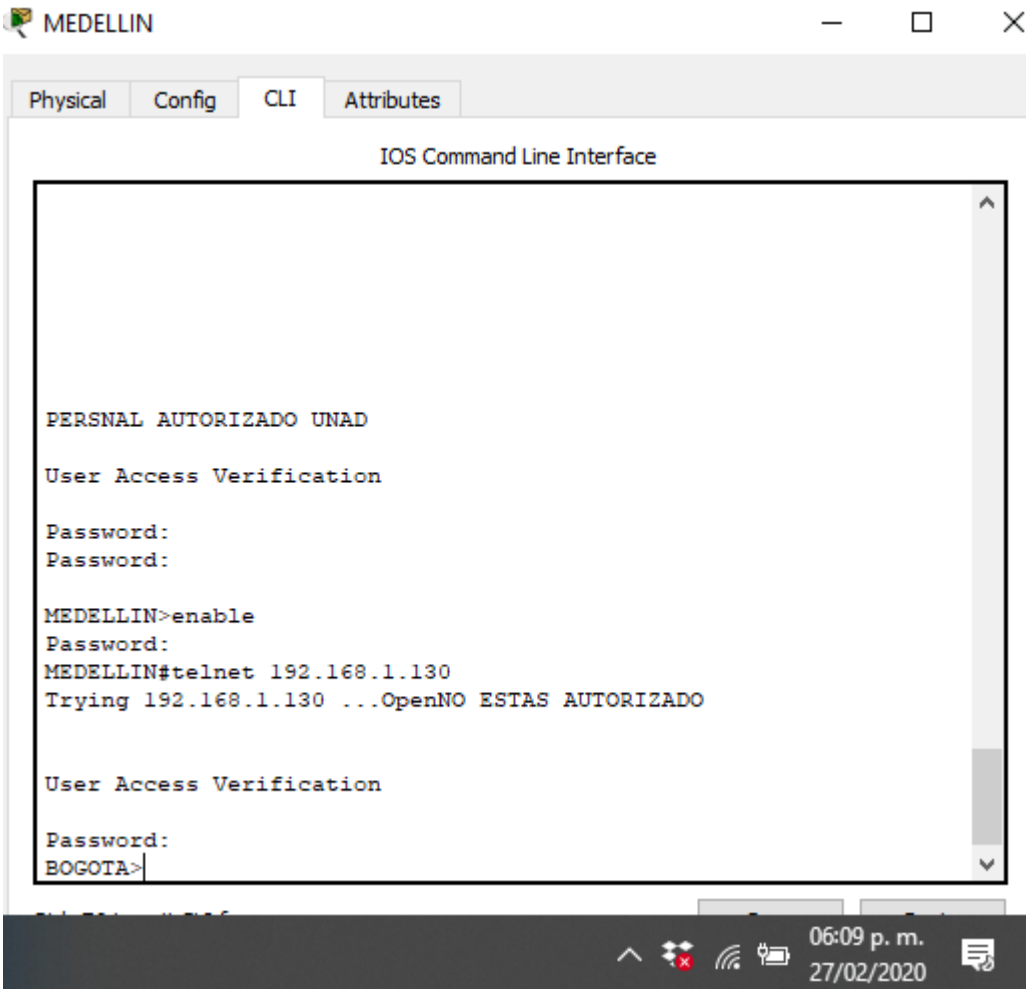


Figura 17. Conexión Telnet Medellin-Bogota

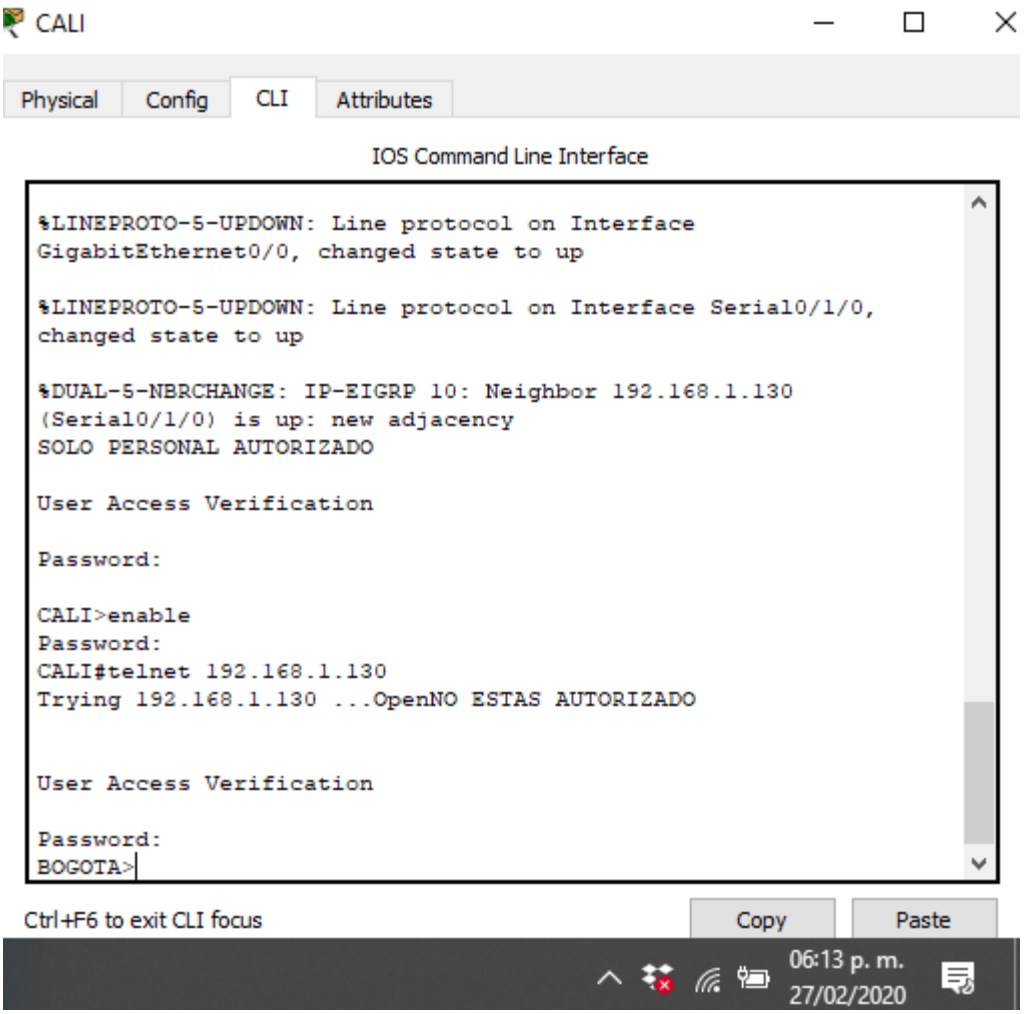


Figura 18. Conexión Telnet entre routers Cali-Bogota

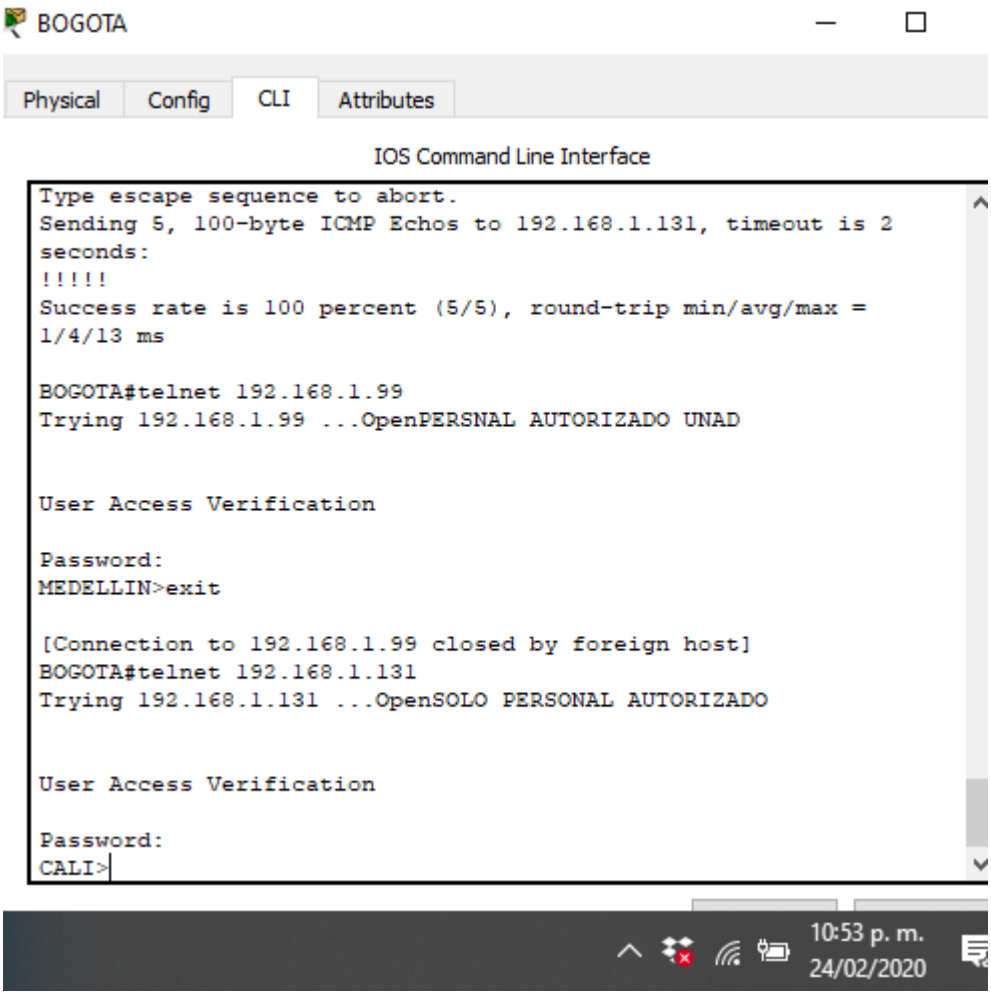


Figura 19. Conexión Telnet entre routers Bogota- Medellin y Cali

1.4.2 LIMITACIONES DE ACCESO

- **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#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#access-list 1 permit 192.168.1.6 0.0.0.224
BOGOTA(config)#access-list 1 deny any
BOGOTA(config)#int se0/1/0
BOGOTA(config-if)#ip access-group 1 out
BOGOTA(config-if)#exit
BOGOTA(config)#int se0/1/1
BOGOTA(config-if)#ip access-group 1 out
BOGOTA(config-if)#exit
```

- **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(config)#access-list 111 permit ip 192.168.1.32 0.0.0.31 host 192.168.1.6
MEDELLIN(config)#int g0/0
MEDELLIN(config-if)#ip access-group 111 in
MEDELLIN(config-if)#exit
MEDELLIN(config)#
```

```
CALI#conf t
CALI(config)#access-list 111 permit ip 192.168.1.64 0.0.0.31 host 192.168.1.6
CALI(config)#int g0/0
CALI(config-if)#ip access-group 111 in
CALI(config-if)#exit
CALI(config)#
```

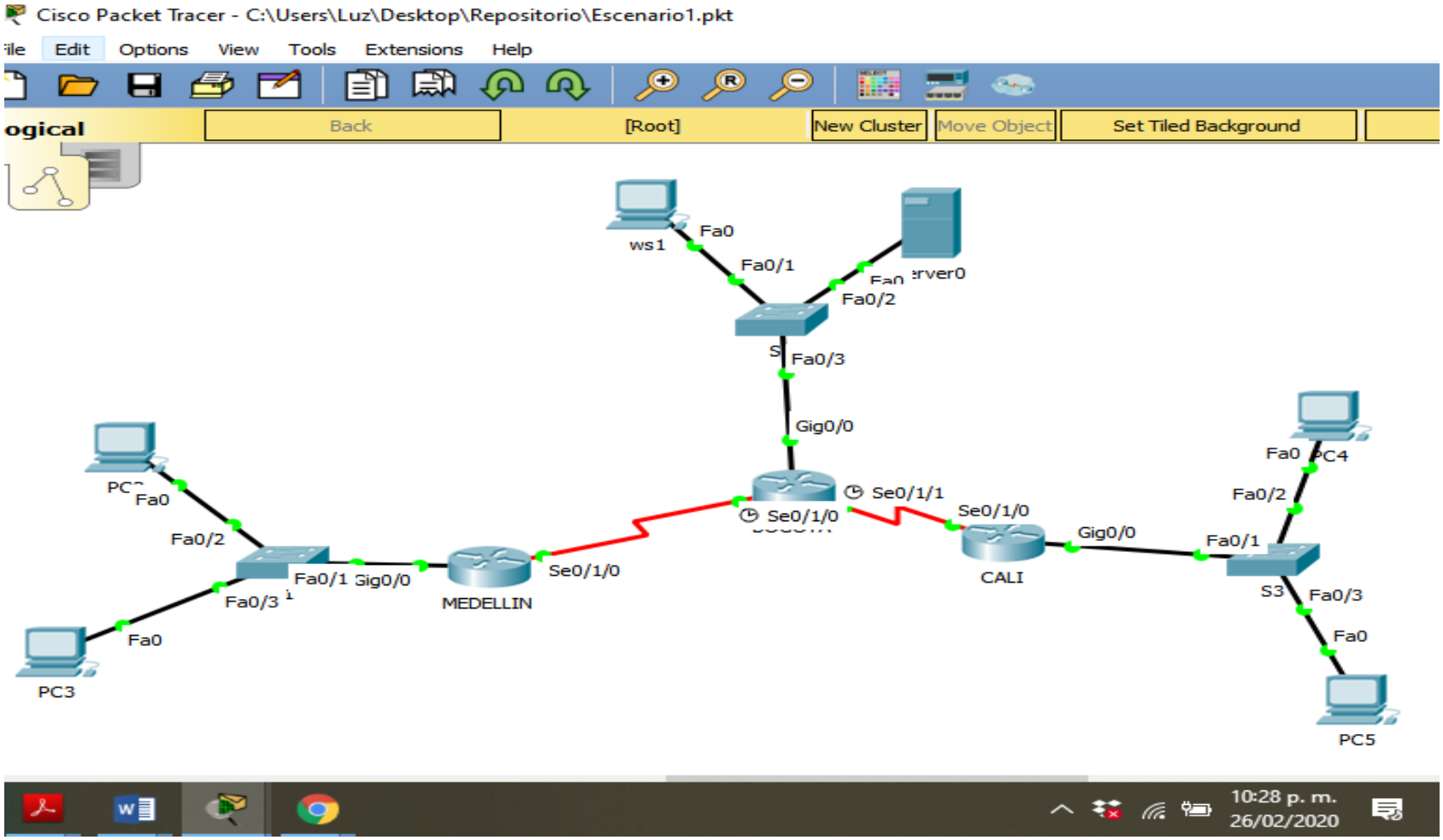
1.4.3 Comprobación de la red instalada.

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

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

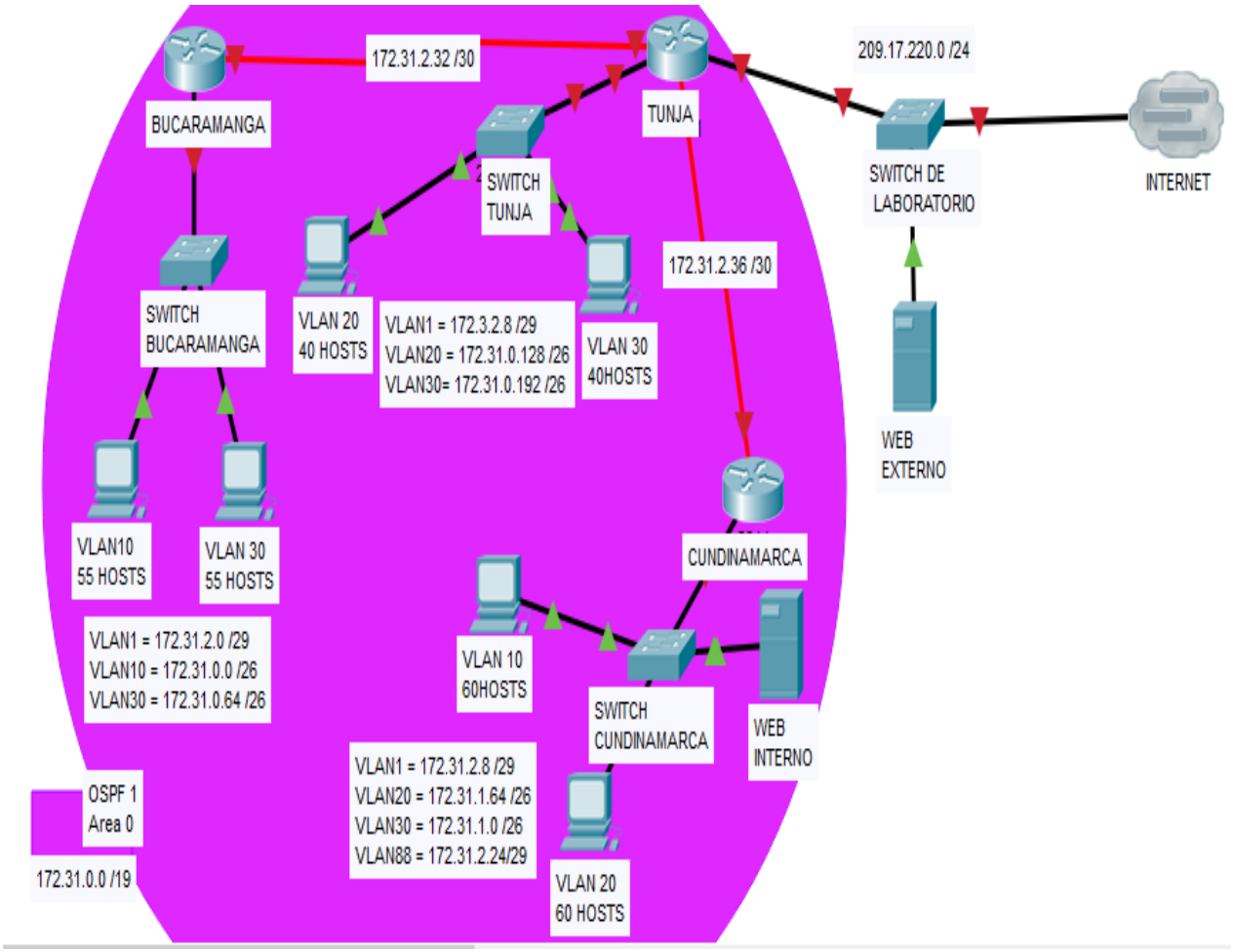
	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	FALLIDO
	WS_1	Router BOGOTA	EXITOSO
	Servidor	Router CALI	FALLIDO
	Servidor	Router MEDELLIN	FALLIDO
TELNET	LAN del Router MEDELLIN	Router CALI	FALLIDO
	LAN del Router CALI	Router CALI	FALLIDO
	LAN del Router MEDELLIN	Router MEDELLIN	FALLIDO
	LAN del Router CALI	Router MEDELLIN	FALLIDO
PING	LAN del Router CALI	WS_1	EXITOSO
	LAN del Router MEDELLIN	WS_1	EXITOSO
	LAN del Router MEDELLIN	LAN del Router CALI	EXITOSO
PING	LAN del Router CALI	Servidor	EXITOSO
	LAN del Router MEDELLIN	Servidor	EXITOSO
	Servidor	LAN del Router MEDELLIN	EXITOSO
	Servidor	LAN del Router CALI	EXITOSO
	Router CALI	LAN del Router MEDELLIN	FALLIDO
	Router MEDELLIN	LAN del Router CALI	FALLIDO

1.4.4. TOPOLOGIA



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:

1. Todos los routers deberán tener los siguiente:
   - Configuración básica.
   - Autenticación local con AAA.
   - Cifrado de contraseñas.
   - Un máximo de internos para acceder al router.
   - Máximo tiempo de acceso al detectar ataques.
   - Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.

2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca
3. El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).

4. El enrutamiento deberá tener autenticación.
5. Listas de control de acceso:
   - Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.
   - Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.
   - Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.
   - Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.
   - Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.
   - Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.

- Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.
- Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los routers e internet.

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

Aspectos a tener en cuenta

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

2.1. CONFIGURACIÓN BÁSICA ROUTER BUCARAMANGA

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BUCARAMANGA
BUCARAMANGA(config)#no ip domain-lookup
BUCARAMANGA(config)#enable secret cisco
BUCARAMANGA(config)#login
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#password cisco
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#line vty 0 4
BUCARAMANGA(config-line)#password cisco
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#service password-encryption
BUCARAMANGA(config)#banner motd #SOLO PERSONAL AUTORIZADO#
BUCARAMANGA(config)#exit
BUCARAMANGA#
BUCARAMANGA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
BUCARAMANGA#
```

2.1.1 INTERFACES Y SERIALES

```
BUCARAMANGA(config)#int serial 0/1/0
BUCARAMANGA(config-if)#ip add 172.31.2.34 255.255.255.252
BUCARAMANGA(config-if)#no shutdown
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#int g0/0.1
BUCARAMANGA(config-subif)#encapsulation dot1q 1
BUCARAMANGA(config-subif)#ip add 172.31.2.1 255.255.255.248
BUCARAMANGA(config-subif)#int g0/0.10
BUCARAMANGA(config-subif)#encapsulation dot1q 10
BUCARAMANGA(config-subif)#ip add 172.31.0.1 255.255.255.192
BUCARAMANGA(config-subif)#int g0/0.30
BUCARAMANGA(config-subif)#encapsulation dot1q 30
BUCARAMANGA(config-subif)#ip add 172.31.0.65 255.255.255.192
BUCARAMANGA(config-subif)#int g0/0
BUCARAMANGA(config-if)#no shutdown
```

LEVANTADO INTERFAZ Y ASIGNADO IP

```
BUCARAMANGA(config-if)#int serial 0/1/0
BUCARAMANGA(config-if)#ip address 172.31.2.34 255.255.255.252
BUCARAMANGA(config-if)#no shutdown
```

2.1.2 CONFIGURACION DEL PROTOCOLO OSPF

```
BUCARAMANGA(config-if)#router ospf 1
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)#end
```

2.1.3 AUTENTICACIÓN LOCAL CON AAA.

```
BUCARAMANGA(config)#username admin secret 12345
BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#aaa authentication login AAA-LOGIN local
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#login authentication AAA-LOGIN
BUCARAMANGA(config-line)#line vty 0 4
BUCARAMANGA(config-line)#login authentication AAA-LOGIN
```

2.1.4 Un máximo de internos para acceder al router Y Máximo tiempo de acceso al detectar ataques

```
BUCARAMANGA(config)#login block-for 10 attempts 3 within 60
```

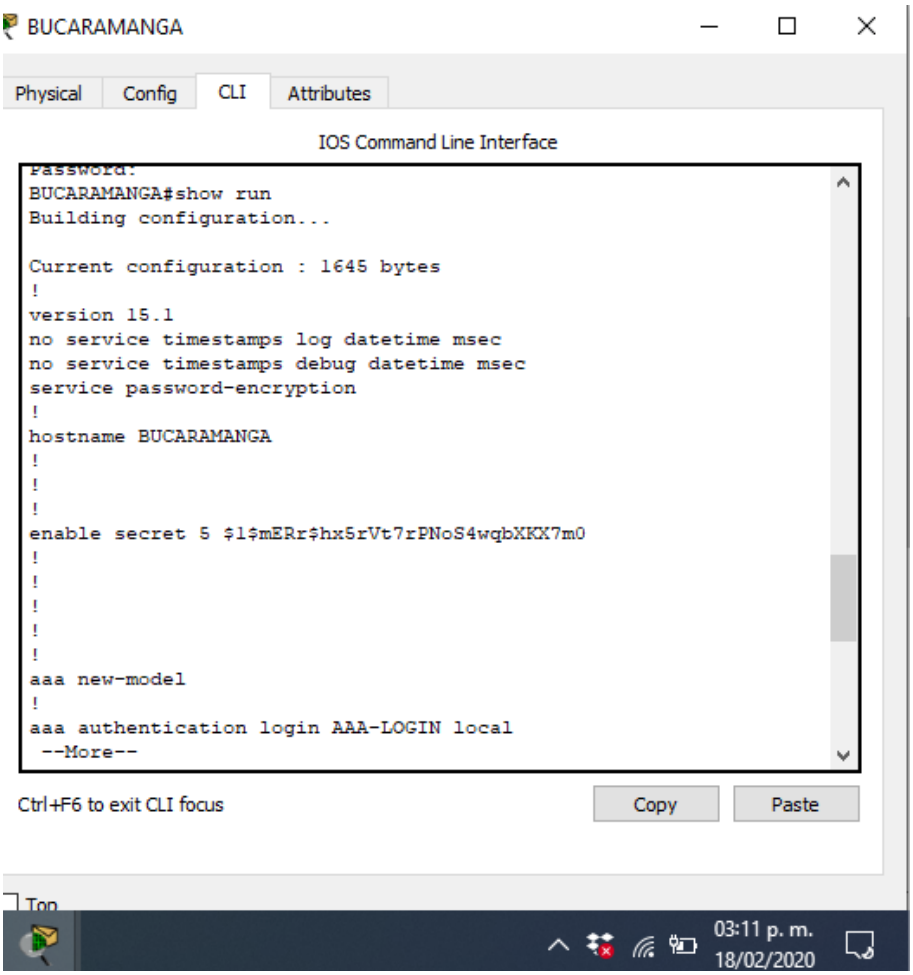


Figura 20.Verificación autenticación AAA router Bucaramanga

2.2 CONFIGURACION BASICA ROUTER TUNJA

Router>enable

Router#conf t

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

Router(config)#hostname TUNJA

```
TUNJA(config)#enable secret cisco
TUNJA(config)#no ip domain-lookup
TUNJA(config)#line console 0
TUNJA(config-line)#password cisco
TUNJA(config-line)#login
TUNJA(config-line)#exit
TUNJA(config)#line vty 0 4
TUNJA(config-line)#password cisco
TUNJA(config-line)#login
TUNJA(config-line)#exit
TUNJA(config)#banner motd #TUNJA ACCESO A PERSONAL AUTORIZADO#
TUNJA(config)#exit
TUNJA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
TUNJA#
```

2.2.1 CONFIGURACION INTERFACES Y SERIALES DEL ROUTER TUNJA

```
TUNJA(config)#int s0/1/0
TUNJA(config-if)#ip add 172.31.2.33 255.255.255.252
TUNJA(config-if)#no shu
TUNJA(config-if)#exit

TUNJA(config)#int s0/1/1
TUNJA(config-if)#ip address 172.31.2.37 255.255.255.252
TUNJA(config-if)#no sh
TUNJA(config-if)#exit
```

TUNJA(config)#int g0/0.1
TUNJA(config-subif)#encapsulation dot1q 1
TUNJA(config-subif)#ip address 172.3.2.9 255.255.255.248
TUNJA(config-subif)#int g0/0.20
TUNJA(config-subif)#encapsulation dot1q 20
TUNJA(config-subif)#ip address 172.31.0.129 255.255.255.192
TUNJA(config-subif)#int g0/0.30
TUNJA(config-subif)#encapsulation dot1q 30
TUNJA(config-subif)#ip address 172.31.0.193 255.255.255.192
TUNJA(config-subif)#int g0/0
TUNJA(config-if)#no sh
TUNJA(config-if)#exit

- Levantando interfaz

TUNJA(config)#int g0/1
TUNJA(config-if)#ip address 209.165.220.1 255.255.255.0
TUNJA(config-if)#no sh
TUNJA (config-if)#exit

2.2.2. PROTOCOLO OSPF
(BASES DE DATOS ENTRE ROUTER PARA SOLUCIÓN LAS TRANSFERENCIAS EN CASO DE QUE ALGUNO FALLE).

TUNJA(config-if)#router ospf 1
TUNJA(config-router)#network 172.3.2.8 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)#end

2.2.3 AUTENTICACIÓN LOCAL AAA Y VERIFICACIÓN

TUNJA#conf t

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

TUNJA(config)#username admin secret 12345

TUNJA(config)#aaa new-model

TUNJA(config)#aaa authentication login AAA-LOGIN local

TUNJA(config)#line console 0

TUNJA(config-line)#login authentication AAA-LOGIN

TUNJA(config-line)#line vty 0 4

TUNJA(config-line)#login authentication AAA-LOGIN

TUNJA(config-line)#exit

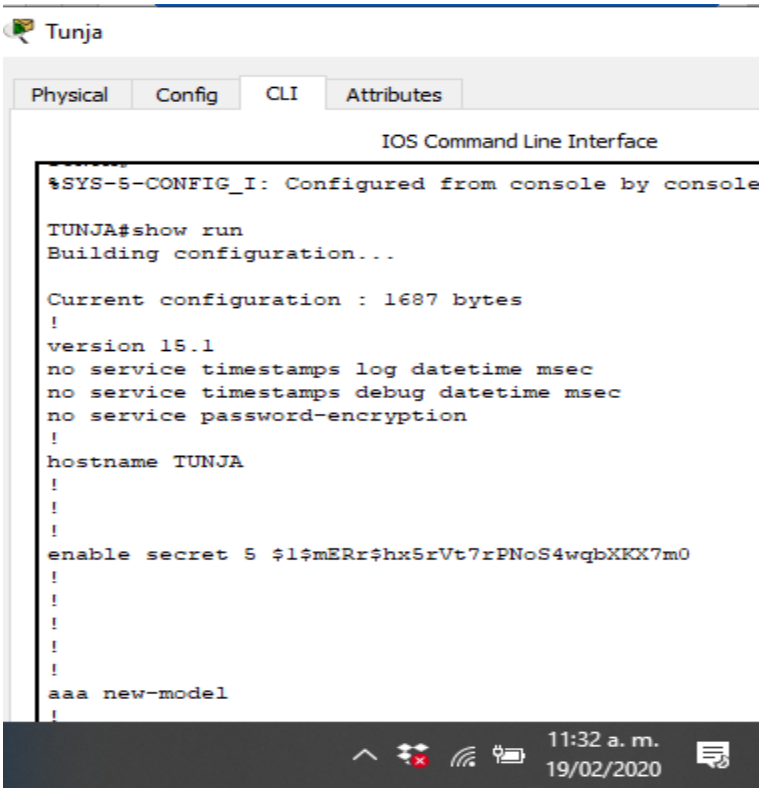


Figura 21. Verificación autenticación AAA router TUNJA

2.2.4 MAXIMO DE INTENTOS Y TIEMPO PARA ACCEDER Y DETECTAR ATAQUES.

TUNJA(config)#login block-for 10 attempts 4 within 60

2.3 CONFIGURACION ROUTER CUNDINAMARCA

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CUNDINAMARCA
CUNDINAMARCA(config)#enable secret cisco
CUNDINAMARCA(config)#service password-encryption
CUNDINAMARCA(config)#no ip domain-lookup
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#password cisco
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#line vty 0 4
CUNDINAMARCA(config-line)#password cisco
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#exit
CUNDINAMARCA(config)#banner motd #CUNDINAMARCA, PROHIBIDO PERSONA NO AUTORIZADO#
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
CUNDINAMARCA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

2.3.1 INTERFACCES Y SERIALES CUNDINAMARCA

CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#int g0/0.1
CUNDINAMARCA(config-subif)#encapsulation dot1q 1
CUNDINAMARCA(config-subif)#ip address 172.31.2.9 255.255.255.248
CUNDINAMARCA(config-subif)#int g0/0.20
CUNDINAMARCA(config-subif)#encapsulation dot1q 20
CUNDINAMARCA(config-subif)#ip address 172.31.1.65 255.255.255.192
CUNDINAMARCA(config-subif)#int g0/0.30
CUNDINAMARCA(config-subif)#encapsulation dot1q 30
CUNDINAMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192
CUNDINAMARCA(config-subif)#int g0/0.88
CUNDINAMARCA(config-subif)#encapsulation dot1q 88
CUNDINAMARCA(config-subif)#ip address 172.31.2.25 255.255.255.248
CUNDINAMARCA(config-subif)#int g0/0
CUNDINAMARCA(config-if)#no sh

- Levantando interface de cundinamarca hacia tunja

CUNDINAMARCA(config-if)#int s0/1/0
CUNDINAMARCA(config-if)#ip address 172.31.2.38 255.255.255.252
CUNDINAMARCA(config-if)#no sh

2.3.2 ENRUTAMIENTO OSPF DE CUNDINAMARCA

CUNDINAMARCA(config)#router ospf 1
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 172.31.2.8 0.0.0.7 area 0
CUNDINAMARCA(config-router)#network 172.31.2.24 0.0.0.7 area 0

CUNDINAMARCA(config-router)#network 172.31.2.36 0.0.0.3 area 0
CUNDINAMARCA(config-router)#
CUNDINAMARCA(config-router)#end
CUNDINAMARCA#

2.3.3 AUTENTICACON LOCAL AAA CUNDINAMARCA Y VERIFICACION

CUNDINAMARCA(config)#username admin secret 12345
CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#aaa authentication login AAA-LOGIN local
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#login authentication AAA-LOGIN
CUNDINAMARCA(config-line)#line vty 0 4
CUNDINAMARCA(config-line)#login authentication AAA-LOGIN
CUNDINAMARCA(config-line)#exit

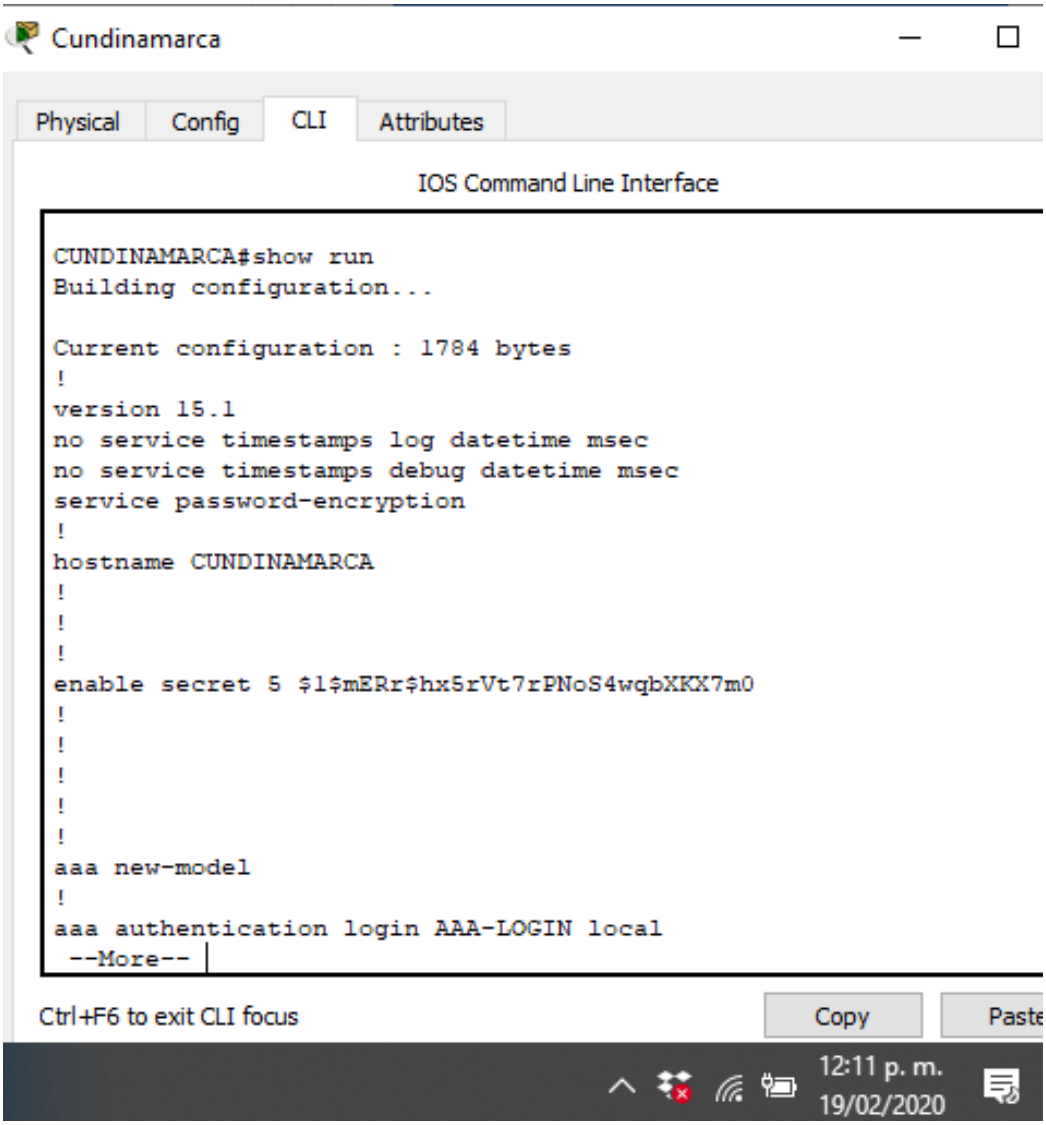


Figura 22. Verificación autenticación AAA router Cundinamarca

2.3.4 CONFIGURACIÓN MÁXIMO DE INTENTO Y TIEMPO PARA ACCEDER Y DETECTAR ATAQUES

CUNDINAMARCA(config)#login block-for 10 attempts 4 within 60

2.4 CONFIGURACION DE SWITCH Y VLANS

Configuraciones del switch Bucaramanga

Switch>enable
Switch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SWbucaramanga
SWbucaramanga(config)#enable password cisco
SWbucaramanga(config)#line console 0
SWbucaramanga(config-line)#exec-timeout 6 0
SWbucaramanga(config-line)#logging synchronous
SWbucaramanga(config-line)#password cisco
SWbucaramanga(config-line)#login
SWbucaramanga(config-line)#line vty 0 15
SWbucaramanga(config-line)#exec-timeout 6 0
SWbucaramanga(config-line)#logging synchronous
SWbucaramanga(config-line)#password cisco
SWbucaramanga(config-line)#login
SWbucaramanga(config-line)#exit
SWbucaramanga(config)#

- CONFIGURACION DE VLANS SWITCH

SWbucaramanga>ena
Password:
SWbucaramanga#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SWbucaramanga(config)#vlan 1
SWbucaramanga(config-vlan)#vlan 10
SWbucaramanga(config-vlan)#vlan 30

```
SWbucaramanga(config-vlan)#int f0/1
SWbucaramanga(config-if)#switchport mode access
SWbucaramanga(config-if)#switchport access vlan 10
SWbucaramanga(config-if)#int f0/2
SWbucaramanga(config-if)#switchport mode access
SWbucaramanga(config-if)#switchport access vlan 30
SWbucaramanga(config-if)#int g0/1
SWbucaramanga(config-if)#switchport mode trunk
SWbucaramanga(config-if)#int vlan 1
SWbucaramanga(config-if)#ip address 172.31.2.3 255.255.255.248
SWbucaramanga(config-if)#no shutdown

SWbucaramanga(config-if)#ip default-gateway 172.31.2.1
```

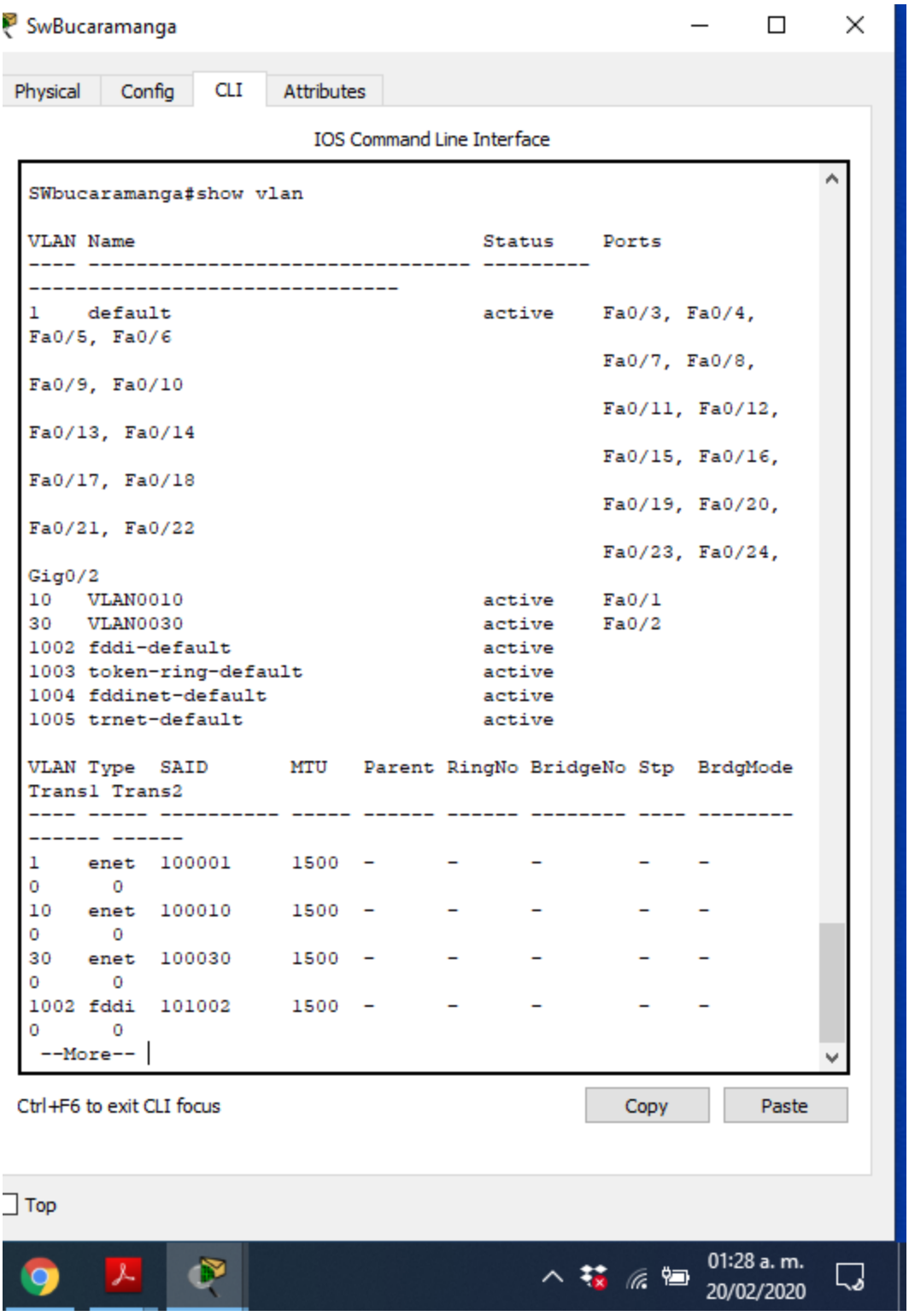


Figura 23. Switch y Vlans Bucaramanga

- **Configuraciones del switch Tunja**

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SWTunja
SWTunja(config)#enable password cisco
SWTunja(config)#line console 0
SWTunja(config-line)#exec-timeout 6 0
SWTunja(config-line)#logging synchronous
SWTunja(config-line)#password cisco
SWTunja(config-line)#login
SWTunja(config-line)#line vty 0 15
SWTunja(config-line)#exec-timeout 6 0
SWTunja(config-line)#logging synchronous
SWTunja(config-line)#password cisco
SWTunja(config-line)#login
SWTunja(config-line)#exit
SWTunja(config)#exit
SWTunja#
SWTunja#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

- VLANS SWITCH TUNJA

```
SWTunja>enable
Password:
SWTunja#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
SWTunja(config)#vlan 1
SWTunja(config-vlan)#vlan 20
SWTunja(config-vlan)#vlan 30
SWTunja(config-vlan)#int f0/1
SWTunja(config-if)#switchport mode access
SWTunja(config-if)#switchport access vlan 20
SWTunja(config-if)#int f0/2
SWTunja(config-if)#switchport mode access
SWTunja(config-if)#switchport access vlan 30
SWTunja(config-if)#int g0/1
SWTunja(config-if)#switchport mode trunk
SWTunja(config-if)#int vlan 1
SWTunja(config-if)#ip address 172.3.2.11 255.255.255.248
SWTunja(config-if)#no shutdown
SWTunja(config-if)#ip default-gateway 172.3.2.9
```

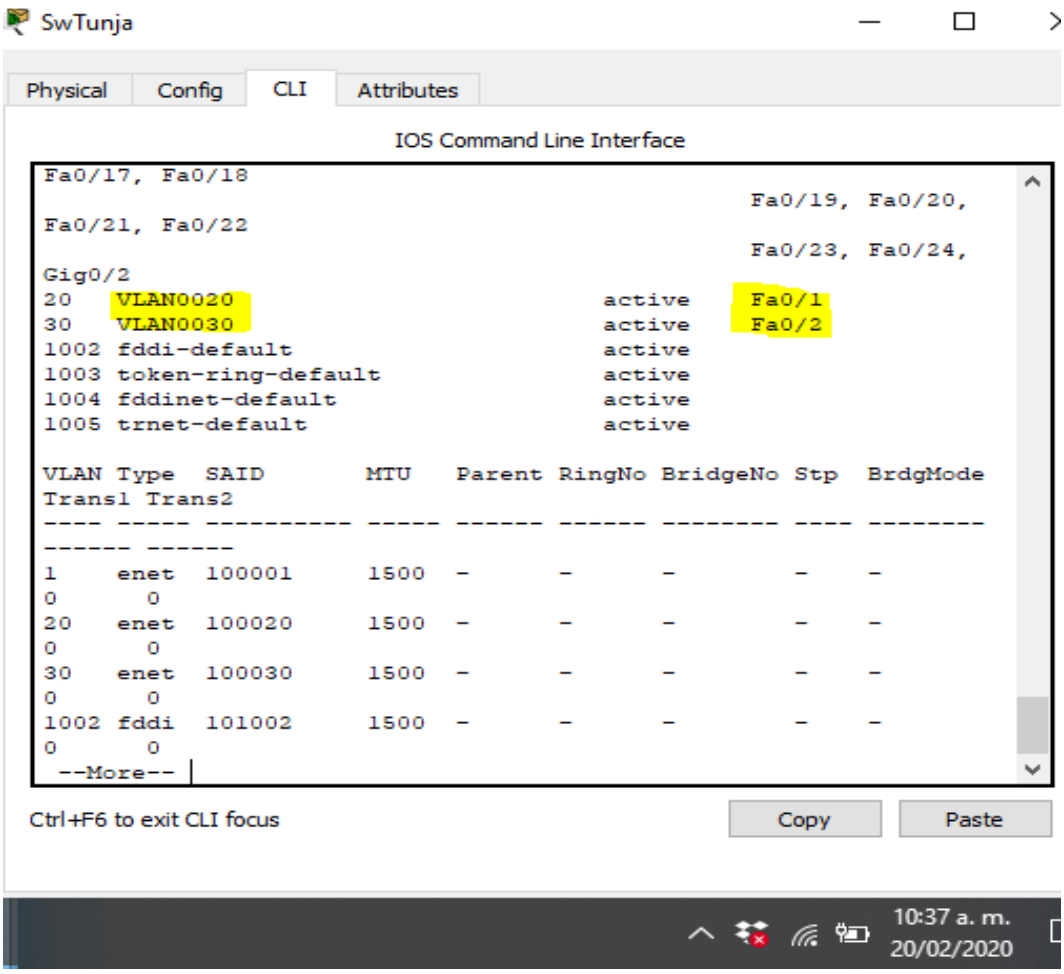


Figura 24. Switch y Vlans Tunja

Configuraciones switch Cundinamarca

Switch#conf t

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

Switch(config)#hostname SWcundinamarca

SWcundinamarca(config)#enable password cisco

SWcundinamarca(config)#line console 0

SWcundinamarca(config-line)#exec-timeout 6 0

SWcundinamarca(config-line)#logging synchronous

SWcundinamarca(config-line)#password cisco

SWcundinamarca(config-line)#login

SWcundinamarca(config-line)#line vty 0 15
SWcundinamarca(config-line)#exec-timeout 6 0
SWcundinamarca(config-line)#logging synchronous
SWcundinamarca(config-line)#password cisco
SWcundinamarca(config-line)#login
SWcundinamarca(config-line)#exit
SWcundinamarca(config)#exit
SWcundinamarca#
SWcundinamarca#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

- **Vlans switch**

Password:
SWcundinamarca#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SWcundinamarca(config)#vlan 20
SWcundinamarca(config-vlan)#vlan 30
SWcundinamarca(config-vlan)#vlan 88
SWcundinamarca(config-vlan)#exit
SWcundinamarca(config)#int f0/1
SWcundinamarca(config-if)#switchport mode access
SWcundinamarca(config-if)#switchport access vlan 20
SWcundinamarca(config-if)#int fa0/2
SWcundinamarca(config-if)#switchport mode access
SWcundinamarca(config-if)#switchport access vlan 30
SWcundinamarca(config-if)#int fa0/3
SWcundinamarca(config-if)#switchport mode access
SWcundinamarca(config-if)#switchport access vlan 88

SWcundinamarca(config-if)#int g0/1

SWcundinamarca(config-if)#switchport mode trunk

SWcundinamarca(config-if)#int vlan 1

SWcundinamarca(config-if)#ip address 172.31.2.11 255.255.255.248

SWcundinamarca(config-if)#no sh

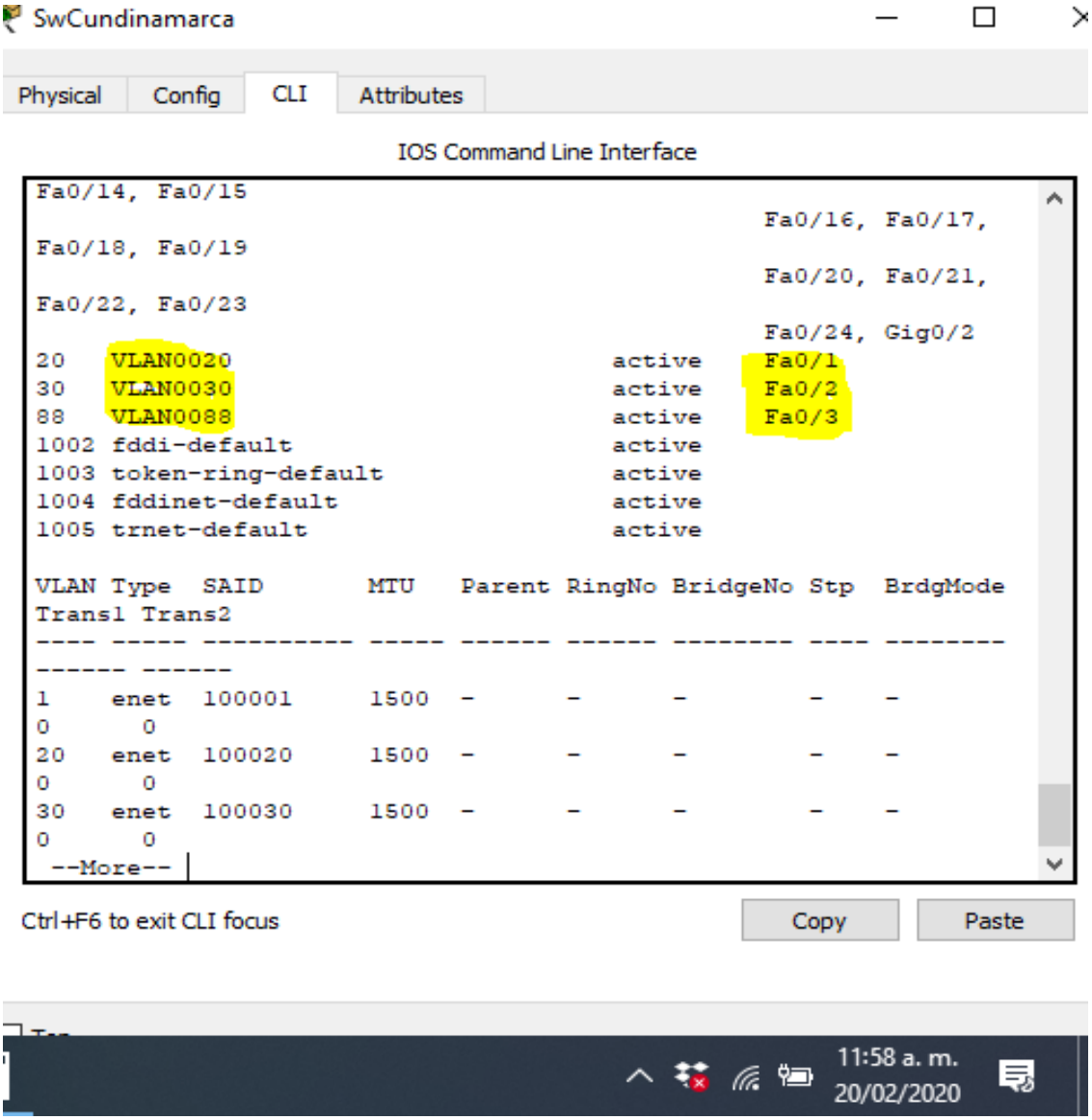


Figura 25. Switch y Vlans Cundinamarca

2.5 SERVIDOR TFTP.

Web interno y almacenamiento de archivos de routers.

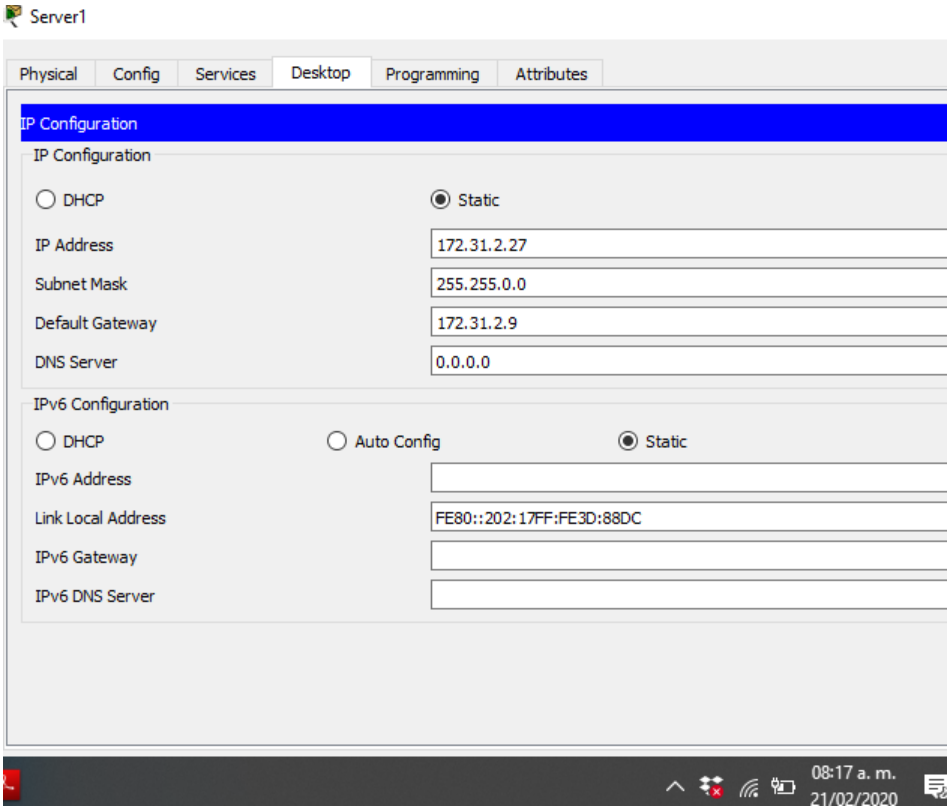


Figura 26. Asignando Ip al server

- CONFIGURACION SERVER. COPIANDO ARCHIVOS

CUNDINAMARCA#ping 172.31.2.27

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.31.2.27, timeout is 2 seconds:

.

Success rate is 80 percent (4/5), round-trip min/avg/max = 0/1/4 ms

CUNDINAMARCA#copy running-config tftp

Address or name of remote host []? 172.31.2.27

Destination filename [CUNDINAMARCA-confg]?

Writing running-config...!!

[OK - 1962 bytes]

TUNJA#copy running-config tftp
Address or name of remote host []? 172.31.2.27
Destination filename [TUNJA-confg]?

Writing running-config...!!
[OK - 1865 bytes]

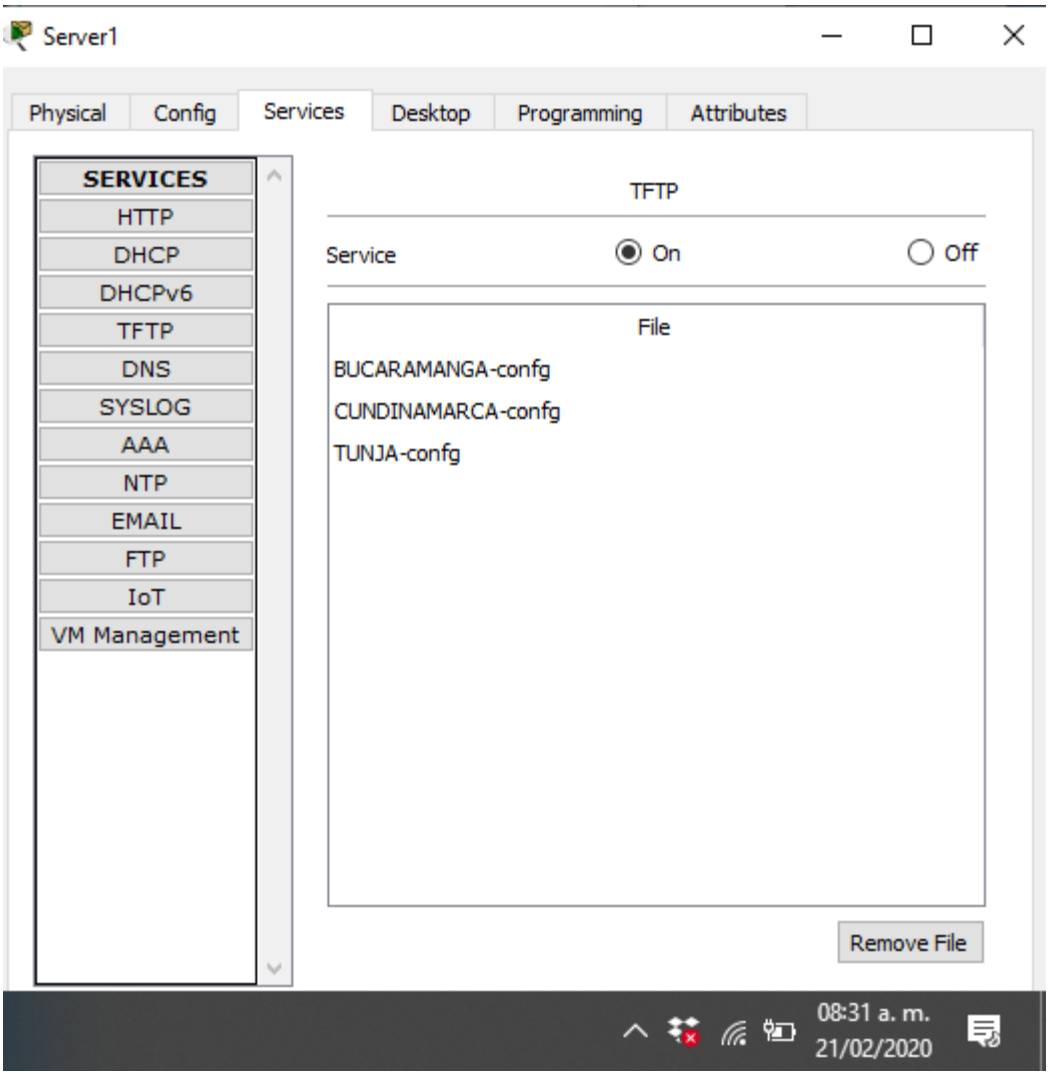


Figura 26. Verificacion archivos Copiados de las redes.

2.6 Proporcionando solo direcciones a los hosts de Bucaramanga y Cundinamarca

SOLO PERSONAL AUTORIZADO
User Access Verification
Username: admin
Password:
BUCARAMANGA>enable
Password:
BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#interface g0/0.10
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.33
BUCARAMANGA(config-subif)#int g0/0.30
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.33
BUCARAMANGA(config-subif)#exit
BUCARAMANGA(config)#

CUNDINAMARCA, PROHIBIDO PERSONA NO AUTORIZADO
User Access Verification
Username: admin
Password:
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#int g0/0.20
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#int g0/0.30

CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#exit
CUNDINAMARCA(config)#

TUNJA ACCESO A PERSONAL AUTORIZADO

User Access Verification

Username: admin
Password:
TUNJA>enable
Password:
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#ip dhcp excluded-address 172.31.0.1 172.31.0.4
TUNJA(config)#ip dhcp excluded-address 172.31.0.65 172.31.0.68
TUNJA(config)#ip dhcp excluded-address 172.31.1.65 172.31.1.68
TUNJA(config)#ip dhcp excluded-address 172.31.1.1 172.31.1.4
TUNJA(config)#ip dhcp pool vlan10B
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 172.31.2.27
TUNJA(dhcp-config)#ip dhcp pool vlan30B
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 172.31.2.27
TUNJA(config)#ip dhcp pool vlan20C
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 172.31.2.27
TUNJA(dhcp-config)#ip dhcp pool vlan30C
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 172.31.2.27
TUNJA(dhcp-config)#exit
TUNJA(config)#

2.7 SERVIDOR CON NAT Y PAT

Web server con NAT estático y equipos con NAT de sobrecarga (PAT).

TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#ip nat inside source static 172.31.2.27 209.165.220.10
TUNJA(config)#ip access-list standard NAT-ACL
TUNJA(config-std-nacl)#permit 172.31.0.0 0.0.255.255
TUNJA(config-std-nacl)#ip nat inside source list NAT-ACL interface g0/1 overload
TUNJA(config)#int g0/1
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#int g0/0.1
TUNJA(config-subif)#ip nat inside
TUNJA(config-subif)#int g0/0.20
TUNJA(config-subif)#ip nat inside
TUNJA(config-subif)#int g0/0.30
TUNJA(config-subif)#ip nat inside
TUNJA(config-subif)#int s0/1/0
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#int s0/1/1
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit

TUNJA(config)#ip route 0.0.0.0 0.0.0.0 209.165.220.5

TUNJA(config)#router ospf 1

TUNJA(config-router)#default-information originate

TUNJA(config-router)#exit

TUNJA#wr

Building configuration...

[OK]

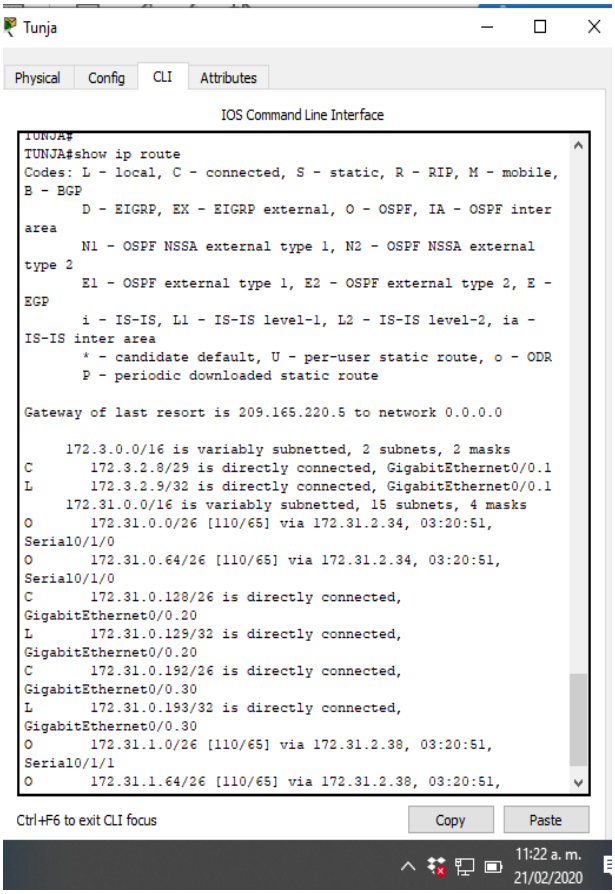


Figura 27.Configuración NAT router Tunja.

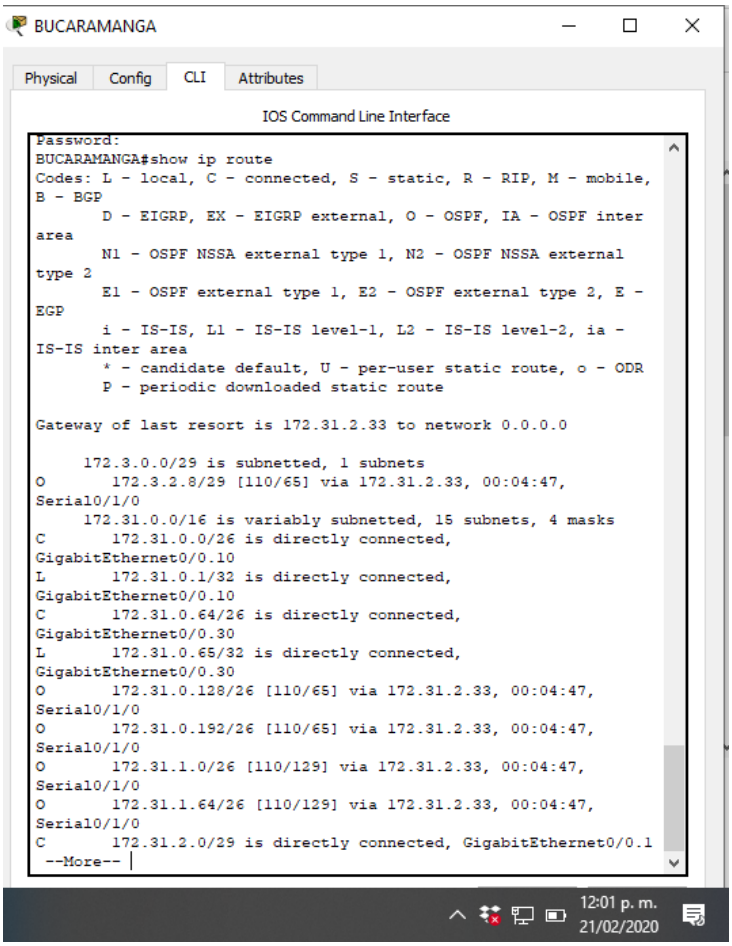


Figura 28.Configuración NAT router Bucaramanga

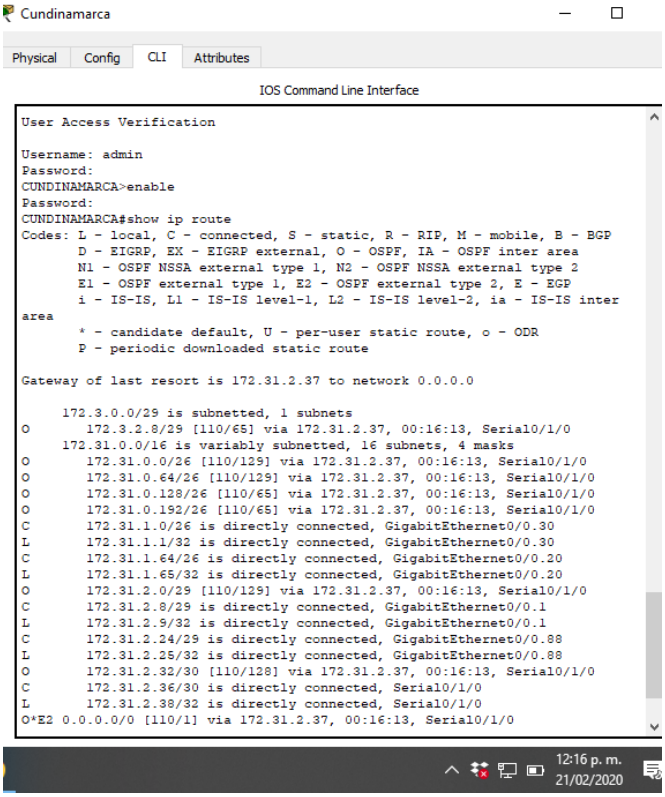


Figura 29. Configuración NAT router Cundinamarca

2.8 El enrutamiento deberá tener autenticación.

BUCARAMANGA#config t

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

BUCARAMANGA(config)#int s0/1/0

BUCARAMANGA(config-if)#ip ospf authentication message-digest

BUCARAMANGA(config-if)#ip ospf message-digest-key 1 md5 ospfospf

BUCARAMANGA(config-if)#exit

BUCARAMANGA(config)#end

BUCARAMANGA#

TUNJA#conf t

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

TUNJA(config)#interface s0/1/0

TUNJA(config-if)#ip ospf authentication message-digest
TUNJA(config-if)#ip ospf message-digest-key 1 md5 ospfospf
TUNJA(config-if)#
09:20:54: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/1/0 from LOADING to FULL, Loading Done

TUNJA(config-if)#interface s0/1/1
TUNJA(config-if)#ip ospf authentication message-digest
TUNJA(config-if)#ip ospf message-digest-key 1 md5 ospfospf
TUNJA(config-if)#end

CUNDINAMARCA(config)#interface s0/1/0
CUNDINAMARCA(config-if)#ip ospf authentication message-digest
CUNDINAMARCA(config-if)#ip ospf message-digest-key 1 md5 ospfospf
CUNDINAMARCA(config-if)#end

2.9 Listas de control de acceso

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

Username: admin
Password:
CUNDINAMARCA>enable
Password:
CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#access-list 152 deny ip 172.31.1.64 0.0.0.63 209.165.220.0 0.0.0.255
CUNDINAMARCA(config)#access-list 152 permit udp any any eq bootps

CUNDINAMARCA(config)#access-list 152 permit ip any any
CUNDINAMARCA(config)#int g0/0.20
CUNDINAMARCA(config-subif)#ip access-group 152 in
CUNDINAMARCA(config-subif)#end

Los hosts de VLAN 30 en Cundinamarca si acceden a internet y no a la red interna de Tunja.

CUNDINAMARCA#conf t
CUNDINAMARCA(config)#access-list 153 permit tcp 172.31.1.0 0.0.0.63 host 209.165.220.5 eq 80
CUNDINAMARCA(config)#access-list 153 deny ip any any
CUNDINAMARCA(config)#int g0/0.30
CUNDINAMARCA(config-subif)#ip access-group 153 in
CUNDINAMARCA(config-subif)#exit
CUNDINAMARCA(config)#

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

TUNJA>enable
Password:
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#access-list 152 permit tcp 172.31.0.192 0.0.0.63 209.165.220.5 0.0.0.255 eq 80

TUNJA(config)#access-list 152 permit tcp 172.31.0.192 0.0.0.63 209.165.220.5 0.0.0.255 eq 21
TUNJA(config)#int g0/0.30
TUNJA(config-subif)#ip access-group 152 in
TUNJA(config-subif)#exit
TUNJA(config)#

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

TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#access-list 153 permit ip 172.31.0.128 0.0.0.63 172.31.1.64 0.0.0.63
TUNJA(config)#access-list 153 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
TUNJA(config)#int g0/0.20
TUNJA(config-subif)#ip access-group 153 in
TUNJA(config-subif)#exit

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

BUCARAMANGA(config)#access-list 152 permit tcp 172.31.0.64 0.0.0.63 host 209.165.220.5 eq 80
BUCARAMANGA(config)#int g0/0.30
BUCARAMANGA(config-subif)#ip access-group 152 in
BUCARAMANGA(config-subif)#exit
BUCARAMANGA(config)#access-list 153 permit ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.0.63
BUCARAMANGA(config)#access-list 153 deny ip any any

```
BUCARAMANGA(config)#int g0/0.30
BUCARAMANGA(config-subif)#ip access-group 153 in
BUCARAMANGA(config-subif)#end
BUCARAMANGA#
```

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

```
BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#access-list 152 permit ip 172.31.0.0 0.0.0.63 172.31.1.64
0.0.0.63
BUCARAMANGA(config)#access-list 152 permit ip 172.31.0.0 0.0.0.63 172.31.0.128
0.0.0.63
BUCARAMANGA(config)#int g0/0.10
BUCARAMANGA(config-subif)#ip access-group 152 in
BUCARAMANGA(config-subif)#end
```

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

```
BUCARAMANGA(config)#access-list 153 deny ip 172.31.2.0 0.0.0.7 172.31.0.0
0.0.0.63
BUCARAMANGA(config)#access-list 153 deny ip 172.31.0.64 0.0.0.63 172.31.0.0
0.0.0.63
```

```
BUCARAMANGA(config)#access-list 153 permit ip any any
BUCARAMANGA(config)#int g0/0.10
BUCARAMANGA(config-subif)#ip access-group 153 out
BUCARAMANGA(config-subif)#end
```

```
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#access-list 153 deny ip 172.3.2.8 0.0.0.7 172.31.0.128 0.0.0.63
TUNJA(config)#access-list 153 deny ip 172.3.0.192 0.0.0.63 172.31.0.128 0.0.0.63
TUNJA(config)#access-list 153 permit ip any any
TUNJA(config)#int g0/0.20
TUNJA(config-subif)#ip access-group 153 out
TUNJA(config-subif)#end
```

```
CUNDINAMARCA#config t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#access-list 153 deny ip 172.31.2.8 0.0.0.7 172.31.1.64
0.0.0.63
CUNDINAMARCA(config)#access-list 153 deny ip 172.31.1.0 0.0.0.63 172.31.1.64
0.0.0.63
CUNDINAMARCA(config)#access-list 153 deny ip 172.31.2.24 0.0.0.7 172.31.1.64
0.0.0.63
CUNDINAMARCA(config)#access-list 153 permit ip any any
CUNDINAMARCA(config)#int g0/0.20
CUNDINAMARCA(config-subif)#ip access-group 153 out
CUNDINAMARCA(config-subif)#end
```

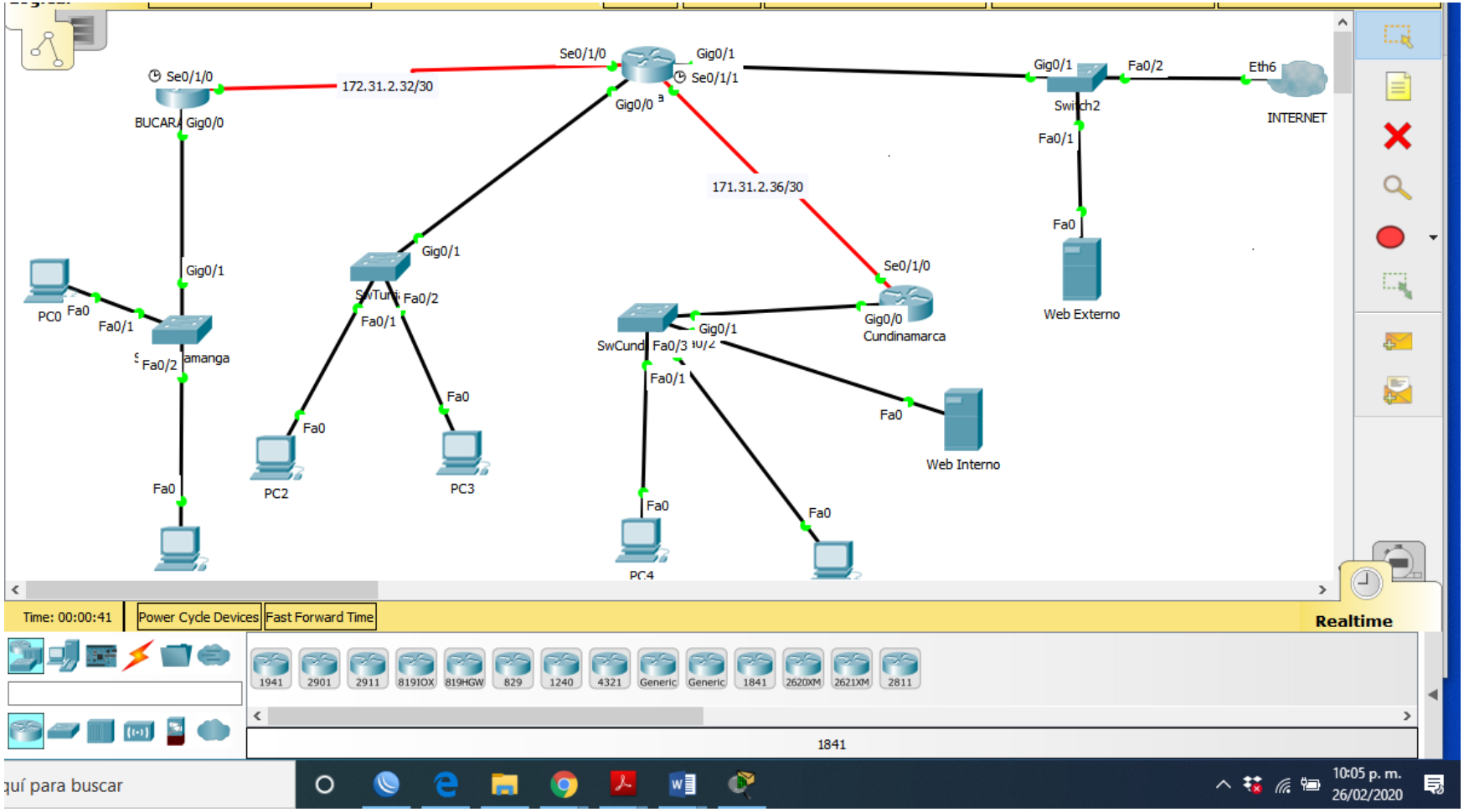
- Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los routers e internet.

```
BUCARAMANGA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#access-list 9 permit 172.31.2.0 0.0.0.7
BUCARAMANGA(config)#access-list 9 permit 172.3.2.8 0.0.0.7
BUCARAMANGA(config)#access-list 9 permit 172.31.2.8 0.0.0.7
BUCARAMANGA(config)#line vty 0 4
BUCARAMANGA(config-line)#access-class 9 in
BUCARAMANGA(config-line)#end
BUCARAMANGA#

TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#access-list 9 permit 172.31.2.0 0.0.0.7
TUNJA(config)#access-list 9 permit 172.3.2.8 0.0.0.7
TUNJA(config)#access-list 9 permit 172.31.2.8 0.0.0.7
TUNJA(config)#line vty 0 4
TUNJA(config-line)#access-class 9 in
TUNJA(config-line)#end
TUNJA#

CUNDINAMARCA(config)#access-list 9 permit 172.31.2.0 0.0.0.7
CUNDINAMARCA(config)#access-list 9 permit 172.3.2.8 0.0.0.7
CUNDINAMARCA(config)#access-list 9 permit 172.31.2.8 0.0.0.7
CUNDINAMARCA(config)#line vty 0 4
CUNDINAMARCA(config-line)#access-class 9 in
CUNDINAMARCA(config-line)#end
```

TOPOLOGIA ESCENARIO DOS



CONCLUSIONES

Durante el desarrollo de esta última actividad práctica se ha logrado poner en práctica diferentes conceptos y procedimientos que han sido parte de la temática desarrollada durante el curso.

Dentro de esta práctica se han llevado a cabo temas de vital importancia en la configuración de una red como lo son el direccionamiento IP, la creación de subredes, las conexiones físicas de los diferentes equipos que hacen parte de la red, la configuración de routers y demás temas necesarios para el correcto funcionamiento de la red.

En este se observó un adecuado aprendizaje de los diferentes comandos que se aprendieron en el transcurso del diplomado y se obtuvieron conceptos mucho más claros para el diseño de una red, utilizando estos durante las prácticas en Packet Tracert.

Bibliografía

Lopez, G. d. (Productor). (2016). *Configuración del protocolo de enrutamiento EIGRP en packet tracer 2/2* [Video]. Recuperado el 10 de Diciembre de 2019, de https://www.youtube.com/watch?v=7nZoXD8g20w

Guzman, D. P. (Productor). (2017). *Protocolo EIGRP con Balanceo de Carga* [Video]. Recuperado el 09 de Diciembre de 2019, de https://www.youtube.com/watch?v=efhdC8b6M7c

Gerometta, O. (2017). *http://librosnetworking.blogspot.com/.* Recuperado el 09 de Diciembre de 2019, de http://librosnetworking.blogspot.com/2017/12/comandos-show-ip-route.html

clara, g. L. (24 de mayo de 2014). *https://www.youtube.com/*. (g. L. clara, Productor) Recuperado el 2019, de https://www.youtube.com/watch?v=kZq_xICNSGQ

Gerometta, O. (2017). *http://librosnetworking.blogspot.com/.* Recuperado el 09 de Diciembre de 2019, de http://librosnetworking.blogspot.com/2017/12/comandos-show-ip-route.html

clara, g. L. (24 de mayo de 2014). *https://www.youtube.com/*. (g. L. clara, Productor) Recuperado el 2019, de https://www.youtube.com/watch?v=kZq_xICNSGQ

Gerometta, O. (2017). *http://librosnetworking.blogspot.com.* Recuperado el 11 de Diciembre de 2019, de http://librosnetworking.blogspot.com/2018/03/comandos-show-cdp-neighbors.html

CISCO NETWORKING. (21 de Agosto de 2013). *Comandos de configuracion de dispositivos cisco.* (slideshare, Ed.) Recuperado el 11 de Diciembre de 2019, de https://es.slideshare.net/samuelhuertasorjuela/comandos-de-configuracion-de-dispositivos-cisco