

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

Evaluación – Prueba de habilidades prácticas CCNA

Presentado a:

Ingeniero Giovanni Alberto Bracho

Estudiante:

Sebastian Muñoz Artunduaga

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
INGENIERIA DE SISTEMAS
LA PRIMAVERA, VICHADA
15 DE DICIEMBRE DEL 2019

TABLA DE CONTENIDO

RESUMEN	3
ABSTRACT	4
INTRODUCCIÓN.....	5
OBJETIVOS	6
DESCRIPCIÓN GENERAL DE LA PRUEBA DE HABILIDADES	7
Escenario 1	8
Parte 1: Asignación de direcciones IP:.....	9
Parte 2: Configuración Básica.....	12
Parte 3: Configuración de Enrutamiento.....	18
Parte 4: Configuración de las listas de Control de Acceso.....	23
Parte 5: Comprobación de la red instalada.....	28
Escenario 2	30
Aspectos a tener en cuenta.....	38
CONCLUSIONES.....	44
BIBLIOGRAFIA.....	45

RESUMEN

Este trabajo se realiza con el objetivo de demostrar de una forma práctica los conocimientos obtenidos en el transcurso del diplomado de Profundización CISCO el cual nos permite diseñar e implementar soluciones integradas LAN/WAN, de esta manera evaluando al estudiante sin cuenta con las habilidades necesarias para la resolución de este tipo de problemas que son los que se ven en la actualidad en el ambiente laboral.

Para el desarrollo de esta actividad contamos con dos escenarios en los cuales se nos permitirá aplicar los conocimientos de configuración de servicios DHCP, RIPv2, enlaces troncales y la implementación de NAT evaluando las competencias al realizar la solución de estas dos prácticas.

ABSTRACT

This work is carried out with the objective of demonstrating in a practical way the knowledge obtained during the course of the CISCO deepening diploma which allows us to design and implement integrated LAN / WAN solutions, thus evaluating the student without the necessary skills to the resolution of these types of problems that are what are currently seen in the work environment.

For the development of this activity we have two scenarios in which we will be able to apply the knowledge of DHCP services configuration, RIPv2, trunk links and the implementation of NAT evaluating the competences when solving these two practices.

INTRODUCCIÓN

En la actualidad se manejan diferentes sistemas de datos en todas las empresas en Colombia brindando un intercambio de información tanto a sus clientes como entre sus empleados por lo que esto conlleva a estructurar redes telemáticas para la interconectividad dando una disponibilidad de la información y comunicación en todo momento, para esto se adquiere una capacitación por medio de la UNAD y CISCO para que el personal de estudiantes sea lo más idóneo para solucionar diferentes problemas y tengan una mayor competitividad en el mercado, permitiendo a los estudiantes capacitarse para acceder a una de las certificaciones más requeridas que es la CCNA la cual garantiza que el profesional cuenta con todas las habilidades necesarias para brindar un soporte técnico óptimo.

En este informe encontraremos la práctica y aplicación del conocimiento adquirido en el transcurso de este diplomado lo que permite al estudiante desenvolverse en un ambiente real dando diferentes soluciones a problemas impartidos lo cual requiere su correcto análisis, comprensión y ejecución, obteniendo de esta manera una retroalimentación por parte del tutor que garantiza que cuenta con las habilidades necesarias para obtener su certificación.

OBJETIVOS

Objetivo general

Por medio de dos escenarios aplicar el conocimiento práctico adquirido en el transcurso del diplomado.

Objetivos específicos

- Establecer la configuración primaria y de seguridad para un router.
- Realizar las configuraciones establecidas para los equipos de switch que conforman cada topología.
- Por medio de distintos comandos verificar el correcto funcionamiento de las topologías para confirmar el funcionamiento.

DESCRIPCIÓN GENERAL DE LA PRUEBA DE HABILIDADES

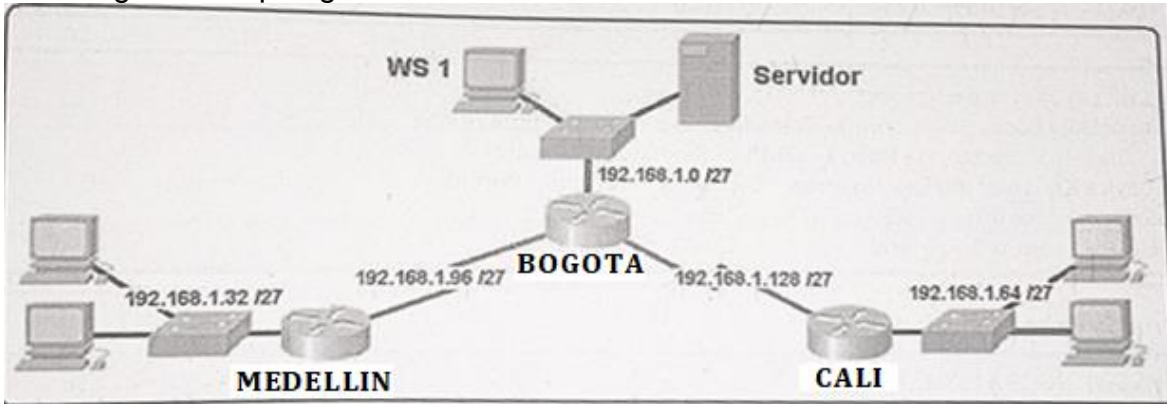
La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para esta actividad, el estudiante dispone de cerca de dos semanas para realizar las tareas asignadas en cada uno de los **dos (2) escenarios propuestos**, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos **ping, traceroute, show ip route, entre otros**.

Teniendo en cuenta que la Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: **Packet Tracer** o **GNS3**.

Escenario 1

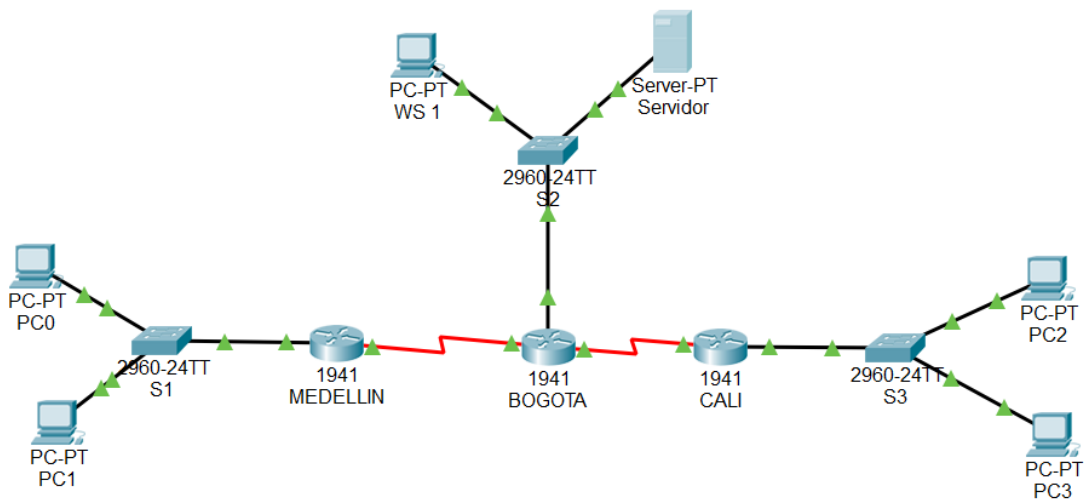
Figura 1. Topología Planteada



Descripción de las actividades

Se realiza la conexión de la topología planteada para el escenario 1 en el simulador packet tracer, con los cables correspondientes para cada dispositivo.

Conexión de Topología Escenario 1



Parte 1: Asignación de direcciones IP:

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

bits prestados = 2^n , donde n es el número de bits

Por ejemplo, si deseamos tener un subneteo de red en ocho partes, se toman 3 N bits:

$$2^n = 2^3 = 8$$

La forma de poder conocer el número de host que cada sub red puede tener como máximo está dado por:

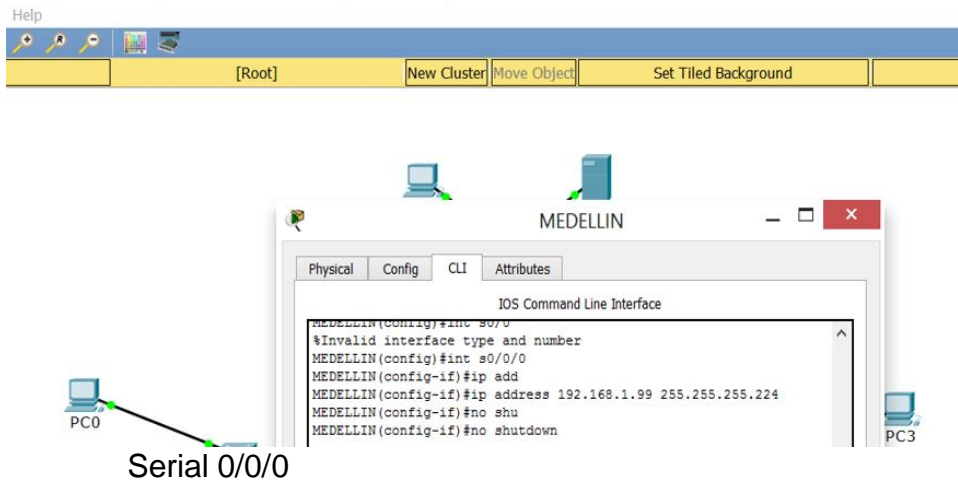
$$2^n - 2 = 2^5 - 2 = 32 - 2 = 30$$

Así las cosas, el siguiente paso es poder crear las ocho tablas respectivas que nos darán las direcciones de cada red para obtener:

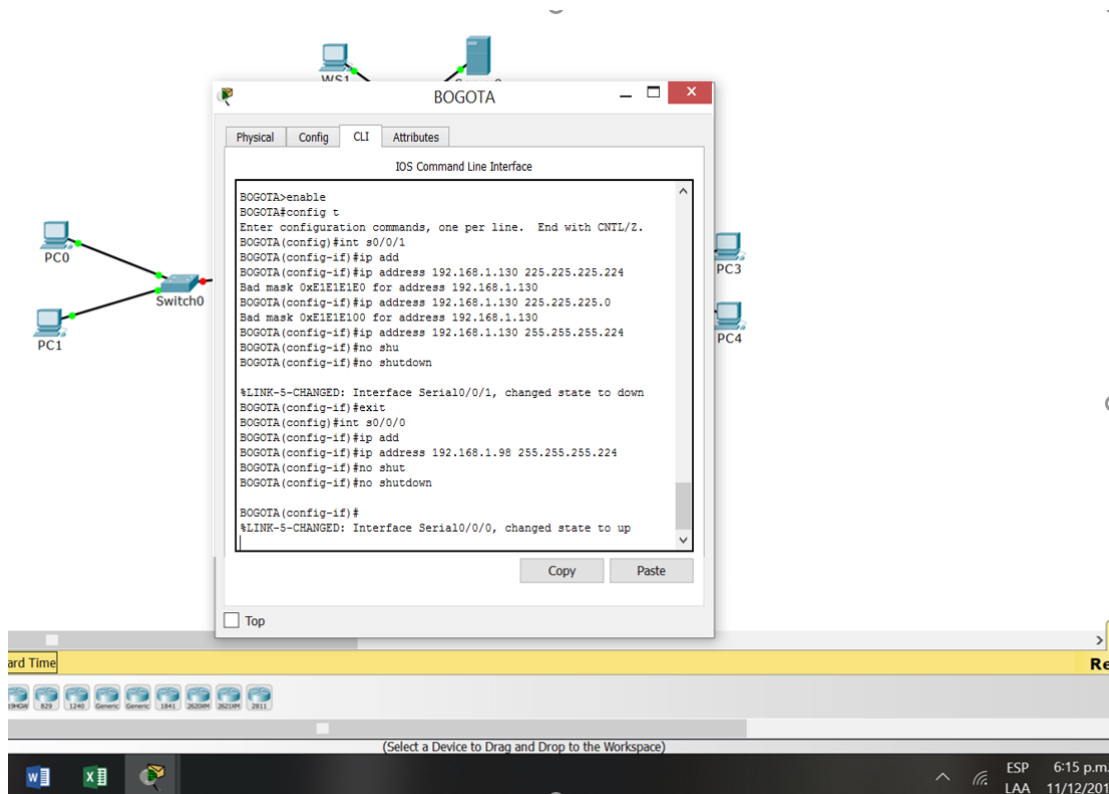
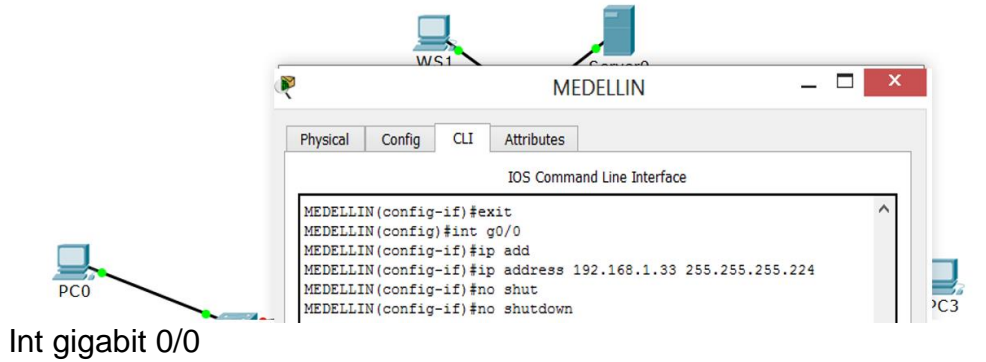
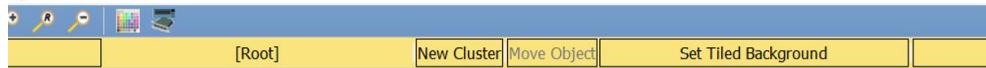
SUBRED	dirección de red	Rango de Host	Dirección de difusión
0	192.168.1.0/27	192.168.1.1 – 192.168.1.30	192.168.1.31
1	192.168.1.32/27	192.168.1.33 – 192.168.1.62	192.168.1.63
2	192.168.1.64/27	192.168.1.65 – 192.168.1.94	192.168.1.95
3	192.168.1.96/27	192.168.1.97 – 192.168.1.126	192.168.1.127
4	192.168.1.128/27	192.168.1.129 – 192.168.1.158	192.168.1.159
5	192.168.1.160/27	192.168.1.161 – 192.168.1.190	192.168.1.191
6	192.168.1.192/27	192.168.1.193 – 192.168.1.222	192.168.1.223
7	192.168.1.224/27	192.168.1.225 – 192.168.1.254	192.168.1.255

b. Asignar una dirección IP a la red.

nents\UNAD 2019-2\DIPLMADO DE CISCO\ESCENARIO 1.pkt



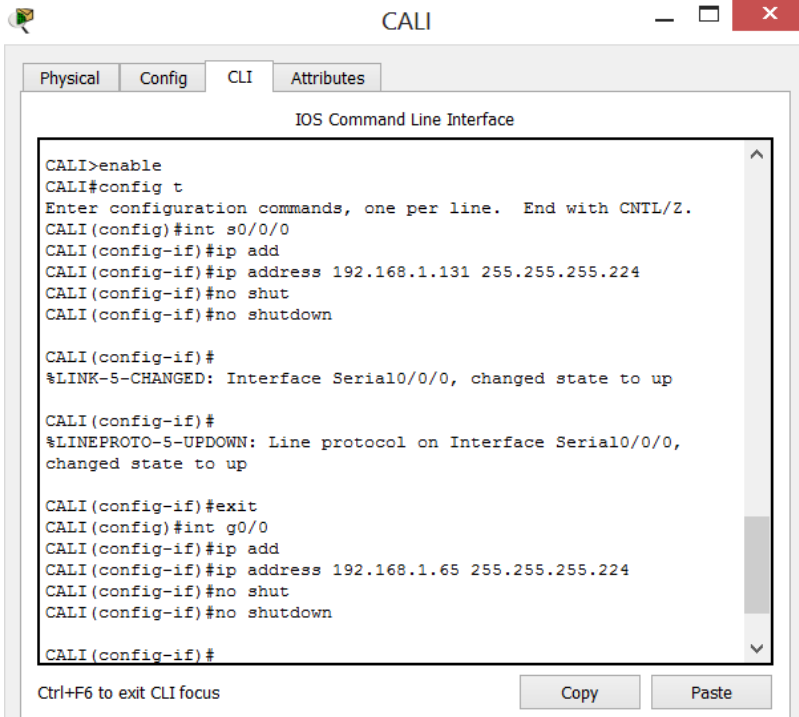
elp



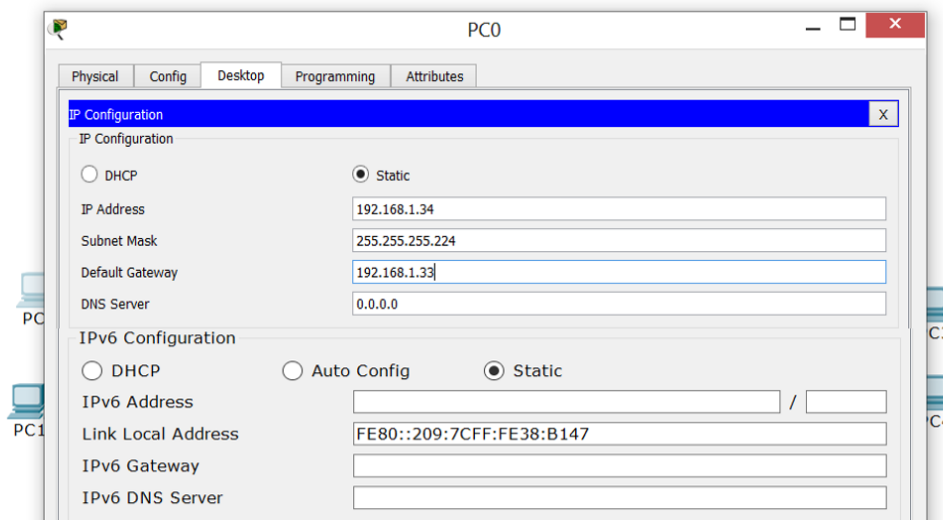
Router Bogotá, puertos serial 0/0 y 0/1

```
BOGOTA(config-if)#exit
BOGOTA(config)#int g0/0
BOGOTA(config-if)#ip add
BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224
BOGOTA(config-if)#no shu
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#exit
BOGOTA(config)#
```

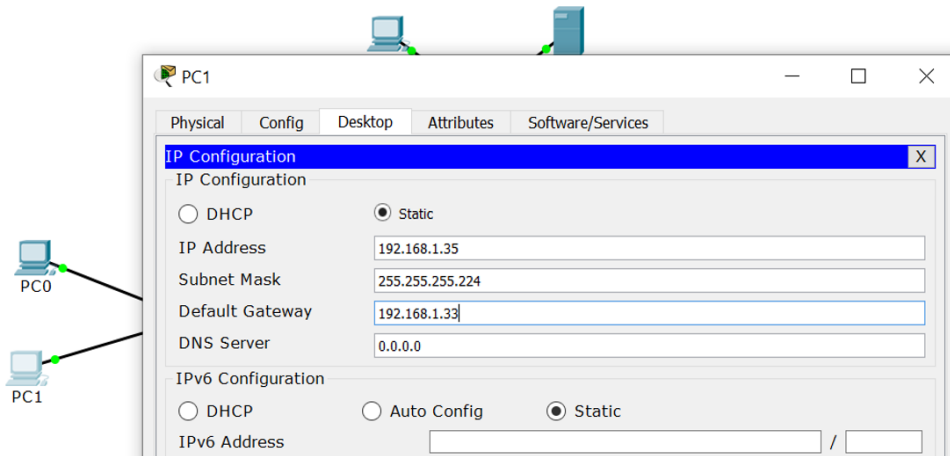
Puerto gigabit 0/0 en el router BOGOTA



Router cali, configuración puertos s0/0/0 y gigabit 0/0



IP PC 0 MEDELLIN



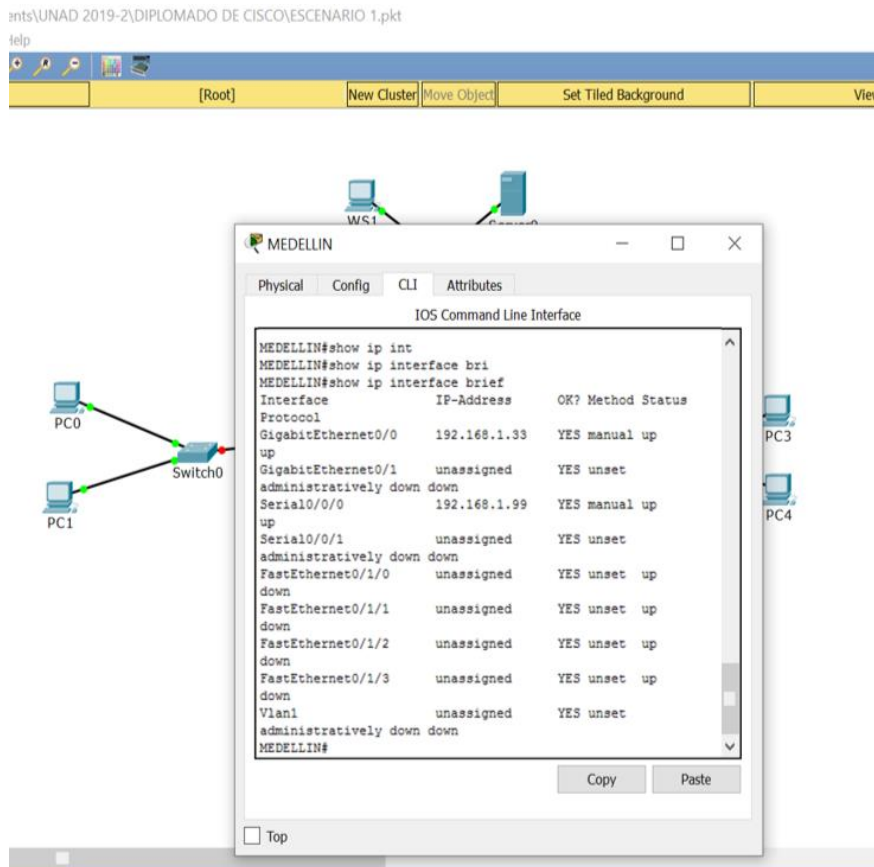
IP PC 1 MEDELLIN
 Parte 2: Configuración Básica.

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

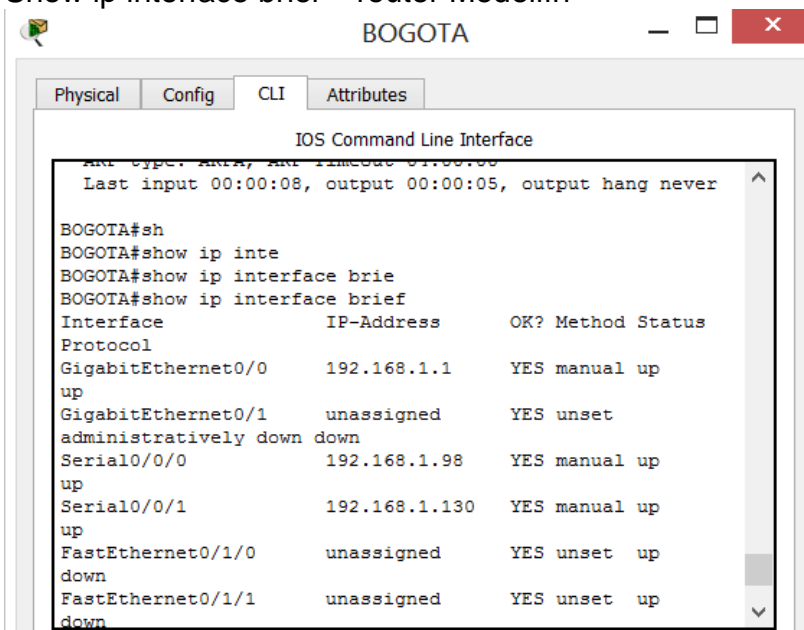
Tabla 1. Tabla de Direccionamiento Escenario 1

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

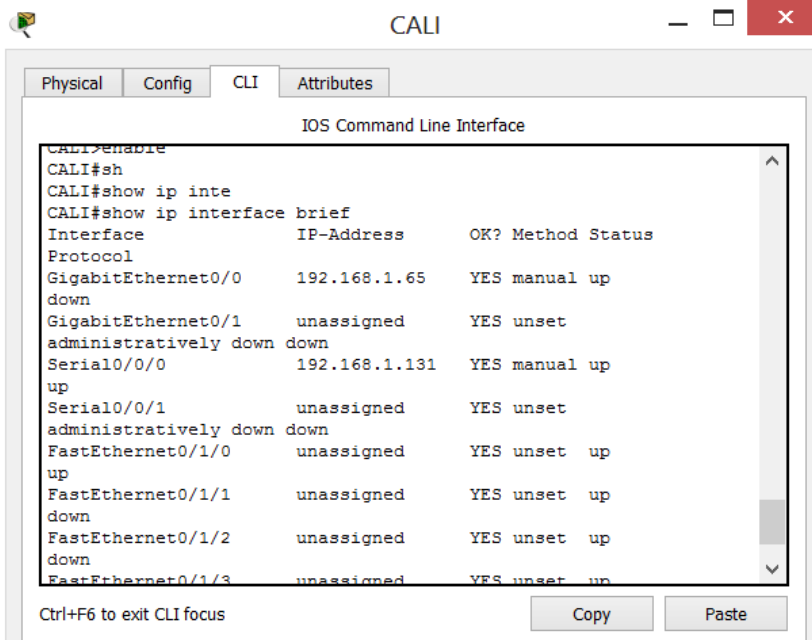
b. Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.



Show ip interface brief – router Medellín



Show ip interface brief – router Bogotá

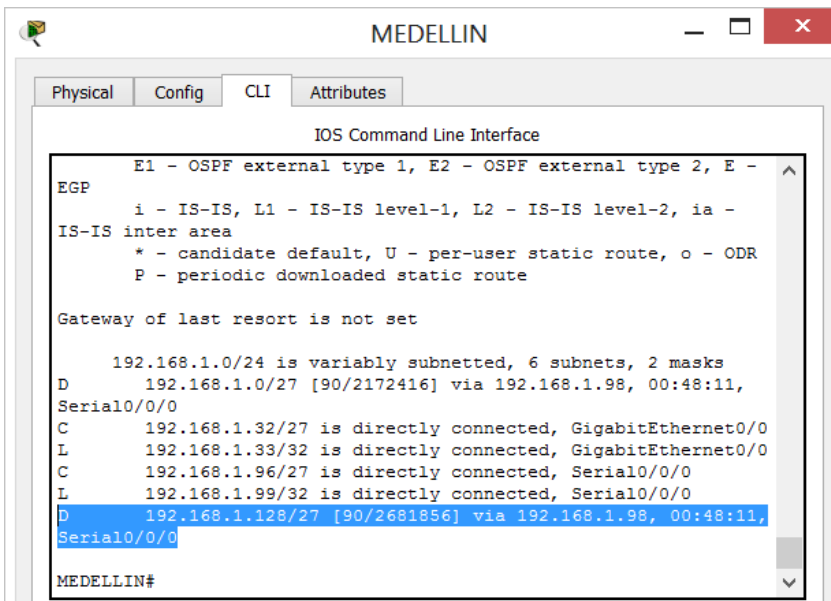


The screenshot shows the CLI window for router CALI. The command 'show ip interface brief' has been executed, resulting in the following output:

```
CALI>enable
CALI#sh
CALI#show ip inte
CALI#show ip interface brief
Interface                IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0      192.168.1.65    YES manual up
down
GigabitEthernet0/1      unassigned      YES unset
administratively down down
Serial0/0/0              192.168.1.131  YES manual up
up
Serial0/0/1              unassigned      YES unset
administratively down down
FastEthernet0/1/0       unassigned      YES unset up
up
FastEthernet0/1/1       unassigned      YES unset up
down
FastEthernet0/1/2       unassigned      YES unset up
down
FastEthernet0/1/3       unassigned      YES unset up
```

Show ip interface brief – router Cali

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



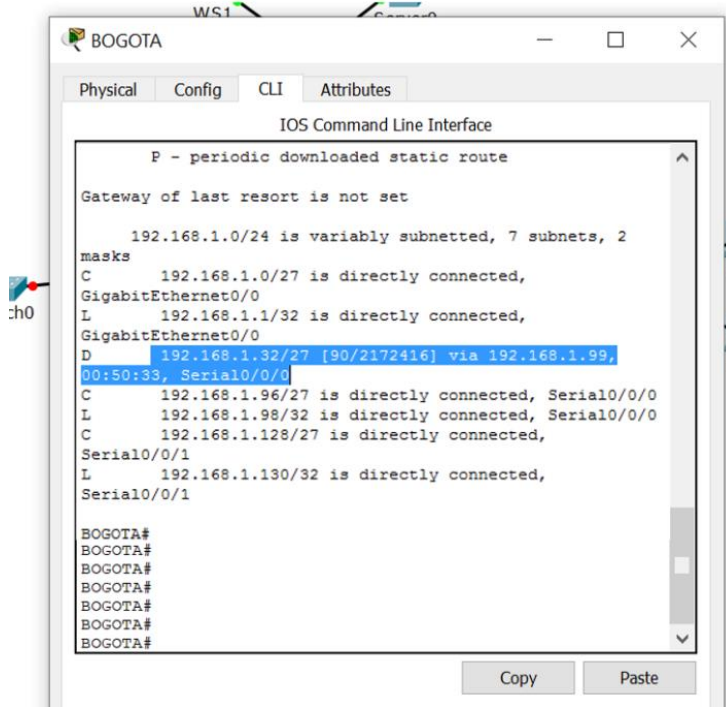
The screenshot shows the CLI window for router MEDELLIN. The command 'show ip route' has been executed, resulting in the following output:

```
MEDELLIN#show ip route
E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

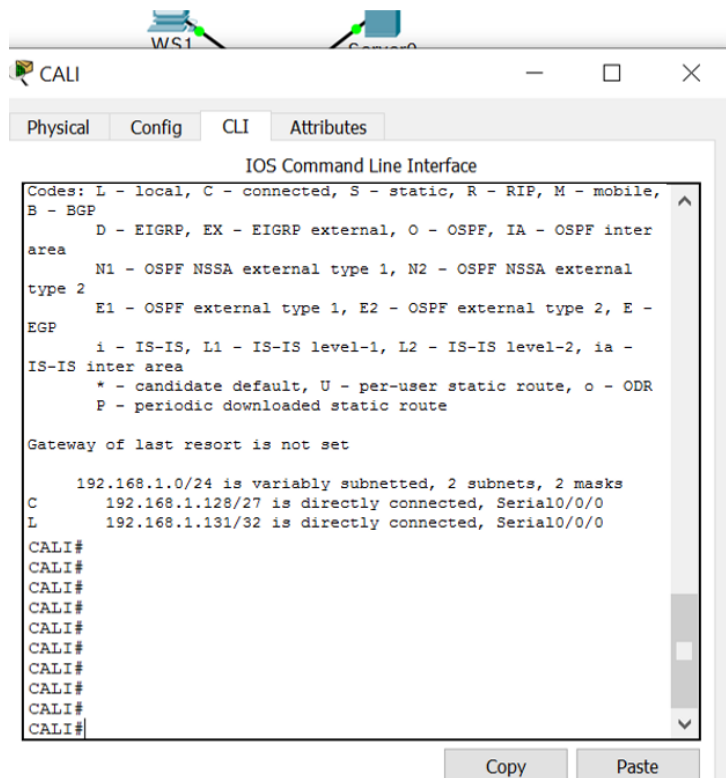
Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 6 subnets, 2 masks
D    192.168.1.0/27 [90/2172416] via 192.168.1.98, 00:48:11,
Serial0/0/0
C    192.168.1.32/27 is directly connected, GigabitEthernet0/0
L    192.168.1.33/32 is directly connected, GigabitEthernet0/0
C    192.168.1.96/27 is directly connected, Serial0/0/0
L    192.168.1.99/32 is directly connected, Serial0/0/0
D    192.168.1.128/27 [90/2681856] via 192.168.1.98, 00:48:11,
Serial0/0/0
MEDELLIN#
```

Show IP route – Medellin



Show IP route – Bogotá



Show IP route – Cali

- d. Realizar un diagnóstico de vecinos usando el comando cdp.
Es probable que debido a que en ningún momento se usó el comando **cdp run** en ninguna interfaz la salida es negativa:

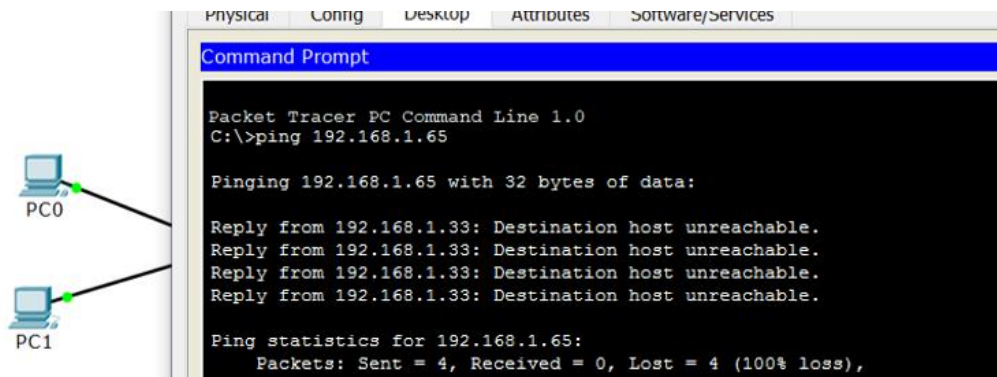
```
MEDELLIN#sh
MEDELLIN#show cdp inter
MEDELLIN#show cdp interface
% CDP is not enabled
MEDELLIN#
```

```
BOGOTA#sh
BOGOTA#show cdp inter
BOGOTA#show cdp interface
% CDP is not enabled
BOGOTA#
```

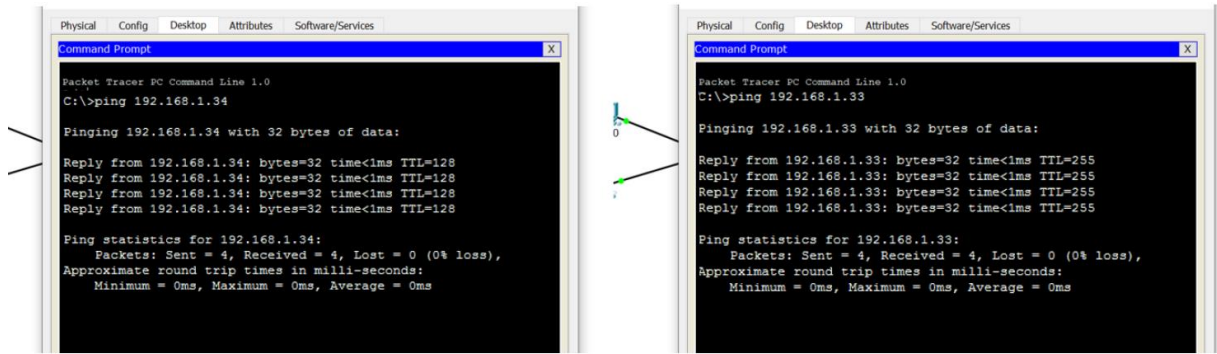
```
CALI#sh
CALI#show cdp inter
CALI#show cdp interface
% CDP is not enabled
CALI#
```

Salida del comando show cdp interface

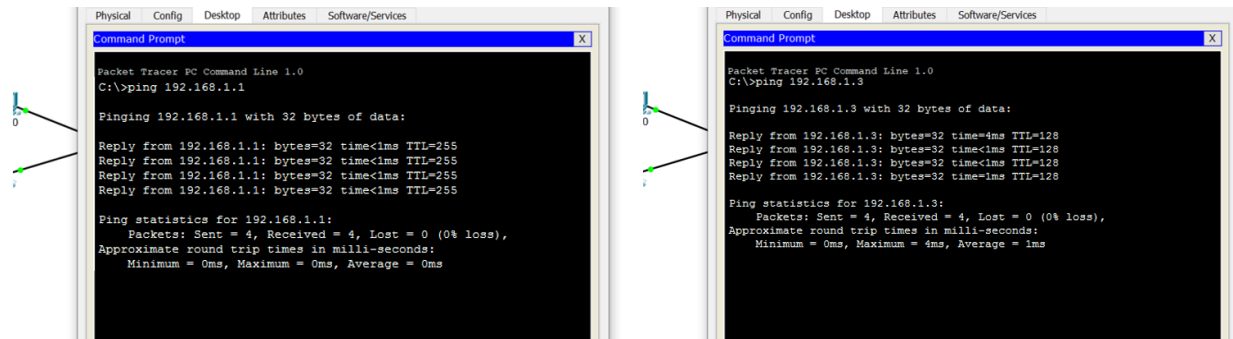
- e. Realizar una prueba de conectividad en cada tramo de la ruta usando Ping.



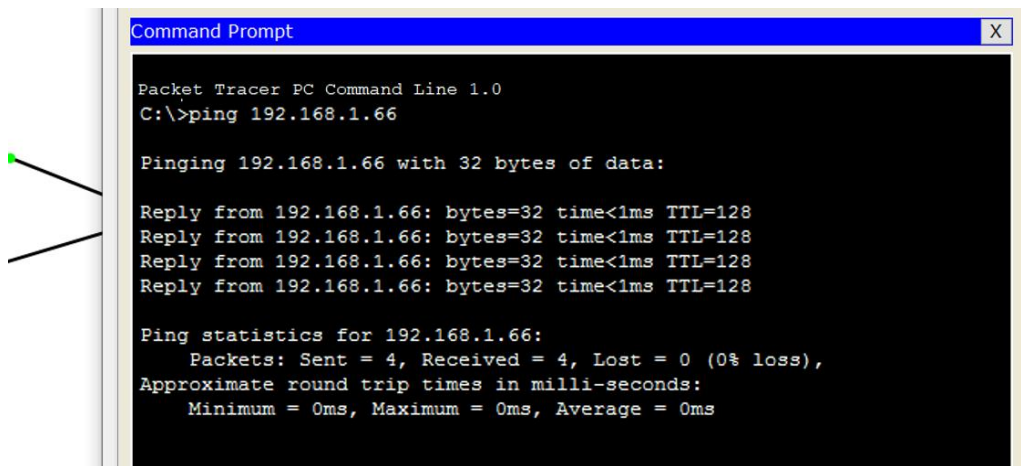
Ping fallido entre el pc 1, red Medellín y router Cali



Ping correcto entre la red Medellín



Ping correcto entre PC WS 1 y servidor red Bogotá

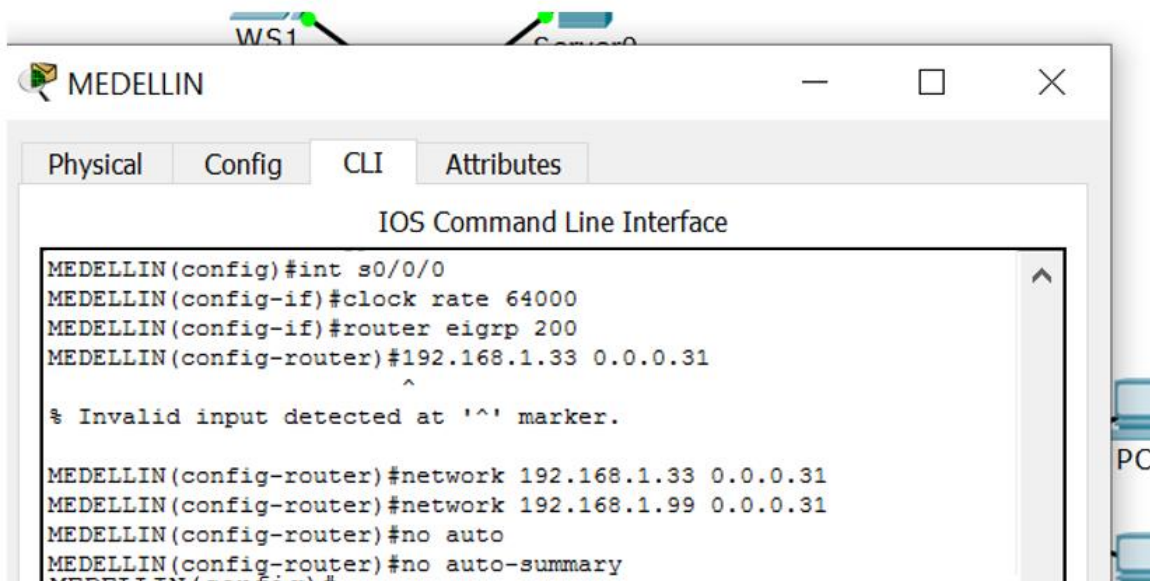


Ping correcto entre la red de Cali

Parte 3: Configuración de Enrutamiento.

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

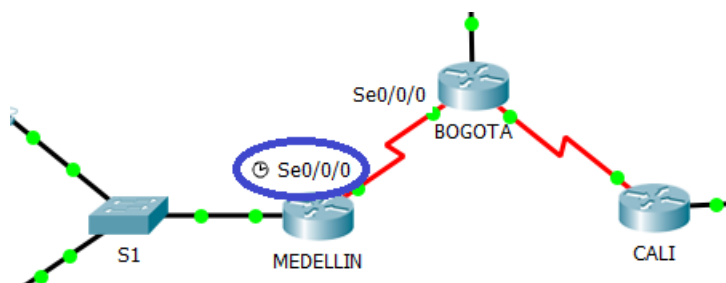
Aunque los dispositivos cuentan con las direcciones IP de la tabla anterior, se debe iniciar el protocolo de comunicación EIGRP en cada uno de los routers:



```
MEDELLIN(config)#int s0/0/0
MEDELLIN(config-if)#clock rate 64000
MEDELLIN(config-if)#router eigrp 200
MEDELLIN(config-router)#192.168.1.33 0.0.0.31
^
% Invalid input detected at '^' marker.
MEDELLIN(config-router)#network 192.168.1.33 0.0.0.31
MEDELLIN(config-router)#network 192.168.1.99 0.0.0.31
MEDELLIN(config-router)#no auto
MEDELLIN(config-router)#no auto-summary
MEDELLIN(config-router)#
```

Protocolo EIGRP router medellin,

En la imagen anterior se evidencia como al puerto serial 0/0/0 se le configura (únicamente en el extremo de Medellín) el reloj de 64.000, para verificar en cuál de los dos extremos se debe configurar el reloj se puede en packet tracer ubicar el puntero del cursor y únicamente en uno de ellos se verá reflejado un pequeño reloj:



Imagen, Topología que evidencia el pin al que se debe configurar el reloj
Para la configuración del protocolo EIGRP del router Bogotá y Cali tenemos:

```

CNTL/Z.
BOGOTA(config)#router eigrp 200
BOGOTA(config-router)#net
BOGOTA(config-router)#network 192.168.1.1 0.0.0.224
EIGRP: Invalid address/mask combination (discontiguous
mask)
BOGOTA(config-router)#network 192.168.1.130 0.0.0.31
BOGOTA(config-router)#network 192.168.1.1 0.0.0.31
BOGOTA(config-router)#network 192.168.1.98 0.0.0.31
BOGOTA(config-router)#no auto
BOGOTA(config-router)#no auto-summary

```

Protocolo EIGRP router Bogotá

```

CALI>enable
CALI#config t
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#router eigrp 200
CALI(config-router)#net
CALI(config-router)#network 192.168.1.65 0.0.0.31
CALI(config-router)#network 192.168.1.131 0.0.0.31
CALI(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 200: Neighbor 192.168.1.130
(Serial0/0/0) is up: new adjacency

```

Protocolo EIGRP router Cali

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

hace uso del comando **show ip eigrp neighbors** donde el número del sistema autónomo es 200 según la tabla

```

BOGOTA>enable
BOGOTA#show ip eigrp neighbors 200
IP-EIGRP neighbors for process 200
H   Address           Interface           Hold Uptime       SRTT
RTO  Q   Seq                               (sec)             (ms)
---  -   -
Cnt  Num
0   192.168.1.99      Se0/0/0            11  02:54:37  40
1000 0   5
1   192.168.1.131    Se0/0/1            13  01:14:08  40
1000 0   7

```

MEDELLIN

Physical Config CLI Attributes

IOS Command Line Interface

```
MEDELLIN>enable
MEDELLIN#show ip eigrp neighbors 200
IP-EIGRP neighbors for process 200
H  Address          Interface      Hold Uptime    SRTT  RTO
Q  Seq
                               (sec)         (ms)
Cnt Num
0  192.168.1.98     Se0/0/0       14  02:54:53  40   1000
```

CALI

Physical Config CLI Attributes

IOS Command Line Interface

```
CALI>enable
CALI#show ip eigrp neighbors 200
IP-EIGRP neighbors for process 200
H  Address          Interface      Hold Uptime    SRTT  RTO  Q
Q  Seq
                               (sec)         (ms)         Cnt
Num
0  192.168.1.130    Se0/0/0       13  01:14:39  40   1000  0
4
```

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

Se realiza mediante el comando **show ip eigrp topology 200**:

CALI

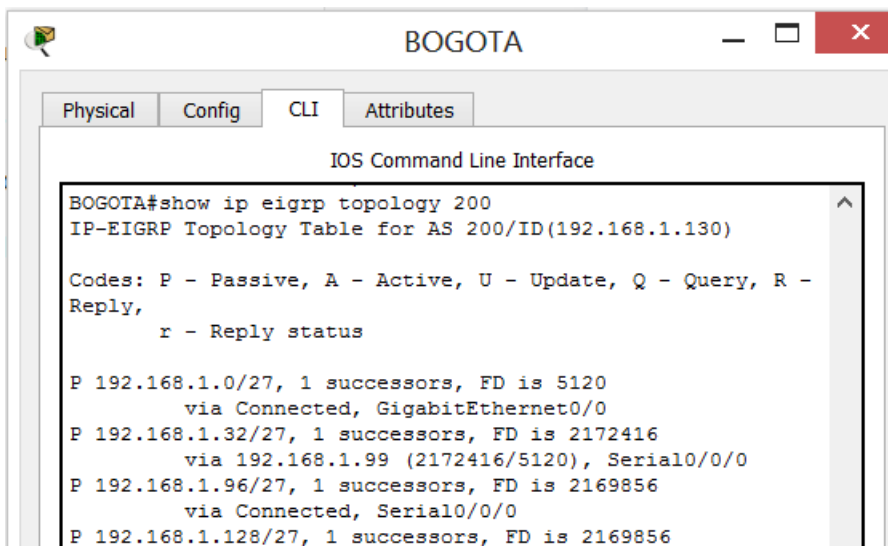
Physical Config CLI Attributes

IOS Command Line Interface

```
CALI#show ip eigrp topology 200
IP-EIGRP Topology Table for AS 200/ID(192.168.1.131)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

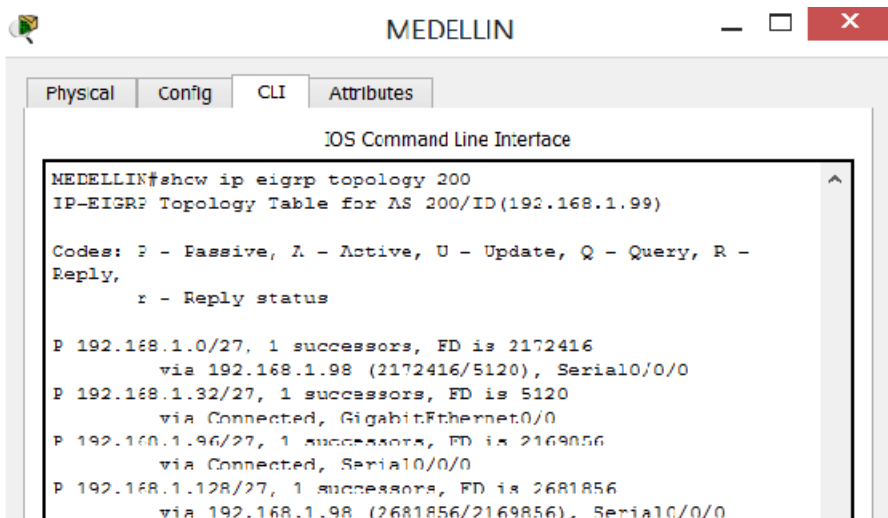
P 192.168.1.0/27, 1 successors, FD is 2172416
   via 192.168.1.130 [2172416/5120], Serial0/0/0
P 192.168.1.32/27, 1 successors, FD is 2684416
   via 192.168.1.130 [2684416/2172416], Serial0/0/0
P 192.168.1.96/27, 1 successors, FD is 2681856
   via 192.168.1.130 [2681856/2169856], Serial0/0/0
P 192.168.1.128/27, 1 successors, FD is 2169856
   via Connected, Serial0/0/0
```



```
BOGOTA#show ip eigrp topology 200
IP-EIGRP Topology Table for AS 200/ID(192.168.1.130)

Codes: P - Passive, A - Active, U - Update, Q - Query, R -
Reply,
       r - Reply status

P 192.168.1.0/27, 1 successors, FD is 5120
   via Connected, GigabitEthernet0/0
P 192.168.1.32/27, 1 successors, FD is 2172416
   via 192.168.1.99 (2172416/5120), Serial0/0/0
P 192.168.1.96/27, 1 successors, FD is 2169856
   via Connected, Serial0/0/0
P 192.168.1.128/27, 1 successors, FD is 2169856
```



```
MEDELLIN#shcw ip eigrp topology 200
IP-EIGRP Topology Table for AS 200/ID(192.168.1.99)

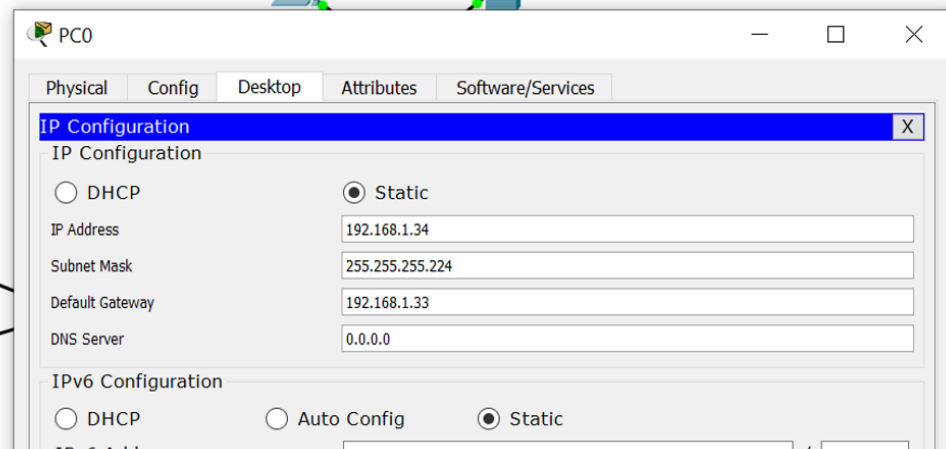
Codes: P - Passive, A - Active, U - Update, Q - Query, R -
Reply,
       r - Reply status

P 192.168.1.0/27, 1 successors, FD is 2172416
   via 192.168.1.98 (2172416/5120), Serial0/0/0
P 192.168.1.32/27, 1 successors, FD is 5120
   via Connected, GigabitEthernet0/0
P 192.168.1.96/27, 1 successors, FD is 2169856
   via Connected, Serial0/0/0
P 192.168.1.128/27, 1 successors, FD is 2681856
   via 192.168.1.98 (2681856/2169856), Serial0/0/0
```

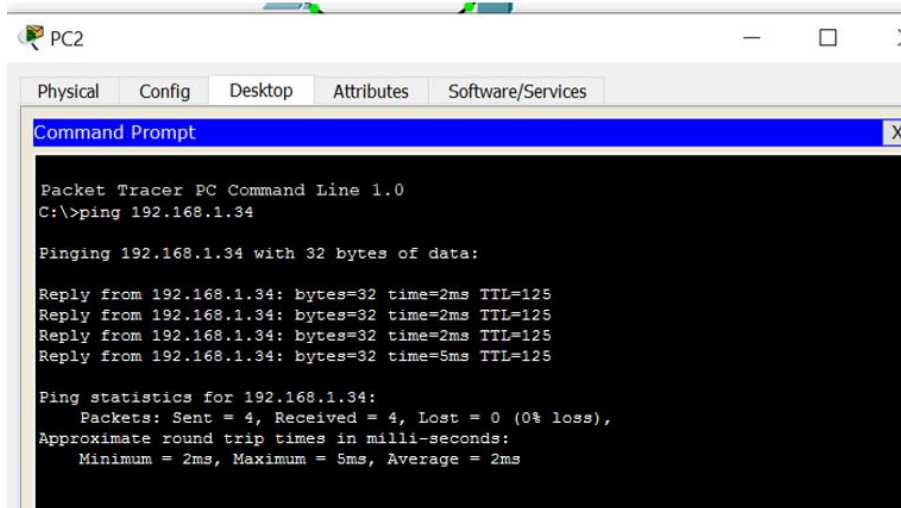
d. Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí. Realizar esta prueba desde un host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor.

Para realizar esta verificación usaremos el comando PING

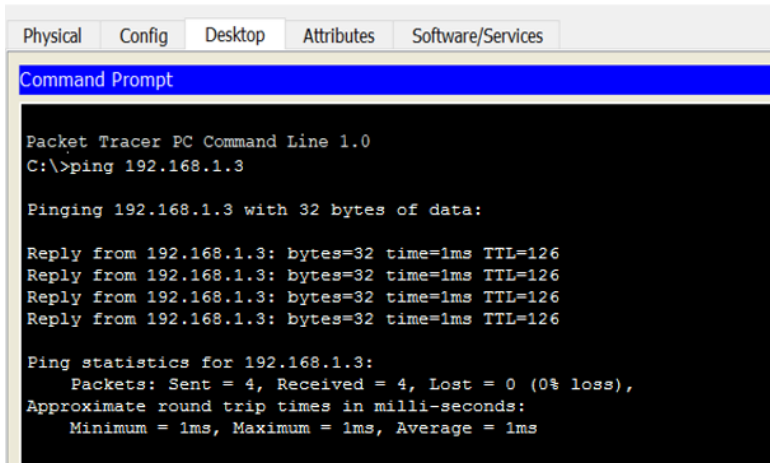
dirección IP asignada en el PC0



la consola del PC2 de la red CALI y hacer ping:



Ping exitoso entre PC2 RED Cali y Servidor red BOGOTA



```
Physical  Config  Desktop  Attributes  Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126
Reply from 192.168.1.3: bytes=32 time=1ms TTL=126

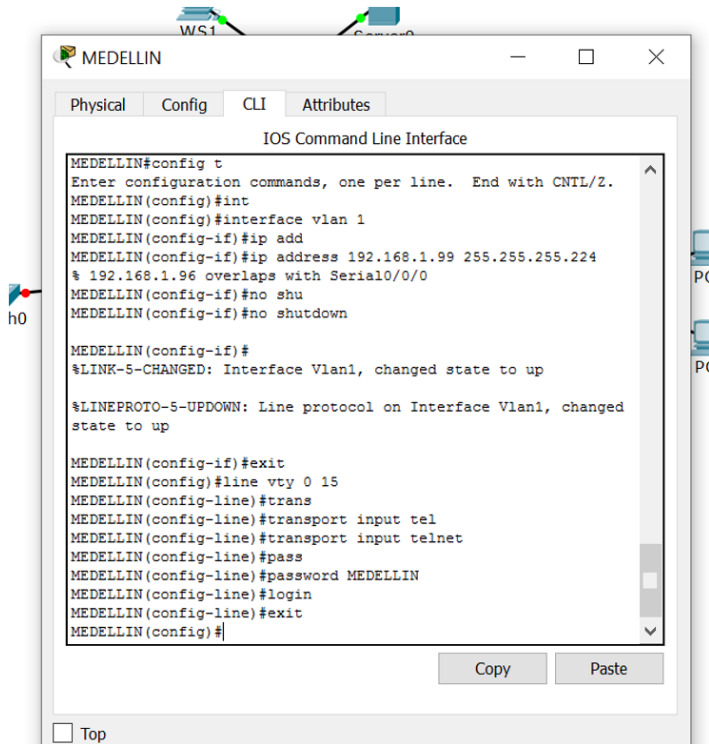
Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

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

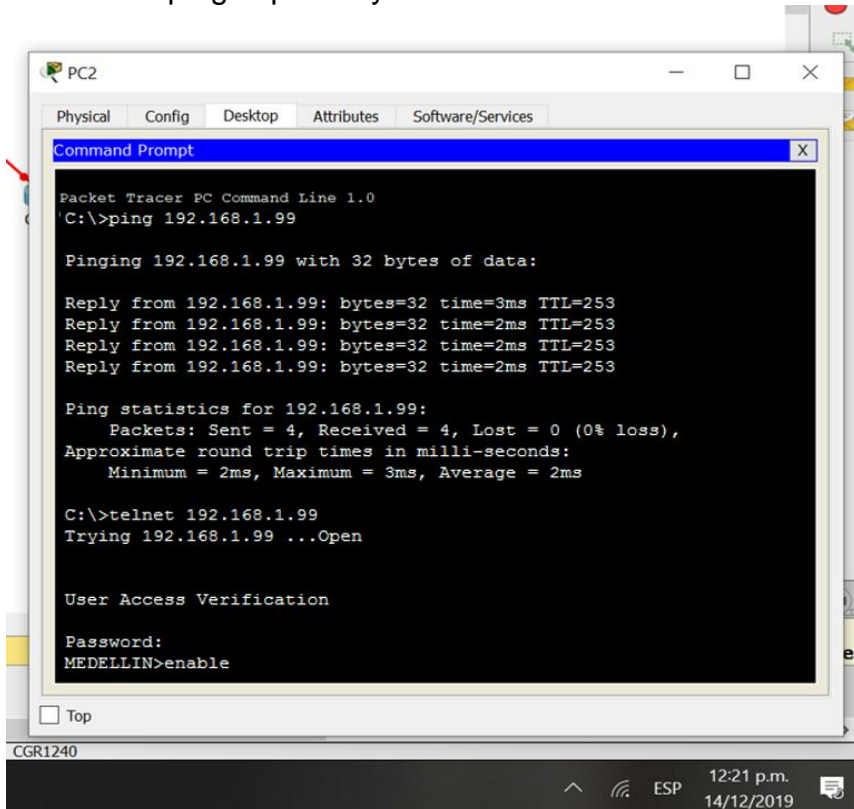
En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo. El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers. Las condiciones para crear las ACL son las siguientes:

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

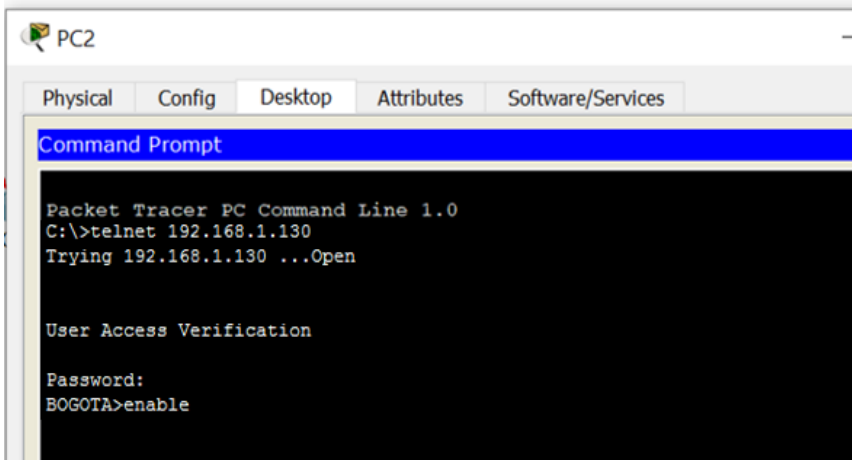
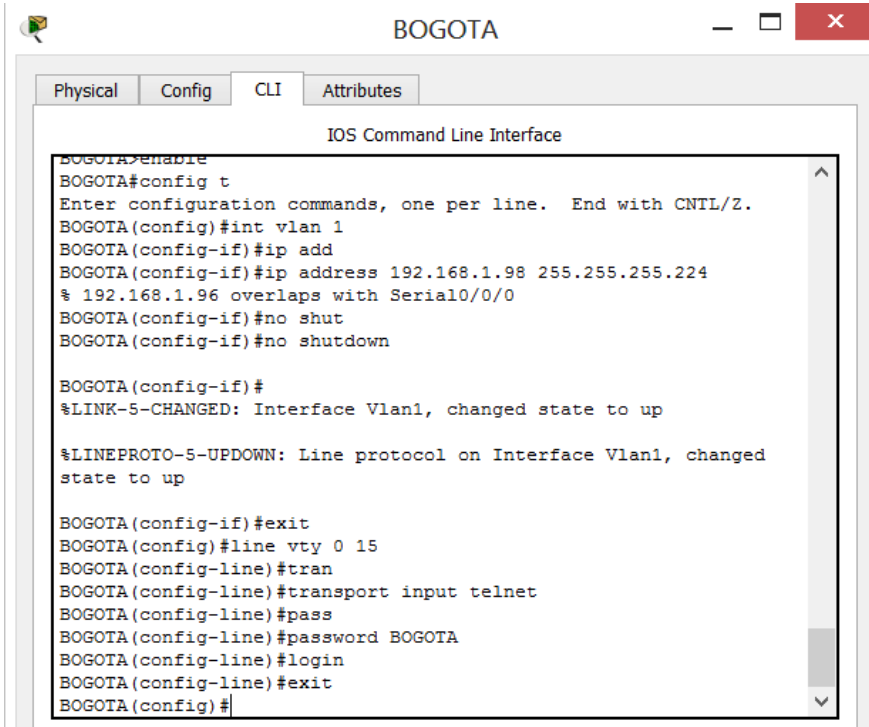
- a. El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.

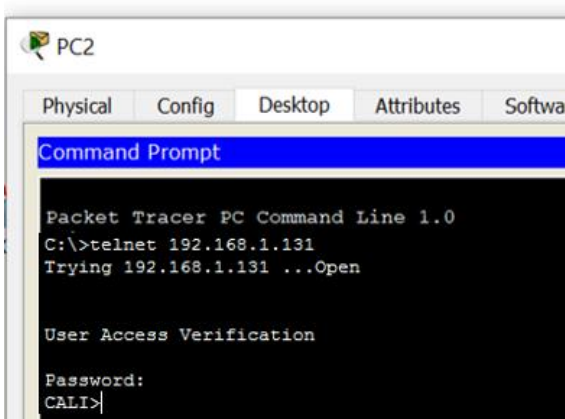
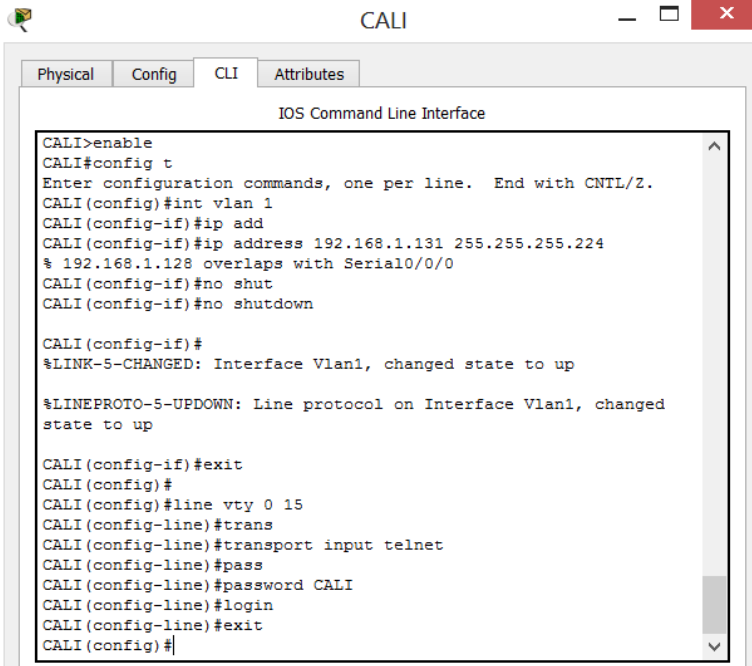


Se realizar ping al puerto y de ser exitoso desde la consola escribir ping

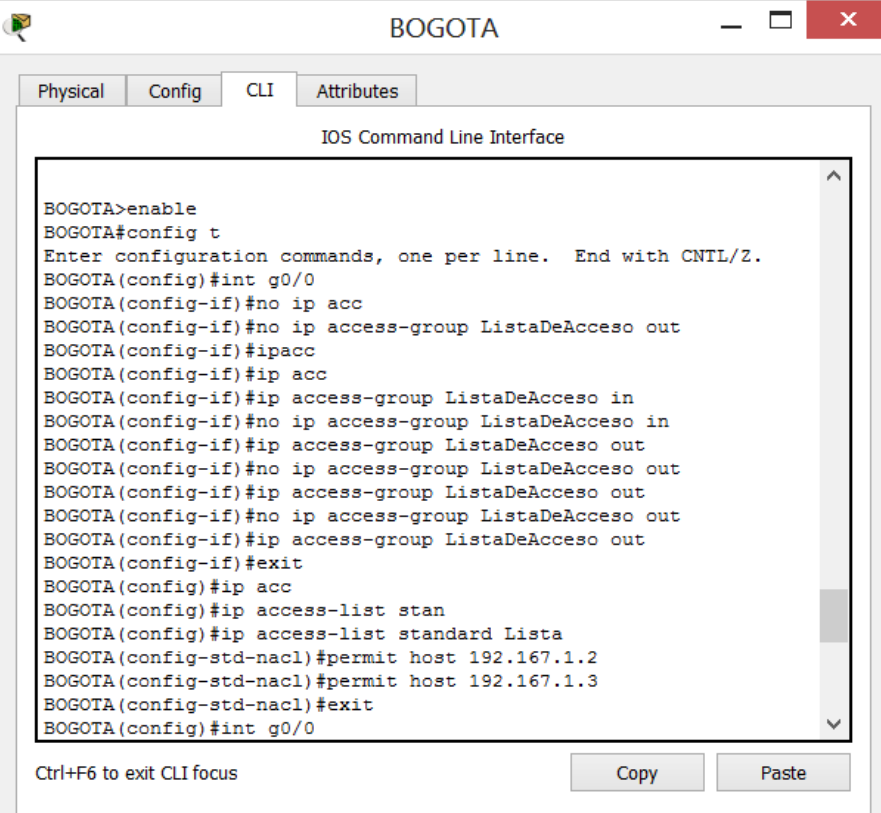


Conexión Telnet correcta entre PC2 (red CALI) y router MEDELLIN



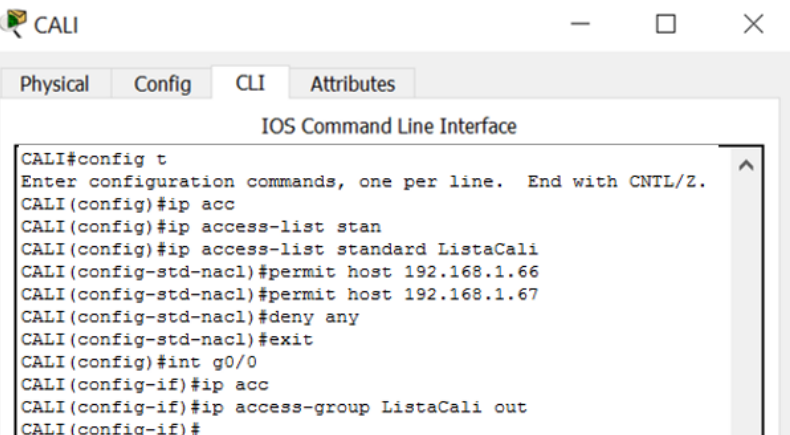


b. Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor.



```
BOGOTA>enable
BOGOTA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#int g0/0
BOGOTA(config-if)#no ip acc
BOGOTA(config-if)#no ip access-group ListaDeAcceso out
BOGOTA(config-if)#ipacc
BOGOTA(config-if)#ip acc
BOGOTA(config-if)#ip access-group ListaDeAcceso in
BOGOTA(config-if)#no ip access-group ListaDeAcceso in
BOGOTA(config-if)#ip access-group ListaDeAcceso out
BOGOTA(config-if)#no ip access-group ListaDeAcceso out
BOGOTA(config-if)#ip access-group ListaDeAcceso out
BOGOTA(config-if)#no ip access-group ListaDeAcceso out
BOGOTA(config-if)#ip access-group ListaDeAcceso out
BOGOTA(config-if)#exit
BOGOTA(config)#ip acc
BOGOTA(config)#ip access-list stan
BOGOTA(config)#ip access-list standard Lista
BOGOTA(config-std-nacl)#permit host 192.167.1.2
BOGOTA(config-std-nacl)#permit host 192.167.1.3
BOGOTA(config-std-nacl)#exit
BOGOTA(config)#int g0/0
```

c. Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor.



```
CALI#config t
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#ip acc
CALI(config)#ip access-list stan
CALI(config)#ip access-list standard ListaCali
CALI(config-std-nacl)#permit host 192.168.1.66
CALI(config-std-nacl)#permit host 192.168.1.67
CALI(config-std-nacl)#deny any
CALI(config-std-nacl)#exit
CALI(config)#int g0/0
CALI(config-if)#ip acc
CALI(config-if)#ip access-group ListaCali out
CALI(config-if)#
```

Lista de control de acceso CALI

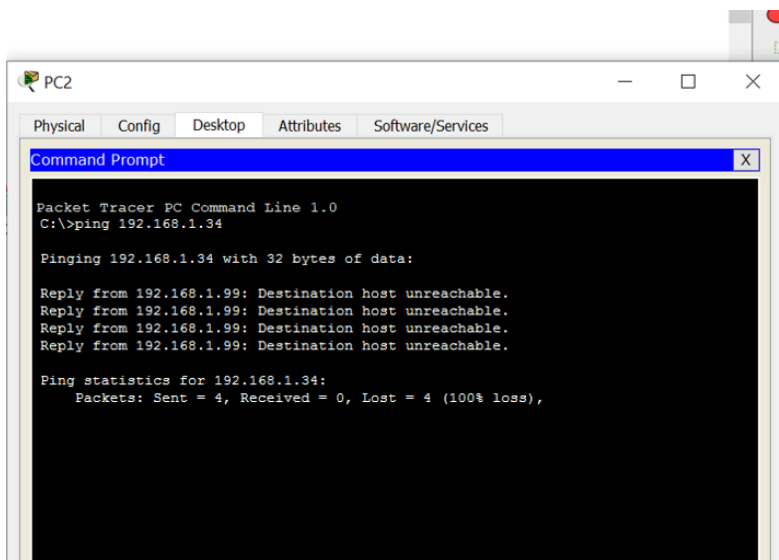
```
IOS Command Line Interface

MEDELLIN>enable
MEDELLIN#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#ip acc
MEDELLIN(config)#ip access-list stan
MEDELLIN(config)#ip access-list standard ListaMedellin
MEDELLIN(config-std-nacl)#permit host 192.168.1.34
MEDELLIN(config-std-nacl)#permit host 192.168.1.35
MEDELLIN(config-std-nacl)#deny any
MEDELLIN(config-std-nacl)#exit
MEDELLIN(config)#int g0/0
MEDELLIN(config-if)#ip acc
MEDELLIN(config-if)#ip access-group Lista out
MEDELLIN(config-if)#ip access-group ListaMedellin out
MEDELLIN(config-if)#
```

Lista de control de acceso MEDELLIN

Parte 5: Comprobación de la red instalada.

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



Resultado de ping Entre PC2 y PC0

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.130: Destination host unreachable.
Reply from 192.168.1.130: Destination host unreachable.
Reply from 192.168.1.130: Destination host unreachable.
Reply from 192.168.1.130: Destination host unreachable.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Ping entre PC2 y servidor

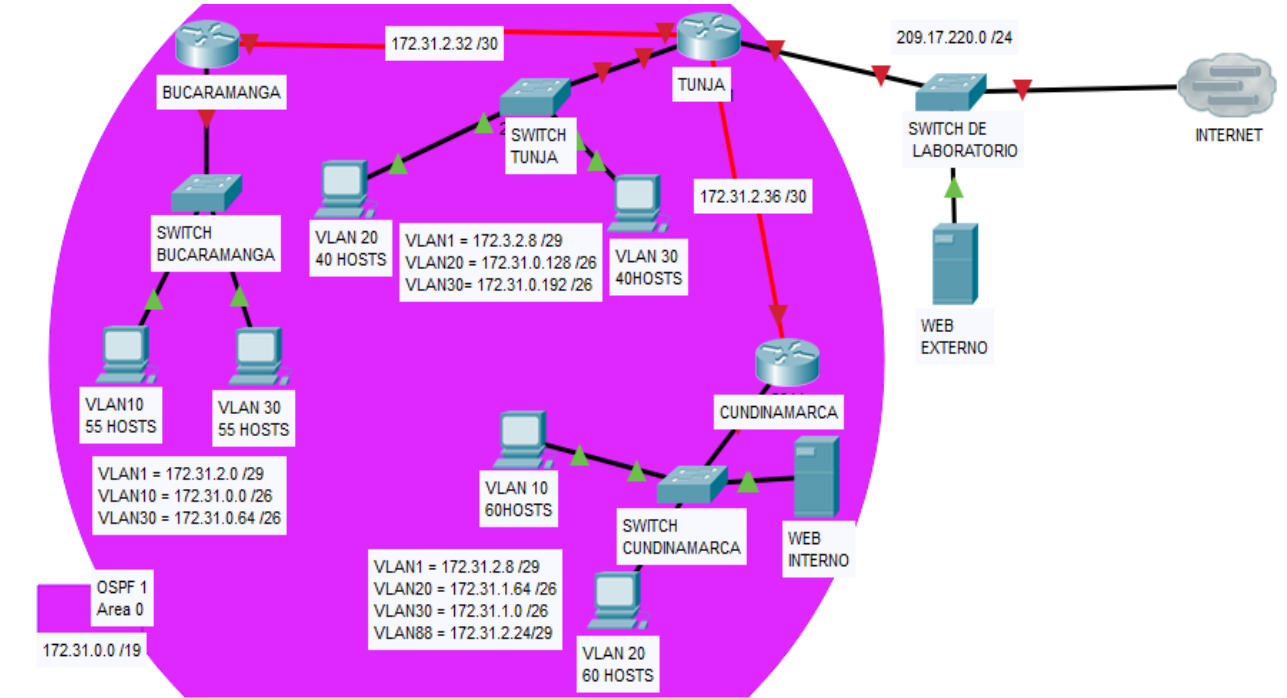
b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red e.

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	Correcto
	WS_1	Router BOGOTA	Correcto
	Servidor	Router CALI	Correcto
	Servidor	Router MEDELLIN	Correcto
TELNET	LAN del Router MEDELLIN	Router CALI	Correcto
	LAN del Router CALI	Router CALI	Incorrecto
	LAN del Router MEDELLIN	Router MEDELLIN	Incorrecto
	LAN del Router CALI	Router MEDELLIN	Correcto
PING	LAN del Router CALI	WS_1	Incorrecto
	LAN del Router MEDELLIN	WS_1	Incorrecto
	LAN del Router MEDELLIN	LAN del Router CALI	Incorrecto
PING	LAN del Router CALI	Servidor	Incorrecto
	LAN del Router MEDELLIN	Servidor	Incorrecto
	Servidor	LAN del Router MEDELLIN	Correcto
	Servidor	LAN del Router CALI	Correcto
	Router CALI	LAN del Router MEDELLIN	Incorrecto
	Router MEDELLIN	LAN del Router CALI	Incorrecto

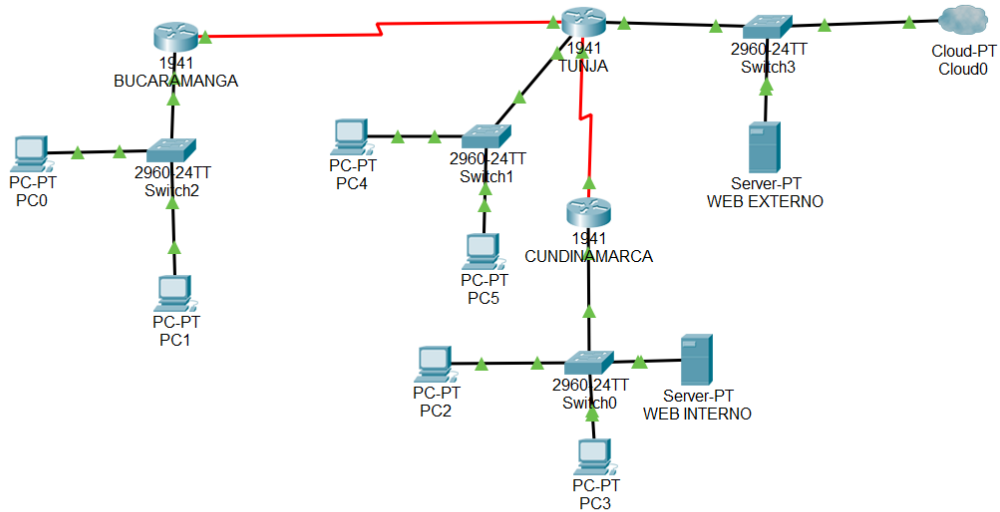
Escenario 2

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.

Topología planteada para el Escenario 2

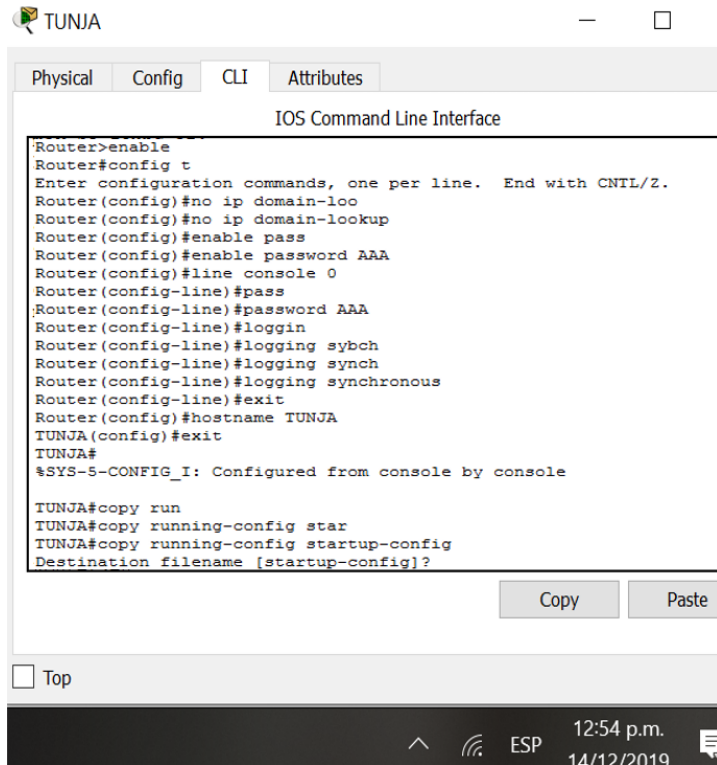


Conexión Topología Escenario 2

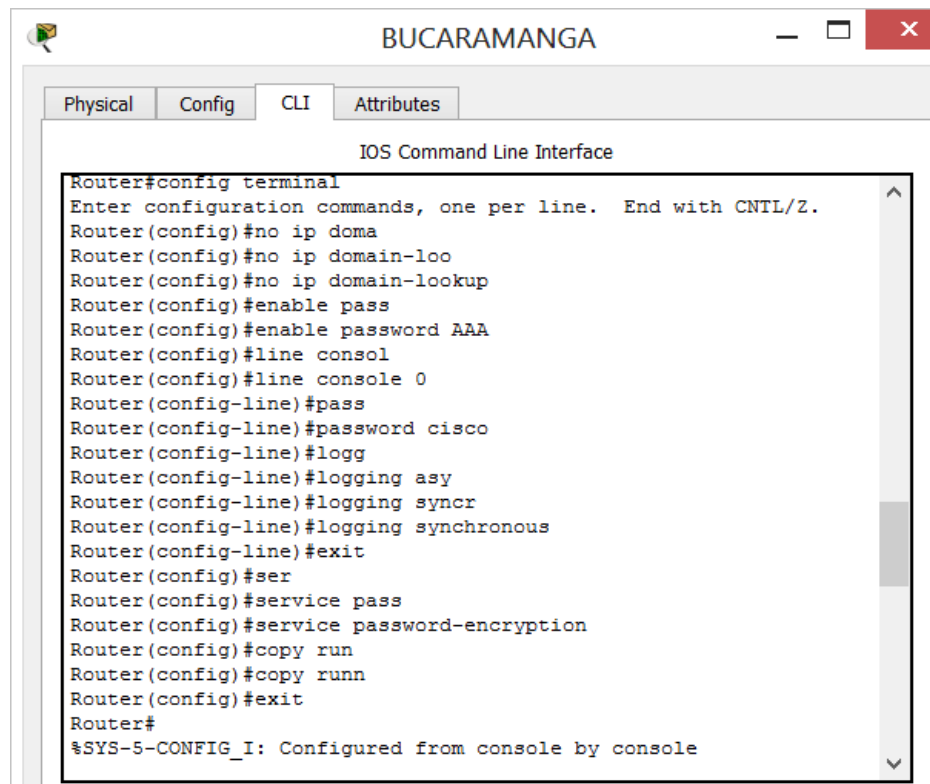


1. Todos los routers deberán tener los siguiente:

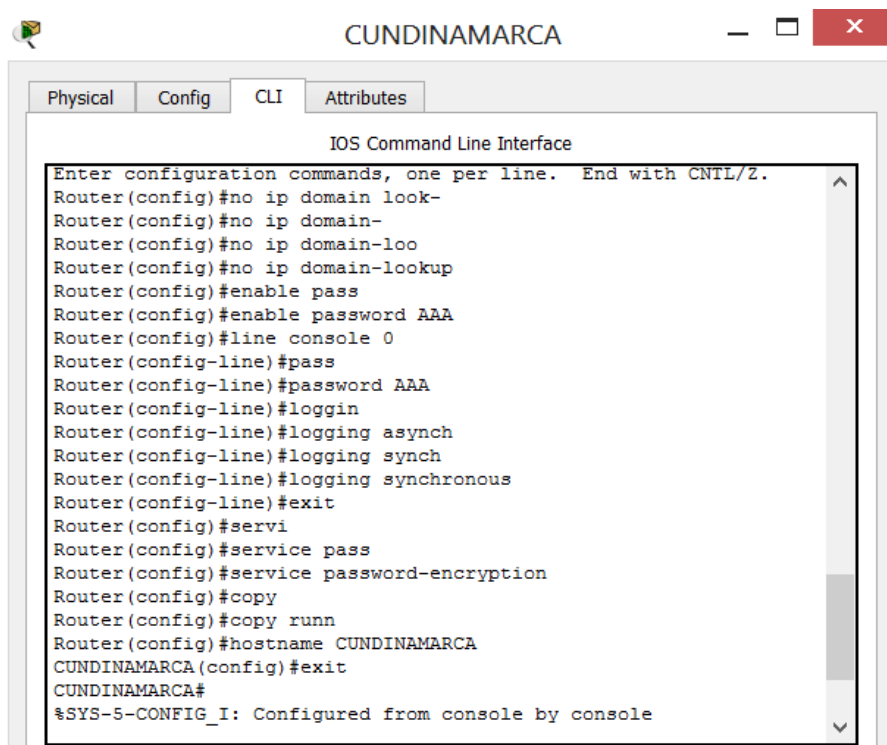
- Configuración básica.
- Autenticación local con AAA.
- Cifrado de contraseñas.
- Un máximo de internos para acceder al router.
- Máximo tiempo de acceso al detectar ataques.
- Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.



Configuración básica Tunja



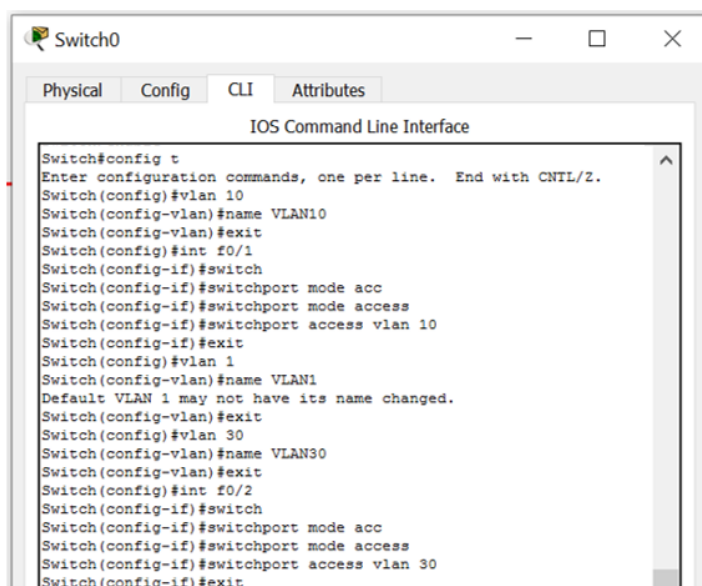
Configuración básica Bucaramanga



```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain look-
Router(config)#no ip domain-
Router(config)#no ip domain-loo
Router(config)#no ip domain-lookup
Router(config)#enable pass
Router(config)#enable password AAA
Router(config)#line console 0
Router(config-line)#pass
Router(config-line)#password AAA
Router(config-line)#loggin
Router(config-line)#logging asynch
Router(config-line)#logging synch
Router(config-line)#logging synchronous
Router(config-line)#exit
Router(config)#servi
Router(config)#service pass
Router(config)#service password-encryption
Router(config)#copy
Router(config)#copy runn
Router(config)#hostname CUNDINAMARCA
CUNDINAMARCA(config)#exit
CUNDINAMARCA#
%SYS-5-CONFIG_I: Configured from console by console
```

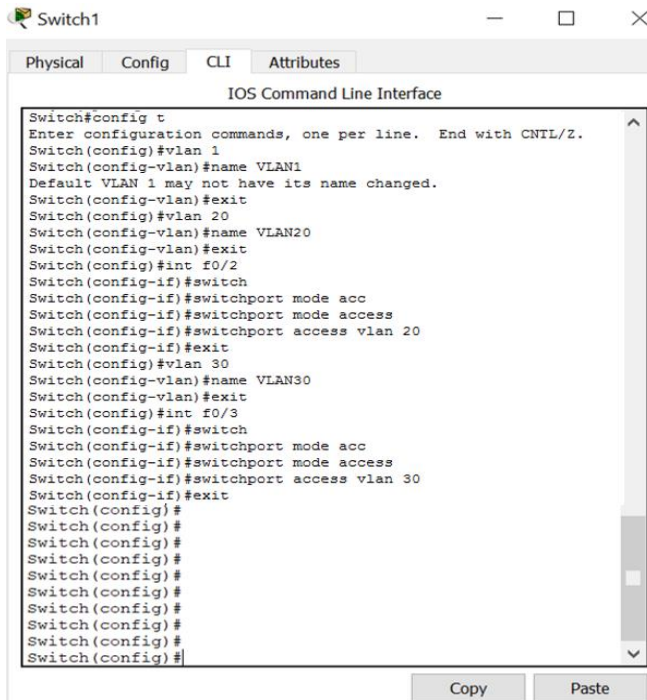
Configuración básica Cundinamarca

Para el switch Bucaramanga tenemos:



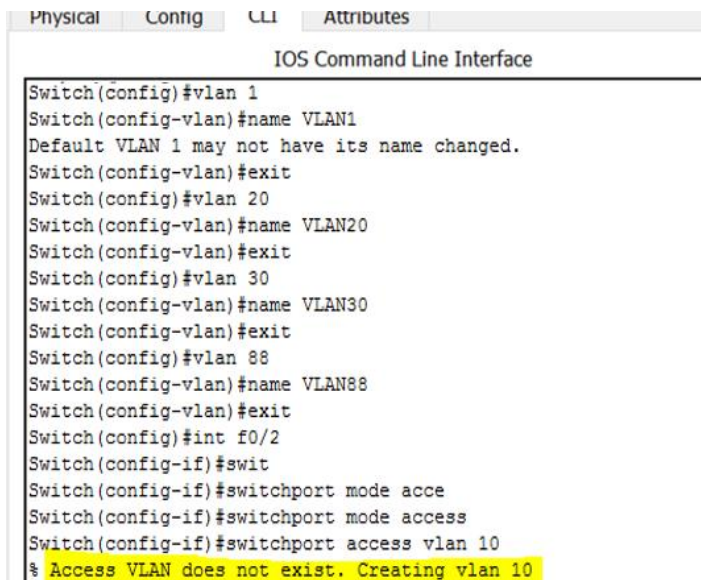
```
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name VLAN10
Switch(config-vlan)#exit
Switch(config)#int f0/1
Switch(config-if)#switch
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#vlan 1
Switch(config-vlan)#name VLAN1
Default VLAN 1 may not have its name changed.
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name VLAN30
Switch(config-vlan)#exit
Switch(config)#int f0/2
Switch(config-if)#switch
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
```

Para el switch Tunja tenemos:



```
Switch1
Physical Config CLI Attributes
IOS Command Line Interface
Switch#config t
Enter configuration commands, one per line. End with CNIL/Z.
Switch(config)#vlan 1
Switch(config-vlan)#name VLAN1
Default VLAN 1 may not have its name changed.
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name VLAN20
Switch(config-vlan)#exit
Switch(config)#int f0/2
Switch(config-if)#switch
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name VLAN30
Switch(config-vlan)#exit
Switch(config)#int f0/3
Switch(config-if)#switch
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
```

para el switch Cundinamarca se tiene:



```
Physical Config CLI Attributes
IOS Command Line Interface
Switch(config)#vlan 1
Switch(config-vlan)#name VLAN1
Default VLAN 1 may not have its name changed.
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name VLAN20
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name VLAN30
Switch(config-vlan)#exit
Switch(config)#vlan 88
Switch(config-vlan)#name VLAN88
Switch(config-vlan)#exit
Switch(config)#int f0/2
Switch(config-if)#swit
Switch(config-if)#switchport mode acce
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
```

Creación VLAN 1, 20, 30, 88 en Switch Cundinamarca

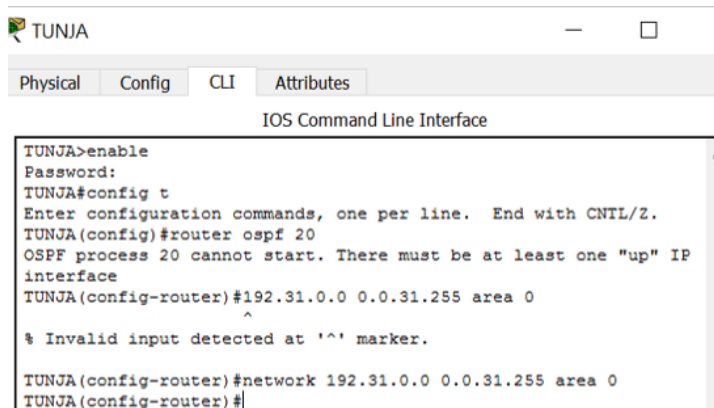
al intentar asignar la VLAN 10 al puerto f0/2 genera error por no existir dicha VLAN, esto debido a un posible error en la gráfica dada por la segunda topología, por lo tanto, se crea otra VLAN y se asigna según corresponde:

```
Switch(config)#int f0/2
Switch(config-if)#swit
Switch(config-if)#switchport mode acce
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
% Access VLAN does not exist. Creating vlan 10
Switch(config-if)#exit
Switch(config)#vlan 10
Switch(config-vlan)#name VLAN10
Switch(config-vlan)#exit
Switch(config)#int f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#int f0/3
Switch(config-if)#
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int f0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
```

Asignación VLAN switch Cundinamarca a los puertos

Como paso seguido, se debe configurar el área 0 mediante el protocolo OSPF en cada router como:



```
TUNJA>enable
Password:
TUNJA#config t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#router ospf 20
OSPF process 20 cannot start. There must be at least one "up" IP
interface
TUNJA(config-router)#192.31.0.0 0.0.31.255 area 0
^
% Invalid input detected at '^' marker.
TUNJA(config-router)#network 192.31.0.0 0.0.31.255 area 0
TUNJA(config-router)#
```

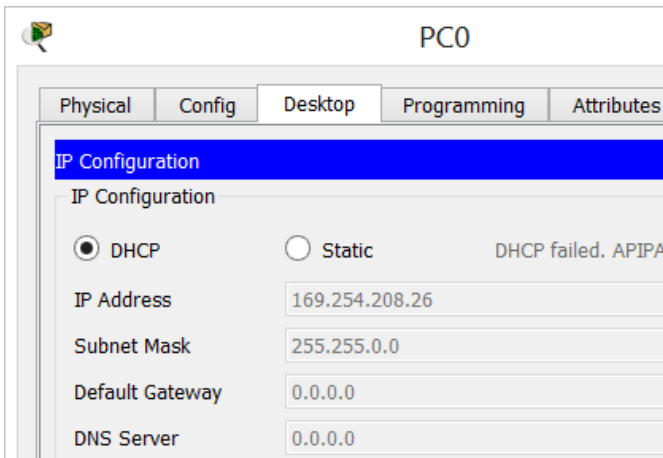
```
CUNDINAMARCA>enable
Password:
Password:
CUNDINAMARCA#config t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#router ospf 20
OSPF process 20 cannot start. There must be at least one "up" IP
interface
CUNDINAMARCA(config-router)#networ
CUNDINAMARCA(config-router)#network 172.31.0.0 0.0.31.255 area 0
CUNDINAMARCA(config-router)#
```

```
BUCARAMANGA>enable
Password: |
BUCARAMANGA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#router ospf 1
OSPF process 1 cannot start. There must be at least one "up" IP
interface
BUCARAMANGA(config-router)#exit
BUCARAMANGA(config)#router ospf 20
OSPF process 20 cannot start. There must be at least one "up" IP
interface
BUCARAMANGA(config-router)#netw
BUCARAMANGA(config-router)#network 172.31.0.0 0.0.31.255
% Incomplete command.
BUCARAMANGA(config-router)#network 172.31.0.0 0.0.31.255 area 0
BUCARAMANGA(config-router)#
```

Configuración OSPF de los 3 routers

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

Para poder tener una óptima conectividad con el protocolo DHCP se debe tomar cada host de las redes y que cada uno solicite de manera dinámica las direcciones IP:



Para el router de Bucaramanga se tiene:

```
BUCARAMANGA>enable
Password:
BUCARAMANGA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#ip dhcp exclu
BUCARAMANGA(config)#ip dhcp excluded-address 172.31.0.129
172.31.0.255|
BUCARAMANGA(config)#ip dhcp pool DHCP_BUCARA
BUCARAMANGA(dhcp-config)#172.31.0.0 255.255.255.192
^
% Invalid input detected at '^' marker.

BUCARAMANGA(dhcp-config)#network 172.31.0.0 255.255.255.192
BUCARAMANGA(dhcp-config)#default
BUCARAMANGA(dhcp-config)#default-router 172.31.0.1
BUCARAMANGA(dhcp-config)#dns-ser
BUCARAMANGA(dhcp-config)#dns-server 8.8.8.8
BUCARAMANGA(dhcp-config)#
```

```

CUNDINAMARCA>enable
Password:
CUNDINAMARCA#config t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#ip dhcp exclu
CUNDINAMARCA(config)#ip dhcp excluded-address 172.31.1.129
172.31.1.255
CUNDINAMARCA(config)#ip dhcp exclude
CUNDINAMARCA(config)#ip dhcp pool DHCP_CUNDI
CUNDINAMARCA(dhcp-config)#network 172.31.1.0 255.255.255.192
CUNDINAMARCA(dhcp-config)#defau
CUNDINAMARCA(dhcp-config)#default-router 172.31.1.1
CUNDINAMARCA(dhcp-config)#dns-s
CUNDINAMARCA(dhcp-config)#dns-server 8.8.8.8
CUNDINAMARCA(dhcp-config)#

```

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 acceso 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

```
BUCARAMANGA>enable
Password:
BUCARAMANGA#config t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#int s0/0/0
BUCARAMANGA(config-if)#descri
BUCARAMANGA(config-if)#description conn
BUCARAMANGA(config-if)#description connectio
BUCARAMANGA(config-if)#ip add
BUCARAMANGA(config-if)#ip address 172.31.2.33 255.255.255.252
BUCARAMANGA(config-if)#no shut
BUCARAMANGA(config-if)#clock rate 128000
BUCARAMANGA(config-if)#no shut
BUCARAMANGA(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
BUCARAMANGA(config-if)#
```

R Bucaramanga S0/0/0

```
BUCARAMANGA(config)#int g0/0
BUCARAMANGA(config-if)#ip add
BUCARAMANGA(config-if)#ip address 172.31.0.1 255.255.225.192
Bad mask 0xFFFFE1C0 for address 172.31.0.1
BUCARAMANGA(config-if)#ip address 172.31.0.1 255.255.255.192
BUCARAMANGA(config-if)#no shu
BUCARAMANGA(config-if)#no shutdown

BUCARAMANGA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

BUCARAMANGA(config-if)#
```

R Bucaramanga G0/0

```
TUNJA>enable
Password:
TUNJA#config t
Enter configuration commands, one per line. End with CNTL/Z
TUNJA (config)#int s0/0/0
TUNJA (config-if)#ip add
TUNJA (config-if)#ip address 172.31.2.34 255.255.255.252
TUNJA (config-if)#no shut
TUNJA (config-if)#no shutdown

TUNJA (config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

TUNJA (config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up

TUNJA (config-if)#
```

R Tunja puerto s0/0/0

```
TUNJA (config)#int s0/0/1
TUNJA (config-if)#ip add
TUNJA (config-if)#ip address 172.31.2.36 255.255.255.252
Bad mask /30 for address 172.31.2.36
TUNJA (config-if)#ip address 172.31.2.37 255.255.255.252
TUNJA (config-if)#clock rate 128000
TUNJA (config-if)#no shut
TUNJA (config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
TUNJA (config-if)#exit
TUNJA (config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

R Tunja puerto S0/0/1

```
TUNJA (config)#int g0/0
TUNJA (config-if)#ip add
TUNJA (config-if)#ip address 172.31.2.129 255.255.255.192
TUNJA (config-if)#no shut
TUNJA (config-if)#no shutdown

TUNJA (config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

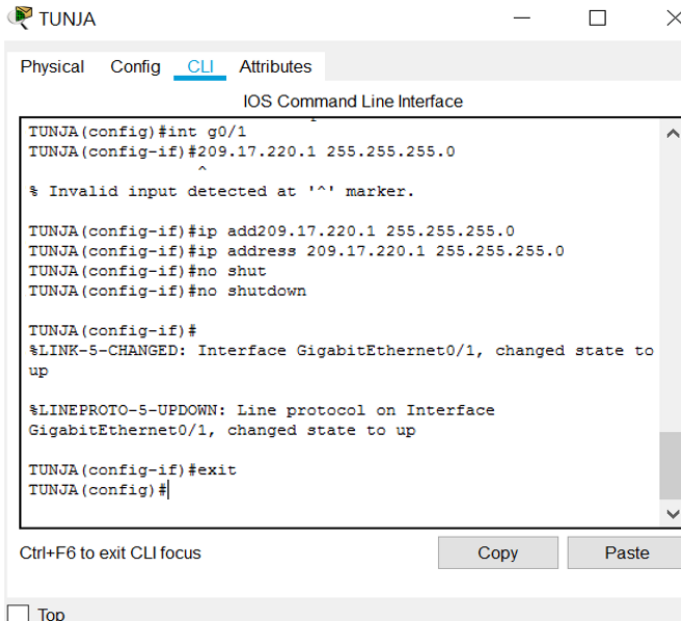
TUNJA (config-if)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

R Tunja puerto G0/0



The screenshot shows a terminal window titled 'TUNJA' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal output shows the following commands and responses:

```
TUNJA(config)#int g0/1
TUNJA(config-if)#209.17.220.1 255.255.255.0
^
% Invalid input detected at '^' marker.

TUNJA(config-if)#ip add209.17.220.1 255.255.255.0
TUNJA(config-if)#ip address 209.17.220.1 255.255.255.0
TUNJA(config-if)#no shut
TUNJA(config-if)#no shutdown

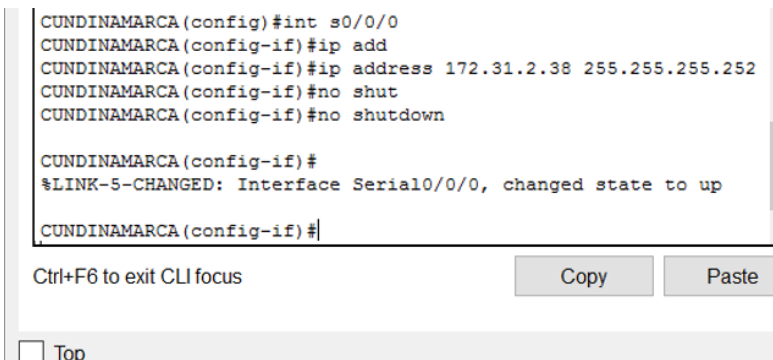
TUNJA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up

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

Below the terminal output, there are buttons for 'Copy' and 'Paste', and a 'Top' button at the bottom left.

R Tunja Puerto G0/1



The screenshot shows a terminal window titled 'CUNDINAMARCA' with the 'CLI' tab active. The terminal output shows the following commands and responses:

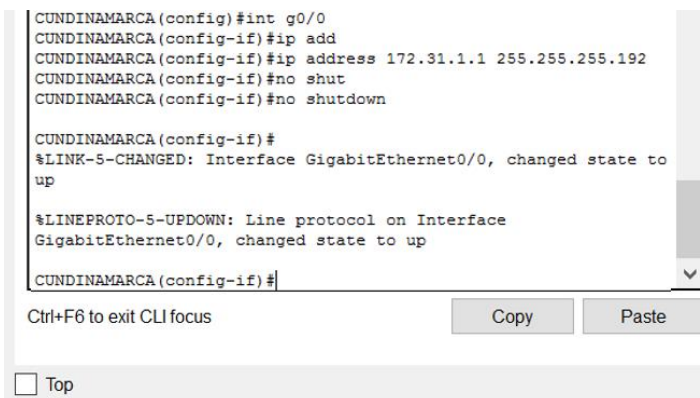
```
CUNDINAMARCA(config)#int s0/0/0
CUNDINAMARCA(config-if)#ip add
CUNDINAMARCA(config-if)#ip address 172.31.2.38 255.255.255.252
CUNDINAMARCA(config-if)#no shut
CUNDINAMARCA(config-if)#no shutdown

CUNDINAMARCA(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

CUNDINAMARCA(config-if)#
```

Below the terminal output, there are buttons for 'Copy' and 'Paste', and a 'Top' button at the bottom left.

R Cundinamarca S0/0/0



The screenshot shows a terminal window titled 'CUNDINAMARCA' with the 'CLI' tab active. The terminal output shows the following commands and responses:

```
CUNDINAMARCA(config)#int g0/0
CUNDINAMARCA(config-if)#ip add
CUNDINAMARCA(config-if)#ip address 172.31.1.1 255.255.255.192
CUNDINAMARCA(config-if)#no shut
CUNDINAMARCA(config-if)#no shutdown

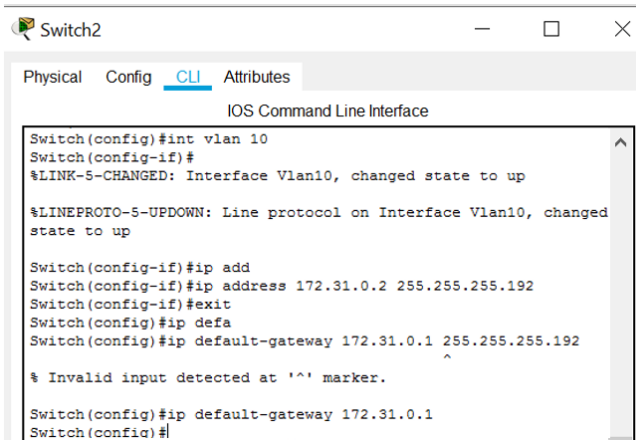
CUNDINAMARCA(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

CUNDINAMARCA(config-if)#
```

Below the terminal output, there are buttons for 'Copy' and 'Paste', and a 'Top' button at the bottom left.

R Cundinamarca – interfaz G0/0



The screenshot shows the CLI interface of a switch named 'Switch2'. The 'CLI' tab is selected. The terminal output shows the configuration of VLAN 10. The commands and their outputs are as follows:

```
Switch(config)#int vlan 10
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

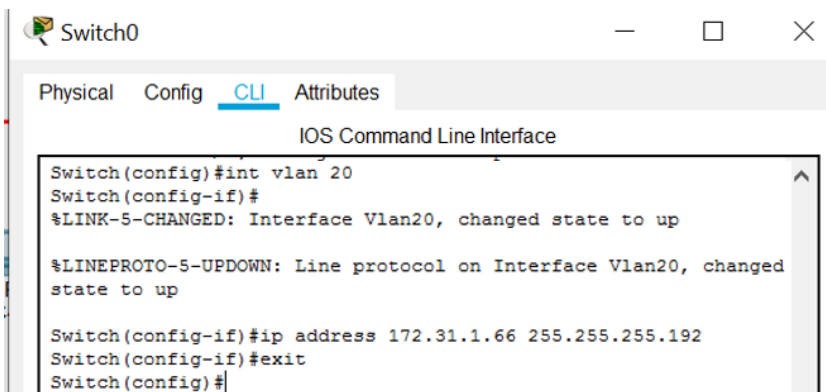
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed
state to up

Switch(config-if)#ip add
Switch(config-if)#ip address 172.31.0.2 255.255.255.192
Switch(config-if)#exit
Switch(config)#ip defa
Switch(config)#ip default-gateway 172.31.0.1 255.255.255.192

% Invalid input detected at '^' marker.

Switch(config)#ip default-gateway 172.31.0.1
Switch(config)#
```

Switch Red Bucaramanga – config VLAN 10



The screenshot shows the CLI interface of a switch named 'Switch0'. The 'CLI' tab is selected. The terminal output shows the configuration of VLAN 20. The commands and their outputs are as follows:

```
Switch(config)#int vlan 20
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed
state to up

Switch(config-if)#ip address 172.31.1.66 255.255.255.192
Switch(config-if)#exit
Switch(config)#
```

Switch Red CUNDINAMARCA – config VLAN 20

```
Switch(config-if)#ip address 172.31.1.66 255.255.255.192
Switch(config-if)#exit
Switch(config)#int vlan 10
Switch(config-if)#ip address 172.31.1.2 255.255.255.192
Switch(config-if)#exit
Switch(config)#int vlan 1
Switch(config-if)#ip address 172.31.2.9 255.255.255.248
Switch(config-if)#exit
Switch(config)#vlan 88
Switch(config-vlan)#name VLAN88
Switch(config-vlan)#exit
Switch(config)#int vlan 88
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan88, changed state to up

Switch(config-if)#ip address 172.31.2.25 255.255.255.248
Switch(config-if)#exit
Switch(config)#
```

Switch Red CUNDINAMARCA – config VLAN 10 y 88

```
Switch(config)#int vlan 20
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed
state to up

Switch(config-if)#ip address 172.31.0.129 255.255.255.192
Switch(config-if)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name VLAN30
Switch(config-vlan)#exit
Switch(config)#int vlan 30
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed
state to up

Switch(config-if)#172.31.0.193 255.255.255.192
^
% Invalid input detected at '^' marker.

Switch(config-if)#ip address 172.31.0.193 255.255.255.192
```

Switch Red CUNDINAMARCA – config VLAN 20 y 30

CONCLUSIONES

Esta actividad realizada permitió demostrar el aprendizaje obtenido en el transcurso del diplomado, por medio del software Packet Tracer que nos permitió dar solución a los dos escenarios dados de esta forma brindando las herramientas necesarias para resolver cada problema planteado para estas topologías.

Después de terminar esta actividad me permitió reflexionar lo importante que es un ingeniero de sistemas en la actualidad al darle solución a este tipo de problemas facilitando las comunicaciones de muchas personas y haciendo de esta manera un trabajo más eficiente para todo el mundo.

BIBLIOGRAFIA

Capacity. Cisco CCNA – Cómo Configurar VLAN en Cisco Switch. Recuperado de: <http://blog.capacityacademy.com/2014/06/06/cisco-ccna-como-configurar-vlan-en-switch-cisco/>

IT Networking Career Opportunities - Cisco. (n.d.). Retrieved December 14, 2019, from <https://www.cisco.com/c/en/us/training-events/training-certifications/it-networking-career-opportunities.html>

Amberg, E. (2014). CCNA 1 Powertraining: ICND1/CCENT (100-101). Heidelberg: MITP. Recuperado de <http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=979032&lang=es&site=ehost-live>

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

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

Guía de Diseño de OSPF. Cisco. Recuperado de: https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/7039-1.html