DIPLOMADO DE PROFUNDIZACIÓN CISCO

PRUEBA DE HABILIDADES

Entregado por:

PAULO ANDRÉS JIMENEZ MARTÍNEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
INGENIERIA DE SISTEMAS
DOSQUEBRADAS
DICIEMBRE DE 2019
PRUEBA DE HABILIDADES

PAULO ANDRES JIMENEZ MARTINEZ

DIPLOMADO CISCO-TRABAJO DE GRADO

TUTOR-DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
INGENIERIA DE SISTEMAS
DOSQUEBRADAS
DICIEMBRE DE 2019

Tabla de contenido

Tabla de ilustración

Resumen

El presente proyecto está centrado en la solución oportuna de dos escenarios en los que se busca lograr una óptima solución en el desarrollo y funcionamiento de sus diferentes redes, en donde se busca poder abordar y analizar las diferentes temáticas, lo anterior desde sus diversos puntos de vista y análisis, para determinar en lo posible las diferentes causas exactas que se puedan presentar, se identificaran sus necesidades de red existentes y cada uno de los requerimientos necesarios para su pronta solución, se busca lograr la estructuración de la información que sea requerida y de esta forma se podrá crear una estrategia con la cual se asegure una solución eficiente y rápida.

Buscando dar claridad a la información presentada con el fin de sacar soluciones viables y lograr tratar esta práctica.

Palabras clave: escenarios, funcionamiento, redes, estructuración, soluciones.

Abstract

The present project is focused on the timely solution of two scenarios in which it is sought to achieve an optimal solution in the development and operation of its different networks, where it is sought to be able to address and analyze the different themes, the above from its various points of view and analysis, to determine as much as possible the different exact causes that may arise, their existing network needs will be identified and each one of the requirements necessary for its prompt solution, it is sought to achieve the structuring of the information that is required and of This way you can create a strategy that ensures an efficient and fast solution.

Seeking to clarify the information presented in order to draw viable solutions and manage to address this practice.

Keywords: scenarios, operation, networks, structuring, solutions.

OBJETIVOS

Objetivo general

Adquirir los conocimientos y las diferentes habilidades en el manejo y estudio de la prueba de habilidades en los diferentes escenarios solicitados en cisco packet tracer, en los enrutamientos y soluciones de la red, resolviendo cada uno de los pasos que allí se plantean en el Diplomado de Profundización Cisco denominado prueba de habilidades.

Objetivos específicos

- Buscar y analizar las posibles soluciones, manejo de la herramienta packet tracer.
- Aplicar el conocimiento en las configuraciones básicas de los router.
- Conocer la estructura de la topología y su funcionamiento.
- Identificar los diferentes protocolos en el diseño de seguridad de la red.
- Configurar y aplicar el enrutamiento OSPF con autenticación en cada router.
- Habilitar las diferentes VLAN en la red.
- Aprender a configurar los protocolos DHCP en los router.
- configurar NAT estático y de sobrecarga.
- Definir los protocolos de enrutamiento EIGRP.
- Comprender los diferentes direccionamientos y las máscaras de la red.

Introducción

El presente trabajo se realiza con el fin de adquirir el conocimiento necesario en el manejo de redes las cuales son parte fundamental en nuestros entornos diarios, pues gracias a esto podemos comunicarnos a diario y desde cualquier parte del mundo, son esenciales para nuestros entornos laborales y diferentes servicios que son necesarios en la vida cotidiana, en el presente trabajo denominado prueba de habilidades de cisco, el cual se va a desarrollar en la plataforma de packet tracer la cual se divide en 2 escenarios con topologías de red diferentes y en busca de soluciones que están expuestas con diferentes necesidades. Diseño de Redes, Administración e implementación de Redes, Operación y gestión de Redes. Para el desarrollo de las prácticas propuestas en diversas situaciones. Utilizando los conceptos adquiridos, para la comprensión análisis e interpretación de situaciones, problemas en contextos del desarrollo profesional donde es oportuna y acertada su aplicabilidad y donde es importante el uso de los medios que nos brinda la UNAD.

Se abordará cada una de las necesidades de red más necesarias que se aplica en una topología amplia entre diferentes ciudades, se mostraran los diversos protocolos y la manera en que se van a implementar en la red, logrando una comunicación entre las ciudades que allí se solicitan, estas con protocolos de enrutamiento, los enlaces que se van a manejar desde los diferentes router y la manera en que se determinara la ruta mas confiable para comunicar cada red y su manera de ejecución es decir, incluir la información que se va a tener del tipo de red y los diferentes router que se van a tener de vecinos en dichas redes.

Evaluación – Prueba de habilidades prácticas CCNA

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.

Desarrollo de los escenarios

Escenario 1

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

Topología de red

Los requerimientos solicitados son los siguientes:

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

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

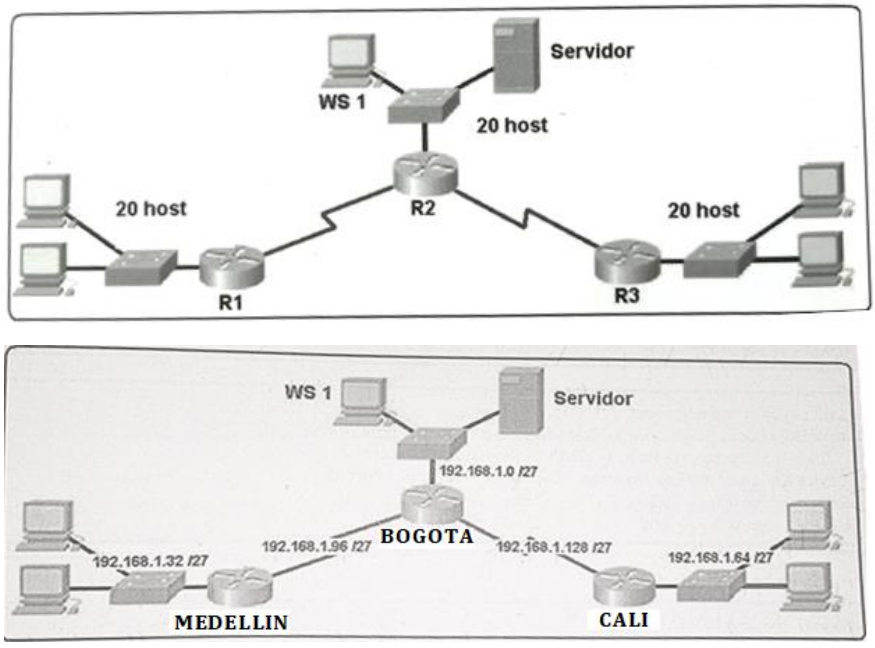
Parte 3: La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.

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

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

Parte 6: Configuración final.

Ilustración 1 topología de la red



Desarrollo de la actividad

Como trabajo inicial se debe realizar lo siguiente.

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).
- Realizar la conexión fisica de los equipos con base en la topología de red

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

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.

Red	Red	192.	168.	1.	000	0	0000	192.168.1.0
	Primero	192.	168.	1.	000	0	0001	192.168.1.1

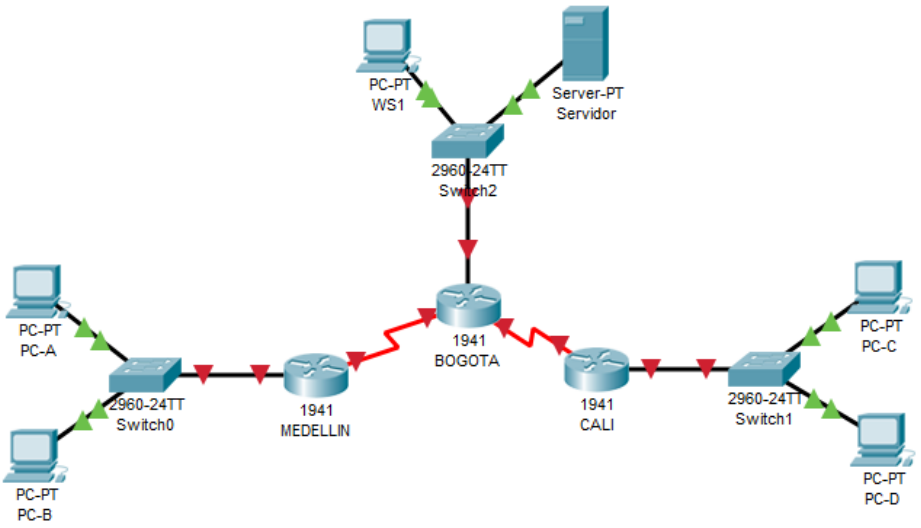
0		192.	168.	1.	000	1	1110	192.168.1.30
		192.	168.	1.	000	1	1111	192.168.1.31
Red 1	Red Primero	192.	168.	1.	001	0	0000	192.168.1.32
		192.	168.	1.	001	0	0001	192.168.1.33
		192.	168.	1.	001	1	1110	192.168.1.62
		192.	168.	1.	001	1	1111	192.168.1.63
• Red 2	Red Primero	192.	168.	1.	010	0	0000	192.168.1.64
		192.	168.	1.	010	0	0001	192.168.1.65
		192.	168.	1.	010	1	1110	192.168.1.94
		192.	168.	1.	010	1	1111	192.168.1.95
• Red 3	Red Primero	192.	168.	1.	011	0	0000	192.168.1.96
		192.	168.	1.	011	0	0001	192.168.1.97
		192.	168.	1.	011	1	1110	192.168.1.126
		192.	168.	1.	011	1	1111	192.168.1.127
• Red 4	Red Primero	192.	168.	1.	100	0	0000	192.168.1.128
		192.	168.	1.	100	0	0001	192.168.1.129
		192.	168.	1.	100	1	1110	192.168.1.158
		192.	168.	1.	100	1	1111	192.168.1.159
• Red 5	Red Primero	192.	168.	1.	101	0	0000	192.168.1.160
		192.	168.	1.	101	0	0001	192.168.1.161
		192.	168.	1.	101	1	1110	192.168.1.190
		192.	168.	1.	101	1	1111	192.168.1.191
• Red 6	Red Primero	192.	168.	1.	110	0	0000	192.168.1.192
		192.	168.	1	110	0	0001	192.168.1.193
		192.	168.	1.	110	1	1110	192.168.1.222
		192.	168.	1.	110	1	1111	192.168.1.223
• Red 7	Red Primero	192.	168.	1.	111	0	0000	192.168.1.224
		192.	168.	1.	111	0	0001	192.168.1.225
		192.	168.	1.	111	1	1110	192.168.1.254
		192.	168.	1.	111	1	1111	192.168.1.255

https://www.seaccna.com/calculo-de-subredes-ipv4/

https://www.calculadora-redes.com/

Se realizará la conexión física de los equipos con base en la topología de red

Ilustración 2 topología de la red



b. Asignar una dirección IP a la red.

Asignaremos 192.168.1.0

Parte 2: Configuración Básica.

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

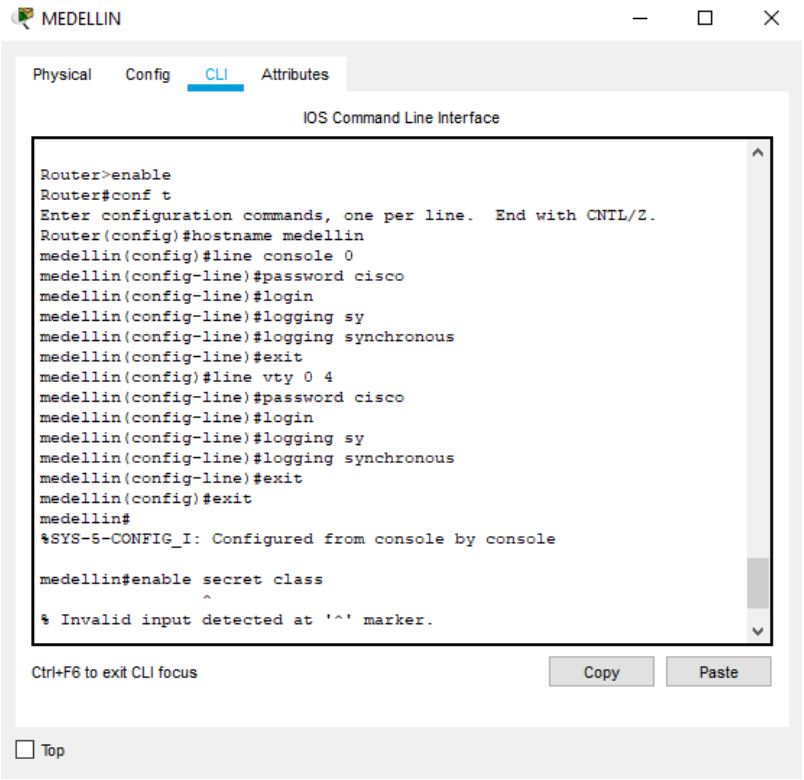
	R1	R2	R3
Nombre de Host	**MEDELLIN**	**BOGOTA**	**CALI**
Dirección de Ip en interfaz Serial 0/0	192.168.1.99	192.168.1.98	
Dirección de Ip en interfaz Serial 0/1		192.168.1.130	192.168.1.131
Dirección de Ip en interfaz GB 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	**Eigrp**	**Eigrp**	**Eigrp**
Sistema Autónomo	10	10	10
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0
	IP	**Mascara**	**Gateway**
PC-A	192.168.1.35	255.255.255.224	192.168.1.0
PC-B	192.168.1.36	255.255.255.224	192.168.1.0
PC-C	192.168.1.66	255.255.255.224	192.168.1.0
PC-D	192.168.1.67	255.255.255.224	192.168.1.0
WS1	192.168.1.226	255.255.255.224	192.168.1.0

Servidor PT	192.168.1.227	255.255.255.224	192.168.1.0

Vamos a dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, Para esta configuracion vamos a utilizar la contraseña de cisco.

Configuramos el router con sus diferentes contraseñas:

Ilustración 3 R1-Medellin

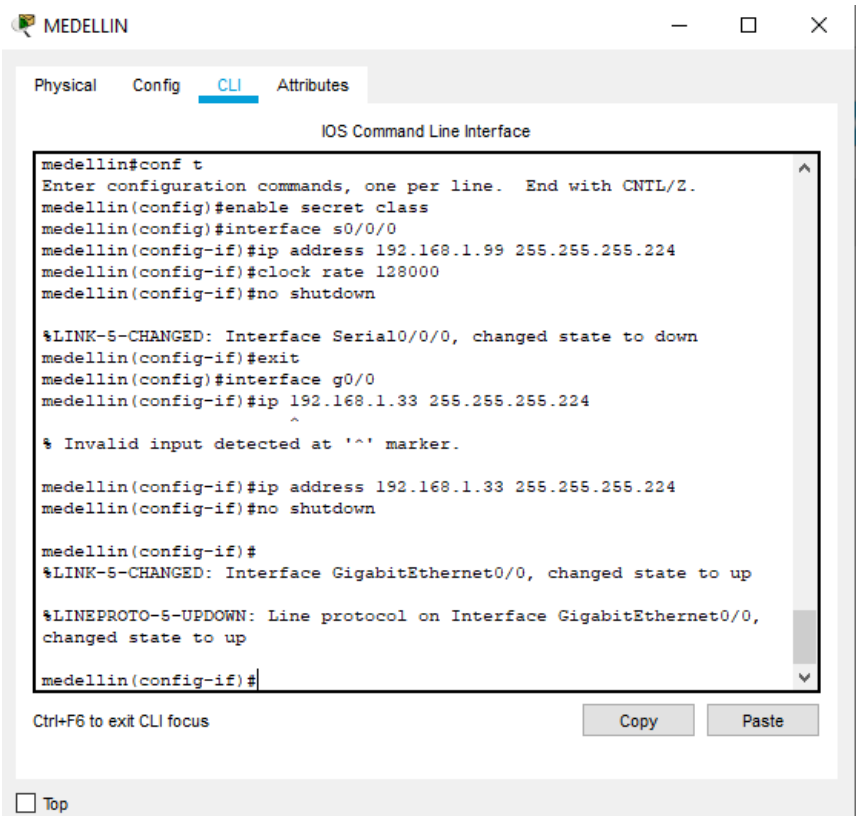


Los comandos utilizados son los siguientes :

Router>enable
Router#configure terminal
Router(config)#no ip domain-lookup
Router(config)#hostname Medellín
Medellín(config)# line console 0
Medellín(config-line) #password cisco
Medellín(config-line) #login
Medellín(config-line) #logging synchronous
Medellín(config-line) #exit
Medellín(config)# line vty 0 4
Medellín(config-line) #password cisco
Medellín(config-line) #login
Medellín(config-line) #logging synchronous

Medellín(config-line) #exit
Medellín(config)#exit

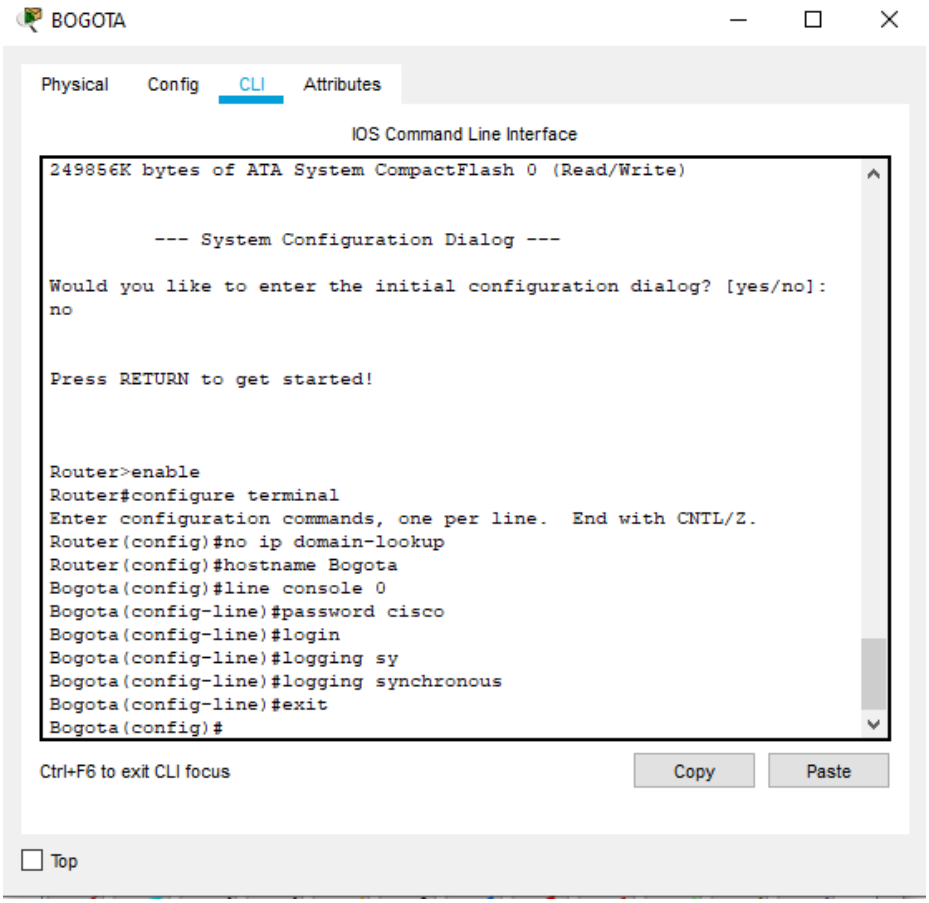
Ilustración 4 Medellín 2



Los comandos utilizados son los siguientes :

Medellín>enable
Medellín# configure terminal
Medellín(config)# enable secret class
Medellín(config)# interface s0/0/0
Medellín(config-if)# ip address 192.168.1.99 255.255.255.224
Medellín(config-if)#clock rate 128000
Medellín(config-if)#no shutdown
Medellín(config)#interface g0/0
Medellín(config-if)# ip address 192.168.1.33 255.255.255.224
Medellín(config-if)#no shutdown

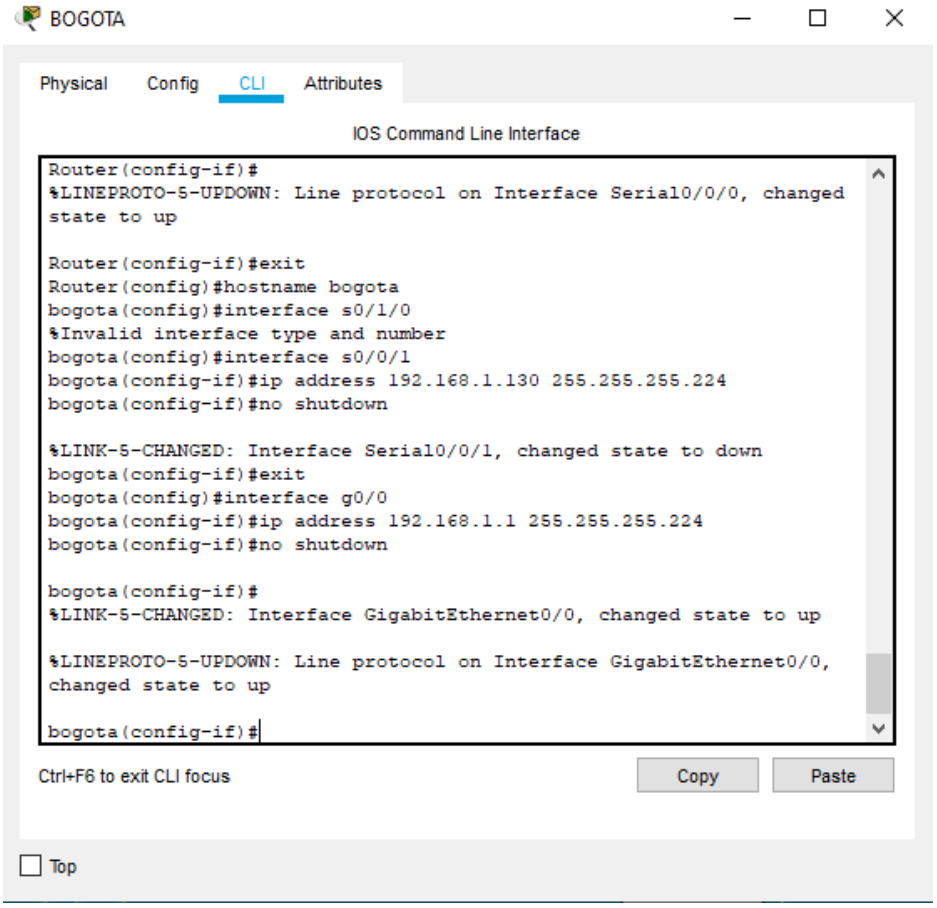
Ilustración 5 R2-Bogota



Los comando utilizados son los siguientes

Router>enable
Router#configure terminal
Router(config)#no ip domain-lookup
Router(config)#hostname Bogotá
Bogotá(config)# line console 0
Bogotá(config-line)#password cisco
Bogotá(config-line)#login
Bogotá (config-line)#logging synchronous
Bogotá (config-line)#exit
Bogotá (config)# line vty 0 4
Bogotá (config-line)#password cisco
Bogotá (config-line)#login
Bogotá (config-line)#logging synchronous
Bogotá (config-line)#exit
Bogotá(config)#exit

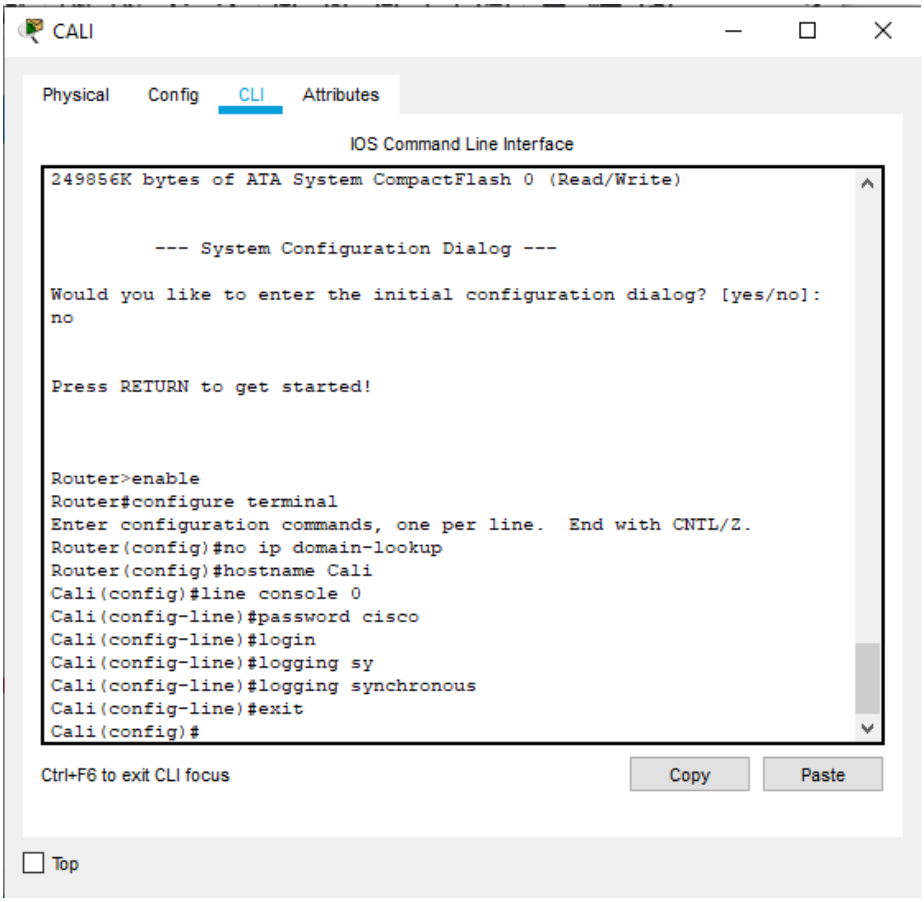
Ilustración 6 Bogotá 2



Los comando utilizados son los siguientes

Bogotá>enable
Bogotá # configure terminal
Bogotá (config)# enable secret class
Bogotá (config)# interface s0/0/0
Bogotá (config-if)# ip address 192.168.1.98 255.255.255.224
Bogotá (config)# interface s0/0/1
Bogotá (config-if)# ip address 192.168.1.130 255.255.255.224
Bogotá (config-if)#no shutdown
Bogotá (config)#interface g0/0
Bogotá (config-if)# ip address 192.168.1.1 255.255.255.224
Bogotá (config-if)#no shutdown

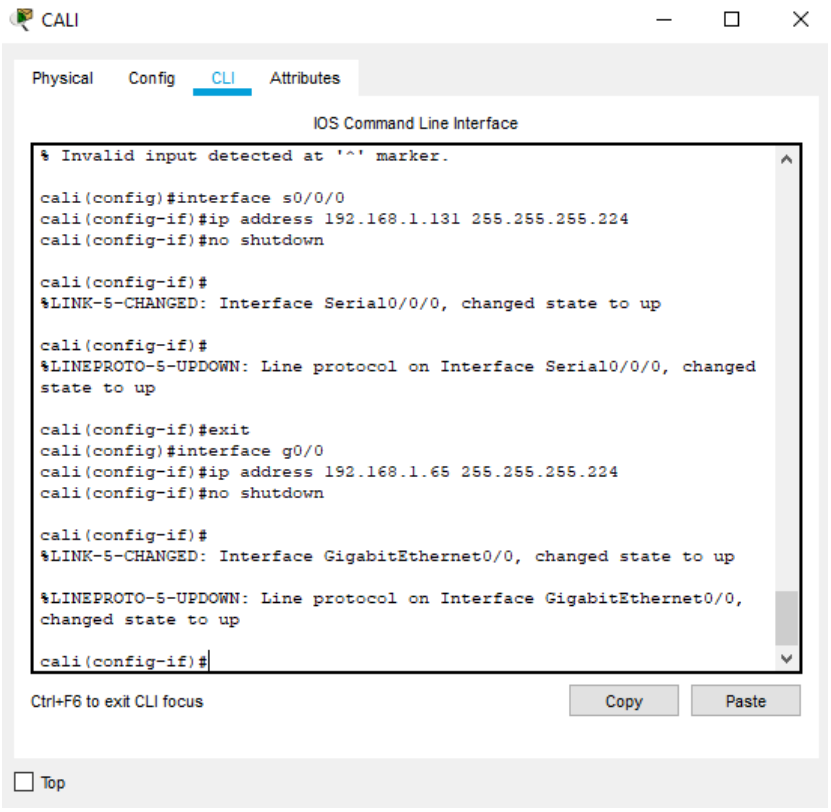
Ilustración 7 R3-Cali



Los comando utilizados son los siguientes

Router>enable
Router#configure terminal
Router(config)#no ip domain-lookup
Router(config)#hostname Cali
Cali(config)# line console 0
Cali (config-line)#password cisco
Cali (config-line)#login
Cali (config-line)#logging synchronous
Cali (config-line)#exit
Cali (config)# line vty 0 4
Cali (config-line)#password cisco
Cali (config-line)#login
Cali (config-line)#logging synchronous
Cali (config-line)#exit
Cali (config)#exit

Ilustración 8 Cali 2



Los comando utilizados son los siguientes

Bogotá>enable
Bogotá # configure terminal
Bogotá (config)# enable secret class
Bogotá (config)# interface s0/0/0
Bogotá (config-if)# ip address 192.168.1.131 255.255.255.224
Bogotá (config)#interface g0/0
Bogotá (config-if)# ip address 192.168.1.65 255.255.255.224
Bogotá (config-if)#no shutdown
Luego vamos asignarle la direccion ip a las computadoras para esto dejamos como Gateway la ip de la puerta de enlace que seria 192.168.1.0

PCS-Medellin
PC-A

Ip address: 192.168.1.35
Sudnet Mask: 255.255.255.224
Default Gateway: 192.168.1.0

PC-B

Ip address: 192.168.1.36
Sudnet Mask: 255.255.255.224
Default Gateway: 192.168.1.0

PCS-Bogota
WS1

Ip address: 192.168.1.226
Sudnet Mask: 255.255.255.224
Default Gateway: 192.168.1.0

Servidor

Ip address: 192.168.1.227
Sudnet Mask: 255.255.255.224
Default Gateway: 192.168.1.0

PCS-Cali
PC-C

Ip address: 192.168.1.66
Sudnet Mask: 255.255.255.224
Default Gateway: 192.168.1.0

PC-D

Ip address: 192.168.1.67
Sudnet Mask: 255.255.255.224
Default Gateway: 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.

Verificamos la la tabla de enrutamiento en cada uno de los router con el comando #show ip route.

Ilustración 9 R1-Medellin

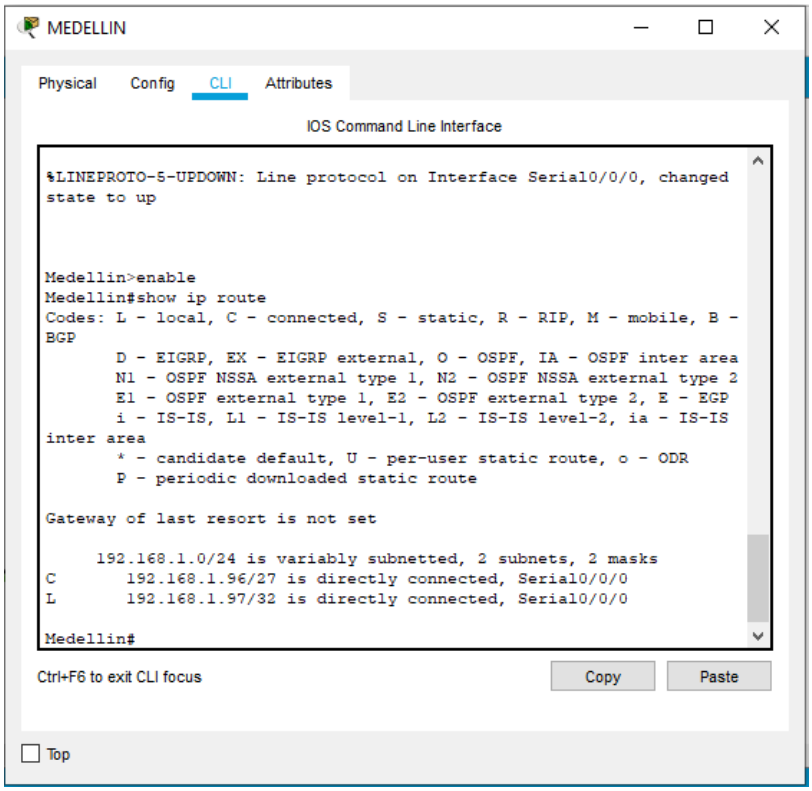


Ilustración 10 R2-Bogota

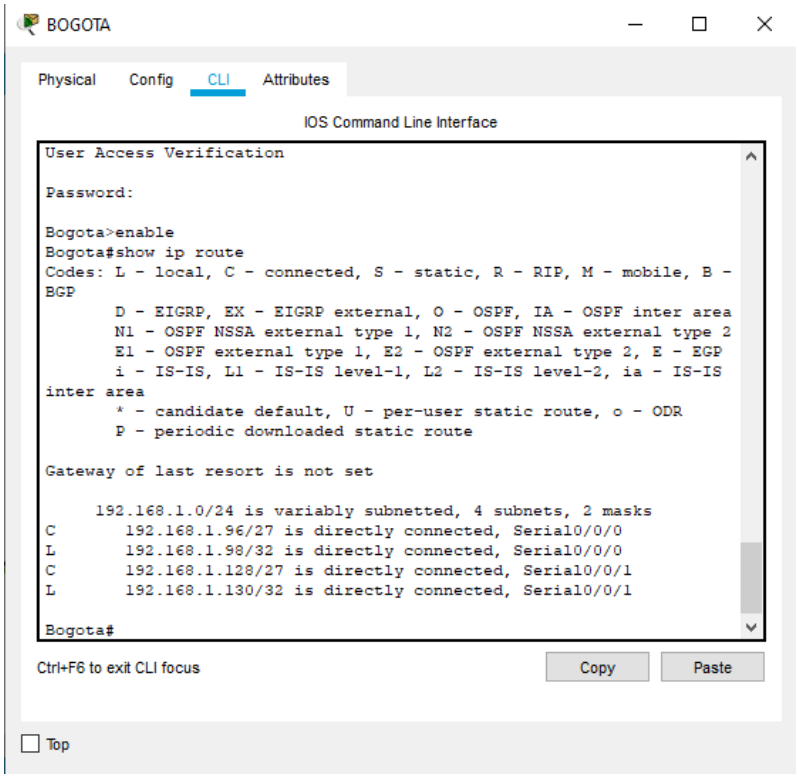
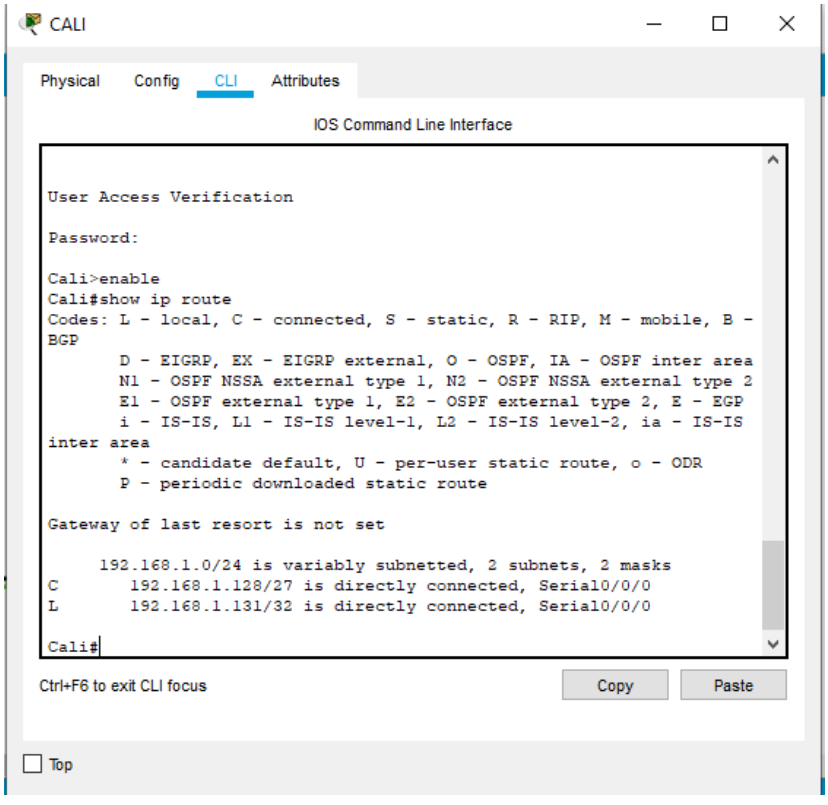


Ilustración 11 R3-Cali



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

Ilustración 12 R1-Medellin

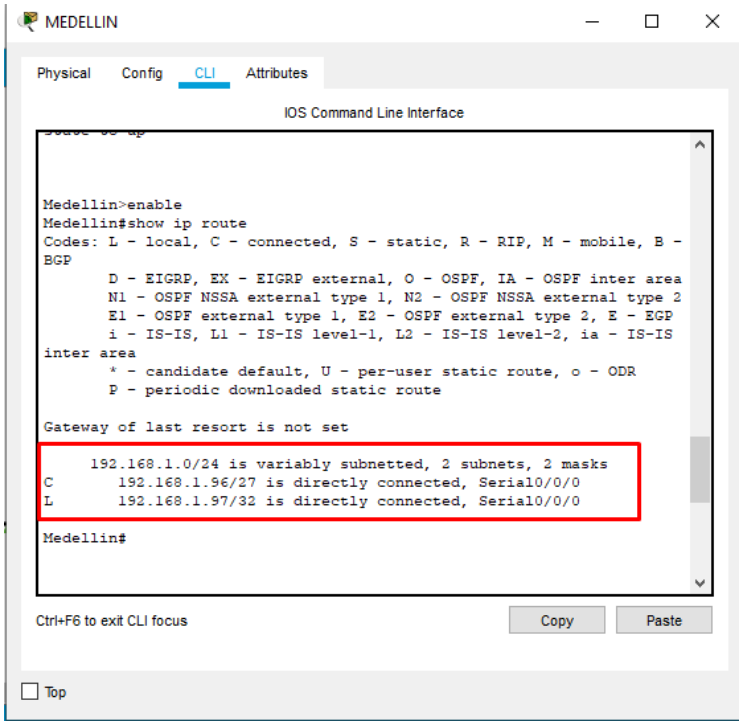


Ilustración 13 R2-Bogota

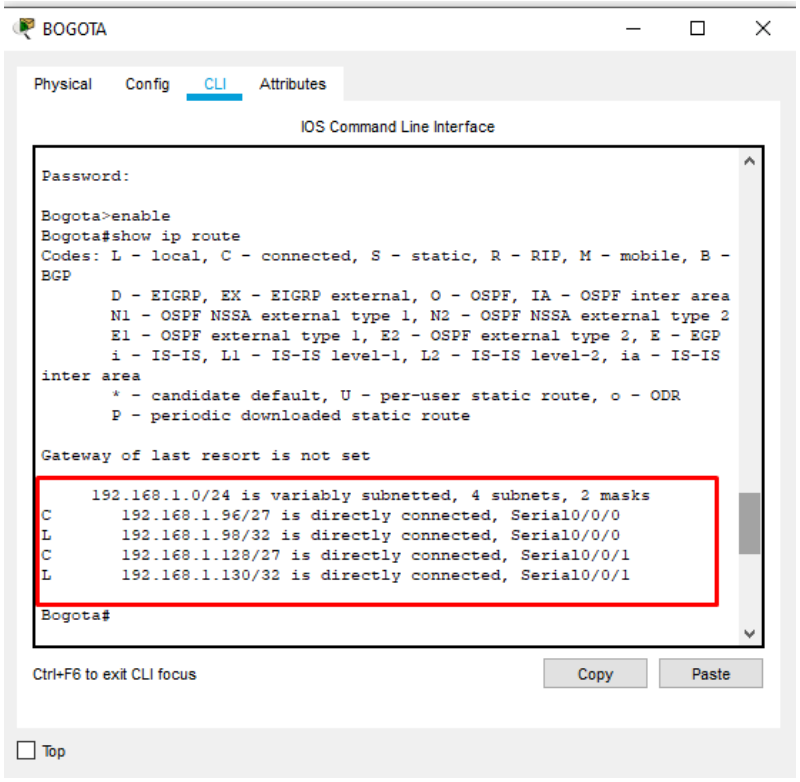
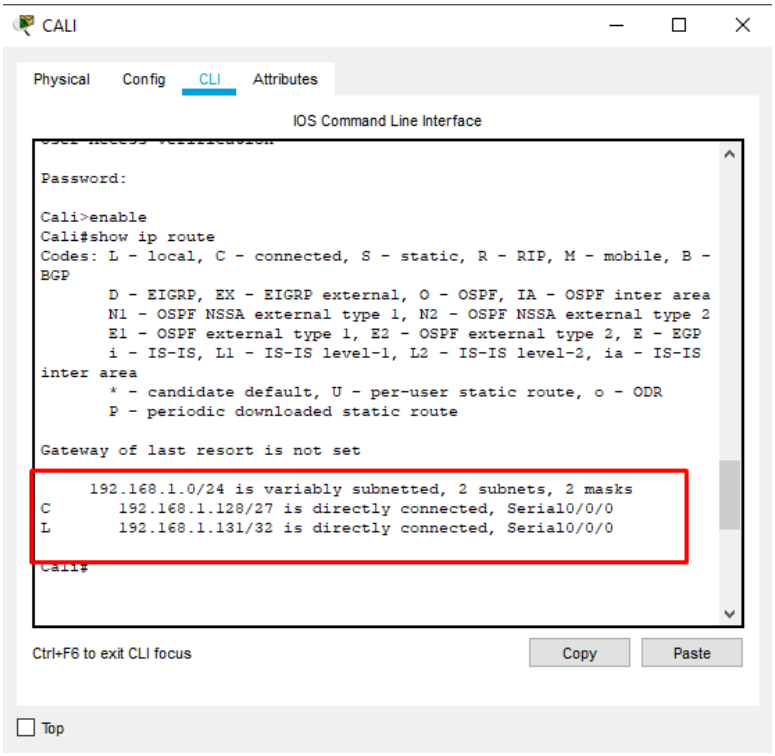


Ilustración 14 R3-Cali



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

Verificamos ingresando el comando #show cdp neighbors

Ilustración 15 R1-Medellin

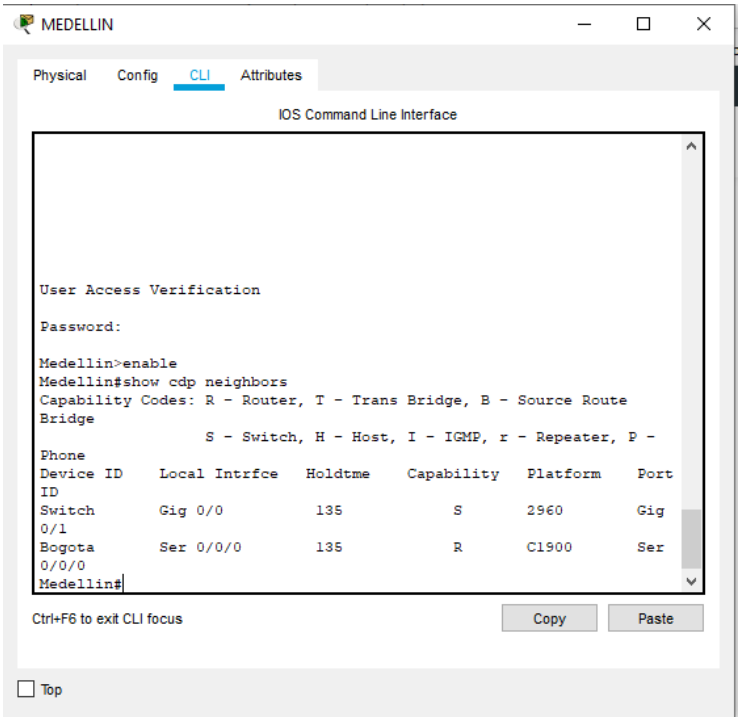


Ilustración 16 R2-Bogota

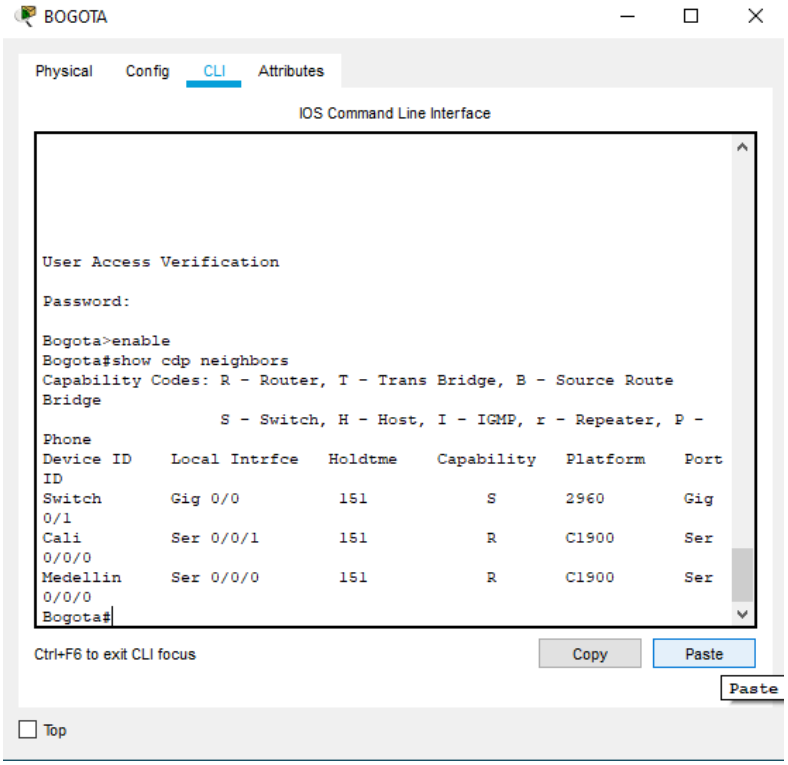
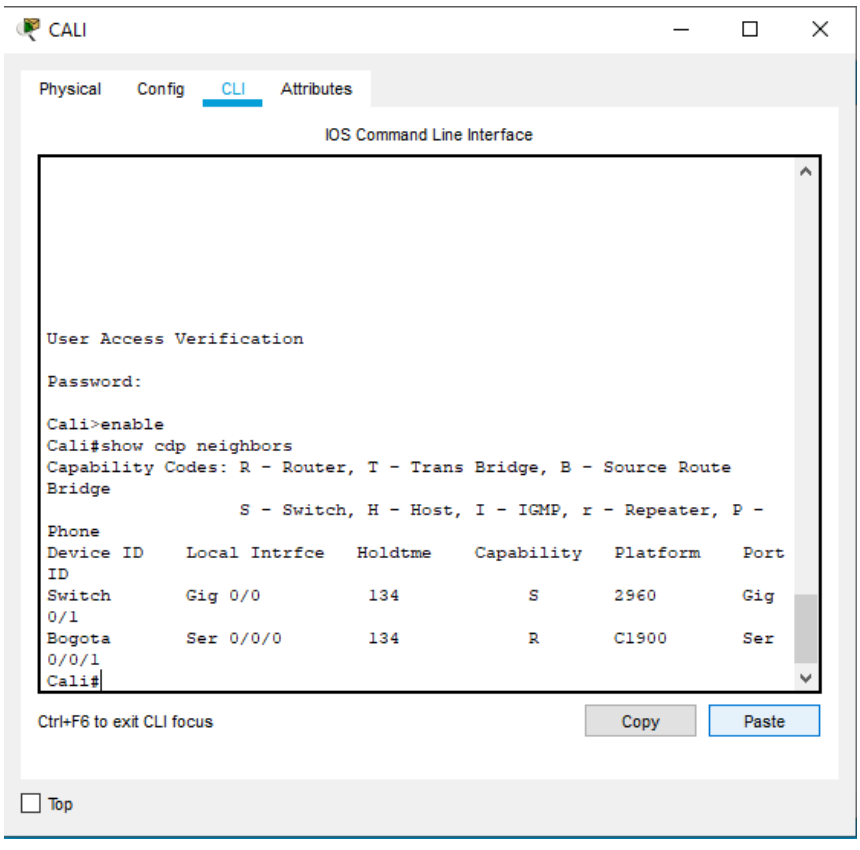


Ilustración 17 R3-Cali

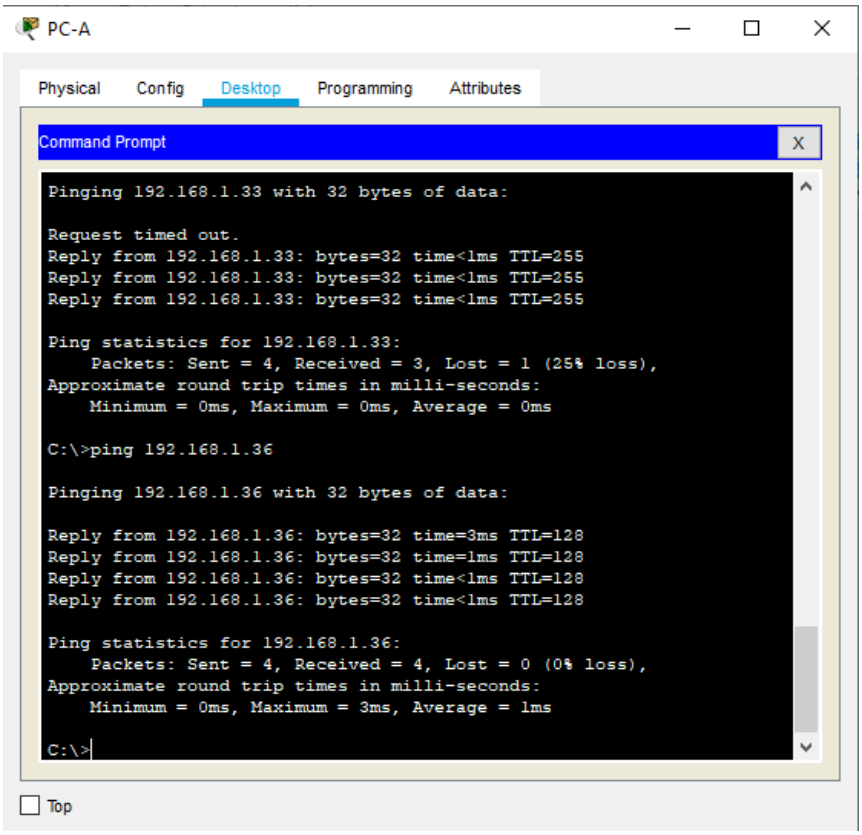


e. Realizar una prueba de conectividad en cada tramo de la ruta usando Ping.

Hacemos ping para verificar conectividad entre redes:

La primer red nos muestre una conectividad entre ella, esto haciendo ping entre 192.168.1.35 a 192.168.1.36

Ilustración 18 PING PC-A



Hacemos ping en el router:

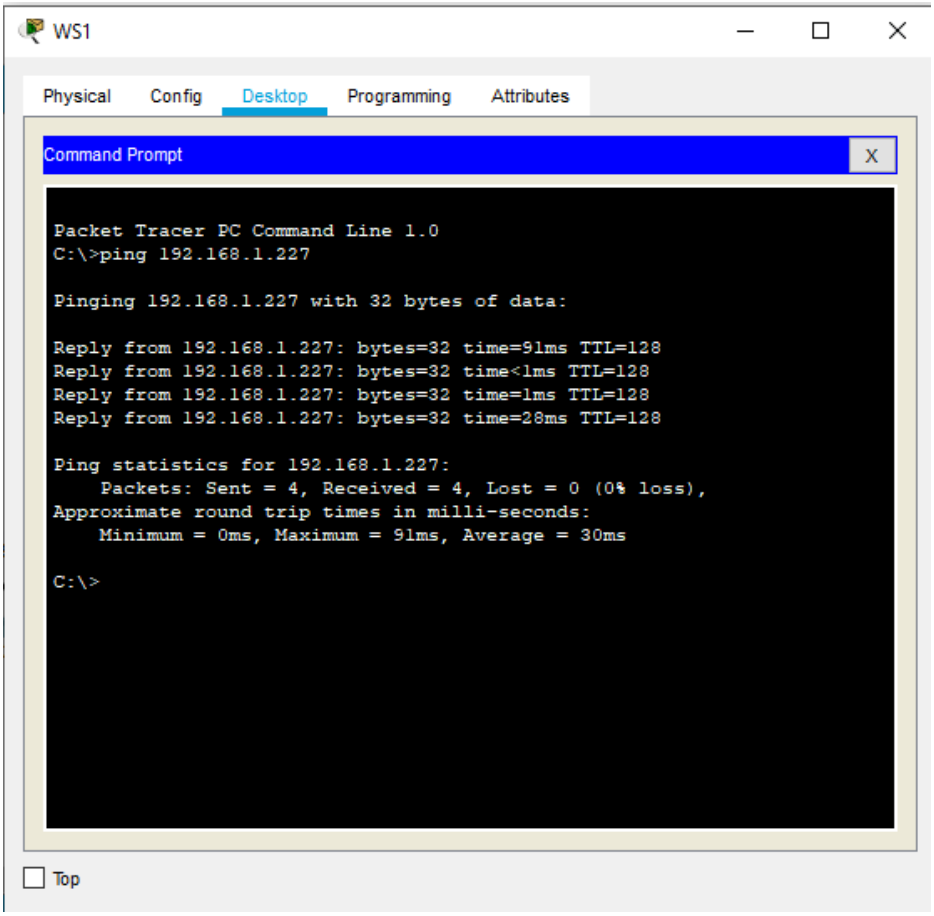
Ilustración 19 PING en router

```
medellin>enable
Password:
medellin#ping 192.168.1.35

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.35, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

La segunda red nos muestre una conectividad entre ella, esto haciendo ping entre 192.168.1.226 a 192.168.1.227

Ilustración 20 PING WS1



Hacemos ping en el router:

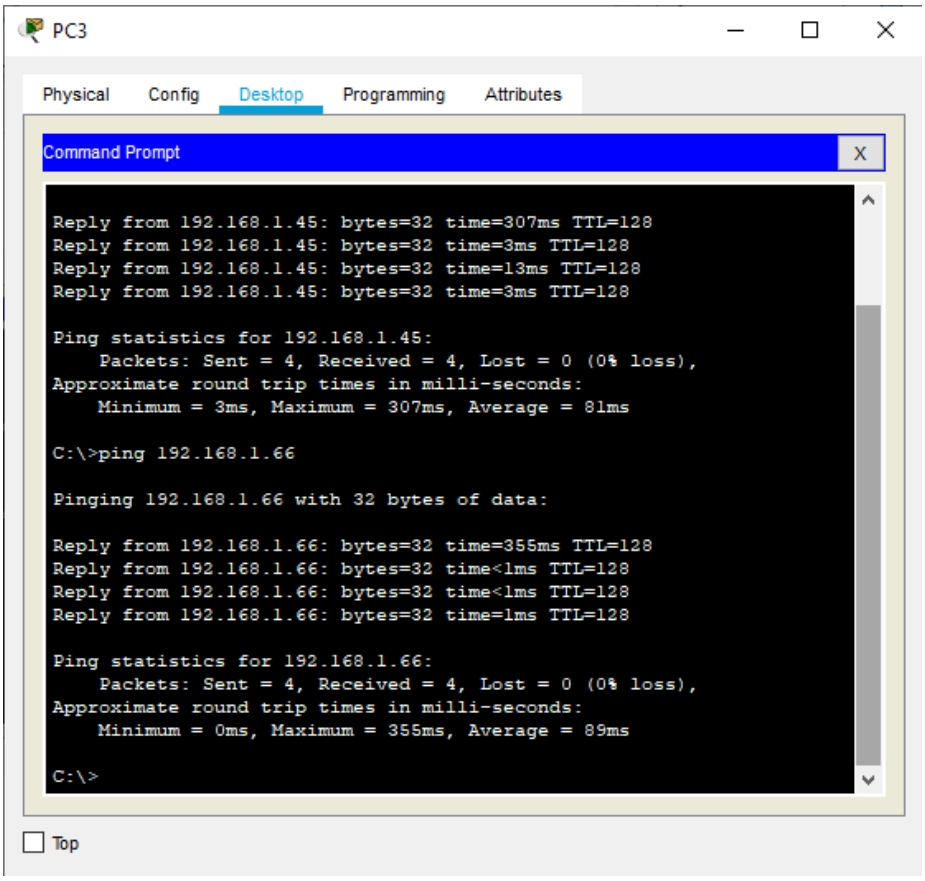
Ilustración 21 PING en router

```
bogota>enable
Password:
Password:
bogota#ping 192.168.1.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms
```

La tercera red nos muestre una conectividad entre ella, esto haciendo ping entre 192.168.1.67 a 192.168.1.66

Ilustración 22 PING PC-3



Hacemos ping en el router:

Ilustración 23 PING en router

```
cali>ping 192.168.1.67

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.67, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms

cali>
```

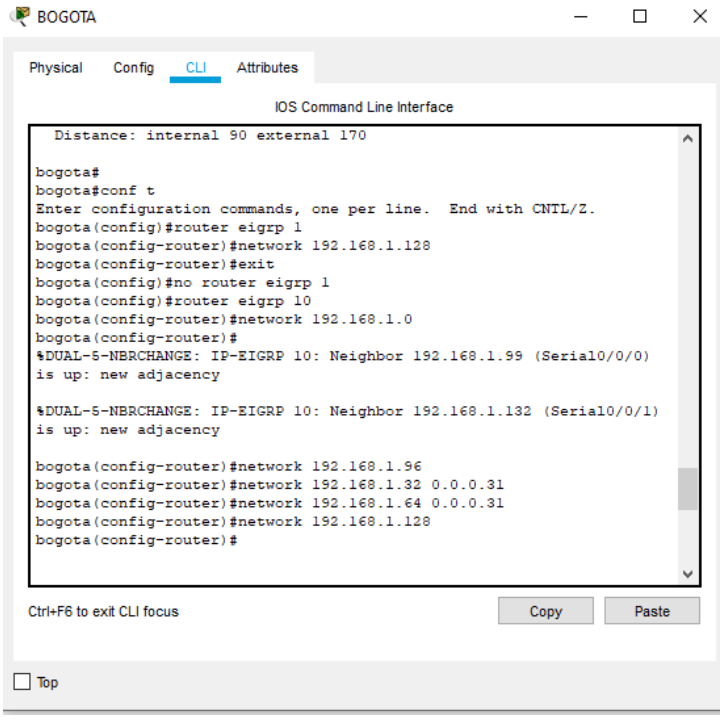
Parte 3: Configuración de Enrutamiento.

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

Iniciamos con:

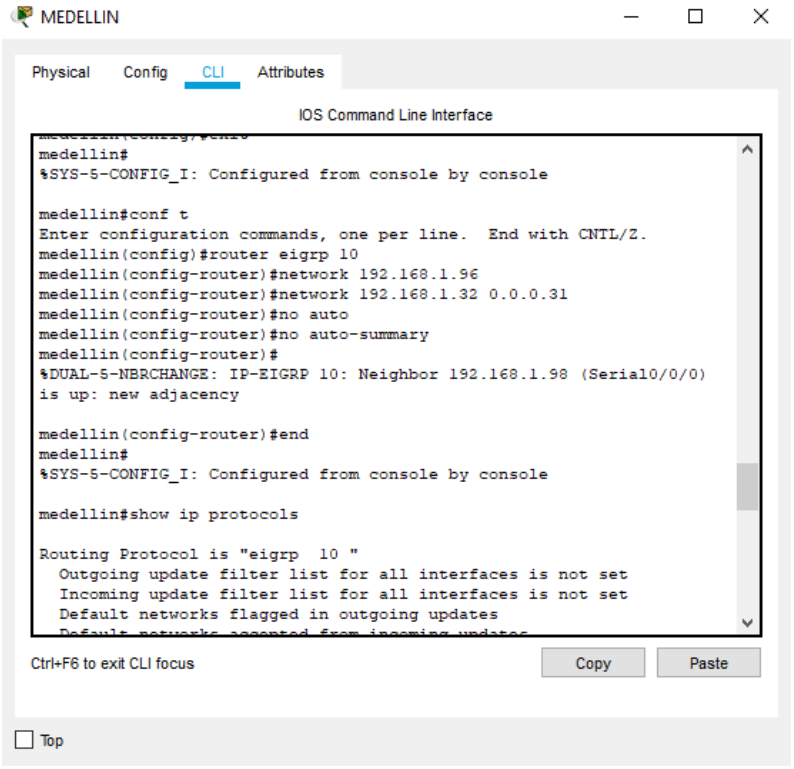
Asignamos el eigrp en Bogotá

Ilustración 24 EIGRP en Bogotá



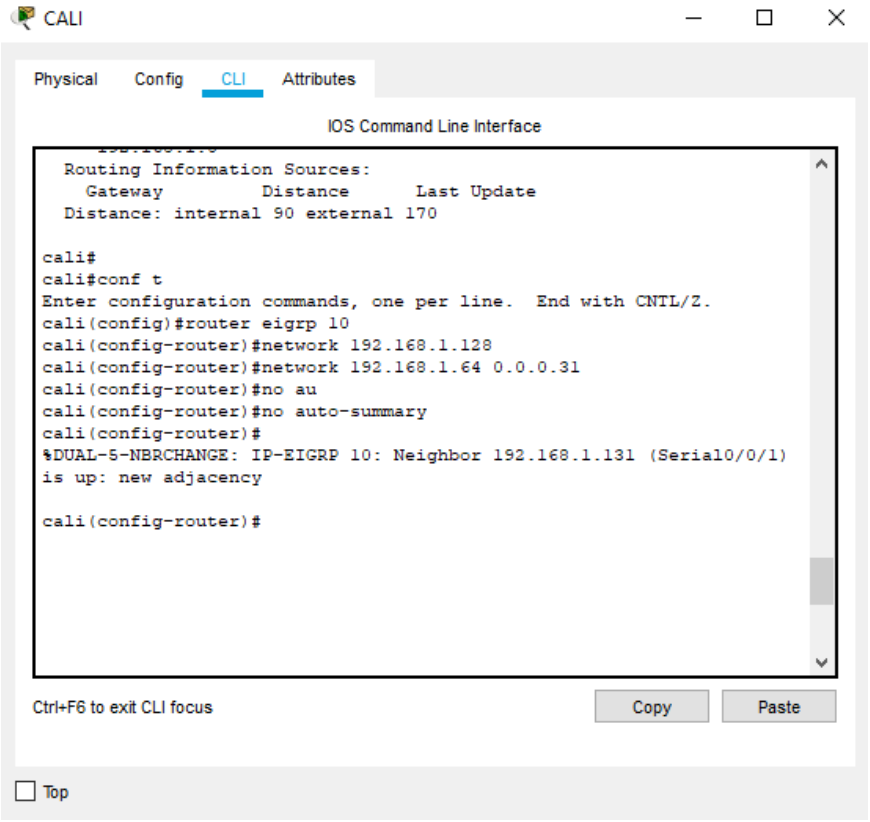
Asignamos el eigrp en Medellín

Ilustración 25 EIGRP en Medellín



Asignamos el eigrp en Cali

Ilustración 26 EIGRP en Cali



Los comandos que se van a utilizar son los siguientes:

Medellín>enable
Medellín# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Medellín(config)#router eigrp 10
Medellín(config-router)#network 192.168.1.96
Medellín(config-router)#network 192.168.1.32 0.0.0.31
Medellín(config-router)#no auto-summary
Medellín(config-router)#exit
Medellín(config)#exit
Medellín#
%SYS-5-CONFIG_I: Configured from console by console
Medellín#

Cali>enable
Cali #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cali (config)#router eigrp 10
Cali (config-router)#network 192.168.1.128
Cali (config-router)#network 192.168.1.54 0.0.0.31
Cali (config-router)#no auto-summary

Cali (config-router)#exit
Cali (config)#exit
Cali #
%SYS-5-CONFIG_I: Configured from console by console
Cali #

Bogotá>enable
Bogotá #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Bogotá (config)#router eigrp 10
Bogotá (config-router)#network 192.168.1.0
Bogotá (config-router)#no auto-summary
Bogotá (config-router)#exit
Bogotá (config)#exit
Bogotá #
%SYS-5-CONFIG_I: Configured from console by console
Bogotá #

Asignamos el comando #redistribute static

Ilustración 27 Medellín-comando #redistribute static

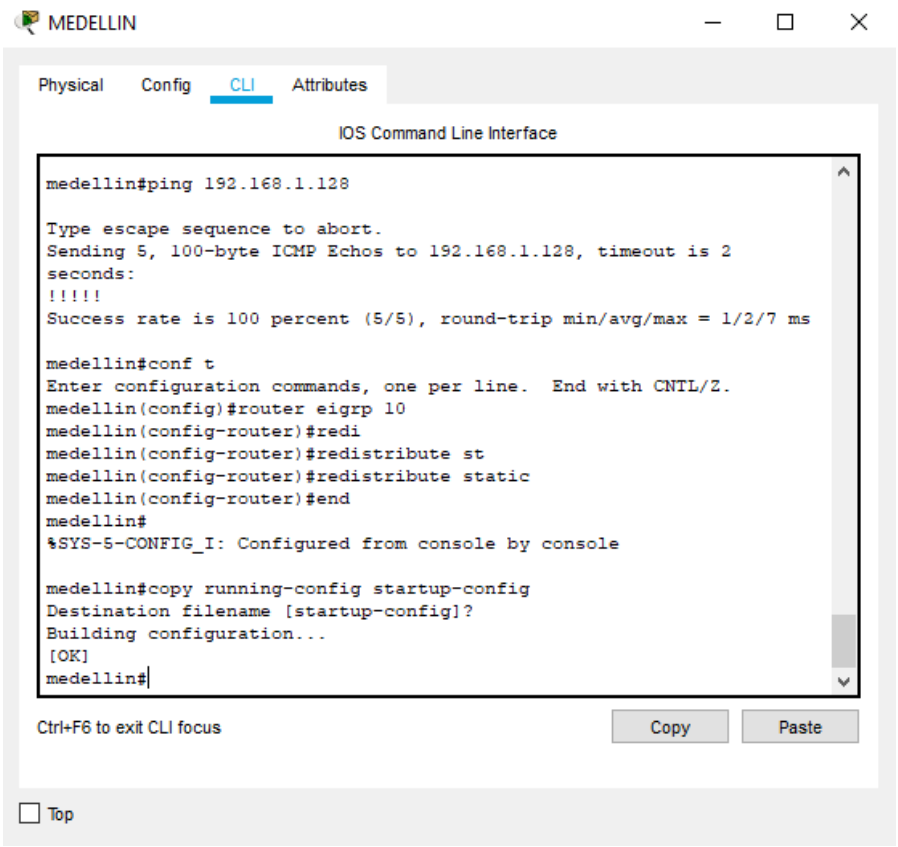


Ilustración 28 Bogotá-comando #redistribute static

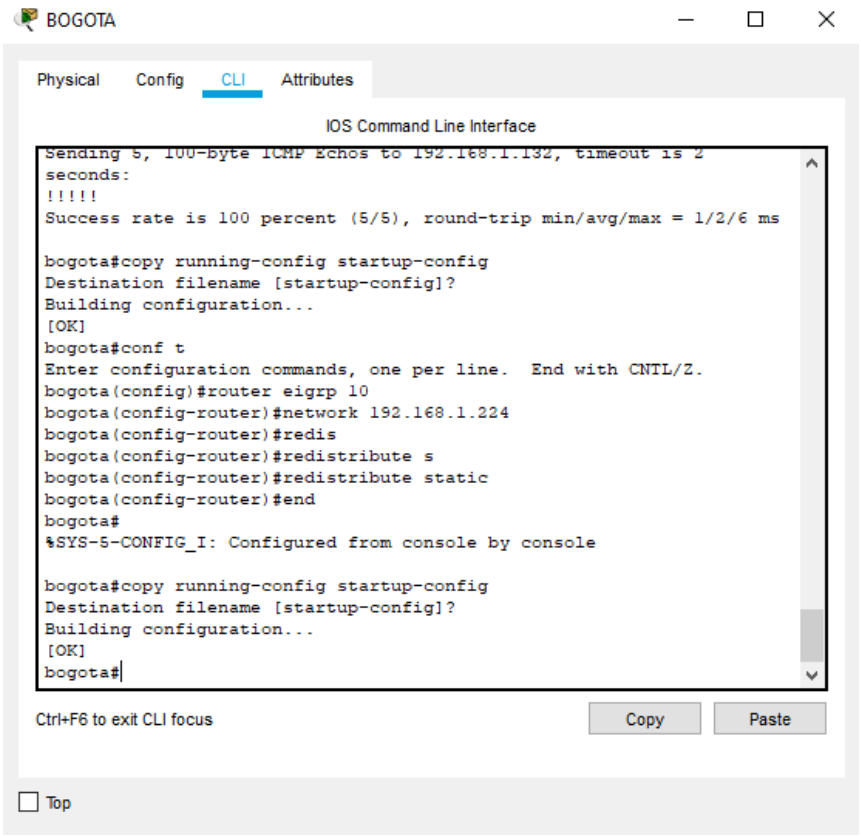
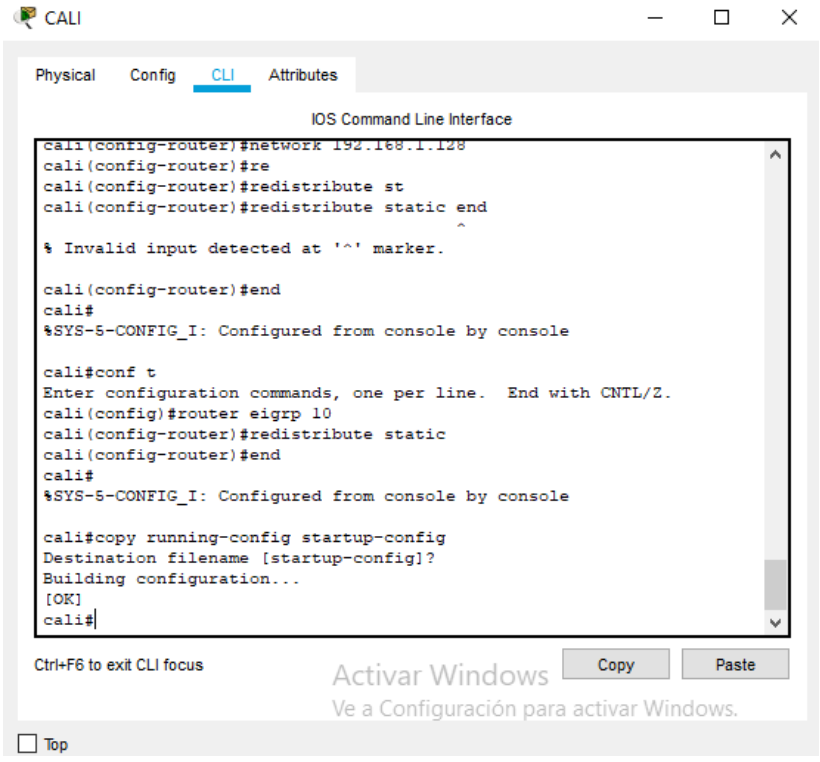


Ilustración 29 Cali-comando #redistribute static



b. Verificar si existe vecindad con los routers configurados con EIGRP. Vamos a utilizar el comando show ip eigrp neighbor.

Ilustración 30 Medellín-comando show ip eigrp

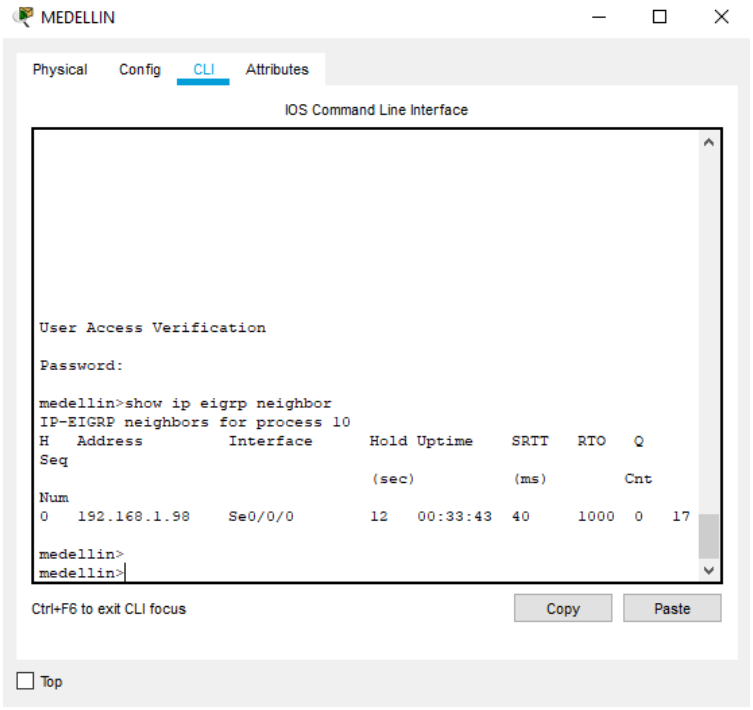


Ilustración 31 Bogotá-comando show ip eigrp

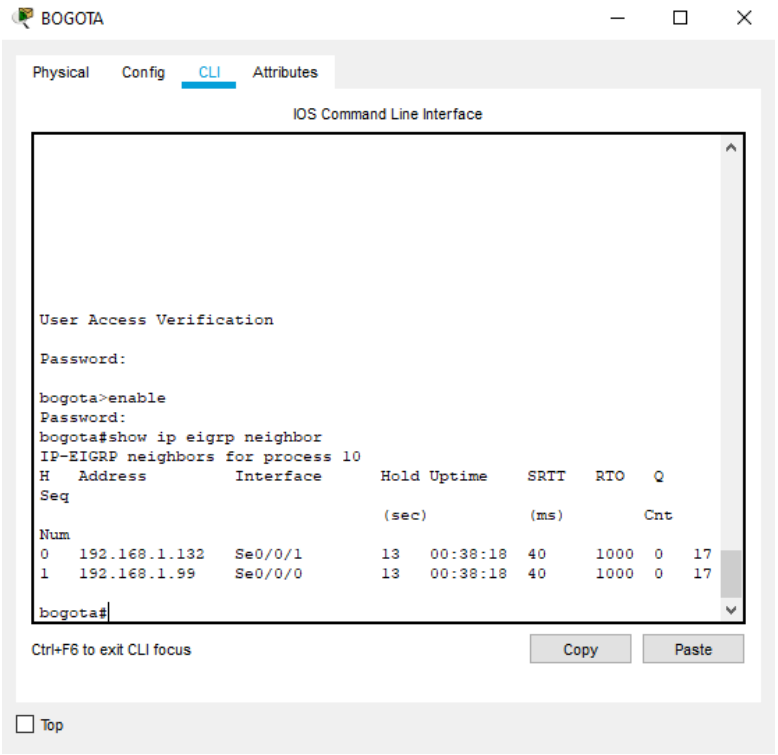
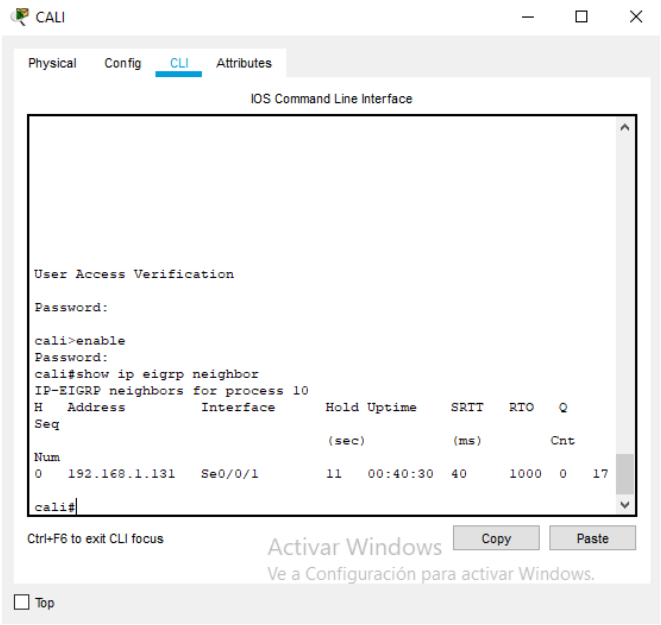


Ilustración 32 Cali-comando show ip eigrp



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

Vamos a utilizar el comando show ip route

Ilustración 33 Medellín-comando #show ip route

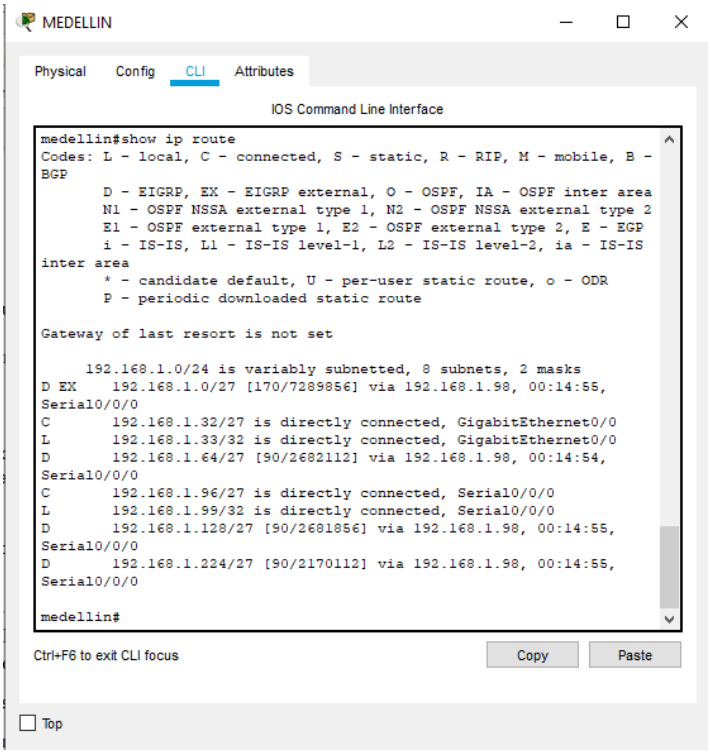


Ilustración 34 Bogotá-comando #show ip route

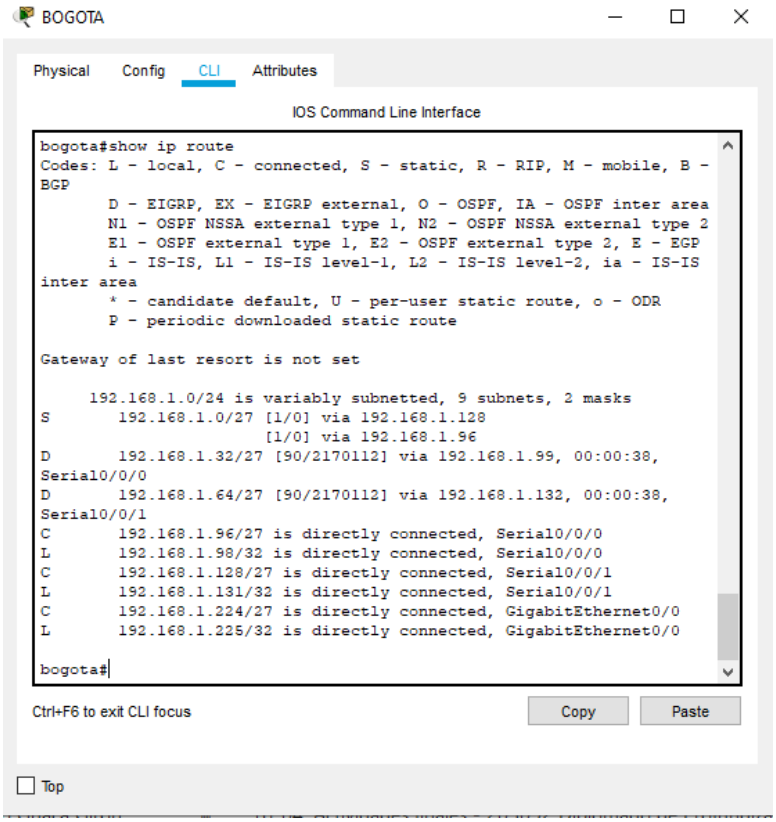
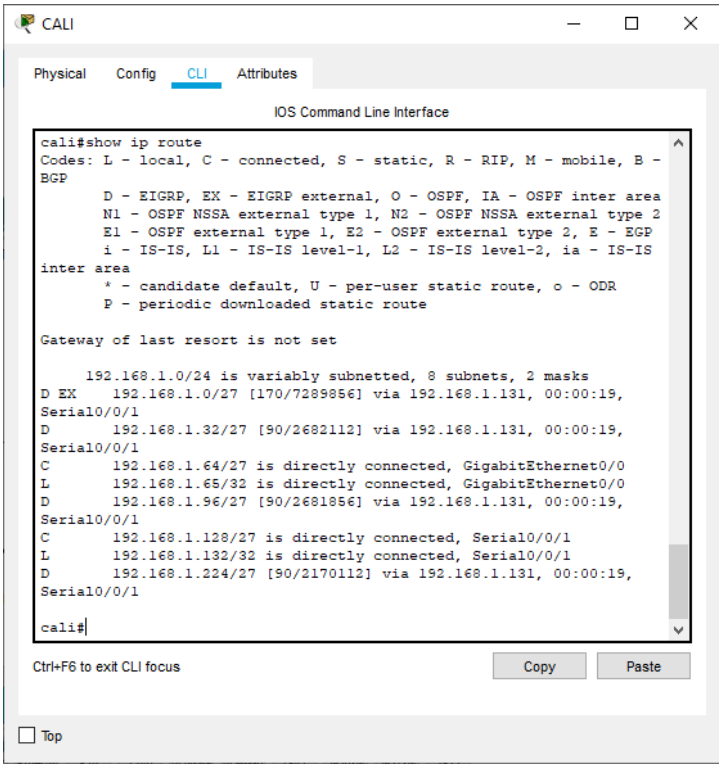


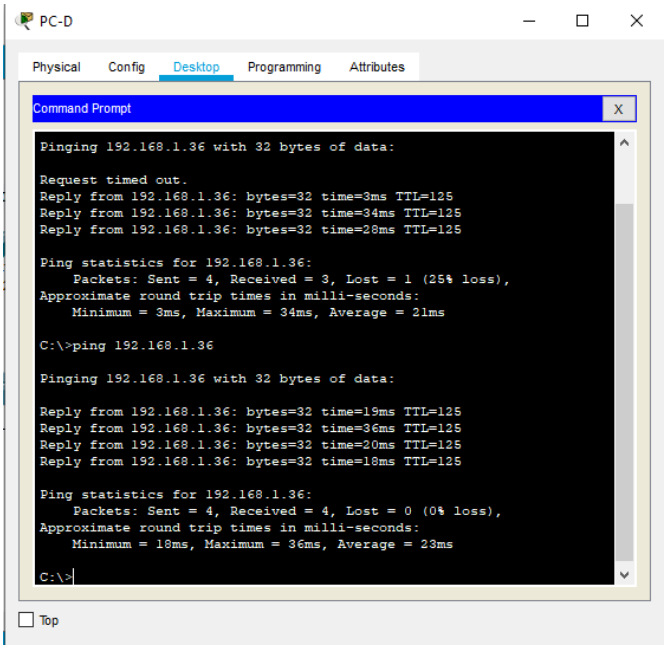
Ilustración 35 Cali-comando #show ip route



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.

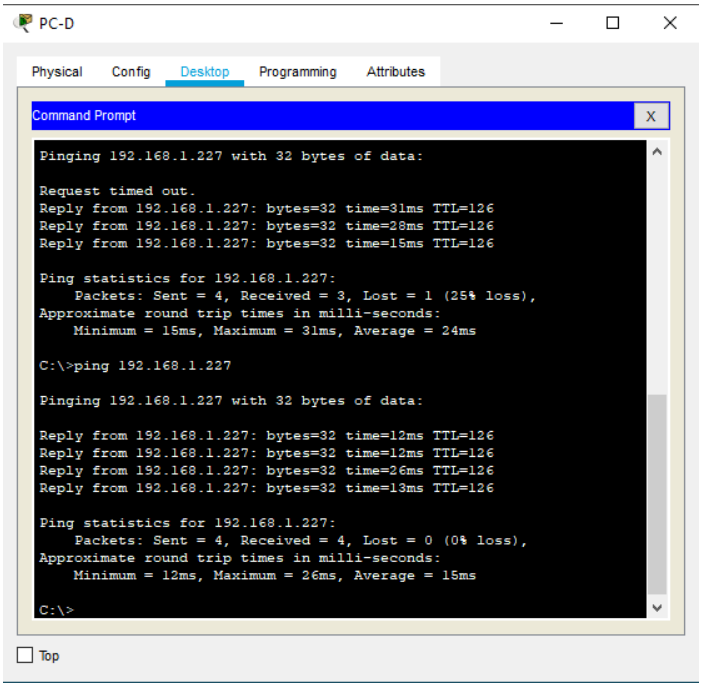
En este paso vamos a hacer PING PC-D A PC-B

Ilustración 36 PING PC-D A PC-B



En este paso vamos a hacer PING PC-D A Servido

Ilustración 37PING PC-D A Servido



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

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

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

Conexión de Medellín por medio de telnet a Bogotá y Cali:

Ilustración 38 conexión TELNET

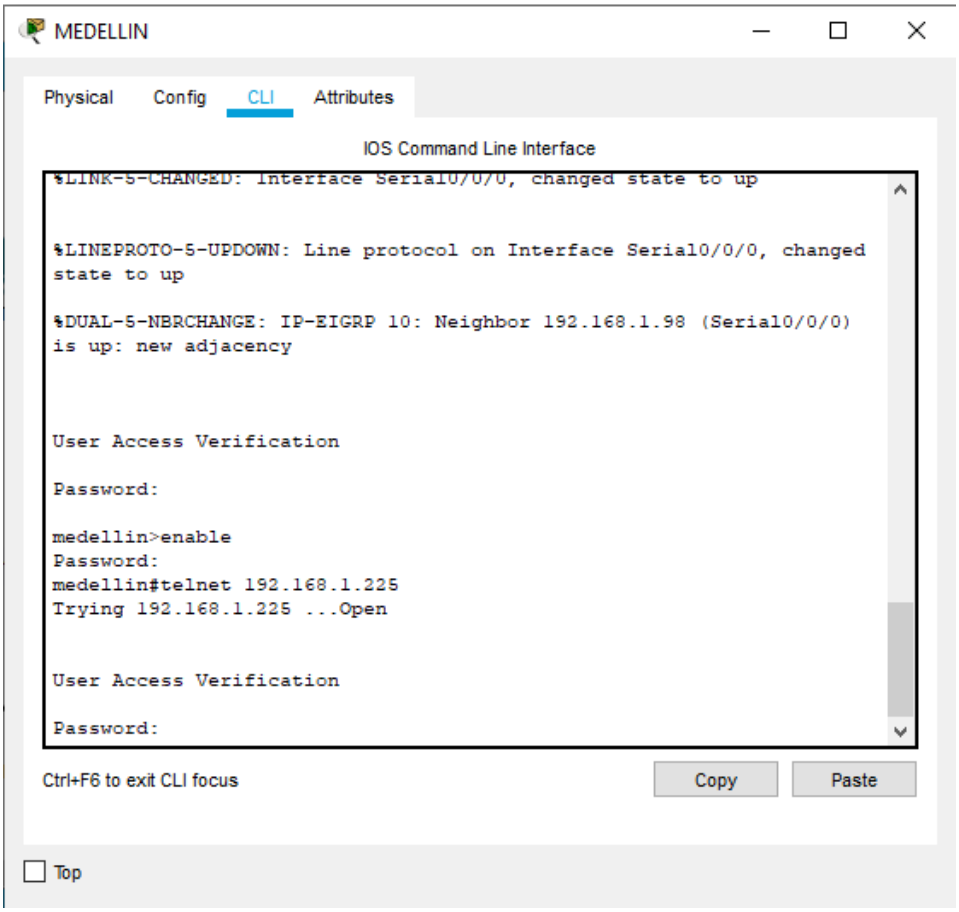
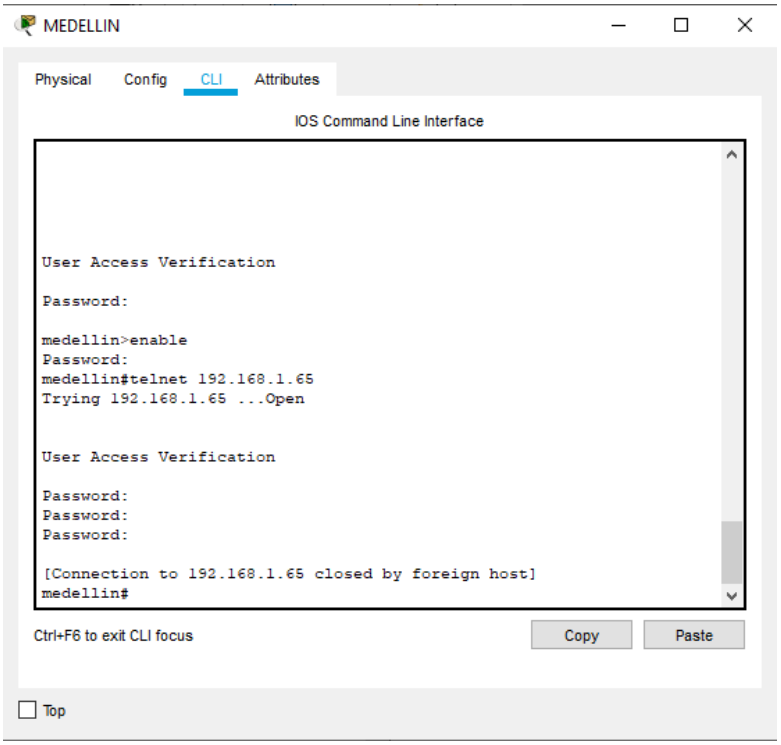
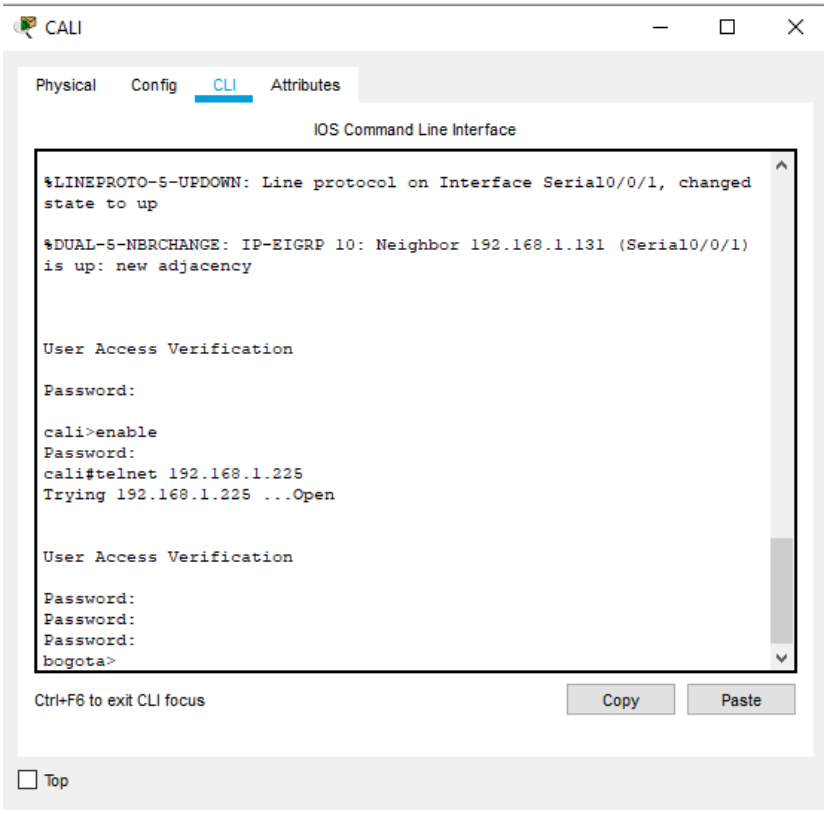


Ilustración 39 Conexión TELNET



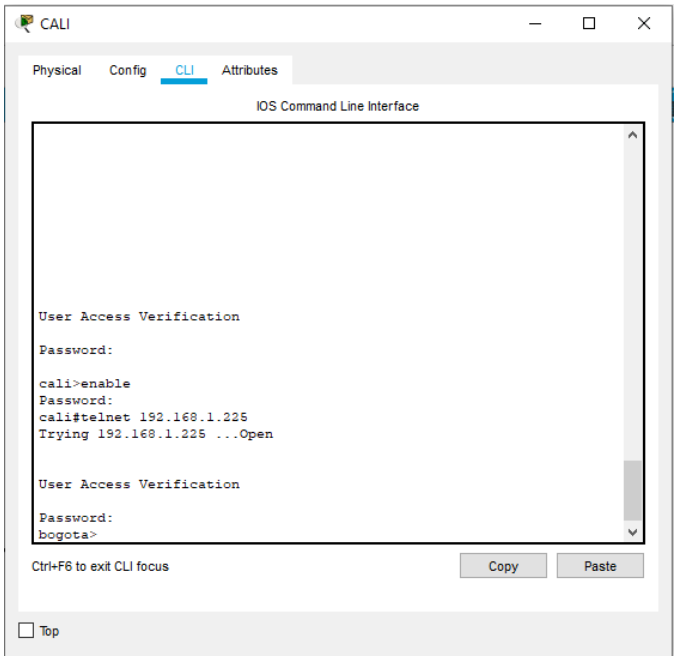
Conexión de Cali por medio de telnet a Medellín:

Ilustración 40 Conexión TELNET



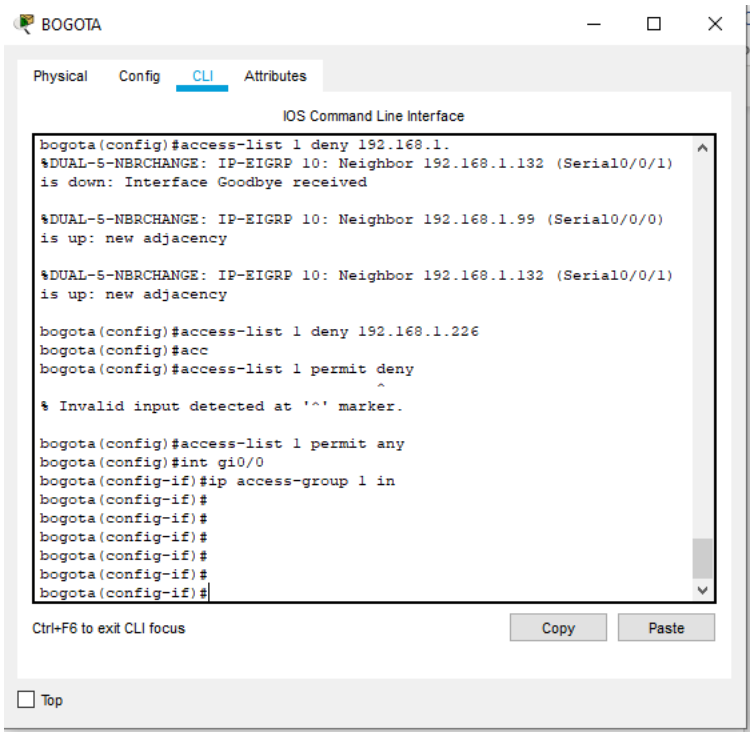
Conexión de Cali por medio de telnet a Bogotá:

Ilustración 41 Conexión TELNET



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

Ilustración 42 Bogotá



Utilizamos los siguientes comandos

Bogotá(config)#access-list 1 deny 192.168.1.226
Bogotá(config)#acc
Bogotá(config)#access-list 1 permit any
Bogotá(config)#int gi0/0
Bogotá(config-if)#ip access-group 1 in
Bogotá(config-if)#

verificamos haciendo ping

Ilustración 43 PING

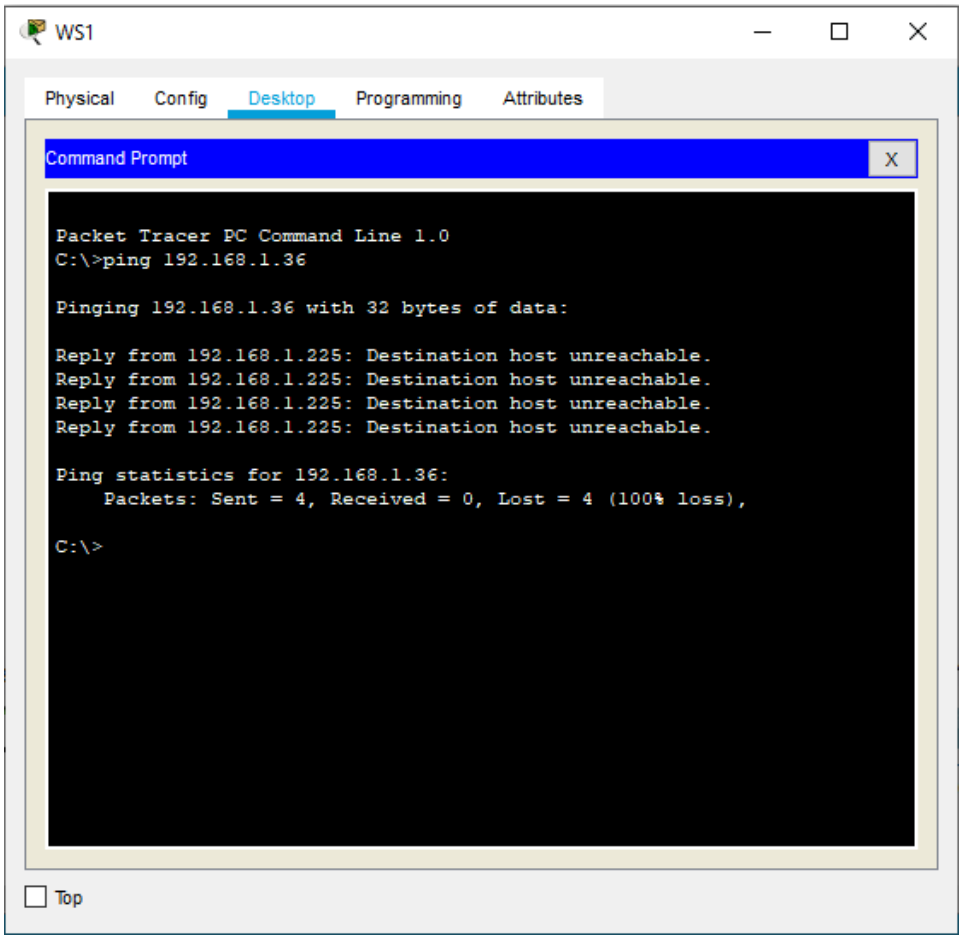
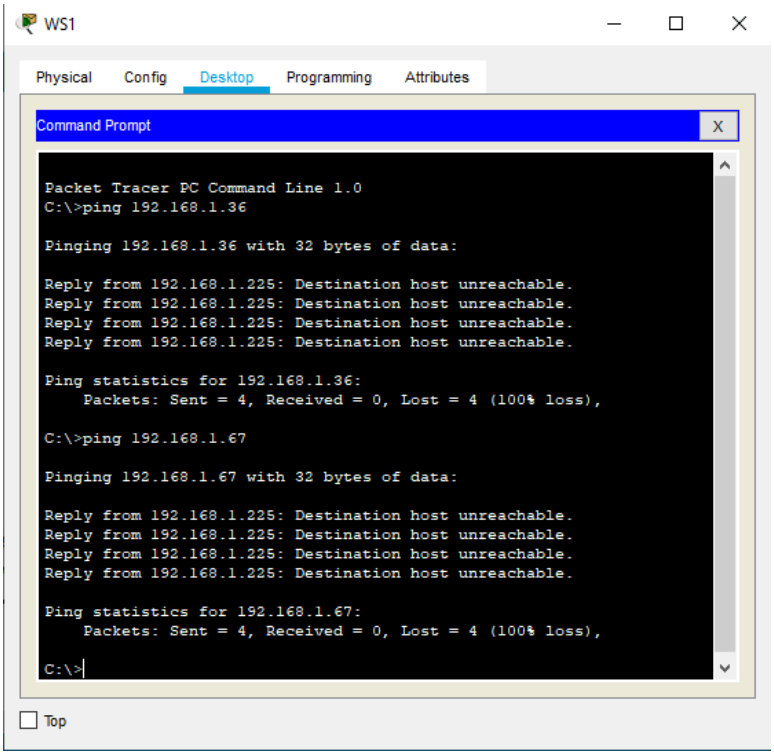


Ilustración 44 PING



Podemos verificar que el servidor si tiene conexión con toda la red.

Ilustración 45 Conexión del servidor con la red

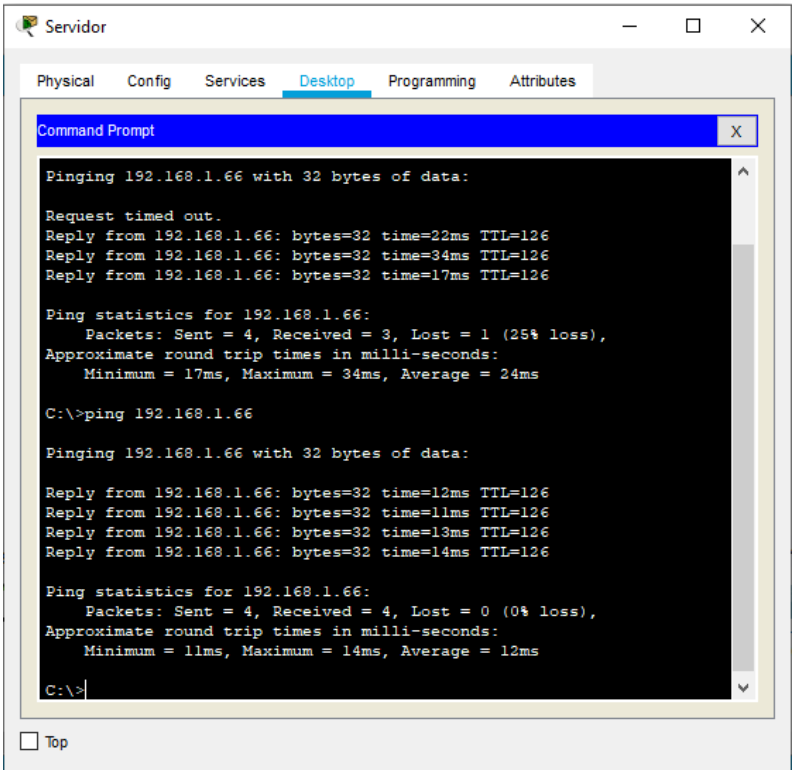
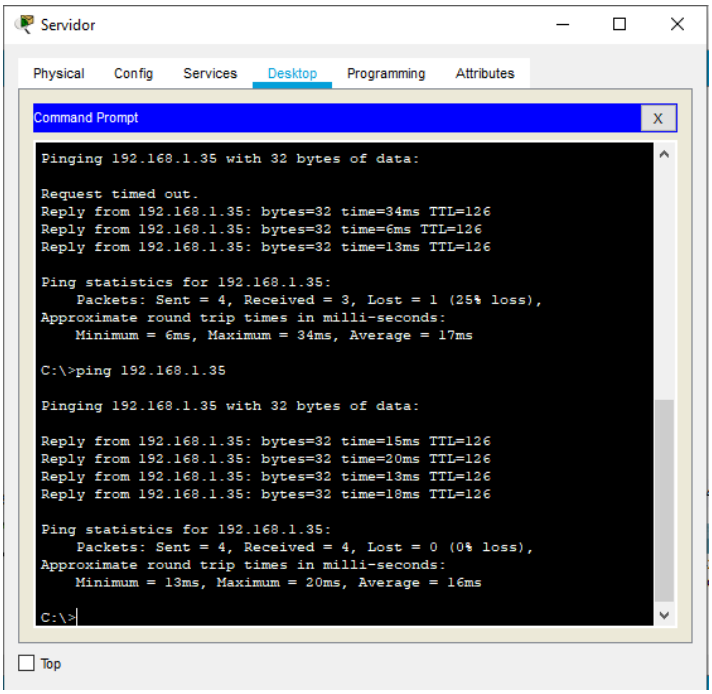
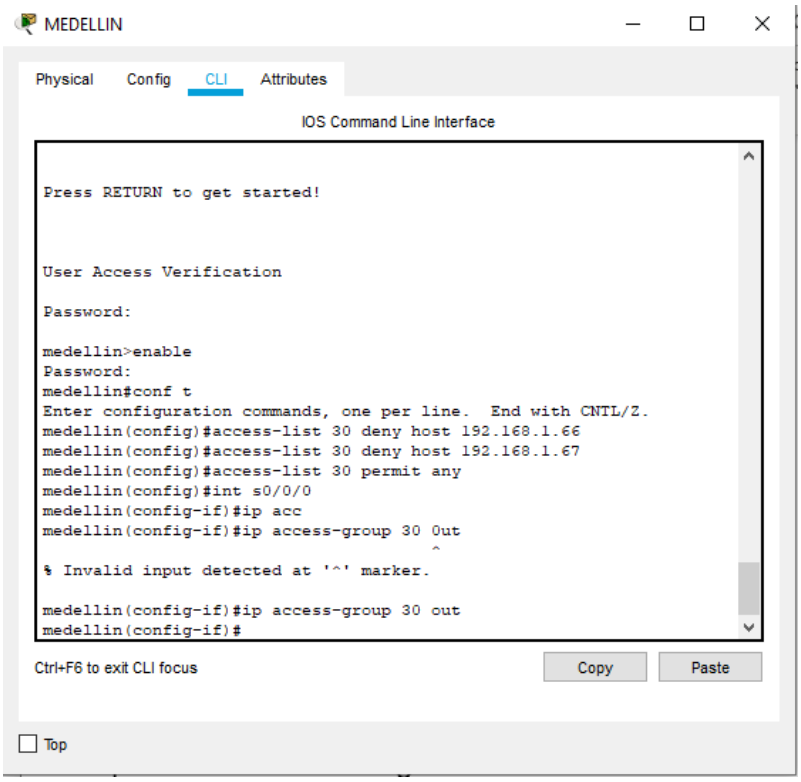


Ilustración 46 Conexión con la red



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

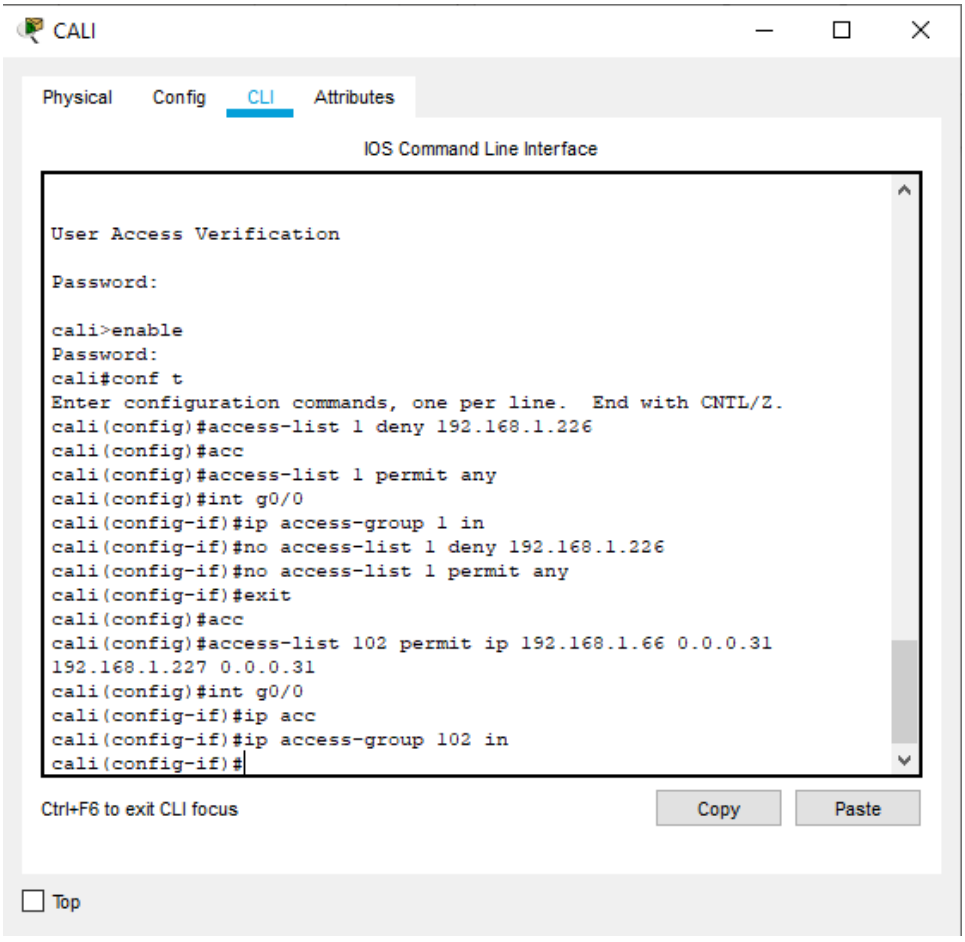
Ilustración 47 Medellín



Los comandos para utilizar son los siguientes:

medellin>enable
Password:
medellin#conf t
Enter configuration commands, one per line. End with CNTL/Z.
medellin(config)#access-list 30 deny host 192.168.1.66
medellin(config)#access-list 30 deny host 192.168.1.67
medellin(config)#access-list 30 permit any
medellin(config)#int s0/0/0
medellin(config-if)#ip acc
medellin(config-if)#ip access-group 30 out
medellin(config-if)#

Ilustración 48 Cali



Los comandos para utilizar son los siguientes:

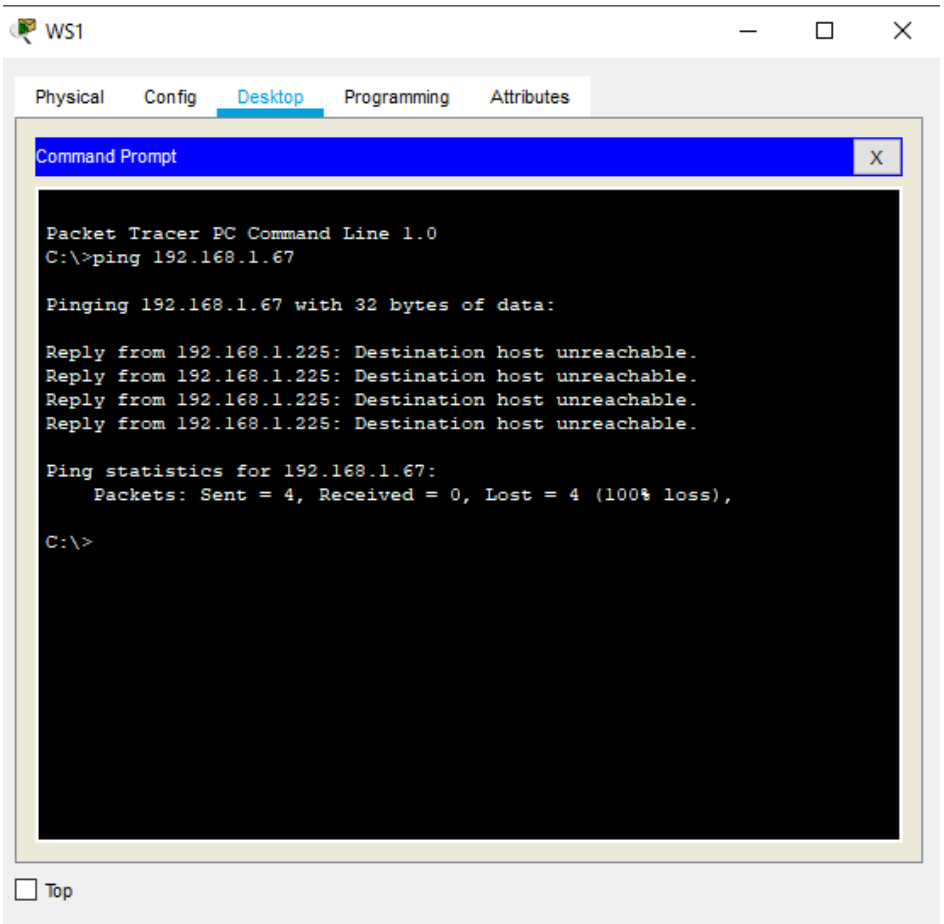
Cali>enable
Password:
cali#conf t
Enter configuration commands, one per line. End with CNTL/Z.

Cali(config)#access-list 1 deny 192.168.1.226
Cali(config)#acc
Cali(config)#access-list 1 permit any
Cali(config)#int g0/0
Cali(config-if)#ip access-group 1 in
Cali(config-if)#no access-list 1 deny 192.168.1.226
Cali(config-if)#no access-list 1 permit any
Cali(config-if)#exit
Cali(config)#acc
Cali(config)#access-list 102 permit ip 192.168.1.66 0.0.0.31 192.168.1.227 0.0.0.31
Cali(config)#int g0/0
Cali(config-if)#ip acc
Cali(config-if)#ip access-group 102 in
Cali(config-if)#

luego de esto hacemos ping entre Pcs para comprobar conectividad.

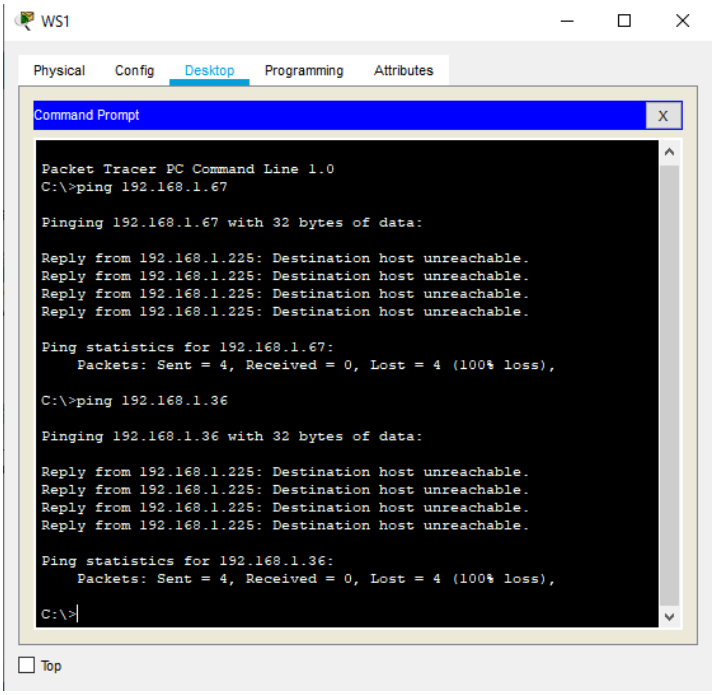
Ping de SW1 al PC-D perteneciente a la red de Cali 192.168.1.67.

Ilustración 49 Ping de SW1 al PC-D



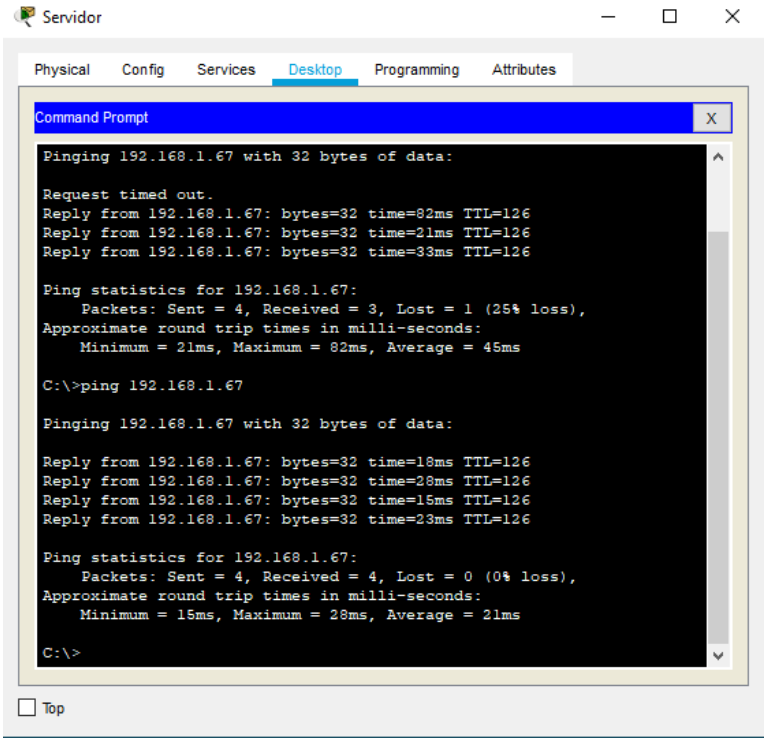
Ping de SW1 al PC-B perteneciente a la red de Cali 192.168.1.36.

Ilustración 50 Ping de SW1 al PC-B



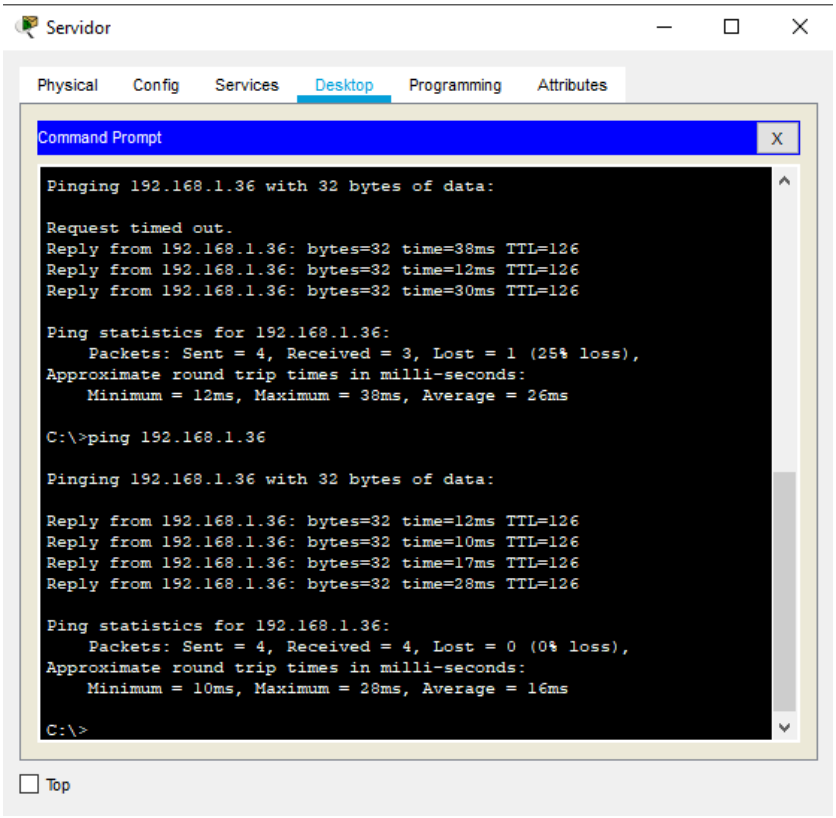
Ping de Servidor al PC-D 192.168.1.67 perteneciente a la red de Cali.

Ilustración 51 Ping de Servidor al PC-D



Ping de Servidor al PC-B 192.168.1.36 perteneciente a la red de Medellín.

Ilustración 52 Ping de Servidor al PC-B



Con esto logramos analizar que se hicieron los procesos de manera correcta y damos por terminado el primer escenario solicitado en esta prueba final de habilidades.

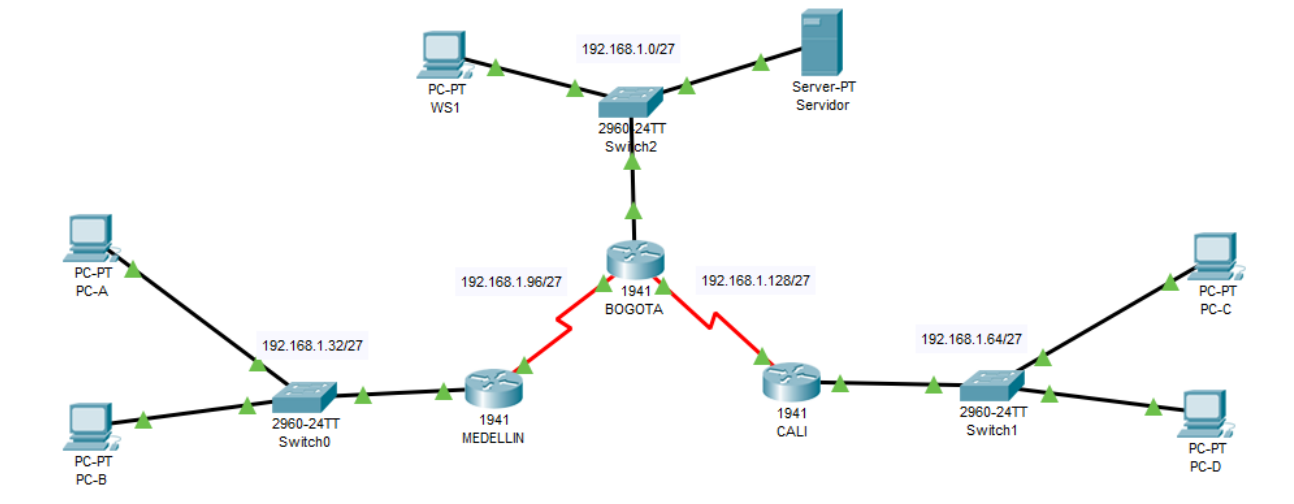
Parte 5: Comprobación de la red instalada.

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

	ORIGEN	DESTINO	RESULTADO
TELNET	**Router MEDELLIN**	**Router CALI**	Conexión exitosa
	WS_1	**Router BOGOTA**	Sin conexión
	Servidor	**Router CALI**	Conexión exitosa
	Servidor	**Router MEDELLIN**	Conexión exitosa

TELNET	LAN del Router MEDELLIN	Router CALI	Sin Conexión
	LAN del Router CALI	Router CALI	Sin Conexión
	LAN del Router MEDELLIN	Router MEDELLIN	Sin Conexión
	LAN del Router CALI	Router MEDELLIN	Sin Conexión
PING	LAN del Router CALI	WS_1	Falla Ping
	LAN del Router MEDELLIN	WS_1	Falla Ping
	LAN del Router MEDELLIN	LAN del Router CALI	Falla Ping
PING	LAN del Router CALI	Servidor	Ping exitoso
	LAN del Router MEDELLIN	Servidor	Ping exitoso
	Servidor	LAN del Router MEDELLIN	Ping exitoso
	Servidor	LAN del Router CALI	Ping exitoso
	Router CALI	LAN del Router MEDELLIN	Falla Ping
	Router MEDELLIN	LAN del Router CALI	Falla Ping

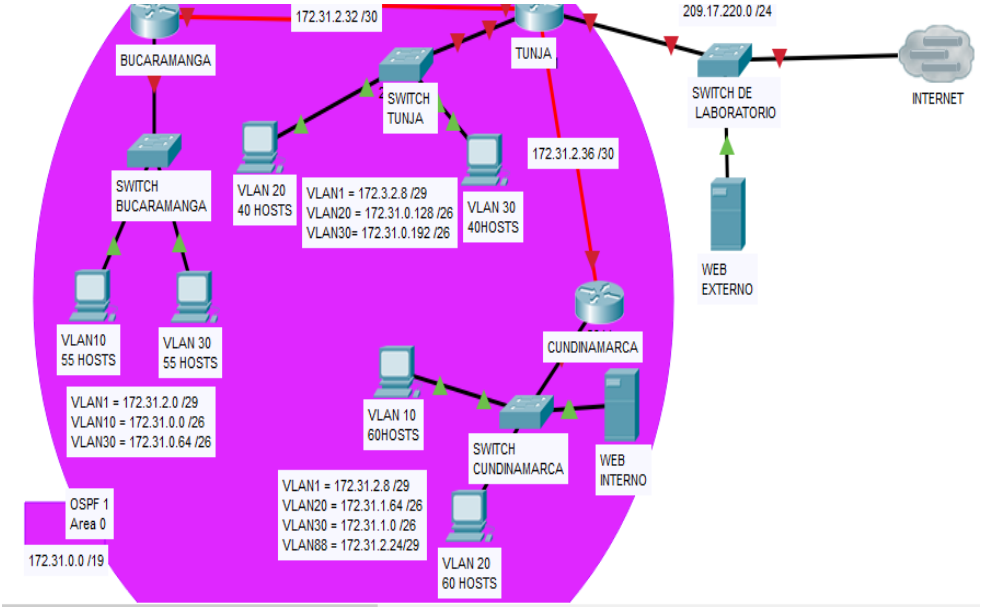
Ilustración 53 Topología conectada totalmente



Escenario 2

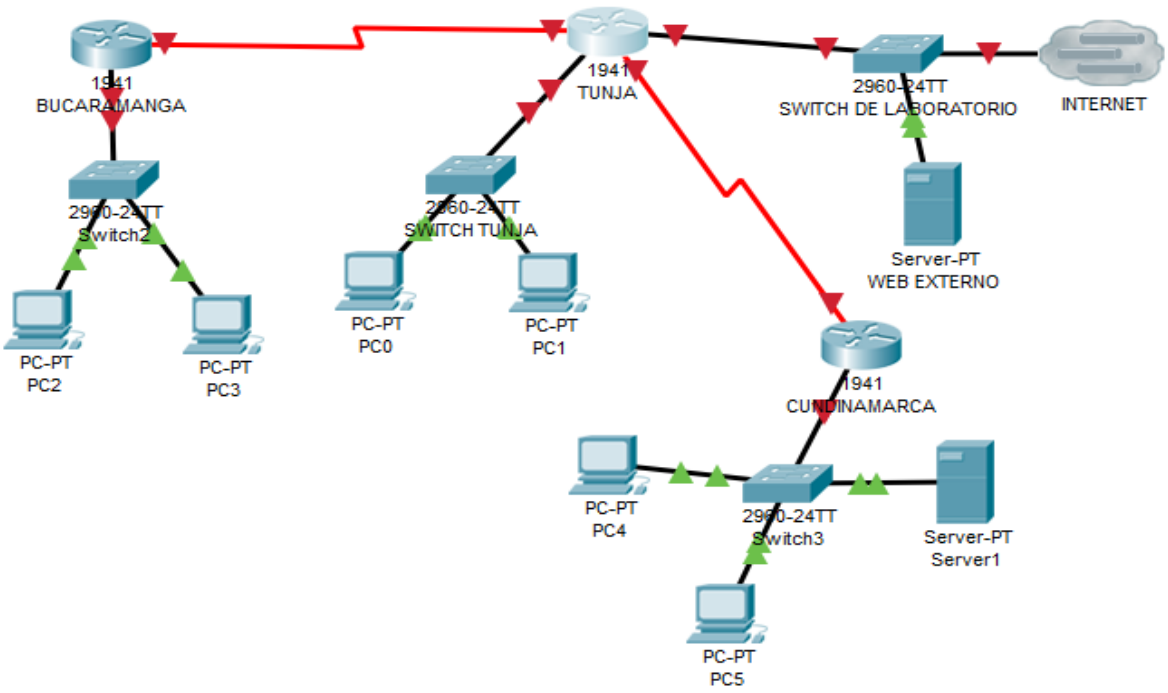
Una empresa tiene la conexión a internet en una red Ethernet, lo cual deben adaptarlo para facilitar que sus routers y las redes que incluyen puedan, por esa vía, conectarse a internet, pero empleando las direcciones de la red LAN original.

Ilustración 54 Escenario 2



Tenemos la topologia como se solicita en la red: Topologia

Ilustración 55 Topología Escenario 2



Desarrollo

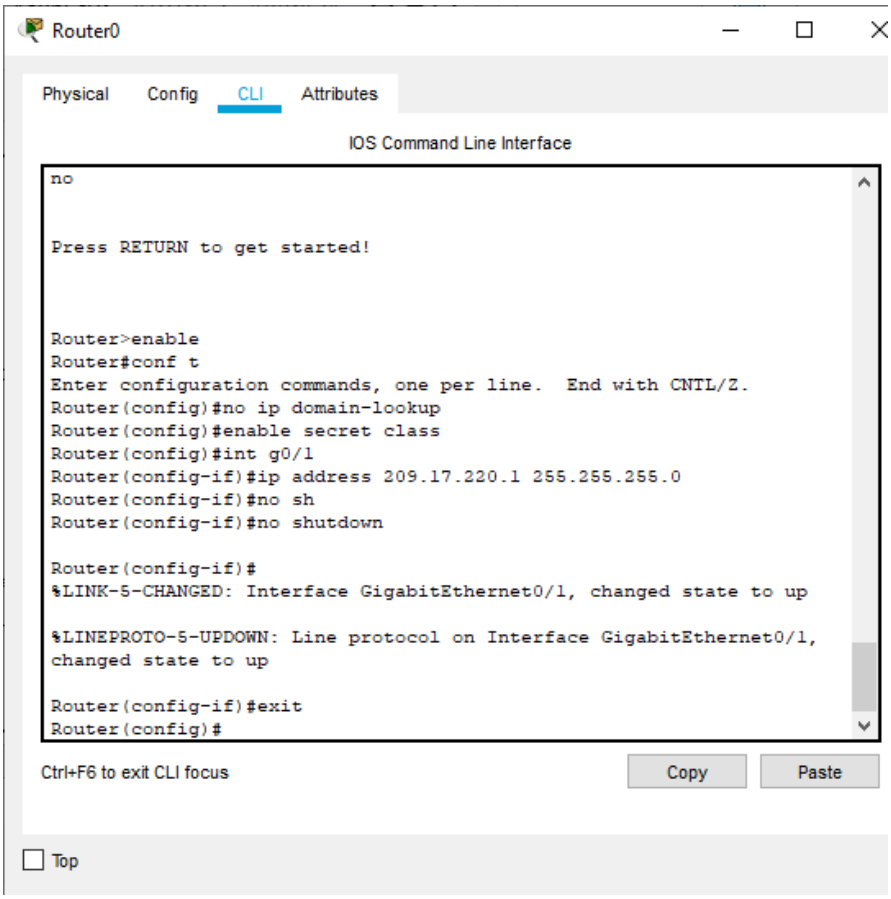
Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:

    - Configuración básica.

Le hacemos la configuración a cada uno de los router como se muestra a continuación

Ilustración 56 Tunja



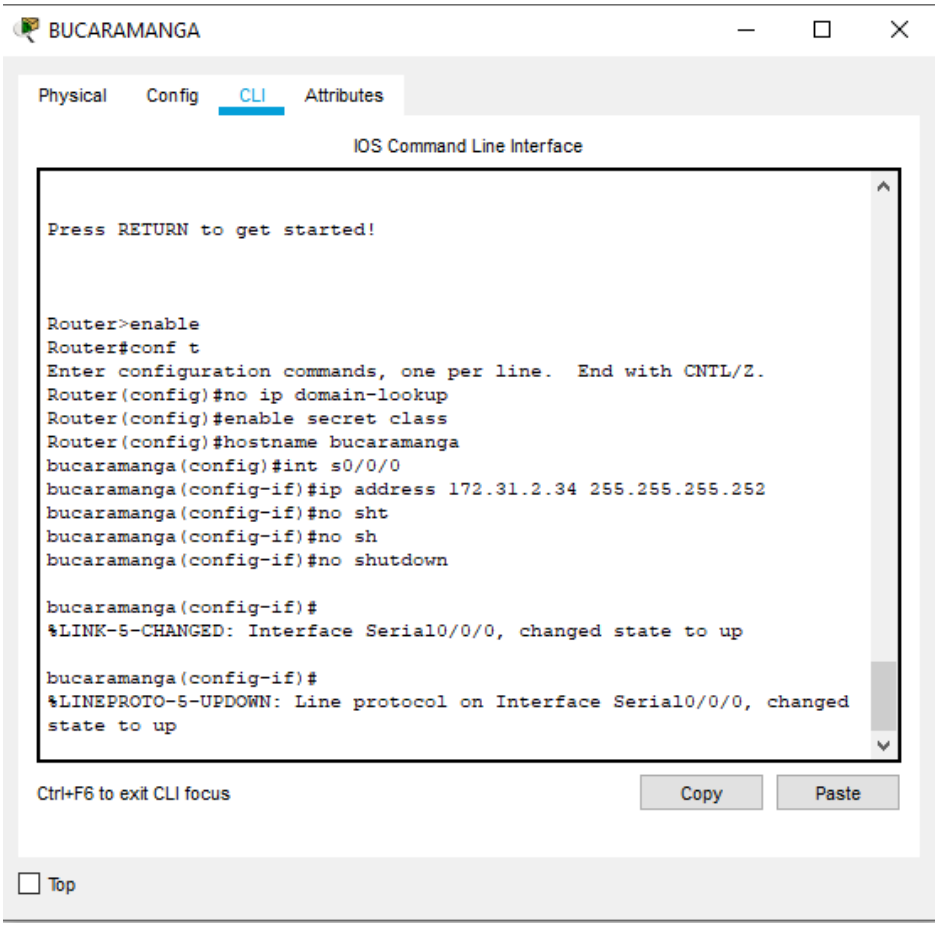
Los comandos que se van a ejecutar son los siguientes:

Router>enable
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#enable secret class
Router(config)#int g0/1
Router(config-if)#ip address 209.17.220.1 255.255.255.0
Router(config-if)#no sh
Router(config-if)#no shutdown

Nos quedó pendiente la configuración del hostname, pero más Adelante se hace como corresponde.

Pasamos a configurar:

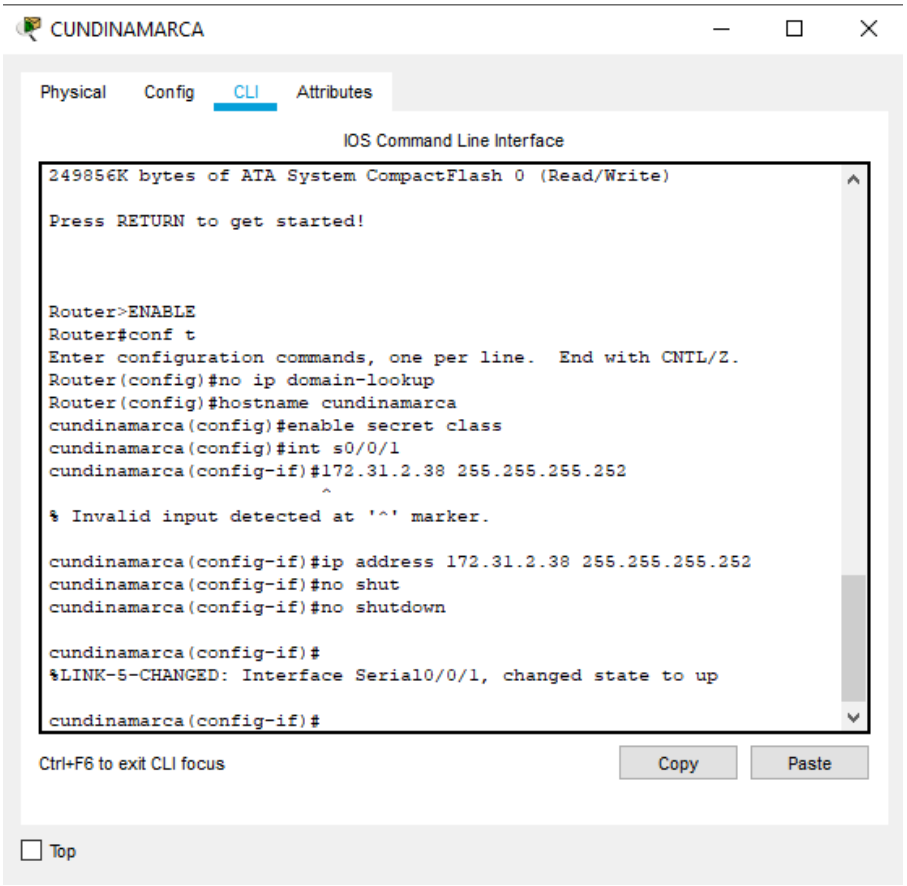
Ilustración 57 Bucaramanga



Los comandos que se van a utilizar son los siguientes:

Router>enable
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#enable secret class
Router(config)#hostname Bucaramanga
Bucaramanga(config)#int s0/0/0
Bucaramanga(config-if)#ip address 172.31.2.34 255.255.255.252
Bucaramanga(config-if)#no sh
Bucaramanga(config-if)#no shutdown

Ilustración 58 Cundinamarca



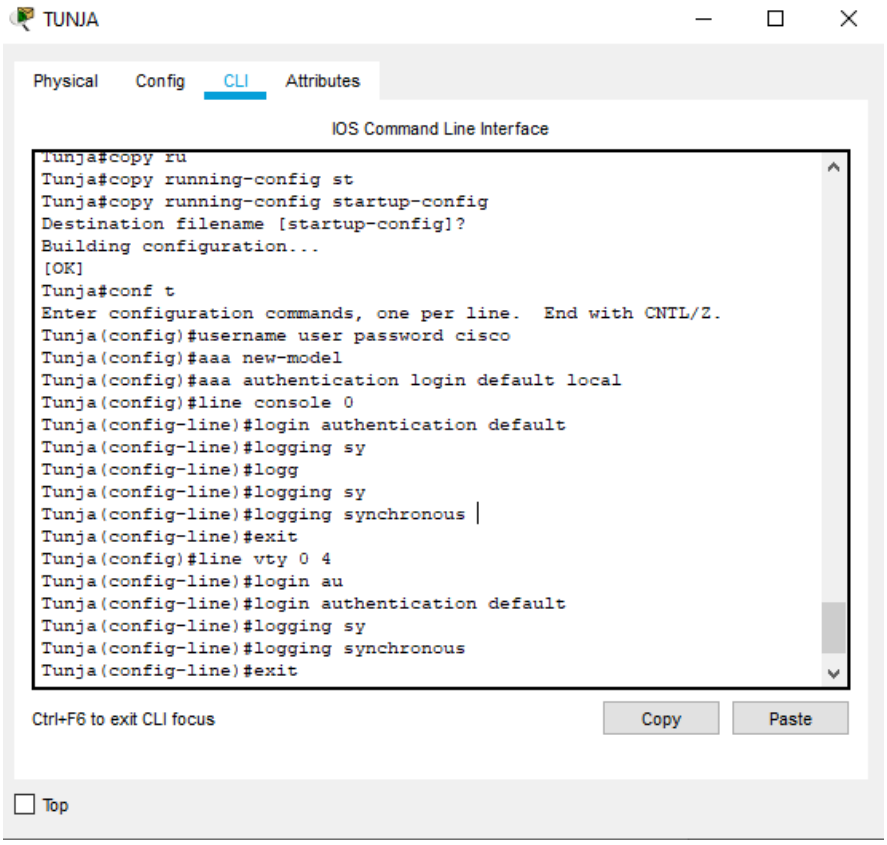
Los comandos que se van a utilizar son los siguientes:

Router>enable
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname Cundinamarca
Cundinamarca(config)#enable secret class
Cundinamarca(config)#int s0/0/1
Cundinamarca(config-if)#ip address 172.31.2.38 255.255.255.252
Cundinamarca(config-if)#no shut
Cundinamarca(config-if)#no shutdown

- Autenticación local con AAA.

Se va a validar el siguiente proceso de la siguiente manera:

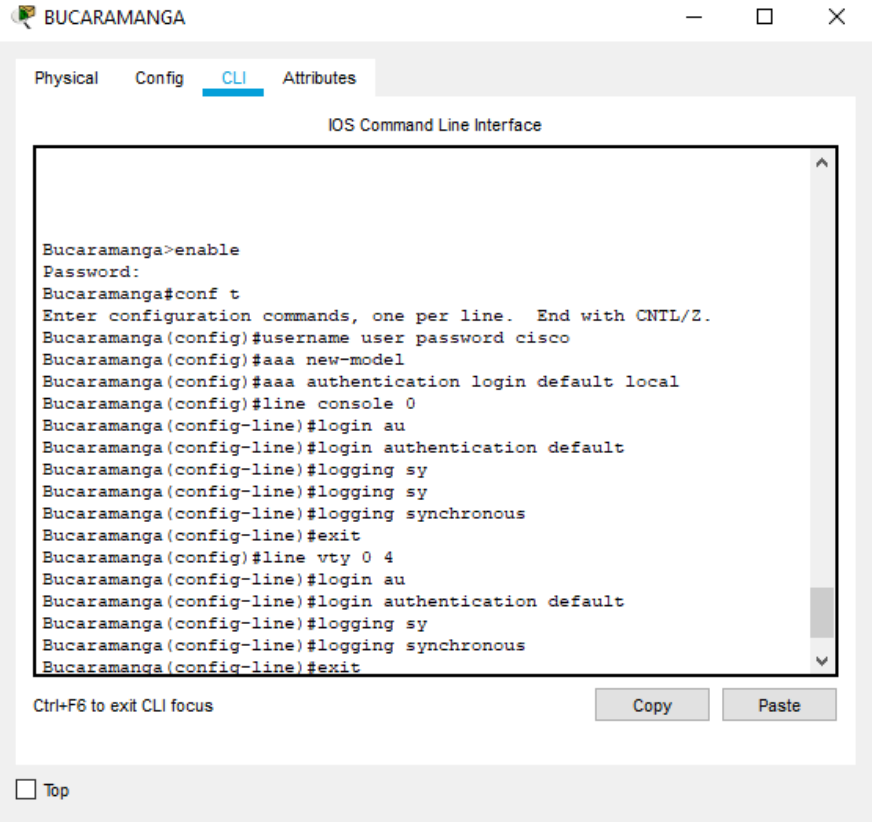
Ilustración 59 Tunja- Autenticación AAA



Los comandos que se van a utilizar son los siguientes:

Tunja# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#username user password cisco
Tunja(config)#aaa new-model
Tunja(config)#aaa authentication login default local
Tunja(config)#line console 0
Tunja(config-line)#login authentication default
Tunja(config-line)#logging sy
Tunja(config-line)#logging synchronous
Tunja(config-line)#exit
Tunja(config)#line vty 0 4
Tunja(config-line)#login authentication default
Tunja(config-line)#logging synchronous
Tunja(config-line)#exit
Tunja(config)#service password-encryption
Tunja(config)#

Ilustración 60 Bucaramanga- Autenticación AAA

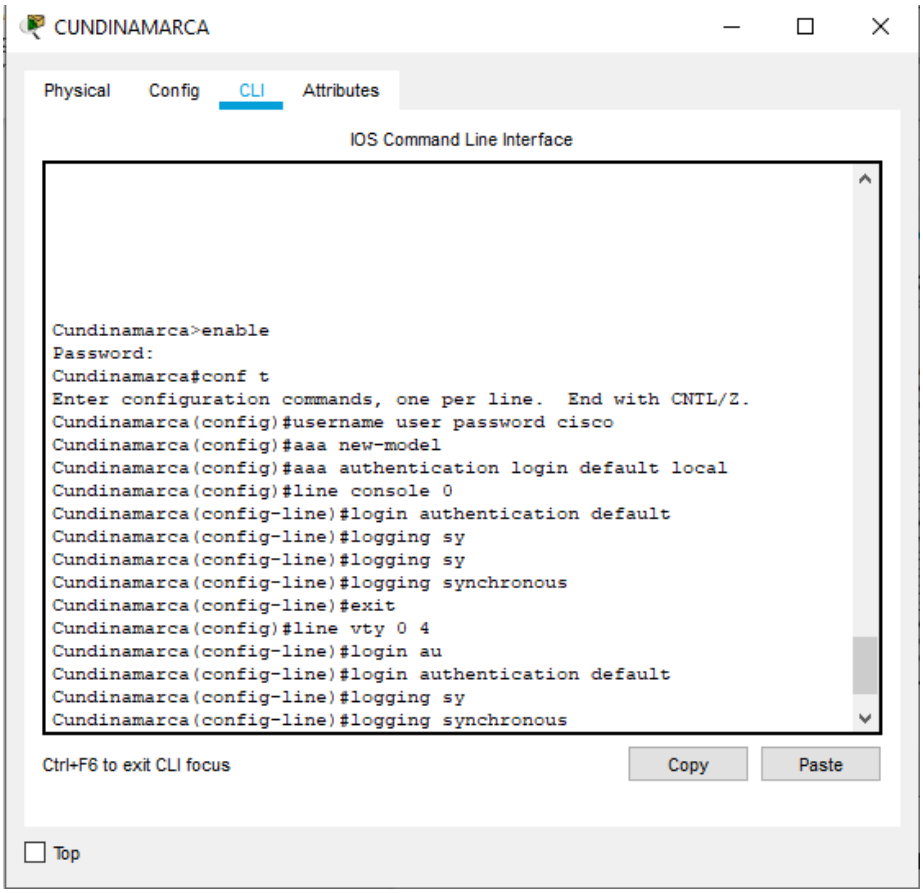


Los comandos a utilizar serán los siguientes:

Bucaramanga>enable
Password:
Bucaramanga# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bucaramanga(config)#username user password cisco
Bucaramanga(config)#aaa new-model
Bucaramanga(config)#aaa authentication login default local
Bucaramanga(config)#line console 0
Bucaramanga(config-line)#login au
Bucaramanga(config-line)#login authentication default
Bucaramanga(config-line)#logging sy
Bucaramanga(config-line)#logging sy
Bucaramanga(config-line)#logging synchronous
Bucaramanga(config-line)#exit
Bucaramanga(config)#line vty 0 4
Bucaramanga(config-line)#login au
Bucaramanga(config-line)#login authentication default
Bucaramanga(config-line)#logging sy
Bucaramanga(config-line)#logging synchronous
Bucaramanga(config-line)#exit
Bucaramanga(config)#service en

Bucaramanga(config)#service pass
Bucaramanga(config)#service password-encryption
Bucaramanga(config)#

Ilustración 61 Cundinamarca- Autenticación AAA



Los comandos para utilizar serán los siguientes:

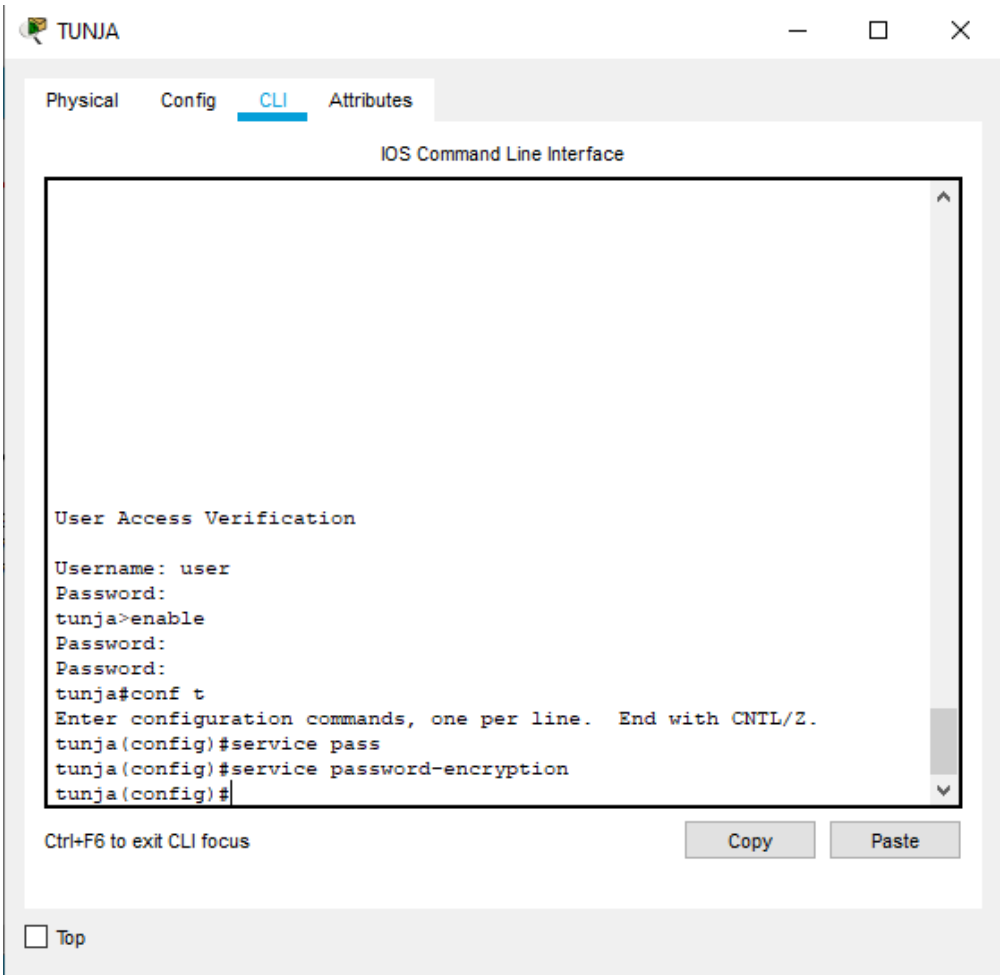
Cundinamarca>enable
Password:
Cundinamarca # conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cundinamarca(config)#username user password cisco
Cundinamarca(config)#aaa new-model
Cundinamarca(config)#aaa authentication login default local
Cundinamarca(config)#line console 0
Cundinamarca(config-line)#login authentication default
Cundinamarca(config-line)#logging synchronous
Cundinamarca(config-line)#exit
Cundinamarca(config)#line vty 0 4
Cundinamarca(config-line)#login authentication default
Cundinamarca(config-line)#logging synchronous
Cundinamarca(config-line)#exit

Cundinamarca(config)#service password-encryption
Cundinamarca(config)#

- Cifrado de contraseñas.

Ahora vamos a aplicar el cifrado de contraseñas de la siguiente manera

Ilustración 62 Tunja- Cifrado de contraseña

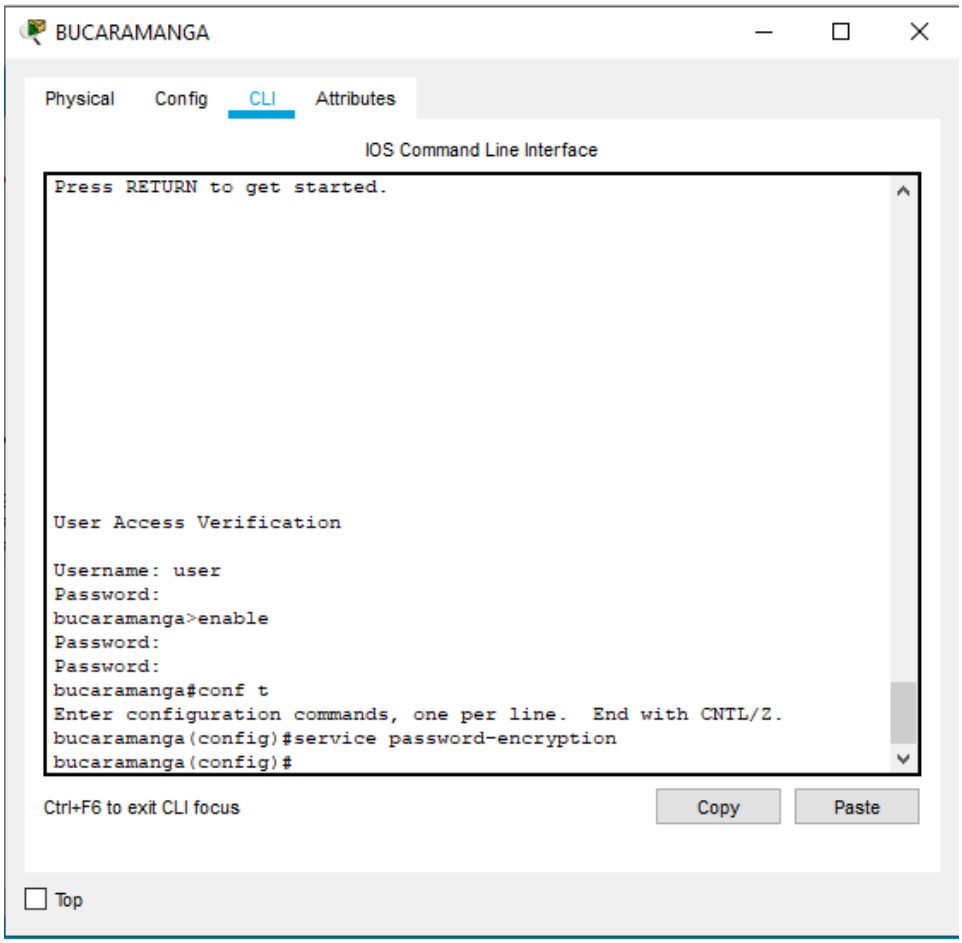


Los comandos para utilizar serán los siguientes:

Username: user
Password:
Tunja>enable
Password:
Password:
Tunja# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#service pass

Tunja(config)#service password-encryption
Tunja(config)#

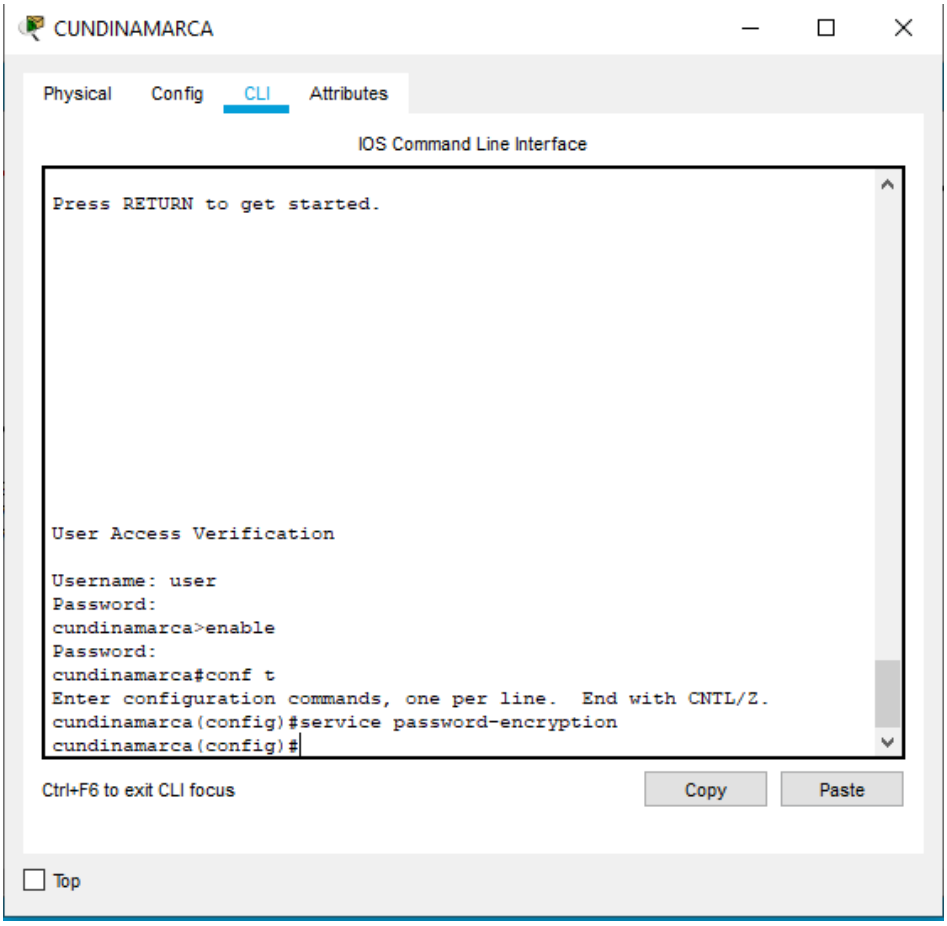
Ilustración 63 Bucaramanga-- Cifrado de contraseña



Los comandos que Vamos a utilizar serán los siguientes:

Username: user
Password:
Bucaramanga>enable
Password:
Password:
Bucaramanga# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bucaramanga(config)#service password-encryption
Bucaramanga(config)#

Ilustración 64 Cundinamarca-- Cifrado de contraseña



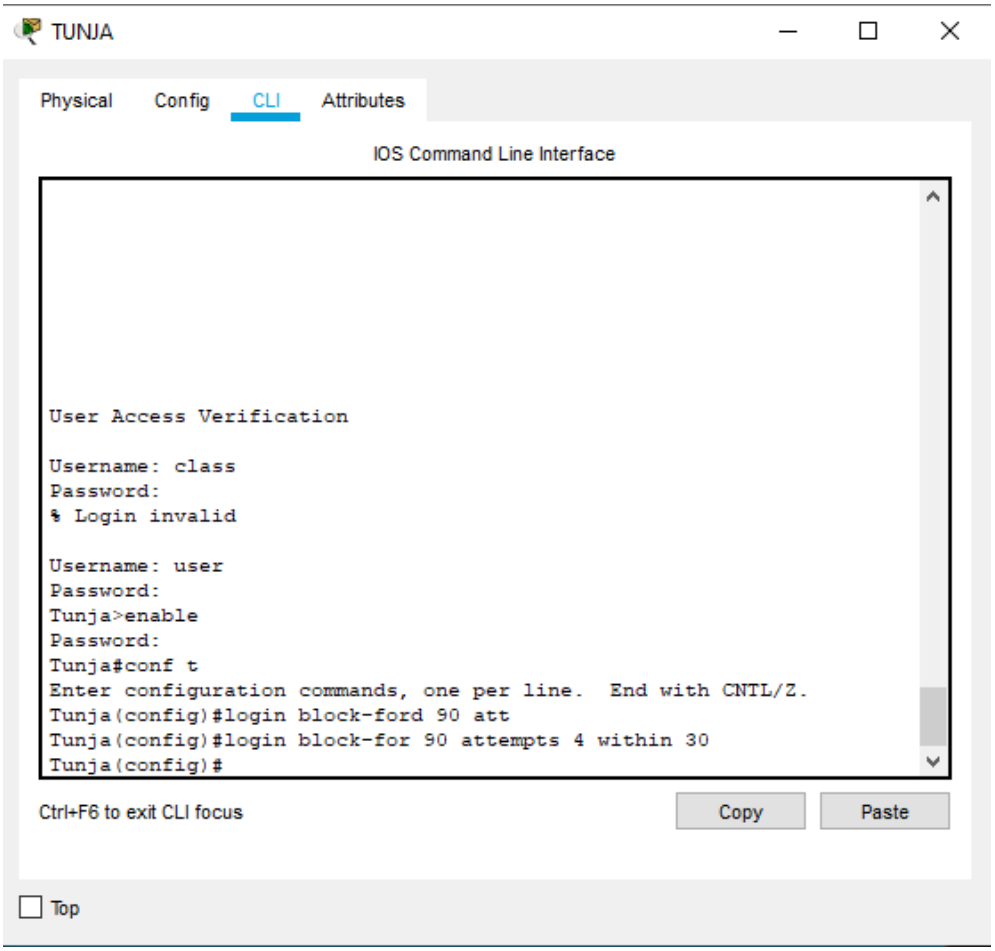
Los comandos que vamos a utilizar serán los siguientes:

Username: user
Password:
Cundinamarca>enable
Password:
Cundinamarca# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cundinamarca(config)#service password-encryption
Cundinamarca(config)#

- Un máximo de internos para acceder al router.

  Para este punto de la actividad vamos a utilizar login block-for 90 attempts 4 within 30 como comando.

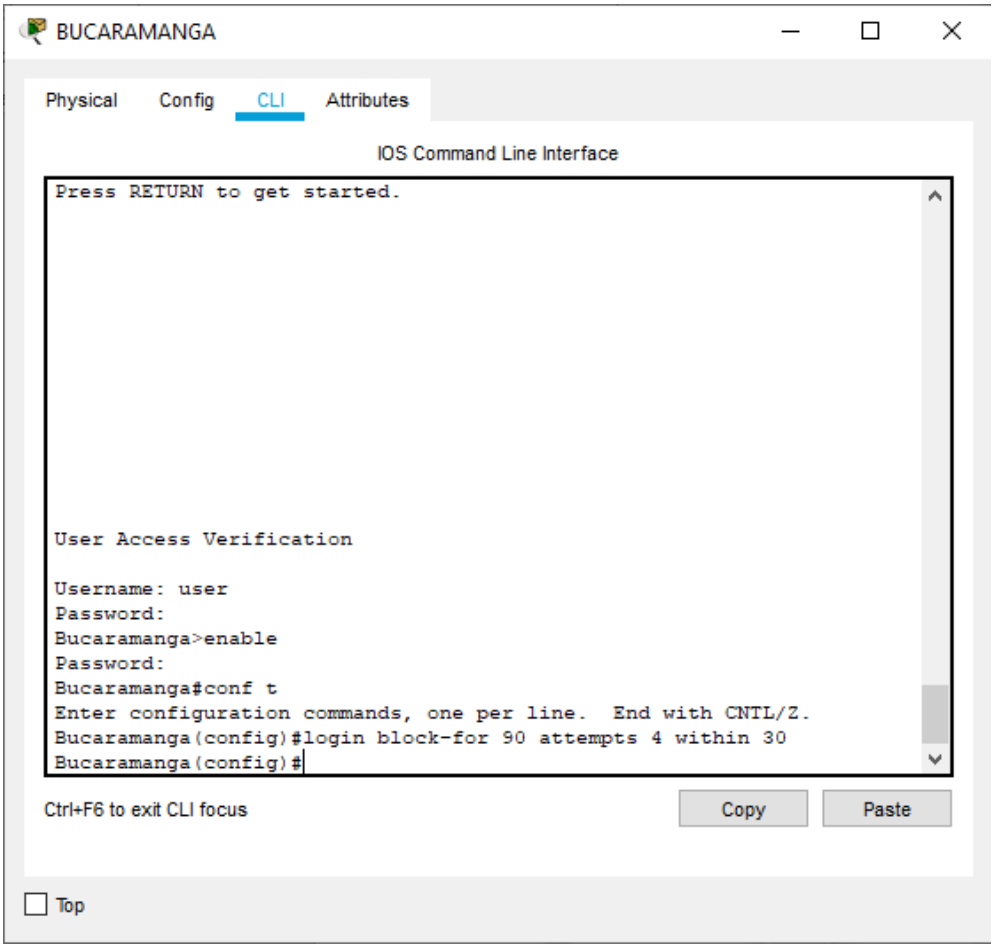
Ilustración 65 Tunja- Máximo de intentos



Los códigos para utilizar serán los siguientes:

Tunja# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#login block-ford 90 att
Tunja(config)#login block-for 90 attempts 4 within 30
Tunja(config)#

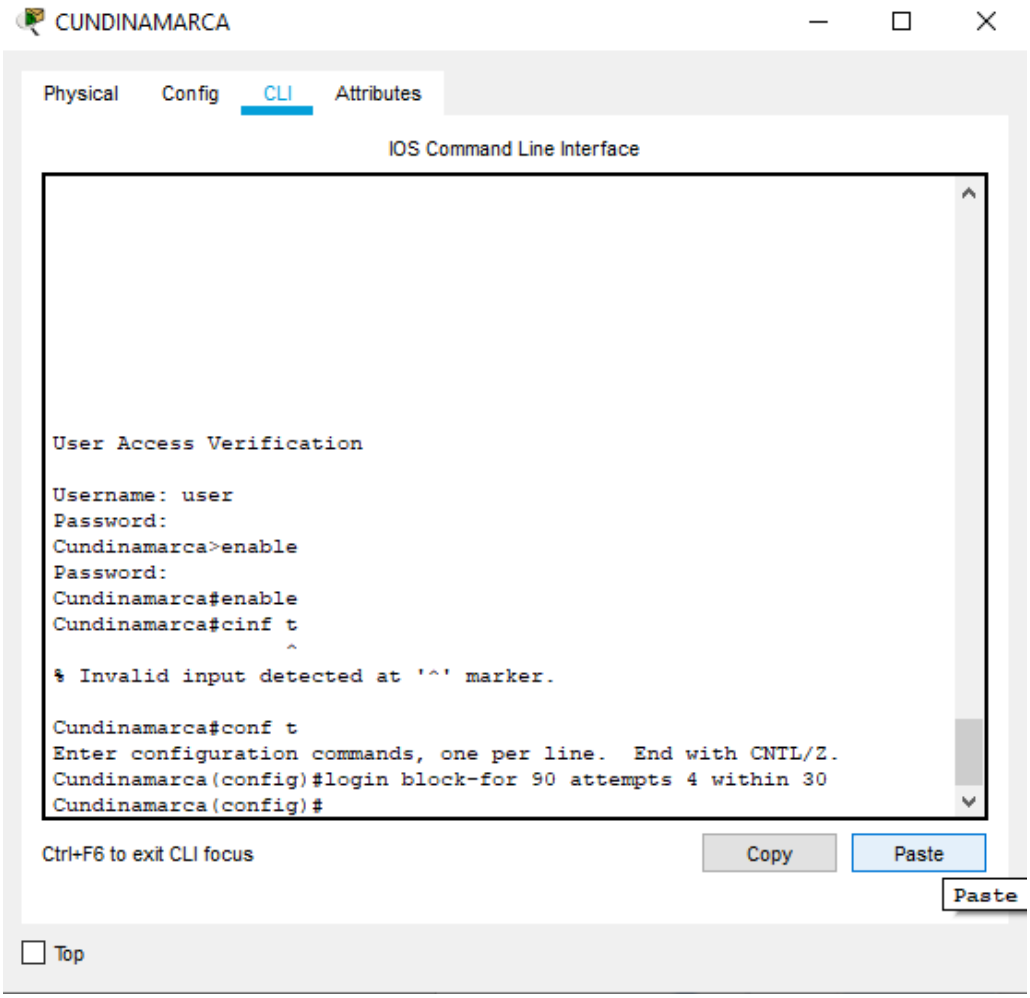
Ilustración 66 Bucaramanga-- Máximo de intentos



Los comandos para ejecutar serán los siguientes

Bucaramanga# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bucaramanga(config)#login block-for 90 attempts 4 within 30
Bucaramanga(config)#

Ilustración 67 Cundinamarca- Máximo de intentos

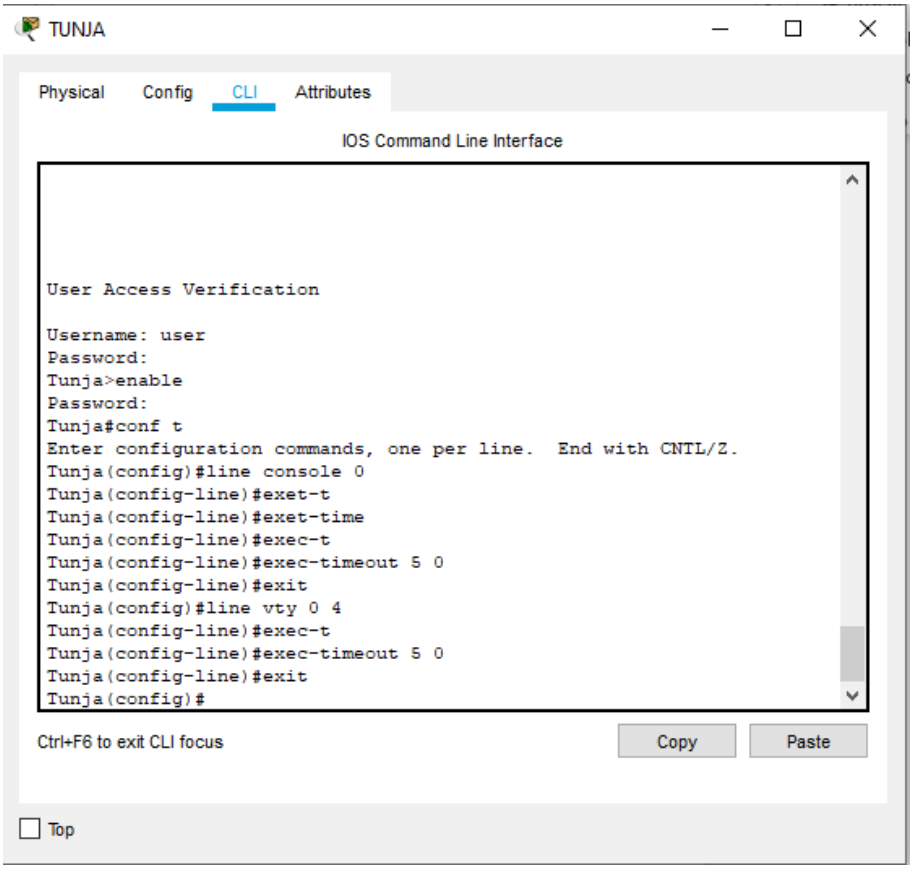


Los comandos para utilizar serán los siguientes

Cundinamarca# enable
Cundinamarca# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cundinamarca(config)#login block-for 90 attempts 4 within 30
Cundinamarca(config)#

- Máximo tiempo de acceso al detectar ataques.

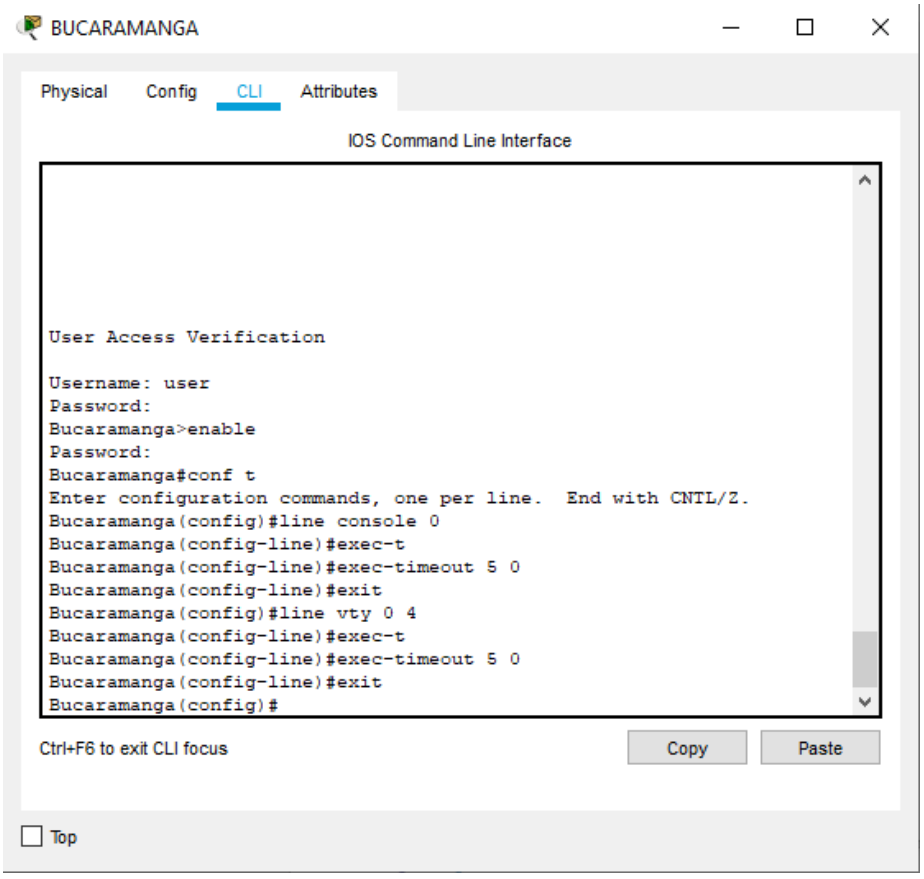
Ilustración 68 Tunja- Máximo tiempo de acceso al detectar ataques



Para esta parte se va a utilizar el siguiente comando:

Tunja# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#line console 0
Tunja(config-line)#exec-timeout 5 0
Tunja(config-line)#exit
Tunja(config)#line vty 0 4
Tunja(config-line)#exec-t
Tunja(config-line)#exec-timeout 5 0
Tunja(config-line)#exit
Tunja(config)#

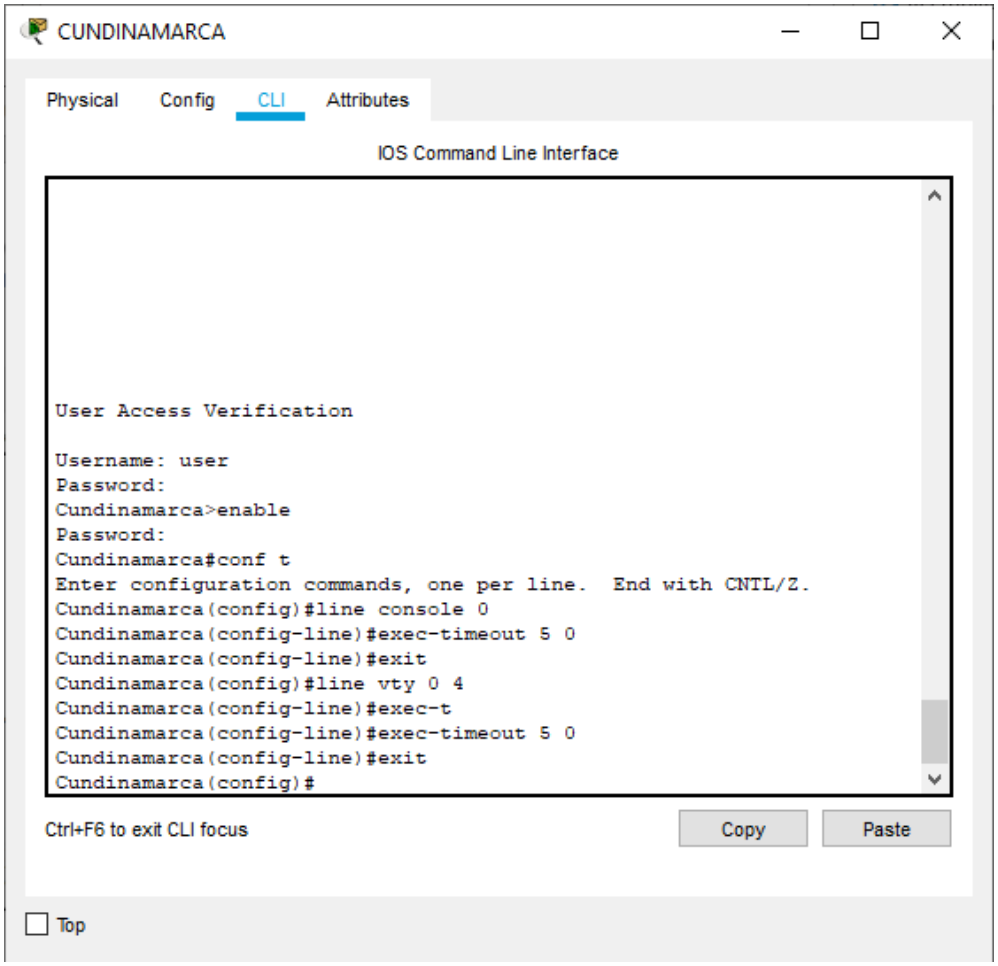
Ilustración 69 Bucaramanga-- Máximo tiempo de acceso al detectar ataques



Para esta parte se va a utilizar el siguiente comando:

Bucaramanga# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bucaramanga(config)#line console 0
Bucaramanga(config-line)#exec-t
Bucaramanga(config-line)#exec-timeout 5 0
Bucaramanga(config-line)#exit
Bucaramanga(config)#line vty 0 4
Bucaramanga(config-line)#exec-t
Bucaramanga(config-line)#exec-timeout 5 0
Bucaramanga(config-line)#exit
Bucaramanga(config)#

Ilustración 70 Cundinamarca- Máximo tiempo de acceso al detectar ataques



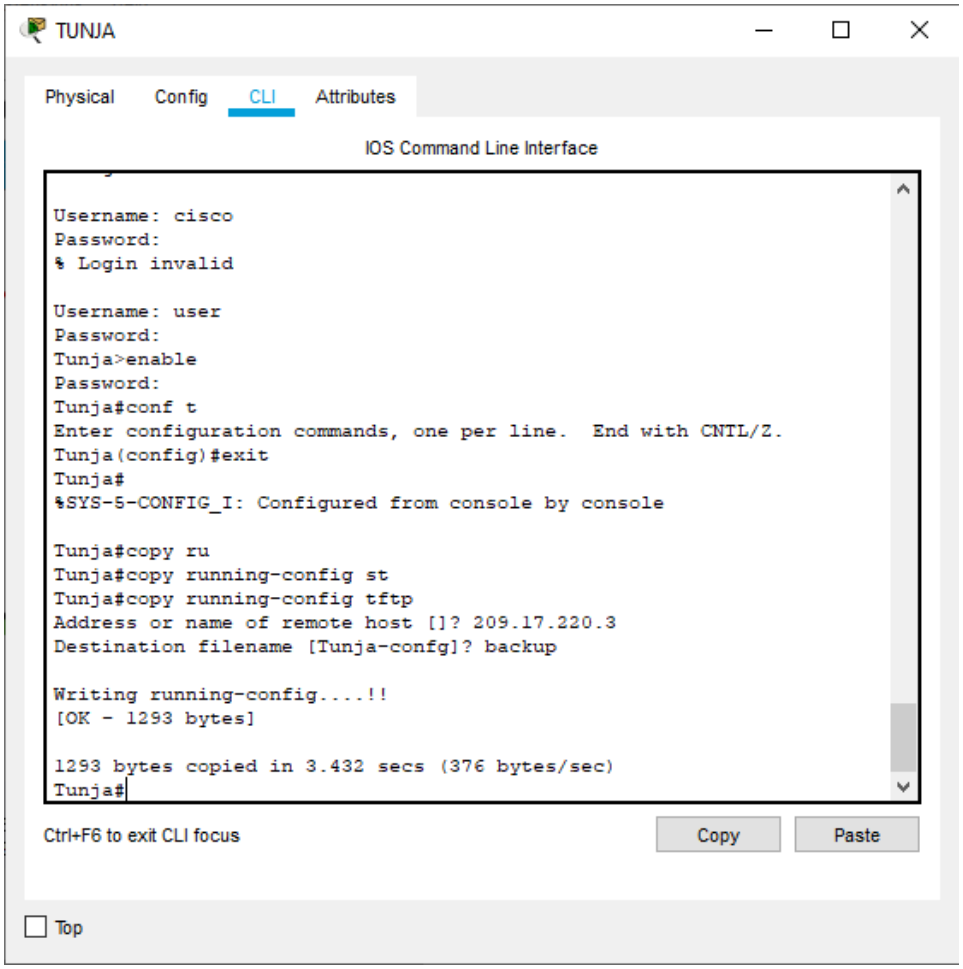
Para esta parte se va a utilizar el siguiente comando:

Cundinamarca# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cundinamarca(config)#line console 0
Cundinamarca(config-line)#exec-timeout 5 0
Cundinamarca(config-line)#exit
Cundinamarca(config)#line vty 0 4
Cundinamarca(config-line)#exec-t
Cundinamarca(config-line)#exec-timeout 5 0
Cundinamarca(config-line)#exit
Cundinamarca(config)#

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

Almacenamiento de la configuración del servidor tftp en el router, se aplica de la siguiente manera:

Ilustración 71 Tunja- servidor TFTP



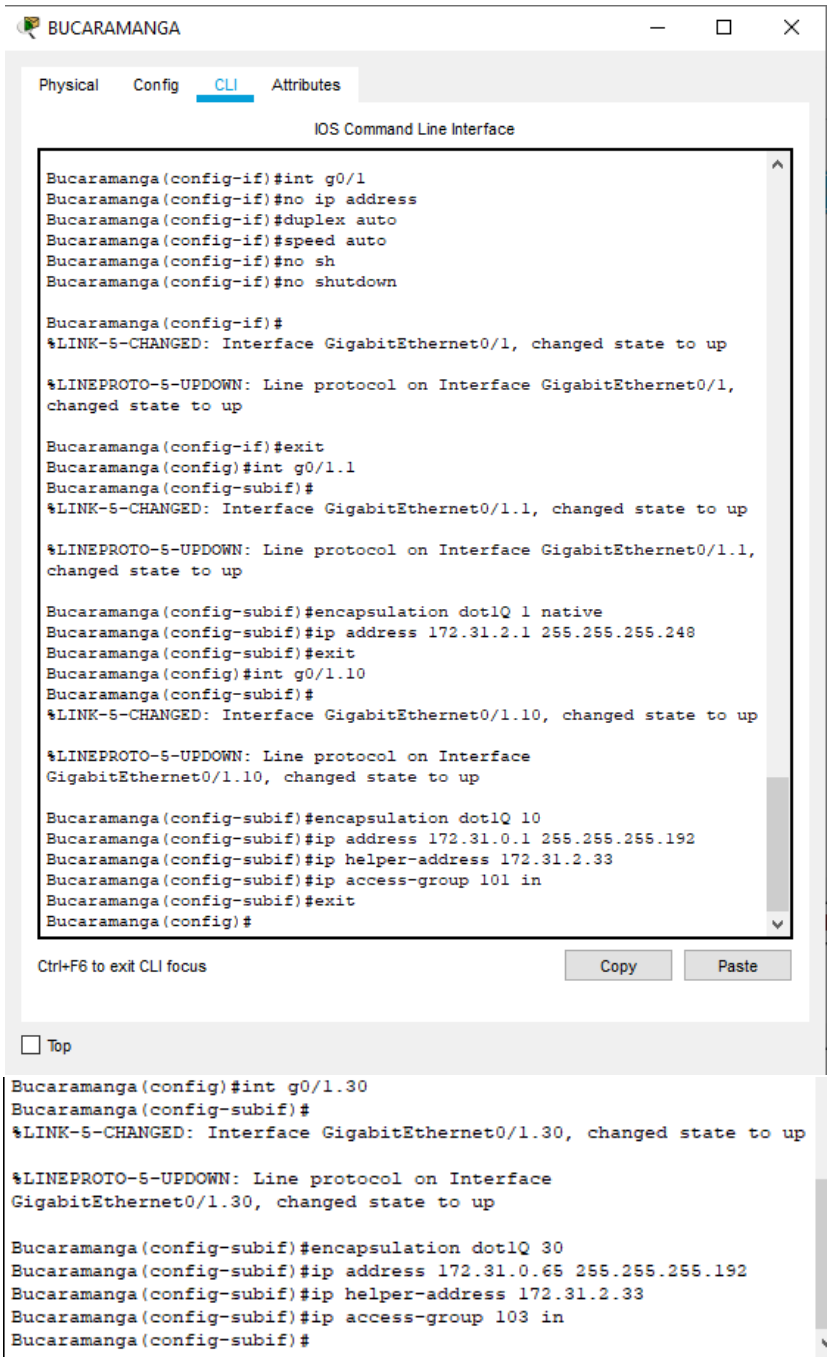
Los comandos para utilizar son los siguientes:

Tunja# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#exit
Tunja#
%SYS-5-CONFIG_I: Configured from console by console
Tunja# copy ru
Tunja# copy running-config tftp
Address or name of remote host []? 209.17.220.3
Destination filename [Tunja-confg]? backup
Writing running-config....!!
[OK - 1293 bytes]
1293 bytes copied in 3.432 secs (376 bytes/sec)

Tunja#

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

Ilustración 72 Bucaramanga- se le asigna DHCP



Los comandos para utilizar serán los siguientes:

Bucaramanga# conf t
Enter configuration commands, one per line. End with CNTL/Z.

Bucaramanga(config)#int g0/0
Bucaramanga(config-if)#no ip address
Bucaramanga(config-if)#duplex auto
Bucaramanga(config-if)#speed auto
Bucaramanga(config-if)#no sh
Bucaramanga(config-if)#no shutdown
Bucaramanga(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
Bucaramanga(config-if)#shu
Bucaramanga(config-if)#shutdown
Bucaramanga(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down
Bucaramanga(config-if)#int g0/1
Bucaramanga(config-if)#no ip address
Bucaramanga(config-if)#duplex auto
Bucaramanga(config-if)#speed auto
Bucaramanga(config-if)#no sh
Bucaramanga(config-if)#no shutdown
Bucaramanga(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
Bucaramanga(config-if)#exit
Bucaramanga(config)#int g0/1.1
Bucaramanga(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.1, changed state to up
Bucaramanga(config-subif)#encapsulation dot1Q 1 native
Bucaramanga(config-subif)#ip address 172.31.2.1 255.255.255.248
Bucaramanga(config-subif)#exit
Bucaramanga(config)#int g0/1.10
Bucaramanga(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.10, changed state to up
Bucaramanga(config-subif)#encapsulation dot1Q 10
Bucaramanga(config-subif)#ip address 172.31.0.1 255.255.255.192
Bucaramanga(config-subif)#ip helper-address 172.31.2.33
Bucaramanga(config-subif)#ip access-group 101 in
Bucaramanga(config-subif)#exit
Bucaramanga(config)#int g0/1.30
Bucaramanga(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.30, changed state to up
Bucaramanga(config-subif)#encapsulation dot1Q 30

Bucaramanga(config-subif)#ip address 172.31.0.65 255.255.255.192
Bucaramanga(config-subif)#ip helper-address 172.31.2.33
Bucaramanga(config-subif)#ip access-group 103 in
Bucaramanga(config-subif)#

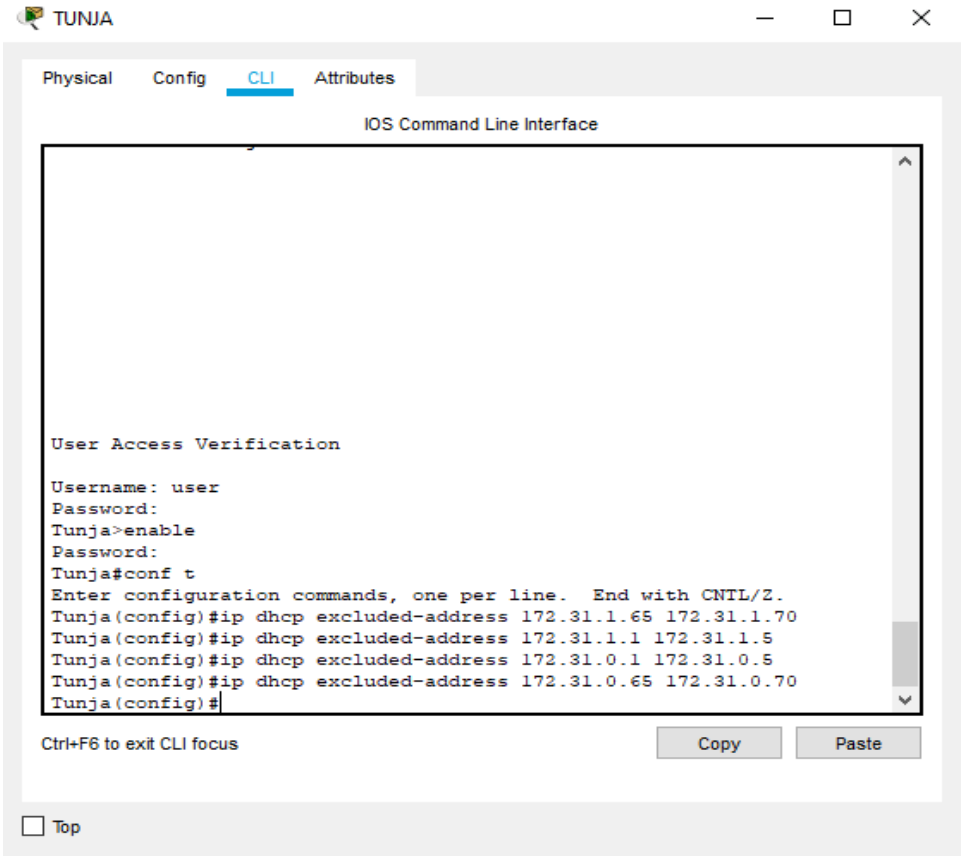
Cundinamarca

Los comandos para utilizar serán los siguientes:

Cundinamarca# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cundinamarca(config)#int g0/1
Cundinamarca(config-if)#no ip address
Cundinamarca(config-if)#duplex auto
Cundinamarca(config-if)#speed auto
Cundinamarca(config-if)#exit
Cundinamarca(config)#int g0/1.1

Cundinamarca(config-subif)#encapsulation dot1Q 1 native
Cundinamarca(config-subif)#ip address 172.31.2.10 255.255.255.248
Cundinamarca(config-subif)#exit
Cundinamarca(config)#int g0/1
Cundinamarca(config-if)#no shutdown
Cundinamarca(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
%LINK-5-CHANGED: Interface GigabitEthernet0/1.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.1, changed state to up
Cundinamarca(config-if)#exit
Cundinamarca(config)#int g0/1.10
Cundinamarca(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.10, changed state to up
Cundinamarca(config-subif)#encapsulation dot1Q 10
Cundinamarca(config-subif)#ip address 172.31.1.65 255.255.255.192
Cundinamarca(config-subif)#ip helper-address 172.31.2.38
Cundinamarca(config-subif)#ip access-group 101 in
Cundinamarca(config-subif)#exit
Cundinamarca(config)#int g0/1.20
Cundinamarca(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.20, changed state to up
Cundinamarca(config-subif)#encapsulation dot1Q 20
Cundinamarca(config-subif)#ip address 172.31.1.1 255.255.255.192
Cundinamarca(config-subif)#ip helper-address 172.31.2.38
Cundinamarca(config-subif)#ip helper-address 172.31.2.37
Cundinamarca(config-subif)#ip access-group 102 in
Cundinamarca(config-subif)#exit
Cundinamarca(config)#int g0/1.10
Cundinamarca(config-subif)#ip helper-address 172.31.2.37
Cundinamarca(config-subif)#exit
Cundinamarca(config)#int g0/1.88
Cundinamarca(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1.88, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1.88, changed state to up
Cundinamarca(config-subif)#encapsulation dot1Q 88 native
Cundinamarca(config-subif)#ip address 172.31.2.25 255.255.255.248
Cundinamarca(config-subif)#exit
Cundinamarca(config)#

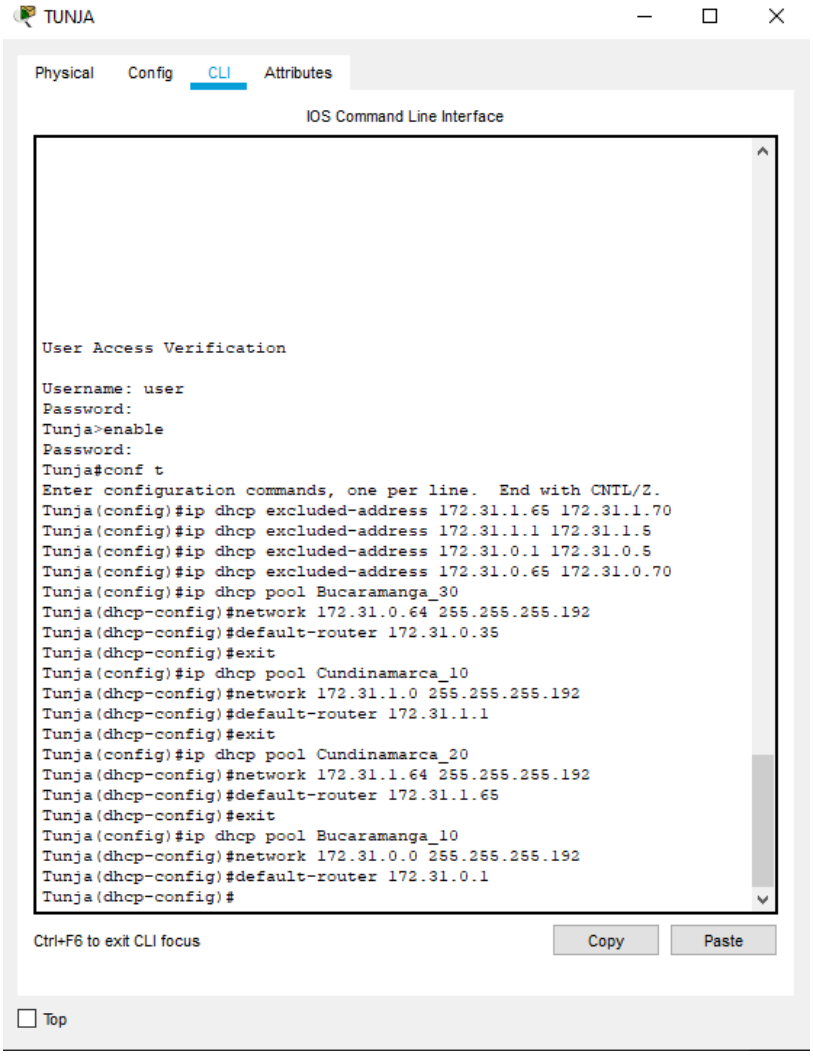
Ilustración 73 Tunja



Los comandos para utilizar serán los siguientes:

Tunja# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#ip dhcp excluded-address 172.31.1.65 172.31.1.70
Tunja(config)#ip dhcp excluded-address 172.31.1.1 172.31.1.5
Tunja(config)#ip dhcp excluded-address 172.31.0.1 172.31.0.5
Tunja(config)#ip dhcp excluded-address 172.31.0.65 172.31.0.70
Tunja(config)#

Tunja

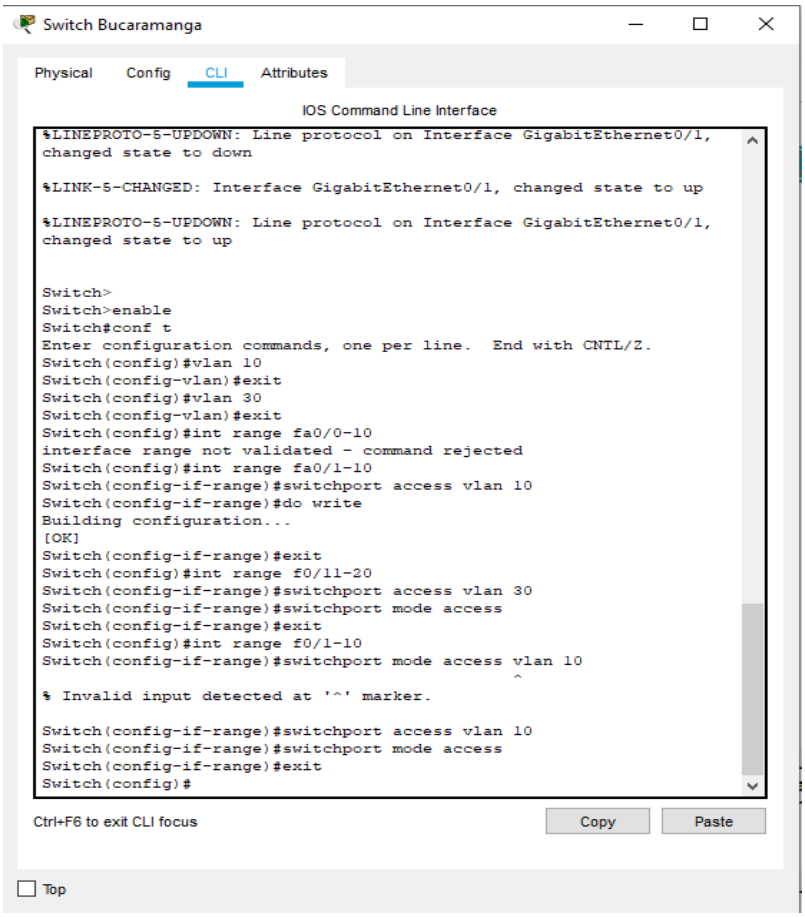


Tunja# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#ip dhcp excluded-address 172.31.1.65 172.31.1.70
Tunja(config)#ip dhcp excluded-address 172.31.1.1 172.31.1.5
Tunja(config)#ip dhcp excluded-address 172.31.0.1 172.31.0.5
Tunja(config)#ip dhcp excluded-address 172.31.0.65 172.31.0.70
Tunja(config)#ip dhcp pool Bucaramanga_30
Tunja(dhcp-config)#network 172.31.0.64 255.255.255.192
Tunja(dhcp-config)#default-router 172.31.0.35
Tunja(dhcp-config)#exit
Tunja(config)#ip dhcp pool Cundinamarca_10
Tunja(dhcp-config)#network 172.31.1.0 255.255.255.192
Tunja(dhcp-config)#default-router 172.31.1.1
Tunja(dhcp-config)#exit
Tunja(config)#ip dhcp pool Cundinamarca_20
Tunja(dhcp-config)#network 172.31.1.64 255.255.255.192
Tunja(dhcp-config)#default-router 172.31.1.65
Tunja(dhcp-config)#exit

Tunja(config)#ip dhcp pool Bucaramanga_10
Tunja(dhcp-config)#network 172.31.0.0 255.255.255.192
Tunja(dhcp-config)#default-router 172.31.0.1
Tunja(dhcp-config)#

Configuramos el switch

Ilustración 74 Switch Bucaramanga

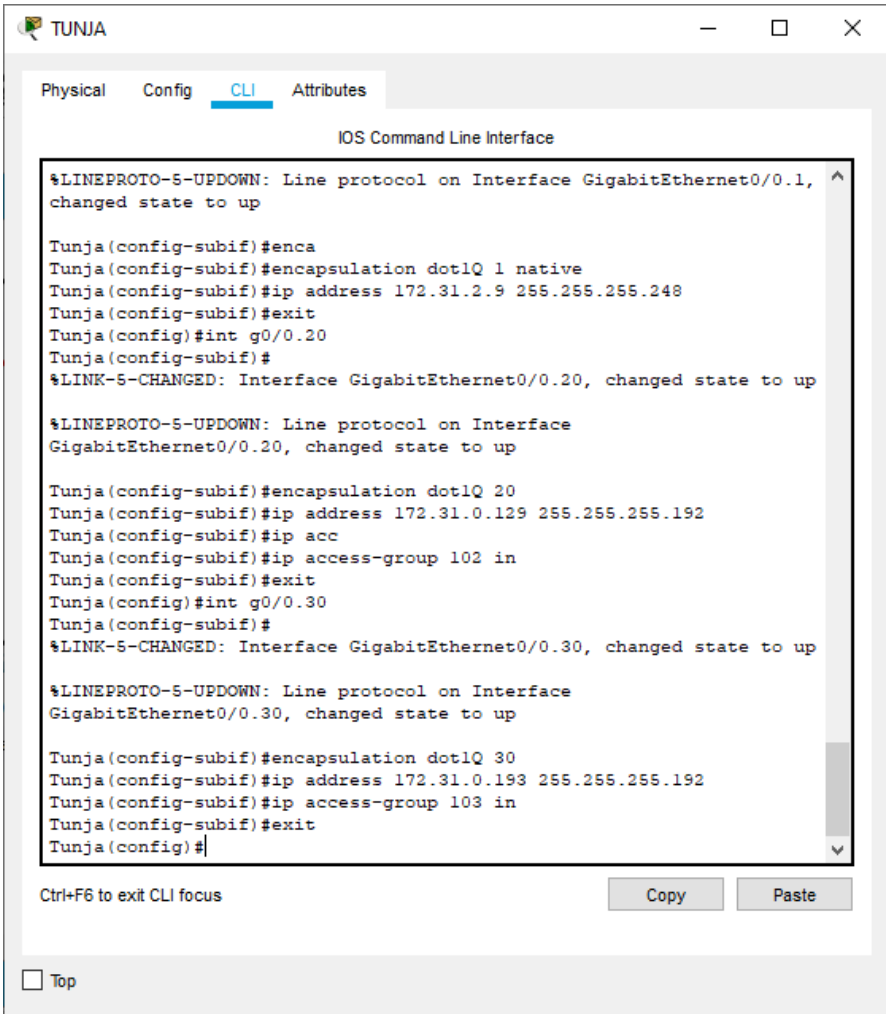


Switch>
Switch>enable
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#exit
Switch(config)#int range fa0/0-10
interface range not validated - command rejected
Switch(config)#int range fa0/1-10
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#do write
Building configuration...
[OK]

Switch(config-if-range)#exit
Switch(config)#int range f0/11-20
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#exit
Switch(config)#int range f0/1-10
Switch(config-if-range)#switchport mode access vlan 10
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#exit
Switch(config)#

Configuramos los router

Ilustración 75 Tunja



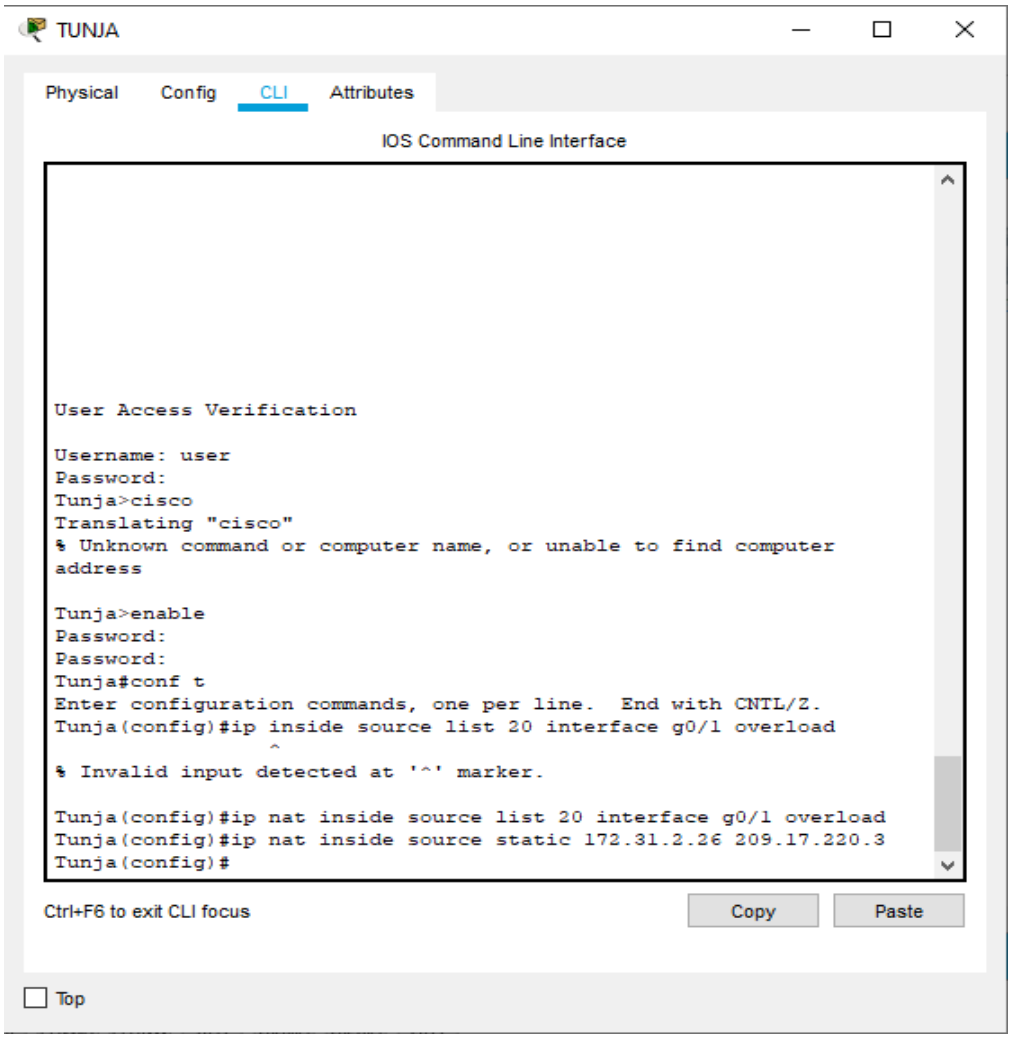
Los comandos para utilizar serán los siguientes:

Tunja# conf t

Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#int g0/0
Tunja(config-if)#no ip address
Tunja(config-if)#ip nat outside
Tunja(config-if)#duplex auto
Tunja(config-if)#speed auto
Tunja(config-if)#exit
Tunja(config)#int g0/0
Tunja(config-if)#no sh
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)#int g0/0.1
Tunja(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.1, changed state to up
Tunja(config-subif)#enca
Tunja(config-subif)#encapsulation dot1Q 1 native
Tunja(config-subif)#ip address 172.31.2.9 255.255.255.248
Tunja(config-subif)#exit
Tunja(config)#int g0/0.20
Tunja(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.20, changed state to up
Tunja(config-subif)#encapsulation dot1Q 20
Tunja(config-subif)#ip address 172.31.0.129 255.255.255.192
Tunja(config-subif)#ip acc
Tunja(config-subif)#ip access-group 102 in
Tunja(config-subif)#exit
Tunja(config)#int g0/0.30
Tunja(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.30, changed state to up
Tunja(config-subif)#encapsulation dot1Q 30
Tunja(config-subif)#ip address 172.31.0.193 255.255.255.192
Tunja(config-subif)#ip access-group 103 in
Tunja(config-subif)#exit
Tunja(config)#

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

Ilustración 76 Tunja- configuración NAT

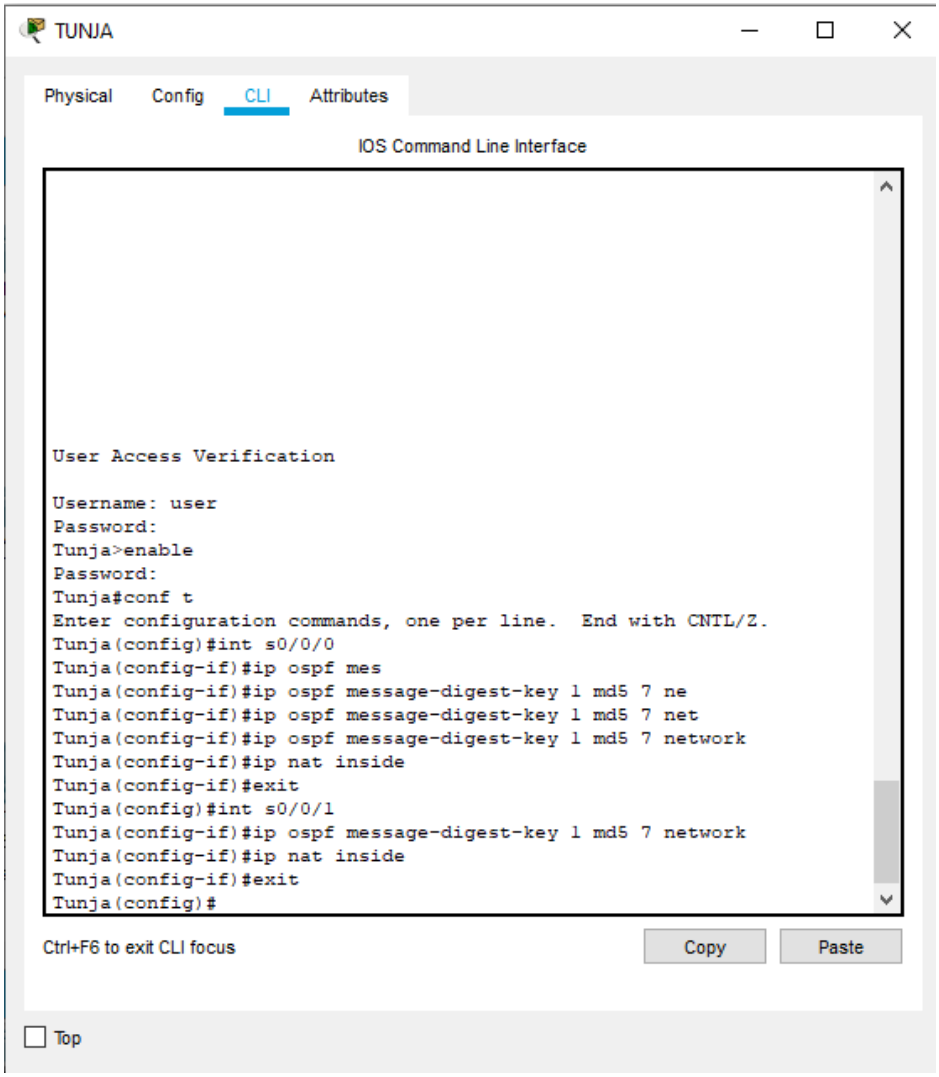


Los comandos para utilizar serán los siguientes:

Tunja>enable
Password:
Password:
Tunja# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#ip inside source list 20 interface g0/1 overload
Tunja(config)#ip nat inside source list 20 interface g0/1 overload
Tunja(config)#ip nat inside source static 172.31.2.26 209.17.220.3
Tunja(config)#

4. El enrutamiento deberá tener autenticación.

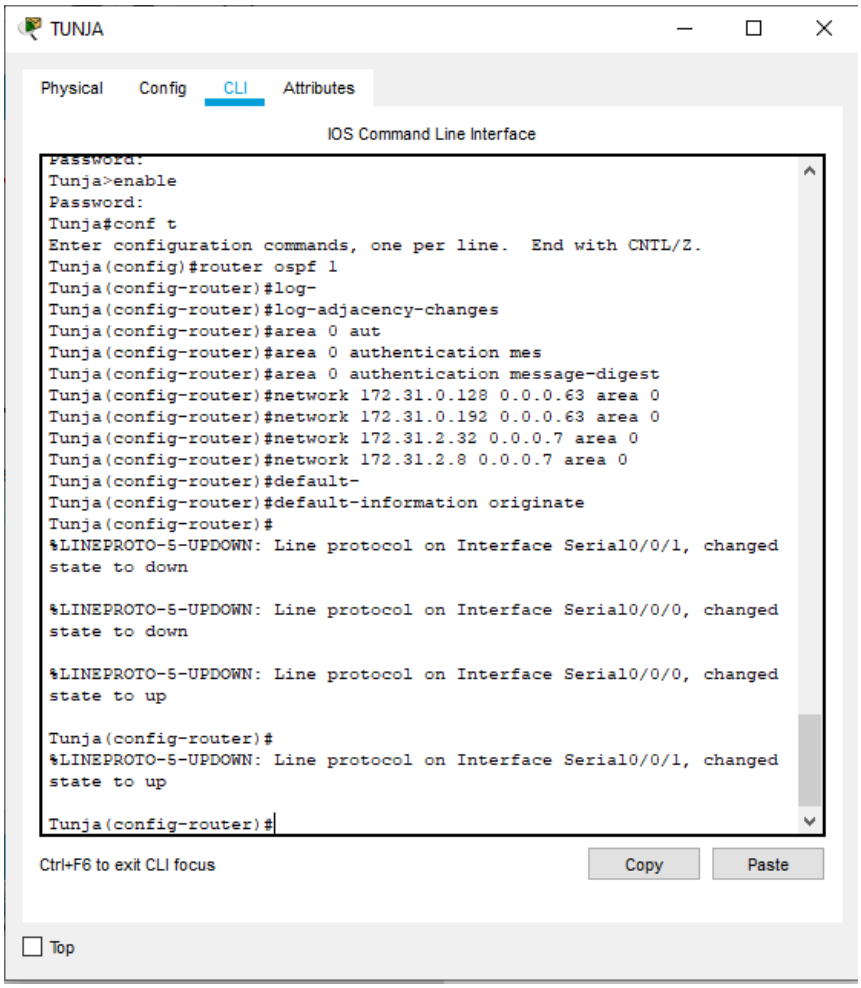
Ilustración 77 Tunja- Autenticación enrutamiento



Los comandos para utilizar serán los siguientes:

Tunja# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#int s0/0/0
Tunja(config-if)#ip ospf mes
Tunja(config-if)#ip ospf message-digest-key 1 md5 7 ne
Tunja(config-if)#ip ospf message-digest-key 1 md5 7 net
Tunja(config-if)#ip ospf message-digest-key 1 md5 7 network
Tunja(config-if)#ip nat inside
Tunja(config-if)#exit
Tunja(config)#int s0/0/1
Tunja(config-if)#ip ospf message-digest-key 1 md5 7 network
Tunja(config-if)#ip nat inside
Tunja(config-if)#exit
Tunja(config)#

Ilustración 78 Tunja

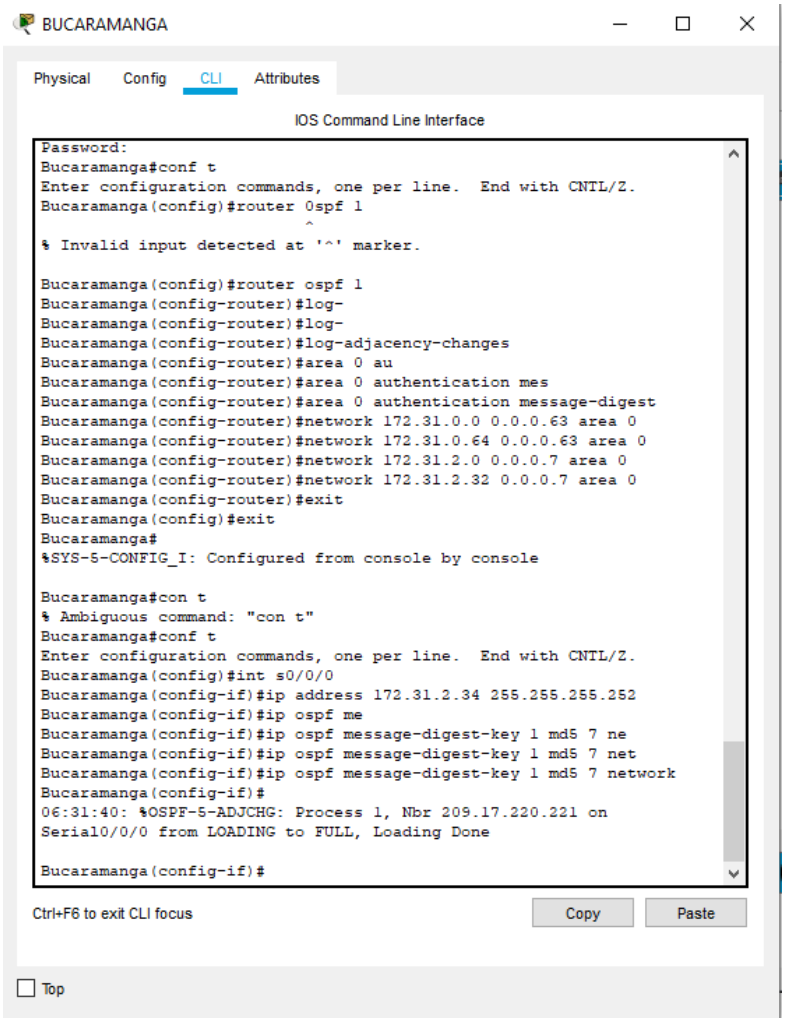


Los comandos para utilizar serán los siguientes:

Tunja# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#router ospf 1
Tunja(config-router)#log-
Tunja(config-router)#log-adjacency-changes
Tunja(config-router)#area 0 aut
Tunja(config-router)#area 0 authentication mes
Tunja(config-router)#area 0 authentication message-digest
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 0.0.0.7 area 0
Tunja(config-router)#network 172.31.2.8 0.0.0.7 area 0
Tunja(config-router)#default-
Tunja(config-router)#default-information originate
Tunja(config-router)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Tunja(config-router)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
Tunja(config-router)#

Ilustración 79 Bucaramanga

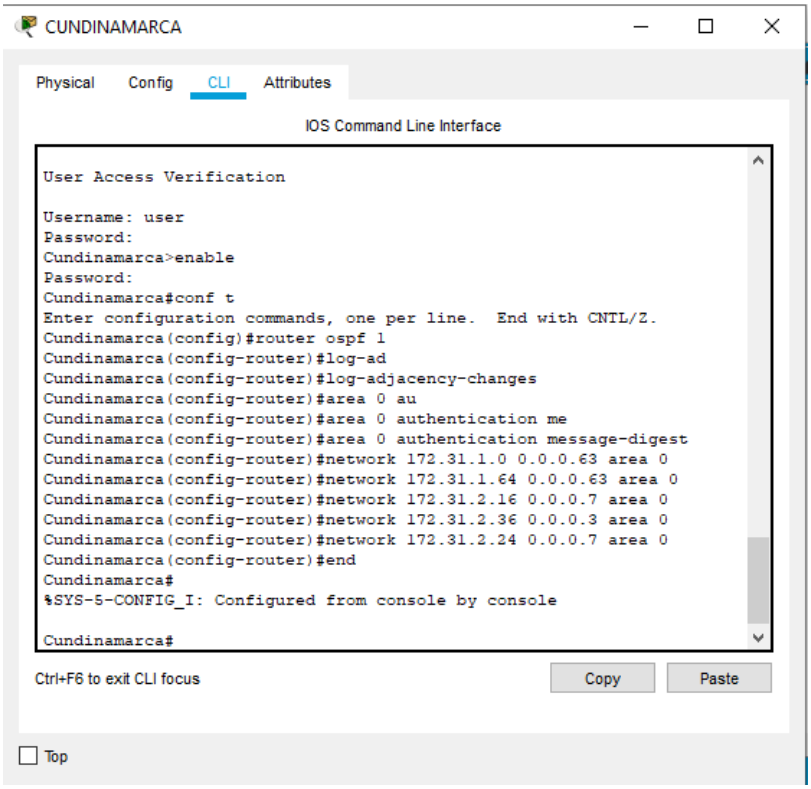


Los comandos para utilizar serán los siguientes:

Bucaramanga# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bucaramanga(config)#router ospf 1
Bucaramanga(config-router)#log-
Bucaramanga(config-router)#log-

Bucaramanga(config-router)#log-adjacency-changes
Bucaramanga(config-router)#area 0 au
Bucaramanga(config-router)#area 0 authentication mes
Bucaramanga(config-router)#area 0 authentication message-digest
Bucaramanga(config-router)#network 172.31.0.0 0.0.0.63 area 0
Bucaramanga(config-router)#network 172.31.0.64 0.0.0.63 area 0
Bucaramanga(config-router)#network 172.31.2.0 0.0.0.7 area 0
Bucaramanga(config-router)#network 172.31.2.32 0.0.0.7 area 0
Bucaramanga(config-router)#exit
Bucaramanga(config)#exit
Bucaramanga#
%SYS-5-CONFIG_I: Configured from console by console
Bucaramanga# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bucaramanga(config)#int s0/0/0
Bucaramanga(config-if)#ip address 172.31.2.34 255.255.255.252
Bucaramanga(config-if)#ip ospf me
Bucaramanga(config-if)#ip ospf message-digest-key 1 md5 7 ne
Bucaramanga(config-if)#ip ospf message-digest-key 1 md5 7 net
Bucaramanga(config-if)#ip ospf message-digest-key 1 md5 7 network
Bucaramanga(config-if)#
06:31:40: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.221 on Serial0/0/0 from LOADING to FULL, Loading Done
Bucaramanga(config-if)#

Ilustración 80 Cundinamarca



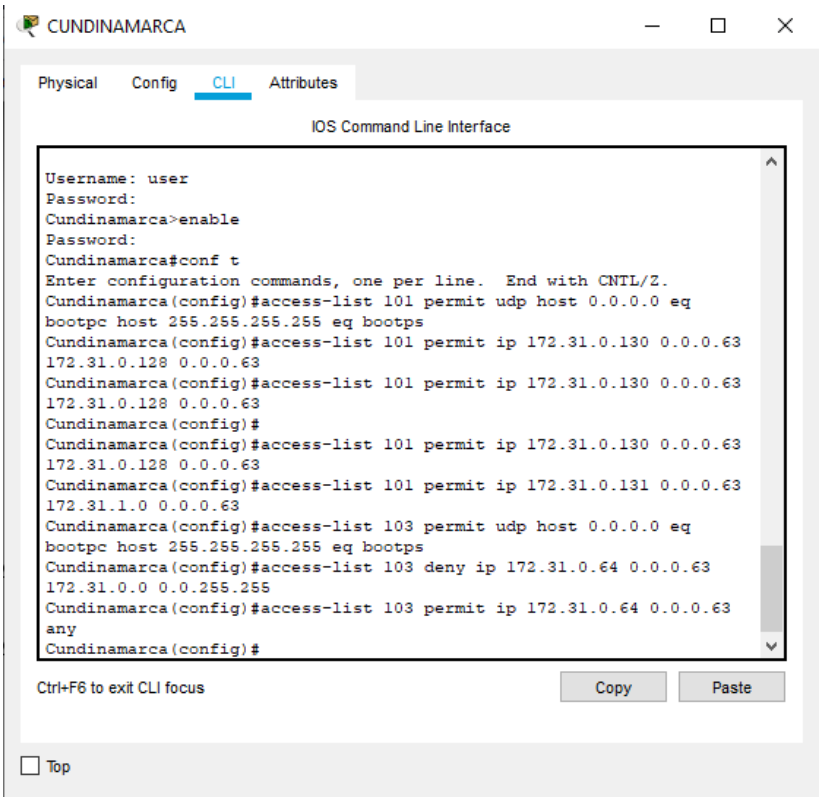
Los comandos para utilizar serán los siguientes:

Cundinamarca#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cundinamarca(config)#router ospf 1
Cundinamarca(config-router)#log-ad
Cundinamarca(config-router)#log-adjacency-changes
Cundinamarca(config-router)#area 0 au
Cundinamarca(config-router)#area 0 authentication me
Cundinamarca(config-router)#area 0 authentication message-digest
Cundinamarca(config-router)#network 172.31.1.0 0.0.0.63 area 0
Cundinamarca(config-router)#network 172.31.1.64 0.0.0.63 area 0
Cundinamarca(config-router)#network 172.31.2.16 0.0.0.7 area 0
Cundinamarca(config-router)#network 172.31.2.36 0.0.0.3 area 0
Cundinamarca(config-router)#network 172.31.2.24 0.0.0.7 area 0
Cundinamarca(config-router)#end

5. Listas de control de acceso:

Se configura la lista de acceso o acces-list en cada uno de los router

Ilustración 81 Cundinamarca-lista de control de acceso

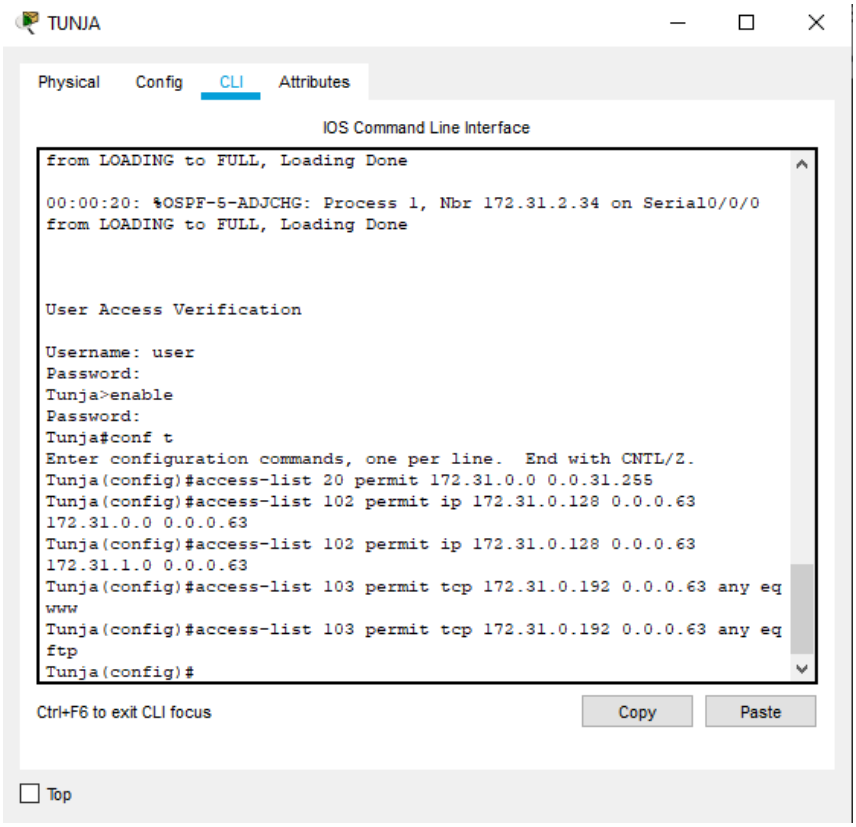


Los comandos para utilizar serán los siguientes:

Cundinamarca>enable
Password:

Cundinamarca#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cundinamarca(config)#access-list 101 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
Cundinamarca(config)#
Cundinamarca(config)#access-list 101 permit ip 172.31.0.130 0.0.0.63 172.31.0.128 0.0.0.63
Cundinamarca(config)#access-list 101 permit ip 172.31.0.131 0.0.0.63 172.31.1.0 0.0.0.63
Cundinamarca(config)#access-list 103 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
Cundinamarca(config)#access-list 103 deny ip 172.31.0.64 0.0.0.63 172.31.0.0 0.0.255.255
Cundinamarca(config)#access-list 103 permit ip 172.31.0.64 0.0.0.63 any
Cundinamarca(config)#

Ilustración 82 Tunja-lista de control de acceso

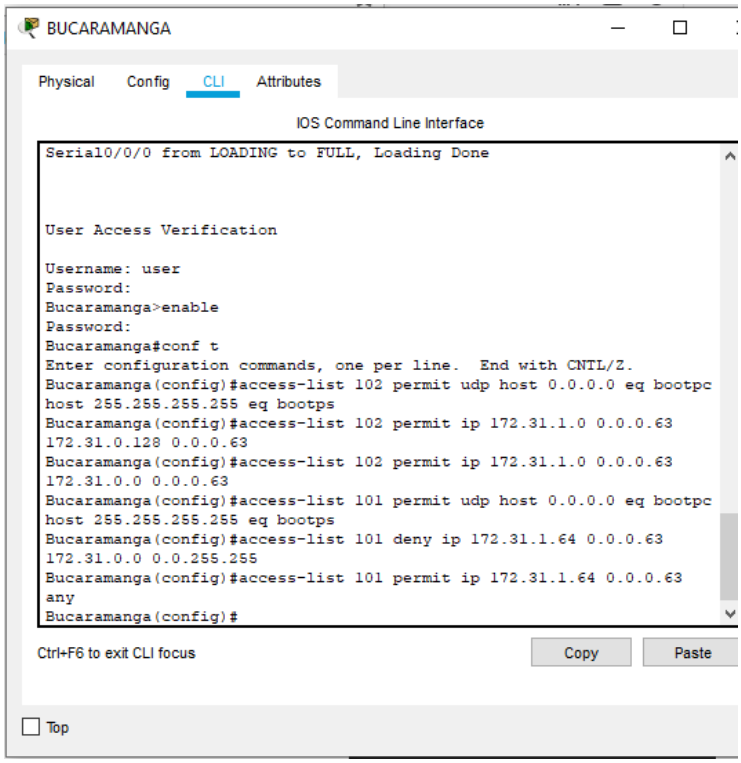


Los comandos para utilizar serán los siguientes:

Tunja>enable
Password:
Tunja#conf t
Enter configuration commands, one per line. End with CNTL/Z.

Tunja(config)#access-list 20 permit 172.31.0.0 0.0.31.255
Tunja(config)#access-list 102 permit ip 172.31.0.128 0.0.0.63 172.31.0.0 0.0.0.63
Tunja(config)#access-list 102 permit ip 172.31.0.128 0.0.0.63 172.31.1.0 0.0.0.63
Tunja(config)#access-list 103 permit tcp 172.31.0.192 0.0.0.63 any eq www
Tunja(config)#access-list 103 permit tcp 172.31.0.192 0.0.0.63 any eq ftp
Tunja(config)#

Ilustración 83 Bucaramanga-lista de control de acceso



Los comandos para utilizar serán los siguientes:

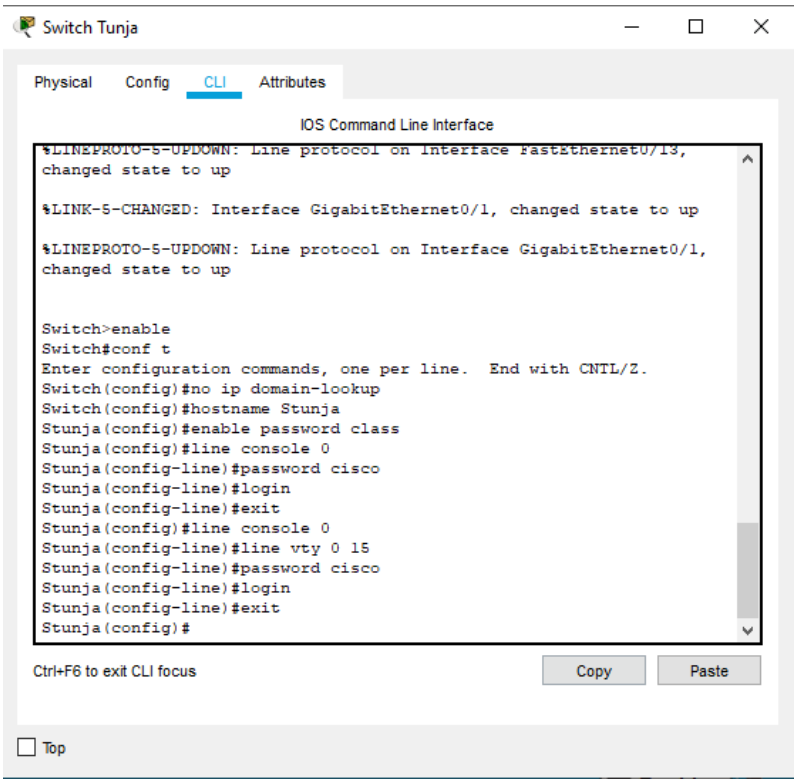
Bucaramanga>enable
Password:
Bucaramanga#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bucaramanga(config)#access-list 102 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
Bucaramanga(config)#access-list 102 permit ip 172.31.1.0 0.0.0.63 172.31.0.128 0.0.0.63
Bucaramanga(config)#access-list 102 permit ip 172.31.1.0 0.0.0.63 172.31.0.0 0.0.0.63
Bucaramanga(config)#access-list 101 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
Bucaramanga(config)#access-list 101 deny ip 172.31.1.64 0.0.0.63 172.31.0.0 0.0.255.255
Bucaramanga(config)#access-list 101 permit ip 172.31.1.64 0.0.0.63 any
Bucaramanga(config)#

Vamos a realizar la configuración de los switch

- 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.

Le asignaremos las contraseñas correspondientes a cada uno de los switch de la red:

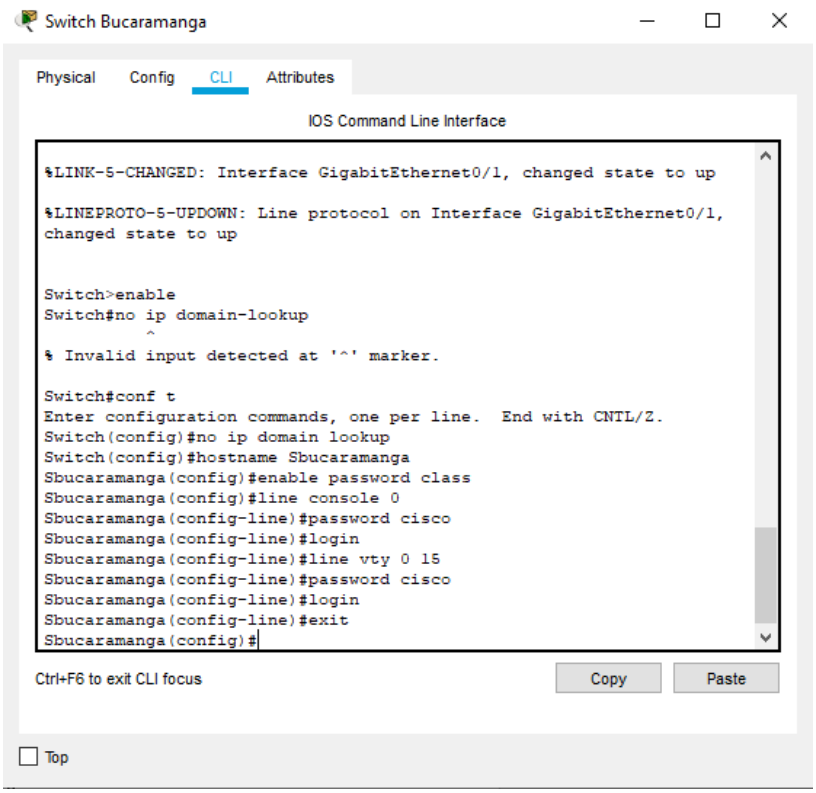
Ilustración 84 Switch Tunja



Los comandos para utilizar serán los siguientes:

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname Stunja
Stunja(config)#enable password class
Stunja(config)#line console 0
Stunja(config-line)#password cisco
Stunja(config-line)#login
Stunja(config-line)#exit
Stunja(config)#line console 0
Stunja(config-line)#line vty 0 15
Stunja(config-line)#password cisco
Stunja(config-line)#login
Stunja(config-line)#exit
Stunja(config)#

Ilustración 85 Switch Bucaramanga

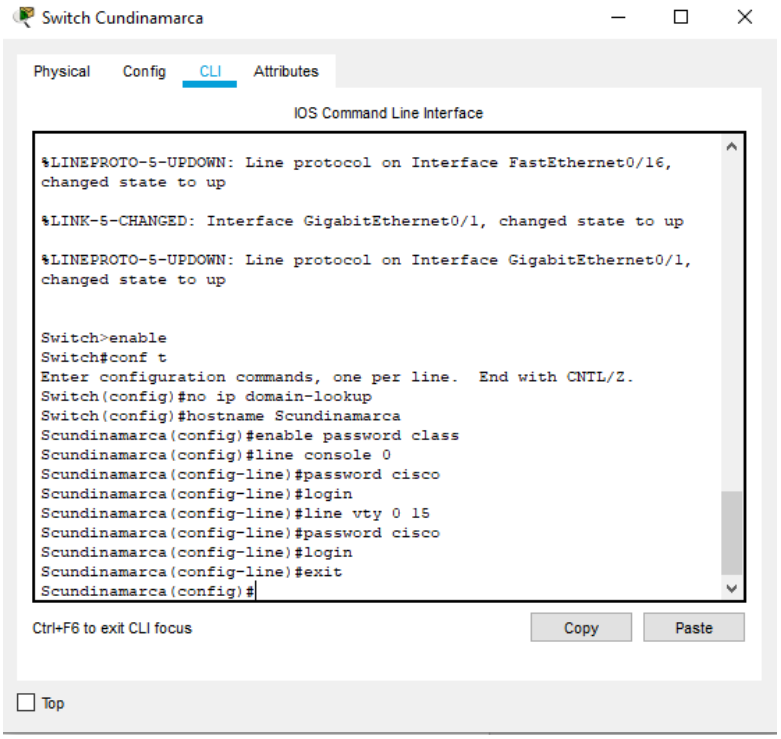


Los comandos para utilizar serán los siguientes:

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain lookup

Switch(config)#hostname Sbucaramanga
Sbucaramanga(config)#enable password class
Sbucaramanga(config)#line console 0
Sbucaramanga(config-line)#password cisco
Sbucaramanga(config-line)#login
Sbucaramanga(config-line)#line vty 0 15
Sbucaramanga(config-line)#password cisco
Sbucaramanga(config-line)#login
Sbucaramanga(config-line)#exit
Sbucaramanga(config)#!
Sbucaramanga#

Ilustración 86 Switch Cundinamarca

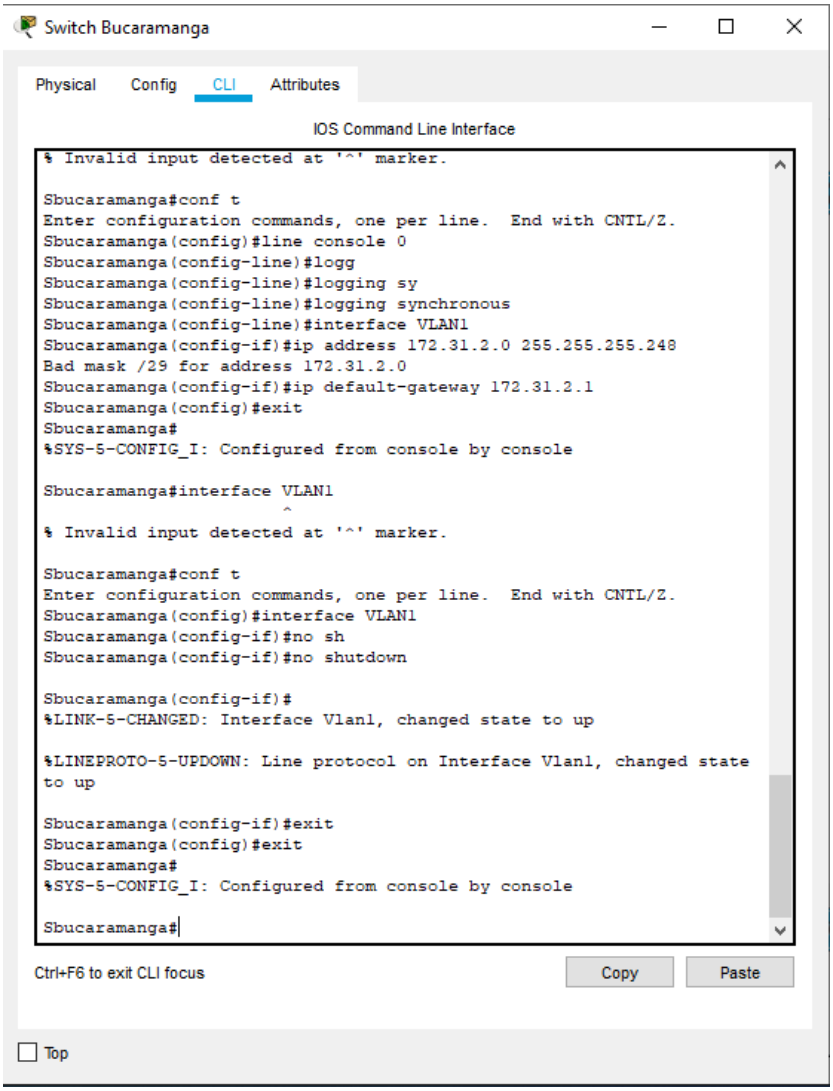


Los comandos para utilizar serán los siguientes:

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname Scundinamarca
Scundinamarca(config)#enable password class
Scundinamarca(config)#line console 0
Scundinamarca(config-line)#password cisco
Scundinamarca(config-line)#login
Scundinamarca(config-line)#line vty 0 15

Scundinamarca(config-line)#password cisco
Scundinamarca(config-line)#login
Scundinamarca(config-line)#exit
Scundinamarca(config)#

Ilustración 87 Switch Bucaramanga



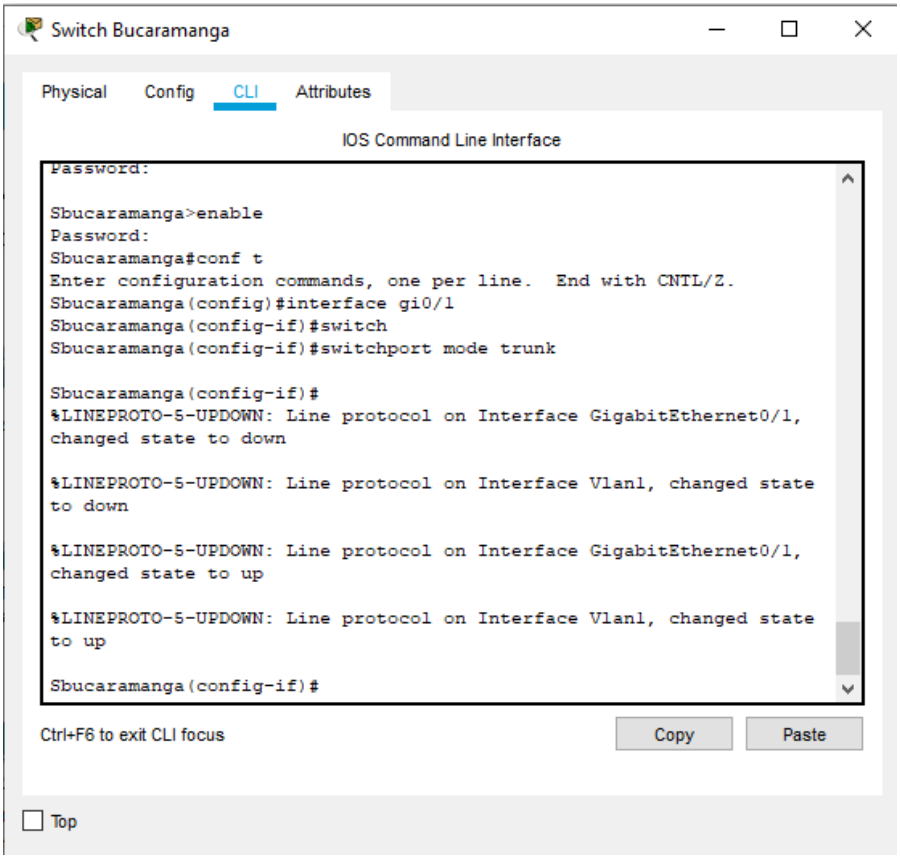
Los comandos para utilizar serán los siguientes:

Sbucaramanga#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Sbucaramanga(config)#line console 0
Sbucaramanga(config-line)#logg
Sbucaramanga(config-line)#logging sy
Sbucaramanga(config-line)#logging synchronous
Sbucaramanga(config-line)#interface VLAN1
Sbucaramanga(config-if)#ip address 172.31.2.0 255.255.255.248
Bad mask /29 for address 172.31.2.0

Sbucaramanga(config-if)#ip default-gateway 172.31.2.1
Sbucaramanga(config)#exit
Sbucaramanga#
%SYS-5-CONFIG_I: Configured from console by console
Sbucaramanga#interface VLAN1
Sbucaramanga#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Sbucaramanga(config)#interface VLAN1
Sbucaramanga(config-if)#no sh
Sbucaramanga(config-if)#no shutdown
Sbucaramanga(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
Sbucaramanga(config-if)#exit
Sbucaramanga(config)#exit
Sbucaramanga#
%SYS-5-CONFIG_I: Configured from console by console
Sbucaramanga#

Le vamos a asignar el puerto troncal:

Ilustración 88 Bucaramanga- Puerto troncal

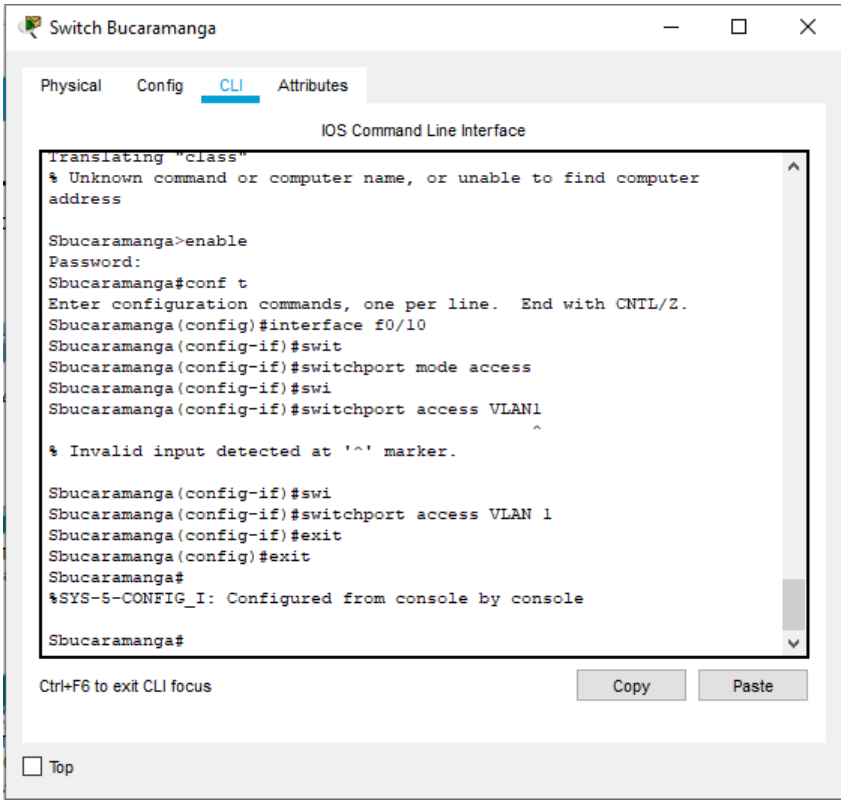


Sbucaramanga>enable

Password:
Sbucaramanga#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Sbucaramanga(config)#interface gi0/1
Sbucaramanga(config-if)#switch
Sbucaramanga(config-if)#switchport mode trunk
Sbucaramanga(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
Sbucaramanga(config-if)#

Asigne el puerto de acceso para las pc:

Ilustración 89 Bucaramanga- Puerto de acceso PC

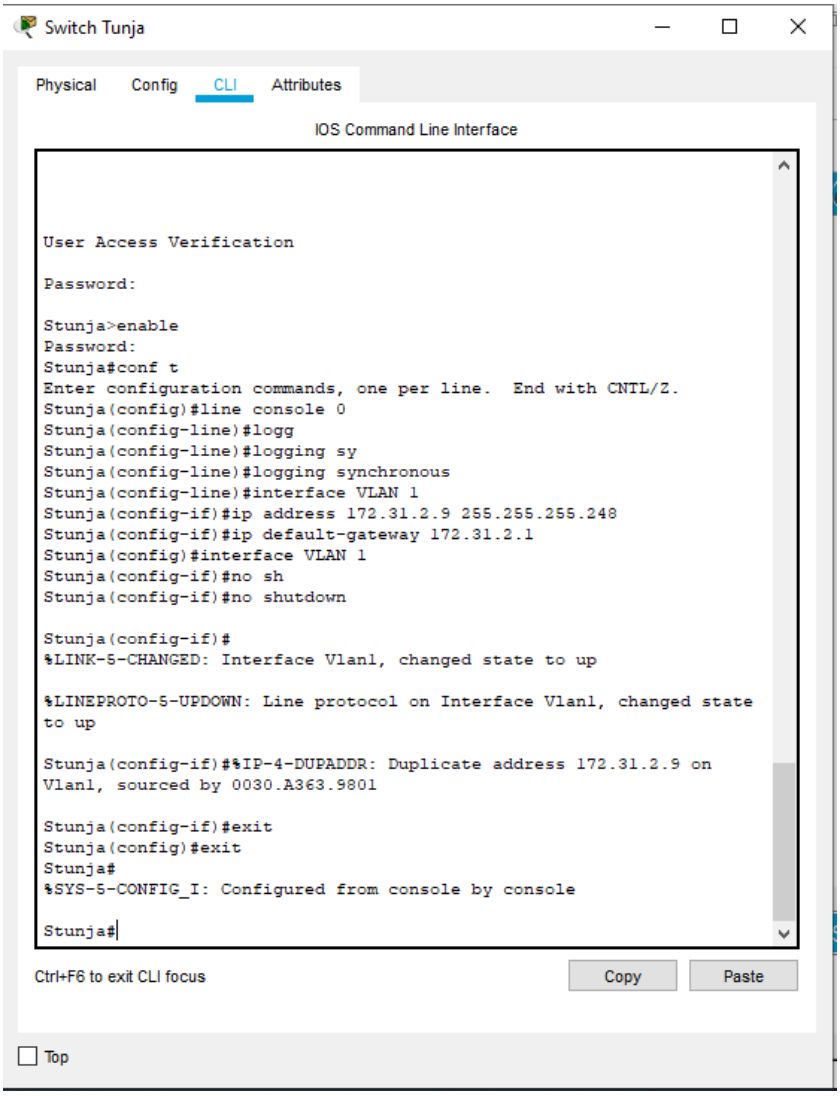


Los comandos para utilizar serán los siguientes:

Sbucaramanga>enable
Password:
Sbucaramanga#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Sbucaramanga(config)#interface f0/10

Sbucaramanga(config-if)#swit
Sbucaramanga(config-if)#switchport mode access
Sbucaramanga(config-if)#swi
Sbucaramanga(config-if)#swi
Sbucaramanga(config-if)#switchport access VLAN 1
Sbucaramanga(config-if)#exit
Sbucaramanga(config)#exit
Sbucaramanga#
%SYS-5-CONFIG_I: Configured from console by console
Sbucaramanga#

Ilustración 90 Switch Tunja- Puerto de acceso PC



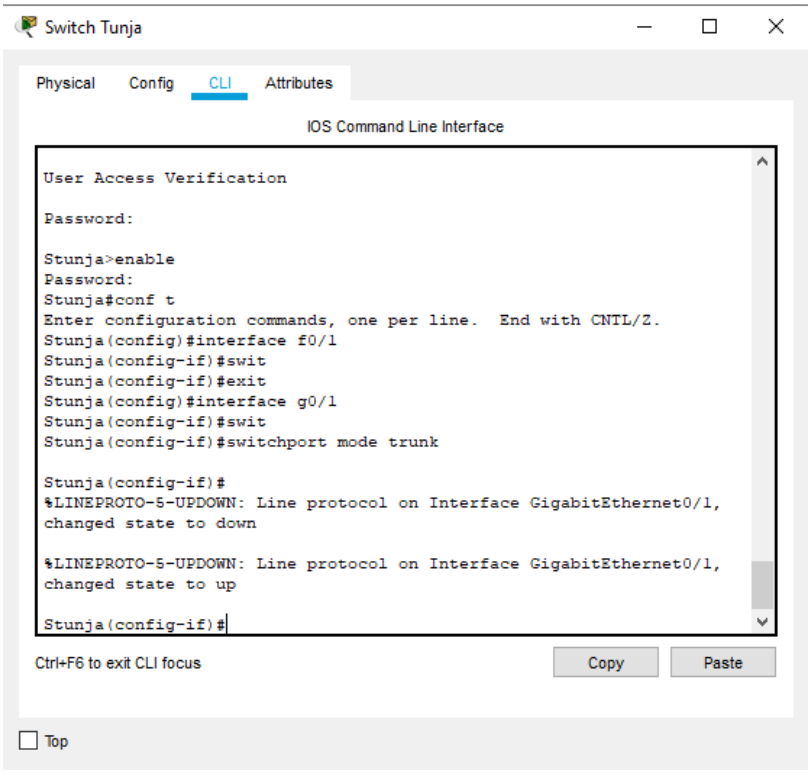
Los comandos para utilizar serán los siguientes:

Stunja>enable
Password:
Stunja#conf t

Enter configuration commands, one per line. End with CNTL/Z.
Stunja(config)#line console 0
Stunja(config-line)#logg
Stunja(config-line)#logging sy
Stunja(config-line)#logging synchronous
Stunja(config-line)#interface VLAN 1
Stunja(config-if)#ip address 172.31.2.9 255.255.255.248
Stunja(config-if)#ip default-gateway 172.31.2.1
Stunja(config)#interface VLAN 1
Stunja(config-if)#no sh
Stunja(config-if)#no shutdown
Stunja(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
Stunja(config-if)#%IP-4-DUPADDR: Duplicate address 172.31.2.9 on Vlan1, sourced by 0030.A363.9801
Stunja(config-if)#exit
Stunja(config)#exit
Stunja#
%SYS-5-CONFIG_I: Configured from console by console
Stunja#

Ahora le vamos a asignar los puertos troncales:

Ilustración 91 Switch Tunja- Puerto troncal

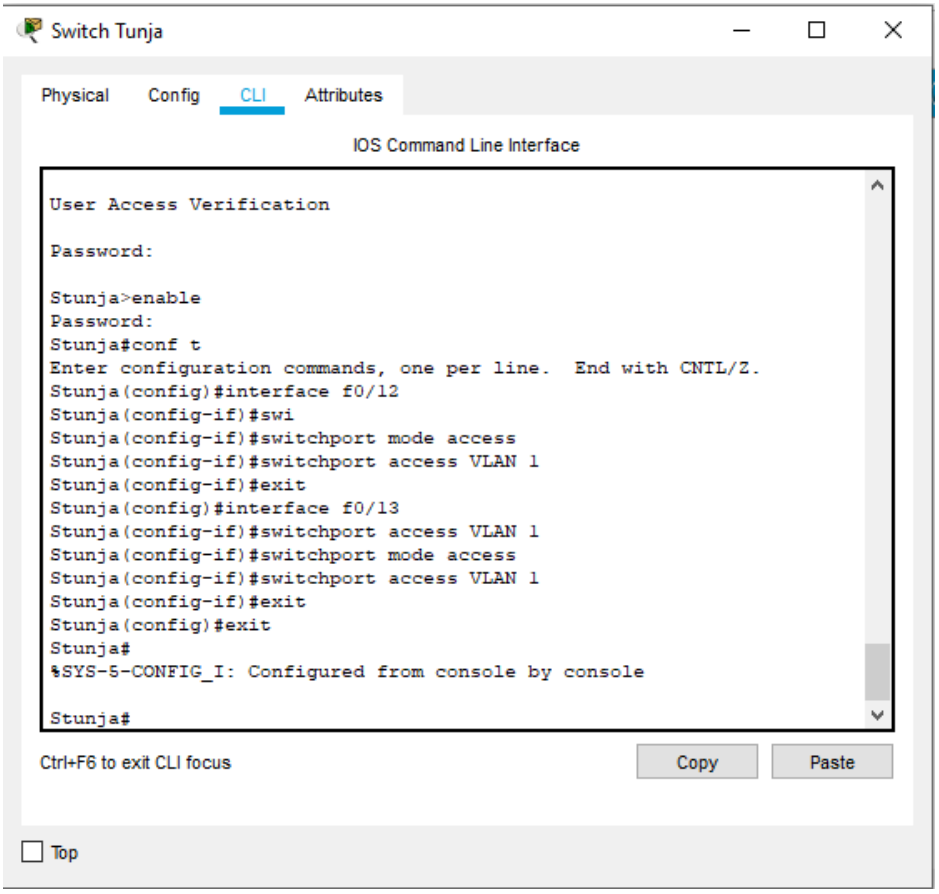


Los comandos que vamos a utilizar serán los siguientes:

Stunja>enable
Password:
Stunja#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Stunja(config)#interface f0/1
Stunja(config-if)#swit
Stunja(config-if)#exit
Stunja(config)#interface g0/1
Stunja(config-if)#swit
Stunja(config-if)#switchport mode trunk
Stunja(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
Stunja(config-if)#

Vamos a cargar las VLAN

Ilustración 92 Switch Tunja- VLAN

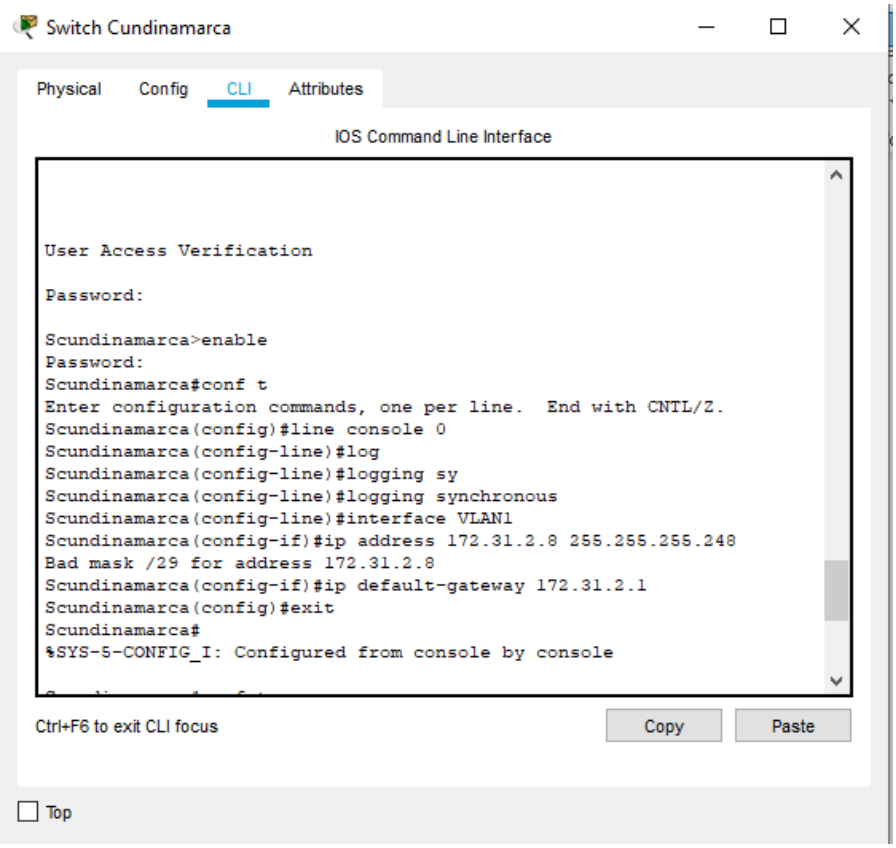


Los comandos que vamos a utilizar serán los siguientes:

Stunja>enable
Password:
Stunja#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Stunja(config)#interface f0/12
Stunja(config-if)#swi
Stunja(config-if)#switchport mode access
Stunja(config-if)#switchport access VLAN 1
Stunja(config-if)#exit
Stunja(config)#interface f0/13
Stunja(config-if)#switchport access VLAN 1
Stunja(config-if)#switchport mode access
Stunja(config-if)#switchport access VLAN 1
Stunja(config-if)#exit
Stunja(config)#exit
Stunja#
%SYS-5-CONFIG_I: Configured from console by console
Stunja#

Ahora vamos a configurar el switch de Cundinamarca:

Ilustración 93 Switch- Cundinamarca

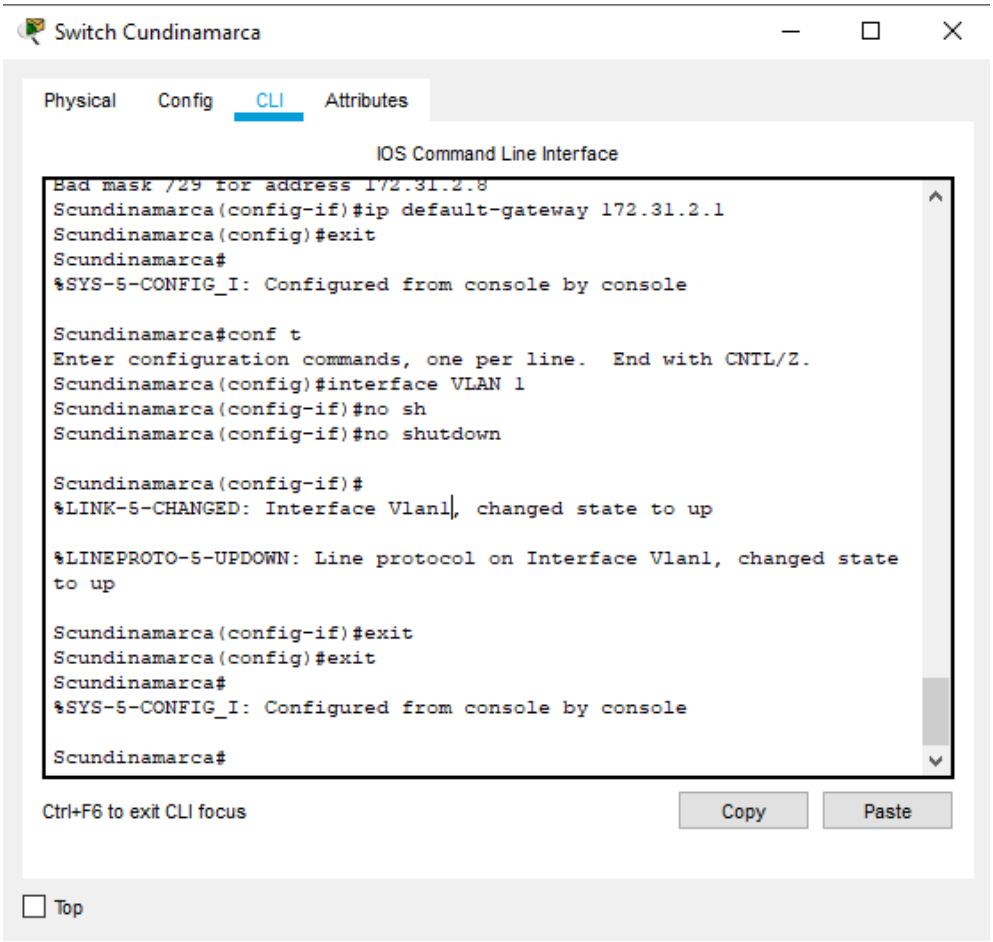


Los comandos que vamos a utilizar serán los siguientes:

Scundinamarca>enable
Password:
Scundinamarca#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Scundinamarca(config)#line console 0
Scundinamarca(config-line)#log
Scundinamarca(config-line)#logging sy
Scundinamarca(config-line)#logging synchronous
Scundinamarca(config-line)#interface VLAN1
Scundinamarca(config-if)#ip address 172.31.2.8 255.255.255.248
Bad mask /29 for address 172.31.2.8
Scundinamarca(config-if)#ip default-gateway 172.31.2.1
Scundinamarca(config)#exit
Scundinamarca#
%SYS-5-CONFIG_I: Configured from console by console

Ahora configuramos la VLAN

Ilustración 94 Switch Cundinamarca VLAN

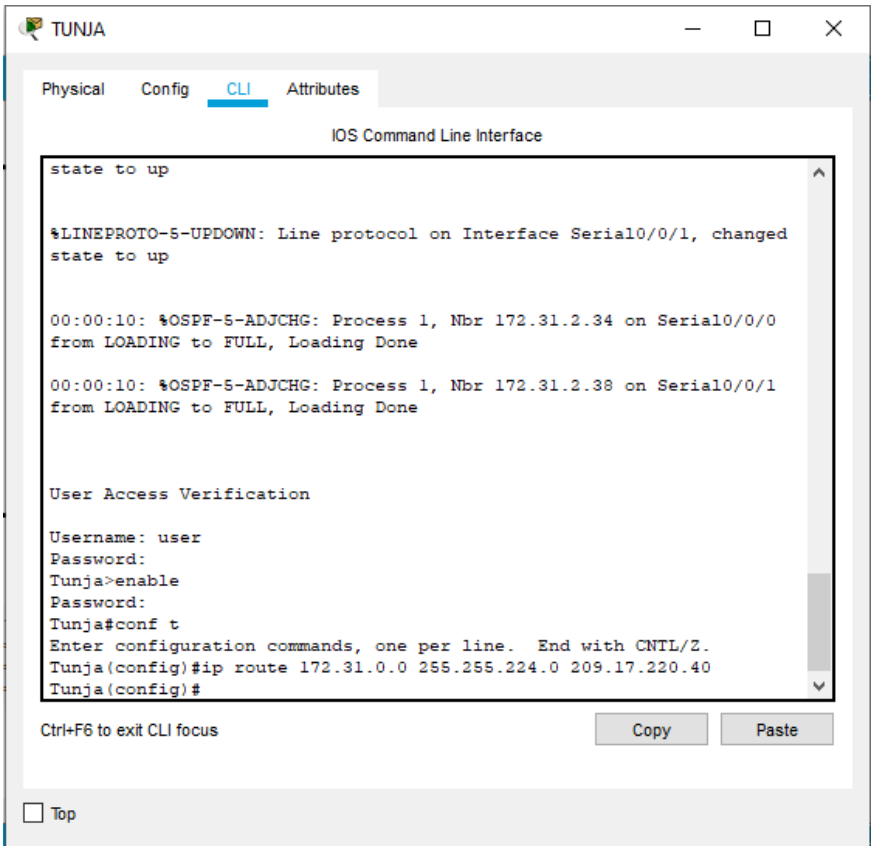


Los comandos que vamos a utilizar serán los siguientes:

Scundinamarca#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Scundinamarca(config)#interface VLAN 1
Scundinamarca(config-if)#no sh
Scundinamarca(config-if)#no shutdown
Scundinamarca(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
Scundinamarca(config-if)#exit
Scundinamarca(config)#exit
Scundinamarca#
%SYS-5-CONFIG_I: Configured from console by console
Scundinamarca#

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

Ilustración 95 Tunja-VLSM



Los comandos que vamos a utilizar serán los siguientes:

Tunja#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Tunja(config)#ip route 172.31.0.0 255.255.224.0 209.17.220.40

Tunja(config)#

Se pueden evidenciar los equipos de la red con conexión DHCP:

Ilustración 96 PC-Red-Bucaramanga con DHCP

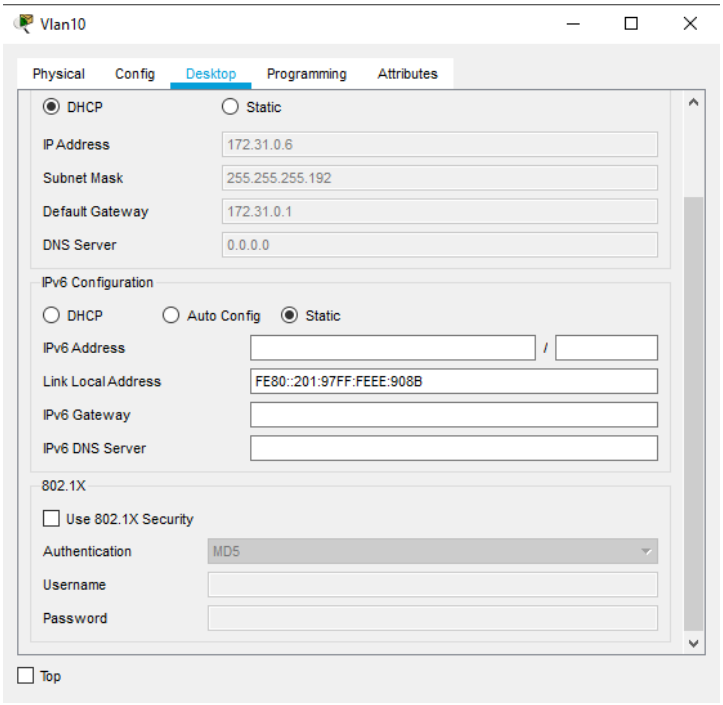
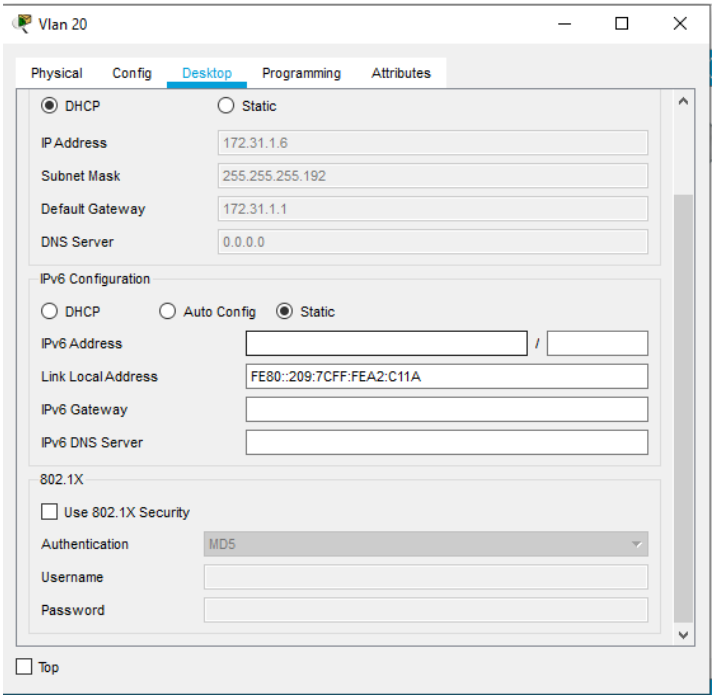


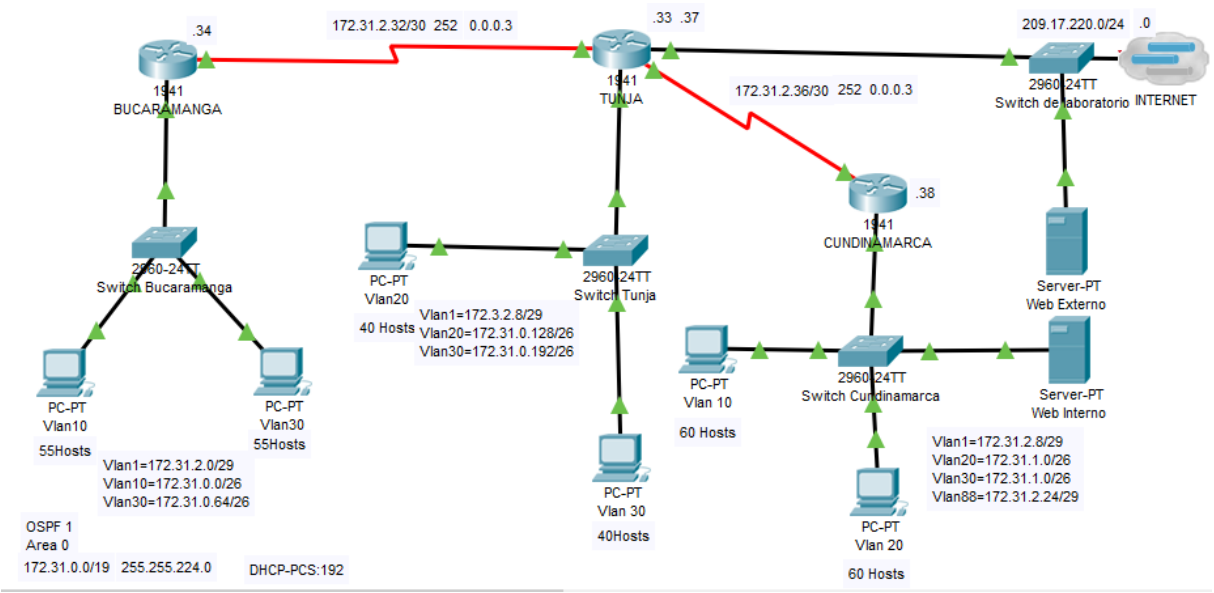
Ilustración 97 PC-Red-Cundinamarca con DHCP



Aspectos para 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

Ilustración 98 Topología con total funcionamiento



Conclusiones

- Las practicas desarrolladas durante el diplomado que corresponden al CCNA1 Y CCNA2 nos brindaron información muy útil para el desarrollo de esta prueba de habilidades.
- Al momento de buscar soluciones para el desarrollo de la actividad correspondiente a las topologías de los escenarios nos dejan algunos inconvenientes presentados a la hora de aplicar algunos comandos, pues algunos fueron nuevos para nosotros.
- Con las practicas puestas en marcha nos podemos afianzar mucho más en el manejo de la herramienta packet tracer.
- Es de anotar que se obtiene conocimiento en la asignación de direcciones IP y la configuración básica en cada uno de los equipos de la red.
- Se aplico el conocimiento obtenido entre ellos la ejecución de los comandos #show ip route para verificar la tabla de enrutamiento, como también su balanceo de carga.
- Se usaron los comandos como #show cdp neighbors para realizar un diagnóstico de vecinos en la red, se evidencia la conectividad en la red utilizando el comando PING
- Se consultaron diversos medios como videos y páginas de internet con el fin de reforzar los conocimientos básicos en el enrutamiento EIGRP y despejar dudas al momento de adelantar configuraciones en los routers, nos permite ver verificar la vecindad en la red con el comando #show ip eigrp.
- Se realizaron variaciones en las configuraciones de la lista de control de acceso, a fin de generar ayudas que nos permitieran a través de los diversos comandos evaluar la no conectividad de las redes.
- Se realizar la autenticación local con AAA en la red, como también el cifrado de contraseñas y se establece un servidor TFTP para el escenario 2.
- Evidenciamos la aplicación de DHCP como se solicita para la red, dejando en funcionamiento el mismo y dando solución a los requerimientos.
- Asi mismo se logra evidenciar a lo largo de la actividad que los dos escenarios confirman el funcionamiento de lo solicitado en la actividad.

Referencias bibliográficas

Gerometta Oscar, (2015), 28 de Junio, Que es una SVI, recuperado de http://librosnetworking.blogspot.com/2015/06/que-es-una-svi.html

ConfiguraciónDHCP en Router (s.f), 27 de Mayo de 2018, recuperado de https://apuntesdecisco.blogspot.com/2008/07/configuracin-de-dhcp-en-el-router.html

CISCO. (1 de Febrero de 2016). Cisco Connected Grid Ethernet Switch Module Interface Card Software Configuration Guide.Obtenido de http://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/switch_module_swcg/cgr-esm-configuration/config_vlans.html#33099

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Disponible en https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1
- CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Disponible en https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1
- CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Disponible en https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

Mis Libros de Networking. (2006). Recuperado el 02 de 06 de 2018, de Mis Libros de Networking.com: http://librosnetworking.blogspot.com/2013/09/el-router-id-en-ospf.html

Todo informática, Copyright © 2015 All Right Reserved-Created by-Como crear y configurar VLANs: https://www.tadoinformatica.com/2016/09/cisco-ccna-como-crear-y-configurar.html

Mikro Ways, recuperdo 05 de agosto de 2009- configuración de VLANs con cisco: https://www.mikroways.net/2009/08/05/configuracion-de-vlans-con-cisco/