PRUEBA DE HABILIDADES PRÁCTICAS CCNA, DISEÑO DE UNA RED DE TELECOMUNICACIONES

AUTOR:

YEISON MORENO RODRÍGUEZ

Trabajo de grado diplomado de profundización

Tutor Del Diplomado: Efrain Alejandro Perez
Director Del Diplomado: Juan Carlos Vesga

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA,
ECBTI,
INGENIERIA DE SISTEMAS,
BOGOTA
2019

Agradecimiento eterno a mis Padres Rigoberto Moreno
y Luz Marina Villa por su apoyo incondicional.

CONTENIDO

pág.

RESUMEN (ABSTRACT)

El documento que se presenta a continuación tiene como finalidad presentar las prácticas y las habilidades CCNA adquiridas durante el periodo calendario N°4: (16-04) del año 2019, con respecto al diplomado de profundización CISCO (Diseño e implementación de soluciones e integradas LAN/WAN). Contiene Introducción, Objetivos y la evidencia del desarrollo de dos escenarios en los cuales se pone a prueba los conocimientos que se desarrolló en el diplomado. No obstante el documento cumple con las normas ICONTEC 1486 exigidas por la universidad UNAD, debido a que el documento es de vital importancia para el grado de la carrera profesional. **Palabras Claves:** Diplomado, Escenario, red, comando y configuración.

INTRODUCCIÓN

El siguiente documento contiene el desarrollo de dos escenarios de plataforma CISCO en este caso se desarrolló en Packet Tracert (herramienta de simulación en tiempo real). En el cual se propuso situaciones complejas o sencillas de redes LAN/WAN. Es importante y cabe aclarar que se documentó los códigos o comandos con los cuales se da respuesta a las situaciones o problemas planteados. Ya que de esta forma se logra medir nuestro conocimiento y habilidad para poder aplicar soluciones a problemas de redes.

Previamente a este trabajo final se llevó a cabo 4 guía de actividades.
A lo largo del periodo 4, el desarrollo de los ejercicios se compartía en el foro colaborativo del campus virtual de la universidad donde se recibió retroalimentación por parte del tutor o incluso de nuestros compañeros. También se hizo una matriculación en la plataforma Networking o academia CISCO donde se presentaron evaluaciones frente a los temas vistos a lo largo del curso.

OBJETIVOS

- Determinar la solución a los dos escenarios planteados.
- Diseñar la topología de las redes propuestas en los escenarios.
- Elaborar el documento con las normas ICONTEC 1486.
- Cumplir con los requerimientos solicitados en los dos escenarios.

1. DESARROLLO DE LOS DOS ESCENARIOS

DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

1.1 ESCENARIO 1

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

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.

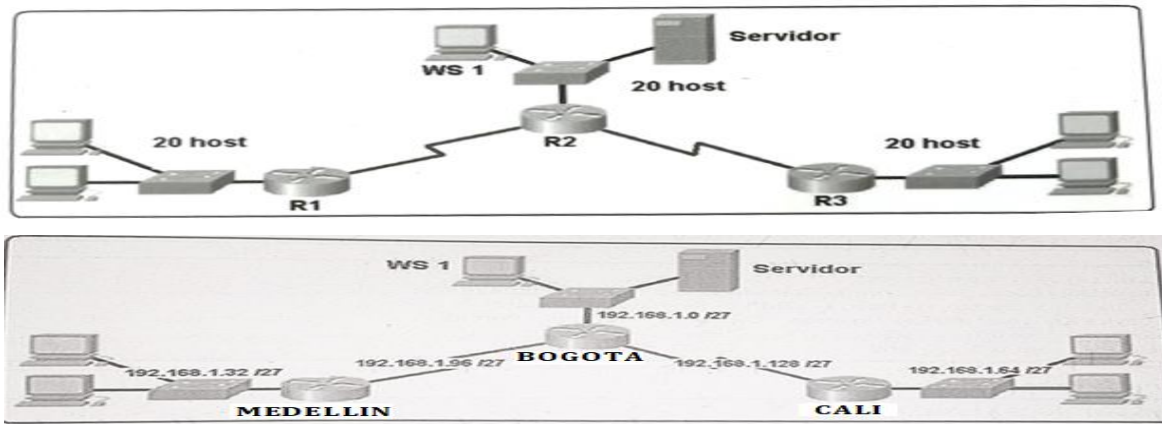
Parte 2: Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.

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.



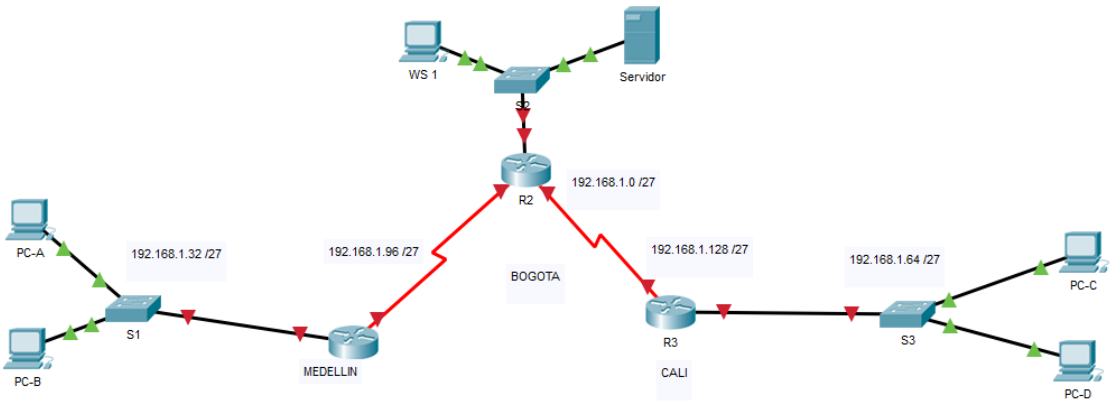
DESARROLLO

Como trabajo inicial se debe realizar lo siguiente.

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

DESCRIPCION

Como paso inicial para el desarrrolo del escenario se procede a realizar la conexión y la instalacion de todos los equipos correspodientes al escenario 1 el cual tien su conexión via fisica y el cable de color rojo. Configurar la topología de red, de acuerdo con las siguientes especificaciones.

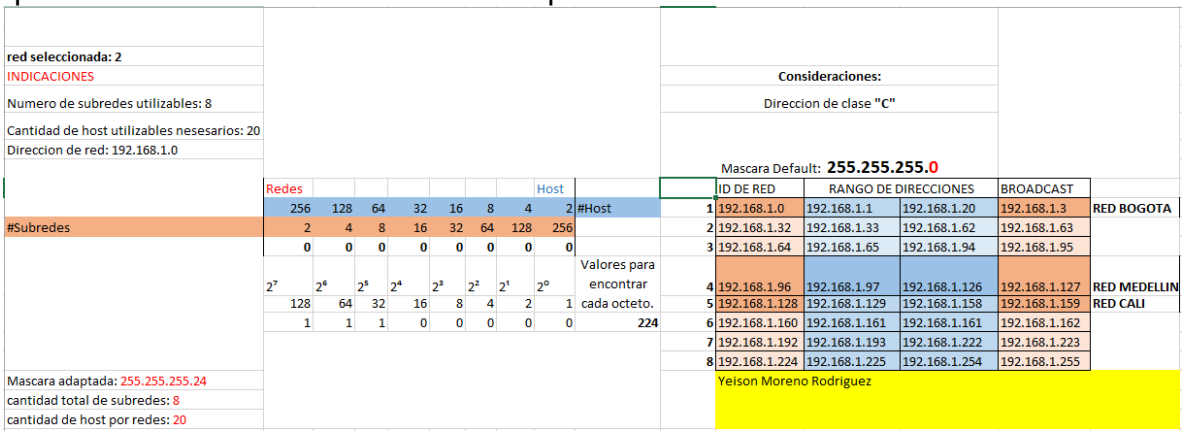


1.2.1 Parte 1: asignación de direcciones ip:

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

DESCRIPCION

Se procede a dividir la red en subredes ya que la comunicion o los paquetes de datos deben comunicarse entre redes especificas, ademas los mas importante que las redes funcionen de forma indepediente entre si.



red seleccionada: 2
INDICACIONES
Numero de subredes utilizables: 8
Cantidad de host utilizables nesesarios: 20
Direccion de red: 192.168.1.0

Consideraciones:
Direccion de clase "C"
Mascara Default: 255.255.255.0

	Redes							Host			ID DE RED	RANGO DE DIRECCIONES		BROADCAST	
	256	128	64	32	16	8	4	2	#Host	1	192.168.1.0	192.168.1.1	192.168.1.20	192.168.1.3	RED BOGOTA
#Subredes	2	4	8	16	32	64	128	256		2	192.168.1.32	192.168.1.33	192.168.1.62	192.168.1.63	
	0	0	0	0	0	0	0	0		3	192.168.1.64	192.168.1.65	192.168.1.94	192.168.1.95	
	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	Valores para encontrar	4	192.168.1.96	192.168.1.97	192.168.1.126	192.168.1.127	RED MEDELLIN
	128	64	32	16	8	4	2	1	cada octeto.	5	192.168.1.128	192.168.1.129	192.168.1.158	192.168.1.159	RED CALI
	1	1	1	0	0	0	0	0	224	6	192.168.1.160	192.168.1.161	192.168.1.161	192.168.1.162	
										7	192.168.1.192	192.168.1.193	192.168.1.222	192.168.1.223	
										8	192.168.1.224	192.168.1.225	192.168.1.254	192.168.1.255	

Mascara adaptada: 255.255.255.24
cantidad total de subredes: 8
cantidad de host por redes: 20
Yeison Moreno Rodriguez

c. Asignar una dirección IP a la red.

DESCRIPCION

Es de suma importancia asignar a cada uno de los dispostivos de las subredes o de la red asignar una ip para su identificacion dentro de la misma red, es por eso importante hacer el subneteo y que cadad dispositivo tenga su ip para cambios que al administrador desea realizar como permisos o denegar accesos.

Asignacion de una dirección IP a los Routers.

```
Router_Medellin#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router_Medellin(config)#interface gi0/0
Router_Medellin(config-if)#ip address 192.168.1.33 255.255.255.224
Router_Medellin(config-if)#interface se0/0/1
Router_Medellin(config-if)#ip address 192.168.1.97 255.255.255.224
Router_Medellin(config-if)#exit
```

```
Router_Bogota>enable
Password:
Router_Bogota#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router_Bogota(config)#interface gi0/0
Router_Bogota(config-if)#ip address 192.168.1.1 255.255.255.224
Router_Bogota(config-if)#interface se0/0/0
Router_Bogota(config-if)#ip address 192.168.1.129 255.255.255.224
Router_Bogota(config-if)#
```

```
Router_Cali>enable
Password:
Router_Cali#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router_Cali(config)#interface gi0/0
Router_Cali(config-if)#ip address 192.168.1.65 255.255.255.224
Router_Cali(config-if)#interface se0/0/0
Router_Cali(config-if)#ip address 192.168.1.130 255.255.255.224
Router_Cali(config-if)#
```

Asignacion de una dirección IP a los Switch

```
S1>enable
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int vlan 1
S1(config-if)#ip address 192.168.1.37 255.255.255.224
S1(config-if)#
```

```
S2>enable
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#int vlan 1
S2(config-if)#ip address 192.168.1.1 255.255.255.224
S2(config-if)#
```

```
S3>enable
S3#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#int vlan 1
S3(config-if)#ip address 192.168.1.70 255.255.255.224
S3(config-if)#

Asignacion de una dirección IP a la Configuración de la red MEDELLIN

PC-A
IP Address 192.168.1.35
Subnet mask 255.255.255.0
Default Gateway 192.168.1.96

PC-B
IP Address 192.168.1.36
Subnet mask 255.255.255.0
Default Gateway 192.168.1.96

Asignacion de una dirección IP a la Configuración de la red BOGOTA

WS 1
IP Address 192.168.1.2
Subnet mask 255.255.255.0
Default Gateway 192.168.1.0

SERVIDOR
IP Address 192.168.1.3
Subnet mask 255.255.255.0
Default Gateway 192.168.1.0

Asignacion de una dirección IP a la Configuración de la red CALI

PC-C
IP Address 192.168.1.68
Subnet mask 255.255.255.0
Default Gateway 192.168.1.128

PC-D
IP Address 192.168.1.67
Subnet mask 255.255.255.0
Default Gateway 192.168.1.128

1.2.1.1 Parte 2: configuración básica.

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

DESCRIPCION

Para completar la configuracion de los routers Medelin y Cali se utilizo las siguientes direciones IP

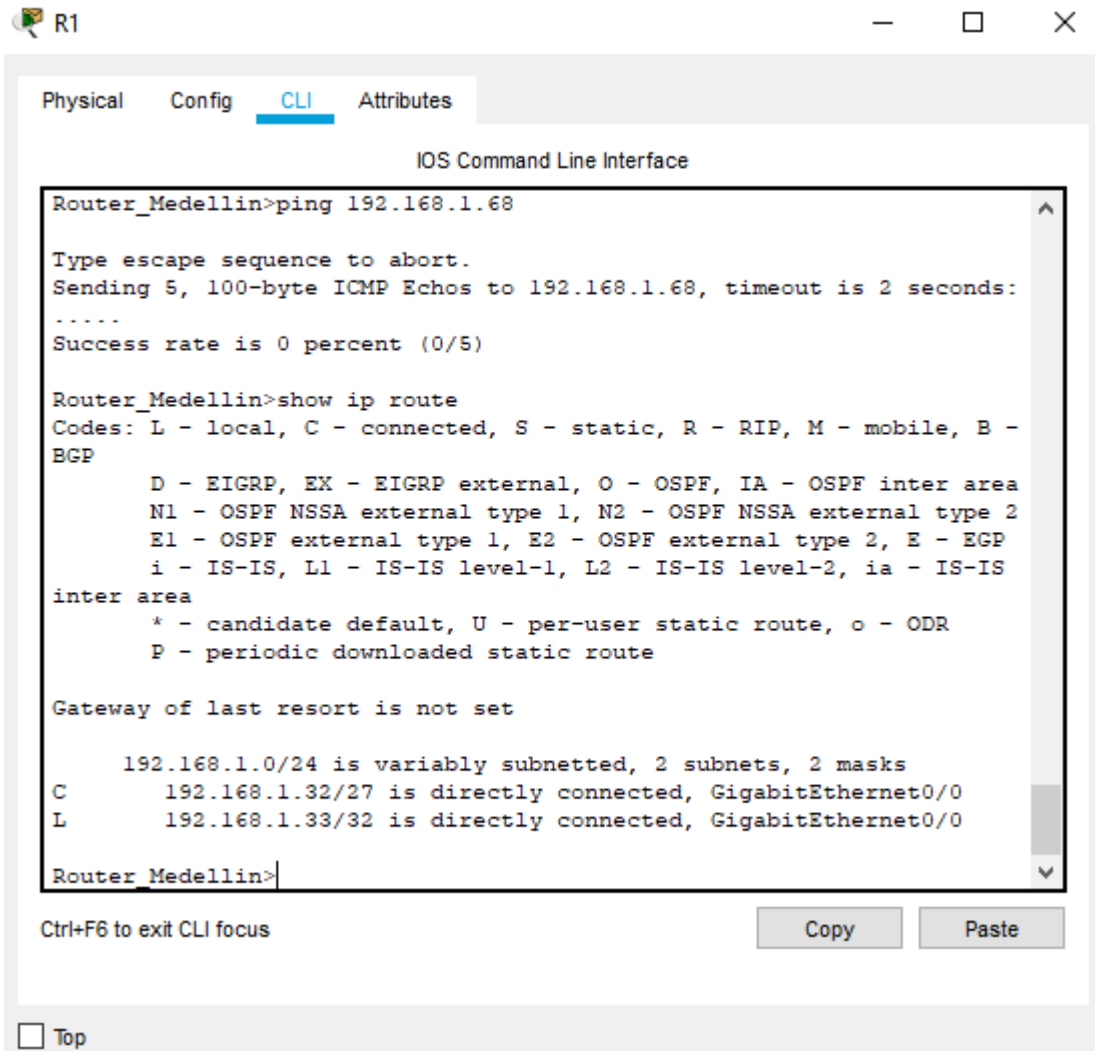
192.168.1.97 MEDELLIN
192.168.1.65 CALI

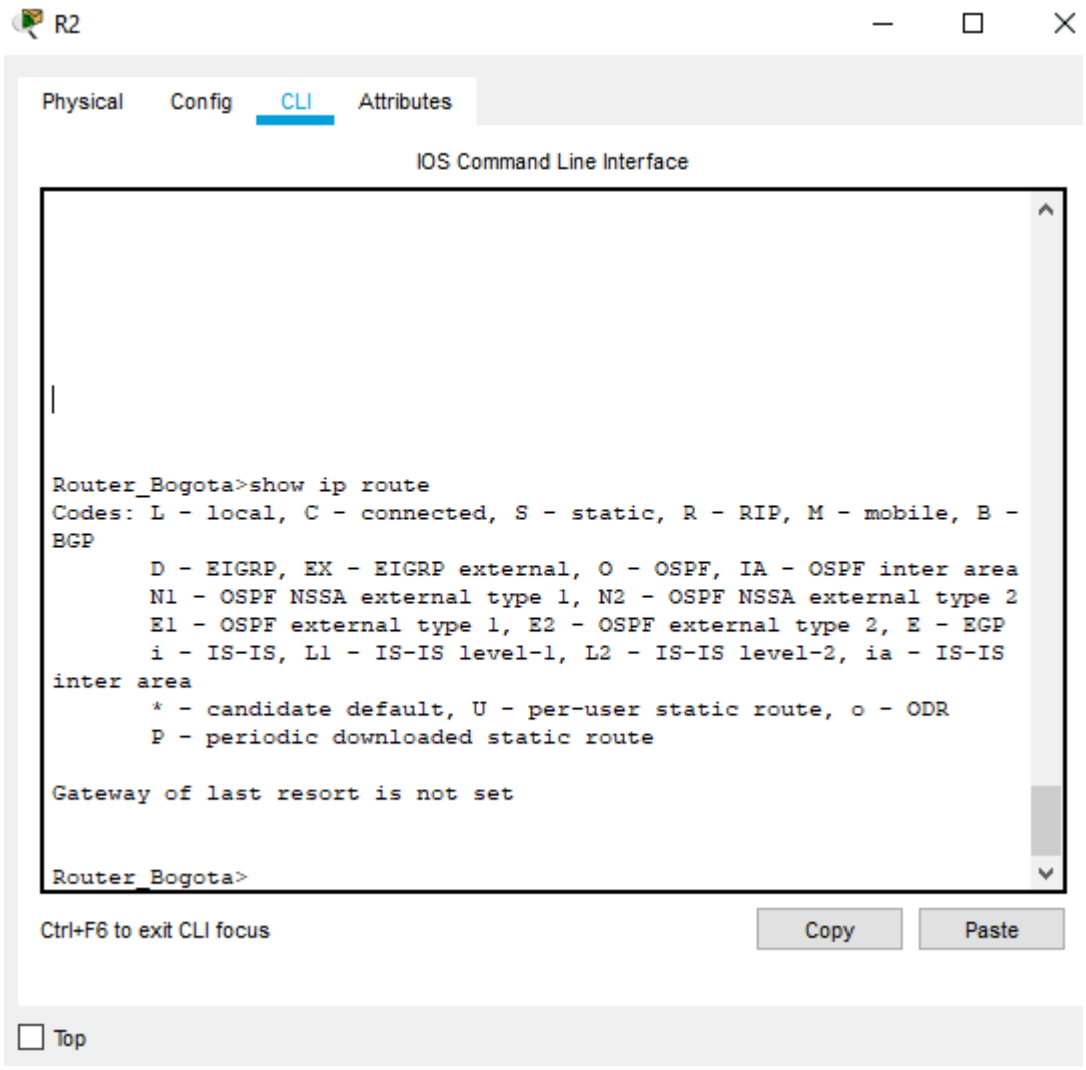
	R1	R2	R3
Nombre de Host	**MEDELLIN**	**BOGOTA**	**CALI**
Dirección de Ip en interfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/1	192.168.1.97	192.168.1.130	192.168.1.65
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	**Eigrp**	**Eigrp**	**Eigrp**
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

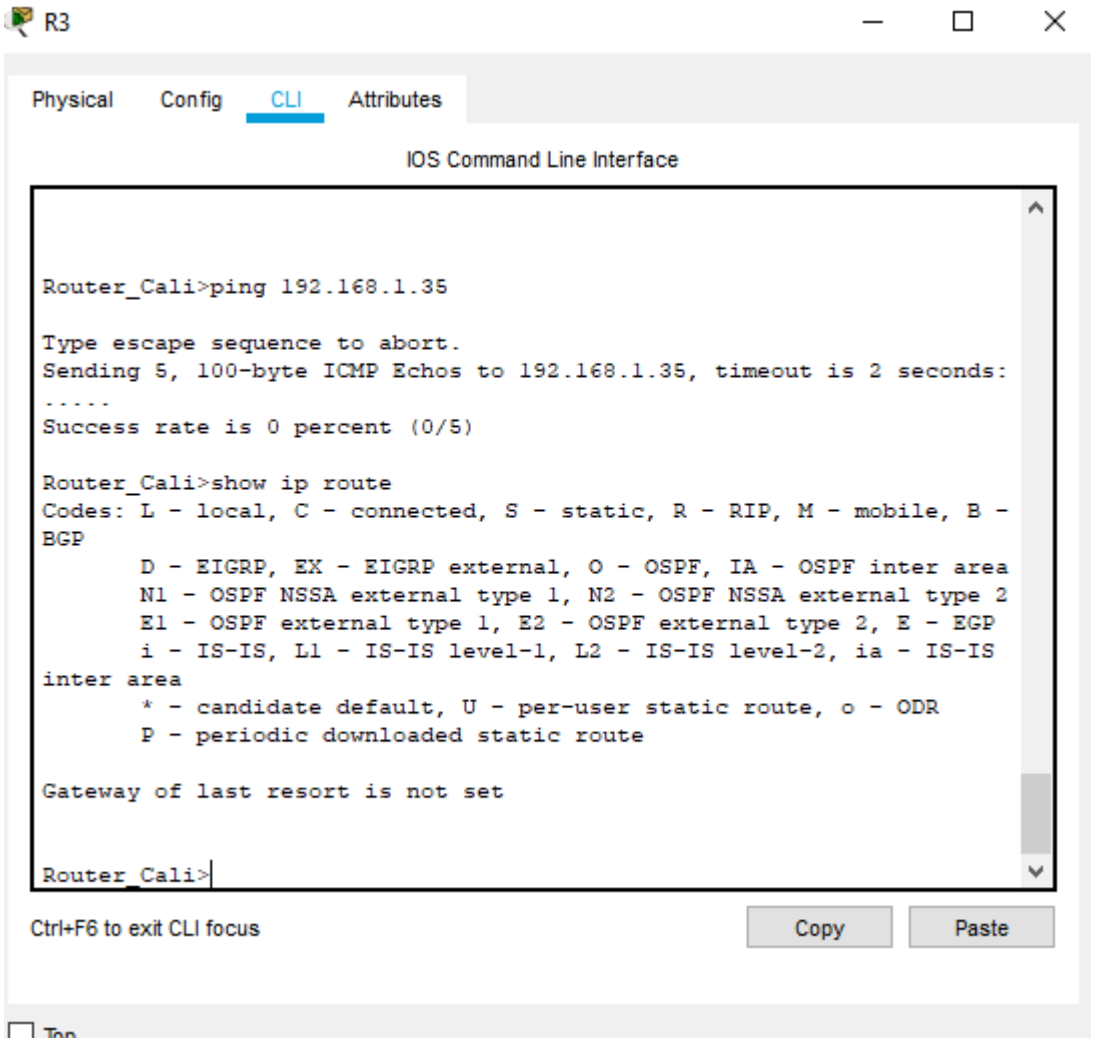
b. Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

DESCRIPCIÓN

Nos permite consulta los archivos de datos que se encuentra en la RAM y se usa para almacenar la información de la ruta sobre redes remotas y conectadas directamente.


R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router_Medellin>ping 192.168.1.68
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.68, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Router_Medellin>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.32/27 is directly connected, GigabitEthernet0/0
L 192.168.1.33/32 is directly connected, GigabitEthernet0/0
Router_Medellin>
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

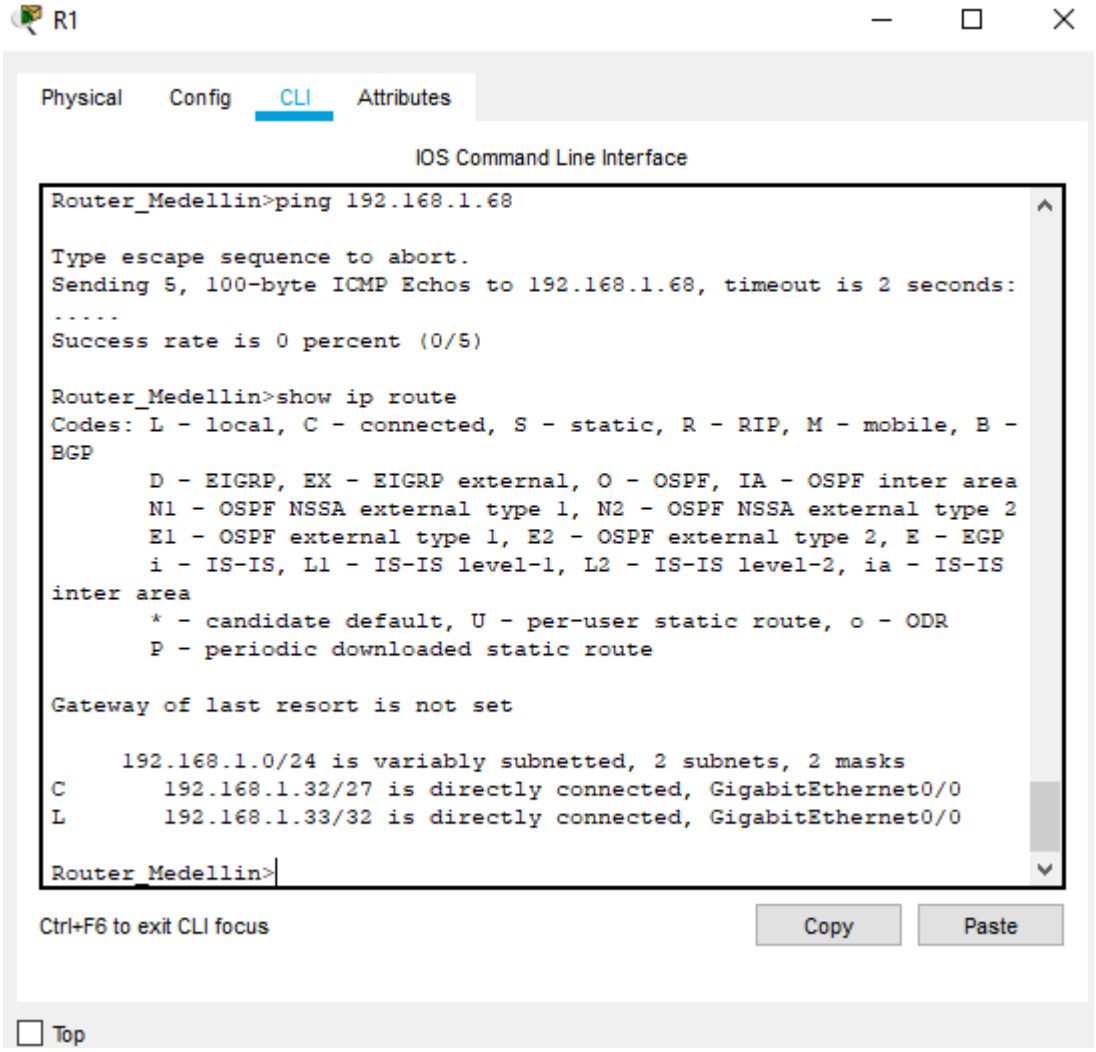

R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router_Bogota>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
Router_Bogota>
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

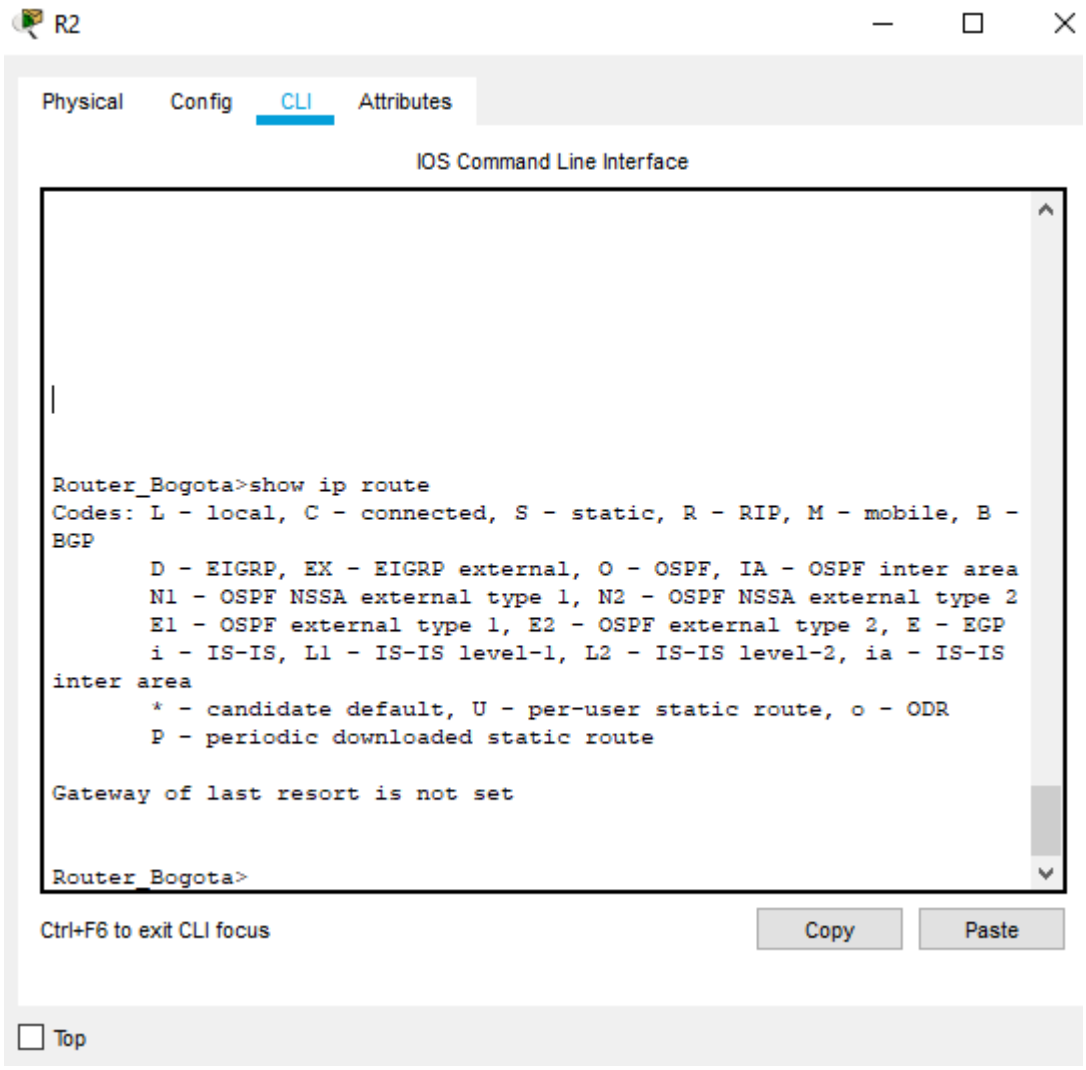

R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router_Cali>ping 192.168.1.35
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.35, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Router_Cali>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
Router_Cali>
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

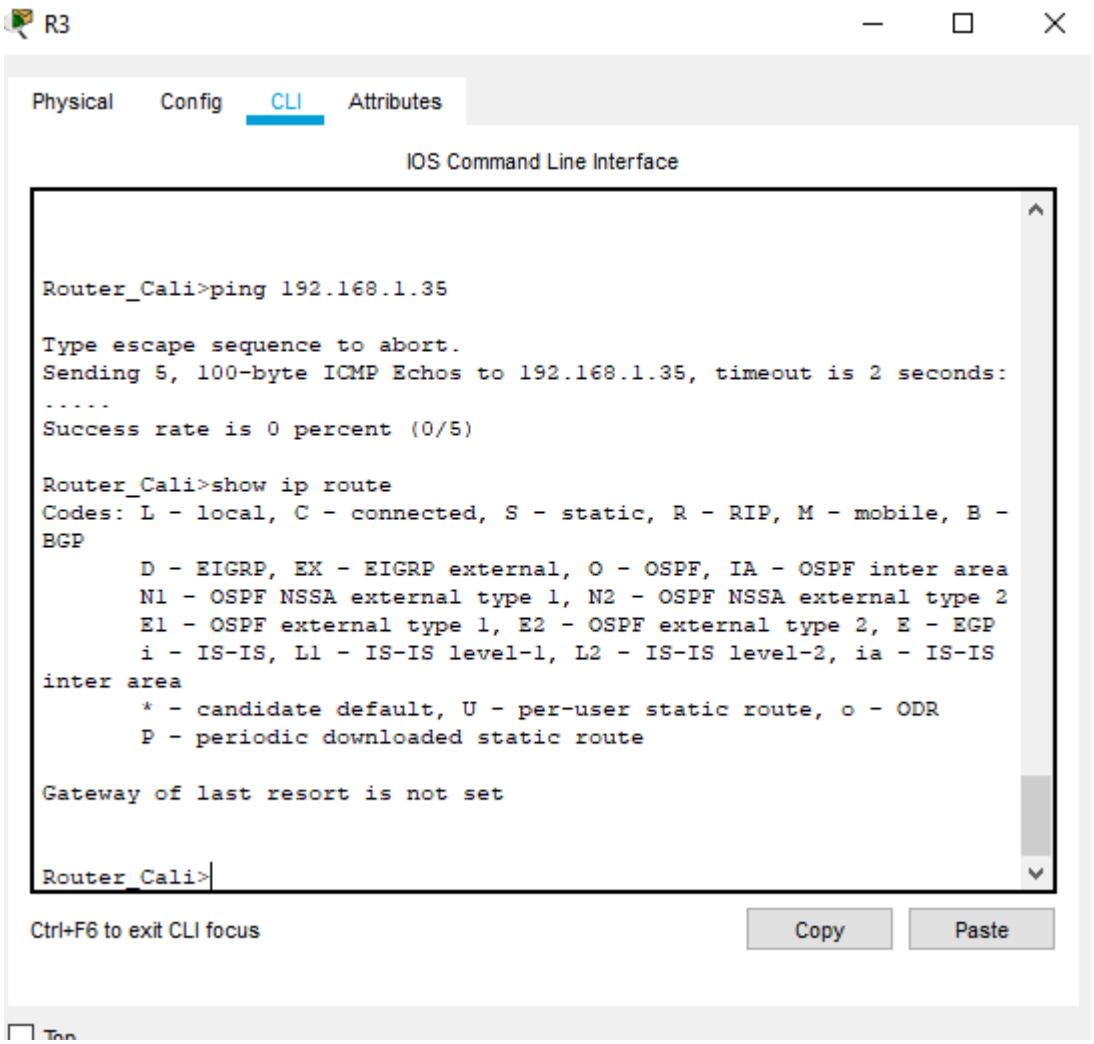
c. Verificar el balanceo de carga que presentan los routers.

DESCRIPCION

Mediante el comando **show ip route** (utilizado en el anterior punto). Con el cual conocemos la asignacion o balanceo de la carga de las solicitudes que llegan de los clientes o dispositivos. Se procede a tomar la evidencia de como el balanceo de cargas de cada router.




R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router_Bogota>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
Router_Bogota>
Ctrl+F6 to exit CLI focus
Copy
Paste
Top



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

DESCRIPCION

Para poder realizar el diagnostico de los vecinos conectado o sea los switches de cada red se debe activar el cdp con el comando **Cdp Run,** despues se ejecuta el comando **sho cdp neighbors** para conocer los vecinos conectados en este caso los switches o en su defecto los routers.

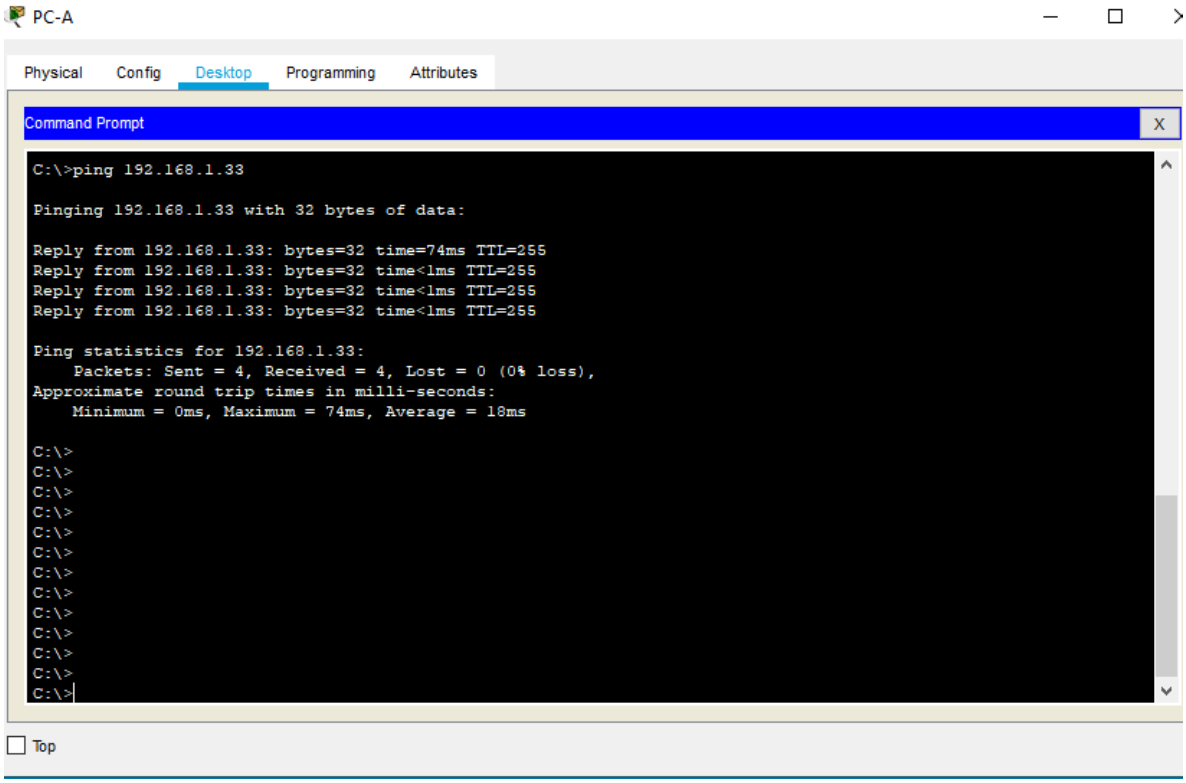
Router_Medellin>enable
Router_Medellin#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router_Medellin(config)#Cdp run
Router_Medellin(config)#exit
Router_Medellin#
%SYS-5-CONFIG_I: Configured from console by console

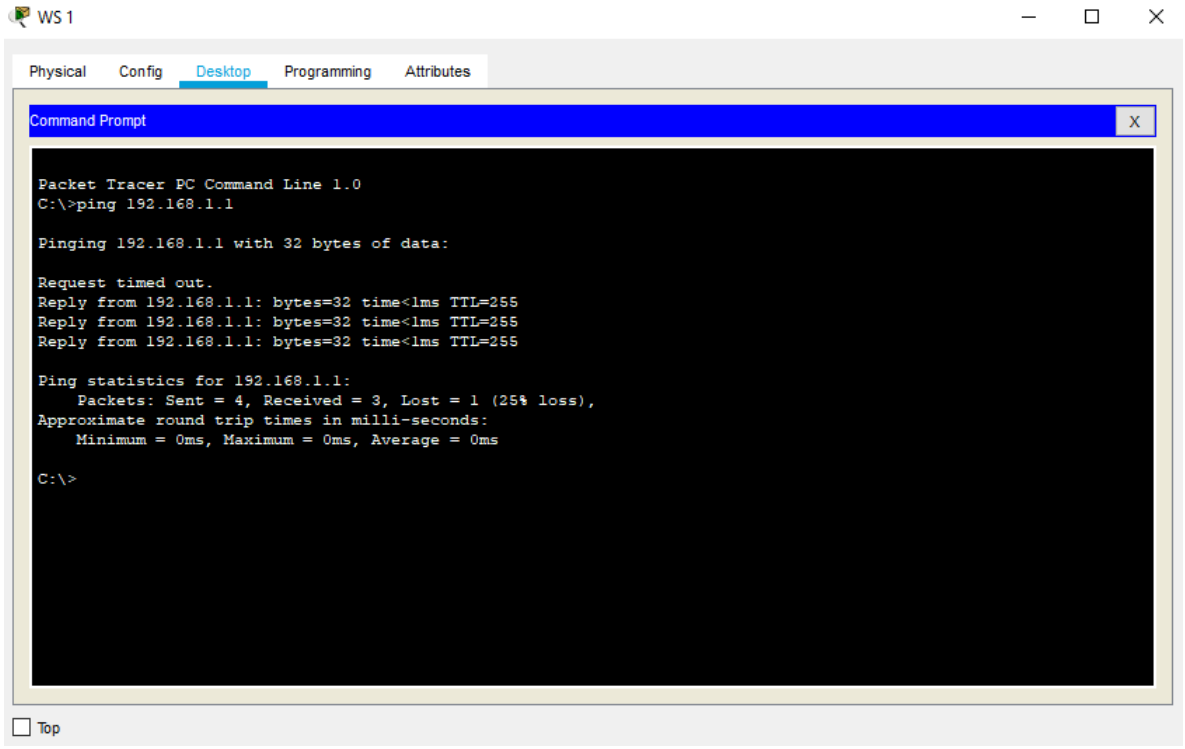
```
Router_Medellin#sho cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
Router_Medellin#

Router_Bogota>enable
Router_Bogota#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router_Bogota(config)#Cdp run
Router_Bogota(config)#exit
Router_Bogota#
%SYS-5-CONFIG_I: Configured from console by console

Router_Bogota#sho cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
Router_Bogota#

Router_Cali>enable
Router_Cali#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router_Cali(config)#Cdp run
Router_Cali(config)#exit
Router_Cali#
%SYS-5-CONFIG_I: Configured from console by console

Router_Cali#sho cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID Local Intrfce Holdtme Capability Platform Port ID
Router_Cali#.
```

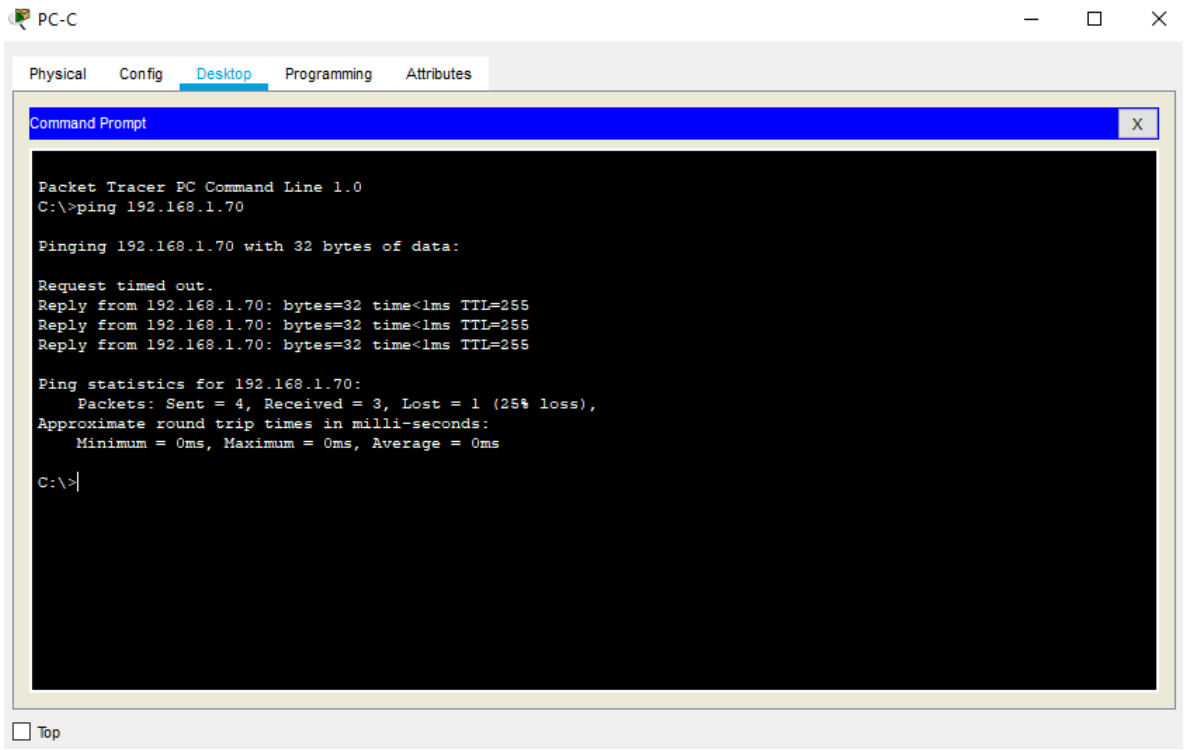
Realizar una prueba de conectividad en cada tramo de la ruta usando Ping

DESCRIPCION

En este paso se tomo cada PC de cada una de las redes y se realiza el respectivo ping a las direcciones ip asignadas a los routes respondiendo el ping, demostrandose asi la conexión entre los dos equipos.




WS 1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top


PC-C
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.70
Pinging 192.168.1.70 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.70: bytes=32 time<1ms TTL=255
Reply from 192.168.1.70: bytes=32 time<1ms TTL=255
Reply from 192.168.1.70: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.1.70:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top

- **Parte 3: configuración de enrutamiento**

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

DESCRIPCIÓN

El comando que utilizamos en este paso fue **router eigrp 1** en el cual se hace recuperación y detección de vecinos y hace un protocolo de transporte confiable.

```
Router_Medellin>enable
Router_Medellin#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router_Medellin(config)#router eigrp 1
Router_Medellin(config-router)#passive-interface gi0/0
Router_Medellin(config-router)#
```

```
Router_Bogota>enable
Router_Bogota#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router_Bogota(config)#router eigrp 1
Router_Bogota(config-router)#passive-interface gi0/0
Router_Bogota(config-router)#
```

```
Router_Cali>enable
Router_Cali#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router_Cali(config)#router eigrp 1
Router_Cali(config-router)#passive-interface gi0/0
Router_Cali(config-router)#
```

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

DESCRIPCIÓN

En este punto se realizó la ejecución del comando **sho ip eigrp topology** donde no se evidencia ningún vecino conectado con la configuración EIGRP.

```
Router_Medellin#sho ip eigrp topology
IP-EIGRP Topology Table for AS 1/ID(0.0.0.0)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status
```

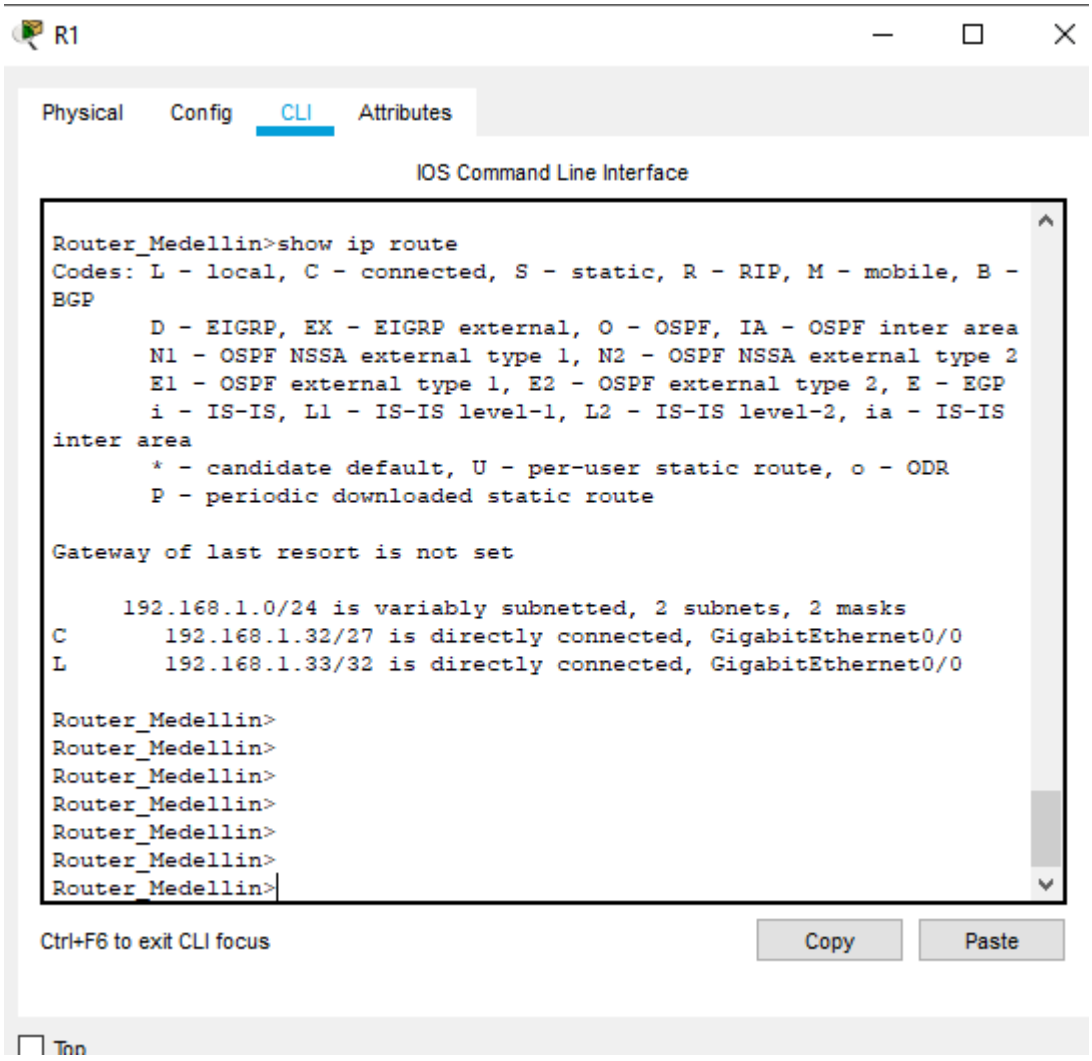
Router_Bogota#sho ip eigrp topology
IP-EIGRP Topology Table for AS 1/ID(192.168.1.129)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status

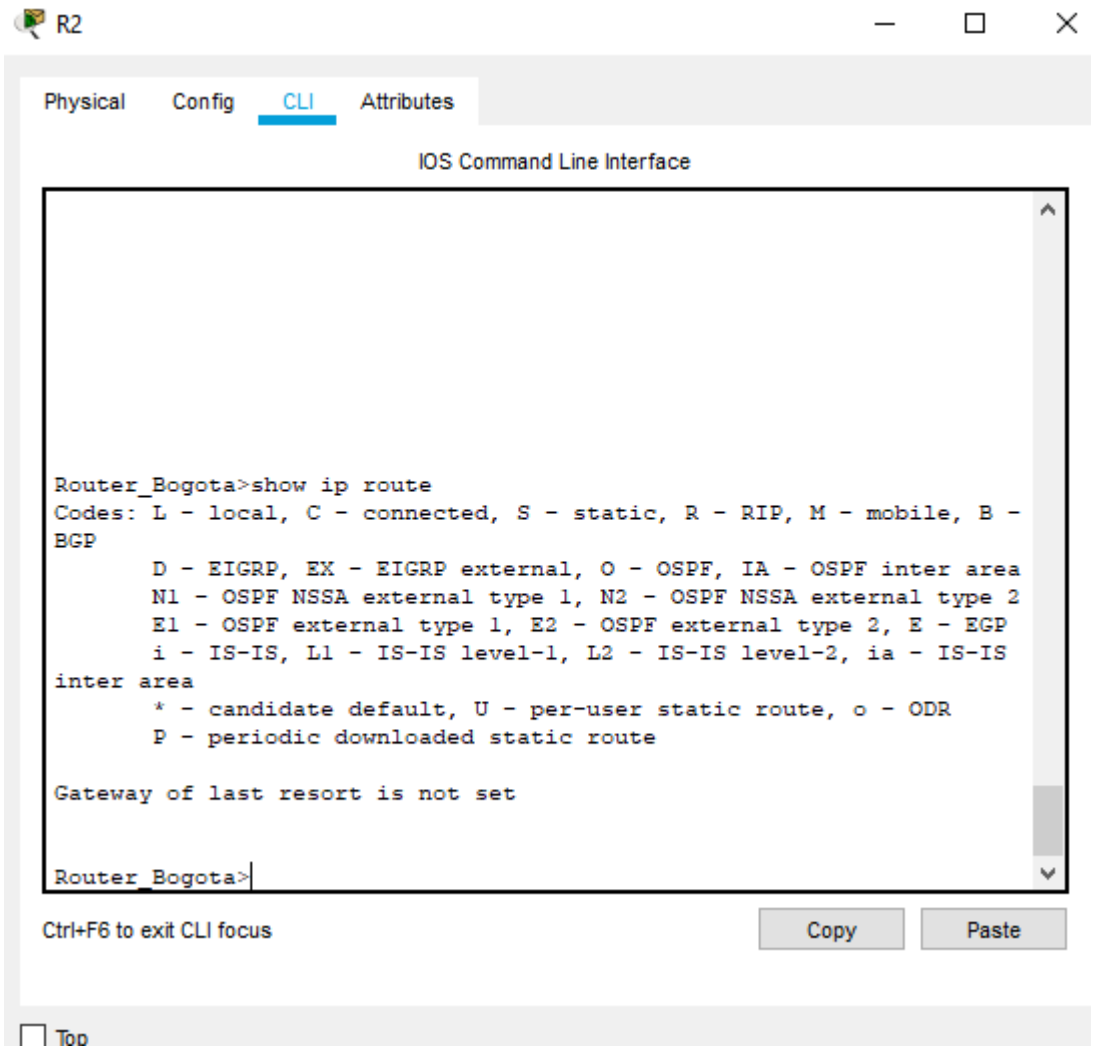
Router_Cali#sho ip eigrp topology
IP-EIGRP Topology Table for AS 1/ID(0.0.0.0)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status

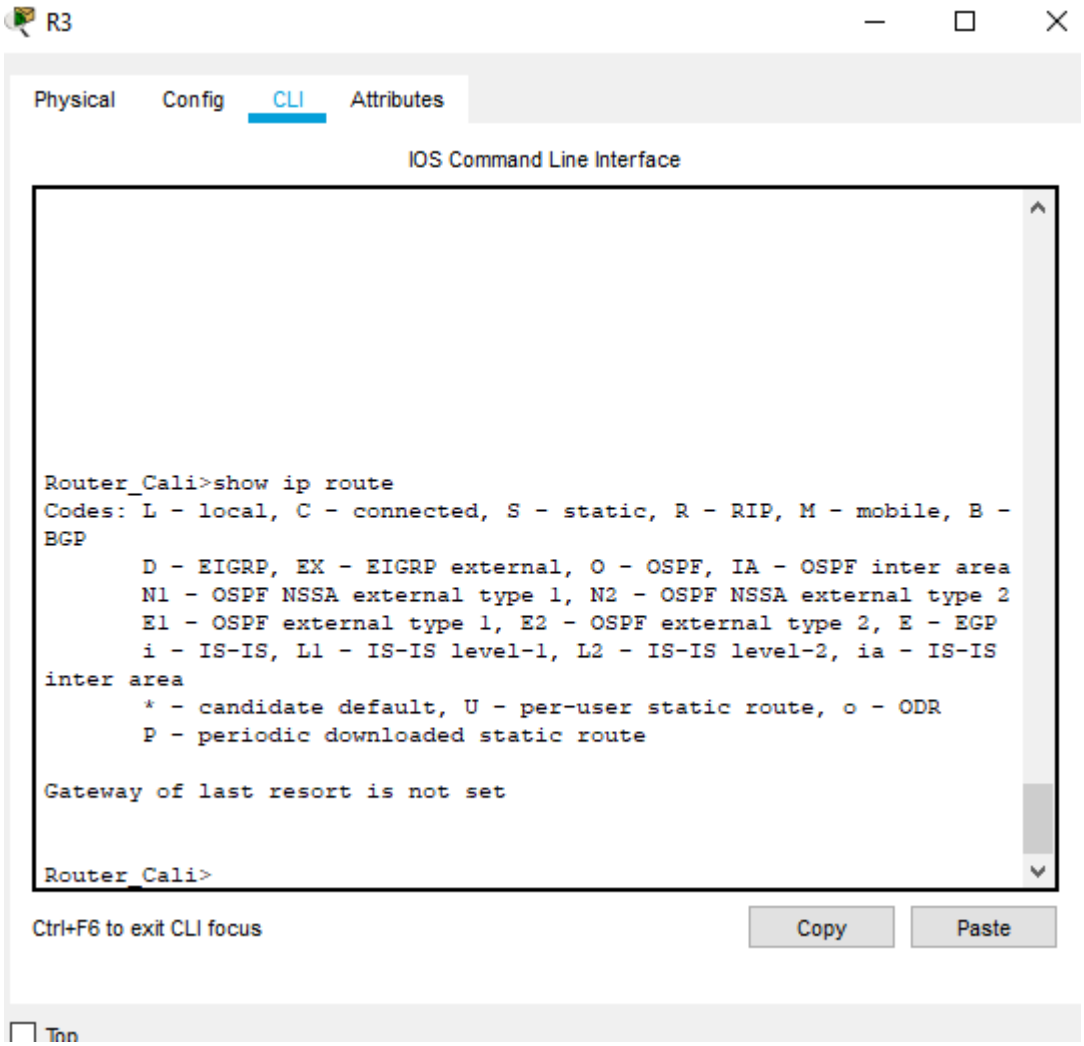
c. Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas.

DESCRIPCIÓN

En este punto utilizamos el comando **show ip route** donde comprobamos cada una de las rutas establecidas en el router de cada red.



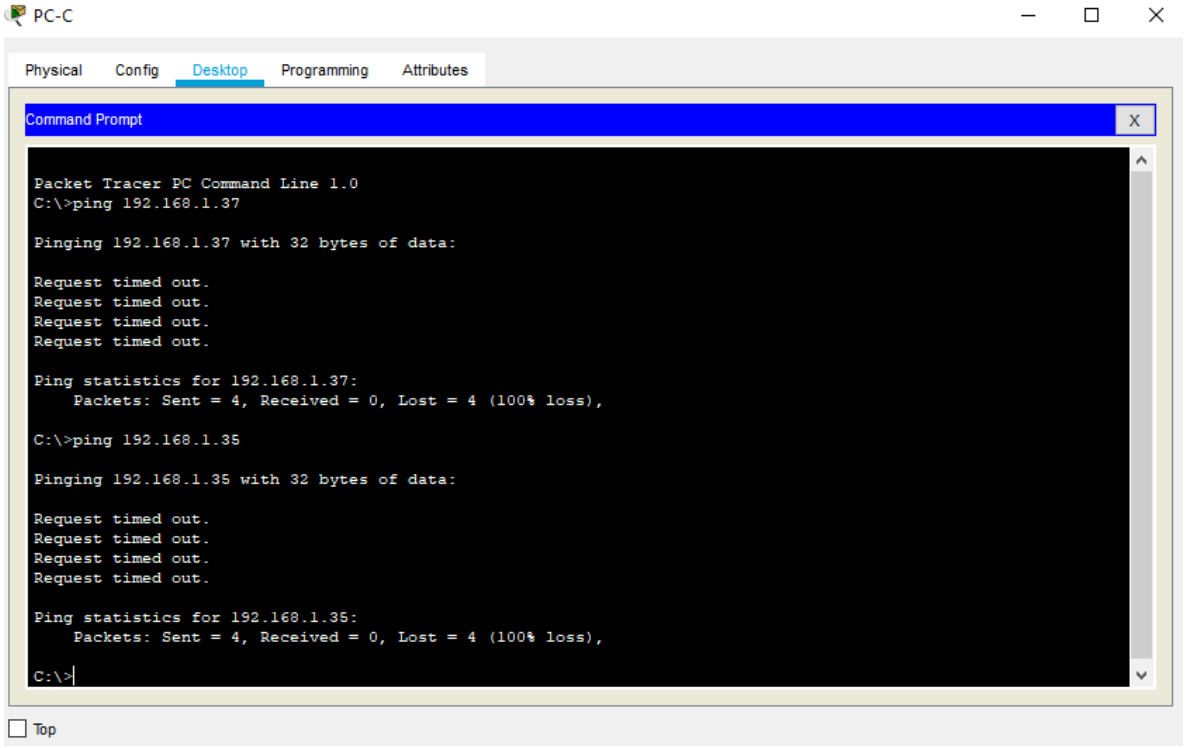

R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router_Bogota>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
Router_Bogota>
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

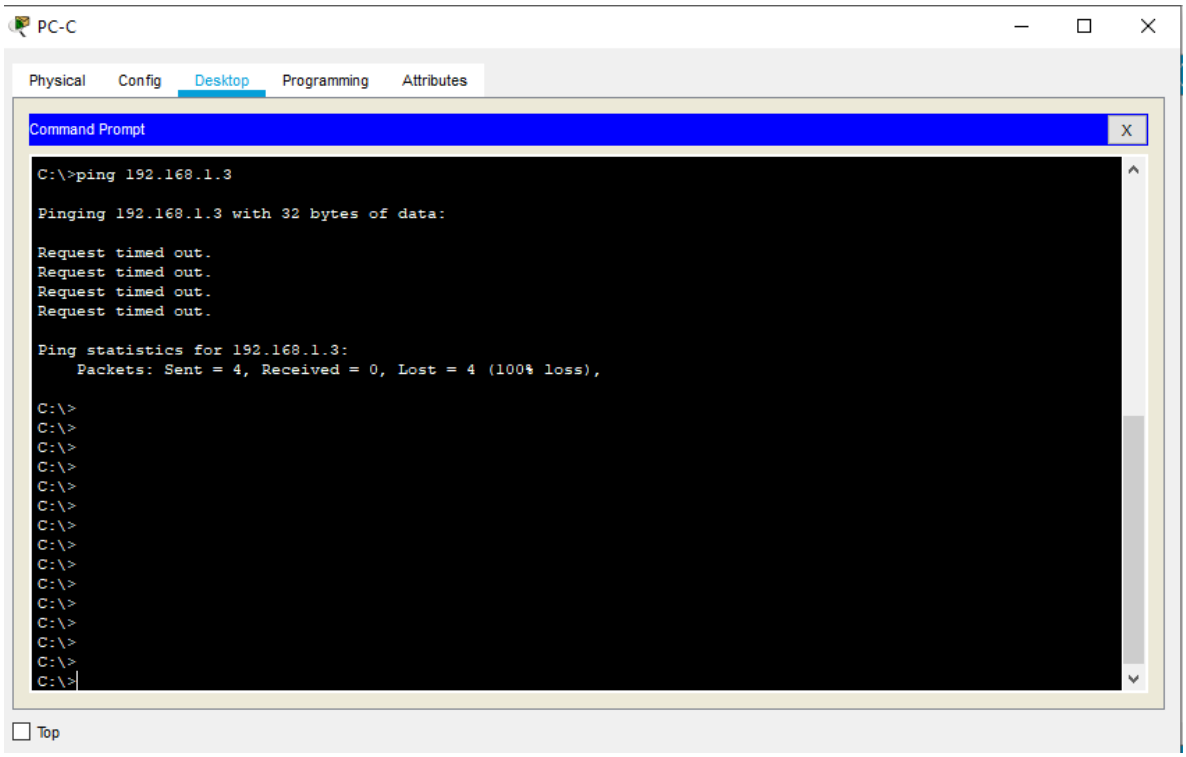


d. Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí. Realizar esta prueba desde un host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor.

DESCRIPCIÓN

En este punto tomamos la LAN de Cali **PC-C** donde los puntos no dio conexión entre si entonces fue fallida.




PC-C
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
C:\>ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
Top

- **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.

DESCRIPCIÓN

En este punto establecimos la conexión telnet del router a los demás router, teniendo como seguridad dos contraseñas.

```
Router_Medellin>enable
Router_Medellin#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router_Medellin(config)#enable secret cisco123
Router_Medellin(config)#line vty 0 4
Router_Medellin(config-line)#password cisco
Router_Medellin(config-line)#login
Router_Medellin(config-line)#exit
Router_Medellin(config)#
```

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

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

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.

DESCRIPCIÓN

Se procede a dar permiso al servidor de la red con el comando **access-list 10 permit 192.168.1.3 0.0.0.0** para que tenga acceso a cualquier dispositivo y en cualquier parte de la red.

Router_Bogota(config)#access-list 10 permit 192.168.1.3 0.0.0.0
Router_Bogota(config)#

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.

DESCRIPCIÓN

Se procede a denegar el acceso a lan MEDELLIN y CALI los dispositivos de las otras redes y solo se da permiso para conectar al servidor al que previamente le dimos acceso en el punto anterior.

Router_Medellin>enable
Password:
Router_Medellin#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router_Medellin(config)#access-list 10 permit 192.168.1.3 0.0.0.0
Router_Medellin(config)#access-list 10 permit 192.168.1.3 0.0.0.0
Router_Medellin(config)#access-list 1 deny 192.168.1.36 0.0.0.255
Router_Medellin(config)#access-list 1 deny 192.168.1.35 0.0.0.255
Router_Medellin(config)#
Router_Medellin(config)#

Router_Cali>enable
Password:
Router_Cali#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router_Cali(config)#access-list 10 permit 192.168.1.3 0.0.0.0
Router_Cali(config)#access-list 10 permit 192.168.1.3 0.0.0.0
Router_Cali(config)#access-list 1 deny 192.168.1.67 0.0.0.255
Router_Cali(config)#access-list 1 deny 192.168.1.68 0.0.0.255
Router_Cali(config)#

❖ **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 e.

DESCRIPCIÓN

En este punto se pide ejecutar dos comandos de suma importancia **ping y telnet** donde el resultado está documentado como **fallido o exitoso.** Donde comprobamos la conexión de los dispositivos entre si.

	ORIGEN	DESTINO	RESULTADO
TELNET	**Router MEDELLIN**	**Router CALI**	Router_Medellin#telnet 192.168.1.65 Trying 192.168.1.65 ... % Connection timed out; remote host not responding Router_Medellin# Denegado
	WS_1	**Router BOGOTA**	C:\>telnet 192.168.1.0 Trying 192.168.1.0 ... % Connection timed out; remote host not responding C:\> denegado
	Servidor	**Router CALI**	Packet Tracer SERVER Command Line 1.0 C:\>telnet 192.168.1.65 Trying 192.168.1.65 ... % Connection timed out; remote host not responding

			C:\> denegado
	Servidor	**Router MEDELLIN**	C:\>telnet 192.168.1.33 Trying 192.168.1.33 ... % Connection timed out; remote host not responding C:\> Denegado
TELNET	**LAN del Router MEDELLIN**	**Router CALI**	Packet Tracer SERVER Command Line 1.0 C:\>telnet 192.168.1.65 Trying 192.168.1.65 ... % Connection timed out; remote host not responding Denegado
	LAN del Router CALI	**Router CALI**	Packet Tracer PC Command Line 1.0 C:\>telnet 192.168.1.65 Trying 192.168.1.65 ... % Connection timed out; remote host not responding C:\> Denegado
	LAN del Router MEDELLIN	**Router MEDELLIN**	Packet Tracer PC Command Line 1.0 C:\>telnet 192.168.1.33 Trying 192.168.1.33 ...Open User Access Verification

			Password: exitoso
	LAN del Router CALI	**Router MEDELLIN**	Packet Tracer PC Command Line 1.0 C:\>telnet 192.168.1.33 Trying 192.168.1.33 ... % Connection timed out; remote host not responding C:\> Exitoso
PING	**LAN del Router CALI**	**WS_1**	C:\>ping 192.168.1.2 Pinging 192.168.1.2 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 192.168.1.2: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\> fallido
	LAN del Router MEDELLIN	**WS_1**	C:\>ping 192.168.1.2 Pinging 192.168.1.2 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 192.168.1.2: Packets: Sent = 4,

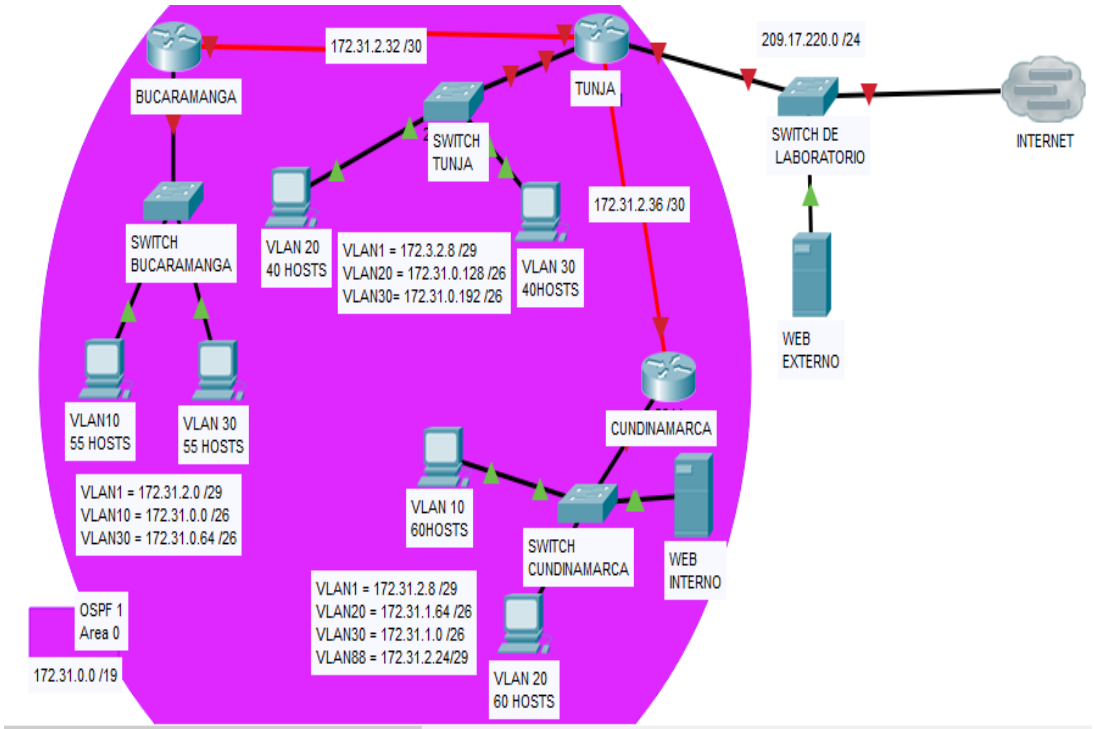
			Received = 0, Lost = 4 (100% loss), C:\> Fallido
	LAN del Router MEDELLIN	**LAN del Router CALI**	C:\>ping 192.168.1.68 Pinging 192.168.1.68 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 192.168.1.68: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), Fallida
PING	**LAN del Router CALI**	**Servidor**	C:\>ping 192.168.1.3 Pinging 192.168.1.3 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 192.168.1.3: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), fallida
	LAN del Router MEDELLIN	**Servidor**	C:\>ping 192.168.1.3 Pinging 192.168.1.3 with 32 bytes of data: Request timed out.

			Request timed out. Request timed out. Request timed out. Ping statistics for 192.168.1.3: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\> Fallida
	Servidor	**LAN del Router MEDELLIN**	C:\>ping 192.168.1.35 Pinging 192.168.1.35 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 192.168.1.35: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss), C:\> Fallida
	Servidor	**LAN del Router CALI**	C:\>ping 192.168.1.68 Pinging 192.168.1.68 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 192.168.1.68: Packets: Sent = 4, Received = 0, Lost = 4

			(100% loss), Fallida
	Router CALI	**LAN del Router MEDELLIN**	Router_Cali>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 0 percent (0/5) Router_Cali> Fallida
	Router MEDELLIN	**LAN del Router CALI**	Router_Medellin>ping 192.168.1.68 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.1.68, timeout is 2 seconds: ..... Success rate is 0 percent (0/5) Router_Medellin> Fallida

2. ESCENARIO 2

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



2.1 DESARROLLO

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:

    - Configuración básica.

DESCRIPCIÓN

En las configuraciones basicas de los router de la red fueron las siguientes se establecio el nombre según el router que se estaba configurando como: **Bucaramanga, Tunja** y **Cundinamarca**. Se establecio la contraseña **cisco** con su debido **login**. Ademas se establecio las direcciones IP de las interfaces y seriales respectivamente de cada uno de los routers.

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

BUCARAMANGA>enable
Password:
BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#interface gigabitEthernet 0/0
BUCARAMANGA(config-if)#no sh

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)#ip address 172.31.0.137 255.255.255.128
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#interface serial 0/0/1
BUCARAMANGA(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
BUCARAMANGA(config-if)#ip address 172.31.2.33 255.255.255.128
```

```
BUCARAMANGA(config-if)#


Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname TUNJA
TUNJA(config)#enable secret cisco
TUNJA(config)#line vty 0 4
TUNJA(config-line)#password cisco
TUNJA(config-line)#login
TUNJA(config-line)#

TUNJA>enable
Password:
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#interface gigabitEthernet 0/0
TUNJA(config-if)#no sh

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)#ip address 209.17.220.1 255.255.255.128
TUNJA(config-if)#exit
TUNJA(config)#interface serial 0/0/0
TUNJA(config-if)#ip address 172.31.2.33 255.255.255.128
TUNJA(config-if)#

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CUNDINAMARCA
CUNDINAMARCA(config)#enable secret cisco
CUNDINAMARCA(config)#line vty 0 4
CUNDINAMARCA(config-line)#password cisco
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#

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

Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#interface gigabitEthernet 0/0
CUNDINAMARCA(config-if)#no sh

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)#ip address 172.31.0.161 255.255.255.128
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#interface serial 0/0/0
CUNDINAMARCA(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
CUNDINAMARCA(config-if)#ip address 172.31.2.34 255.255.255.128
CUNDINAMARCA(config-if)#

- Autenticación local con AAA.

DESCRIPCIÓN

En esta parte se configuro la autenticación local con AAA se estableció el username **Admin** la contraseña **cisco** con su respectivo **login**.

BUCARAMANGA>enable
Password:
BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#username Admin secret cisco
BUCARAMANGA(config)#aaa n
BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#aaa authentication login default local
BUCARAMANGA(config)#

TUNJA>enable
Password:

```
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#username Admin secret cisco
TUNJA(config)#aaa n
TUNJA(config)#aaa new-model
TUNJA(config)#aaa authentication login default local
TUNJA(config)#

CUNDINAMARCA>enable
Password:
CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#username Admin secret cisco
CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#aaa authentication login default local
CUNDINAMARCA(config)#
```

- Cifrado de contraseñas.

DESCRIPCIÓN

En este punto se cifra la contraseña de cada uno de los routers, la contraseña la deje como **cisco** como método de seguridad para la red.

```
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#password cisco

TUNJA(config)#line console 0
TUNJA(config-line)#password cisco
TUNJA(config-line)#

CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#password cisco
CUNDINAMARCA(config-line)#
```

- Un máximo de intentos para acceder al router.

DESCRIPCIÓN

En este punto deje el número de 5 intentos para acceder a los routers, para contrarrestar los ataques a la red.

```
BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#ip ssh authentication-retries 5
BUCARAMANGA(config)#

TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#ip ssh authentication-retries 5
TUNJA(config)#

CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#ip ssh authentication-retries 5
CUNDINAMARCA(config)#
```

- Máximo tiempo de acceso al detectar ataques.

DESCRIPCIÓN

Se estableció un tiempo de 180 segundos para realizar un bloqueo al detectar ataques externas a nuestra red.

```
BUCARAMANGA(config)#login block-for 180 attempts 5 within 180
TUNJA(config)#login block-for 180 attempts 5 within 180
CUNDINAMARCA(config)#login block-for 180 attempts 5 within 180
```

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

DESCRIPCIÓN

Se configuro el servidor TFTP o sea el servidor web interno con la dirección IP **172.31.2.35** donde se crea una copia de seguridad de los archivos de los routers.

```
BUCARAMANGA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
BUCARAMANGA#copy run tftp ?
<cr>
```

BUCARAMANGA#copy run tftp
Address or name of remote host []? 172.31.2.35
Destination filename [BUCARAMANGA-confg]?
Writing running-config.....

TUNJA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
TUNJA#copy run tftp ?
<cr>
TUNJA#copy run tftp
Address or name of remote host []? 172.31.2.35
Destination filename [TUNJA-confg]? Backup
Writing running-config.....

CUNDINAMARCA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CUNDINAMARCA#copy run tftp ?
<cr>
CUNDINAMARCA#copy run tftp
Address or name of remote host []? 172.31.2.35
Destination filename [CUNDINAMARCA-confg]?

Writing running-config.....

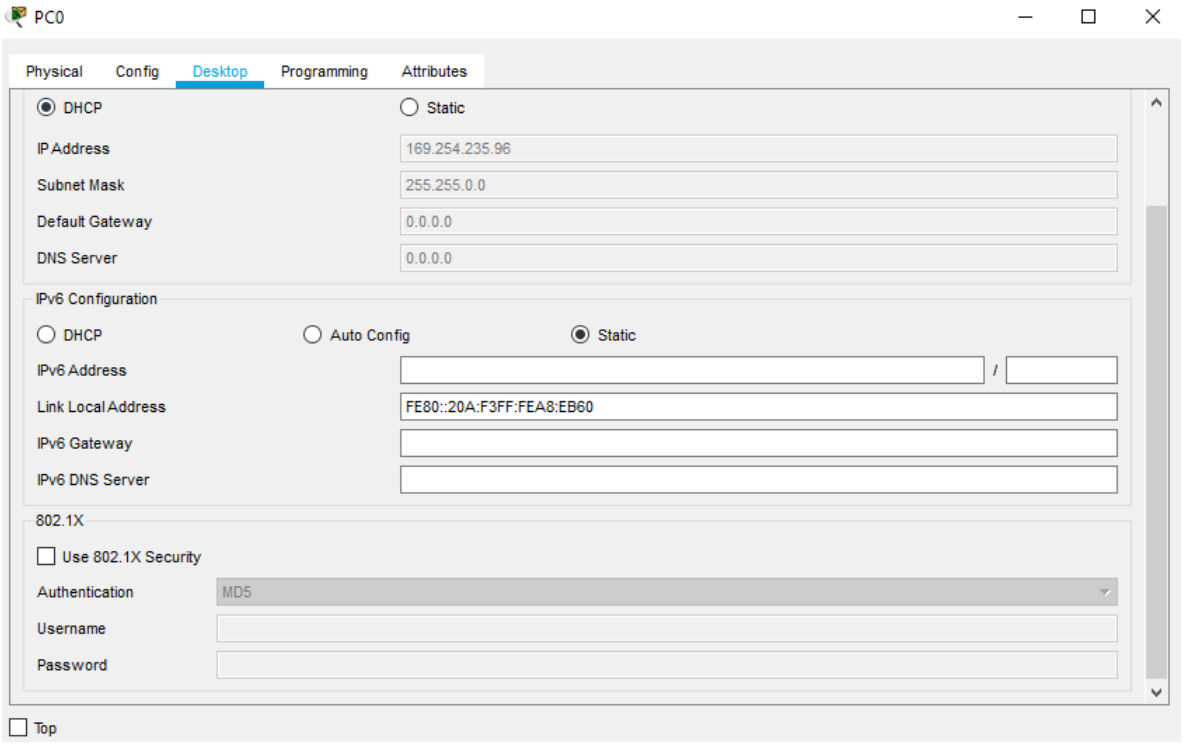
2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca.

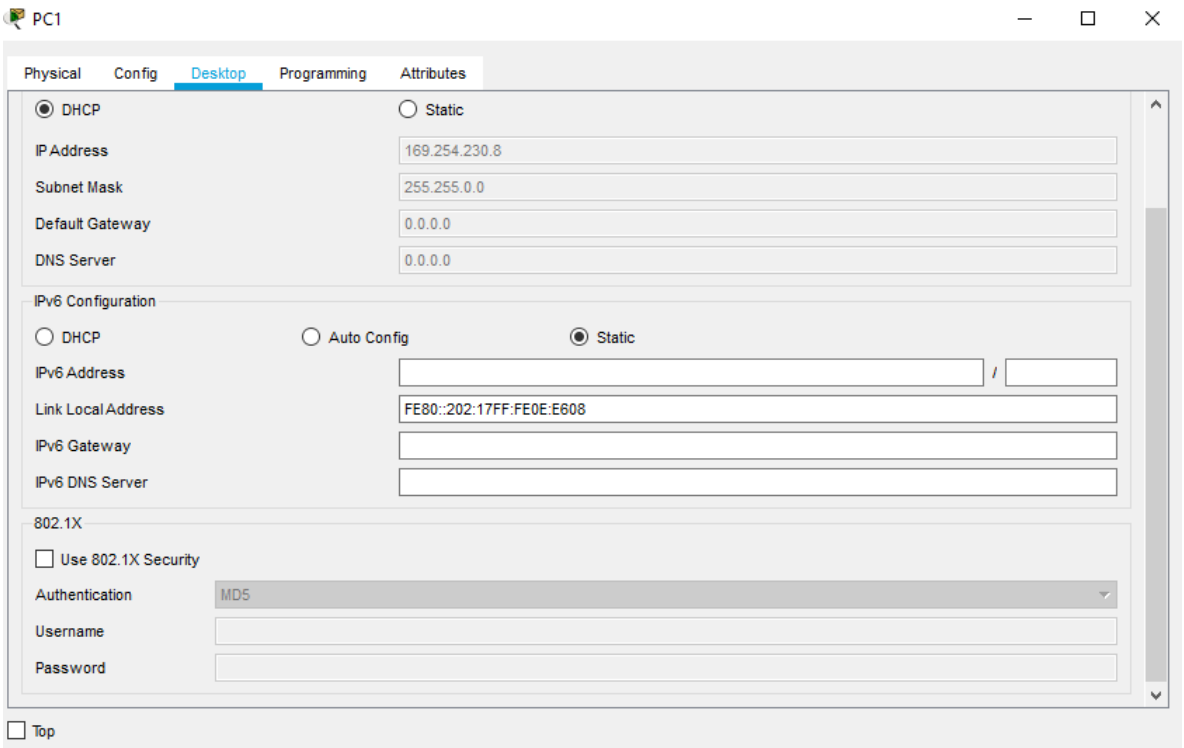
DESCRIPCIÓN

El DHCP nos permite configurar de forma automática la dirección ip y mascara de subred, se aplicó a los host de Bucaramanga y Cundinamarca. Se realizó con el comando **helper-address**.

BUCARAMANGA

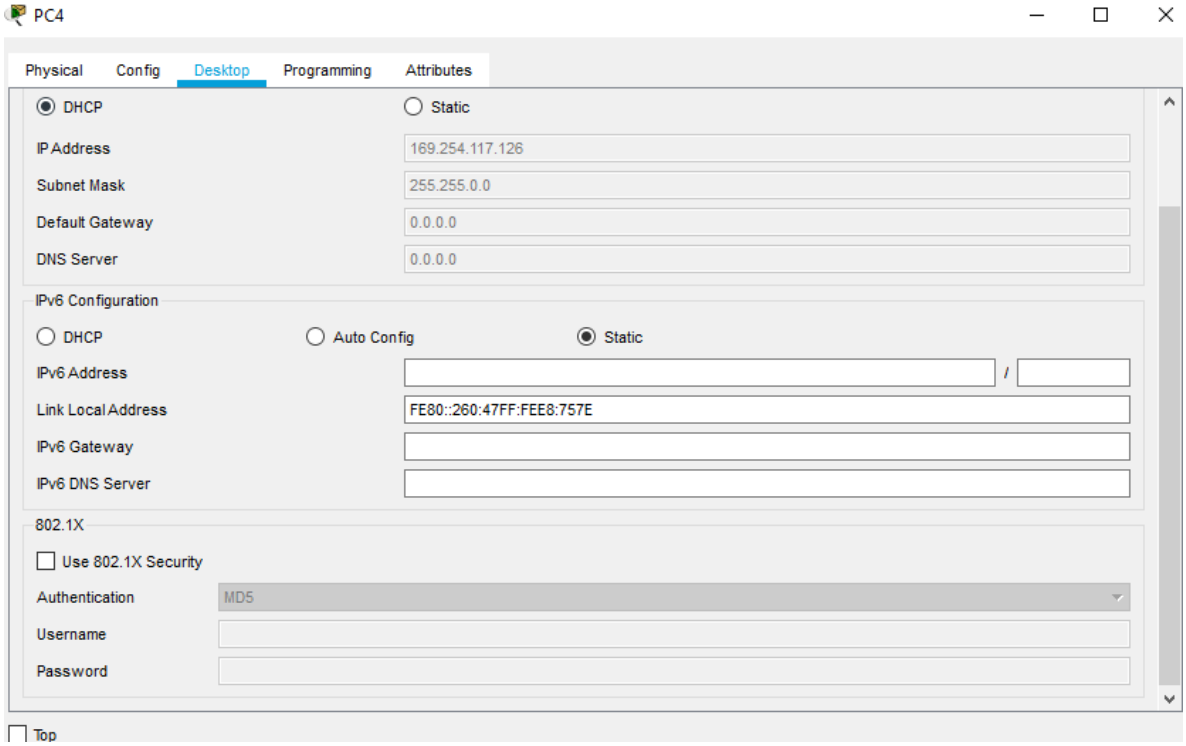
BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#interface gi0/0
BUCARAMANGA(config-if)#ip helper-address 172.31.0.137
BUCARAMANGA(config-if)#

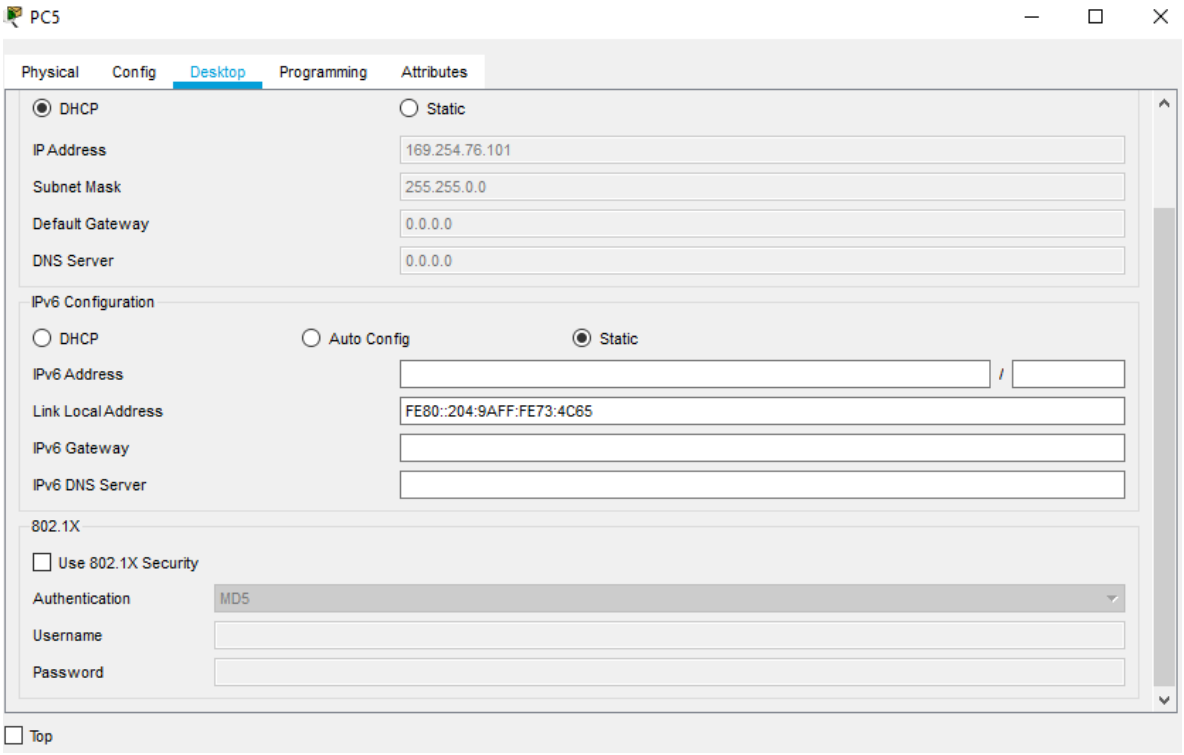




CUNDINAMARCA

Username: Admin
Password:
CUNDINAMARCA>en
Password:
CUNDINAMARCA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CUNDINAMARCA(config)#interface gi0/0
CUNDINAMARCA(config-if)#ip helper-address 172.31.0.161
CUNDINAMARCA(config-if)#





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

DESCRIPCIÓN

En este punto el **servidor web** se configuro con **NAT estático** donde tiene su dirección privada **172.31.2.35,** pero así mismo tiene su ip pública **5.5.5.5** para conectarse a internet. Este mecanismo se aplicó a la red de Cundinamarca y Tunja ya que son las dos redes con **servidor interno** y **externo.**

```
CUNDINAMARCA(config)#ip nat inside source static 172.31.2.35 5.5.5.5
CUNDINAMARCA(config)#interface gi0/0
CUNDINAMARCA(config-if)#ip nat inside
CUNDINAMARCA(config-if)#interface serial 0/0/0
CUNDINAMARCA(config-if)#ip nat outside
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#
```

```
TUNJA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#ip nat inside source static 169.254.238.155 5.5.5.5
TUNJA(config)#interface gi0/0
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#interface serial 0/0/0
TUNJA(config-if)# ip nat outside
TUNJA(config-if)#
```

DESCRIPCIÓN

Para los demás dispositivos se utilizó el mecanismo de **NAT de sobrecarga** donde se traduce las direcciones ip privadas en una sola dirección ip publica **0.0.0.255.** Este mecanismo se aplicó a todas las redes.

```
BUCARAMANGA(config)#access-list 10 permit 172.31.0.137 0.0.0.255
BUCARAMANGA(config)#ip nat inside source list 10 interface serial 0/0/1 overload
BUCARAMANGA(config)#interface gi0/0
BUCARAMANGA(config-if)#ip nat inside
BUCARAMANGA(config-if)#interface serial 0/0/1
BUCARAMANGA(config-if)#ip nat outside
BUCARAMANGA(config-if)#
```

```
TUNJA(config)#access-list 10 permit 209.17.220.1 0.0.0.255
TUNJA(config)#ip nat inside source list 10 interface serial 0/0/1 overload
TUNJA(config)#interface gi0/0
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#interface serial 0/0/1
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#
```

```
CUNDINAMARCA(config)#access-list 10 permit 172.31.0.161 0.0.0.255
CUNDINAMARCA(config)#ip nat inside source list 10 interface serial 0/0/1
overload
CUNDINAMARCA(config)#interface gi0/0
CUNDINAMARCA(config-if)#ip nat inside
CUNDINAMARCA(config-if)#interface serial 0/0/1
CUNDINAMARCA(config-if)#ip nat outside
CUNDINAMARCA(config-if)#
```

4. El enrutamiento deberá tener autenticación.

DESCRIPCIÓN

Se procede a ejecutar en los routers la autenticación con el protocolo **eigrp** que es enrutamiento del tipo vector distancia avanzado, lo cual se utilizó la contraseña **cisco**.

```
BUCARAMANGA(config)#int gi0/0
BUCARAMANGA(config-if)#ip authentication mode eigrp 1 md5
BUCARAMANGA(config-if)#ip authentication key-chain eigrp 1 secretos
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#key chain secretos
BUCARAMANGA(config-keychain)#key 1
BUCARAMANGA(config-keychain-key)#key-string cisco
```

```
TUNJA(config)#int gi0/0
TUNJA(config-if)#ip authentication mode eigrp 1 md5
TUNJA(config-if)#ip authentication key-chain eigrp 1 secretos
TUNJA(config-if)#exit
TUNJA(config)#key chain secretos
TUNJA(config-keychain)#key 1
TUNJA(config-keychain-key)#key-string cisco
TUNJA(config-keychain-key)#
```

```
CUNDINAMARCA(config)#int gi0/0
CUNDINAMARCA(config-if)#ip authentication mode eigrp 1 md5
CUNDINAMARCA(config-if)#ip authentication key-chain eigrp 1 secretos
CUNDINAMARCA(config-if)#exit
CUNDINAMARCA(config)#key chain secretos
CUNDINAMARCA(config-keychain)#key 1
CUNDINAMARCA(config-keychain-key)#key-string cisco
CUNDINAMARCA(config-keychain-key)#
```

5. Listas de control de acceso:

DESCRIPCIÓN

En este punto se podría definir como la forma que puedo administrar o parame trizar la red y su respectiva seguridad con el ACL o lista de control de acceso donde cada host tiene permitido acceder a cierta partes de la red y donde será denegado su acceso.

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

```
CUNDINAMARCA(config)#int vlan 20
CUNDINAMARCA(config-if)#access-list 1 deny 172.31.0.161 0.0.0.255
CUNDINAMARCA(config)#int vlan 20
CUNDINAMARCA(config-if)#access-list 1 permit host 209.17.220.1
CUNDINAMARCA(config)#
```

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

```
CUNDINAMARCA(config)#int vlan 10
CUNDINAMARCA(config-if)#access-list 1 permit host 172.31.0.161
CUNDINAMARCA(config)#int vlan 10
CUNDINAMARCA(config-if)#access-list 1 deny 209.17.220.1 0.0.0.255
    CUNDINAMARCA(config)#
```

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

```
TUNJA(config)#int vlan 30
TUNJA(config-if)#access-list 1 permit host 172.31.2.35
TUNJA(config)#int vlan 30
TUNJA(config-if)#access-list 1 permit host 169.254.238.155
TUNJA(config)#int vlan 30
TUNJA(config-if)#access-list 1 permit host 172.31.2.33
    TUNJA(config)#
```

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

```
TUNJA(config)#int vlan 20
TUNJA(config-if)#access-list 1 permit host 172.31.1.64
TUNJA(config)#int vlan 20
TUNJA(config-if)#access-list 1 permit host 172.31.0.0
TUNJA(config)#
```

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

```
BUCARAMANGA(config)#int vlan 30
BUCARAMANGA(config-if)#access-list 1 permit host 172.31.0.137
BUCARAMANGA(config)#int vlan 30
BUCARAMANGA(config-if)#access-list 1 permit host 172.31.0.0
BUCARAMANGA(config)#
```

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

```
BUCARAMANGA(config)#int vlan 10
BUCARAMANGA(config-if)#access-list 1 permit host 172.31.1.64
BUCARAMANGA(config)#int vlan 10
BUCARAMANGA(config-if)#access-list 1 permit host 172.31.0.128
BUCARAMANGA(config)#int vlan 10
BUCARAMANGA(config-if)#
```

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

De Bucaramanga a Tunja

```
BUCARAMANGA(config)#int vlan 1
BUCARAMANGA(config-if)#access-list 1 deny 172.3.2.8 0.0.0.255
BUCARAMANGA(config)#int vlan 10
BUCARAMANGA(config-if)#access-list 1 deny 172.31.0.128 0.0.0.255
BUCARAMANGA(config)#int vlan 30
BUCARAMANGA(config-if)#access-list 1 deny 172.31.0.192 0.0.0.255
BUCARAMANGA(config)#
```

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

```
BUCARAMANGA(config)#int vlan 1
BUCARAMANGA(config-if)#access-list 1 permit host 172.31.0.137
BUCARAMANGA(config)#

TUNJA(config)#int vlan 1
TUNJA(config-if)#access-list 1 permit host 209.17.220.1
TUNJA(config)#

CUNDINAMARCA(config)#int vlan 1
CUNDINAMARCA(config-if)#access-list 1 permit host 172.31.0.161
CUNDINAMARCA(config)#int vlan 88
CUNDINAMARCA(config-if)#access-list 1 permit host 172.31.0.161
CUNDINAMARCA(config)#
```

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

DESCRIPCIÓN

En este punto se realizó el cálculo de los demás puntos de la red con la ip **172.31.0.0 /18** tenemos en la siguiente tabla el direccionamiento.

Tabla 1. Tabla de direccionamiento.

Dirección ip	Mascar de subred	ciudad
172.31.0.136	/30	Bucaramanga
172.31.0.160	/28	Cundinamarca
172.31.0.128	/27	Tunja

2.1.2 Aspectos a tener en cuenta

- Habilitar VLAN en cada switch y permitir su enrutamiento.

DESCRIPCIÓN

En la topología de la red se da la asignación que debemos darle a cada uno de los vlans con su respectivo ip y mascara de subred. Se ingresó a cada switch y como ya estaba dividido los vlan se proceden a su correspondiente asignación.

Bucaramanga

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#no sh
Switch(config-if)#no shutdown
Switch(config-if)#
Switch(config-if)#ip add 172.3.2.0 255.255.128.0
Switch(config-if)#
Switch(config)#ip default-gateway 172.31.0.137

Switch(config)#interface vlan 10
Switch(config-if)#ip add 172.31.0.0 255.0.0.0
Switch(config-if)#exit
Switch(config)#ip default-gateway 172.31.0.137
Switch(config)#
Switch(config)#interface vlan 30
Switch(config-if)#ip add 172.31.0.64 255.255.255.192
Bad mask /26 for address 172.31.0.64
Switch(config-if)#ip add 172.31.0.64 255.0.0.0
Switch(config-if)#exit
Switch(config)#ip default-gateway 172.31.0.137
Switch(config)#
```

TUNJA

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#ip add 172.3.2.8 255.255.255.248
Bad mask /29 for address 172.3.2.8
Switch(config-if)#ip add 172.3.2.8 255.0.0.0
```

Switch(config-if)#no sh

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
Switch(config)#ip default-gateway 172.31.0.129
Switch(config)#

Switch(config)#interface vlan 20
Switch(config-if)#ip add 172.3.0.128 255.0.0.0
Switch(config-if)#no sh
Switch(config-if)#

Switch(config)#interface vlan 30
Switch(config-if)#ip add 172.31.0.192 255.0.0.0
Switch(config-if)#no sh
Switch(config-if)#exit

CUNDINAMARCA

Switch(config)#int vlan 1
Switch(config-if)#ip add 172.3.2.8 255.0.0.0
Switch(config-if)#no sh
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch(config-if)#ip default-gateway 172.31.0.161
Switch(config)#int vlan 20
Switch(config-if)#ip add 172.31.1.64 255.0.0.0
Switch(config-if)#exit
Switch(config)#int vlan 30
Switch(config-if)#ip add 172.31.1.0 255.0.0.0
Switch(config-if)#exit
Switch(config)#int vlan 88
Switch(config-if)#ip add 172.31.2.24 255.0.0.0
Switch(config-if)#

- Enrutamiento OSPF con autenticación en cada router.

Username: Admin
Password:
BUCARAMANGA>en
Password:
BUCARAMANGA#conf t

Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#router ospf 1
BUCARAMANGA(config-router)#network 172.31.0.137 255.0.0.0 area 0
BUCARAMANGA(config-router)#network 172.31.2.33 255.0.0.0 area 0
BUCARAMANGA(config-router)#exit
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console

TUNJA(config)#router ospf 1
TUNJA(config-router)#network 209.17.220.1 255.0.0.0 area 0
TUNJA(config-router)#network 172.31.2.33 255.0.0.0 area 0
TUNJA(config-router)#exit
TUNJA(config)#exit
TUNJA#
%SYS-5-CONFIG_I: Configured from console by console

CUNDINAMARCA(config)#router ospf 1
CUNDINAMARCA(config-router)#network 172.31.0.161 255.0.0.0 area 0
CUNDINAMARCA(config-router)#network 172.31.2.34 255.0.0.0 area 0
CUNDINAMARCA(config-router)#exit
CUNDINAMARCA(config)#exit
%SYS-5-CONFIG_I: Configured from console by console

- 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

DESCRIPCIÓN

Se procede habilitar la opción de puerto consola y se asigna la contraseña **cisco**.

BUCARAMANGA(config)#line vty 0 4
BUCARAMANGA(config-line)#password cisco

TUNJA(config)#line vty 0 4
TUNJA(config-line)#password cisco

CUNDINAMARCA(config)#line vty 0 4
CUNDINAMARCA(config-line)#password cisco

CONCLUSIONES

El resultado de este documento después de realizado, se determinó la solución a los dos escenarios propuestos como prácticas de habilidades, en donde se midió el conocimiento a lo largo del periodo académico. Se logró diseñar la topología de las dos redes. Además se entrega el archivo con las respectivas normas ICONTEC 1486. Se cumplió con todos los requerimientos solicitados en los dos escenarios.

Desde el punto de vista personal fue una experiencia con un reto sumamente importante debido a que se vio nuevos conocimiento a lo que estaba acostumbrado.

Se logró cumplir con el objetivo final y es poder entregar este trabajo de grado del cual me siento orgulloso y formalmente se logra entregar con todas las condiciones que se solicitó. Desde mi punto de vista el diplomado de profundización fue una experiencia enriquecedora debido a que como ingeniero me enfrentare a múltiples retos y esto significo el poder plantear soluciones a escenarios reales por medio del simulador Packet Tracert.

A mi gusto y decisión la ingeniera de sistemas es un universo maravilloso el cual durante la carrera universitaria se descubrió muchas cosas y funcionalidades, sin embargo en esta profesión nunca se termina de aprender y me siento privilegiado de entregar este archivo como parte de mi graduación.

BIBLIOGRAFÍA

DI TOMASO, Leandro ”Configuración básica de un router”. {En línea}. {15 julio de 2009} disponible en: (https://www.mikroways.net/2009/07/15/configuracion-basica-de-un-router/).

MELENDEZ, Raul “Subneteo de red clase C y configuración en simulador”. {En línea}. {19 noviembre de 2016} disponible en: (https://www.youtube.com/watch?v=Mk8UZYTP3Xo&t=125s).

ARUMADIGITAL“Redes CCNP 019 EIGRP Algoritmo DUAL y balanceo de carga desigual”. {En línea}. {8 diciembre de 2015 } disponible en: (https://www.youtube.com/watch?v=RjlG6p2Tf_0).

David Alejandro “Como restringir el acceso a una red por parte de un HOST”. {En línea}. {6 abril de 2016} disponible en: (https://www.youtube.com/watch?v=CQwS4ftlEZ0).

DIAZ, Marcelo “Examen Final CCNA1 2018 - Aula en línea”. {En línea}. {17 diciembre de 2018} disponible en: (https://www.youtube.com/watch?v=icDB2c3xGz8&t=1830s).

CANOSA FERREIRO, Alejandro” Reforzando la seguridad en los router Cisco” {En línea}. {12 Abril de 2017} disponible en: (https://backtrackacademy.com/articulo/reforzando-la-seguridad-en-los-router-cisco).

BARRETO, Gabriel “Como configurar un Router Cisco como un servidor DHCP en Packet Tracer”. {En línea}. {14 junio de 2013} disponible en: (https://www.youtube.com/watch?v=yudNmI4p1dU).

Diana “Servicio DHCP con ip-helper address”. {En línea}. {17 junio de 2015} disponible en: (https://www.youtube.com/watch?v=dNkvKbKR_90).

QUINTERO, Angie “enrutamiento y configuracion cisco packet tracer ospf”. {En línea}. {8 mayo de 2017} disponible en: (https://www.youtube.com/watch?v=s1iWFFvND7c).

ARUMADIGITAL, “Redes CCNP 022 EIGRP Tabla de enrutamiento y autenticación”. {En línea}. {5 enero de 2016} disponible en: (https://www.youtube.com/watch?v=OODv94WHo1k).