DIPLOMADO DE PROFUNDIZACION – CISCO
(DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)
PRUEBA DE HABILIDADES PRÁCTICAS CCNA (PLATAFORMA CISCO)
EVALUACION FINAL

Presentado por:

Dalwis Jose Florez Ramirez

Tutor:

Giovanni Alberto Bracho

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
INGENIERIA DE SISTEMAS

DICIEMBRE 2019

TABLA DE CONTENIDO

Páginas

RESUMEN

Este documento corresponde a la actividad final del Diplomado de Profundización CCNA, y por intermedio de estas actividades, divididas en dos (2) escenarios nos permitirán identificar el grado de desarrollo de competencias y habilidades que adquirimos durante el diplomado. Lo principal de esta prueba de habilidades es poner a prueba los niveles de comprensión y solución que aprendimos en los diferentes ejercicios y problemas relacionados con el campo emergente de las Redes y Telecomunicaciones. De igual manera se pretende profundizar y demostrar las capacidades de responder aún mundo real con escenarios físicos que tienen pocas diferencias con las simulaciones hechas de topologías de red, configuraciones de dispositivos, insertar paquetes y simulaciones hechas con las herramientas: Packet Tracer o GNS3.

En esta oportunidad se configuraran e interconectaran entre sí cada uno de los dispositivos que forman parte de los escenarios a resolver, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

Palabras Claves: Cisco, Ping, Traceroute, Packet Tracer, Show ip route, Enable, EIGRP, Router, DHCP, VLAN.

ABSTRACT

This document corresponds to the final activity of the CCNA Deepening Diploma, and through these activities, divided into two (2) scenarios will allow us to identify the degree of development of skills and abilities that we acquired during the diploma. The main thing about this skills test is to test the levels of understanding and solution we learned in the different exercises and problems related to the emerging field of Networks and Telecommunications. Similarly, it is intended to deepen and demonstrate the capabilities of responding even in real world with physical scenarios that have few differences with simulations made of network topologies, device configurations, insert packages and simulations made with the tools: Packet Tracer or GNS3.

In this occasion, each of the devices that are part of the scenarios to be resolved will be configured and interconnected, in accordance with the guidelines established for IP addressing, routing protocols and other aspects that are part of the network topology.

Keywords: Cisco, ping, traceroute, Packet Tracer, show ip route, enable, EIGRP, Router, DHCP, VLAN.

INTRODUCCION

Actualmente, en el mundo existen una serie de nuevas tecnologías que hacen la vida del hombre más fácil en muchos aspectos, tales como; el internet, Sistemas Ciber físicos, en los trabajos de oficinas, trabajos de conexión de redes y otras más. De tal manera que estas nuevas tecnologías, están fundamentadas en redes informáticas, permitiendo que las personas se comuniquen, colaboren e interactúen de muchas maneras. Por eso es fundamental como profesionales conocer y apropiarnos de los temas de conexión entre redes, pc, switch y router que permiten la intersección de las redes entre si y su interconexión. Especialmente usando tecnologías de punta como Cisco.

Para esta evaluación de “Prueba de habilidades prácticas CCNA”, nos muestran dos (2) escenarios en donde se nos piden configuraran e interconectar cada uno de los dispositivos que lo conforman y demostrar las habilidades y conocimientos adquiridos en el diplomado, necesarios para instalar, operar y solucionar problemas de una red, como: Asignación de direcciones IP, Configuración Básica, Configuración de Enrutamiento. Configuración de las listas de Control de Acceso. Comprobación de la red instalada para confirmar el óptimo funcionamiento de la red.

OBJETIVOS

GENERAL:

Desarrollar las competencias y habilidades adquiridas durante el diplomado en la comprensión y solución soportadas en el uso de dispositivos de conmutación acorde con las topologías de Networking en los dos (2) escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución.

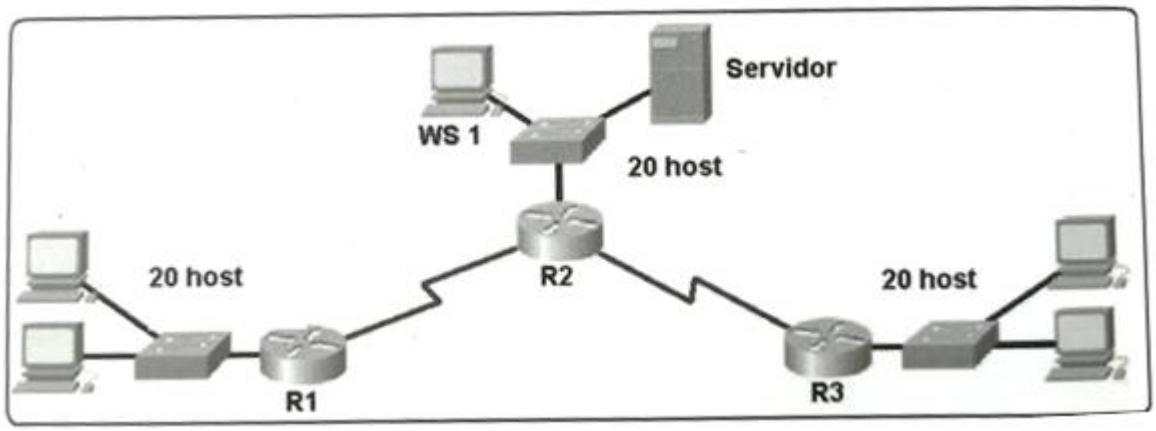
ESPECÍFICOS:

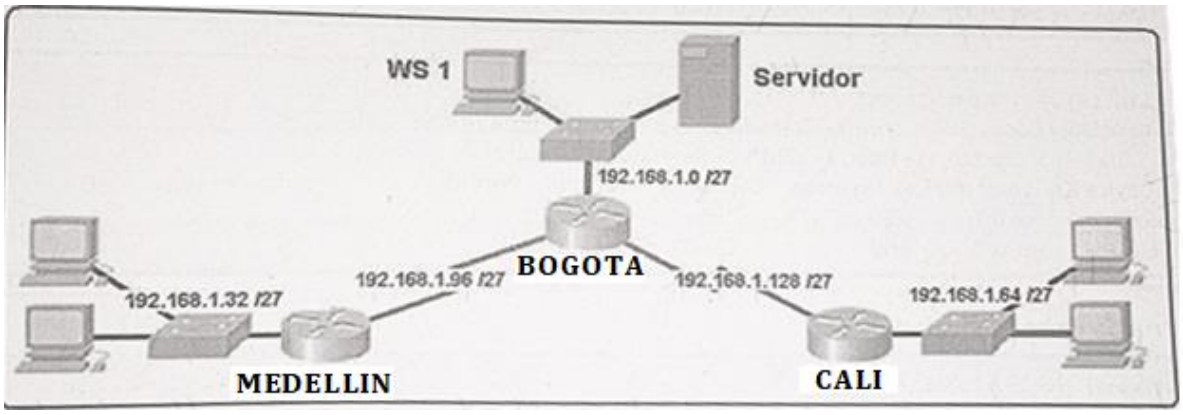
- Análisis de las topologías de los escenarios propuestos.
- Asignación de direccionamiento IP.
- Asignación de los parámetros básicos y la detección de vecinos directamente conectados.
- Configuración básica y de Enrutamiento de la red y subred.
- Configuración de las listas de Control de Acceso.
- Comprobación total de los dispositivos para confirmar el óptimo funcionamiento de la red.
- Configuración final y Documentación de cada solución.

DESARROLLO DE LA PRUEBA DE HABILIDADES

ESCENARIO 1

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





Topología de red:

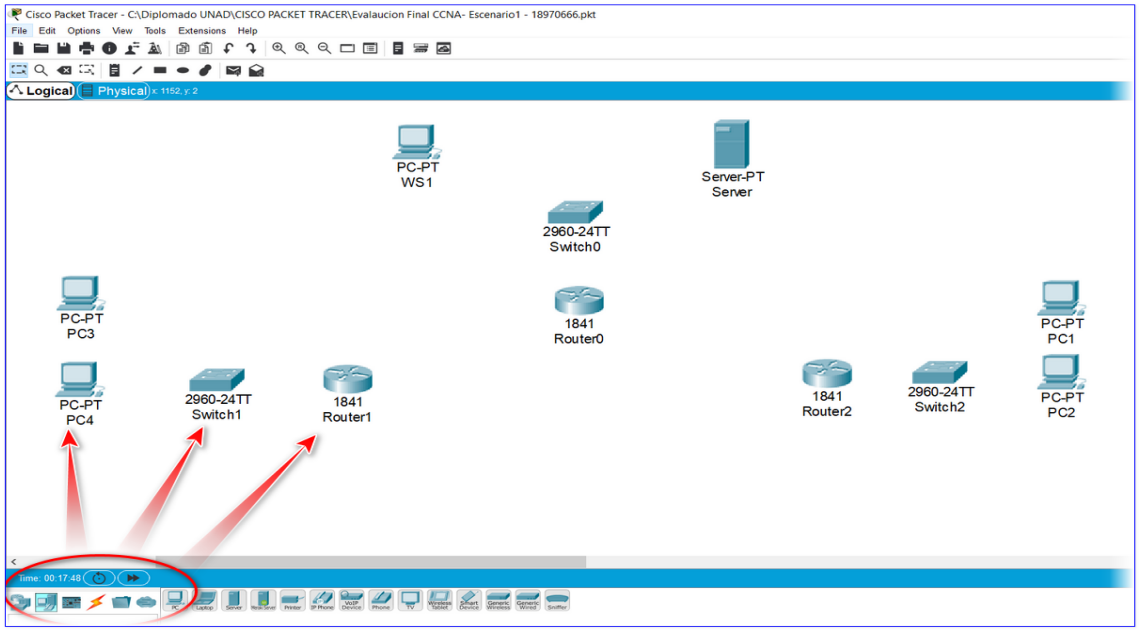
Los Requerimientos solicitados son los siguientes:

- **Parte 1:** Para el direccionamiento IP debe definirse una dirección de acuerdo con el número de hosts requeridos.
- **Parte 2:** Considerar la asignación de los parámetros básicos y la detección de vecinos directamente conectados.
- **Parte 3:** La red y subred establecidas deberán tener una interconexión total, todos los hosts deberán ser visibles y poder comunicarse entre ellos sin restricciones.
- **Parte 4:** Implementar la seguridad en la red, se debe restringir el acceso y comunicación entre hosts de acuerdo con los requerimientos del administrador de red.
- **Parte 5:** Comprobación total de los dispositivos y su funcionamiento en la red.
- **Parte 6:** Configuración final.

Desarrollo:

Como trabajo inicial se debe realizar lo siguiente.

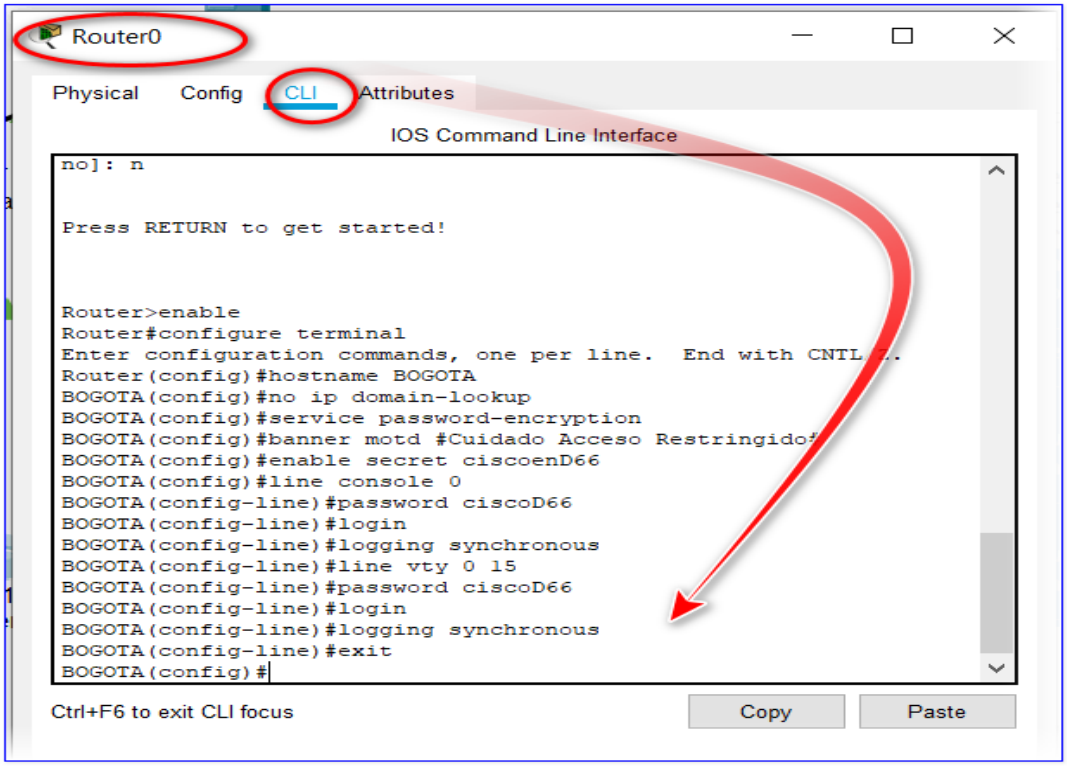
- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).



Todos los dispositivos (Routers y Switch han sido preconfigurados con:

- Enable password: **ciscoenD66**
- Password for console: **ciscoD66**

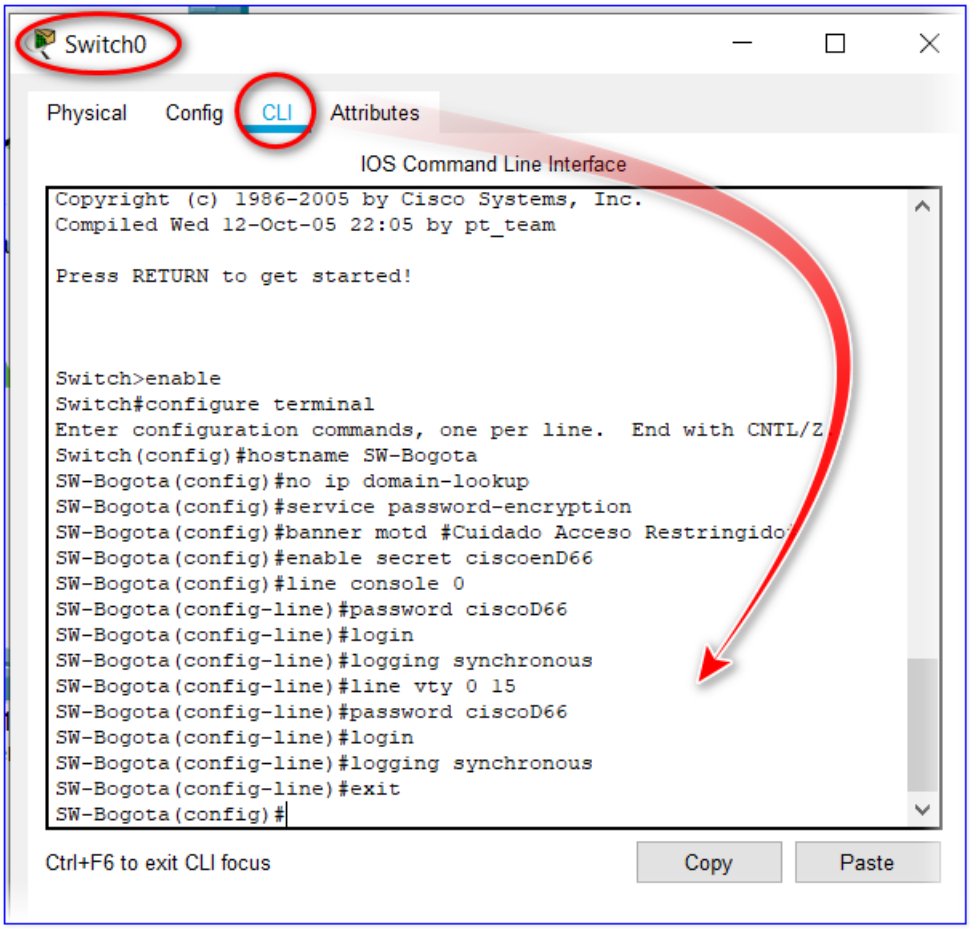
```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA
BOGOTA(config)#no ip domain-lookup
BOGOTA(config)#service password-encryption
BOGOTA(config)#banner motd #Cuidado Acceso Restringido#
BOGOTA(config)#enable secret ciscoenD66
BOGOTA(config)#line console 0
BOGOTA(config-line)#password ciscoD66
BOGOTA(config-line)#login
BOGOTA(config-line)#logging synchronous
BOGOTA(config-line)#line vty 0 15
BOGOTA(config-line)#password ciscoD66
BOGOTA(config-line)#login
BOGOTA(config-line)#logging synchronous
BOGOTA(config-line)#exit
BOGOTA(config)#
```



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN
MEDELLIN(config)#no ip domain-lookup
MEDELLIN(config)#service password-encryption
MEDELLIN(config)#banner motd #Cuidado Acceso Restringido#
MEDELLIN(config)#enable secret ciscoenD66
MEDELLIN(config)#line console 0
MEDELLIN(config-line)#password ciscoD66
MEDELLIN(config-line)#login
MEDELLIN(config-line)#logging synchronous
MEDELLIN(config-line)#line vty 0 15
MEDELLIN(config-line)#password ciscoD66
MEDELLIN(config-line)#login
MEDELLIN(config-line)#logging synchronous
MEDELLIN(config-line)#exit
MEDELLIN(config)#
```

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CALI
CALI(config)#no ip domain-lookup
CALI(config)#service password-encryption
CALI(config)#banner motd #Cuidado Acceso Restringido#
CALI(config)#enable secret ciscoenD66
CALI(config)#line console 0
CALI(config-line)#password ciscoD66
CALI(config-line)#login
CALI(config-line)#logging synchronous
CALI(config-line)#line vty 0 15
CALI(config-line)#password ciscoD66
CALI(config-line)#login
CALI(config-line)#logging synchronous
CALI(config-line)#exit
CALI(config)#
```

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-Bogota
SW-Bogota(config)#no ip domain-lookup
SW-Bogota(config)#service password-encryption
SW-Bogota(config)#banner motd #Cuidado Acceso Restringido#
SW-Bogota(config)#enable secret ciscoenD66
SW-Bogota(config)#line console 0
SW-Bogota(config-line)#password ciscoD66
SW-Bogota(config-line)#login
SW-Bogota(config-line)#logging synchronous
SW-Bogota(config-line)#line vty 0 15
SW-Bogota(config-line)#password ciscoD66
SW-Bogota(config-line)#login
SW-Bogota(config-line)#logging synchronous
SW-Bogota(config-line)#exit
SW-Bogota(config)#
```



```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-Medellin
SW-Medellin(config)#no ip domain-lookup
SW-Medellin(config)#service password-encryption
SW-Medellin(config)#banner motd #Cuidado Acceso Restringido#
SW-Medellin(config)#enable secret ciscoenD66
SW-Medellin(config)#line console 0
SW-Medellin(config-line)#password ciscoD66
SW-Medellin(config-line)#login
SW-Medellin(config-line)#logging synchronous
SW-Medellin(config-line)#line vty 0 15
SW-Medellin(config-line)#password ciscoD66
SW-Medellin(config-line)#login
SW-Medellin(config-line)#logging synchronous
SW-Medellin(config-line)#exit
SW-Medellin(config)#
```

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-Cali
SW-Cali(config)#no ip domain-lookup
SW-Cali(config)#service password-encryption
SW-Cali(config)#banner motd #Cuidado Acceso Restringido#
SW-Cali(config)#enable secret ciscoenD66
SW-Cali(config)#line console 0
SW-Cali(config-line)#password ciscoD66
SW-Cali(config-line)#login
SW-Cali(config-line)#logging synchronous
SW-Cali(config-line)#line vty 0 15
SW-Cali(config-line)#password ciscoD66
SW-Cali(config-line)#login
SW-Cali(config-line)#logging synchronous
SW-Cali(config-line)#exit
SW-Cali(config)#
```

- Realizar la conexión física de los equipos con base en la topología de red.

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

Todos los dispositivos (Routers y Switch han sido preconfigurados con:

- Enable password: **ciscoenD66**
- Password for console: **ciscoD66**

- **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. Asignar una dirección IP a la red.

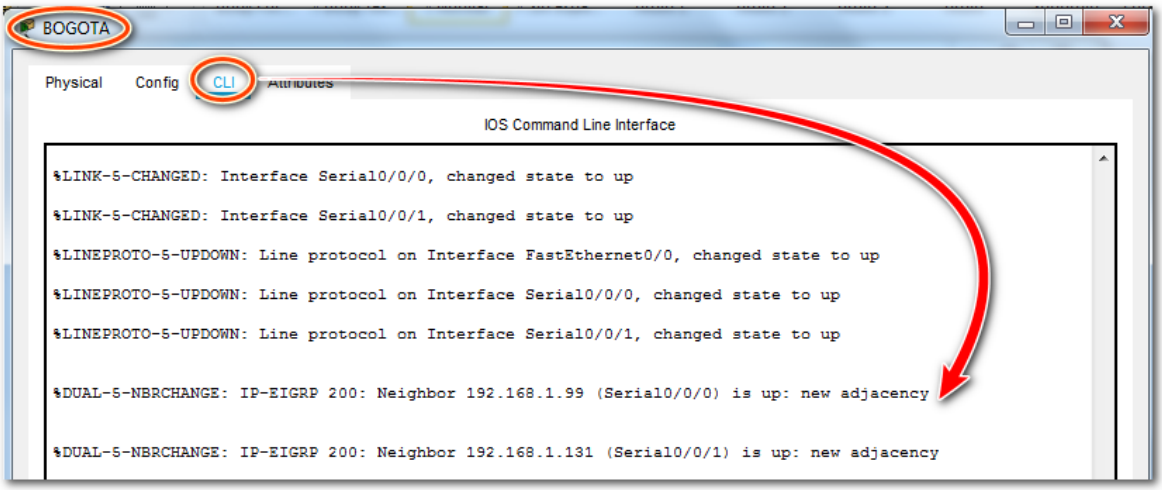
Numero de Subred	Dirección de Subred	Primera Dirección de Host Utilizable	ultima Dirección de Host Utilizable
0-Bogota	192.168.1.0/27	192.168.1.1	192.168.1.30
1-Medellin	192.168.1.32/27	192.168.1.33	192.168.1.62
2-Cali	192.168.1.64/27	192.168.1.65	192.168.1.94
3-Bogota/Medellin	192.168.1.96/27	192.168.1.97	192.168.1.126
4- Bogota/Cali	192.168.1.128/27	192.168.1.129	192.168.1.158
5-Red Futuras	192.168.1.160/27	192.168.1.161	192.168.1.190
6-Red Futuras	192.168.1.192/27	192.168.1.193	192.168.1.222
7-Red Futuras	192.168.1.224/27	192.168.1.225	192.168.1.254

- **Parte 2: Configuración Básica:**

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

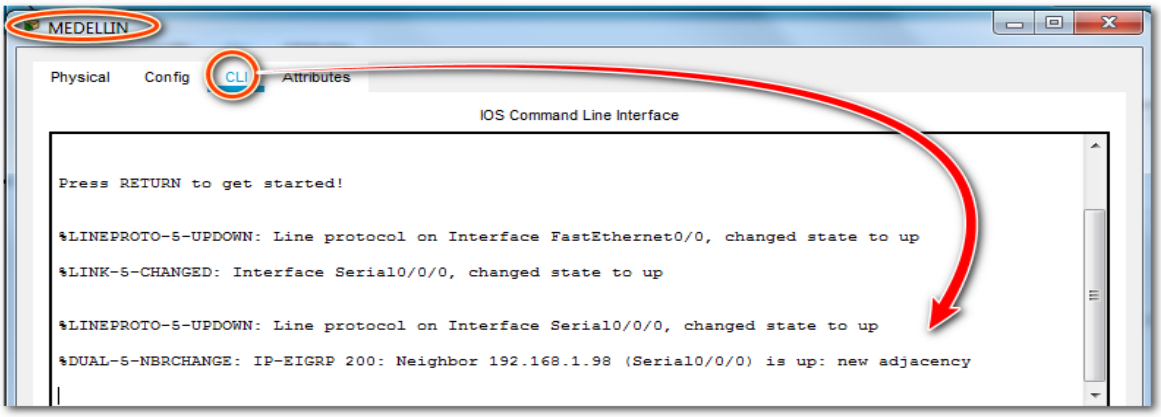
	R1	R2	R3
Nombre de Host	MEDELLIN	BOGOTA	CALI
Dirección de Ip en interfaz Serial 0/0	192.168.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/1		192.168.1.130	
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	Eigrp	Eigrp	Eigrp
Sistema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

```
BOGOTA(config)#int s0/0/0
BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#

BOGOTA(config-if)#int s0/0/1
BOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#

BOGOTA(config-if)#int f0/0
BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224
BOGOTA(config-if)#no shutdown

BOGOTA(config-if)#
BOGOTA(config-if)#router eigrp 200
BOGOTA(config-router)#no auto-summary
BOGOTA(config-router)#network 192.168.1.0 0.0.0.31
BOGOTA(config-router)#network 192.168.1.96 0.0.0.31
BOGOTA(config-router)#network 192.168.1.128 0.0.0.31
BOGOTA(config-router)#
BOGOTA(config-router)#end
```

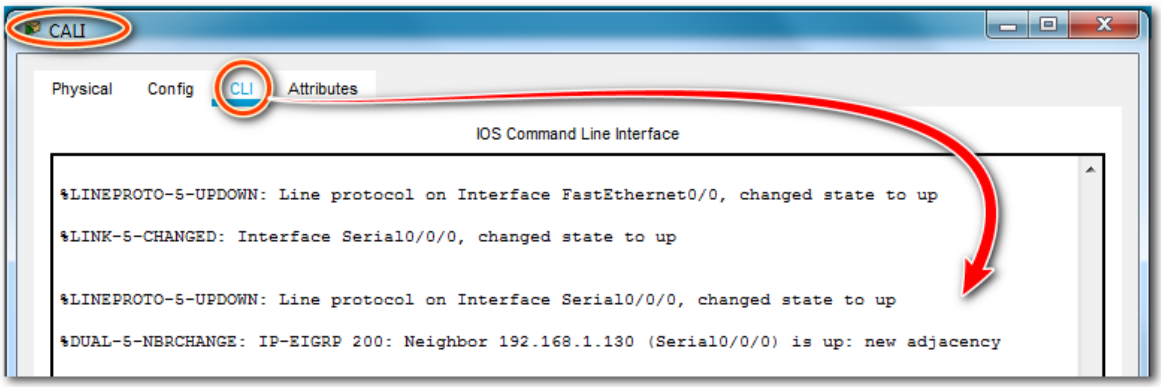



```
MEDELLIN(config-line)#int s0/0/0
MEDELLIN(config-if)#ip address 192.168.1.99 255.255.255.224
MEDELLIN(config-if)#no shutdown

MEDELLIN(config-if)#
MEDELLIN(config-if)#int f0/0
MEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.224
MEDELLIN(config-if)#no shutdown
```

```
MEDELLIN(config-if)#
MEDELLIN(config-if)#router eigrp 200
MEDELLIN(config-router)#no auto-summary
MEDELLIN(config-router)#network 192.168.1.32 0.0.0.31
MEDELLIN(config-router)#network 192.168.1.96 0.0.0.31
MEDELLIN(config-router)#end
MEDELLIN#
```

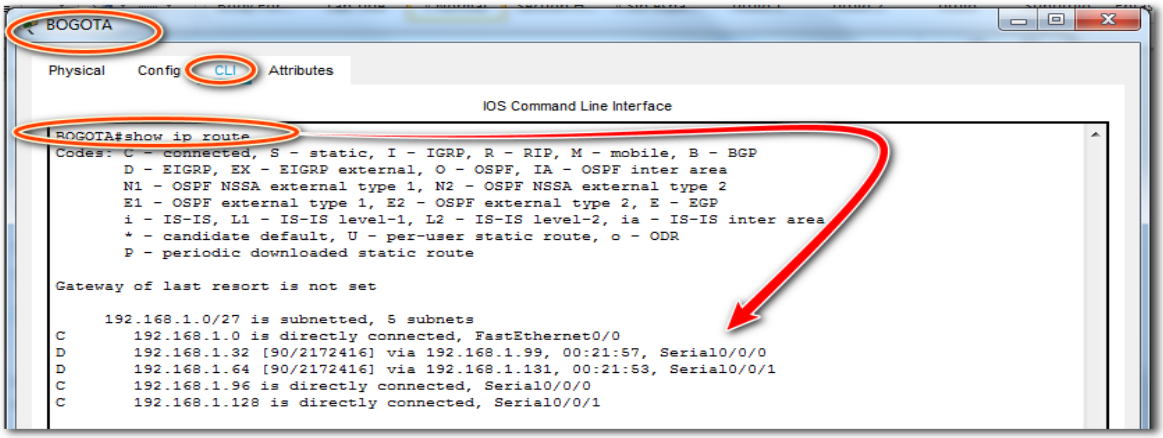



```
CALI(config-line)#int s0/0/0
CALI(config-if)#ip address 192.168.1.131 255.255.255.224
CALI(config-if)#no shutdown

CALI(config-if)#int f0/0
CALI(config-if)#ip address 192.168.1.65 255.255.255.224
CALI(config-if)#no shutdown

CALI(config-if)#
CALI(config-if)#router eigrp 200
CALI(config-router)#no auto-summary
CALI(config-router)#network 192.168.1.64 0.0.0.31
CALI(config-router)#network 192.168.1.128 0.0.0.31
CALI(config-router)#end
```

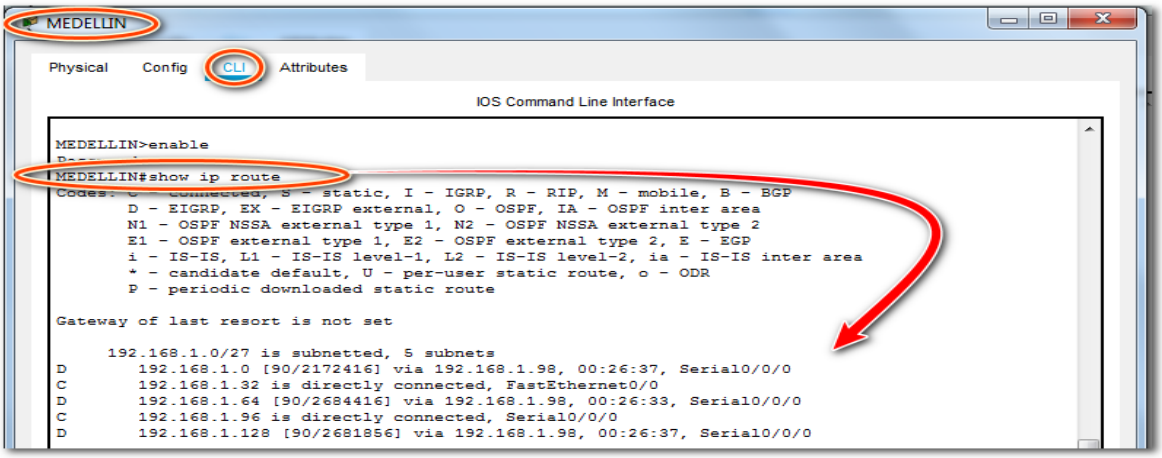


b. Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

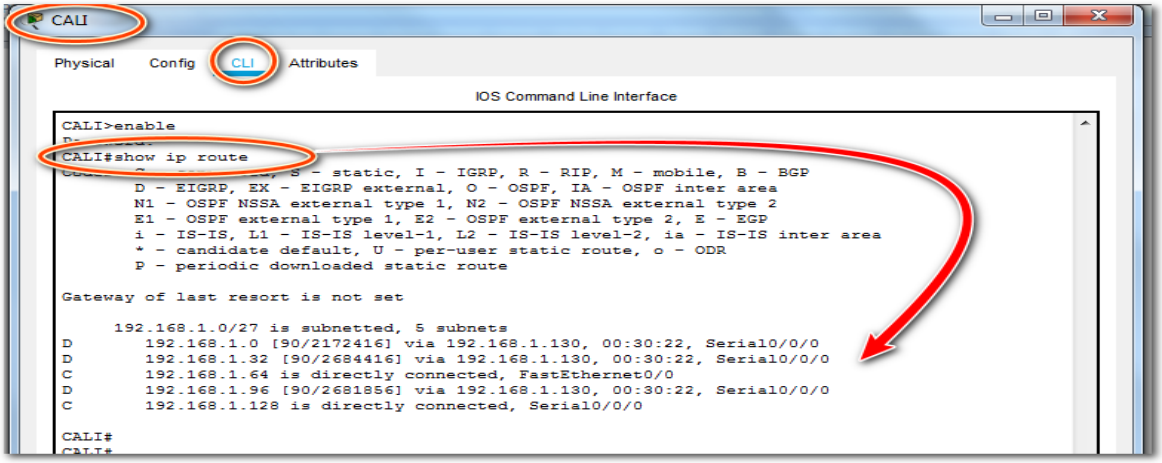
BOGOTA#show ip route



MEDELLIN#show ip route

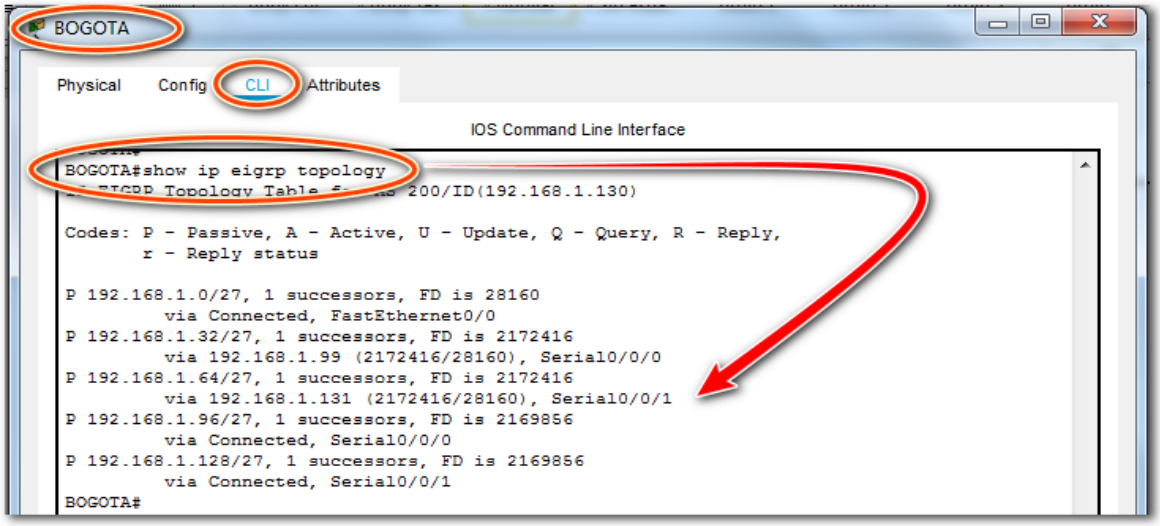


CALI#show ip route

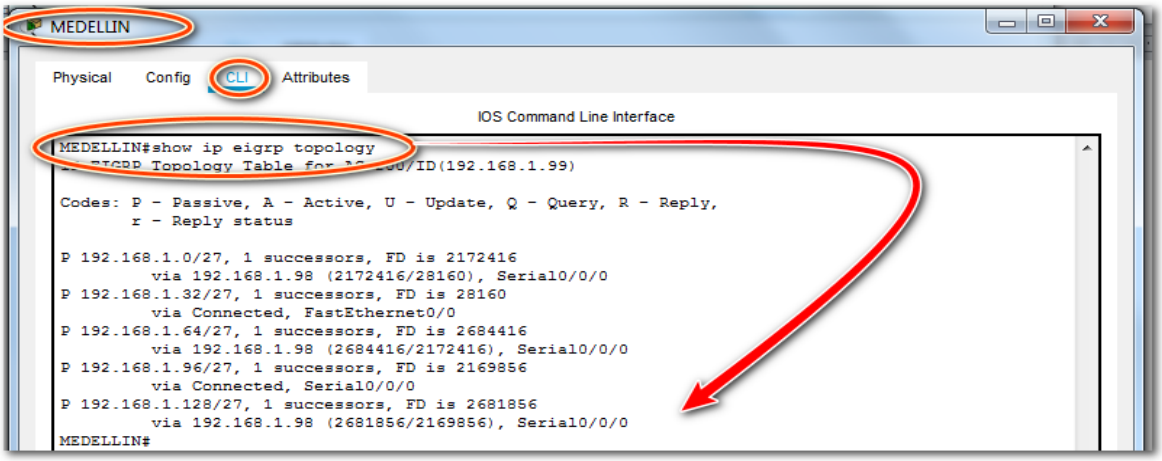


c. Verificar el balanceo de carga que presentan los Routers.

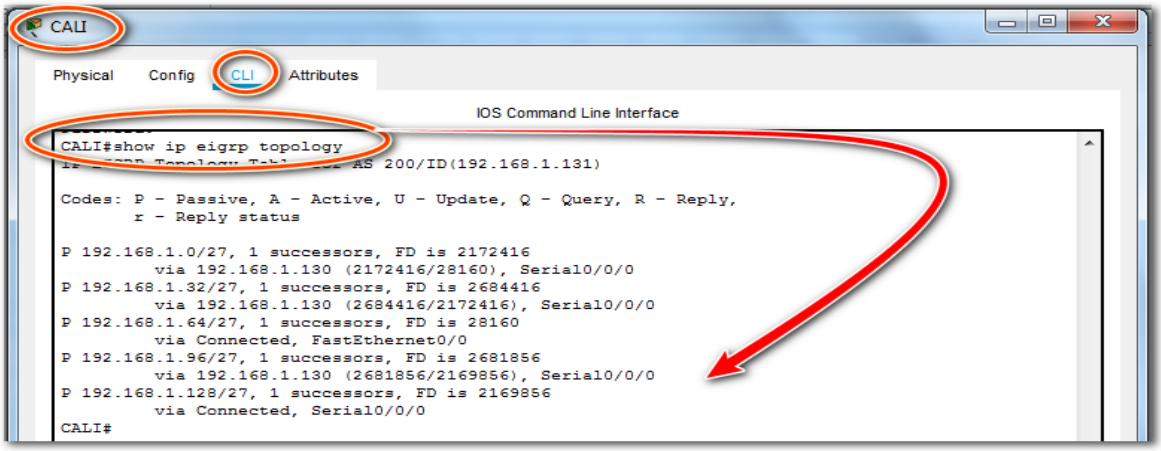
BOGOTA#show ip eigrp topology



MEDELLIN#show ip eigrp topology



CALI#show ip eigrp topology



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

BOGOTA#show cdp neighbor

```
BOGOTA>enable
Password:
BOGOTA#show cdp neighbor
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
SWBOGOTA     Fas 0/0          164            S       2960        Fas 0/1
MEDELLIN     Ser 0/0/0        170            R       C1841       Ser 0/0/0
CALI         Ser 0/0/1        174            R       C1841       Ser 0/0/0
BOGOTA#
```

MEDELLIN#show cdp neighbor

```
MEDELLIN#show cdp neighbor
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
SWMEDELLIN   Fas 0/0          134            S       2960        Fas 0/1
BOGOTA       Ser 0/0/0        135            R       C1841       Ser 0/0/0
MEDELLIN#
```

CALI#show cdp neighbor

```
CALI#show cdp neighbor
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
SWCALI       Fas 0/0          174            S       2960        Fas 0/1
BOGOTA       Ser 0/0/0        174            R       C1841       Ser 0/0/1
CALI#
```

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

```
BOGOTA>enable
Password:
BOGOTA#ping 192.168.1.99

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.99, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/12 ms
```

```
Password:
MEDELLIN#ping 192.168.1.130

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.130, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/15 ms

MEDELLIN#ping 192.168.1.131

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.131, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/7/15 ms
```

```
CALI>enable
Password:
CALI#ping 192.168.1.98

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.98, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6 ms
```

- **Parte 3: Configuración de Enrutamiento.**

a. Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.
b. Verificar si existe vecindad con los routers configurados con EIGRP.

BOGOTA#show ip eigrp neighbor

```
Password:
BOGOTA#show ip eigrp neighbor
IP-EIGRP neighbors for process 200
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt Num
0   192.168.1.99    Se0/0/0         12   00:03:17  40     1000  0   7
1   192.168.1.131   Se0/0/1         14   00:03:15  40     1000  0   7

BOGOTA#
```

MEDELLIN#show ip eigrp neighbor

```
MEDELLIN>enable
Password:
MEDELLIN#show ip eigrp neighbor
IP-EIGRP neighbors for process 200
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt Num
0   192.168.1.98    Se0/0/0         14   00:07:22  40     1000  0   5
```

CALI#show ip eigrp neighbor

```
Password:
Password:
CALI#show ip eigrp neighbor
IP-EIGRP neighbors for process 200
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt Num
0   192.168.1.130   Se0/0/0         14   00:10:32  40     1000  0   6

CALI#
```

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

BOGOTA#show ip route

```
BOGOTA>enable
Password:
BOGOTA#show ip route
Codes: C - connected, S - static, I - IGRP, 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

     192.168.1.0/27 is subnetted, 5 subnets
C       192.168.1.0 is directly connected, FastEthernet0/0
D       192.168.1.32 [90/2172416] via 192.168.1.99, 00:16:26, Serial0/0/0
D       192.168.1.64 [90/2172416] via 192.168.1.131, 00:16:25, Serial0/0/1
C       192.168.1.96 is directly connected, Serial0/0/0
C       192.168.1.128 is directly connected, Serial0/0/1
```

MEDELLIN#show ip route

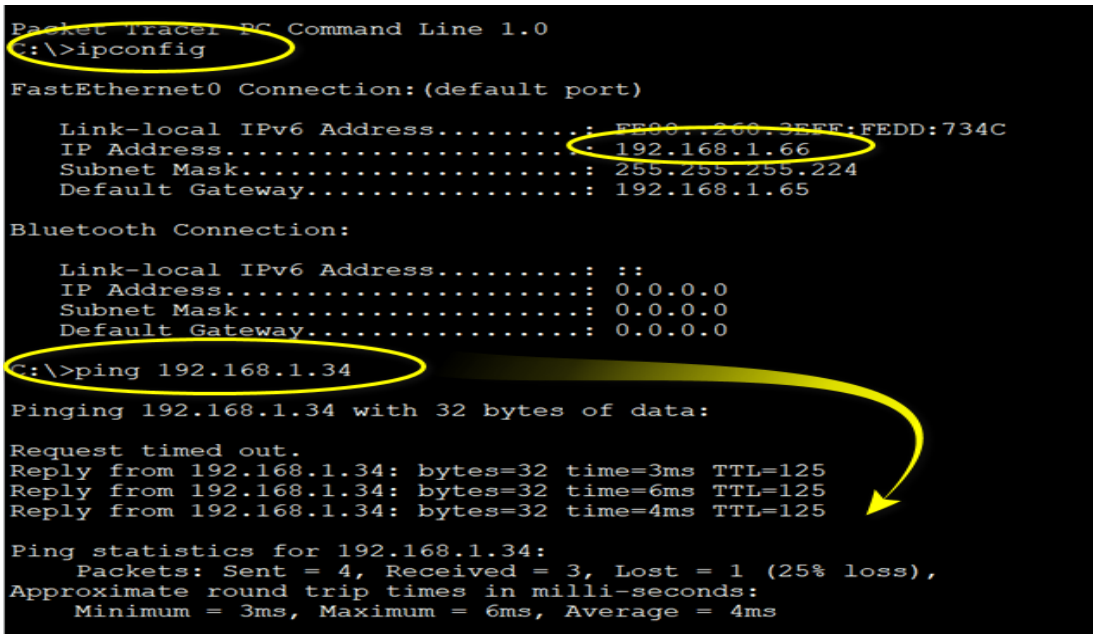
```
MEDELLIN#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, 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

     192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/2172416] via 192.168.1.98, 00:15:51, Serial0/0/0
C       192.168.1.32 is directly connected, FastEthernet0/0
D       192.168.1.64 [90/2684416] via 192.168.1.98, 00:15:50, Serial0/0/0
C       192.168.1.96 is directly connected, Serial0/0/0
D       192.168.1.128 [90/2681856] via 192.168.1.98, 00:15:51, Serial0/0/0
```

CALI#show ip route

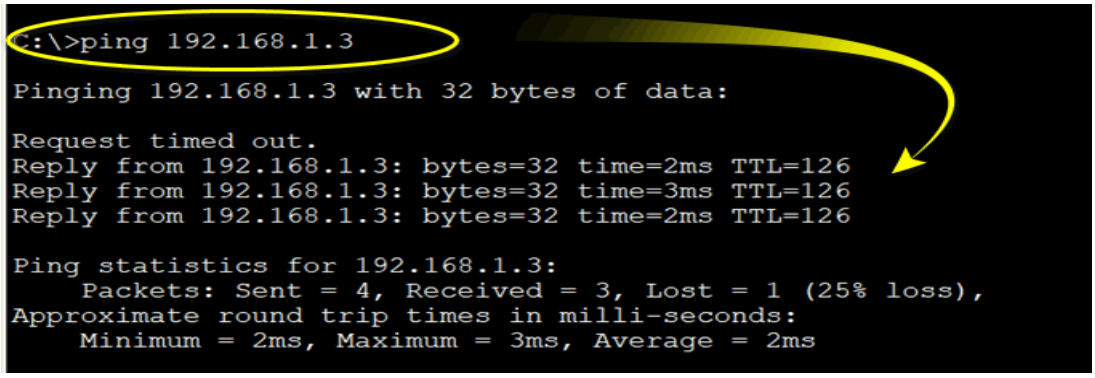
```
CALI#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - 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

     192.168.1.0/27 is subnetted, 5 subnets
D       192.168.1.0 [90/2172416] via 192.168.1.130, 00:15:44, Serial0/0/0
D       192.168.1.32 [90/2684416] via 192.168.1.130, 00:15:44, Serial0/0/0
C       192.168.1.64 is directly connected, FastEthernet0/0
D       192.168.1.96 [90/2681856] via 192.168.1.130, 00:15:44, Serial0/0/0
C       192.168.1.128 is directly connected, Serial0/0/0
```

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

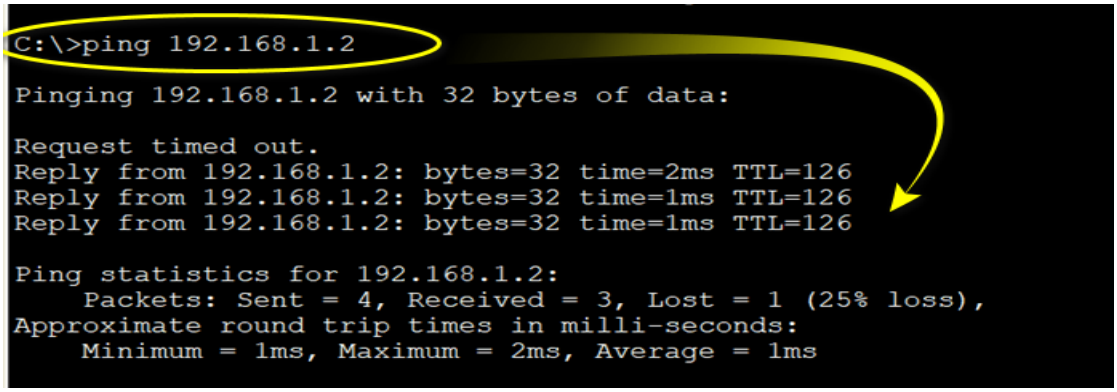
- Del PC1 de la red de CALI al PC3 de la red de MEDELLIN



- Del PC1 de la red de CALI al WS1 de la red de BOGOTA



- Del PC1 de la red de CALI al Servidor de la red de BOGOTA



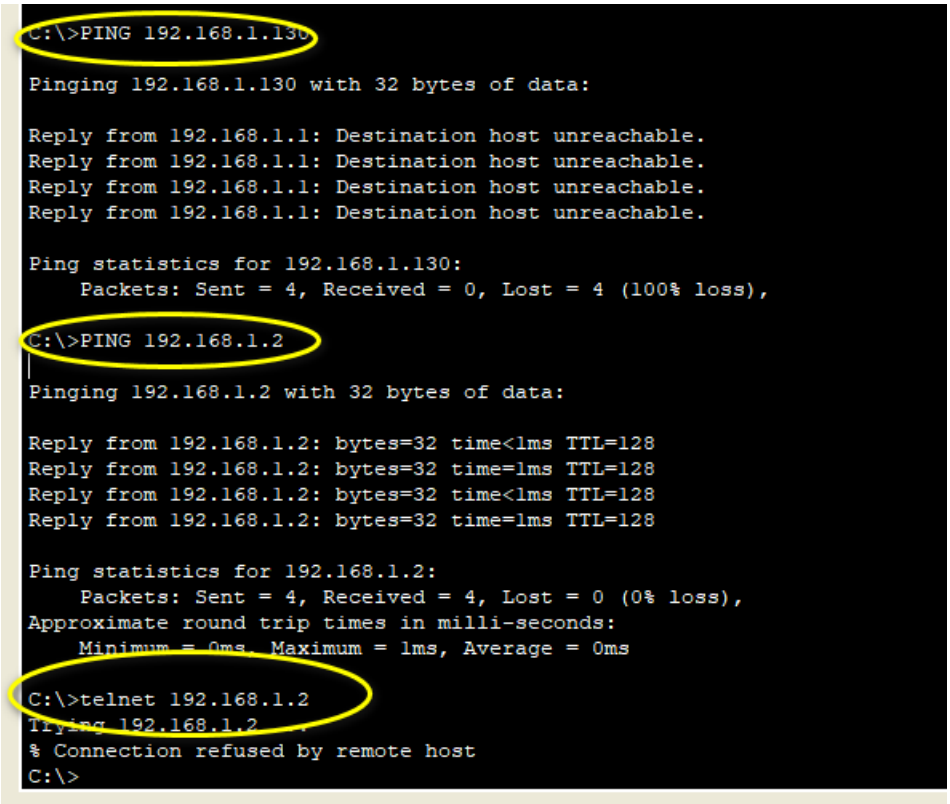
- **Parte 4: Configuración de las listas de Control de Acceso.**

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

```
BOGOTA(config)#access-list 111 permit ip host 192.168.1.30 any
MEDELLIN(config)#access-list 111 permit ip host 192.168.1.30 any
CALI(config)#access-list 111 permit ip host 192.168.1.30 any
```



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.

```
BOGOTA>enable
Password:
BOGOTA#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#access-list 111 permit ip host 192.168.1.30 any
BOGOTA(config)#int f0/0
BOGOTA(config-if)#ip access-group 111 in
```

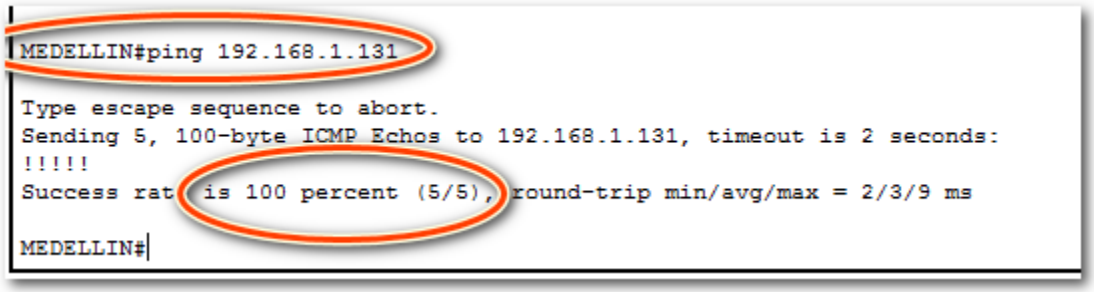
c. Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor.

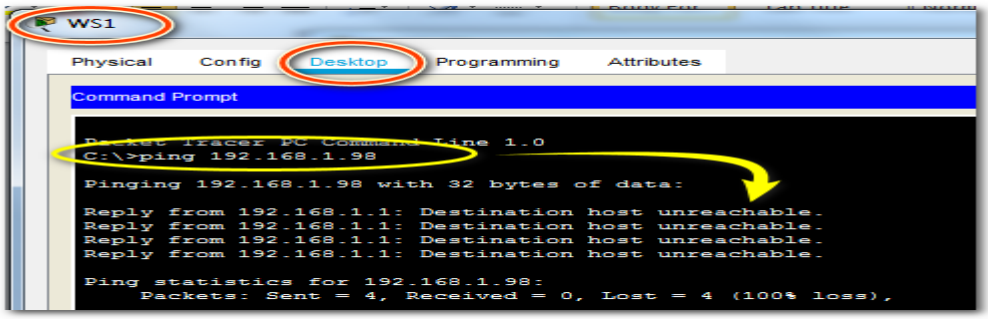
```
MEDELLIN# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#access-list 111 permit ip 192.168.1.32 0.0.0.31
host 192.168.1.30
MEDELLIN(config)#int f0/0
MEDELLIN(config-if)#ip access-group 111 in

CALI# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#access-list 111 permit ip 192.168.1.64 0.0.0.31
host 192.168.1.30
CALI(config)#int f0/0
CALI(config-if)#ip access-group 111 in
```

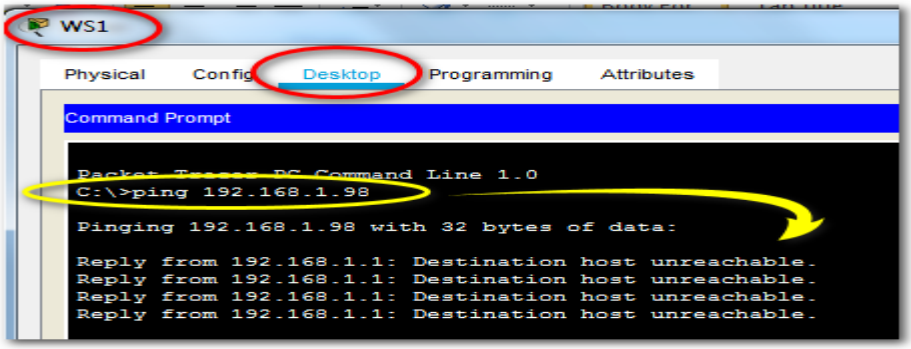
- **Parte 5: Comprobación de la red instalada.**

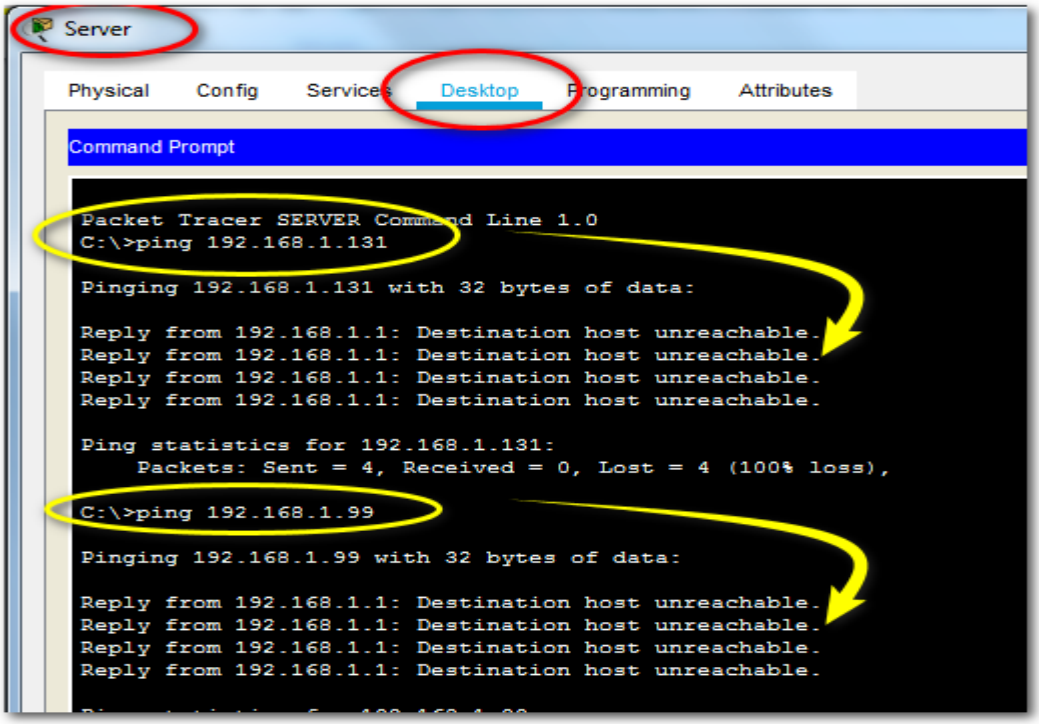
a. Se debe probar que la configuración de las listas de acceso fue exitosa.

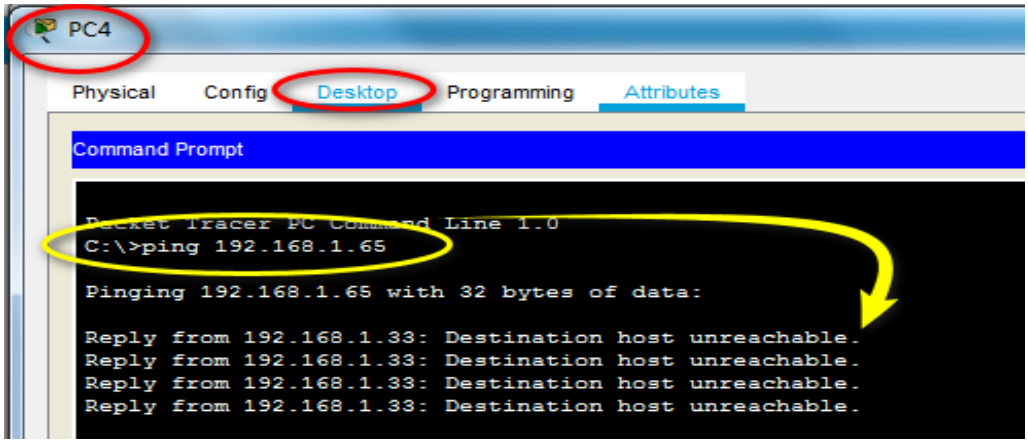
b. Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red.



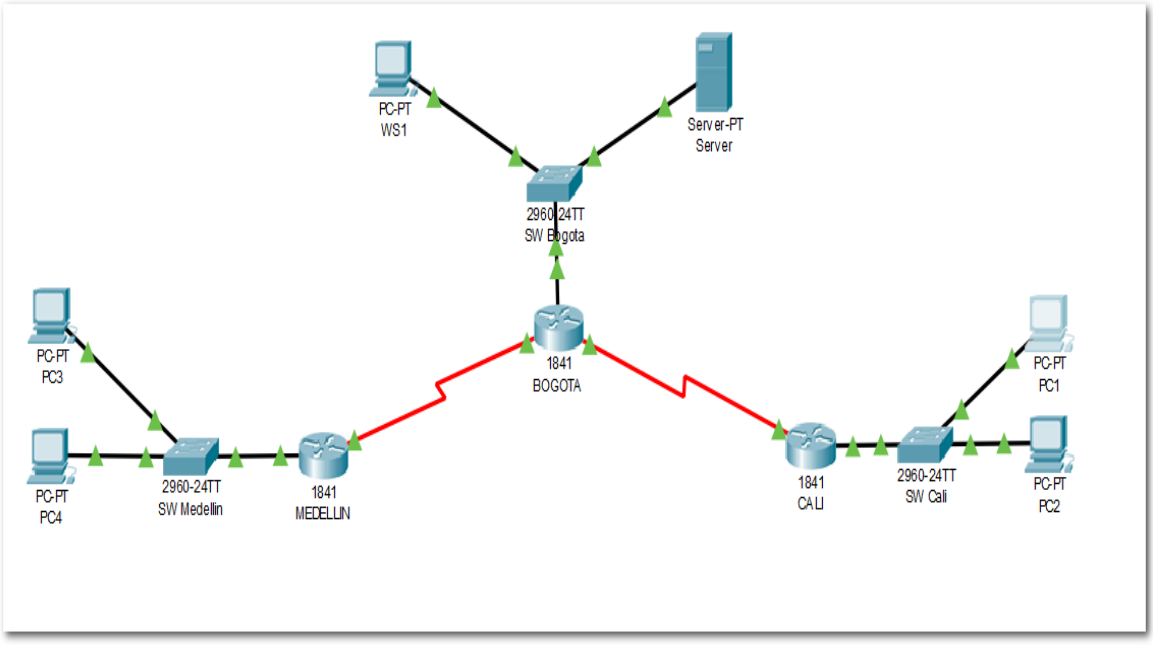



WS1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.98
Pinging 192.168.1.98 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.


Server
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.1.131
Pinging 192.168.1.131 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Ping statistics for 192.168.1.131:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.1.99
Pinging 192.168.1.99 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.


PC4
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.65
Pinging 192.168.1.65 with 32 bytes of data:
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.
Reply from 192.168.1.33: Destination host unreachable.

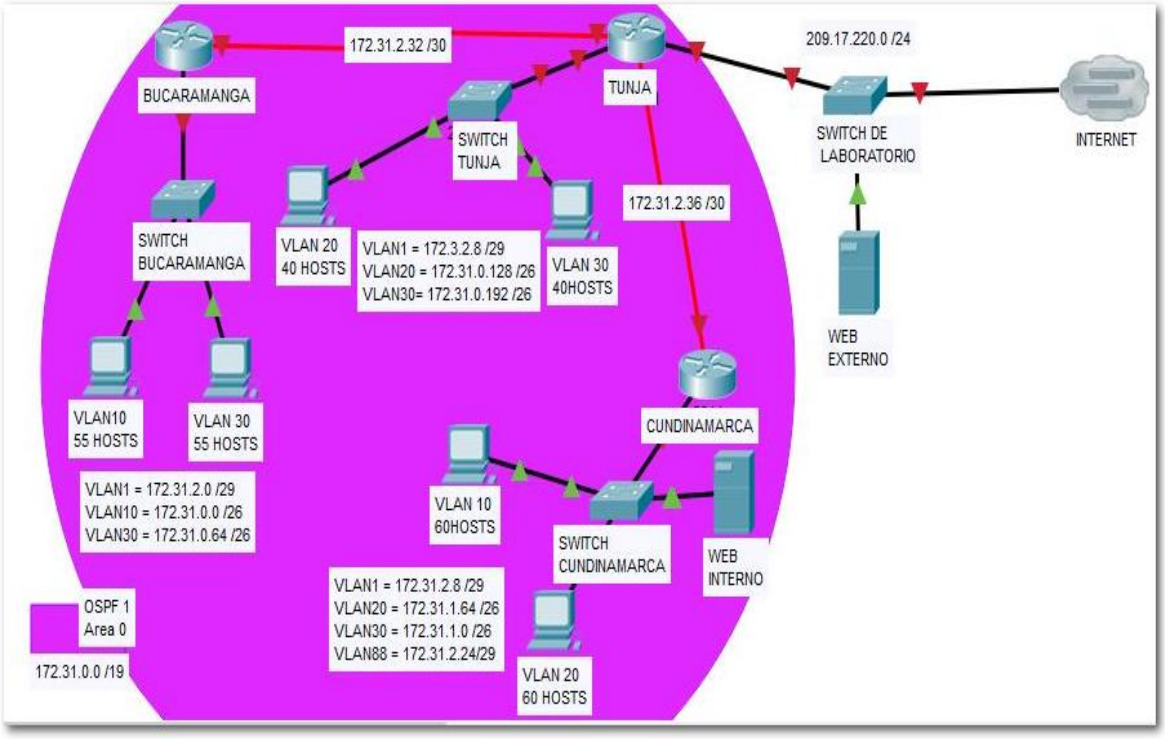
	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	Exitoso
	WS_1	Router BOGOTA	Inalcanzable
	Servidor	Router CALI	Exitoso
	Servidor	Router MEDELLIN	Exitoso
TELNET	LAN del Router MEDELLIN	Router CALI	Exitoso
	LAN del Router CALI	Router CALI	Exitoso
	LAN del Router MEDELLIN	Router MEDELLIN	Exitoso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



DESARROLLO DE LA PRUEBA DE HABILIDADES

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.

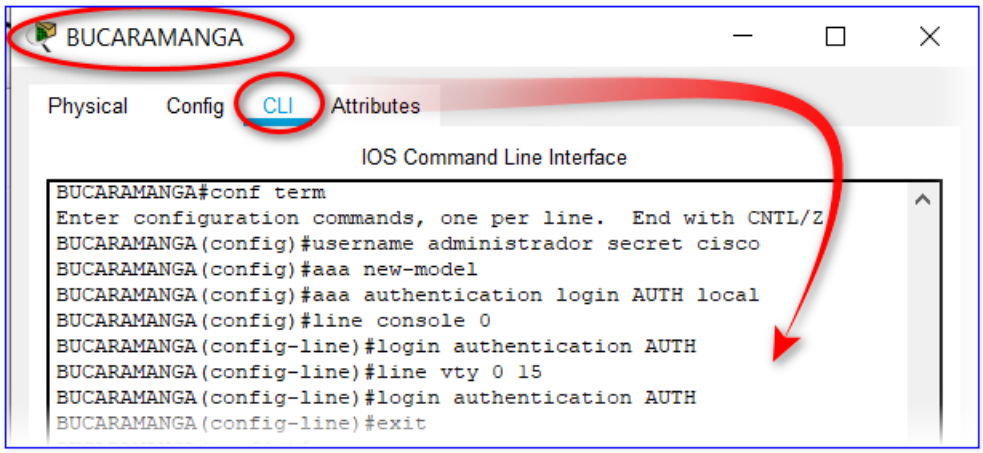


Los siguientes son los requerimientos necesarios:

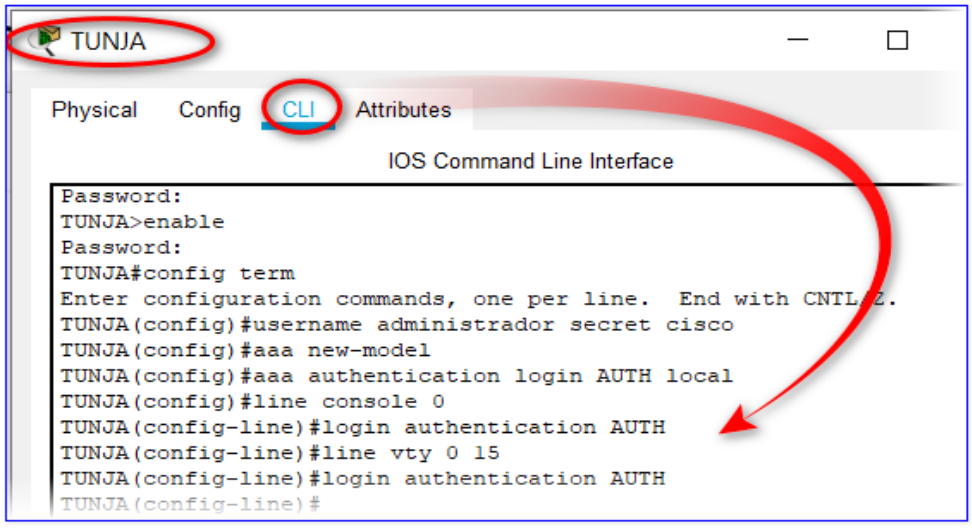
1. **Todos los routers deberán tener los siguiente:**

- Configuración básica.
- Autenticación local con AAA.

```
BUCARAMANGA(config)#username administrador secret cisco
BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#aaa authentication login AUTH local
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#login authentication AUTH
BUCARAMANGA(config-line)#line vty 0 15
BUCARAMANGA(config-line)#login authentication AUTH
BUCARAMANGA(config-line)#exit
```




```
TUNJA(config)#username administrador secret cisco
TUNJA(config)#aaa new-model
TUNJA(config)#aaa authentication login AUTH local
TUNJA(config)#line console 0
TUNJA(config-line)#login authentication AUTH
TUNJA(config-line)#line vty 0 15
TUNJA(config-line)#login authentication AUTH
TUNJA(config-line)#exit
```




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

- Cifrado de contraseñas:

```
BUCARAMANGA(config)#service password-encryption
TUNJA(config)#service password-encryption
CUNDINAMARCA(config)#service password-encryption
```

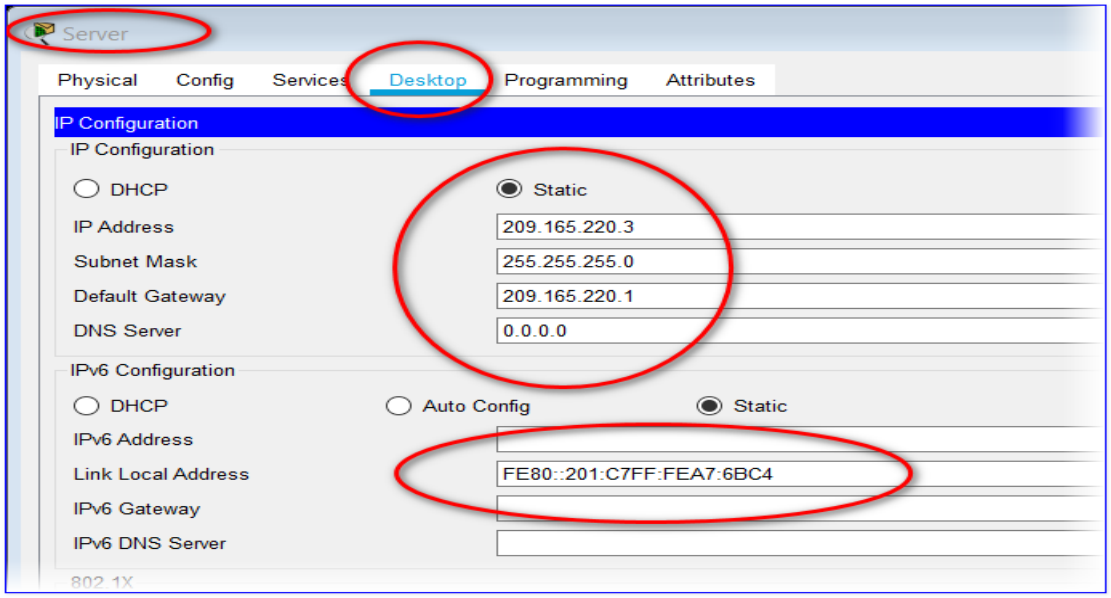
- Un máximo de internos para acceder al router.

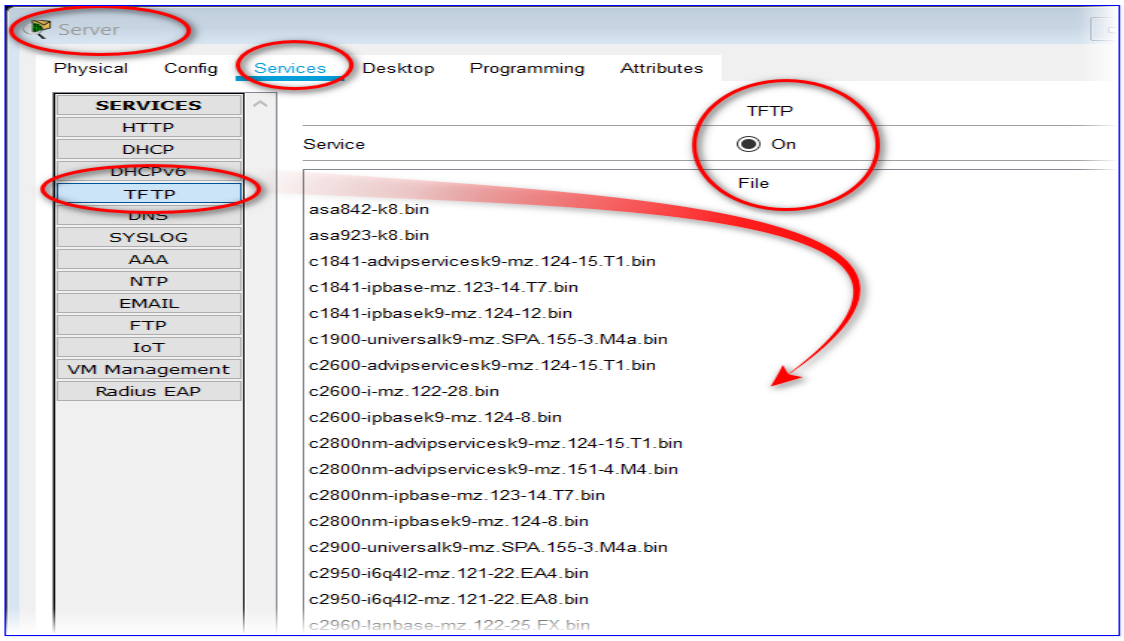
```
BUCARAMANGA(config-line)#login block-for 5 attempts 4 within 60
TUNJA(config-line)#login block-for 5 attempts 4 within 60
CUNDINAMARCA(config-line)#login block-for 5 attempts 4 within 60
```

- Máximo tiempo de acceso al detectar ataques.

```
BUCARAMANGA(config-line)#login block-for 5 attempts 4 within 60
TUNJA(config-line)#login block-for 5 attempts 4 within 60
CUNDINAMARCA(config-line)#login block-for 5 attempts 4 within 60
```

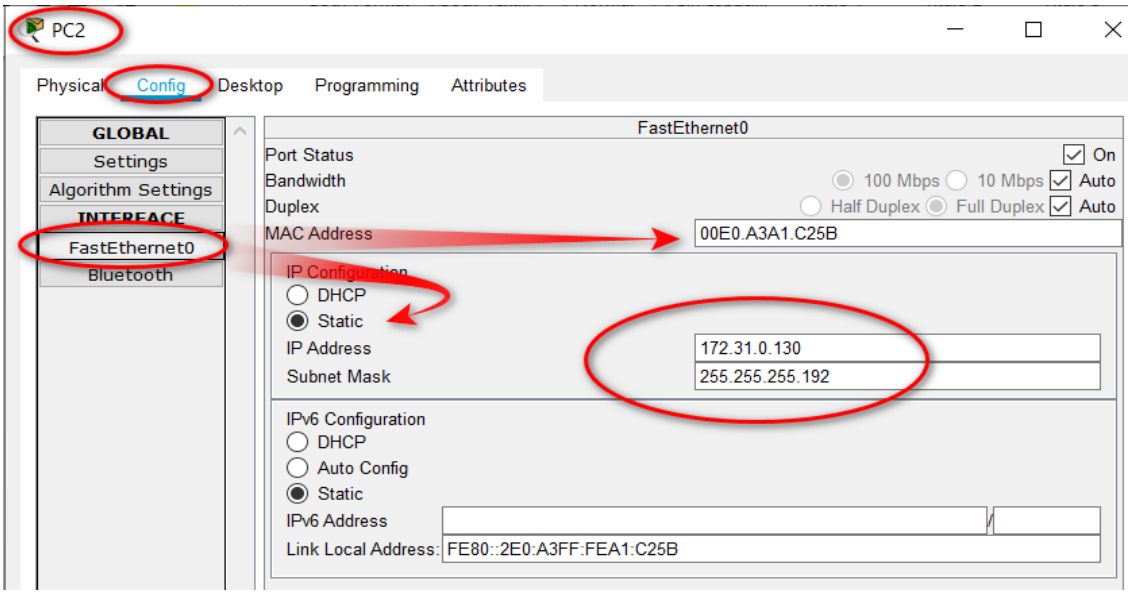
- Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.



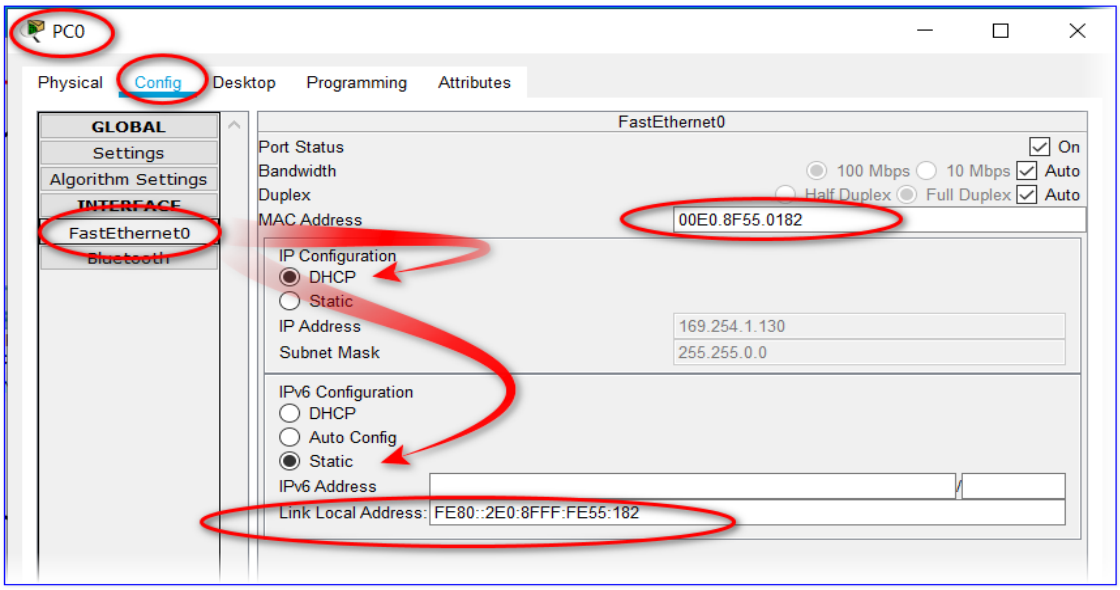


2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca.

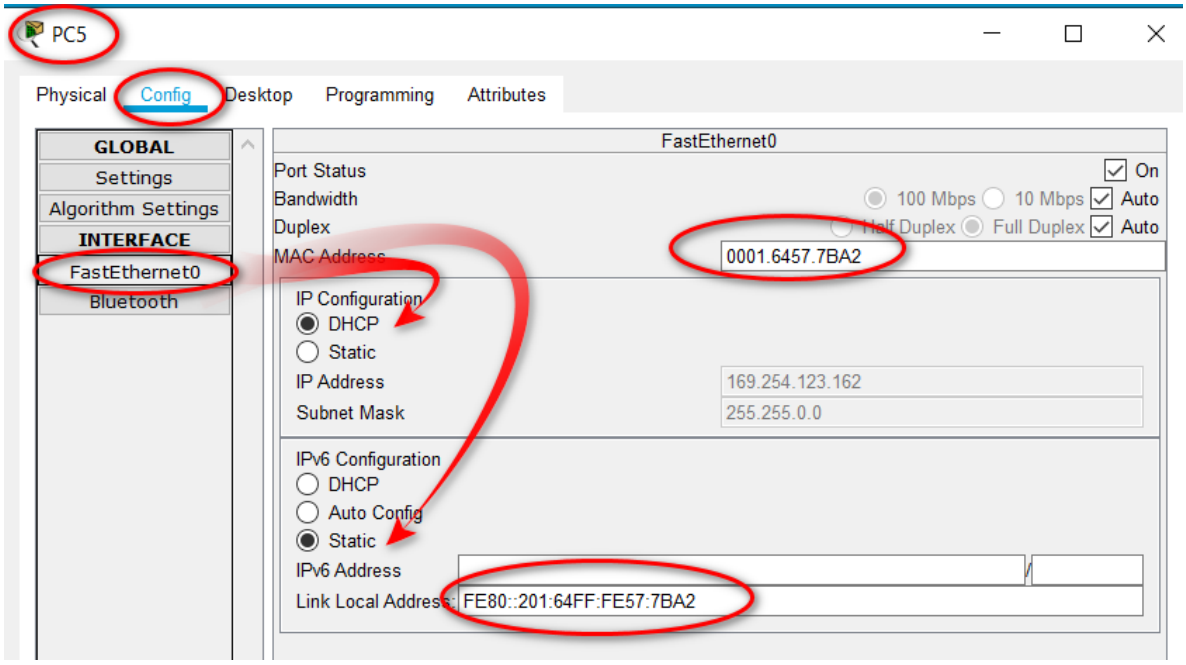
```
TUNJA(config)#ip dhcp excluded-address 172.31.0.1
TUNJA(config)#ip dhcp excluded-address 172.31.0.65
TUNJA(config)#ip dhcp excluded-address 172.31.1.65
TUNJA(config)#ip dhcp excluded-address 172.31.1.1
TUNJA(config)#ip dhcp pool V10B
TUNJA(dhcp-config)#network 172.31.0.0 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.0.1
TUNJA(dhcp-config)#dns-server 172.31.2.28
TUNJA(dhcp-config)#ip dhcp pool V30B
TUNJA(dhcp-config)#network 172.31.0.64 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.0.65
TUNJA(dhcp-config)#dns-server 172.31.2.28
TUNJA(dhcp-config)#ip dhcp pool V20C
TUNJA(dhcp-config)#network 172.31.1.64 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.1.65
TUNJA(dhcp-config)#dns-server 172.31.2.28
TUNJA(dhcp-config)#ip dhcp pool V30C
TUNJA(dhcp-config)#network 172.31.1.0 255.255.255.192
TUNJA(dhcp-config)#default-router 172.31.1.1
TUNJA(dhcp-config)#dns-server 172.31.2.28
TUNJA(dhcp-config)#
```




```
BUCARAMANGA(config)#int f0/0.10
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.33
BUCARAMANGA(config-subif)#int f0/0.30
BUCARAMANGA(config-subif)#ip helper-address 172.31.2.33
BUCARAMANGA(config-subif)#end
BUCARAMANGA#
```

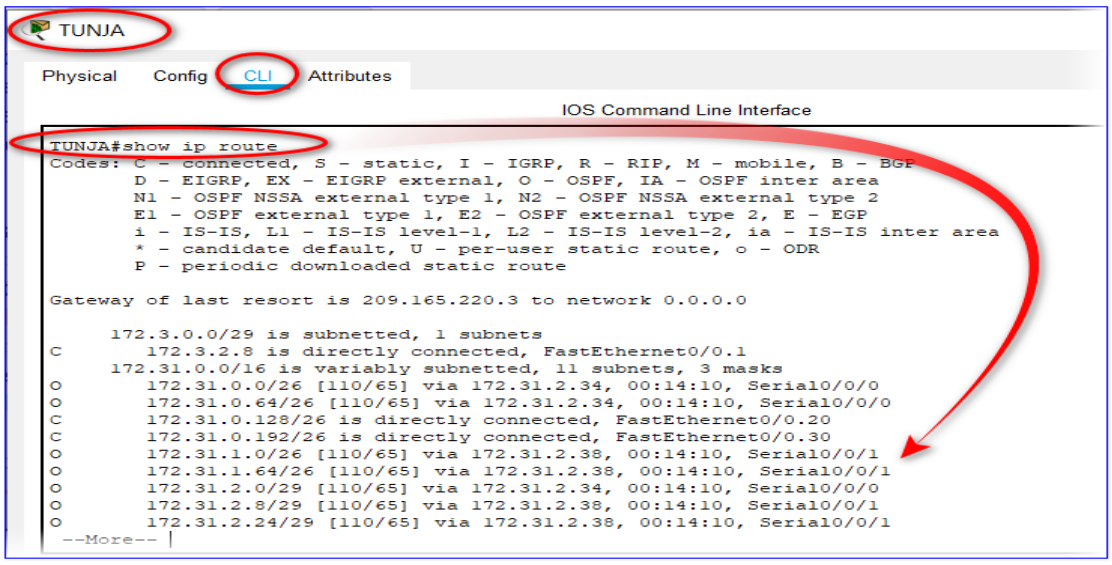


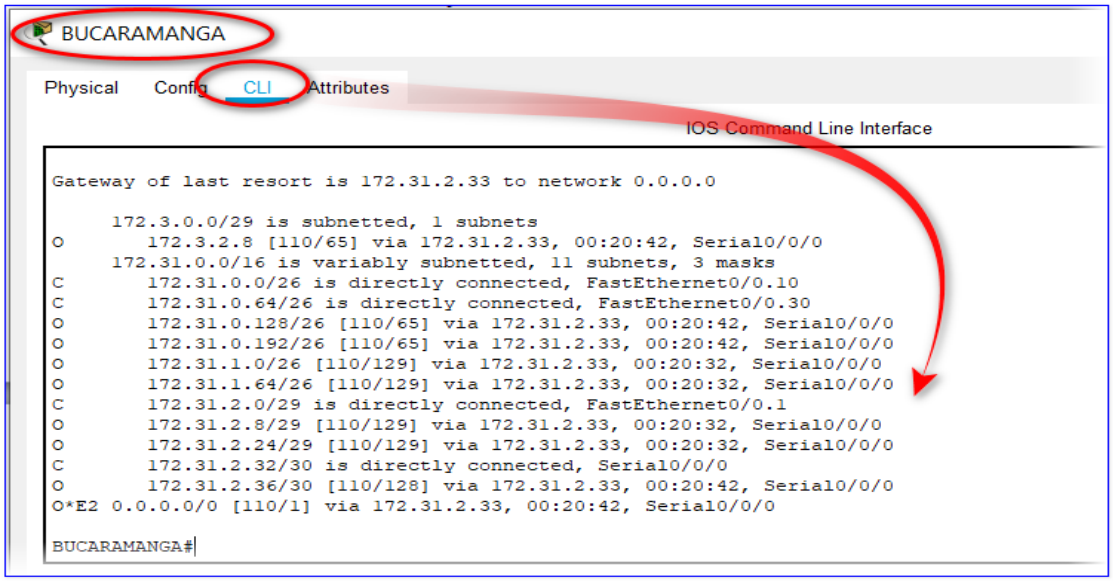

```
CUNDINAMARCA(config)#int f0/0.20
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#int f0/0.30
CUNDINAMARCA(config-subif)#ip helper-address 172.31.2.37
CUNDINAMARCA(config-subif)#end
CUNDINAMARCA#
```

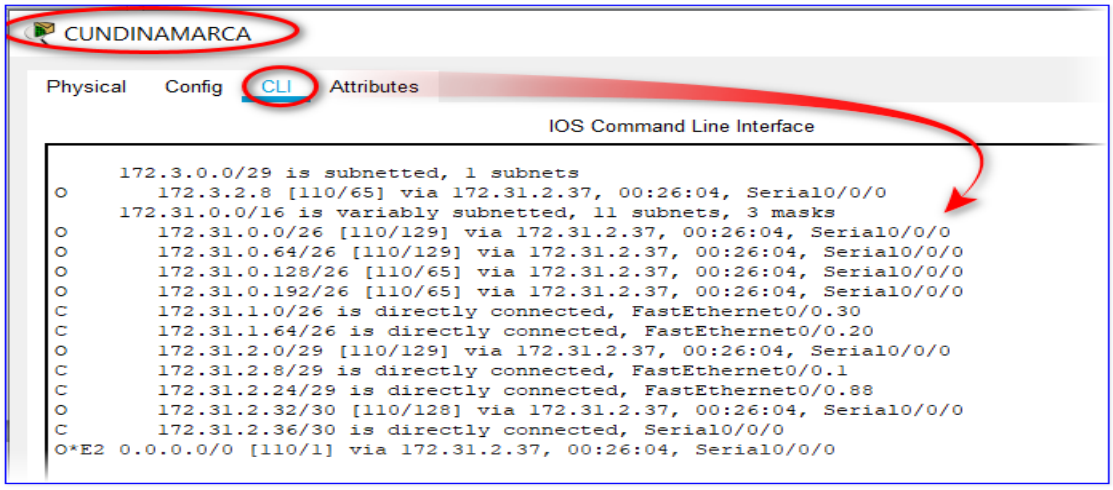


3. El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).

```
TUNJA(dhcp-config)#ip nat inside source static 172.31.2.28
209.165.220.4
TUNJA(config)#access-list 1 permit 172.0.0.0 0.255.255.255
TUNJA(config)#ip nat inside source list 1 interface f0/1
overload
TUNJA(config)#int f0/1
TUNJA(config-if)#ip nat outside
TUNJA(config-if)#int f0/0.1
TUNJA(config-subif)#ip nat inside
TUNJA(config-subif)#int f0/0.20
TUNJA(config-subif)#ip nat inside
TUNJA(config-subif)#int f0/0.30
TUNJA(config-subif)#ip nat inside
TUNJA(config-subif)#int s0/0/0
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#int s0/0/1
TUNJA(config-if)#ip nat inside
TUNJA(config-if)#exit
TUNJA(config)#ip route 0.0.0.0 0.0.0.0 209.165.220.3
TUNJA(config)#router ospf 1
TUNJA(config-router)#default-information originate
TUNJA(config-router)#
```


TUNJA
Physical
Config
CLI
Attributes
IOS Command Line Interface
TUNJA#show ip route
Codes: C - connected, S - static, I - IGRP, 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 209.165.220.3 to network 0.0.0.0
172.3.0.0/29 is subnetted, 1 subnets
C 172.3.2.8 is directly connected, FastEthernet0/0.1
172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks
O 172.31.0.0/26 [110/65] via 172.31.2.34, 00:14:10, Serial0/0/0
O 172.31.0.64/26 [110/65] via 172.31.2.34, 00:14:10, Serial0/0/0
C 172.31.0.128/26 is directly connected, FastEthernet0/0.20
C 172.31.0.192/26 is directly connected, FastEthernet0/0.30
O 172.31.1.0/26 [110/65] via 172.31.2.38, 00:14:10, Serial0/0/1
O 172.31.1.64/26 [110/65] via 172.31.2.38, 00:14:10, Serial0/0/1
O 172.31.2.0/29 [110/65] via 172.31.2.34, 00:14:10, Serial0/0/0
O 172.31.2.8/29 [110/65] via 172.31.2.38, 00:14:10, Serial0/0/1
O 172.31.2.24/29 [110/65] via 172.31.2.38, 00:14:10, Serial0/0/1
--More--

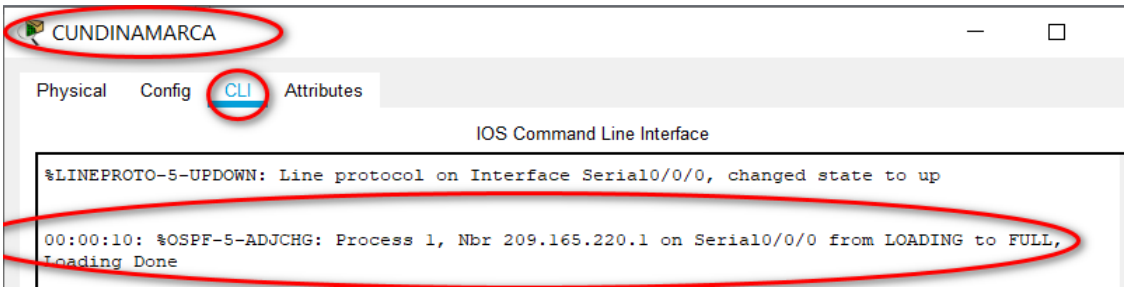

BUCARAMANGA
Physical
Config
CLI
Attributes
IOS Command Line Interface
Gateway of last resort is 172.31.2.33 to network 0.0.0.0
172.3.0.0/29 is subnetted, 1 subnets
O 172.3.2.8 [110/65] via 172.31.2.33, 00:20:42, Serial0/0/0
172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks
C 172.31.0.0/26 is directly connected, FastEthernet0/0.10
C 172.31.0.64/26 is directly connected, FastEthernet0/0.30
O 172.31.0.128/26 [110/65] via 172.31.2.33, 00:20:42, Serial0/0/0
O 172.31.0.192/26 [110/65] via 172.31.2.33, 00:20:42, Serial0/0/0
O 172.31.1.0/26 [110/129] via 172.31.2.33, 00:20:32, Serial0/0/0
O 172.31.1.64/26 [110/129] via 172.31.2.33, 00:20:32, Serial0/0/0
C 172.31.2.0/29 is directly connected, FastEthernet0/0.1
O 172.31.2.8/29 [110/129] via 172.31.2.33, 00:20:32, Serial0/0/0
O 172.31.2.24/29 [110/129] via 172.31.2.33, 00:20:32, Serial0/0/0
C 172.31.2.32/30 is directly connected, Serial0/0/0
O 172.31.2.36/30 [110/128] via 172.31.2.33, 00:20:42, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.31.2.33, 00:20:42, Serial0/0/0
BUCARAMANGA#


CUNDINAMARCA
Physical
Config
CLI
Attributes
IOS Command Line Interface
172.3.0.0/29 is subnetted, 1 subnets
O 172.3.2.8 [110/65] via 172.31.2.37, 00:26:04, Serial0/0/0
172.31.0.0/16 is variably subnetted, 11 subnets, 3 masks
O 172.31.0.0/26 [110/129] via 172.31.2.37, 00:26:04, Serial0/0/0
O 172.31.0.64/26 [110/129] via 172.31.2.37, 00:26:04, Serial0/0/0
O 172.31.0.128/26 [110/65] via 172.31.2.37, 00:26:04, Serial0/0/0
O 172.31.0.192/26 [110/65] via 172.31.2.37, 00:26:04, Serial0/0/0
C 172.31.1.0/26 is directly connected, FastEthernet0/0.30
C 172.31.1.64/26 is directly connected, FastEthernet0/0.20
O 172.31.2.0/29 [110/129] via 172.31.2.37, 00:26:04, Serial0/0/0
C 172.31.2.8/29 is directly connected, FastEthernet0/0.1
C 172.31.2.24/29 is directly connected, FastEthernet0/0.88
O 172.31.2.32/30 [110/128] via 172.31.2.37, 00:26:04, Serial0/0/0
C 172.31.2.36/30 is directly connected, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.31.2.37, 00:26:04, Serial0/0/0

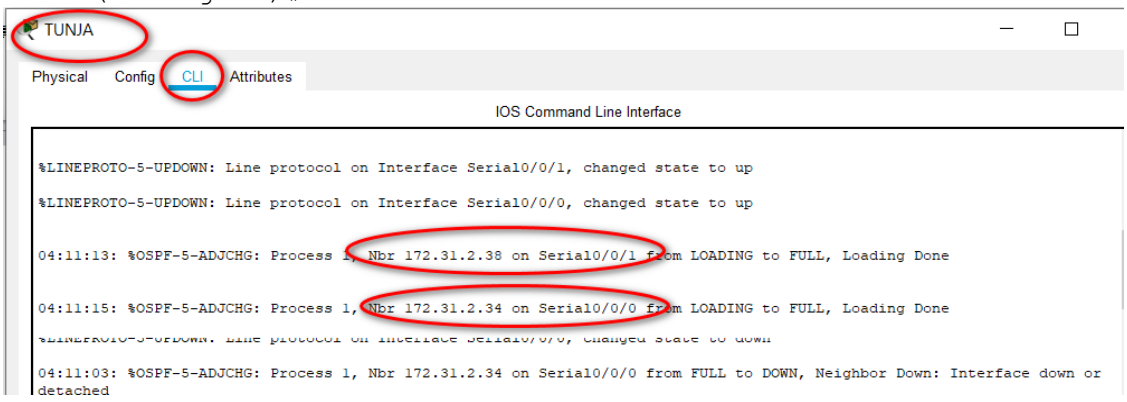
4. El enrutamiento deberá tener autenticación.

```
BUCARAMANGA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#int s0/0/0
BUCARAMANGA(config-if)#ip ospf authentication message-digest
BUCARAMANGA(config-if)#ip ospf message-digest-key 1 md5 cisco
BUCARAMANGA(config-if)#
```


```
CUNDINAMARCA(config)#int s0/0/0
CUNDINAMARCA(config-if)#ip ospf authentication message-digest
CUNDINAMARCA(config-if)#ip ospf message-digest-key 1 md5 cisco
CUNDINAMARCA(config-if)#
```



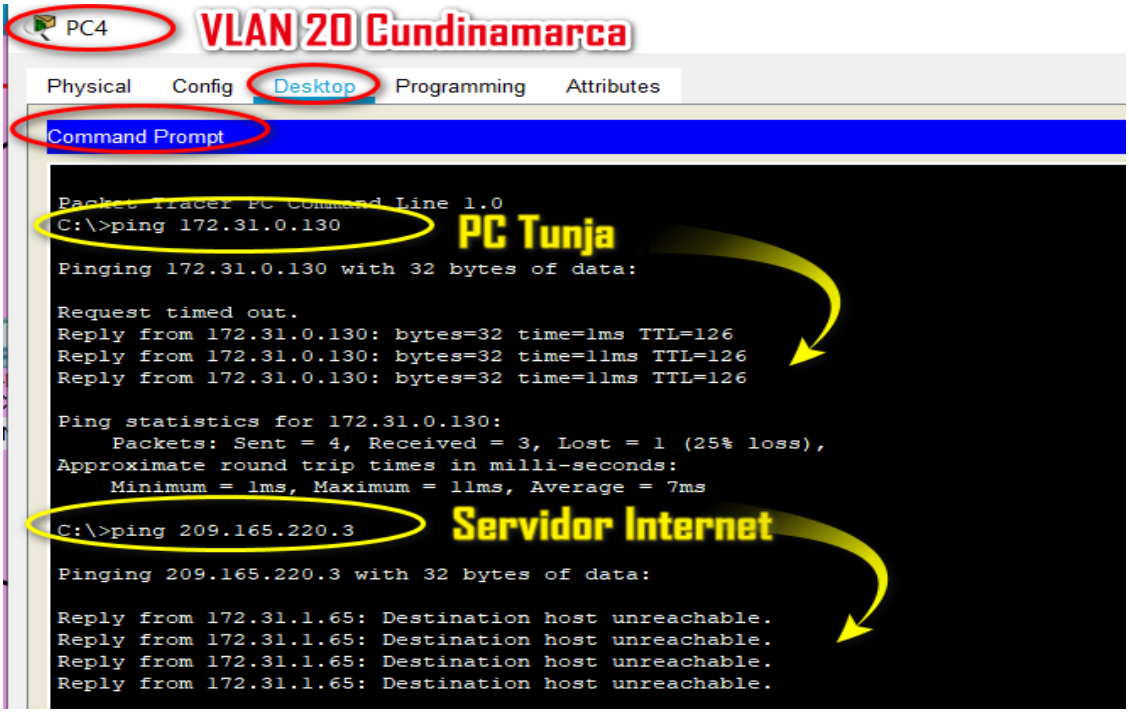

```
TUNJA(config)#int s0/0/0
TUNJA(config-if)#ip ospf authentication message-digest
TUNJA(config-if)#ip ospf message-digest-key 1 md5 cisco
TUNJA(config-if)#int s0/0/1
TUNJA(config-if)#ip ospf authentication message-digest
TUNJA(config-if)#ip ospf message-digest-key 1 md5 cisco
TUNJA(config-if)#
```



5. Listas de control de acceso:

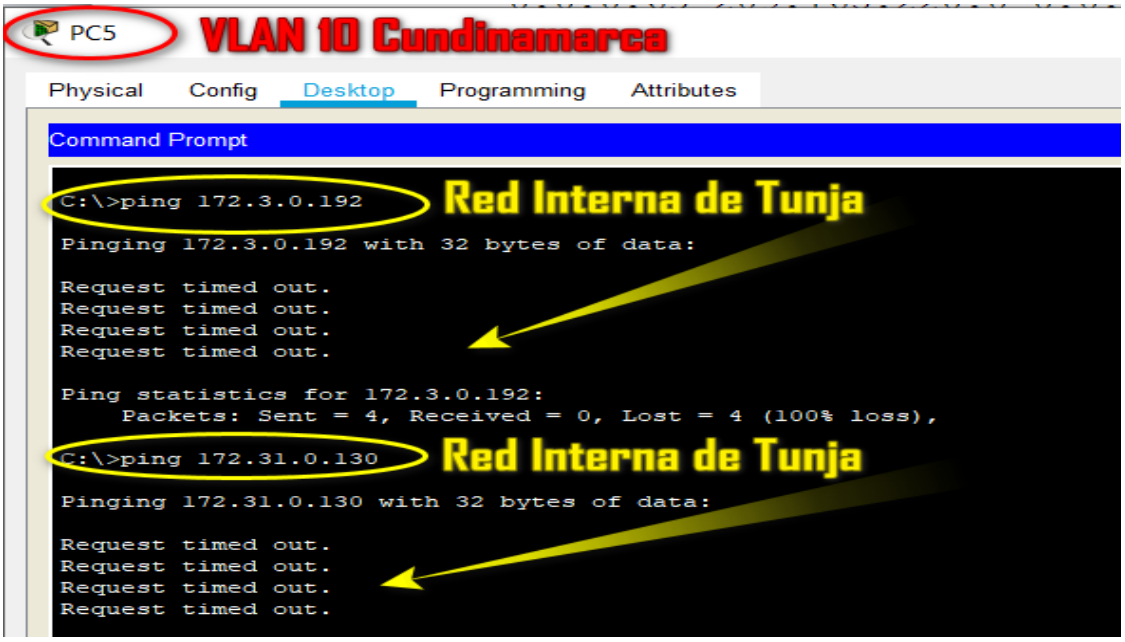
- Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.

```
CUNDINAMARCA(config-subif)#access-list 112 permit ip
172.31.1.0 0.0.0.63 209.165.220.0 0.0.0.255
CUNDINAMARCA(config)#access-list 112 deny ip any any
CUNDINAMARCA(config)#int f0/0.30
CUNDINAMARCA(config-subif)#ip access-group 112 in
CUNDINAMARCA(config-subif)#
```



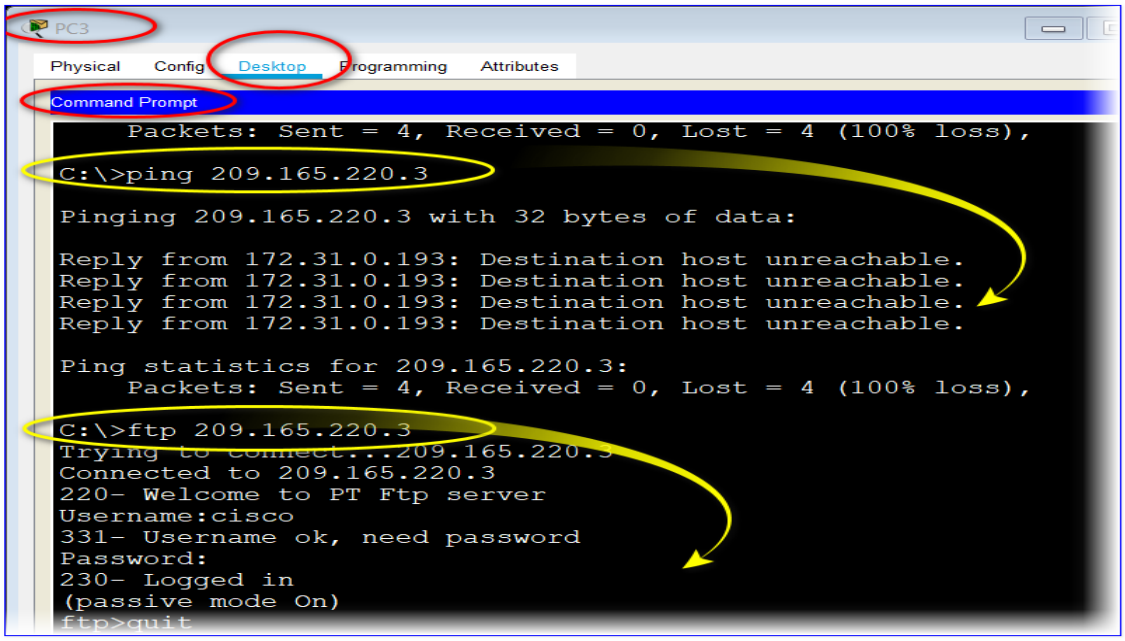
- Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja.

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



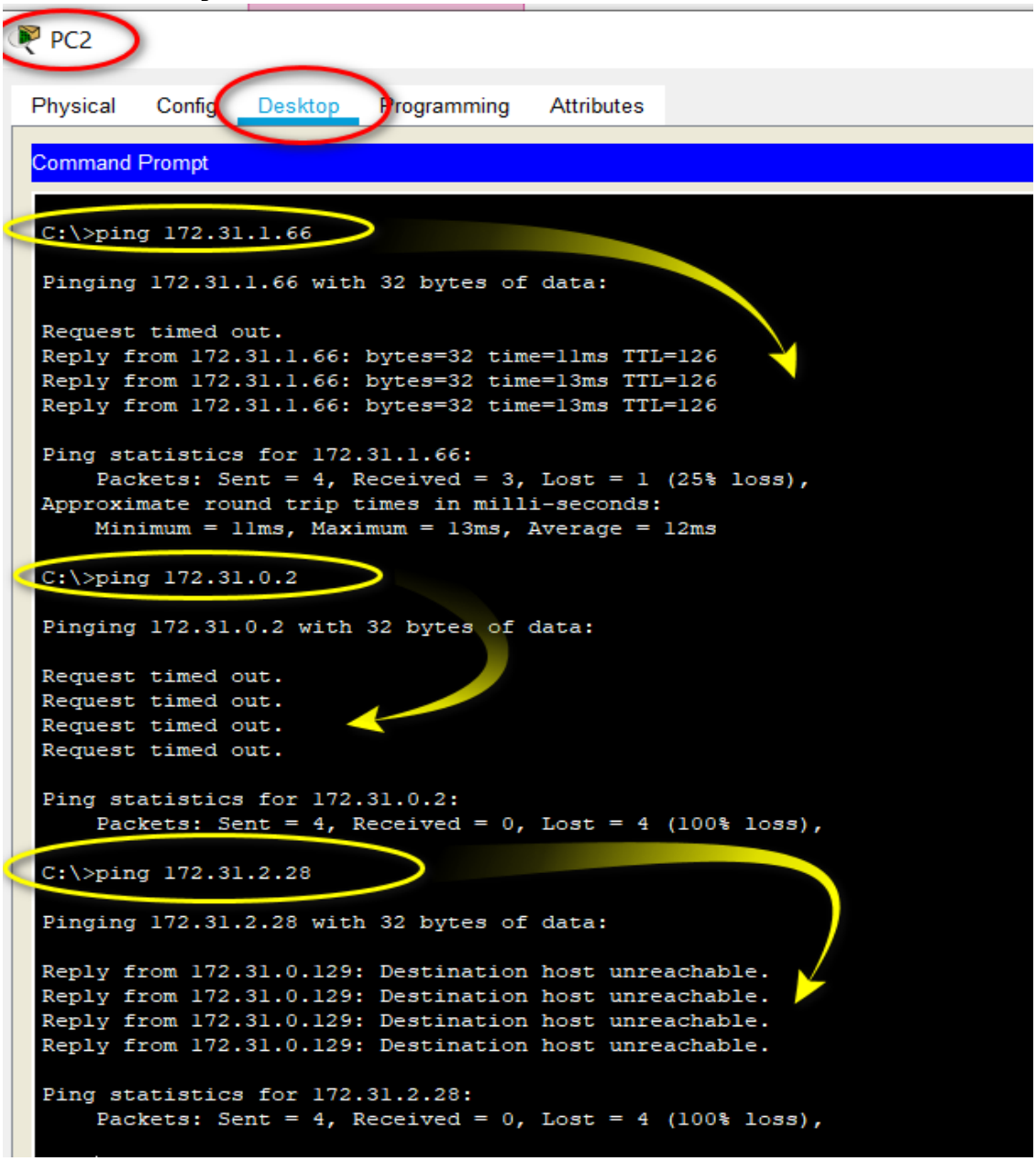
- Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.

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



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

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

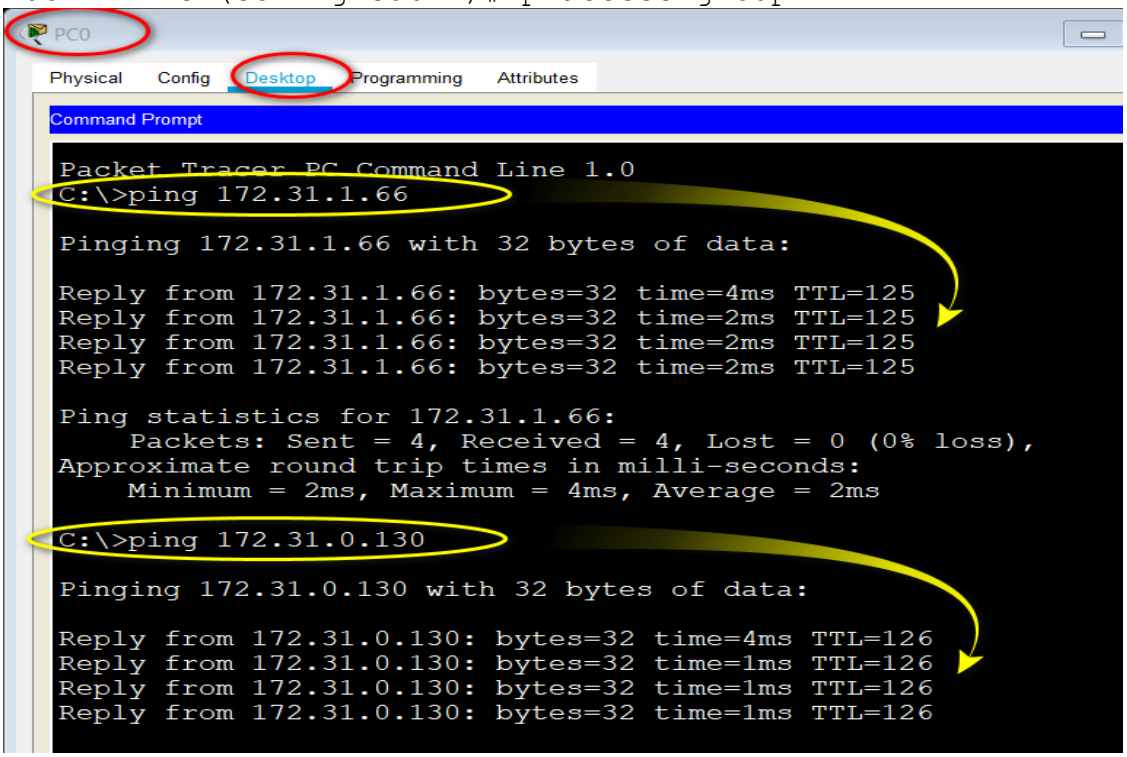


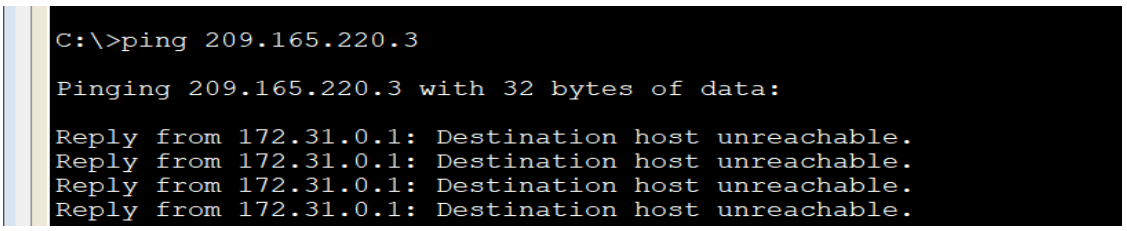
- Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.

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

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

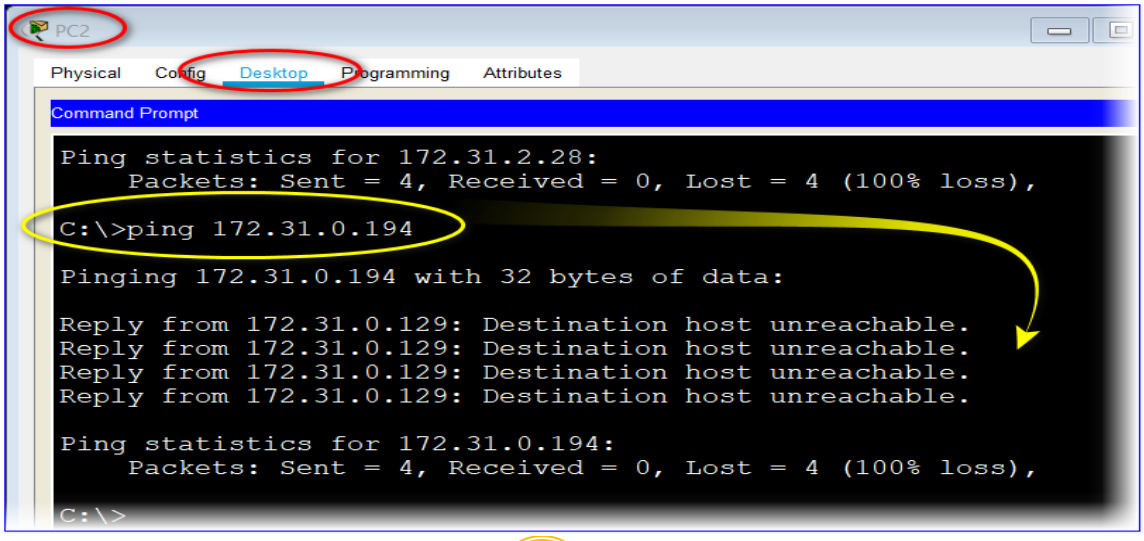
```
BUCARAMANGA(config-subif)#access-list 112 permit ip
172.31.0.0 0.0.0.63 172.31.1.64 0.0.0.63
BUCARAMANGA(config)#access-list 112 permit ip 172.31.0.0
0.0.0.63 172.31.0.128 0.0.0.63
BUCARAMANGA(config)#int f0/0.10
BUCARAMANGA(config-subif)#ip access-group 112 in
```





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

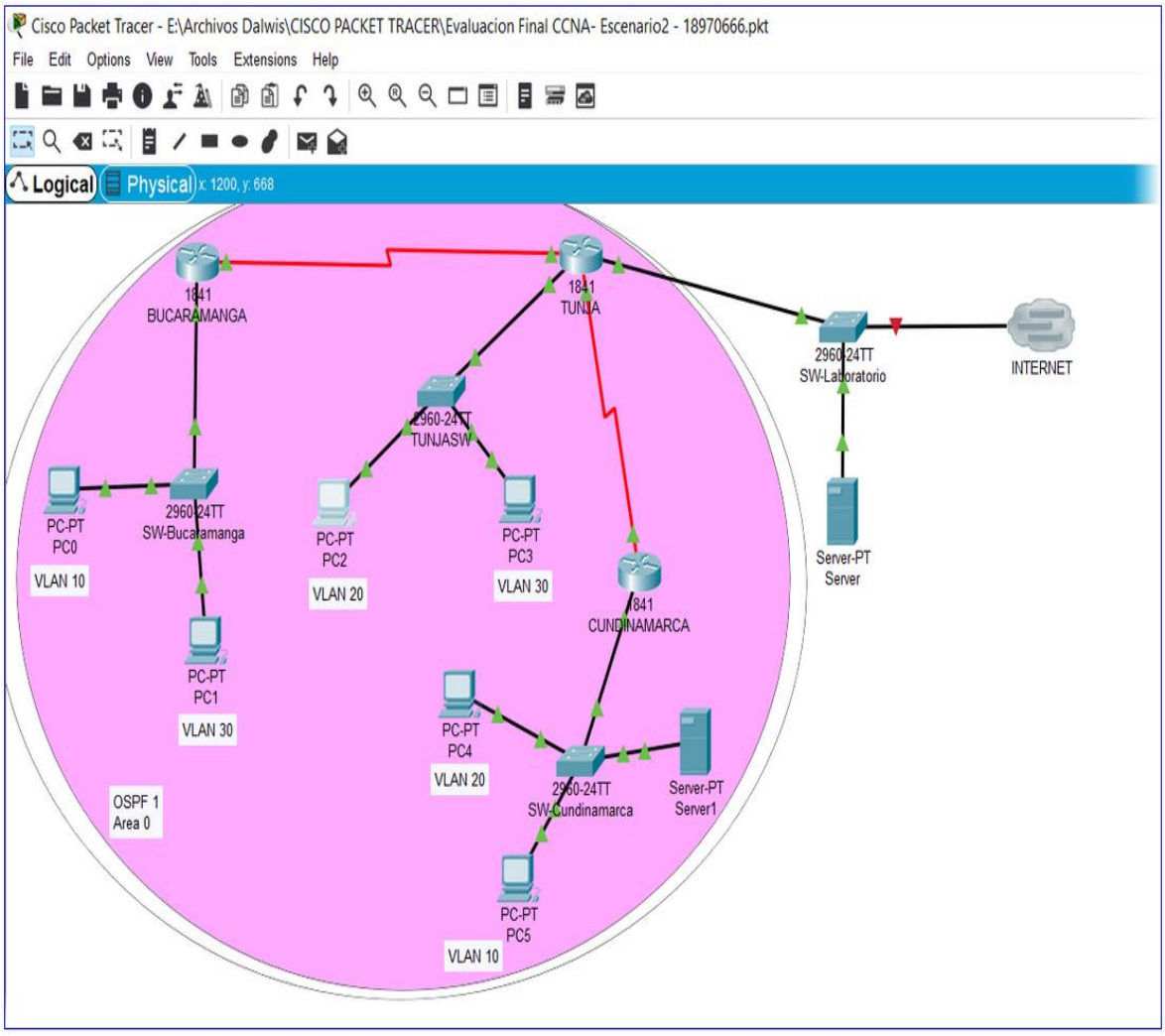
```
BUCARAMANGA(config-subif)#access-list 113 deny ip
172.31.2.0 0.0.0.7 172.31.0.0 0.0.0.63
BUCARAMANGA(config)#access-list 113 deny ip 172.31.0.64
0.0.0.63 172.31.0.0 0.0.0.63
BUCARAMANGA(config)#access-list 113 permit ip any any
BUCARAMANGA(config)#int f0/0.10
BUCARAMANGA(config-subif)#ip access-group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

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

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



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

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

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

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

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



CONCLUSIONES

Una vez culminada esta prueba de habilidades CCNA, en donde se desarrollaron dos (2) escenarios que nos permitieron conocer más del mundo de soluciones integradas LAN/WAN, utilizando herramientas de simulació, necesarios para instalar, operar y solucionar problemas de una red, incluyendo, los conceptos básicos que se utilizan en networking, la configuración de un switch, un router, y poderse conectarse a una red LAN.

Se construyeron topologías simple de red LAN mediante la aplicación de los principios básicos de cableado. Con configuraciones básicas de los dispositivos de red, incluyendo routers y switches e implementando esquemas de direccionamiento IP.

Se diseñaron modelos de redes jerárquicas, seleccionando los dispositivos que la conforman para cada capa. Identificó soluciones tecnológicas, de una red Ethernet, describiendo los problemas relacionados con el aumento del tráfico en una LAN Ethernet y su conmutación. También se utilizó la configuración, verificación de las VLAN, En donde se pudo constatar que el enrutamiento VLAN facilita la comunicación entre los dispositivos aislados por los límites de la VLAN.

Descripción de las razones para la conexión de redes con routers y cómo funcionan las redes de transmisión de datos con sus protocolos. Utilizando la interfaz de línea de comandos para descubrir y gestionar el arranque del router y su configuración. Como administrador de red, debe tener en cuenta que el acceso no debe estar disponible para otros usuarios de la red. Por lo tanto, se debe configurar y aplicar una ACL que permita el acceso de una computadora (PC) a las líneas Telnet, pero que deniegue el resto de las direcciones IPv4 de origen.

REFERENCIAS BIBLIOGRAFICAS

- CISCO. (2014). Exploración de la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

- CISCO. (2014). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1

- CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de:

  https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

- CISCO. (2014). Acceso a la red. Fundamentos de Networking. Recuperado de: https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1

- CISCO. (2014). Ethernet. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1

- CISCO. (2014). Capa de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1

- Vesga, J. (2014). Diseño y configuración de redes con Packet Tracer [OVA]. Recuperado de https://1drv.ms/u/s!AmlJYei-NT1IhgCT9VCtl_pLtPD9

- Vesga, J. (2019). Introducción al Laboratorio Remoto SmartLab [OVI]. Recuperado de http://hdl.handle.net/10596/24167