PRUEBAS DE HABILIDADES CCNA

DIPLOMADO DE PROFUNDIZACIÓN CISCO

(DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN/WAN)

PRESENTADO POR:
EMANUEL PIÑA FUNES

TUTOR

DIEGO EDISON RAMIREZ

DIRECTOR DE DIPLOMADO
PHD. JUAN CARLOS VEGA FERREIRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

BARRANQUILLA COLOMBIA

DIPLOMADO CISCO

DICIEMBRE, 2019

DEDICATORIA

Principalmente quiero dar gracias a Dios todo poderoso por regalarme la oportunidad de finalizar mis estudios, él me ha brindado la ciencia y la sabiduría para poder avanzar cada día , agradezco especialmente a mi madre que creyó en mi cuando más lo necesite y siempre me brindó su apoyo a toda mi familia que me han ayudado de una manera u otra y nunca han dejado de creer en mí , a mis compañeros de la UNAD que me brindaron fuerzas para continuar en cada escenario de la carrera, a mis amigos que siempre hubo una palabra de aliento y por supuesto agradecer a mis tutores de la universidad gracias infinitas a ellos que me han dado concejos que estuvieron allí para ayudarme cuando los desafíos parecían muy grandes pero gracias a sus enseñanzas y valores depositados en mí.

Contenido

Resumen

En el siguiente trabajo veremos el conocimiento del curso de Diplomado de profundización cisco empleado en dos escenarios donde veremos la destreza para resolver problemas ya de un ingeniero en el ámbito de redes , veremos las conectividades de router, switch y aun de servidores para dar vida a redes extendida en varias ciudades y lugares geológicamente distantes pero eso no será inconveniente para el éxito de las conexiones , veremos cómo desde un punto se accede a cada punto de la red y aun veremos cómo se configura la red para hacer restricciones aun dentro de ella , son 2 escenarios llenos de retos que darán grandeza a nuestros estudiantes ya que emplearan cada saber adquirido este semestre en este curso, pero no solo veremos 2 escenarios sino la destreza de cada futuro ingeniero ya que podremos mirar cada línea de código que demuestra e esfuerzo y dedicación de cada uno de ellos pero sobre todo veremos cada uno de los valores y enseñanzas sembrados en estudiantes de parte de la UNAD y sus tutores.

Abstract

The world of technology today brings us great challenges and the world of networks is no exception, then we will see the importance of networks for companies in two different scenarios but where success in connections are the only way forward, in the practical skills test we will put into practice each of the skills acquired in this our diploma we will see how through switch, routers and pc we can cover with the tasks entrusted, we will see the importance of each command and each command line.

In this work we will find each of the processes to provide a solution to what has been raised, for example, we will see the use of commands such as ping, tracer router, show ip route among others that will give truth to each step of the student and demonstrating the structure of the work itself , we will see the vlan configuration, we will see how the student gives AAA authentication and even encrypts each password, connectivity is essential and it can be seen as a network element has a configuration to connect or restrict access and we will still see how DHCP works and server manipulation, this grade work is worthy of the UNAD and each scenario tests the knowledge acquired thus giving a growth opportunity for the student.

Introducción

El mundo de tecnología hoy nos trae grandes desafíos y el mundo de las redes no son la excepción, a continuación veremos la importancia de las redes para las empresas en dos escenarios distintos pero donde el éxito en las conexione son el único camino a seguir, en la prueba de habilidades practicas vamos a poner en práctica cada una de las habilidades adquirida en este nuestro diplomado veremos como a través de switch, routers y pc podremos abarcar con las tareas encargadas, veremos la importancia de cada comando y de cada línea de comando.

En este trabajo encontraremos cada uno de los procesos para brindar solución a lo planteado como por ejemplo veremos el uso de comandos como ping, tracer router, show ip route entre otros que le darán veracidad a cada paso del estudiante y demostrando la estructura del trabajo mismo, veremos la configuración de vlan, veremos como el estudiante le da autentificación AAA y aun cifra cada contraseña, la conectividad es fundamental y se podrá ver como elemento de la red tiene una configuración para conectar o restringir accesos y aun veremos como los DHCP funcionan y manipulación de servidores, este trabajo de grado es digno de la UNAD y cada escenario ponen a prueba los saberes adquiridos dando así una oportunidad de crecimiento para el estudiante .

OBJETIVOS

Objetivo General:

Fomentar en el ingeniero de sistema la capacidad de crear y administrar redes sin importar la topología o el escenario, crear en el ingeniero la destreza de asignar direcciones ip que brinden un orden a cada elemento de la red y a su vez una fácil implementación de esta; Este diplomado cisco específicamente este trabajo le brindan al estudiante de ingeniería y futuro ingeniero la posibilidad de entender el mundo laboral y a lo que se va enfrentar en el día a día en el campo de las redes, ya que veremos la implementación de seguridad en la red, conectividad y aun segmentación de la red en cada uno de los escenario dándole así la formación correcta bajo los valores de la UNAD.

Objetivos Específicos:

- Configurar una red y cada uno de los elemento que la componen de manera optima
- Aprender a implementar la seguridad en las distintas redes.
- Brindar conectividad y óptimo funcionamiento a las distintas redes.
- Crear listas para tener un control de acceso en las redes

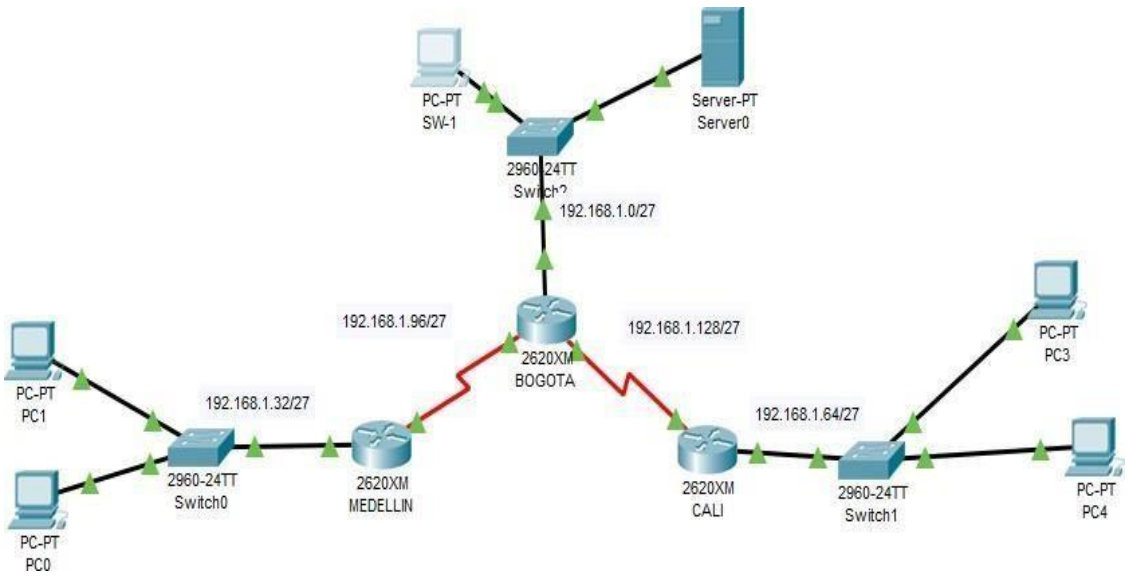
ESCENARIO 1

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.

TOPOLOGIA

3 ROUTERS 2620Mx
3 SWITCHS 2960-24TT
1 SERVIDOR
5 COMPUTADORES

Topología de la red



Asignación de Direcciones IP
Configuración Básica

Configuración de los routers con el comando ip route

BOGOTÁ

Router>ENABLE

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA
BOGOTA(config)#interface fastethernet 0/0
BOGOTA(config-if)#ip address 192.168.1.1 255.255.255.224
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#exit
BOGOTA(config)#interface serial 0/0
BOGOTA(config-if)#ip address 192.168.1.98 255.255.255.224
BOGOTA(config-if)#no shutdown
BOGOTA(config-if)#exit
BOGOTA(config)#interface serial0/1
BOGOTA(config-if)#ip address 192.168.1.130 255.255.255.224
BOGOTA(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1, changed state to down
BOGOTA(config-if)#exit
BOGOTA(config)#end

BOGOTA#enable
BOGOTA#config terminal

Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#ip route 192.168.1.64 255.255.255.224 192.168.1.131
BOGOTA(config)#ip route 192.168.1.32 255.255.255.224 192.168.1.99
BOGOTA(config)#exit
BOGOTA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...

MEDELLÍN

Router>enable
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MEDELLIN
MEDELLIN(config)#interface fastethernet 0/0
MEDELLIN(config-if)#ip address 192.168.1.33 255.255.255.224
MEDELLIN(config-if)#no shutdown
MEDELLIN(config-if)#exit
MEDELLIN(config)#interface s0/0
MEDELLIN(config-if)#ip address 192.168.1.99 255.255.255.224
MEDELLIN(config-if)#no shutdown
MEDELLIN(config-if)#
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
MEDELLIN(config-if)#exit
MEDELLIN(config)#end

MEDELLIN#enable
MEDELLIN#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#ip route 192.168.1.0 255.255.255.224 192.168.1.97
MEDELLIN(config)#ip route 192.168.1.64 255.255.255.224 192.168.1.97
MEDELLIN(config)#exit

MEDELLIN#
%SYS-5-CONFIG_I: Configured from console by console
MEDELLIN#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
MEDELLIN#

CALI

Router>enable
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CALI
CALI(config)#interface fastethernet0/0
CALI(config-if)#ip address 192.168.1.65 255.255.255.224
CALI(config-if)#no shutdown
CALI(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
CALI(config-if)#exit
CALI(config)#interface s0/0
CALI(config-if)#ip address 192.168.1.131 255.255.255.224
CALI(config-if)#no shutdown
CALI(config-if)#
%LINK-5-CHANGED: Interface Serial0/0, changed state to up
CALI(config-if)#exit
CALI(config)#end

CALI#enable

CALI#config terminal

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

CALI(config)#ip route 192.168.1.0 255.255.255.224 192.168.1.129

CALI(config)#ip route 192.168.1.32 255.255.255.224 192.168.1.129

CALI(config)#exit

CALI#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

CALI#

Asignación de direcciones IP Subneteo.

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

Tomo la red como se sugiere y la divido en 8 partes y cada parte en la red/27 con la máscara de subred perteneciente a /27, que es 255.255.255.224:

192.168.1.0/27

192.168.1.32/27

192.168.1.64/27

192.168.1.96/27

192.168.1.128/27

192.168.1.160/27

192.168.1.192/27

192.168.1.224/27

a. Asignar una dirección IP a la red.

La dirección que se le da a la red es la siguiente: 192.168.1.0/24

Asignación de contraseñas en routers

BOGOTA>enable
BOGOTA#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#enable secret cisco
BOGOTA(config)#line consol 0
BOGOTA(config-line)#password emanuel
BOGOTA(config-line)#login
BOGOTA(config-line)#exit

MEDELLIN>enable
MEDELLIN#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#enable secret cisco
MEDELLIN(config)#line consol 0
MEDELLIN(config-line)#password emanuel
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit

CALI>enable
CALI#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)# enable secret cisco
CALI(config)#line consol 0
CALI(config-line)#password emanuel
CALI(config-line)#login

CALI(config-line)#exit

CONFIGURANDO LOS ROUTERS PARA EL LINE VTY 0 4

BOGOTA>enable
Password:
BOGOTA#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#line vty 0 4
BOGOTA(config-line)#password cisco2
BOGOTA(config-line)#login
BOGOTA(config-line)#loggin synchronous
BOGOTA(config-line)#exit

MEDELLIN>enable
Password:
MEDELLIN#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#line vty 0 4
MEDELLIN(config-line)#password cisco2
MEDELLIN(config-line)#login
MEDELLIN(config-line)#loggin synchronous
MEDELLIN(config-line)#exit

CALI>enable
Password:
CALI#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#line vty 0 4
CALI(config-line)#password cisco2
CALI(config-line)#login
CALI(config-line)#loggin synchrounous
CALI(config-line)#loggin synchronous
CALI(config-line)#exit

Parte 2: Configuración Básica.

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>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 type2
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, 05:26:26, Serial0/0
D 192.168.1.64 [90/2172416] via 192.168.1.131, 05:26:23, Serial0/1
C 192.168.1.96 is directly connected, Serial0/0
C 192.168.1.128 is directly connected, Serial0/1

MEDELLIN>enable
Password:
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 type2
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, 05:31:25, Serial0/0
C 192.168.1.32 is directly connected, FastEthernet0/0
D 192.168.1.64 [90/2684416] via 192.168.1.98, 05:31:22, Serial0/0
C 192.168.1.96 is directly connected, Serial0/0
D 192.168.1.128 [90/2681856] via 192.168.1.98, 05:31:25, Serial0/0

CALI>enable
Password:
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 type2
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, 05:32:24, Serial0/0
D 192.168.1.32 [90/2684416] via 192.168.1.130, 05:32:24, Serial0/0
C 192.168.1.64 is directly connected, FastEthernet0/0
D 192.168.1.96 [90/2681856] via 192.168.1.130, 05:32:24, Serial0/0
C 192.168.1.128 is directly connected, Serial0/0

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

MEDELLIN

MEDELLIN>enable
Password:
MEDELLIN#show ip eigrp topology

IP-EIGRP Topology Table for AS 1/ID(192.168.1.99)

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

P 192.168.1.0/27, 1 successors, FD is 2172416
via 192.168.1.98 (2172416/28160), Serial0/0
P 192.168.1.32/27, 1 successors, FD is 28160
via Connected, FastEthernet0/0
P 192.168.1.64/27, 1 successors, FD is 2684416
via 192.168.1.98 (2684416/2172416), Serial0/0
P 192.168.1.96/27, 1 successors, FD is 2169856
via Connected, Serial0/0
P 192.168.1.128/27, 1 successors, FD is 2681856
via 192.168.1.98 (2681856/2169856), Serial0/0

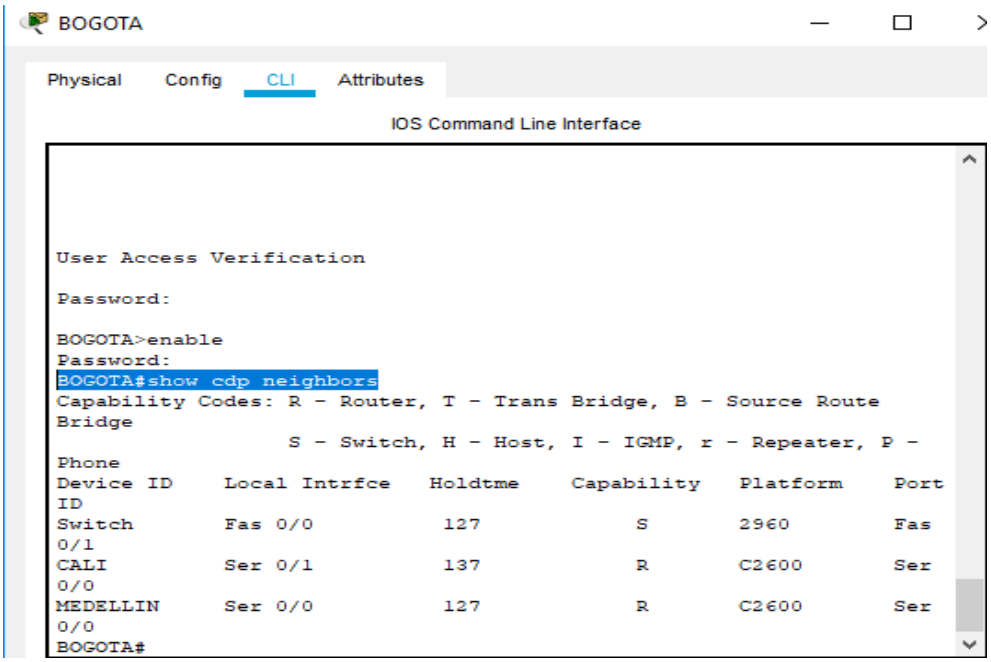
BOGOTA

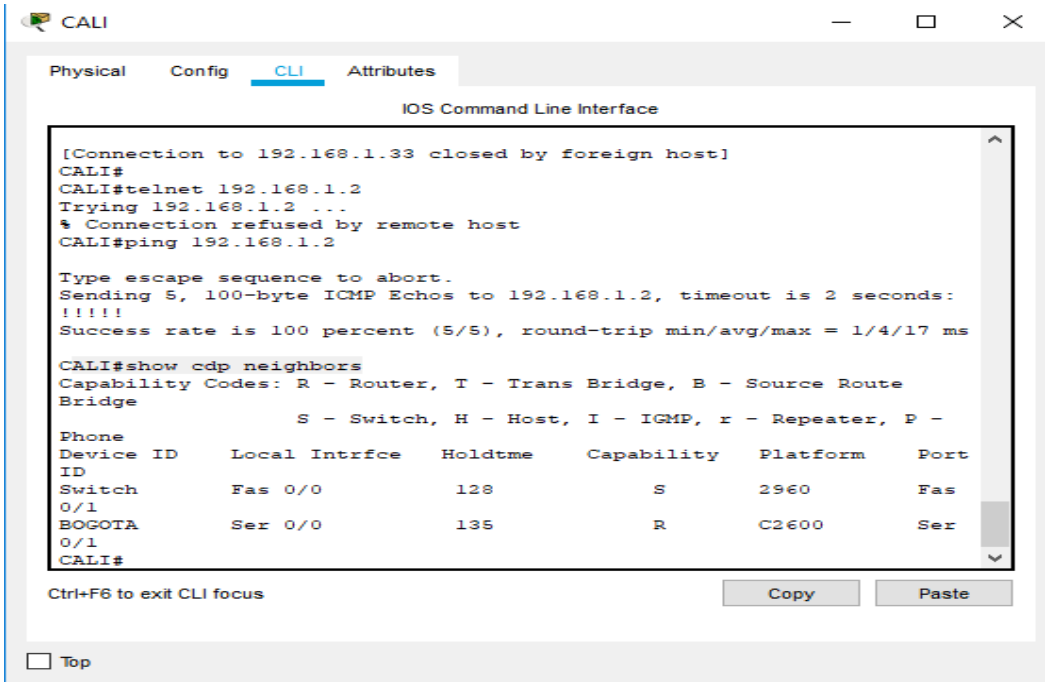
BOGOTA>enable
Password:
BOGOTA#show ip eigrp topology
IP-EIGRP Topology Table for AS 1/ID(192.168.1.130)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status
P 192.168.1.0/27, 1 successors, FD is 28160
via Connected, FastEthernet0/0
P 192.168.1.32/27, 1 successors, FD is 2172416
via 192.168.1.99 (2172416/28160), Serial0/0
P 192.168.1.64/27, 1 successors, FD is 2172416
via 192.168.1.131 (2172416/28160), Serial0/1
P 192.168.1.96/27, 1 successors, FD is 2169856
via Connected, Serial0/0
P 192.168.1.128/27, 1 successors, FD is 2169856
via Connected, Serial0/1

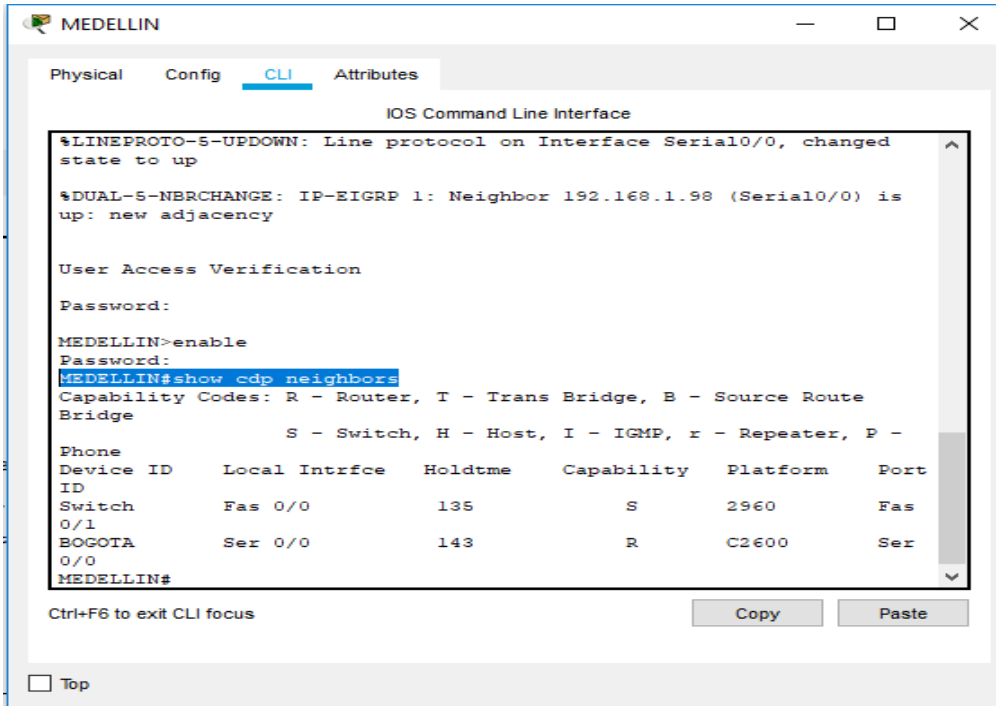
CALI

```
CALI>enable
Password:
CALI#show ip eigrp topology
IP-EIGRP Topology Table for AS 1/ID(192.168.1.131)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - Reply status
P 192.168.1.0/27, 1 successors, FD is 2172416
via 192.168.1.130 (2172416/28160), Serial0/0
P 192.168.1.32/27, 1 successors, FD is 2684416
via 192.168.1.130 (2684416/2172416), Serial0/0
P 192.168.1.64/27, 1 successors, FD is 28160
via Connected, FastEthernet0/0
P 192.168.1.96/27, 1 successors, FD is 2681856
via 192.168.1.130 (2681856/2169856), Serial0/0
P 192.168.1.128/27, 1 successors, FD is 2169856
via Connected, Serial0/0
```

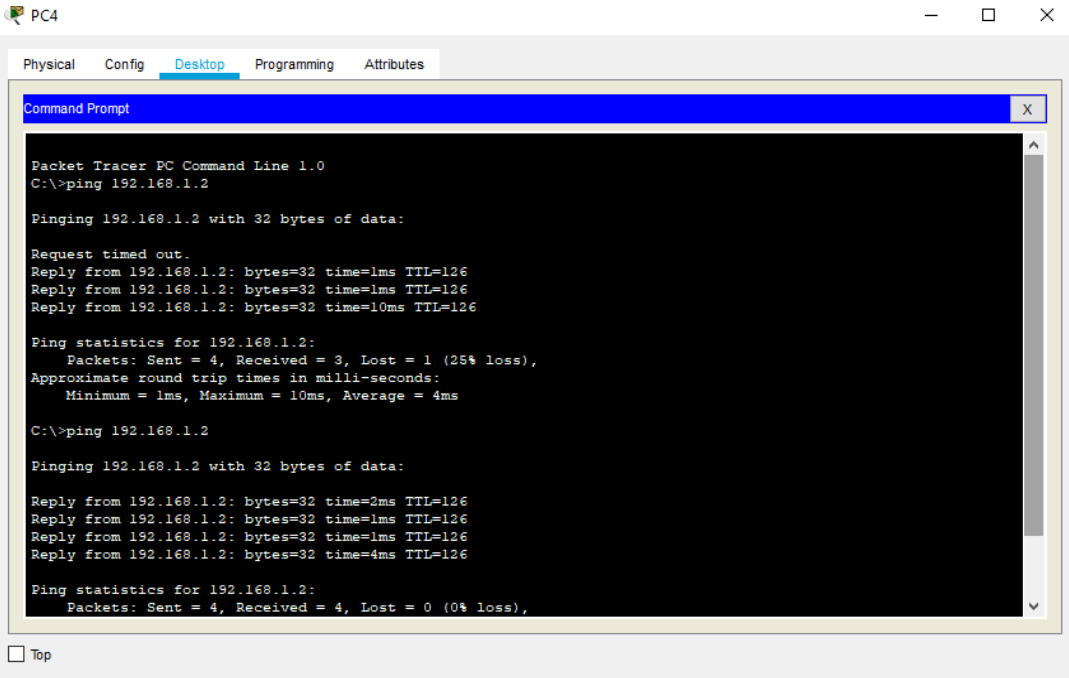
d. Realizar un diagnóstico de vecinos usando el comando cdp.

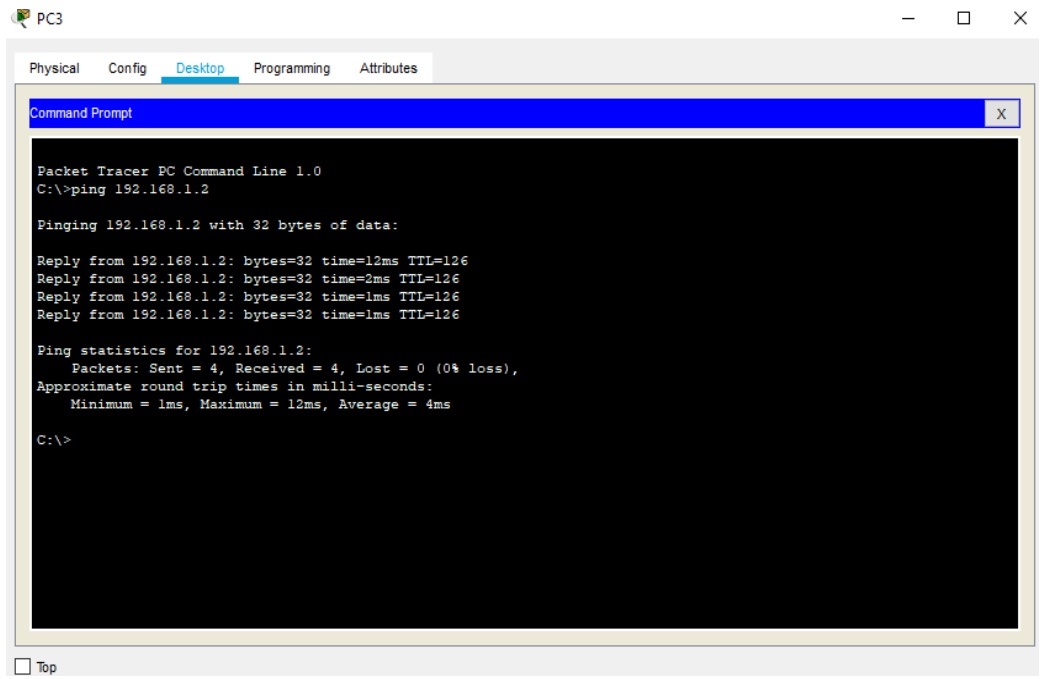



CALI
Physical
Config
CLI
Attributes
IOS Command Line Interface
[Connection to 192.168.1.33 closed by foreign host]
CALI#
CALI#telnet 192.168.1.2
Trying 192.168.1.2 ...
% Connection refused by remote host
CALI#ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/17 ms
CALI#show 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
Switch Fas 0/0 128 S 2960 Fas
0/1
BOGOTA Ser 0/0 135 R C2600 Ser
0/1
CALI#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

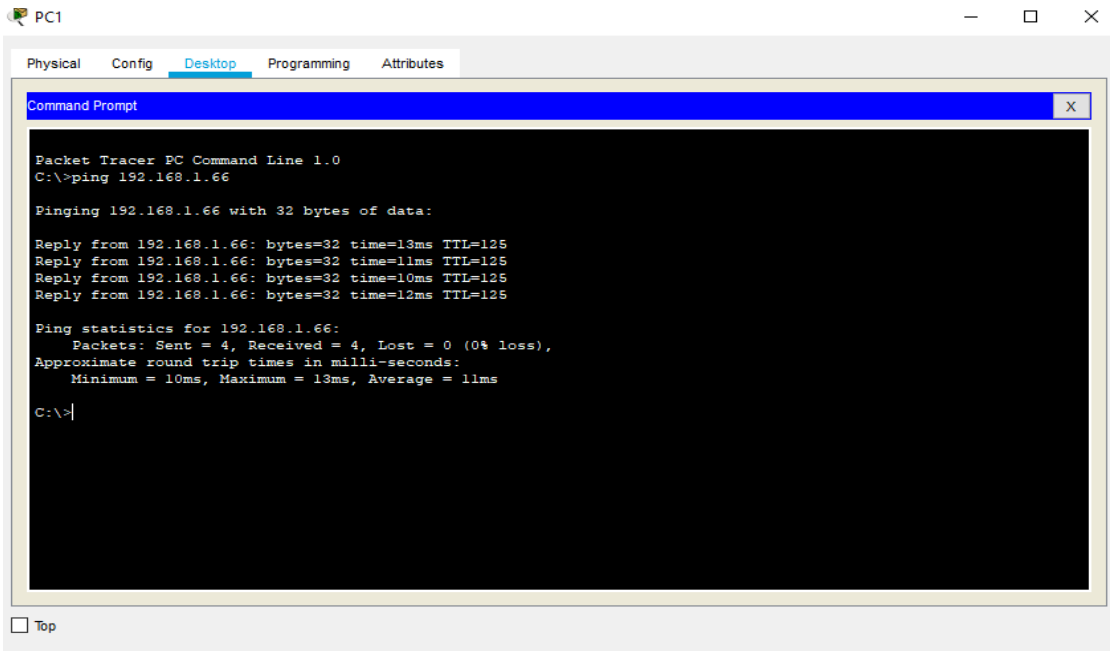

MEDELLIN
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed
state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.1.98 (Serial0/0) is
up: new adjacency
User Access Verification
Password:
MEDELLIN>enable
Password:
MEDELLIN#show 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
Switch Fas 0/0 135 S 2960 Fas
0/1
BOGOTA Ser 0/0 143 R C2600 Ser
0/0
MEDELLIN#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

e. Realizar una prueba de conectividad en cada tramo de la ruta usando Ping. ping de Cali a Bogotá.

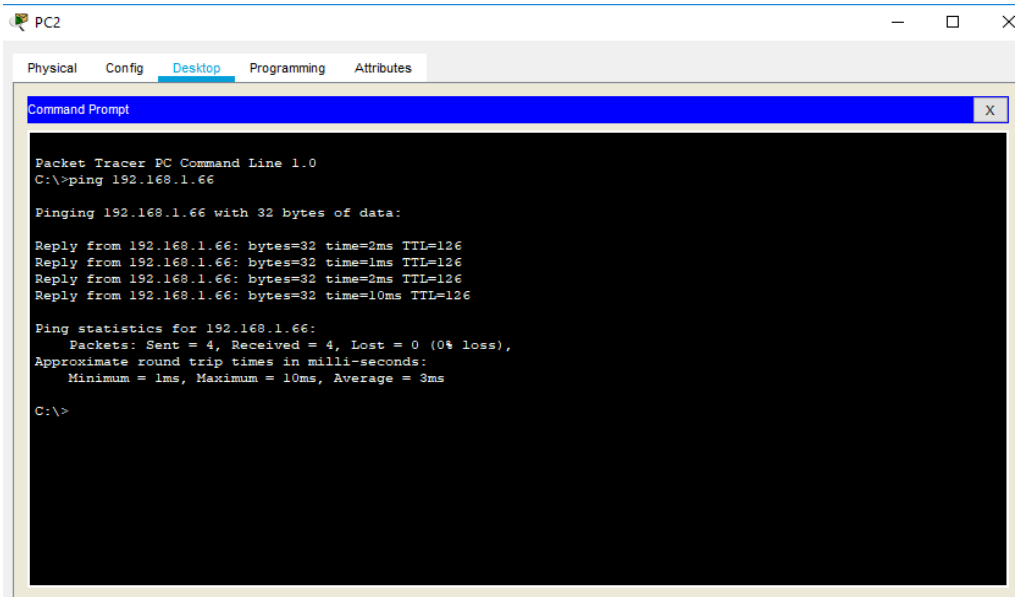


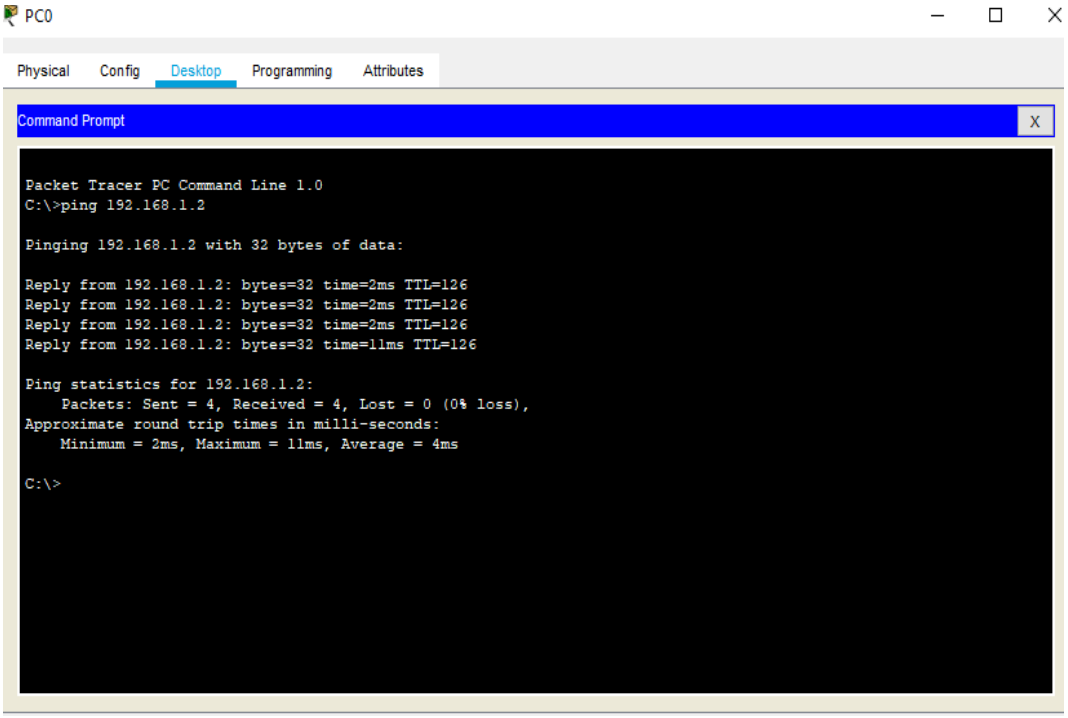


Medellín a Cali

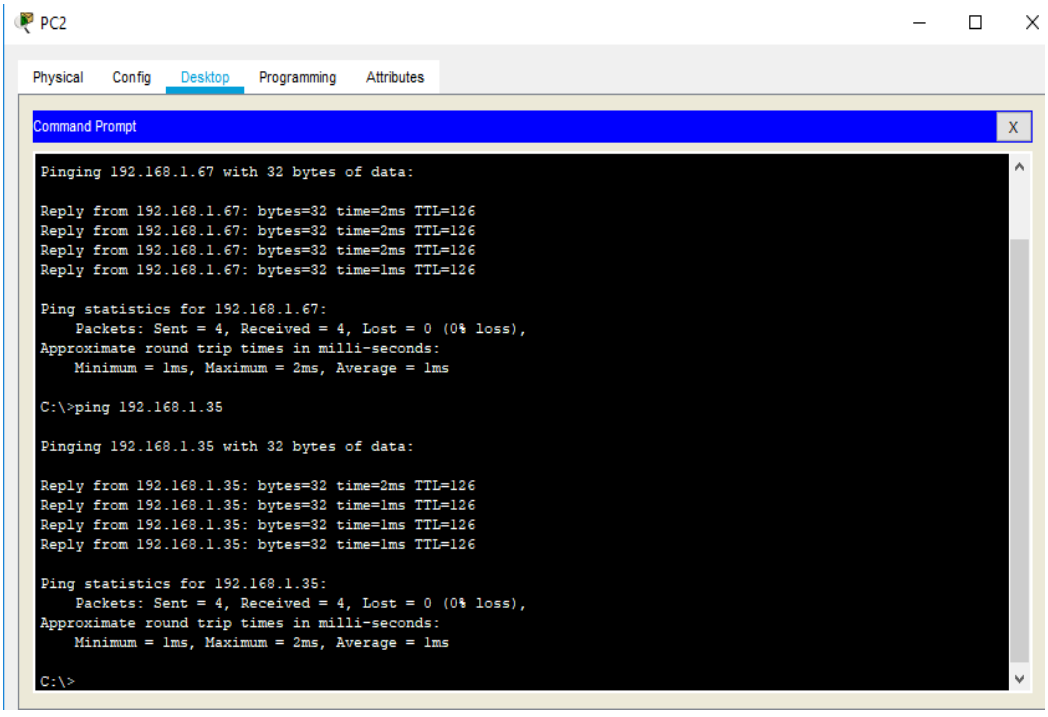


Medellín a Bogotá

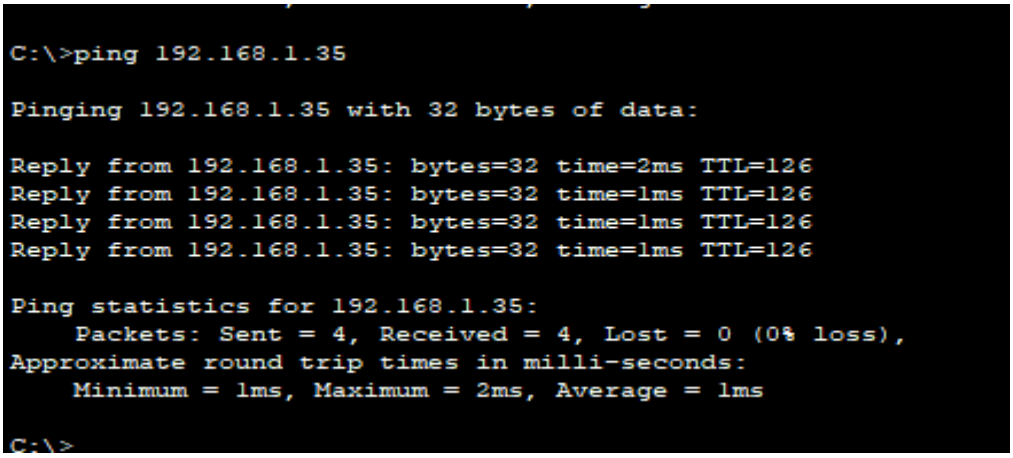




Bogotá a Cali



Bogotá a Medellín



Parte 3: Configuración de Enrutamiento.

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

BOGOTA>enable

BOGOTA#config terminal

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

BOGOTA(config)#router eigrp 200

BOGOTA(config-router)#no auto-summary

BOGOTA(config-router)#network 192.168.1.96

BOGOTA(config-router)#network 192.168.1.0

BOGOTA(config-router)#network 192.168.1.128

BOGOTA(config-router)#end

MEDELLIN>ENABLE

MEDELLIN#config terminal

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

MEDELLIN(config)#router eigrp 200

MEDELLIN(config-router)#no auto-summary

MEDELLIN(config-router)#network 192.168.1.32

Router(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.1.98 (Serial0/0) is up: new adjacency

MDELLIN(config-router)#network 192.168.1.32
MEDELLIN(config-router)#network 192.168.1.96
MEDELLIN(config-router)#end

CALI>enable
CALI#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#router eigrp 200
CALI(config-router)#no auto-summary
CALI(config-router)#network 192.168.1.128
Router(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.1.130 (Serial0/0) is up: new adjacency

CALI(config-router)#network 192.168.1.128
CALI(config-router)#network 192.168.1.64
CALI(config-router)#end
CALI#

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

MEDELLIN>enable

Password:
MEDELLIN#show ip eigrp neighbors
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 13 00:08:19 40 1000 0 8

CALI>enable

Password:
CALI#show ip eigrp neighbors
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 13 00:08:19 40 1000 0 8

BOGOTA>enable

Password:
BOGOTA#show ip eigrp neighbors
IP-EIGRP neighbors for process 200
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 192.168.1.131 Se0/1 13 00:06:44 40 1000 0 7
1 192.168.1.99 Se0/0 10 00:06:43 40 1000 0 7

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

MEDELLIN>enable

Password:
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 type2
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, 00:11:32, Serial0/0
C 192.168.1.32 is directly connected, FastEthernet0/0
D 192.168.1.64 [90/2684416] via 192.168.1.98, 00:11:32, Serial0/0
C 192.168.1.96 is directly connected, Serial0/0
D 192.168.1.128 [90/2681856] via 192.168.1.98, 00:11:32, Serial0/0

BOGOTA>enable

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 type2
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 interarea
* - 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, 00:13:26, Serial0/0
D 192.168.1.64 [90/2172416] via 192.168.1.131, 00:13:28, Serial0/1
C 192.168.1.96 is directly connected, Serial0/0
C 192.168.1.128 is directly connected, Serial0/1

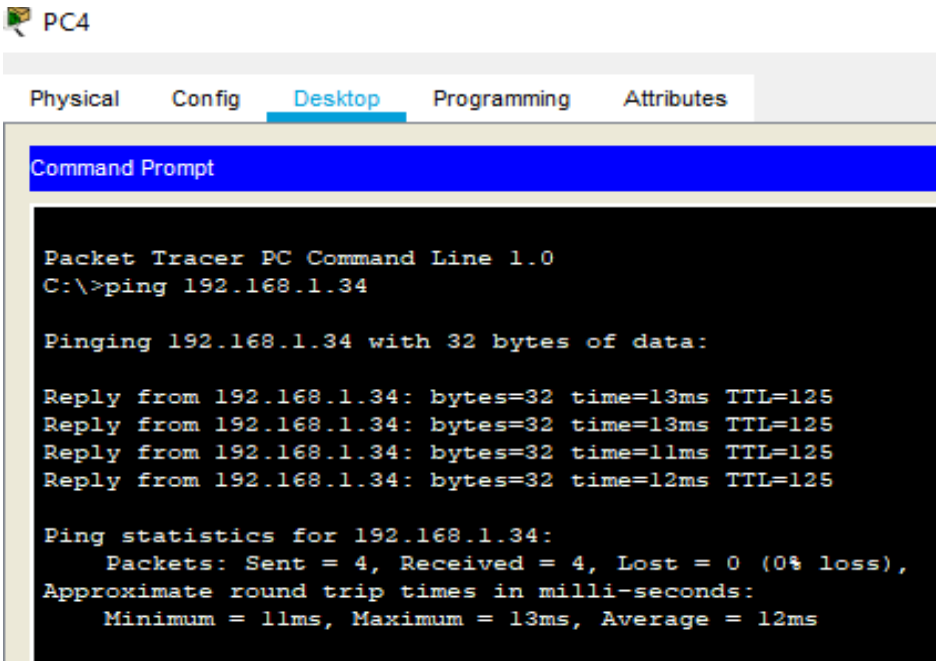
CALI>enable

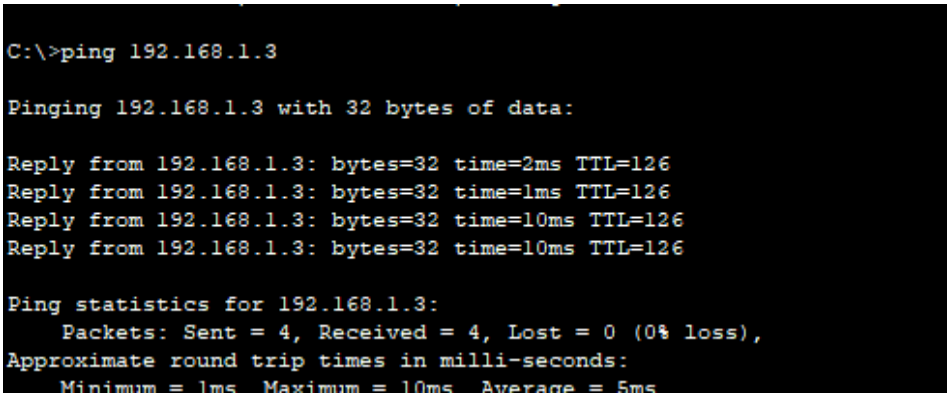
Password:
CALI#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

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, 00:14:20, Serial0/0
D 192.168.1.32 [90/2684416] via 192.168.1.130, 00:14:18, Serial0/0
C 192.168.1.64 is directly connected, FastEthernet0/0
D 192.168.1.96 [90/2681856] via 192.168.1.130, 00:14:18, Serial0/0
C 192.168.1.128 is directly connected, Serial0/0

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.





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

Configuración de las acl

Esto es para permitir solo acceso hacia el servidor

MEDELLIN>enable

Password:

MEDELLIN#configure terminal

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

MEDELLIN(config)#ip access-list extended ServerPT

MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.3 0.0.0.0

MEDELLIN(config-ext-nacl)#exit

MEDELLIN(config)#interface fa0/0

MEDELLIN(config-if)#ip access-group ServerPT in

MEDELLIN(config-if)#end

CALI>enable

Password:

CALI#config terminal

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

CALI(config)#ip access-list extended ServerPT

CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.3 0.0.0.0

CALI(config-ext-nacl)#exit

CALI(config)#int fa0/0

CALI(config-if)#ip access-group ServerPT in

CALI(config-if)#end

BOGOTA>enable

Password:

BOGOTA#config terminal

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

BOGOTA(config)#ip access-list extended ServerPT

BOGOTA(config-ext-nacl)#permit ip 192.168.1.3 0.0.0.0 0.0.0.0 255.255.255.255

BOGOTA(config-ext-nacl)#exit

BOGOTA(config)#interface fa0/0

BOGOTA(config-if)#ip access-group ServerPT in

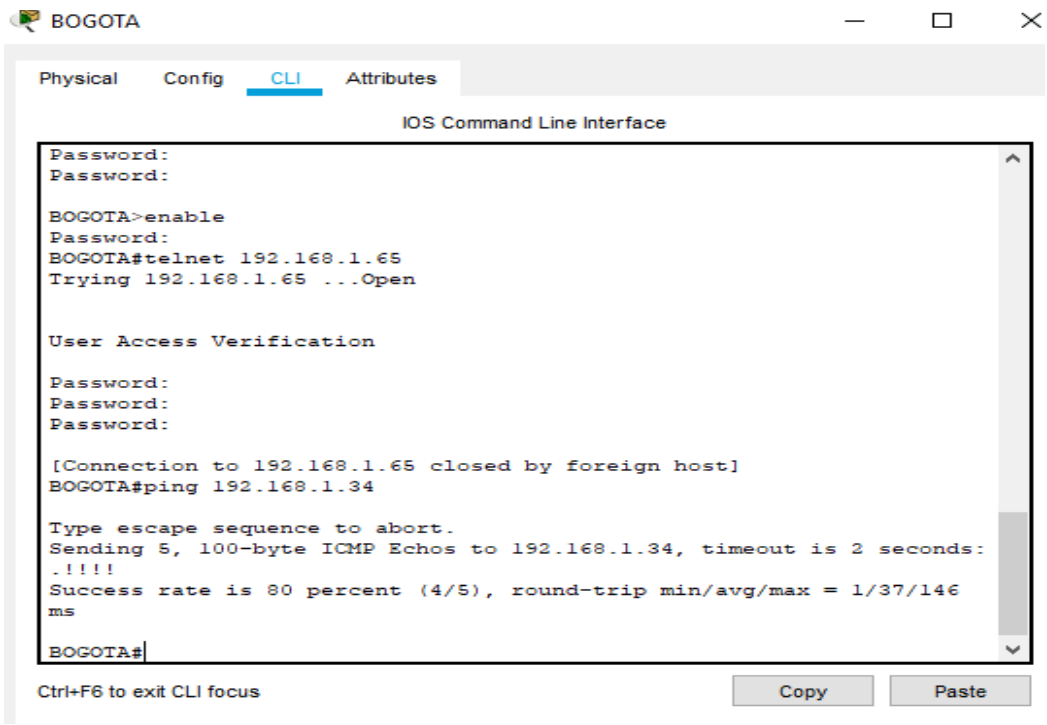
BOGOTA(config-if)#end

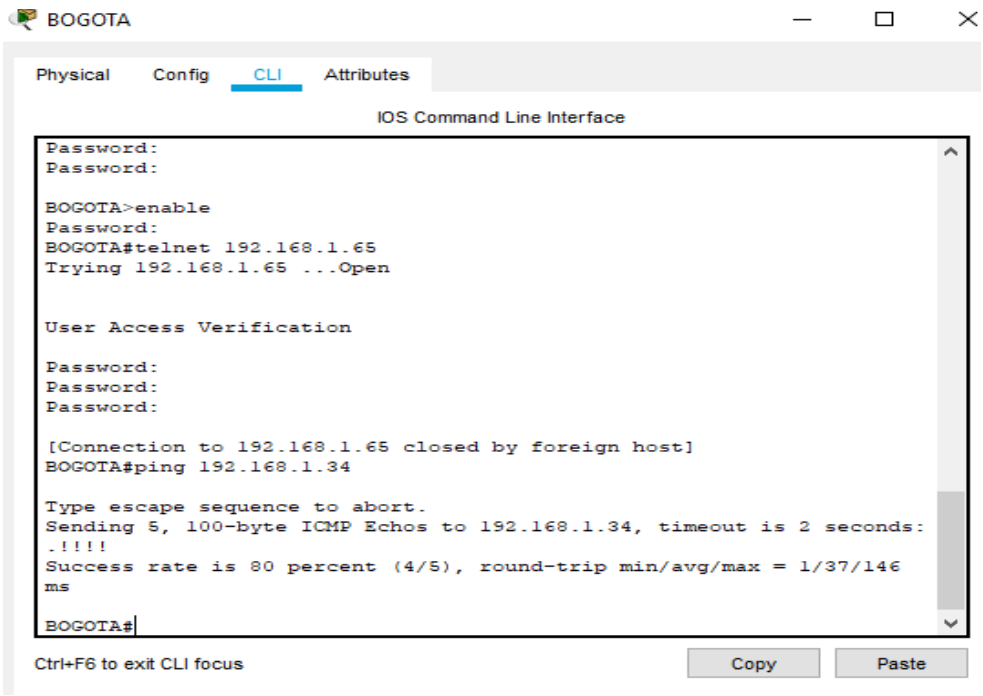
MEDELLIN>enable
Password:
MEDELLIN#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#ip access-list extended ServerPT
MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.33 0.0.0.0
MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.98 0.0.0.0
MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.131 0.0.0.0
MEDELLIN(config-ext-nacl)#end

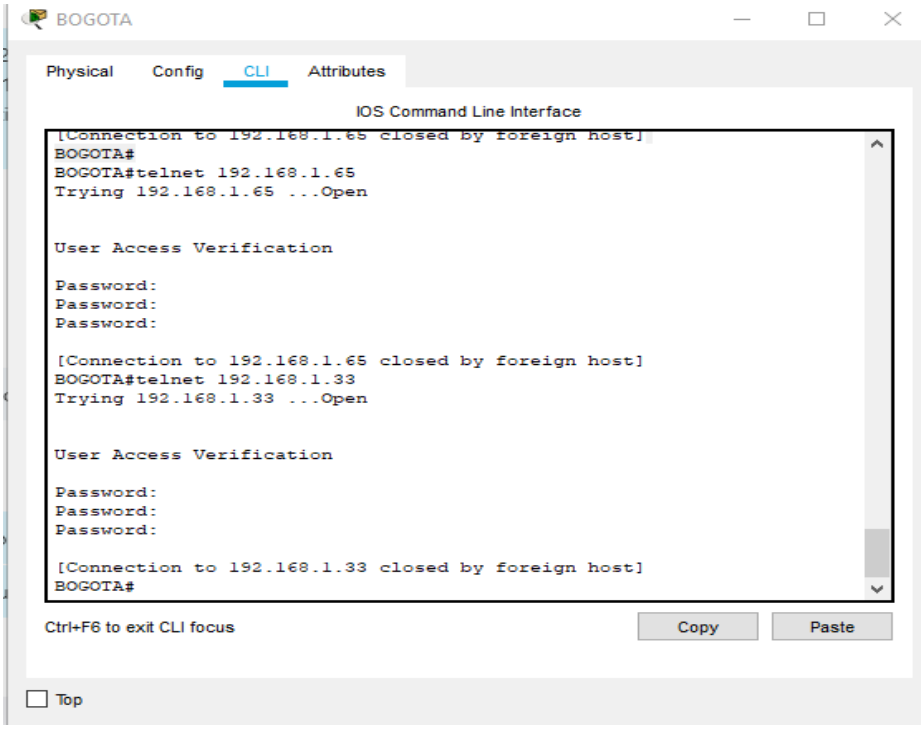
BOGOTA#

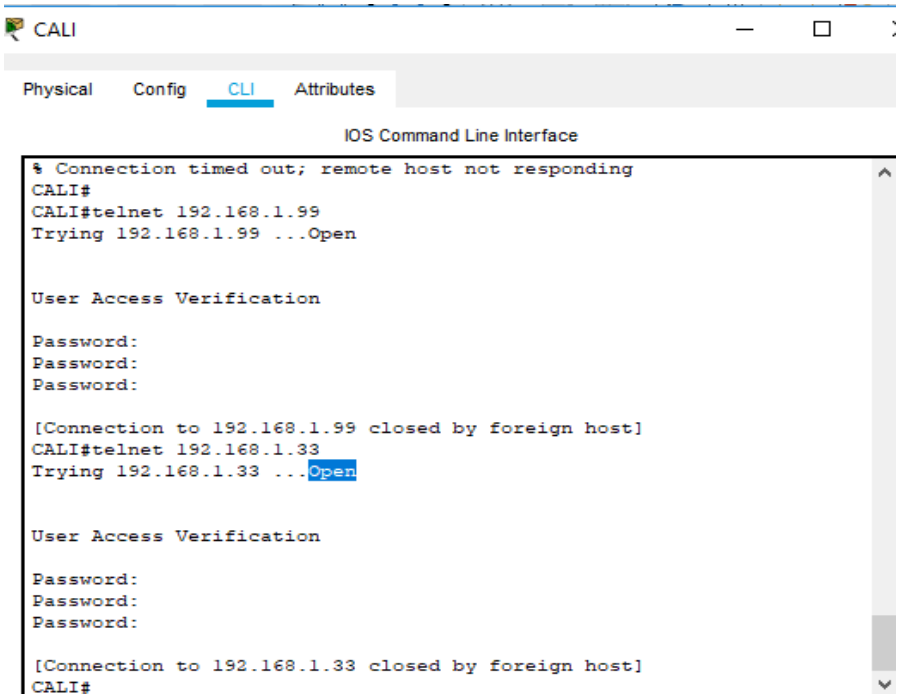
BOGOTA#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#ip access-list extended ServerPT
BOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.99 0.0.0.0
BOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.1 0.0.0.0
BOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.131 0.0.0.0
BOGOTA(config-ext-nacl)#end

CALI>enable
Password:
Password:
CALI#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#ip access-list extended ServerPT
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.99 0.0.0.0
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.1 0.0.0.0
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.65 0.0.0.0
CALI(config-ext-nacl)#end Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red.




BOGOTA
Physical
Config
CLI
Attributes
IOS Command Line Interface
Password:
Password:
BOGOTA>enable
Password:
BOGOTA#telnet 192.168.1.65
Trying 192.168.1.65 ...Open
User Access Verification
Password:
Password:
Password:
[Connection to 192.168.1.65 closed by foreign host]
BOGOTA#ping 192.168.1.34
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.34, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/37/146
ms
BOGOTA#
Ctrl+F6 to exit CLI focus
Copy
Paste


BOGOTA
Physical
Config
CLI
Attributes
IOS Command Line Interface
[Connection to 192.168.1.65 closed by foreign host]
BOGOTA#
BOGOTA#telnet 192.168.1.65
Trying 192.168.1.65 ...Open
User Access Verification
Password:
Password:
Password:
[Connection to 192.168.1.65 closed by foreign host]
BOGOTA#telnet 192.168.1.33
Trying 192.168.1.33 ...Open
User Access Verification
Password:
Password:
Password:
[Connection to 192.168.1.33 closed by foreign host]
BOGOTA#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top



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.

MEDELLIN>enable
Password:
MEDELLIN#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#ip access-list extended ServerPT
MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.33 0.0.0.0
MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.98 0.0.0.0
MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.131 0.0.0.0
MEDELLIN(config-ext-nacl)#end

BOGOTA#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#ip access-list extended ServerPT
BOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.99 0.0.0.0
BOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.1 0.0.0.0

```
BOGOTA(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.131 0.0.0.0
BOGOTA(config-ext-nacl)#end

CALI>enable
Password:
Password:
CALI#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#ip access-list extended ServerPT
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.99 0.0.0.0
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.1 0.0.0.0
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.65 0.0.0.0
CALI(config-ext-nacl)#end
```

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

```
MEDELLIN>enable
Password:
MEDELLIN#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#ip access-list extended ServerPT
MEDELLIN(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.3 0.0.0.0
MEDELLIN(config-ext-nacl)#exit
MEDELLIN(config)#int f0/0
MEDELLIN(config-if)#ip access-group ServerPT in
MEDELLIN(config-if)#end

CALI>enable
Password:
CALI#config t
Enter configuration commands, one per line. End with CNTL/Z.
CALI(config)#ip access-list extended ServerPT
CALI(config-ext-nacl)#permit ip 0.0.0.0 255.255.255.255 192.168.1.3 0.0.0.0
CALI(config-ext-nacl)#exit
CALI(config)#int f0/0
CALI(config-if)#ip access-group ServerPT in
CALI(config-if)#end
```

Parte 5: Comprobación de la red instalada.

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

MEDELLIN#
MEDELLIN#show Access-list
Extended IP access list ServerPT
10 permit ip any host 192.168.1.3
20 permit ip any host 192.168.1.33
30 permit ip any host 192.168.1.98
40 permit ip any host 192.168.1.131

BOGOTA>enable
Password:
BOGOTA#show access-list
Extended IP access list ServerPT
10 permit ip host 192.168.1.3 any
20 permit ip any host 192.168.1.99
30 permit ip any host 192.168.1.1
40 permit ip any host 192.168.1.131

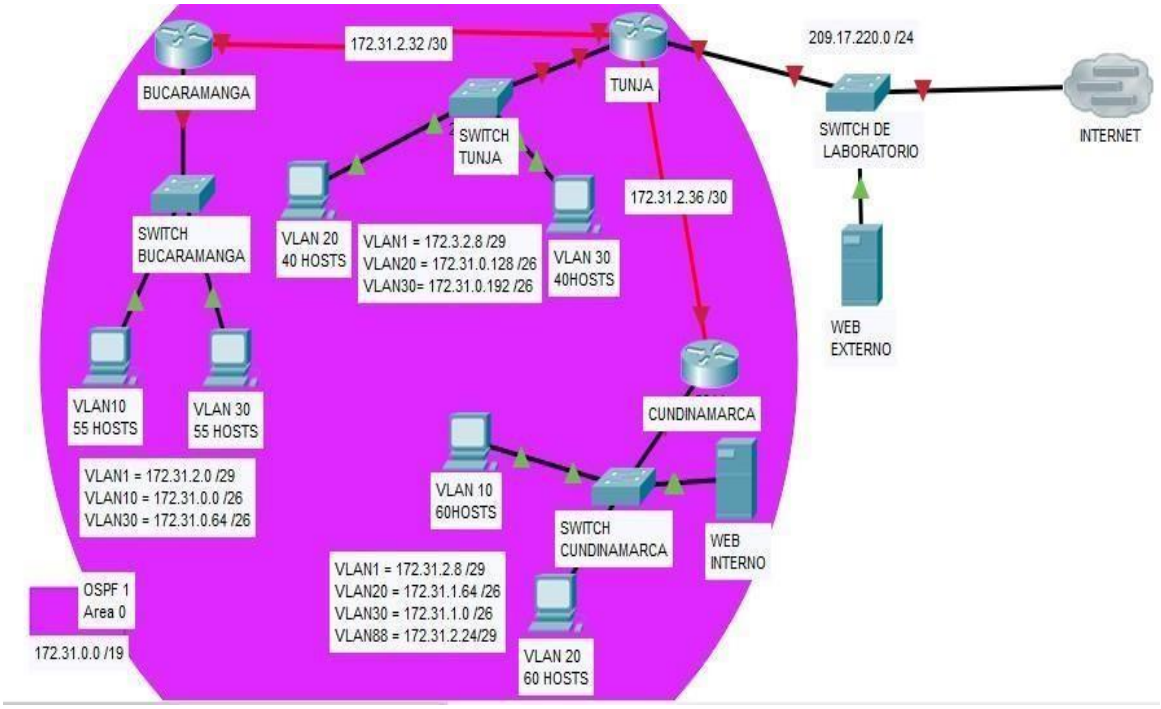
CALI>enable
Password:
CALI#show access-list
Extended IP access list ServerPT
10 permit ip any host 192.168.1.3
20 permit ip any host 192.168.1.99
30 permit ip any host 192.168.1.1
40 permit ip any host 192.168.1.65

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

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	ok
	WS_1	Router BOGOTA	ok
	Servidor	Router CALI	ok
	Servidor	Router MEDELLIN	ok
TELNET	LAN del Router MEDELLIN	Router CALI	falla
	LAN del Router CALI	Router CALI	ok
	LAN del Router MEDELLIN	Router MEDELLIN	ok
	LAN del Router CALI	Router MEDELLIN	falla
PING	LAN del Router CALI	WS_1	falla
	LAN del Router MEDELLIN	WS_1	falla
	LAN del Router MEDELLIN	LAN del Router CALI	falla
PING	LAN del Router CALI	Servidor	ok
	LAN del Router MEDELLIN	Servidor	ok
	Servidor	LAN del Router MEDELLIN	ok
	Servidor	LAN del Router CALI	ok
	Router CALI	LAN del Router MEDELLIN	ok
	Router MEDELLIN	LAN del Router CALI	ok

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 LANoriginal.



Desarrollo

Los siguientes son los requerimientos necesarios:

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

   - **Configuración básica.**

```
Router>en
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BUCARAMANGA
BUCARAMANGA(config)#no ip domain-lookup
BUCARAMANGA(config)#banner motd #Cuidado Acceso Restringido#
BUCARAMANGA(config)#enable secret class123
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#password cisco123
```

```
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#logging synchronous
BUCARAMANGA(config-line)#line vty 0 15
BUCARAMANGA(config-line)#password cisco123
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#logging synchronous
BUCARAMANGA(config)#int f0/0.1
BUCARAMANGA(config-subif)#encapsulation dot1q 1
BUCARAMANGA(config-subif)#ip address 172.31.2.1 255.255.255.248
BUCARAMANGA(config-subif)#int f0/0.10
BUCARAMANGA(config-subif)#encapsulation dot1q 10
BUCARAMANGA(config-subif)#ip address 172.31.0.1 255.255.255.192
BUCARAMANGA(config-subif)#int f0/0.30
BUCARAMANGA(config-subif)#encapsulation dot1q 30
BUCARAMANGA(config-subif)#ip address 172.31.0.65 255.255.255.192
BUCARAMANGA(config-subif)#int f0/0
BUCARAMANGA(config-if)#no shutdown

BUCARAMANGA(config-if)#
BUCARAMANGA(config-if)#
BUCARAMANGA(config-if)#int s0/0/0
BUCARAMANGA(config-if)#ip address 172.31.2.34 255.255.255.252
BUCARAMANGA(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
BUCARAMANGA(config-if)#
BUCARAMANGA(config-if)#router ospf 1
BUCARAMANGA(config-router)#network 172.31.0.0 0.0.0.63 area 0
BUCARAMANGA(config-router)#network 172.31.0.64 0.0.0.63 area 0
BUCARAMANGA(config-router)#network 172.31.2.0 0.0.0.7 area 0
BUCARAMANGA(config-router)#network 172.31.2.32 0.0.0.3 area 0
BUCARAMANGA(config-router)#end
BUCARAMANGA#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1,
changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up

%SYS-5-CONFIG_I: Configured from console by console

BUCARAMANGA#

Router>en
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname TUNJA
TUNJA(config)#no ip domain-lookup
TUNJA(config)#banner motd #Cuidado Acceso Restringido#
TUNJA(config)#enable secret class123
TUNJA(config)#line console 0
TUNJA(config-line)#password cisco123
TUNJA(config-line)#login
TUNJA(config-line)#logging synchronous
TUNJA(config-line)#line vty 0 15
TUNJA(config-line)#password cisco123
TUNJA(config-line)#login
TUNJA(config-line)#logging synchronous
TUNJA(config)#int f0/0.1
TUNJA(config-subif)#encapsulation dot1q 1
TUNJA(config-subif)#ip address 172.3.2.9 255.255.255.248
TUNJA(config-subif)#int f0/0.20
TUNJA(config-subif)#encapsulation dot1q 20
TUNJA(config-subif)#ip address 172.31.0.129 255.255.255.192
TUNJA(config-subif)#int f0/0.30
TUNJA(config-subif)#encapsulation dot1q 30
TUNJA(config-subif)#ip address 172.31.0.193 255.255.255.192
TUNJA(config-subif)#int f0/0
TUNJA(config-if)#no shutdown

TUNJA(config-if)#
TUNJA(config-if)#int s0/0/0
TUNJA(config-if)#ip address 172.31.2.33 255.255.255.252
TUNJA(config-if)#no shutdown

TUNJA(config-if)#

```
TUNJA(config-if)#int s0/0/1
TUNJA(config-if)#ip address 172.31.2.37 255.255.255.252
TUNJA(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
TUNJA(config-if)#int f0/1
TUNJA(config-if)#ip address 209.165.220.1255.255.255.0
TUNJA(config-if)#no shutdown

TUNJA(config-if)#
TUNJA(config-if)#router ospf 1
TUNJA(config-router)#network 172.3.2.8 0.0.0.7 area 0
TUNJA(config-router)#network 172.31.0.128 0.0.0.63 area0
TUNJA(config-router)#network 172.31.0.192 0.0.0.63 area0
TUNJA(config-router)#network 172.31.2.32 0.0.0.3 area 0
TUNJA(config-router)#network 172.31.2.36 0.0.0.3 area 0
TUNJA(config-router)#end
TUNJA#
TUNJA#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1,
changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20,
changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30,
changed state to up

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up
```

%SYS-5-CONFIG_I: Configured from console by console

TUNJA#

Router>en
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname CUNDINAMARCA
CUNDINAMARCA(config)#no ip domain-lookup
CUNDINAMARCA(config)#banner motd #Cuidado Acceso Restringido#
CUNDINAMARCA(config)#enable secret class123
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#password cisco123
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#logging synchronous
CUNDINAMARCA(config-line)#line vty 0 15
CUNDINAMARCA(config-line)#password cisco123
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#logging synchronous
CUNDINAMARCA(config)#int f0/0.1
CUNDINAMARCA(config-subif)#encapsulation dot1q 1
CUNDINAMARCA(config-subif)#ip address 172.31.2.9 255.255.255.248
CUNDINAMARCA(config-subif)#int f0/0.20
CUNDINAMARCA(config-subif)#encapsulation dot1q 20
CUNDINAMARCA(config-subif)#ip address 172.31.1.65 255.255.255.192
CUNDINAMARCA(config-subif)#int f0/0.30
CUNDINAMARCA(config-subif)#encapsulation dot1q 30
CUNDINAMARCA(config-subif)#ip address 172.31.1.1 255.255.255.192
CUNDINAMARCA(config-subif)#int f0/0.88
CUNDINAMARCA(config-subif)#encapsulation dot1q 88
CUNDINAMARCA(config-subif)#ip address 172.31.2.25 255.255.255.248
CUNDINAMARCA(config-subif)#int f0/0
CUNDINAMARCA(config-if)#no shutdown

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

CUNDINAMARCA(config-if)#router ospf 1
CUNDINAMARCA(config-router)#network 172.31.1.0 0.0.0.63 area 0
CUNDINAMARCA(config-router)#network 172.31.1.64 0.0.0.63 area 0

CUNDINAMARCA(config-router)#network 172.31.2.8 0.0.0.7 area 0
CUNDINAMARCA(config-router)#network 172.31.2.24 0.0.0.7 area 0
CUNDINAMARCA(config-router)#network 172.31.2.36 0.0.0.3 area 0
CUNDINAMARCA(config-router)#end
CUNDINAMARCA#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.30, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.88, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.88, changed state to up

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%SYS-5-CONFIG_I: Configured from console by console

CUNDINAMARCA#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

CUNDINAMARCA#
00:14:55: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.220.1 on Serial0/0/0 from LOADING to FULL, Loading Done

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-BUCARAMANGA
SW-BUCARAMANGA(config)#vlan 1

SW-BUCARAMANGA(config-vlan)#vlan 10

SW-BUCARAMANGA(config-vlan)#vlan 30

SW-BUCARAMANGA(config-vlan)#int f0/20

SW-BUCARAMANGA(config-if)#switchport mode access

SW-BUCARAMANGA(config-if)#switchport access vlan 10

SW-BUCARAMANGA(config-if)#int f0/24

SW-BUCARAMANGA(config-if)#switchport mode access

SW-BUCARAMANGA(config-if)#switchport access vlan 30

SW-BUCARAMANGA(config-if)#int f0/1

SW-BUCARAMANGA(config-if)#switchport mode trunk

SW-BUCARAMANGA(config-if)#int vlan 1

SW-BUCARAMANGA(config-if)#ip address 172.31.2.3 255.255.255.248

SW-BUCARAMANGA(config-if)#no shutdown

SW-BUCARAMANGA(config-if)#ip default-gateway 172.31.2.1

SW-BUCARAMANGA(config)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up

%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-TUNJA
```

```
SW-TUNJA(config)#vlan 1
SW-TUNJA(config-vlan)#vlan 20
SW-TUNJA(config-vlan)#vlan 30
SW-TUNJA(config-vlan)#int f0/20
SW-TUNJA(config-if)#switchport mode access
SW-TUNJA(config-if)#switchport access vlan 20
SW-TUNJA(config-if)#int f0/24
SW-TUNJA(config-if)#switchport mode access
SW-TUNJA(config-if)#switchport access vlan 30
SW-TUNJA(config-if)#int f0/1
SW-TUNJA(config-if)#switchport mode trunk

SW-TUNJA(config-if)#
SW-TUNJA(config-if)#int vlan 1
SW-TUNJA(config-if)#ip address 172.3.2.11 255.255.255.248
SW-TUNJA(config-if)#no shutdown

SW-TUNJA(config-if)#
SW-TUNJA(config-if)#ip default-gateway172.3.2.9
SW-TUNJA(config)#
SW-TUNJA(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up

%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

SW-TUNJA(config)#
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-CUNDINAMARCA

SW-CUNDINAMARCA(config)#vlan 1

SW-CUNDINAMARCA(config-vlan)#vlan 20

SW-CUNDINAMARCA(config-vlan)#vlan 30

SW-CUNDINAMARCA(config-vlan)#vlan 88

SW-CUNDINAMARCA(config-vlan)#exit
```

SW-CUNDINAMARCA(config)#int f0/20

SW-CUNDINAMARCA(config-if)#switchport mode access

SW-CUNDINAMARCA(config-if)#switchport access vlan 20

SW-CUNDINAMARCA(config-if)#int f0/24

SW-CUNDINAMARCA(config-if)#switchport mode access

SW-CUNDINAMARCA(config-if)#switchport access vlan 30

SW-CUNDINAMARCA(config-if)#int f0/10

SW-CUNDINAMARCA(config-if)#switchport mode access

SW-CUNDINAMARCA(config-if)#switchport access vlan 88

SW-CUNDINAMARCA(config-if)#int f0/1

SW-CUNDINAMARCA(config-if)#switchport mode trunk

SW-CUNDINAMARCA(config-if)#

SW-CUNDINAMARCA(config-if)#int vlan 1

SW-CUNDINAMARCA(config-if)#ip address 172.31.2.11 255.255.255.248

SW-CUNDINAMARCA(config-if)#no shutdown

SW-CUNDINAMARCA(config-if)#

SW-CUNDINAMARCA(config-if)#ip default-gateway 172.31.2.9

SW-CUNDINAMARCA(config)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

SW-CUNDINAMARCA(config)#

Autenticación local con AAA.

BUCARAMANGA(config-line)#username admi secret class14
BUCARAMANGA(config)#aaa new-model
BUCARAMANGA(config)#aaa authentication login LOGIN local
BUCARAMANGA(config)#line console 0
BUCARAMANGA(config-line)#login authentication LOGIN
BUCARAMANGA(config-line)#line vty 0 15
BUCARAMANGA(config-line)#login authentication LOGIN

TUNJA(config-line)#username admi secret class14
TUNJA(config)#aaa new-model
TUNJA(config)#aaa authentication login LOGIN local
TUNJA(config)#line console 0
TUNJA(config-line)#login authentication LOGIN
TUNJA(config-line)#line vty 0 15
TUNJA(config-line)#login authentication LOGIN

CUNDINAMARCA(config-line)#username admi secret class14
CUNDINAMARCA(config)#aaa new-model
CUNDINAMARCA(config)#aaa authentication login LOGIN local
CUNDINAMARCA(config)#line console 0
CUNDINAMARCA(config-line)#login authentication LOGIN
CUNDINAMARCA(config-line)#line vty 0 15
CUNDINAMARCA(config-line)# login authentication LOGIN

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

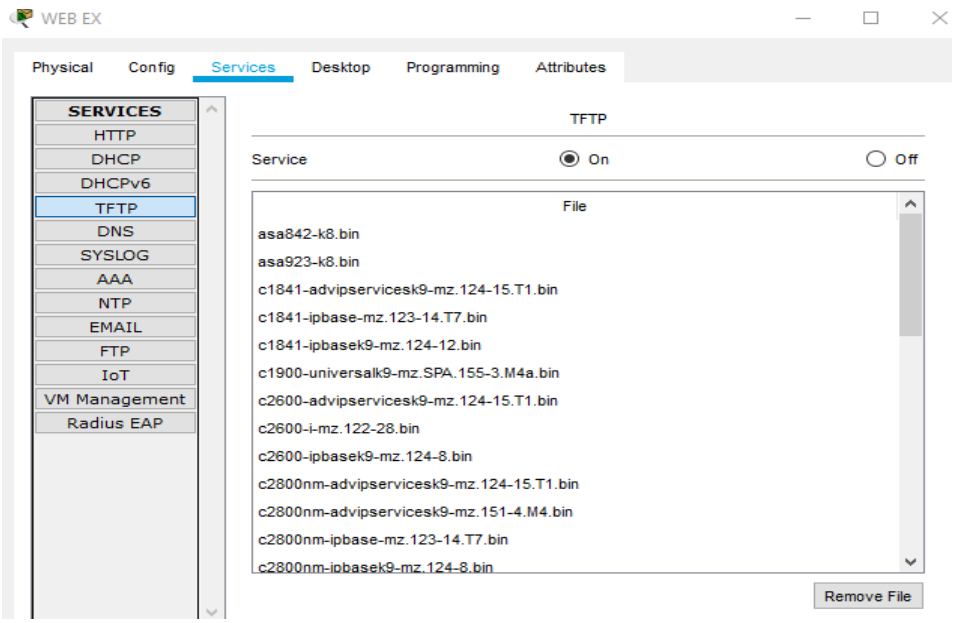
Máximo tiempo de acceso al detectar ataques.

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

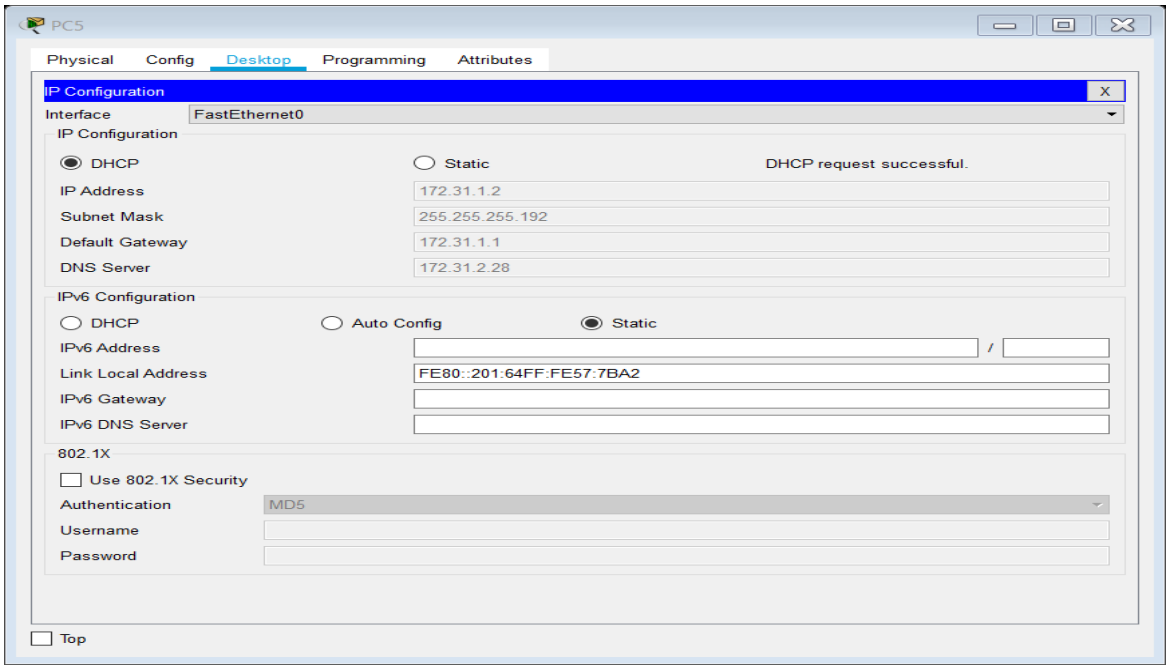
Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers

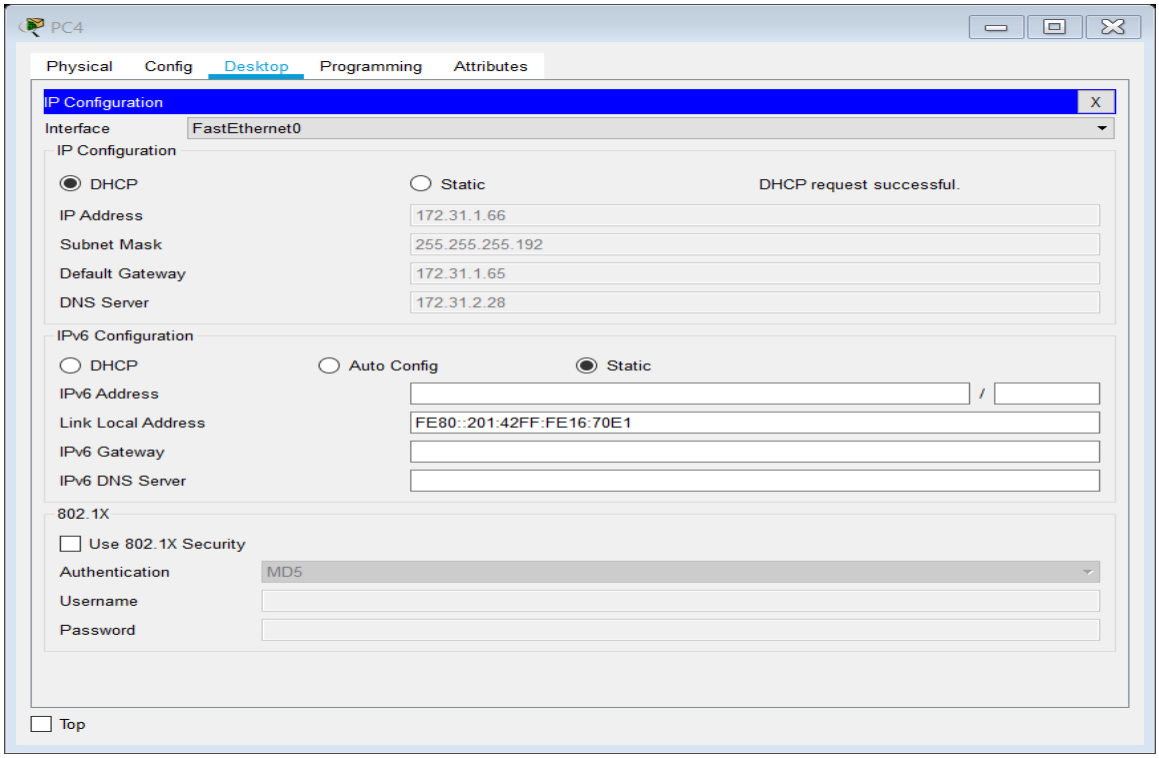


2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca

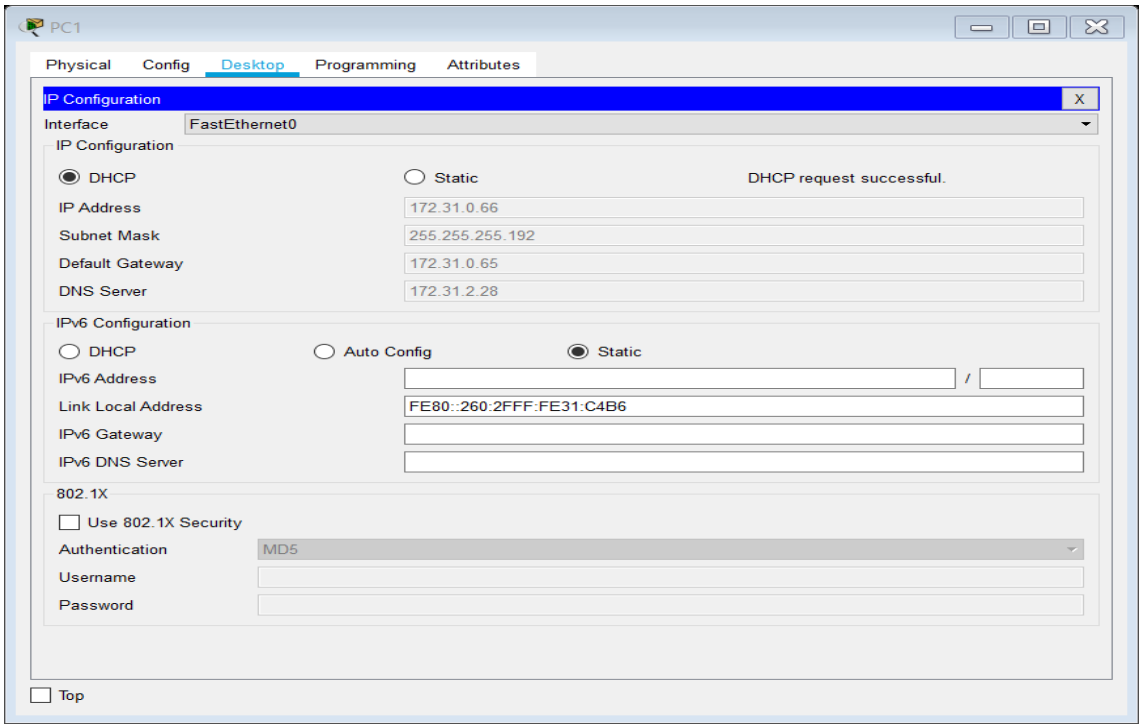
```
TUNJA(config)#ip dhcp excluded-address 172.31.0.1
TUNJA(config)#ip dhcp excluded-address 172.31.0.65
TUNJA(config)#ip dhcp excluded-address 172.31.1.65
TUNJA(config)#ip dhcp excluded-address 172.31.1.1
TUNJA(config)#ip dhcp pool V10B
TUNJA(dhcp-config)#network 172.31.0.0 255.255.255.192
TUNJA(dhcp-config)#default-router 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#
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console

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#
%SYS-5-CONFIG_I: Configured from console by console
```

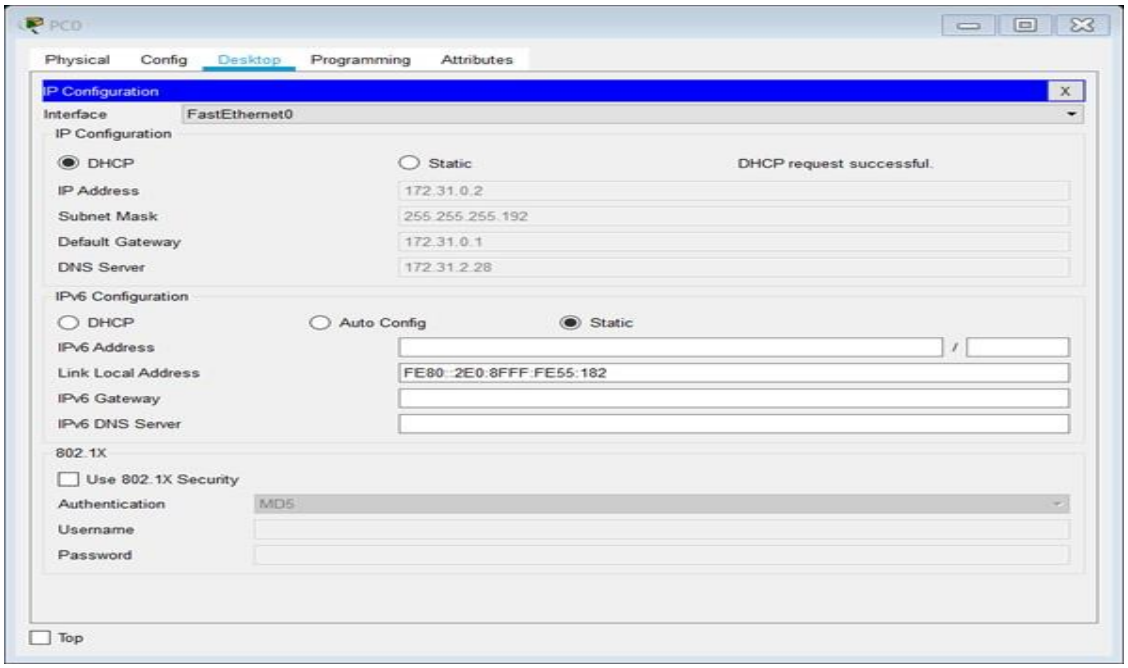
Verificación DHCP Cundinamarca





Verificación DHCP Bucaramanga





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#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 type2
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, 00:24:49, Serial0/0/0
O 172.31.0.64/26 [110/65] via 172.31.2.34, 00:24:49, 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, 00:23:33, Serial0/0/1
O 172.31.1.64/26 [110/65] via 172.31.2.38, 00:23:33, Serial0/0/1
```

O 172.31.2.0/29 [110/65] via 172.31.2.34, 00:24:49, Serial0/0/0
O 172.31.2.8/29 [110/65] via 172.31.2.38, 00:23:33, Serial0/0/1
O 172.31.2.24/29 [110/65] via 172.31.2.38, 00:23:33, Serial0/0/1
C 172.31.2.32/30 is directly connected, Serial0/0/0
C 172.31.2.36/30 is directly connected, Serial0/0/1
C 209.165.220.0/24 is directly connected, FastEthernet0/1
S* 0.0.0.0/0 [1/0] via 209.165.220.3

TUNJA#
BUCARAMANGA#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 type2
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 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, 00:25:08, 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, 00:25:08, Serial0/0/0
O 172.31.0.192/26 [110/65] via 172.31.2.33, 00:25:08, Serial0/0/0
O 172.31.1.0/26 [110/129] via 172.31.2.33, 00:23:42, Serial0/0/0
O 172.31.1.64/26 [110/129] via 172.31.2.33, 00:23:42, 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, 00:23:42, Serial0/0/0
O 172.31.2.24/29 [110/129] via 172.31.2.33, 00:23:42, 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, 00:24:02, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 172.31.2.33, 00:02:01, Serial0/0/0

BUCARAMANGA#

CUNDINAMARCA#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 type2
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 172.31.2.37 to network 0.0.0.0

172.3.0.0/29 is subnetted, 1 subnets
O 172.3.2.8 [110/65] via 172.31.2.37, 00:24:15, 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, 00:24:15, Serial0/0/0
O 172.31.0.64/26 [110/129] via 172.31.2.37, 00:24:15, Serial0/0/0
O 172.31.0.128/26 [110/65] via 172.31.2.37, 00:24:15, Serial0/0/0
O 172.31.0.192/26 [110/65] via 172.31.2.37, 00:24:15, 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, 00:24:15, 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, 00:24:15, 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, 00:02:24, Serial0/0/0

TUNJA#show ip nat translation
Pro Inside global Inside local Outside local Outside global
icmp 209.165.220.1:1 172.31.1.2:1 209.165.220.3:1209.165.220.3:1
icmp 209.165.220.1:2 172.31.1.2:2 209.165.220.3:2209.165.220.3:2
icmp 209.165.220.1:3 172.31.1.2:3 209.165.220.3:3209.165.220.3:3
icmp 209.165.220.1:4 172.31.1.2:4 209.165.220.3:4209.165.220.3:4
--- 209.165.220.4 172.31.2.28 --- —
```

4. **El enrutamiento deberá tener autenticación.**

```
BUCARAMANGA#configure terminal
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 cisco123
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 cisco123
CUNDINAMARCA(config-if)#
```

TUNJA#
00:30:20: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired

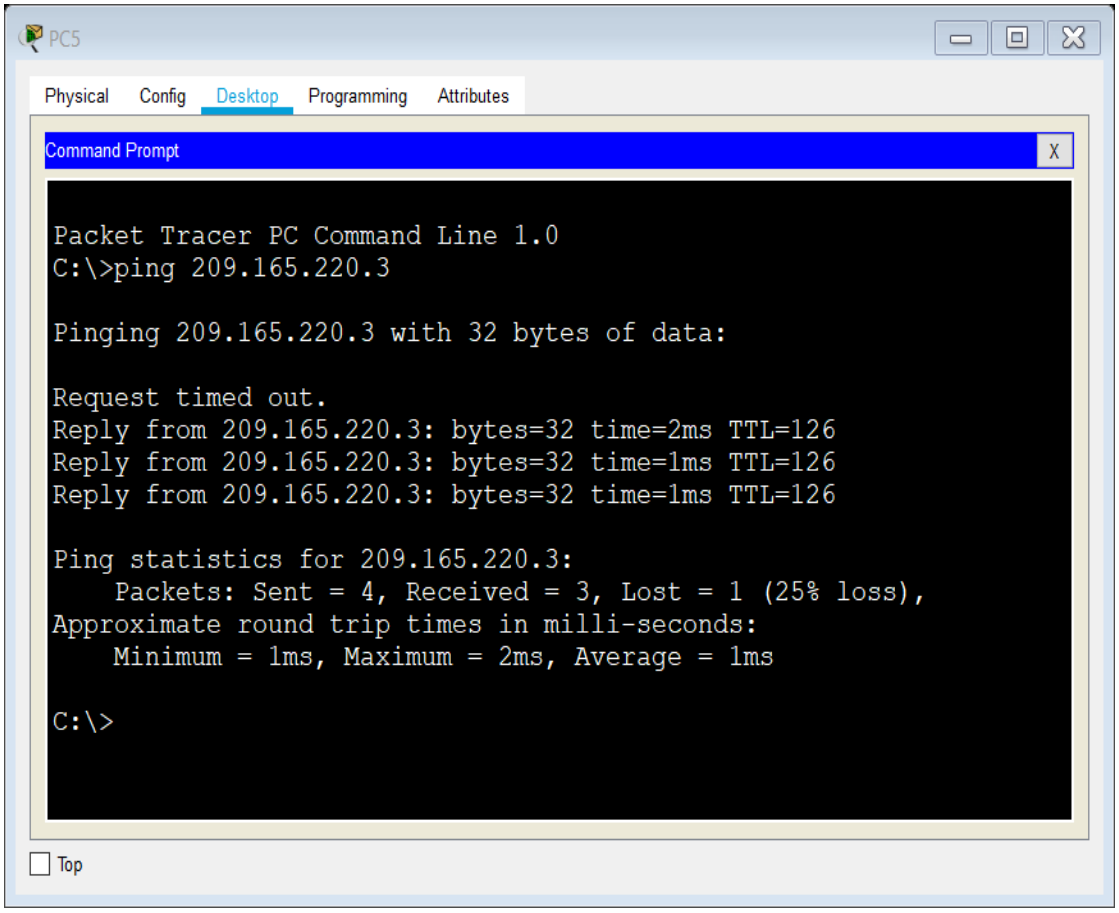
00:30:20: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached

TUNJA#
00:31:32: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.38 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Dead timer expired

00:31:32: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.38 on Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached

TUNJA#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
TUNJA(config)#int s0/0/0
TUNJA(config-if)#ip ospf authentication message-digest
TUNJA(config-if)#ip ospf message-digest-key 1 md5 cisco123
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 cisco123
TUNJA(config-if)#
00:31:40: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.34 on Serial0/0/0 from LOADING to FULL, Loading Done

TUNJA(config-if)#
00:31:42: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.2.38 on Serial0/0/1 from LOADING to FULL, Loading Done



5. Listas de control de acceso:

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

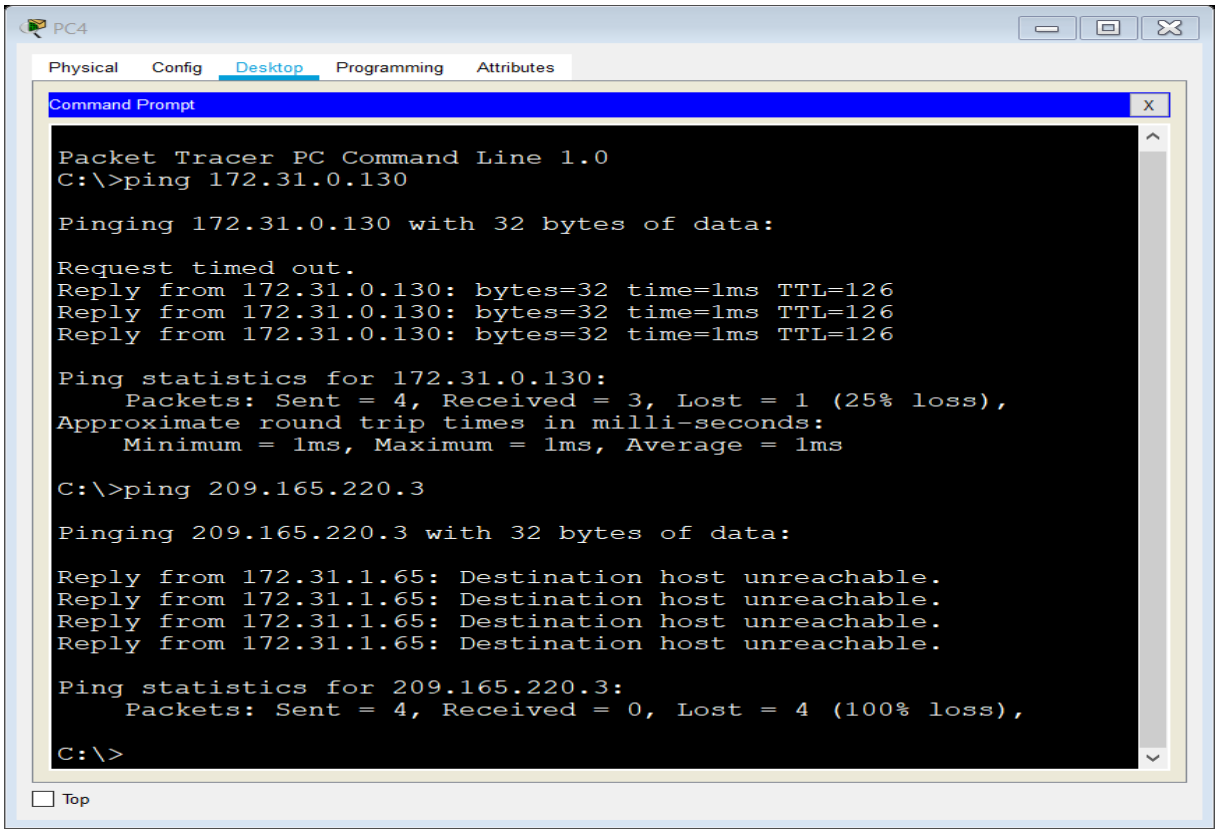
CUNDINAMARCA(config-if)#access-list 111 deny ip 172.31.1.64 0.0.0.63 209.165.220.0 0.0.0.255

CUNDINAMARCA(config)#access-list 111 permit ip any any

CUNDINAMARCA(config)#int f0/0.20

CUNDINAMARCA(config-subif)#ip access-group 111 in

CUNDINAMARCA(config-subif)#



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

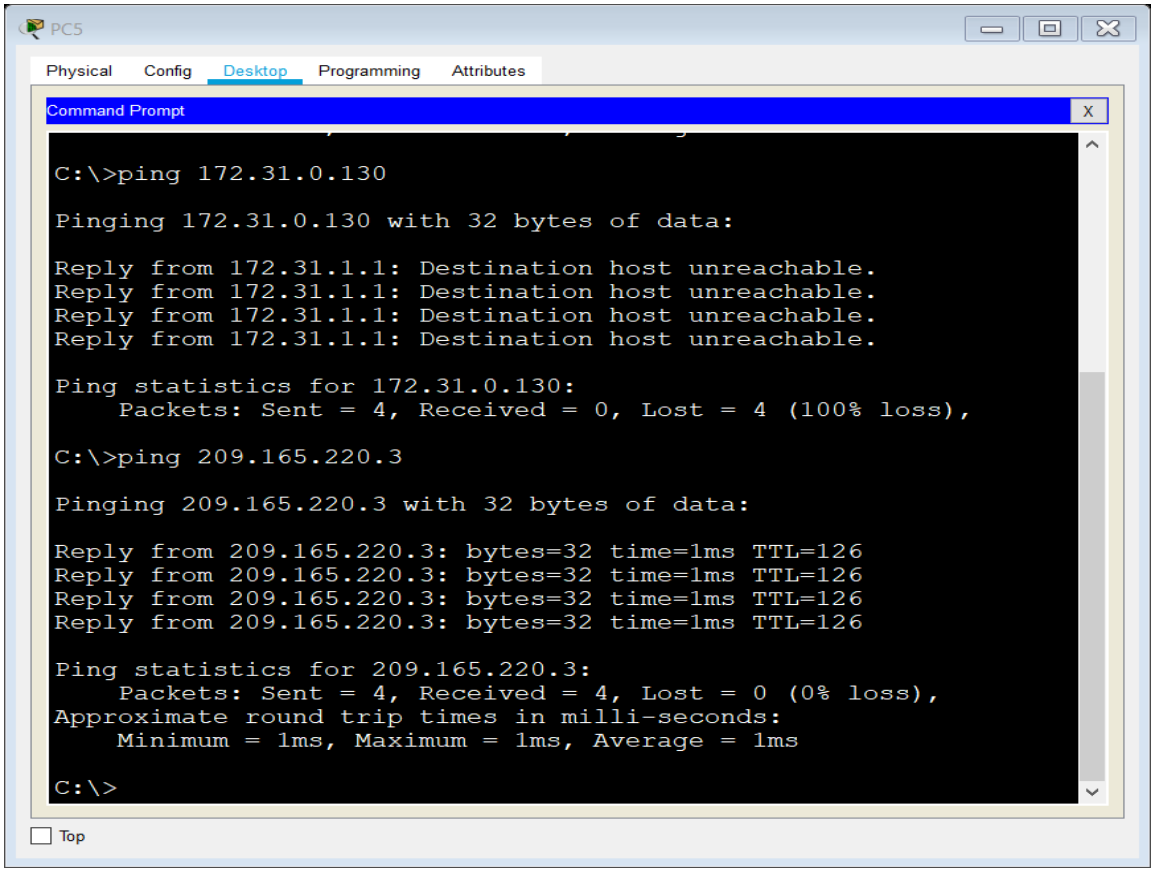
CUNDINAMARCA(config-subif)#access-list 112 permit ip 172.31.1.0 0.0.0.63 209.165.220.0 0.0.0.255

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

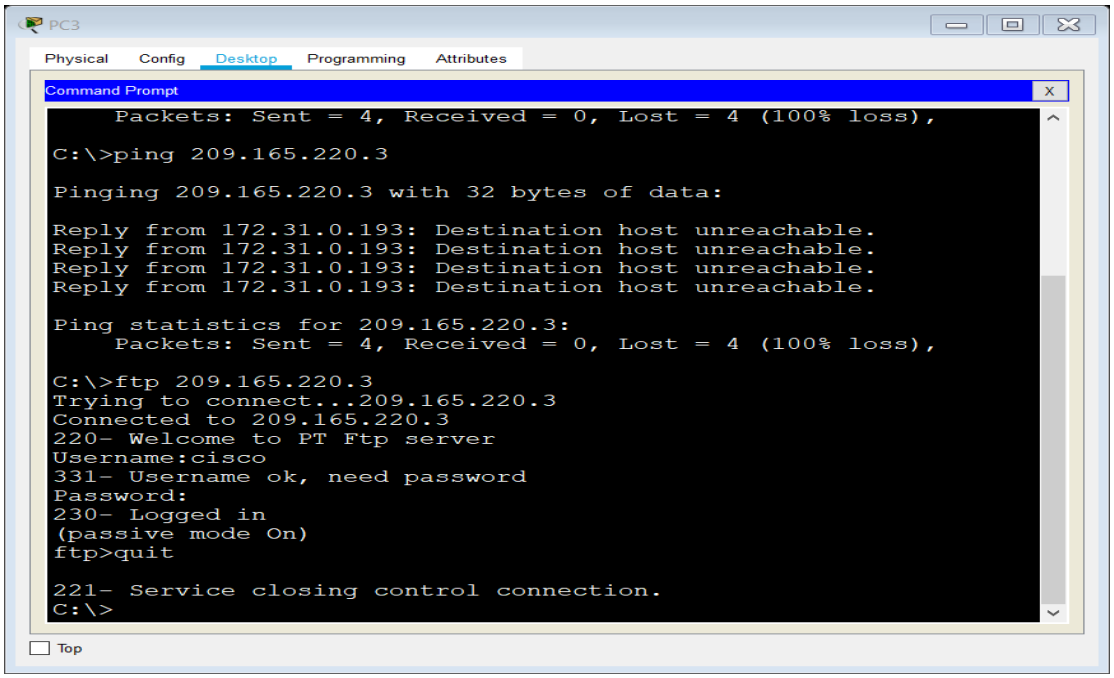
TUNJA(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 80

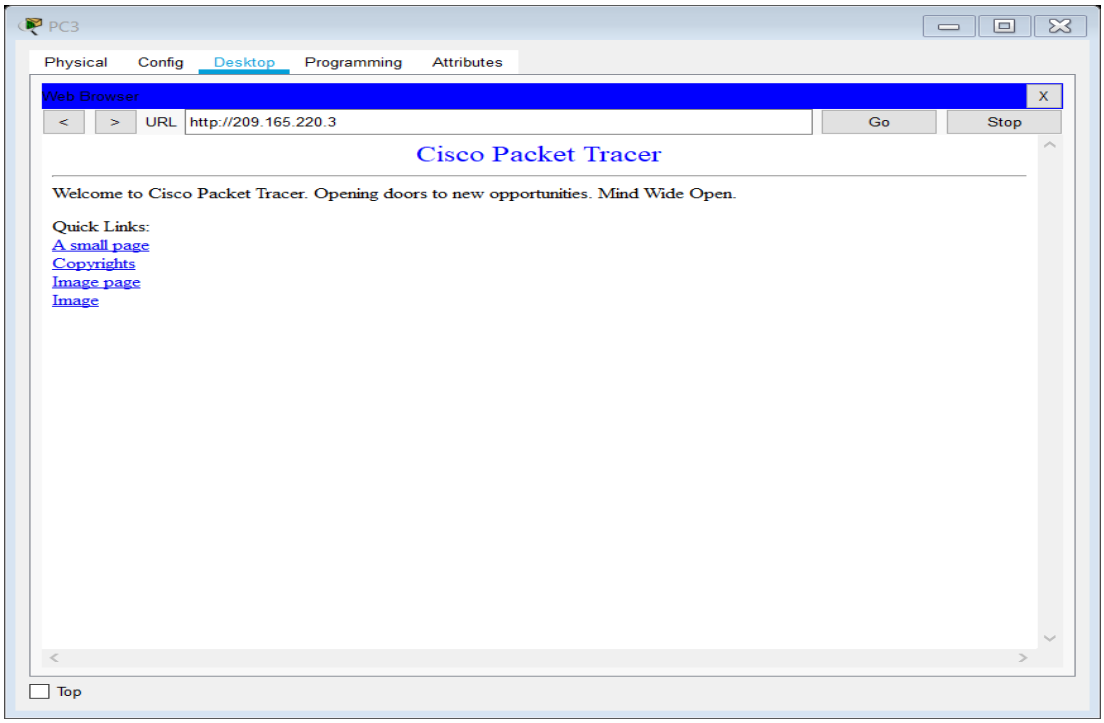
TUNJA(config)#access-list 111 permit tcp 172.31.0.192 0.0.0.63 209.165.220.0 0.0.0.255 eq 21

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

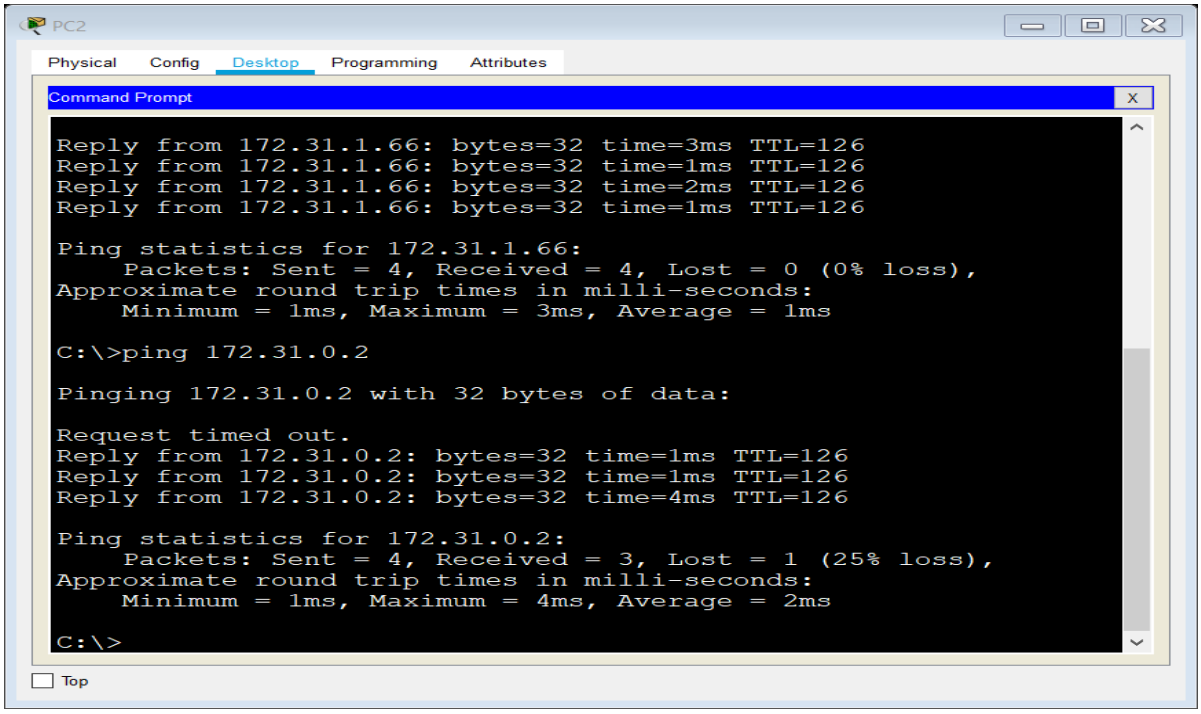


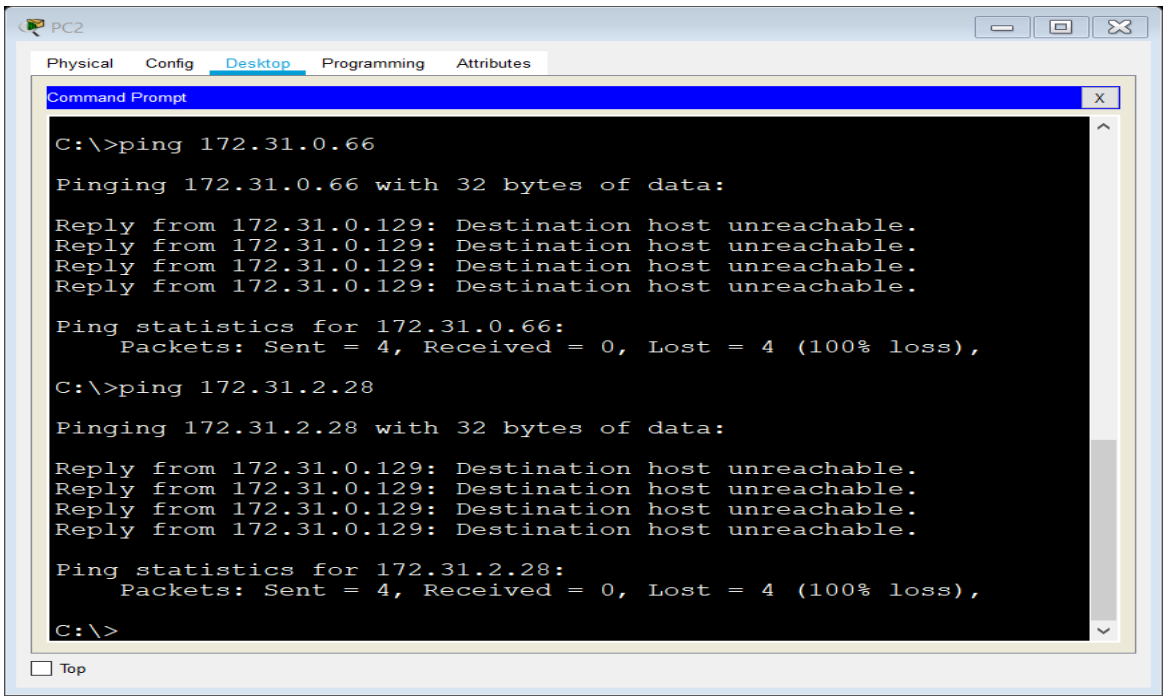


Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.

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
```

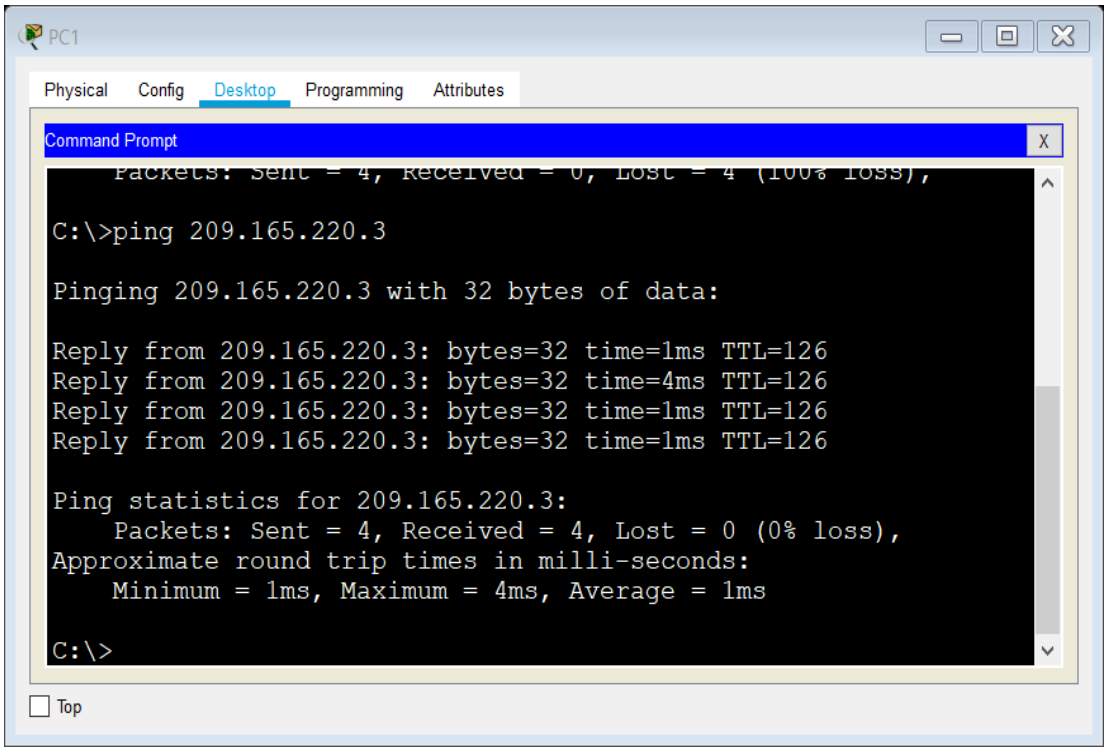




Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.

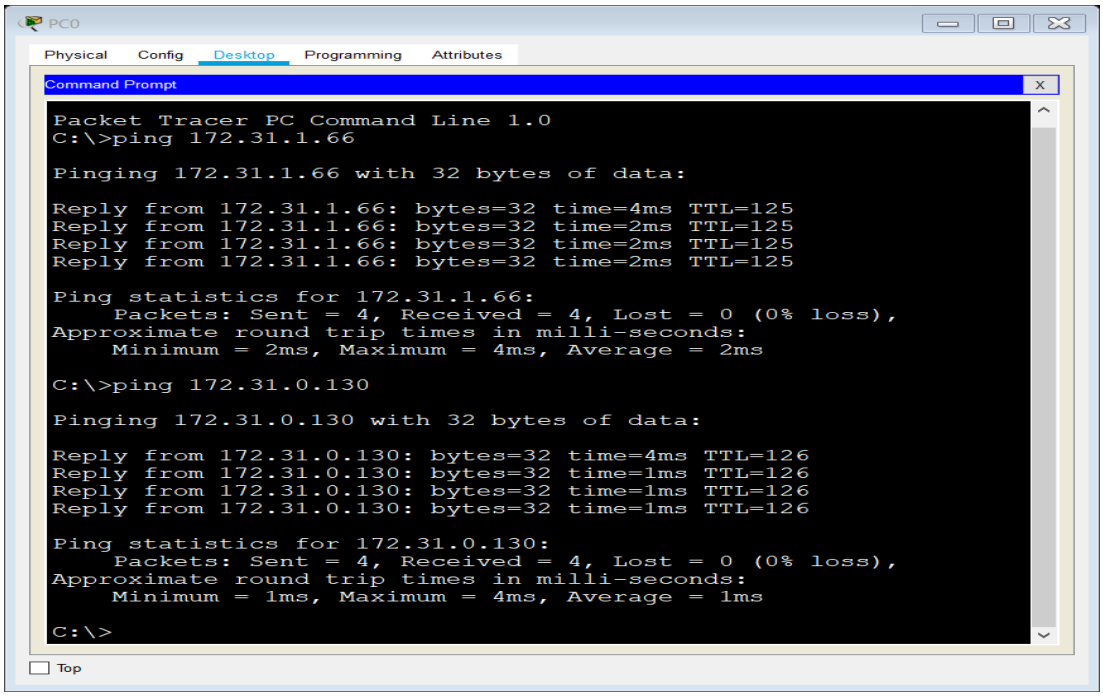
BUCARAMANGA(config)#access-list 111 permit ip 172.31.0.64 0.0.0.63 209.165.220.0 0.0.0.255
BUCARAMANGA(config)#int f0/0.30

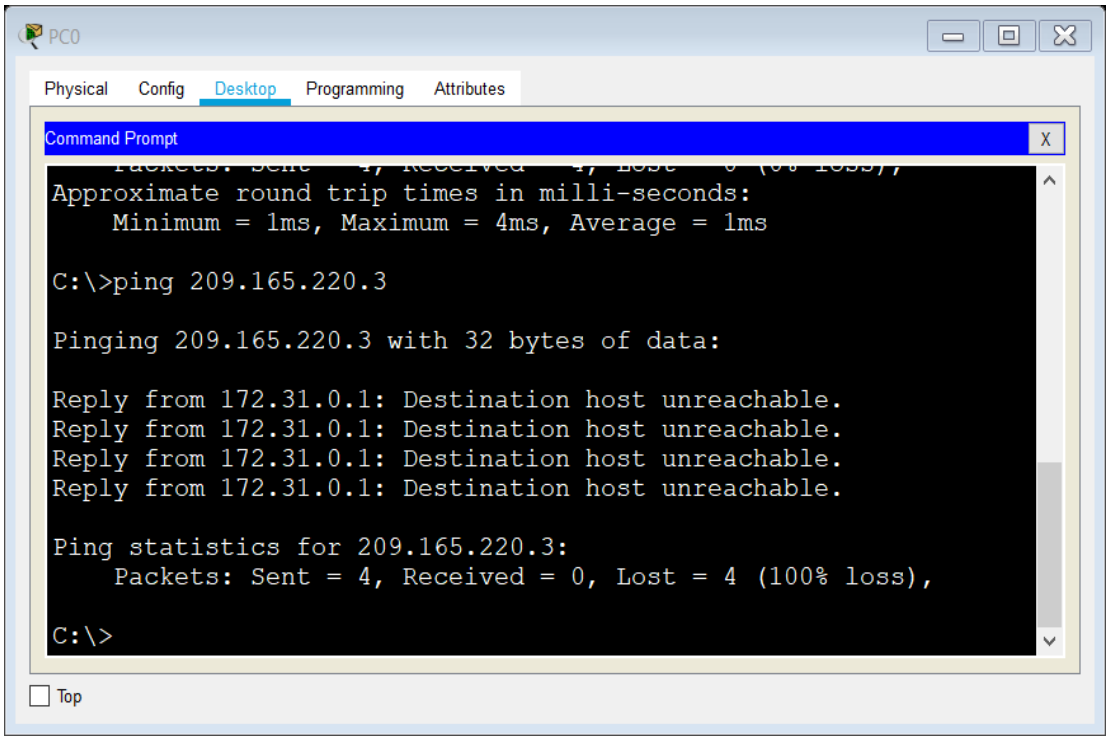
BUCARAMANGA(config-subif)#ip access-group 111 in
BUCARAMANGA(config-subif)#



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

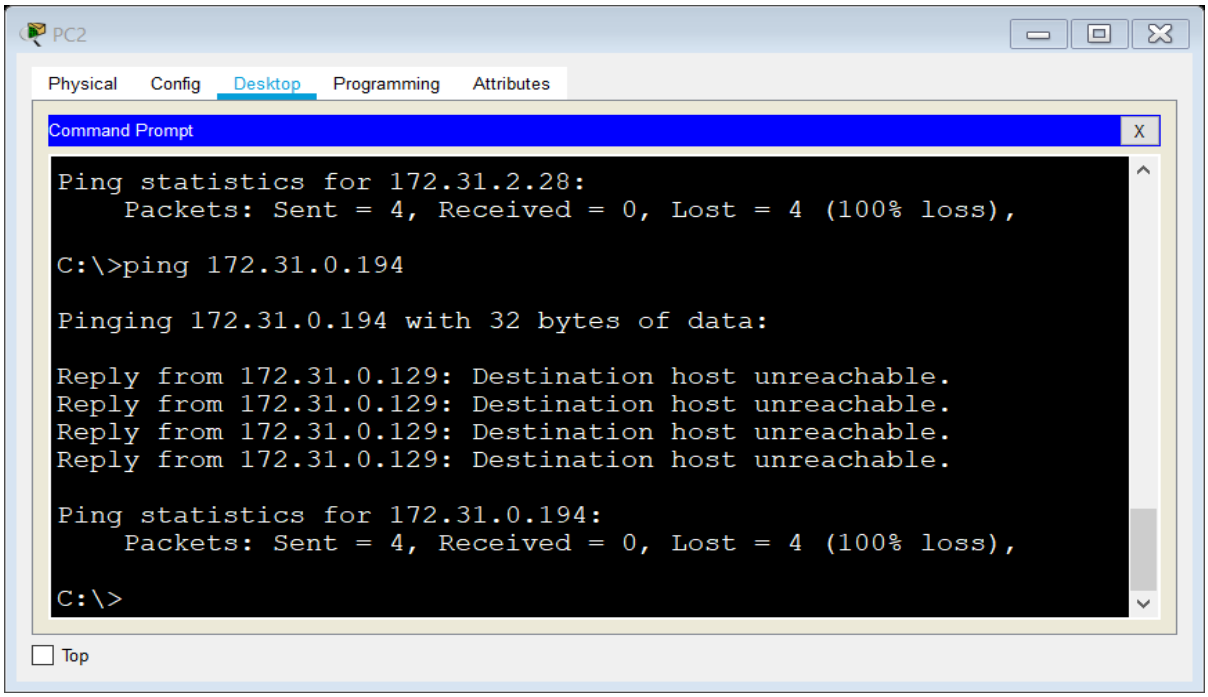


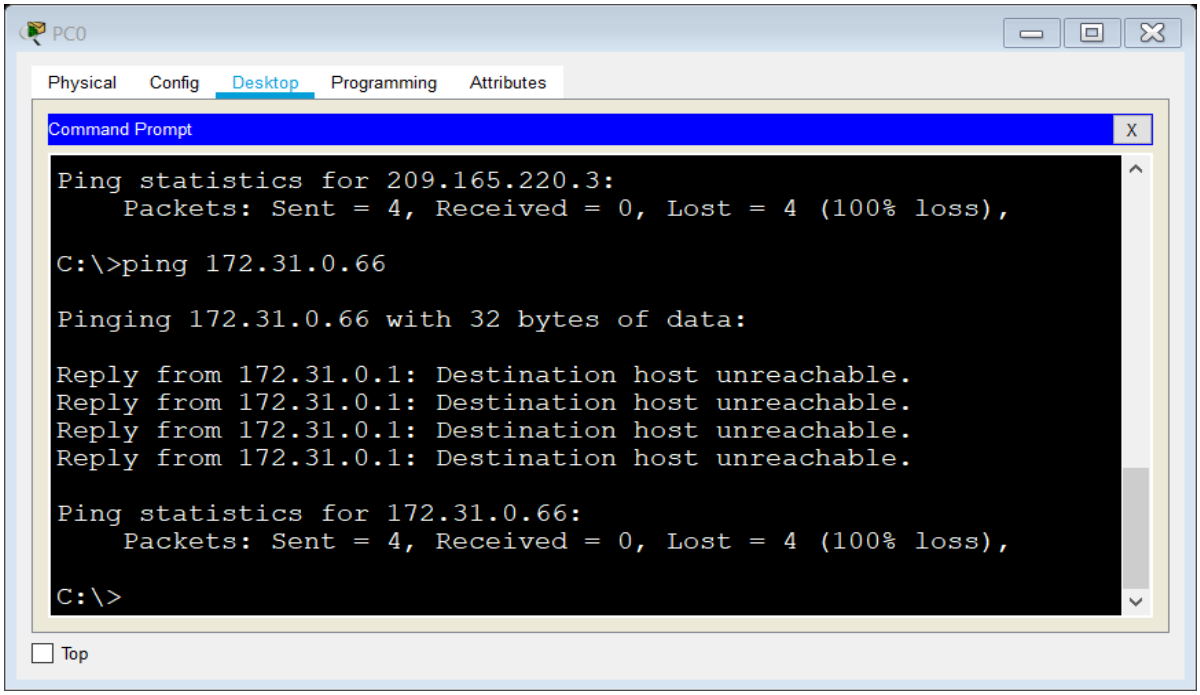


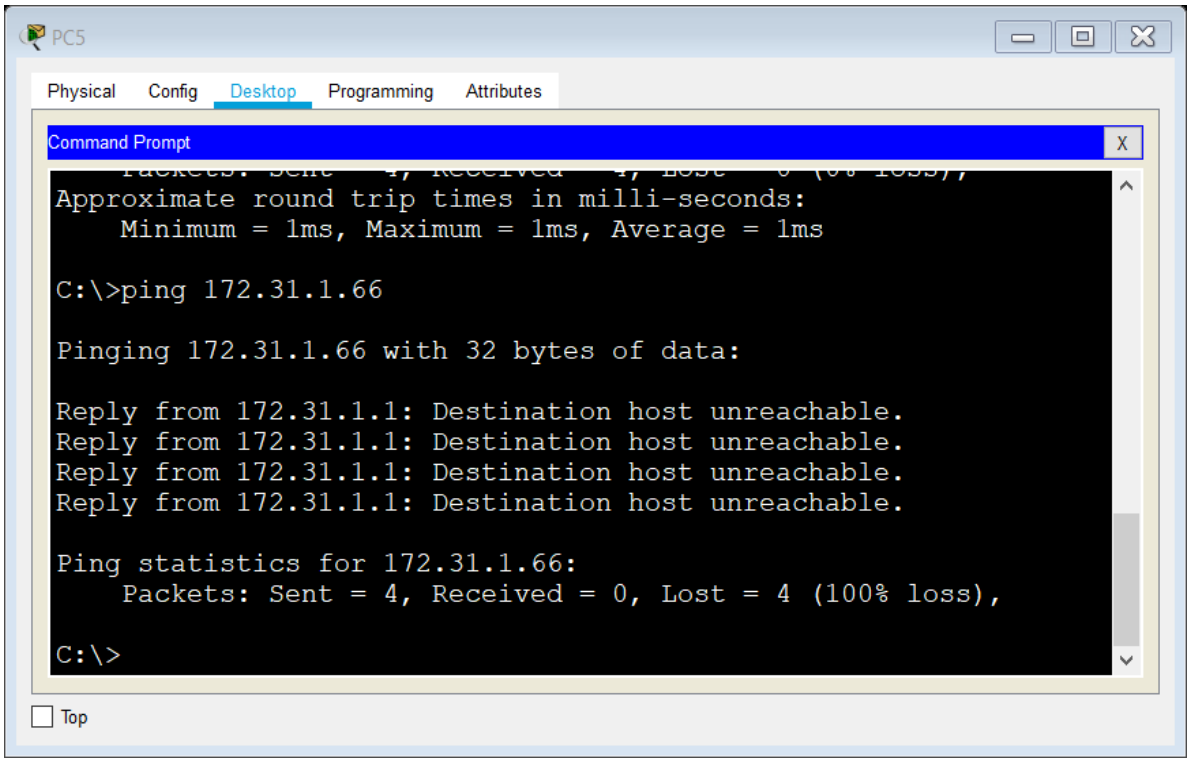
Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.

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
```




PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Ping statistics for 209.165.220.3:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 172.31.0.66
Pinging 172.31.0.66 with 32 bytes of data:
Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.
Reply from 172.31.0.1: Destination host unreachable.
Ping statistics for 172.31.0.66:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Top

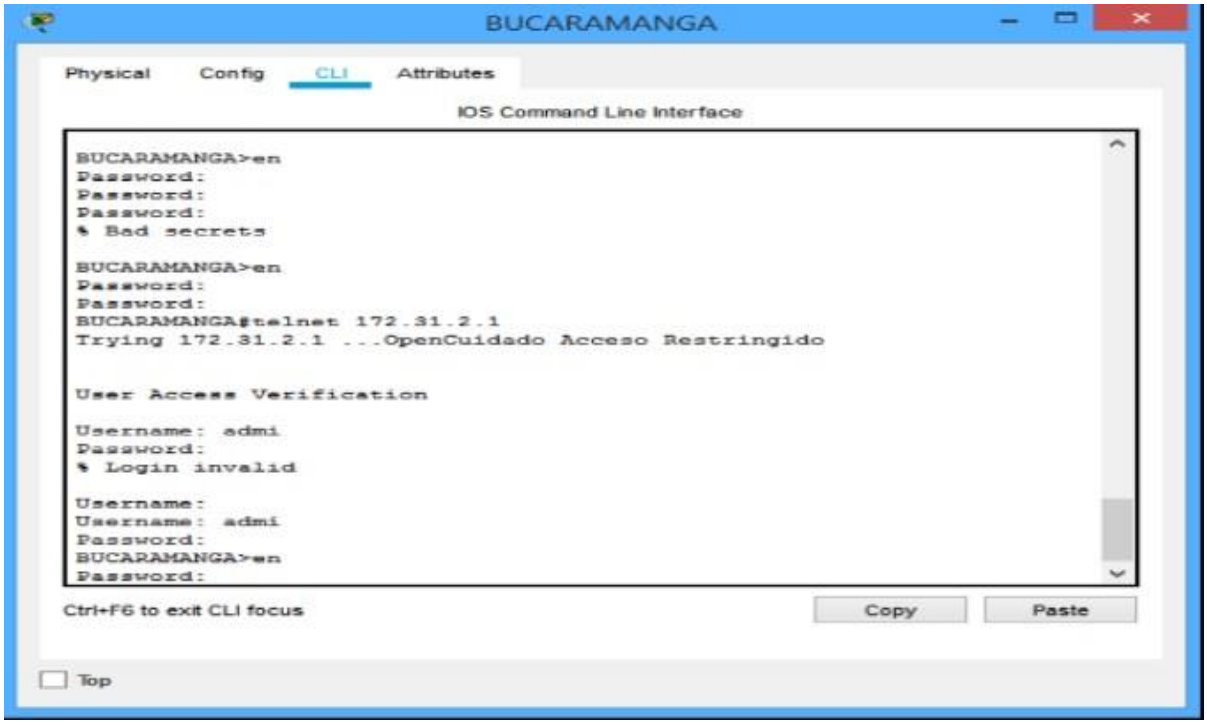

PC5
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\>ping 172.31.1.66
Pinging 172.31.1.66 with 32 bytes of data:
Reply from 172.31.1.1: Destination host unreachable.
Reply from 172.31.1.1: Destination host unreachable.
Reply from 172.31.1.1: Destination host unreachable.
Reply from 172.31.1.1: Destination host unreachable.
Ping statistics for 172.31.1.66:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Top

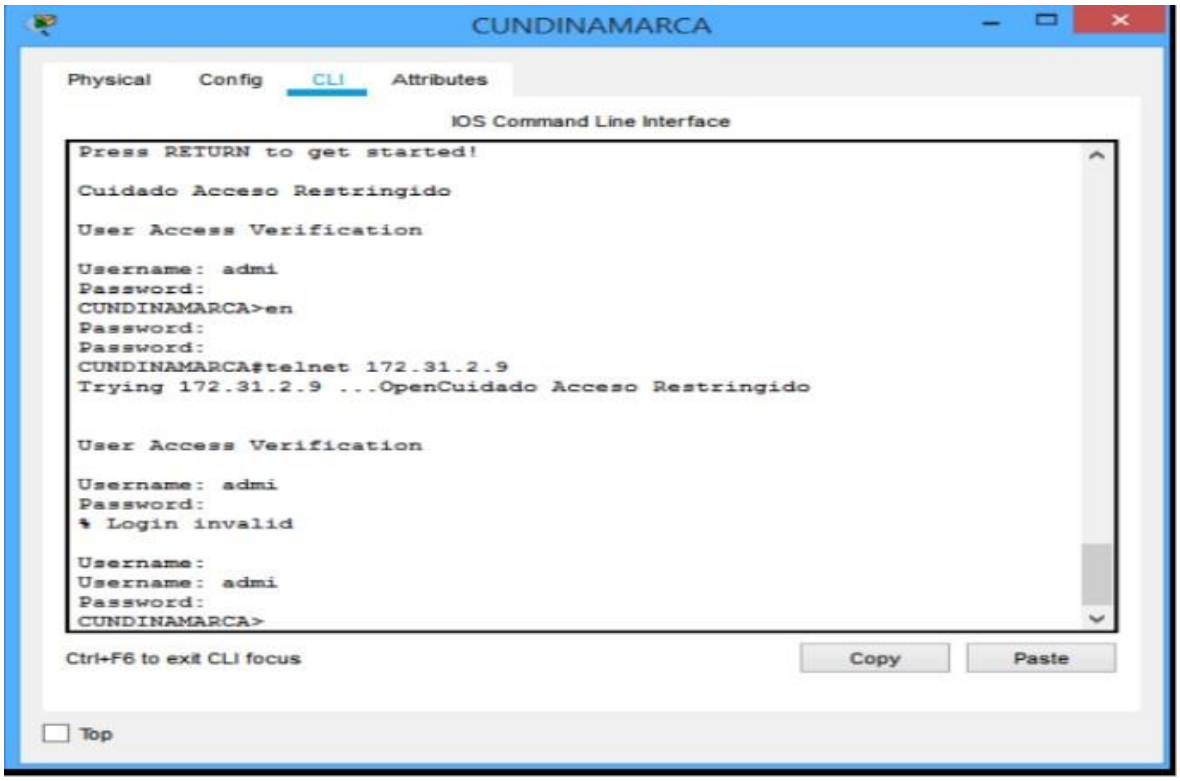
Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los routers e internet.

```
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
Physical
Config
CLI
Attributes
IOS Command Line Interface
Press RETURN to get started!
Cuidado Acceso Restringido
User Access Verification
Username: admi
Password:
CUNDINAMARCA>en
Password:
Password:
CUNDINAMARCA#telnet 172.31.2.9
Trying 172.31.2.9 ...OpenCuidado Acceso Restringido
User Access Verification
Username: admi
Password:
% Login invalid
Username:
Username: admi
Password:
CUNDINAMARCA>
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

Conclusión

A través de este diplomado hemos adquirido los conocimientos para administrar y y configurar las distintas redes con as que nos topemos en la vida laboral y cada uno de los elemento de cada red, hemos sido formados con conocimientos para brindar soluciones y conectividad a cada escenario que se nos presente como profesionales, pero en especial en este trabajo hemos entendido y comprendido las necesidades del mundo de hoy y cómo podemos brindar soluciones prácticas y eficaces a través de los retos que nos brindaron y de manera como pudimos darle solución, pudimos ver desde una configuración simple de direcciones para elementos en la red hasta encapsulamientos y encriptaciones de redes, pero no solo nos llevamos la sabiduría en el área de redes con este diplomado sino siempre tendremos la huella de los valores adquiridos dados por la universidad UNAD y cada uno de sus tutores.

Referencias Bibliográficas

Temática: Introducción a redes conmutadas CISCO. (2014). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1

Temática: Configuración y conceptos básicos de Switching CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

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

Temática: Conceptos de Routing CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1

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

Temática: Enrutamiento Estático CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1

Temática: Enrutamiento Dinámico CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

Temática: OSPF de una sola área CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1 65

Temática: Listas de control de acceso CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y 65 Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1**Temática: DHCP** CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

Temática: Traducción de direcciones IP para IPv4 CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1