Diplomado De Profundización CISCO - Prueba De Habilidades Prácticas

Presentado Por:
Edualguer Alvarado Cáceres

Presentado a:
Giovanni Alberto Bracho

Escuela de Ciencias Básicas, Tecnología e Ingeniería
Universidad Nacional Abierta y a distancia UNAD
Diciembre 2019

Tabla de Contenido

1. Resumen 3
2. Abstract. 4
3. Introducción 5
4. Objetivos 6
5. Desarrollo de los dos escenarios 7
6. Escenario 1 9
7. Parte 1: Asignación de direcciones IP 11
8. Parte 2: Configuración Básica. 12
9. Parte 3: Configuración de Enrutamiento. 21
10. Parte 4: Configuración de las listas de Control de Acceso. 25
11. Parte 5: Comprobación de la red instalada. 29
12. Escenario 2 30
13. Aspectos a tener en cuenta 40
14. Conclusión 41
15. Bibliografía 42

1. Resumen

El presente documento o informe se realizan las actividades de los escenarios propuestos en pruebas de habilidades CCNA representando la topología de red para la aprobación del diplomado de profundización cisco.

Los dos escenarios proponen ciudades como Medellín, Cali y Bogotá lugares geográficos de Colombia, donde se requiriere la configuración de interconexiones de los dispositivos planteados en dicha topología de red establecidos.

Esta actividad se puede desarrollar en cualquiera de las siguientes herramientas: Packet Tracer o Gns3, para nuestra simulación trabajaremos con Packet Tracer y los requerimientos de dicha topología como lo presenta la guía de actividades.

Los problemas propuestos son de descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros

2. Abstract

This document or report carries out the activities of the scenarios proposed in CCNA skills tests representing the network topology for the approval of the cisco deepening diploma.

The two scenarios propose cities such as Medellín, Cali and Bogotá, geographical locations of Colombia, where the interconnection configuration of the devices proposed in said established network topology is required.

This activity can be developed in any of the following tools: Packet Tracer or Gns3, for our simulation we will work with Packet Tracer and the requirements of said topology as presented by the activity guide.

The proposed problems are a detailed description of the step by step of each of the stages carried out during its development, the registration of connectivity verification processes through the use of ping, traceroute, show ip route commands, among others.

3. Introducción

En el presente trabajo se pretende demostrar los conocimientos obtenidos durante el desarrollo del diplomado de profundización cisco CCNA.

Las actividades que se desarrollaron durante el semestre se ven reflejado en el siguiente trabajo temas que fueron llevados en la plataforma de cisco tratando así los capítulos del 1 al 11 de CCNA 1 y CCNA 2; donde se desarrollan los conceptos de routing, enrutamiento entre Vlan por medio de protocolos aplicados en cada dispositivo del simulador de Packet tracer.

Por medio de los problemas planteados en el siguiente documento se realizan soluciones que dan satisfacción a las necesidades que pide el escenario.

4. Objetivos

- Demostrar por medio de topología el desarrollo de los escenarios realizados en Packet Tracer mediante problemas planteados dar solución a dicho planteamiento aplicándolo de manera virtual para luego así llevarlo más adelante a la parte física.

- Ejecutar los conocimientos en entornos controlados con diferentes situaciones que exponen problemáticas que se deben solucionar mediante los conocimientos del curso de profundización.

- Mejorar como futuros profesionales en el entorno en redes completamente certificados mediante el cumplimiento de objetivos concretos y desarrollos de problemáticas concretas acerca de los posibles ambientes que se presentan en un entorno de redes.

5. Desarrollo de los dos escenarios

Evaluación –Prueba de habilidades prácticas CCNA

Descripción general de la prueba de habilidades

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

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

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

- Es muy importante mencionar que esta actividad es de carácter **INDIVIDUAL y OBLIGATORIA.**
- Toda evidencia de **copy-paste o plagio (de la web o de otros informes)** será penalizada con severidad.

Lineamientos para la elaboración del Informe

Finalmente, el informe a presentar deberá cumplir con las normas **ICONTEC 1486** para la presentación de trabajos escritos e incluir los siguientes elementos en su

- **Portada (**no registre su número de identificación**)**
- **Tabla de contenido**
- **Resumen**
- **Abstract**
- **Introducción**
- **Objetivos**
- **Desarrollo de los dos escenarios**
  IMPORTANTE: Para cada uno de los escenarios se debe describir el paso a paso de cada punto realizado y deben digitar el código de configuración aplicado (no incluir imágenes ni capturas de pantalla). Las imágenes o capturas de pantalla sólo serán usadas para evidenciar los resultados de comandos como **ping, traceroute, show ip route, entre otros.**
- **Conclusiones**
- **Bibliografía**

El informe deberá estar acompañado de las respectivas evidencias de configuración de los dispositivos (Packet Tracer ó GNS3), las cuales generarán veracidad al trabajo realizado. **El informe deberá ser entregado en el espacio creado para tal fin en el Campus**.

IMPORTANTE: Teniendo en cuenta que este documento deberá ser entregado al final del curso en el **Repositorio Institucional**, acorde con los lineamientos institucionales para grado. El procedimiento será socializado al finalizar el curso, pero puede ir revisando este link. (Lineamientos para el estudiante que carga trabajo de grado)

6. Escenario 1

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

Topología de red

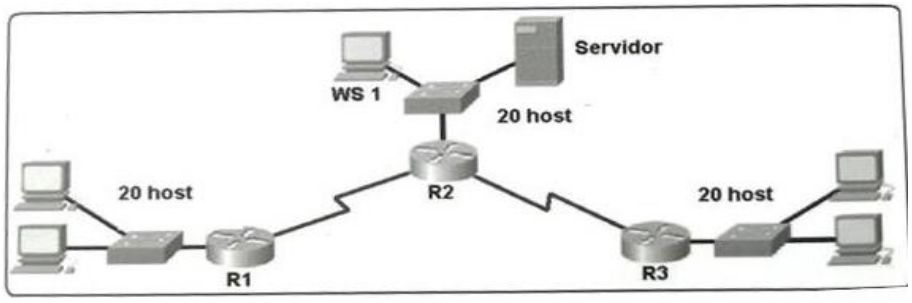
Los requerimientos solicitados son los siguientes:

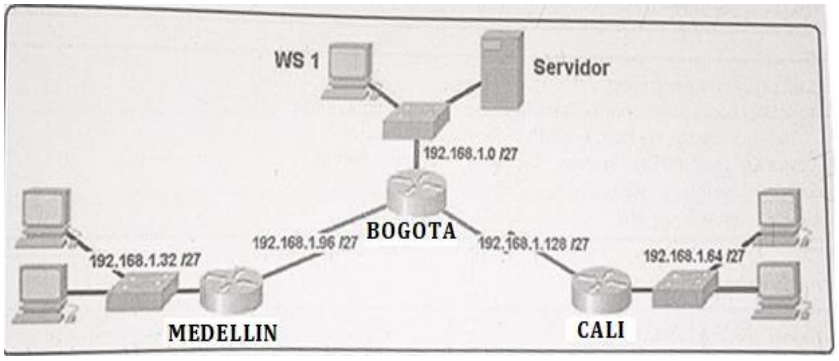
Parte 1: Para el direccionamiento IP debe definirse una dirección de acuerdo con el número de hosts requeridos.

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

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

Parte 4: Implementar la seguridad en la red, se debe restringir el acceso y comunicación entre hosts de acuerdo con los requerimientos del administrador de red.
Parte 5: Comprobación total de los dispositivos y su funcionamiento en la red. Parte 6: Configuración final.





Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

7. Parte 1: Asignación de direcciones IP

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

RED 0	RED	192.168.1.0
	PRIMERO	192.168.1.1
	ULTIMA	192.168.1.30
	BROADCAST	192.168.1.31
RED 1	RED	192.168.1.32
	PRIMERO	192.168.1.33
	ULTIMA	192.168.1.62
	BROADCAST	192.168.1.63
RED 2	RED	192.168.1.64
	PRIMERO	192.168.1.65
	ULTIMA	192.168.1.94
	BROADCAST	192.168.1.95
RED 3	RED	192.168.1.96
	PRIMERO	192.168.1.97
	ULTIMA	192.168.1.126
	BROADCAST	192.168.1.127
RED 4	RED	192.168.1.128
	PRIMERO	192.168.1.129
	ULTIMA	192.168.1.158
	BROADCAST	192.168.1.159
RED 5	RED	192.168.1.160
	PRIMERO	192.168.1.161
	ULTIMA	192.168.1.190
	BROADCAST	192.168.1.191
RED 6	RED	192.168.1.192
	PRIMERO	192.168.1.193
	ULTIMA	192.168.1.222
	BROADCAST	192.168.1.223
RED 7	RED	192.168.1.224
	PRIMERO	192.168.1.225
	ULTIMA	192.168.1.254
	BROADCAST	192.168.1.255

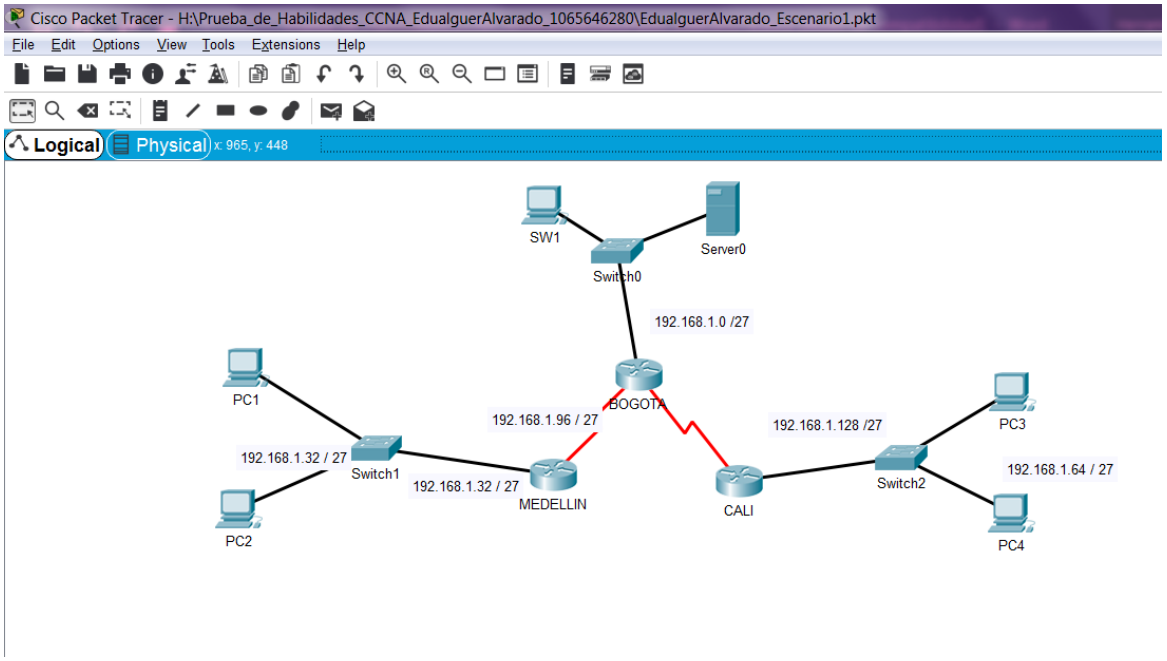
a. Asignar una dirección IP a la red.

Se le asigna la dirección Ip:192.168.1.0

8. Parte 2: Configuración Básica.

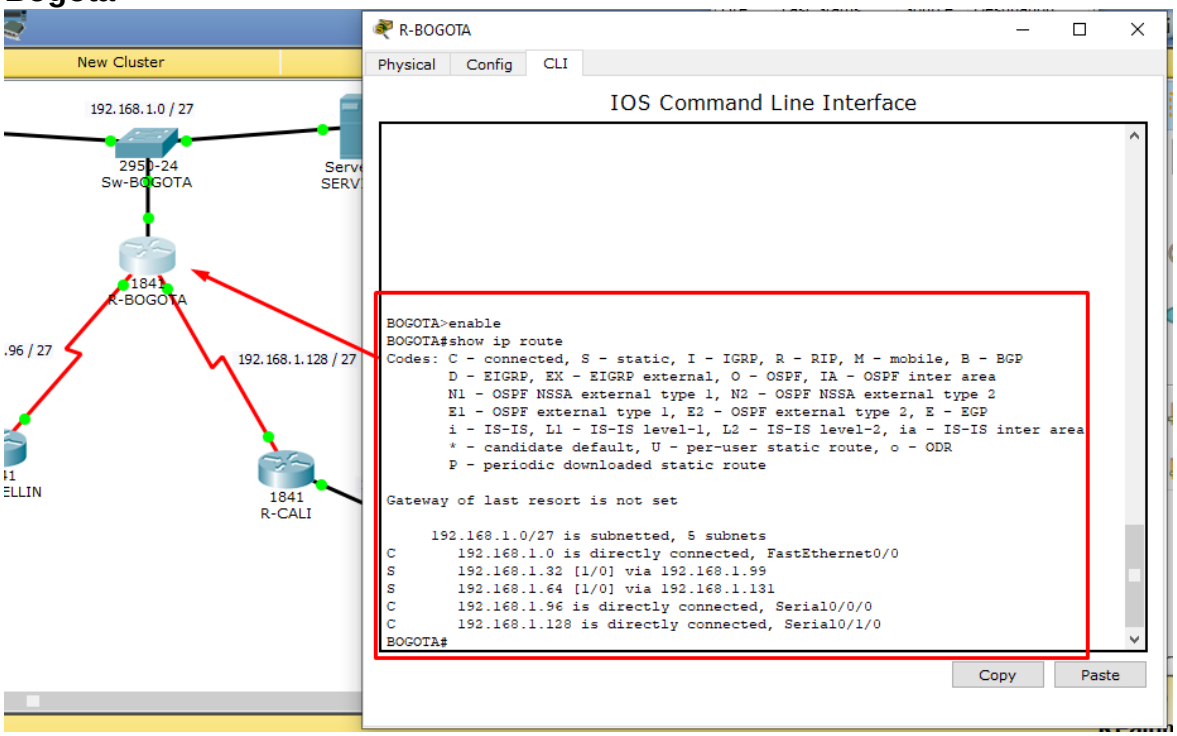
a. Completar la siguiente tabla con la configuración básica de los routers, teniendo en cuenta las subredes diseñadas.

	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



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

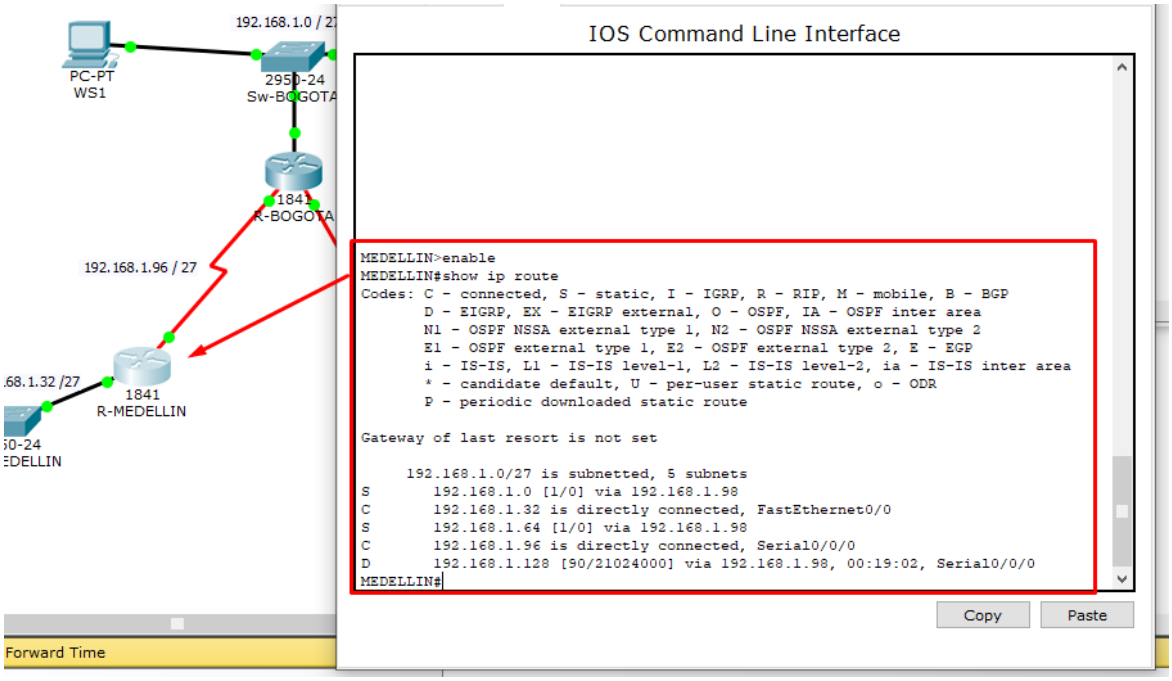
Bogotá



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
S 192.168.1.32 [1/0] via 192.168.1.99
S 192.168.1.64 [1/0] via 192.168.1.131
C 192.168.1.96 is directly connected, Serial0/0/0
C 192.168.1.128 is directly connected, Serial0/1/0

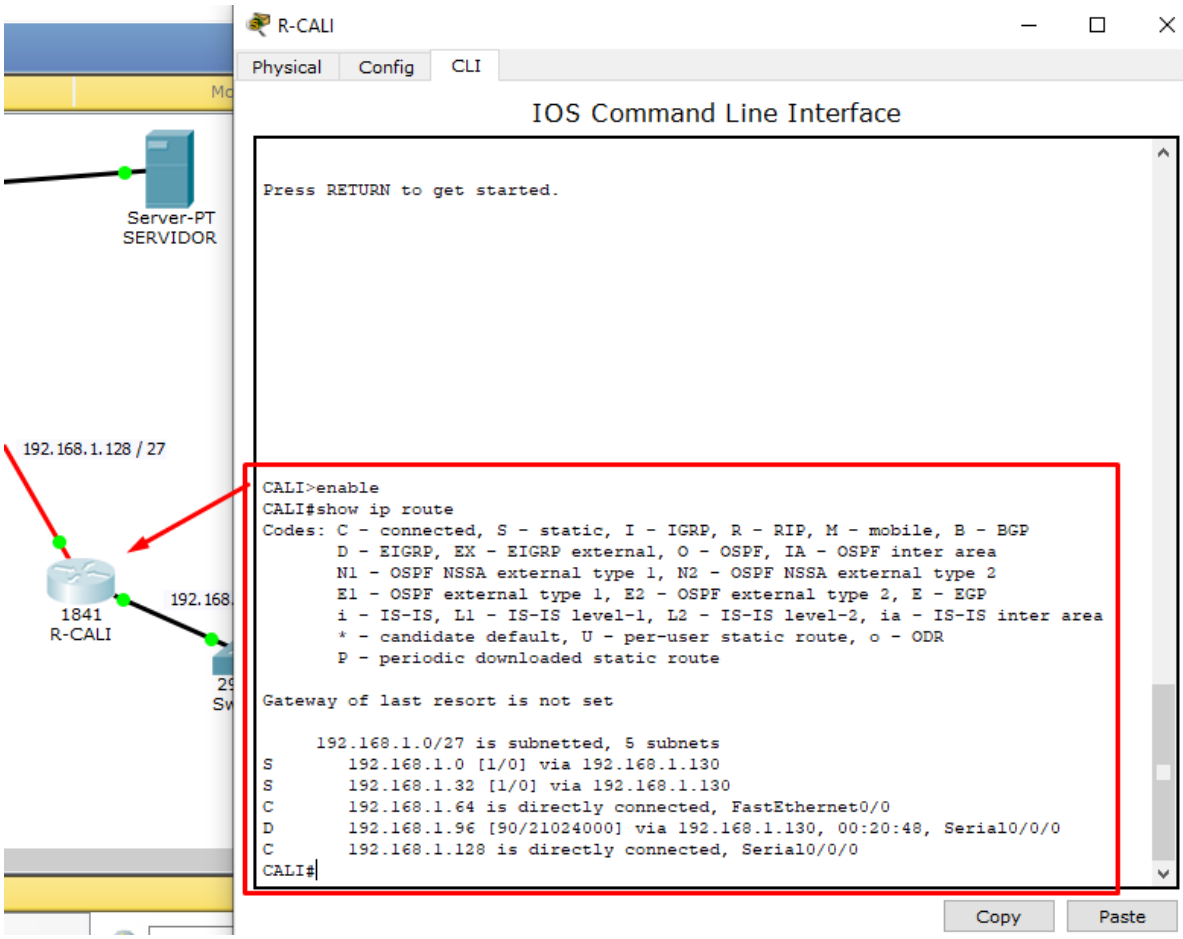
Medellín



Gateway of last resort is not set

192.168.1.0/27 is subnetted, 5 subnets
S 192.168.1.0 [1/0] via 192.168.1.98
C 192.168.1.32 is directly connected, FastEthernet0/0
S 192.168.1.64 [1/0] via 192.168.1.98
C 192.168.1.96 is directly connected, Serial0/0/0
D 192.168.1.128 [90/21024000] via 192.168.1.98, 00:19:02, Serial0/0/0

Cali



Gateway of last resort is not set

192.168.1.0/27 is subnetted, 5 subnets
S 192.168.1.0 [1/0] via 192.168.1.130
S 192.168.1.32 [1/0] via 192.168.1.130
C 192.168.1.64 is directly connected, FastEthernet0/0
D 192.168.1.96 [90/21024000] via 192.168.1.130, 00:20:48, Serial0/0/0
C 192.168.1.128 is directly connected, Serail0/0/0

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

Bogotá

show ip eigrp traffic 200
IP-EIGRP Traffic Statistics for process 200
Hellos sent/received: 18871/12575
Updates sent/received: 22/30
Queries sent/received: 4/0
Replies sent/received: 0/2
Acks sent/received: 30/19
Input queue high water mark 1, 0 drops
SIA-Queries sent/received: 0/0
SIA-Replies sent/received: 0/0

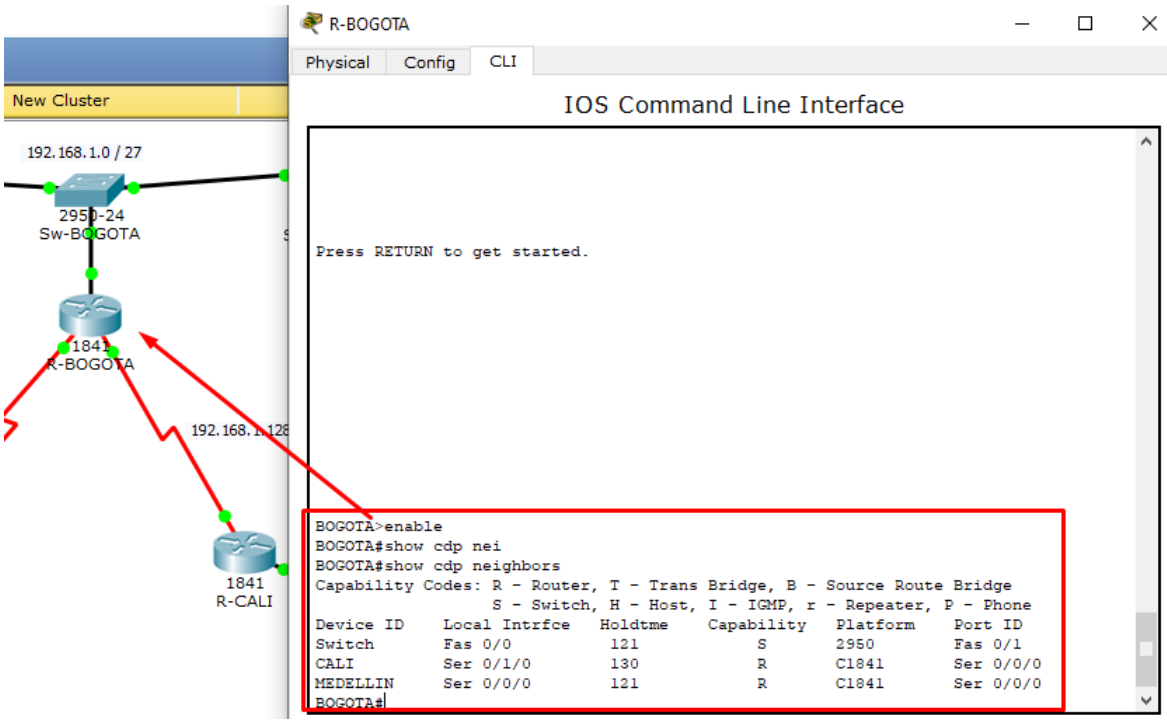
Medellín

IP-EIGRP Traffic Statistics for process 200
Hellos sent/received: 12624/6305
Updates sent/received: 16/10
Queries sent/received: 0/0
Replies sent/received: 0/0
Acks sent/received: 10/16
Input queue high water mark 1, 0 drops
SIA-Queries sent/received: 0/0
SIA-Replies sent/received: 0/0

Cali
IP-EIGRP Traffic Statistics for process 200
Hellos sent/received: 445/220
Updates sent/received: 4/4
Queries sent/received: 0/0
Replies sent/received: 0/0
Acks sent/received: 4/4
Input queue high water mark 1, 0 drops
SIA-Queries sent/received: 0/0
SIA-Replies sent/received: 0/0

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

Bogotá

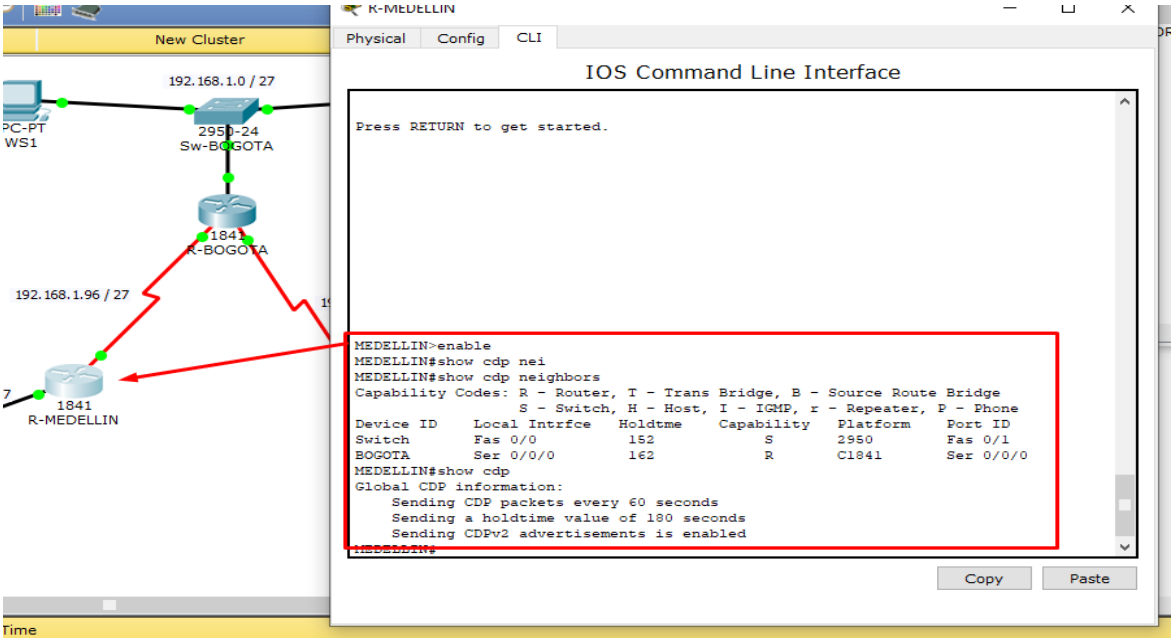


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
Switch	Fas 0/0	121	S	2950	Fas 0/1
CALI	Ser 0/0/1	130	R	C1841	Ser 0/0/0
MEDELLIN	Ser 0/0/0	121	R	C1841	Ser 0/0/0

Medellín



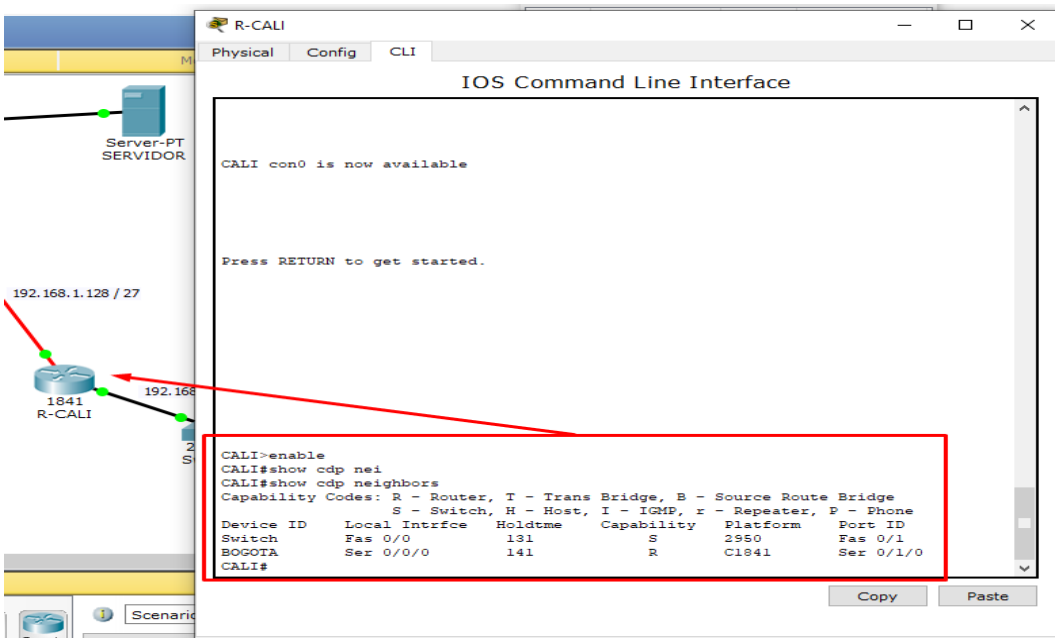
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
Switch	Fas 0/0	152	S	2950	Fas 0/1
BOGOTA	Ser 0/0/0	162	R	C1841	Ser 0/0/0

Global CDP information:
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds
Sending CDPv2 advertisements is enabled

Cali

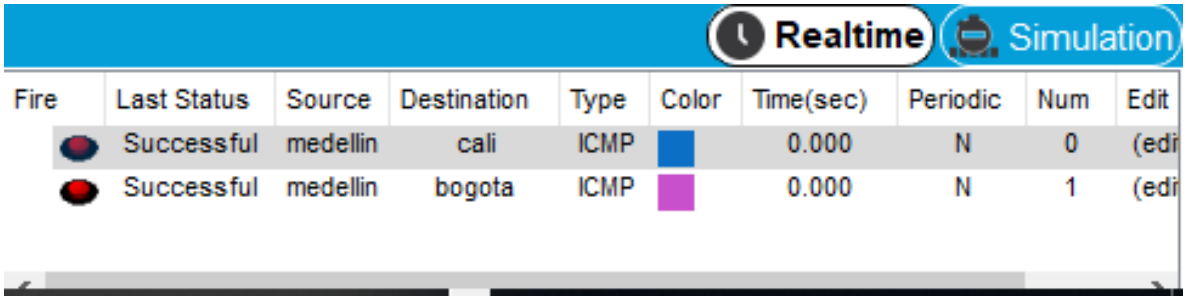


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge

S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

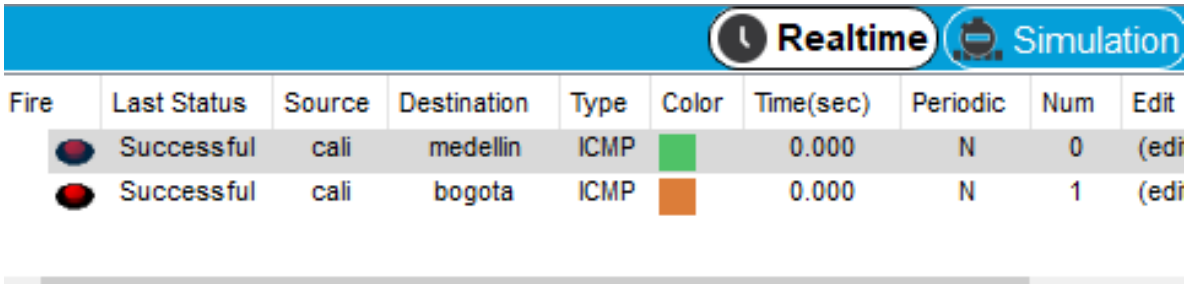
Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
Switch	Fas 0/0	131	S	2950	Fas 0/1
BOGOTA	Ser 0/0/0	141	R	C1841	Ser 0/1/0

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



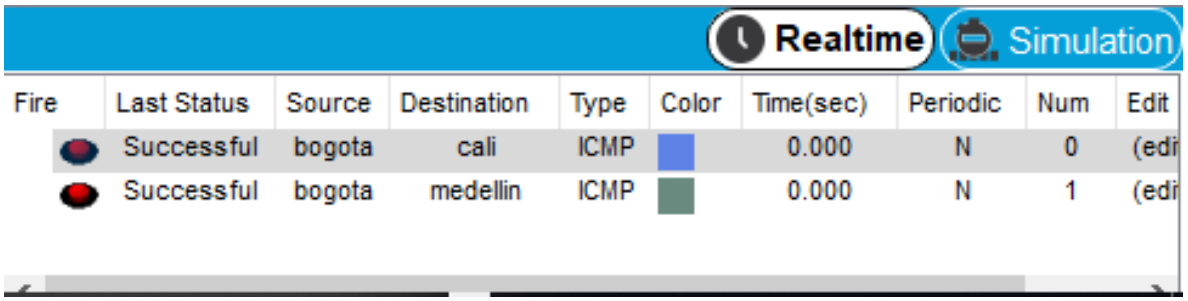
Realtime Simulation

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	medellin	cali	ICMP		0.000	N	0	(edi
	Successful	medellin	bogota	ICMP		0.000	N	1	(edi



Realtime Simulation

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	cali	medellin	ICMP		0.000	N	0	(edi
	Successful	cali	bogota	ICMP		0.000	N	1	(edi



Realtime Simulation

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	bogota	cali	ICMP		0.000	N	0	(edi
	Successful	bogota	medellin	ICMP		0.000	N	1	(edi

9. Parte 3: Configuración de Enrutamiento.

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

Para asignarle el protocolo a cada router es necesario ejecutar los siguientes comandos:

Bogotá

```
BOGOTA>enable
BOGOTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA (config)#router eigrp 1
BOGOTA (config-router) #network 192.168.1.96 0.0.0.31
BOGOTA (config-router)
%DUAL-5-NBRCHANGER: IP-EIGRP 1: Neighbor 192.168.1.99 (Serail0/0/0) is up:
new adjacency

BOGOTA (config-router)#network 192.168.1.0 0.0.0.31
BOGOTA (config-router)#network 192.168.1.128 0.0.0.31
%DUAL-5-NBRCHANGER: IP-EIGRP 1: Neighbor 192.168.1.131 (Serail0/1/0) is
up: new adjacency
```

Medellín

```
MEDELLIN>enable
MEDELLIN#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN (config)#router eigrp 1
MEDELLIN (config-router)#network 192.168.1.32 0.0.0.31
MEDELLIN (config-router)#network 192.168.1.96 0.0.0.31
```

Cali

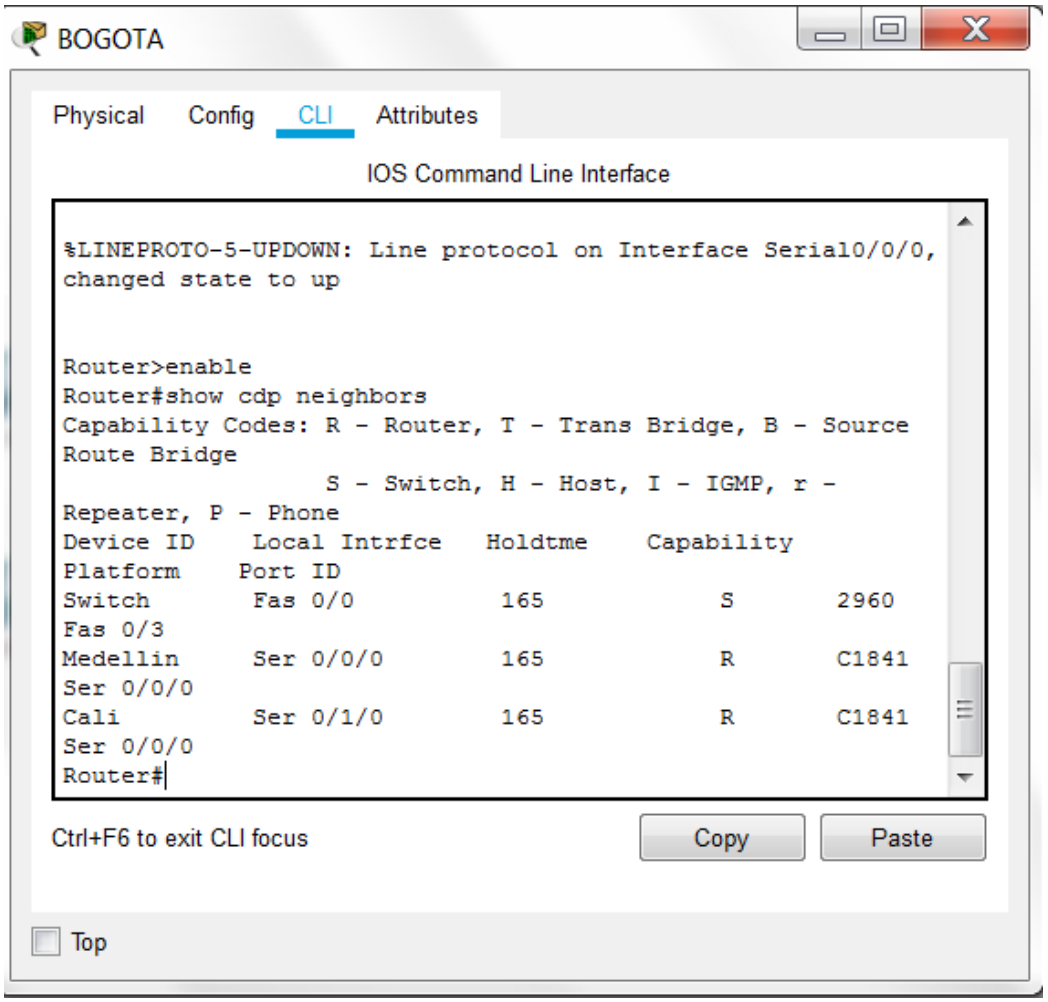
```
CALI>enable
CALI#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CALI (config)#router eigrp 1
CALI (config-router)#network 192.168.1.128 0.0.0.31
%DUAL-5-NBRCHANGER: IP-EIGRP 1: Neighbor 192.168.1.130 (Serail0/0/0) is
up: new adjacency
```

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

Bogotá

bogota#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	165	S	2960	Fas 0/3
Medellin	Ser 0/0/0	165	R	C1841	Ser 0/0/0
Cali	Ser 0/1/0	165	R	C1841	Ser 0/0/0



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

Bogotá

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 [90/20514560] via 192.168.1.99, 00:42:09, Serial0/0/0
D 192.168.1.64 [90/20514560] via 192.168.1.131, 00:37:32, Serail0/1/0
C 192.168.1.96 is directly connected, Serial0/0/0
C 192.168.1.128 is directly connected, Serial0/1/0

Medellín

Gateway of last resort is not set

192.168.1.0/27 is subnetted, 5 subnets
D 192.168.1.0 [90/20514560] via 192.168.1.98, 00:43:12, Serial0/0/0
C 192.168.1.32 is directly connected, FastEthernet0/0
D 192.168.1.64 [90/21026560] via 192.168.1.98, 00:40:23, Serail0/0/0
C 192.168.1.96 is directly connected, Serial0/0/0
D 192.168.1.128 [90/21024000] via 192.168.1.98, 00:42:42, Serial0/0/0

Cali

Gateway of last resort is not set

192.168.1.0/27 is subnetted, 5 subnets
D 192.168.1.0 [90/20514560] via 192.168.1.130, 00:39:47, Serial0/0/0
D 192.168.1.32 [90/21026560] via 192.168.1.130, 00:39:47, Serial0/0/0
C 192.168.1.64 is directly connected, FastEthernet0/0
D 192.168.1.96 [90/21024000] via 192.168.1.130, 00:39:47, Serial0/0/0
C 192.168.1.128 is directly connected, Serial0/0/0

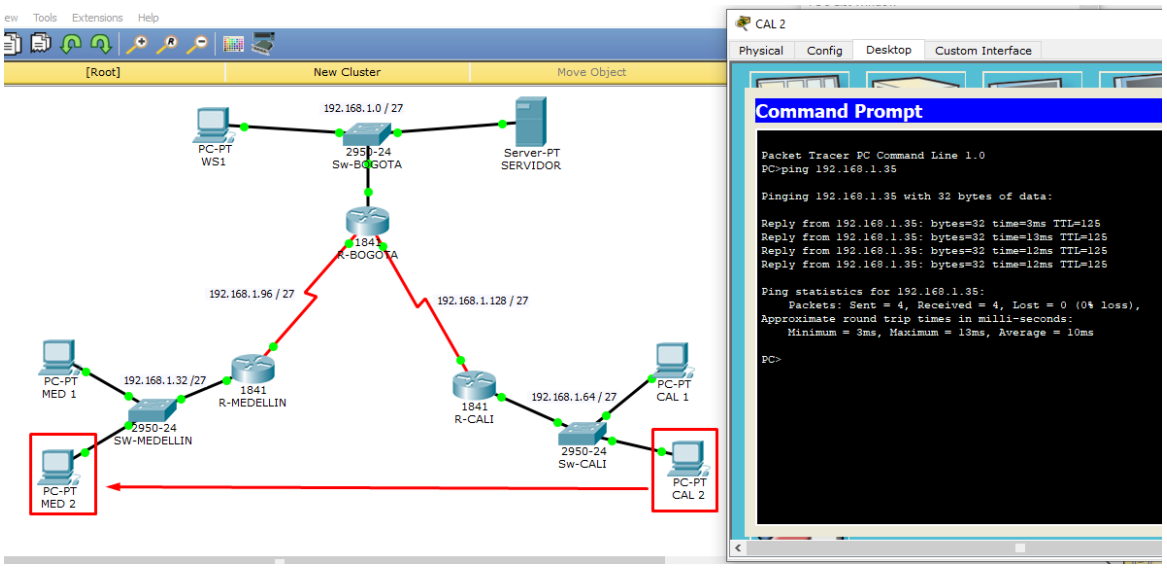
d. Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí. Realizar esta prueba desde un host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor.

De Cali a Medellín si se tiene respuestas.

PC:\>ping 192.168.1.35
Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168.1.35: bytes=32 time=3ms TTL=125
Reply from 192.168.1.35: bytes=32 time=13ms TTL=125
Reply from 192.168.1.35: bytes=32 time=12ms TTL=125
Reply from 192.168.1.35: bytes=32 time=12ms TTL=125

Ping statistics for 192.168.1.35:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 13ms, Average = 10ms



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

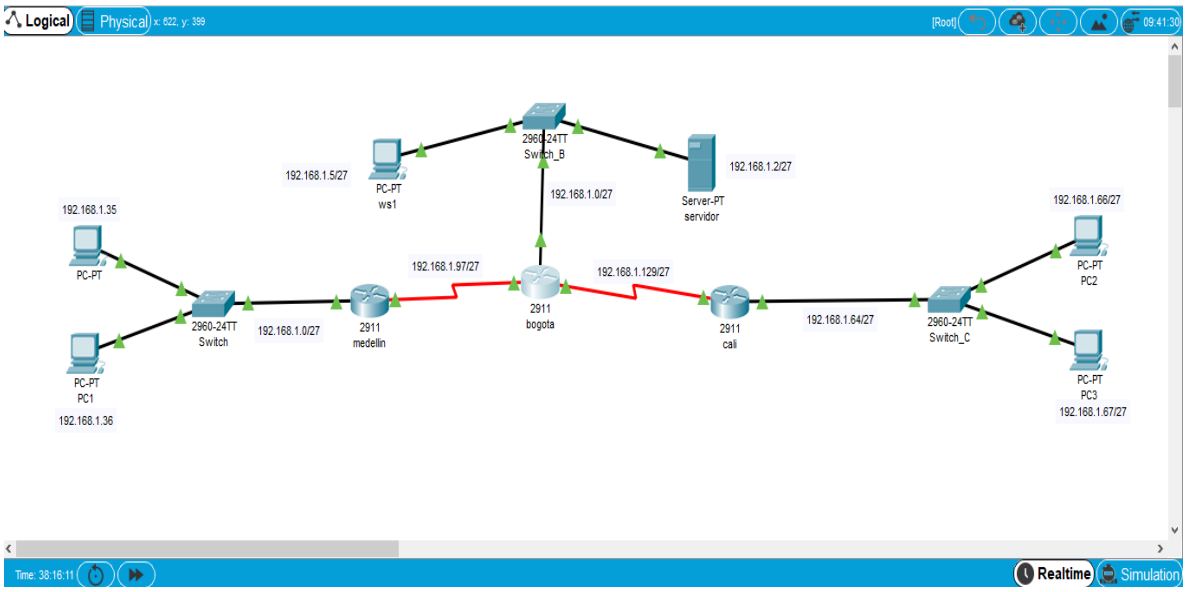
En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo. El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers. Las condiciones para crear las ACL son las siguientes:

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

Enter configuration commands, one per line. End with CNTL/Z.
(config)#access-list 90 deny 192.168.1.32 0.0.0.31
(config)#access-list 91 permit host 192.168.1.2
(config)#inter g0/0
(config-if) #ip access-group 90 out
(config-if) #ip access-group 91 out
(config-if) #exit
(config) #

Se puede evidenciar que el Access List no permite el tráfico a los equipos que no se encuentren dentro de la Red y el Access List 91 permite que tenga acceso al Servidor que se encuentra en la Localidad de Bogotá.

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.



Podemos evidenciar que se obtiene respuesta hacia el ws1como lo pide en la guía.

C:\>ping 192.168.1.66
Pinging 192.168.1.66 with 32 bytes of data:
Reply from 192.168.1.131: Destination host unreachable.
Reply from 192.168.1.131: Destination host unreachable.
Ping statistics for 192.168.1.66:
Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),

```
Control-C
^C
C:\>ping 192.168.1.66

Pinging 192.168.1.66 with 32 bytes of data:

Reply from 192.168.1.131: Destination host unreachable.
Reply from 192.168.1.131: Destination host unreachable.

Ping statistics for 192.168.1.66:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
```

Desde el servidor si se tiene respuesta

C:\>ping 192.168.1.35
Pinging 192.168.1.35 with 32 bytes of data:
Reply from 192.168.1.35: bytes=32 time=3ms TTL=126
Reply from 192.168.1.35: bytes=32 time=0ms TTL=126
Reply from 192.168.1.35: bytes=32 time=1ms TTL=126
Ping statistics for 192.168.1.35:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 5ms, Average = 2ms

C:\>ping 192.168.1.66
Pinging 192.168.1.66 with 32 bytes of data:
Reply from 192.168.1.66: bytes=32 time=0ms TTL=126
Reply from 192.168.1.66: bytes=32 time=0ms TTL=126
Reply from 192.168.1.66: bytes=32 time=0ms TTL=126
Ping statistics for 192.168.1.66:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1msControl-C

```
C:\>ping 192.168.1.35

Pinging 192.168.1.35 with 32 bytes of data:

Reply from 192.168.1.35: bytes=32 time=2ms TTL=126
Reply from 192.168.1.35: bytes=32 time=5ms TTL=126
Reply from 192.168.1.35: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.35:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms

Control-C
^C
C:\>ping 192.168.1.66

Pinging 192.168.1.66 with 32 bytes of data:

Reply from 192.168.1.66: bytes=32 time=1ms TTL=126
Reply from 192.168.1.66: bytes=32 time=1ms TTL=126
Reply from 192.168.1.66: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.66:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

Control-C
^C
C:\>
```

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.

LAN Medellín a LAN Cali

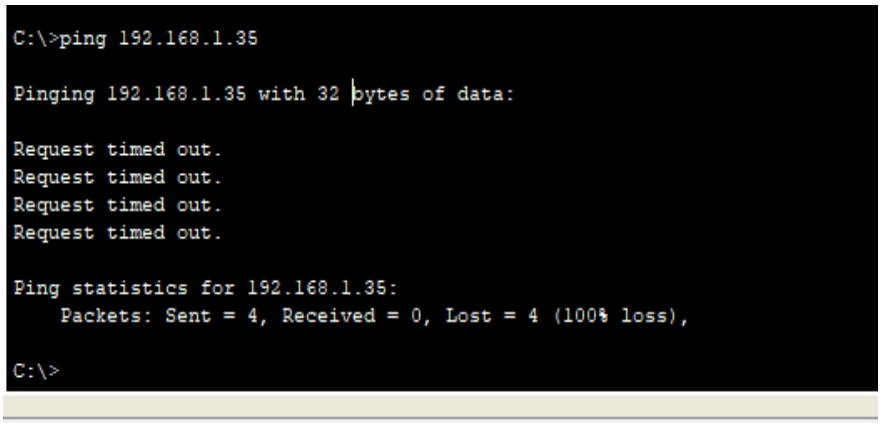
C:\>ping 192.168.1.66
Pinging 192.168.1.66 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.66:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```
C:\>ping 192.168.1.66

Pinging 192.168.1.66 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

LAN Cali a Medellín LAN

C:\>ping 192.168.1.35
Pinging 192.168.1.35 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.35:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),



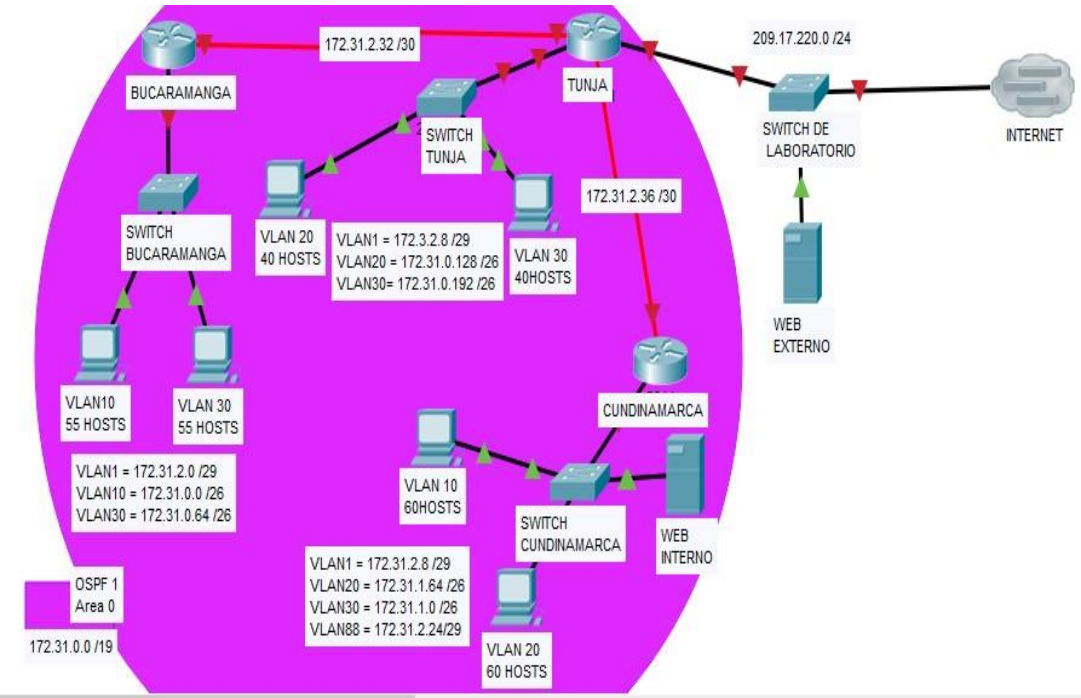
11. Parte 5: Comprobación de la red instalada.

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

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	EXITOSO
	WS_1	Router BOGOTA	EXITOSO
	Servidor	Router CALI	EXITOSO
	Servidor	Router MEDELLIN	EXITOSO
TELNET	LAN del Router MEDELLIN	Router CALI	TIME OUT
	LAN del Router CALI	Router CALI	EXITOSO
	LAN del Router MEDELLIN	Router MEDELLIN	EXITOSO
	LAN del Router CALI	Router MEDELLIN	TIME OUT
PING	LAN del Router CALI	WS_1	TIME OUT
	LAN del Router MEDELLIN	WS_1	TIME OUT
	LAN del Router MEDELLIN	LAN del Router CALI	TIME OUT
PING	LAN del Router CALI	Servidor	EXITOSO
	LAN del Router MEDELLIN	Servidor	EXITOSO
	Servidor	LAN del Router MEDELLIN	EXITOSO
	Servidor	LAN del Router CALI	EXITOSO
	Router CALI	LAN del Router MEDELLIN	TIME OUT
	Router MEDELLIN	LAN del Router CALI	TIME OUT

12. 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.



Desarrollo

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:

- **Configuración básica**

  Realizamos la configuración Inicial, luego aplicamos las configuraciones de IP y realizamos las conexiones físicas entre Reuter y Switches y LAN.

- **Configuración AAA**

  TUNJA (config)#aaa new-model

  TUNJA (config)#username cisco password 123456789
  TUNJA (config)#
  TUNJA#

BUCARAMANGA (config)#aaa new-model
BUCARAMANGA (config)#username cisco password 123456789
BUCARAMANGA (config)#

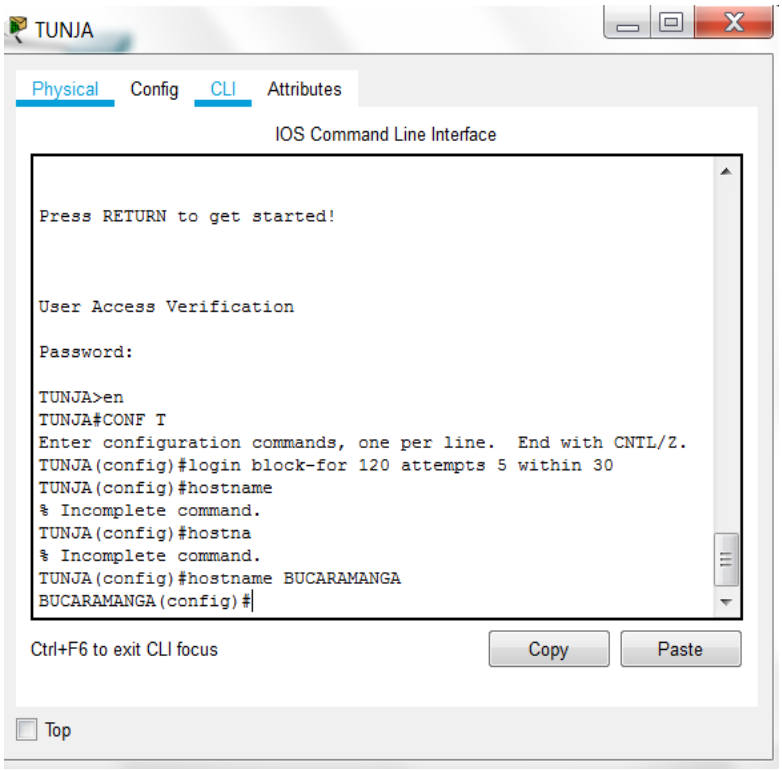
CUNDINAMARCA (config)#aaa new-model
CUNDINAMARCA (config)#username cisco password 123456789
CUNDINAMARCA (config)#

- **Cifrado de contraseñas**

  TUNJA (config)#service password-encryption
  BUCARAMANGA (config)#SERVICE Password-encryption
  CUNDINAMARCA (config)#service password-encryption

- **Un máximo de internos para acceder al Reuter.**

  TUNJA (config)#login block-for 120 attempts 5 within 30
  Router>en
  Router#conf t
  Enter configuration commands, one per line. End with CNTL/Z.
  Router(config)#login block-for 120 attempts 5 within 30
  Router(config)#hostna
  Router(config)#hostname BUCARAMANGA
  BUCARAMANGA (config)#



- **Máximo tiempo de acceso al detectar ataques.**

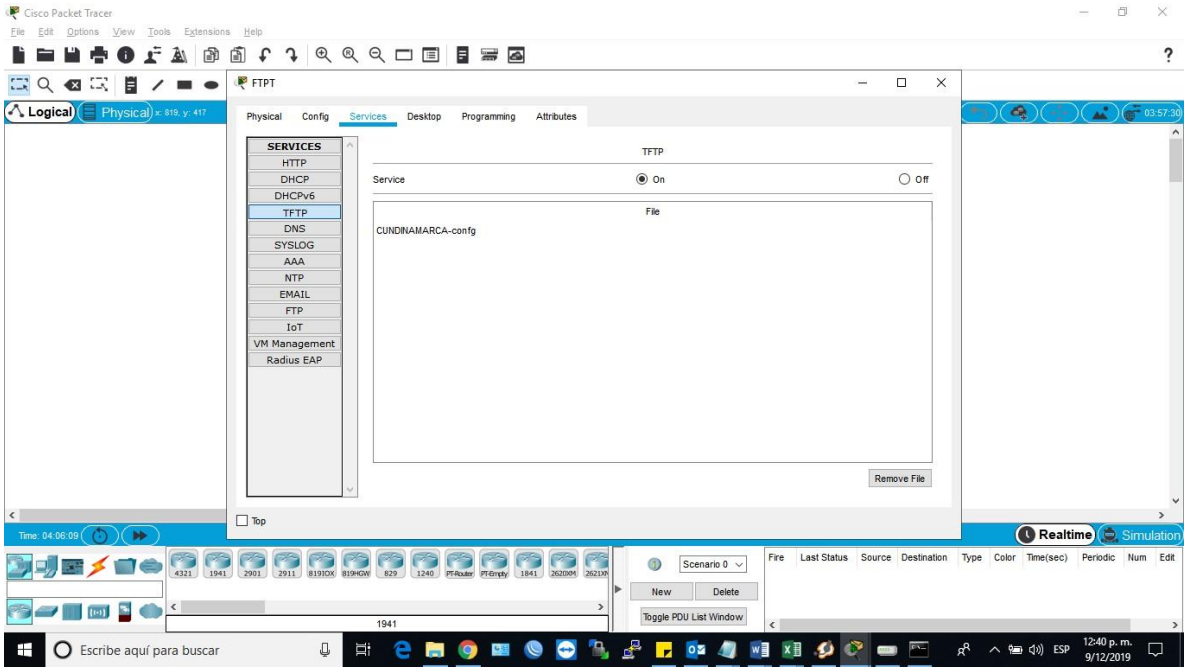
  TUNJA# configure terminal
  TUNJA (config)# line vty
  TUNJA (config-line)# no exec-timeout

  CUNDINAMARCA# configure terminal
  CUNDINAMARCA (config)# line vty
  CUNDINAMARCA (config-line)# no exec-timeout

  BUCARAMANGA# configure terminal
  BUCARAMANGA (config)# line vty
  BUCARAMANGA (config-line)# no exec-timeout

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

Guardo la configuración del Reuter en el servidor

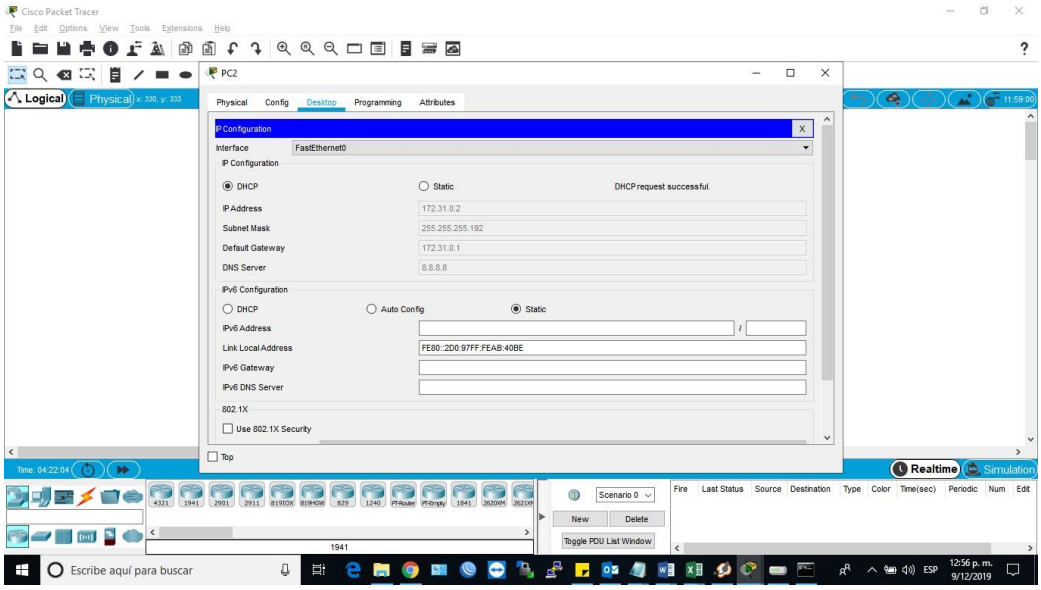


2. El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca

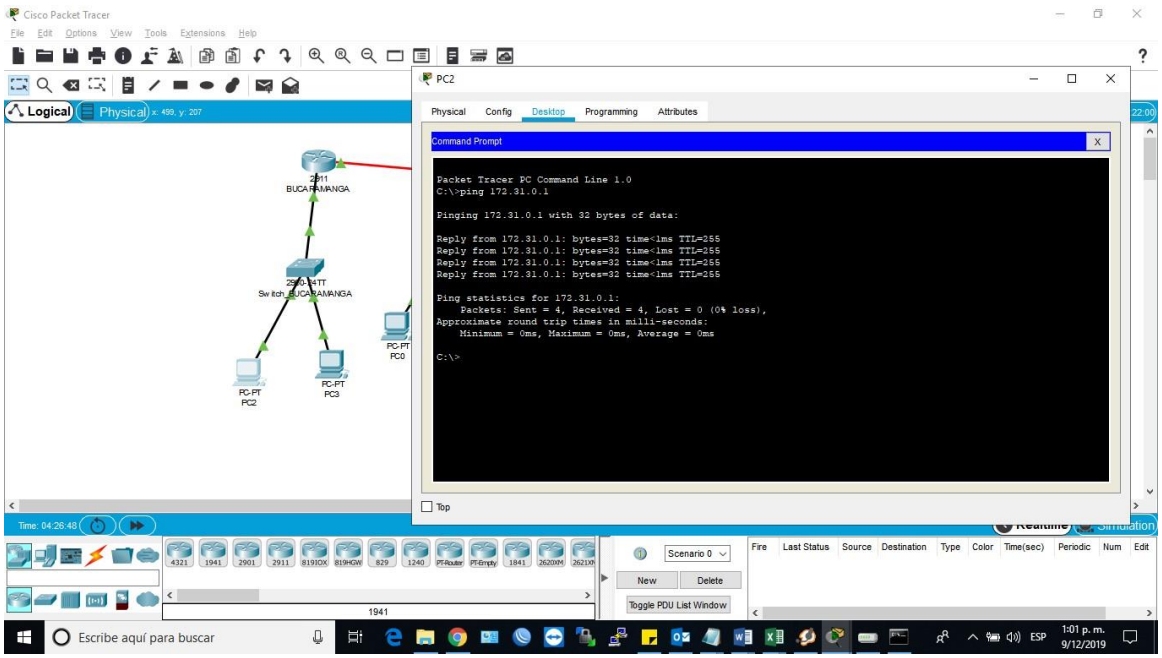
VLAN10

Switch_BUCARAMANGA (dhcp-config) #NETWORK 172.31.0.0 255.255.255.192
Switch_BUCARAMANGA (dhcp-config) #DEFAULT-ROUTER 172.31.0.1
Switch_BUCARAMANGA (dhcp-config) #DNS-SERVER 8.8.8.8
Switch_BUCARAMANGA (dhcp-config) #EXIT

DHCP de la VLAN 10



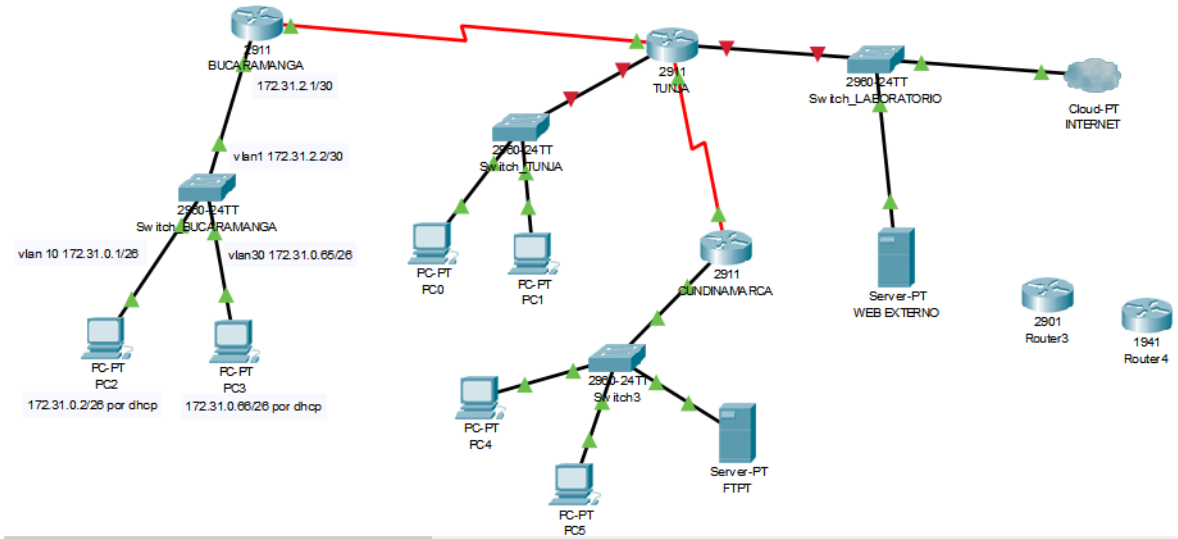
Prueba de conectividad DHCP Bucaramanga



Router de bucarmanga asociando la vlan 1 del switch

BUCARAMANGA#ping 172.31.2.2

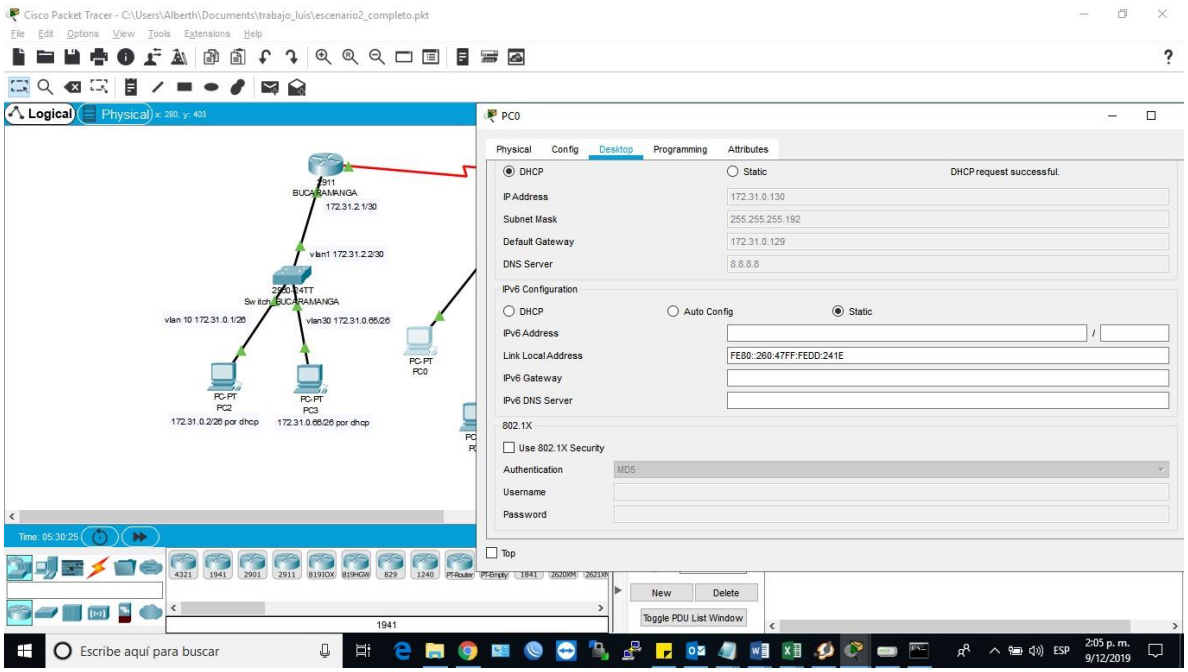
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
BUCARAMANGA#



Configuración VLAN 20

```
Switch(config-if) #ip add
Switch(config-if) #ip address 172.31.0.128 255.255.255.192
Bad mask /26 for address 172.31.0.128
Switch(config-if) #ip address 172.31.0.129 255.255.255.192
Switch(config-if) #
Switch(config-if) #
Switch(config-if) #exit
Switch(config)#dhc
Switch(config)#ip dh
Switch(config)#ip dhcp pool
Switch(config)#ip dhcp pool?
WORD Pool name
Switch(config)#ip dhcp pool vlan
Switch(config)#ip dhcp pool vlan20
Switch(dhcp-config) #?
address Configure a reserved address
default-router Default routers
dns-server Set name server
domain-name Domain name
exit Exit from DHCP pool configuration mode
network Network number and mask
no Negate a command or set its defaults
option Raw DHCP options
Switch(dhcp-config) #net
Switch(dhcp-config) #network 172.31.0.128
Switch(dhcp-config) #network 172.31.0.128 255.255.255.192
Switch(dhcp-config) #network 172.31.0.128 255.255.255.192
Switch(dhcp-config) #de
Switch(dhcp-config) #default-router 172.31.0.129
Switch(dhcp-config) #dn
Switch(dhcp-config) #dns-server 8.8.8.8
Switch(dhcp-config) #exit
Switch(config)#
```

VLAN 20 pc aprende DHCP



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

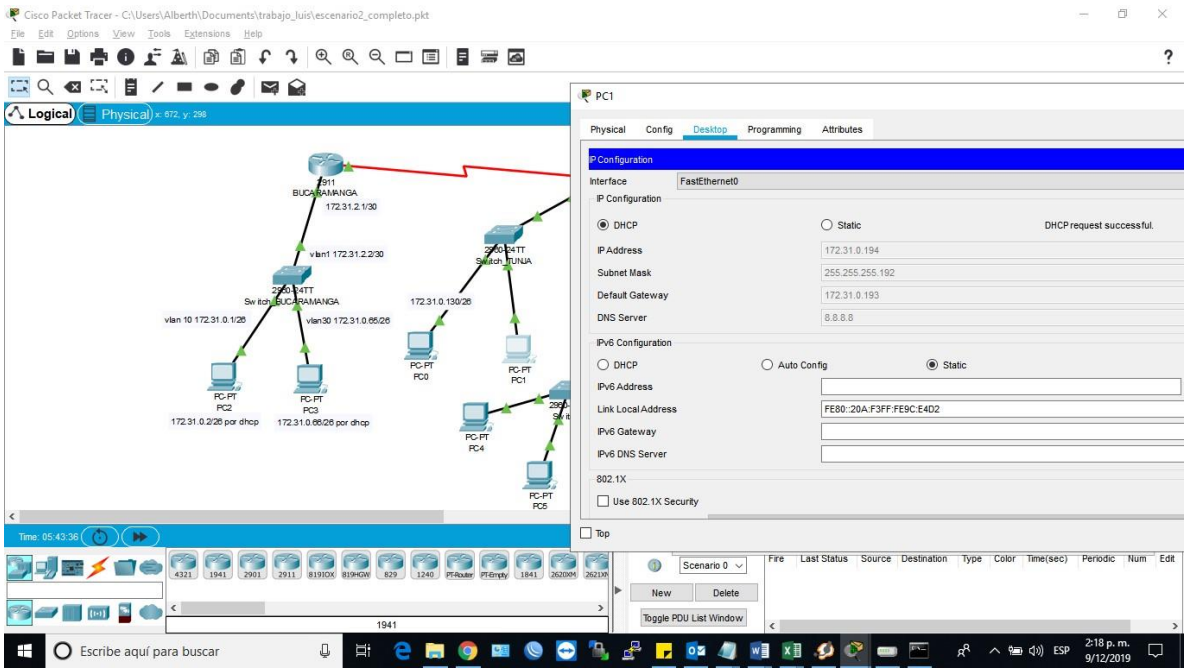
TUNJA (config)#ip nat inside source static 209.17.22.2 5.5.5.5
TUNJA (config)#inter
TUNJA (config)#interface g
TUNJA (config)#interface gigabitEthernet 0/0
TUNJA (config)#interface gigabitEthernet 0/0
TUNJA (config-if) #nat
TUNJA (config-if) #ip nat
TUNJA (config-if) #ip nat ou
TUNJA (config-if) #ip nat outside
TUNJA (config-if) #ip nat outside

Switch(config)#interface fastEthernet 0/2
Switch(config-if) #switchport access vlan 30
Switch(config-if) #exit
Switch(config)#interface vlan 30
%LINK-5-CHANGED: Interface Vlan30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up

Switch(config-if) #ip address 172.31.0.193 255.255.255.192

```
Switch(config-if) #no shutdown
Switch(config-if) #exit
Switch(config)#ip dhcp pool?
WORD Pool name
Switch(config)#ip dhcp pool vlan30
Switch(dhcp-config) #network 172.31.0.192
Switch(dhcp-config) #network 172.31.0.192 255.255.255.192
Switch(dhcp-config) #default-router 172.31.0.193
Switch(dhcp-config) #dn
Switch(dhcp-config) #dns-server 8.8.8.8
Switch(dhcp-config) #exit
Switch(config)#
```

VLAN 30 equipos aprendido DHCP-



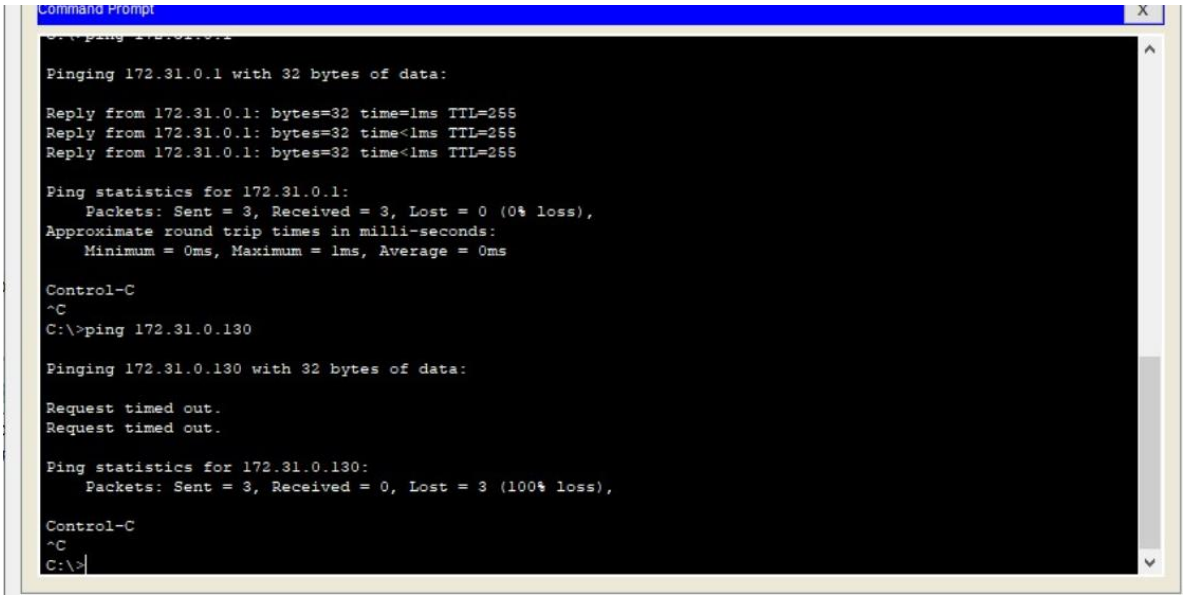
4. El enrutamiento deberá tener autenticación.

```
O - OSPF, IA - OSPF inter área
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
Gateway of last resort is not set
172.3.0.0/16 is variably subnetted, 2 subnets, 2 masks
C 172.3.2.8/29 is directly connected, GigabitEthernet0/1
L 172.3.2.9/32 is directly connected, GigabitEthernet0/1
172.31.0.0/16 is variably subnetted, 4 subnets, 2 masks
C 172.31.2.32/30 is directly connected, Serial0/0/1
L 172.31.2.33/32 is directly connected, Serial0/0/1
C 172.31.2.36/30 is directly connected, Serial0/0/0
L 172.31.2.37/32 is directly connected, Serial0/0/0
209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.17.220.0/24 is directly connected, GigabitEthernet0/0
L 209.17.220.2/32 is directly connected, GigabitEthernet0/0
```

5. Listas de control de acceso:

- Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.
- Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja
- Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.
- Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga.
- Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.
- Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.
- Los hosts de una VLAN no pueden acceder a los de otra VLAN en una ciudad.
- Solo los hosts de las VLAN administrativas y de la VLAN de servidores tienen accedo a los Reuters e internet.

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



13. Aspectos a tener en cuenta

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

14. Conclusión

En el anterior trabajo se desarrollan de manera satisfactoria la topología propuesta; escenario 1 y escenario 2 aplicando así los conocimientos adquiridos en el desarrollo del diplomado, se logran desarrollar y aplicar las configuraciones básicas de enrutamiento y protocolos de configuración.

Se llevó a cabo el diseño de topologías donde el problema era en base a tres ciudades del país de Colombia y se debía configurar según lo solicitado en el documento de pruebas de habilidades.

También aprendí a estipular la ruta definida (la ruta principal) y la sucesora (la de respaldo) en una red y a configurar el ancho de banda de las mismas y por ultimo Al desarrollar esta práctica puedo concluir que, existen protocolos sencillos y fáciles de implementar, los cuales ayudan a establecer de manera estática las direcciones IP de las diferentes interfaces de los distintos dispositivos que conforman una red; haciendo énfasis en el router, donde se pueden usar protocolos para enrutar y comunicar a diferentes redes, tanto LAN como WAN. Pues este proceso de asignar direcciones es complejo de aplicar en redes de gran tamaño.

.

15. Bibliografía

DHCP CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Obtenido de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

Configurar las Listas de acceso IP, 27 de diciembre de 2007, Obtenido de: https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.html

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

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

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

Certificación Cisco. (Internet - Wikipedia)
Recuperado de:
https://es.wikipedia.org/wiki/Certificaci%C3%B3n_Cisco

CISCO Networking Academy Program CCNA 1 and 2 - Version 3.1
Recuperado de:
https://betosamaniego.files.wordpress.com/2011/09/ccna-1-y-2.pdf