PRUEBA DE HABILIDADES PRACTICAS CCNA

DIPLOMADO DE PROFUNDIZACION CISCO CCNA

Estudiante: Luis Gabriel Dorado

Tutor: Juan Carlos Vesga

Universidad Nacional Abierta y a Distancia

Escuela de Ciencias Básicas, Tecnología e Ingeniería

Ingeniería de telecomunicaciones

Popayán

2018

Tabla de contenido

INTRODUCCION

El presente trabajo, hace parte del desarrollo de la prueba de habilidades prácticas, la cual forma parte de las actividades evaluativas de Diplomado de profundización CCNA, la cual busca identificar el nivel de desarrollo de competencias y habilidades que se adquirieron a lo largo del diplomado y a través de la cual se pondrá a prueba los grados de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

La práctica consiste en el desarrollo de las tareas asignadas en cada uno de los 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 uno de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos png, traceroute, show iproute, entre otros.

El desarrollo de la práctica es desarrollado mediante el programa PacketTracer, en el tiempo indicado de dos semanas, y de carácter individual.

1. OBJETIVOS

1.1. Objetivo General

Configuración de cada uno de los dispositivos en el escenario propuesto mediante el programa PacketTracer.

1.1. Objetivos Específicos

- documentar la solución al escenario propuesto
- configurar cada uno de los dispositivos en la solución planteada
- describir el paso a paso de cada una de las etapas realizadas durante el desarrollo de la solución propuesta
- registrar los procesos de verificación de conectividad del uso de comandos pong, tracerouter, show iprouter, entre otros.

2. PLANTEAMIENTO DEL PROBLEMA

2.1. DEFINICION

La práctica es desarrollado, desde el planteamiento de un escenario problema, en el cual se expone el caso de una empresa de tecnología, a cual posee tres sucursales, distribuidas en las ciudades de Bogotá, Medellín y Bucaramanga, en donde se es necesario configurar e interconectar entre si 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.

2.2. JUSTIFICACION

La práctica es desarrollada, con el fin de medir nuestros conocimientos adquiridos durante el desarrollo del diplomado de profundización en CCNA, en la cal de es necesario partir del escenario planteado, promoviendo una solución en donde se establezca:

- configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario
- configurar el protocolo de enrutamiento OSPFv2 bajo los criterios dados.

3. MARCO TEORICO

3.1. PROTOCOLOS DE ENRUTAMIENTO

Un protocolo de enrutamiento se define como la herramienta que permite la comunicación entre los router. La configuración permite a estos equipos seleccionar la ruta que tomara un paquete entre dos nodos en una red de computadores. Los routers sólo conocen las redes conectadas directamente a ellos y a través de los protocolos de enrutamiento los routers anuncian estas redes a los vecinos en primera instancia y luego al resto de equipos de la red, de tal forma los routers adquieren el conocimiento de la topología de la red.

Los diferentes protocolos de enteramientos activos son:

- RIP (RputingInformationProtocol): es uno de los protocolos más antiguos y es ampliamente usado en la actualidad. RIP es un protocolo que tiene como base un vector distancia que usa como métrica el conteo de saltos. este protocolo previene los loops a través de la implementación de un numero límite de saltos permitidos en los caminos de origen – destino (Sciety, 1998)
- EIGRP (Enhanced Interior Gateway RoutingProtocol): Este es un protocolo propietario de CISCO basado en IGRP (Interior Gateway RoutingProtocol). EIGRP es un protocolo de enrutamiento que se basa en vectores distancia con optimizadores para minimizar la inestabilidad de enrutamiento ante cambios en la topología de la red, el uso de ancho de banda y poder de procesamiento del Router. Los equipos que tengan este tipo de protocolo configurado distribuirán la información de enrutamiento a los vecinos con IGRP. La mayoría de las optimizaciones de enrutamiento están basadas en el DiffusingUpdateAlgorithm (DUAL) quien garantiza la operación libre de Loops y provee una convergencia más rápida de los Router

- IS-IS (Instermediantesystem to intermediatesystem): Este es un protocolo de enrutamiento de estado de conexión. Opera de manera segura enviando información de la topología a través de la red de Routers. Los paquetes se envían por el mejor camino que posee el router de la topología de la red. IS-IS es un IGP (InternalGateway Protocol), creado para el uso e un único administrador de dominio o solo una red.
- OSPF (Open ShortestPathFirst): OSPF es un protocolo de enrutameitno con dos características relevantes, es un protocolo libre y está basado en el algortimo de la ruta más corta primero (ShortestPathFirsó SPF), conocido también como algoritmo Dijkstra. Este es un protocolo basado en el estado de la conexión el cual solicita el envió de los avisos de estado de conexión (Link-StateAdvertisementsóLSAs) a todos los demásrouters que se encuentra en la misma área jerárquica. La informacion de las interfaces conectadas, las métricas usadas y otras variables son incluidas en los LSAs de OSPF. Debido a que este protocolo acumula información de los estados de conexión, este utiliza el algoritmo SPF para el cálculo del camino mas corto hacia cada nodo.
- BGP (Border Gateway rotoocol): Este protocolo direcciona el tráfico entre redes o grupo de redes que tiene un mimo administrador y políticas de enrutamiento comunes, también conocidos como sistemas autónomas. El BGP intercambia información de enrutamiento por el internet y es el protocolo usado en las IPS

  Este es un protocolo robusto y escalable; una evidencia de estas características es el hecho de que es el protocolo empleado utiliza distintos parámetros de rutas, atributos de llamada, para definir las políticas de parámetros de rutas atributos de llamada, para definir las políticas de enrutamiento y mantener un estado estable de enrutamiento. Los equipos configurados con BGP intercambian toda la información de enrutamiento con sus vecinos la primera vez que es establecida la conexión TCP.

  Cuando se genera algún cambio sobre la tabla de enrutamiento el router tan solo envía las rutas que han cambiado. BGP no realiza actualizaciones periódicas y aquellas que son enviadas solo contienen la ruta óptima para una red de destino

4. METODOLOGIA

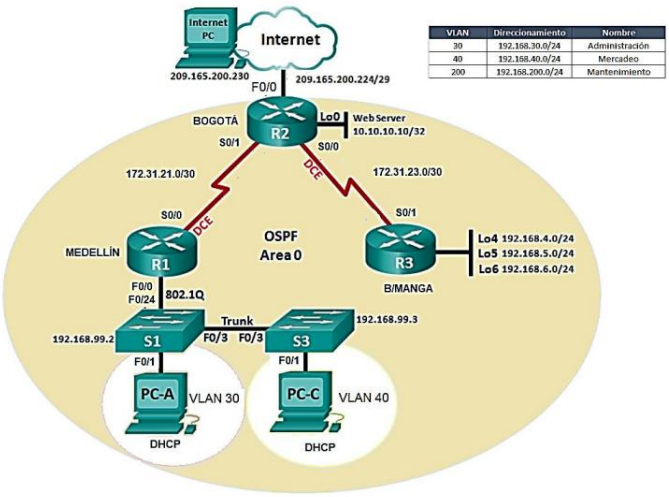
La práctica es desarrollada mediante el software Packettracer de Cisco, el cual es una herramienta que permite simular las redes generando un valor agregado, porque le permite experimentar problemáticas reales, y por ende ofrece herramientas prácticas para solucionar dichas problemáticas, agregando información a su formación profesional y laboral.

5. DESARROLLO DE LA PRÁCTICA

Descripción del escenario propuesto para la prueba de habilidades

Escenario: Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Bogotá, Medellín y Bucaramanga, 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



VLAN	Direccionamiento	Nombre
30	192.168.30.0/24	Administración
40	192.168.40.0/24	Mercadeo
200	192.168.200.0/24	Mantenimiento

1. Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario

Tabla de Direccionamiento IP

Dispositivo	Interfaz	Dirección IP
R1	Serial 0/0/0	172.31.21.1 255.255.255.252
R2	Loopback0	10.10.10.10 255.255.255.255
	Gigabit Ethernet 0/0	209.165.200.225 255.255.255.248
	Serial 0/0/0	172.31.23.1 255.255.255.252
	Serial 0/0/1	172.31.21.1 255.255.255.252
R3	Loopback4	192.168.4.1 255.255.255.0
	Loopback5	192.168.5.1 255.255.255.0
	Loopback6	192.168.6.1 255.255.255.0
	Serial 0/0/1	172.31.23.2 255.255.255.252

2. Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

OSPFv2 area 0

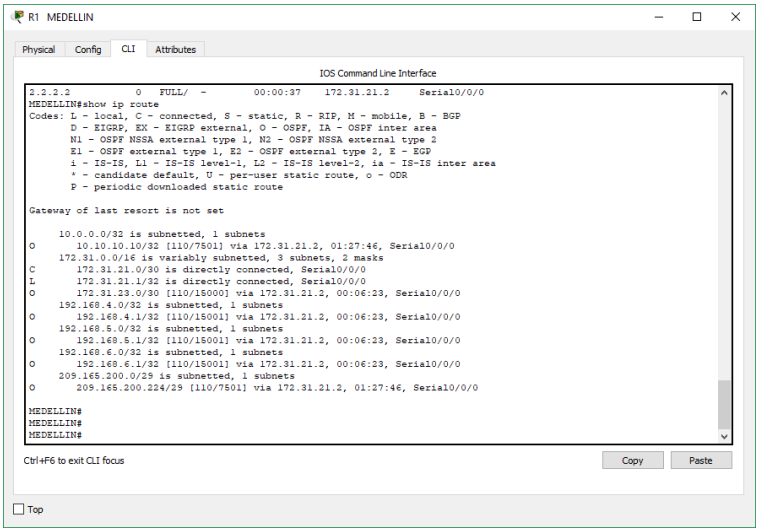
Configuration Item or Task	Specification
Router ID R1	1.1.1.1
Router ID R2	2.2.2.2
Router ID R3	3.3.3.3
Configurartodaslas interfaces LAN comopasivas	
Establecer el ancho de banda para enlaces seriales en	128 Kb/s
Ajustar el costo en la métrica de S0/0	7500

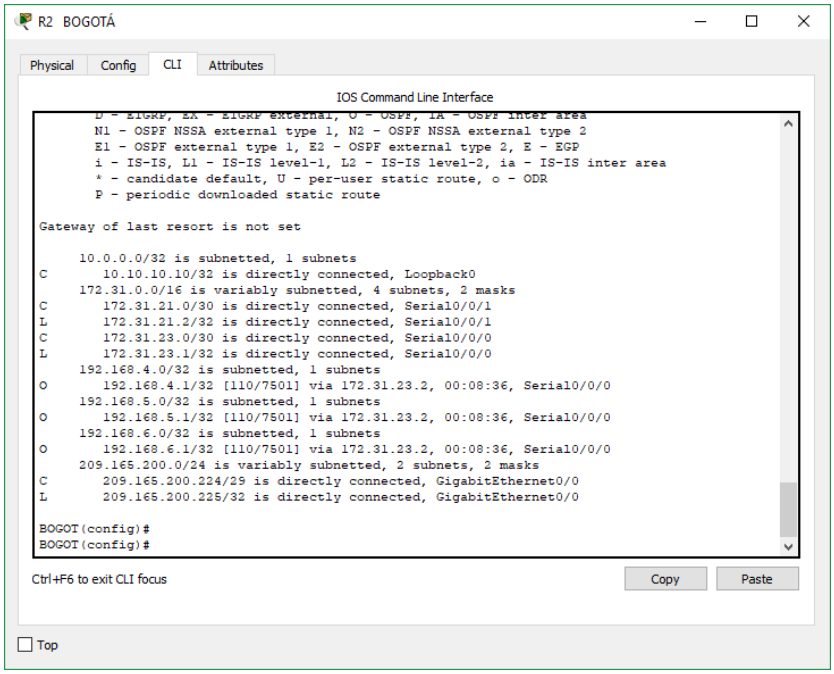
- Para configurar las interfaces como pasivas, se debe realizar dentro de la configuración del protocolo OSPF, con el comando passive-interface y la interfaz que se desee.
- Para establecer el ancho de banda en los enlaces seriales se realiza con el comando bandwith seguido del valor a asignar dentro del modo configuración de interfaz
- Para ajustar el costo en la métrica se realiza con el comando ipospfcost y el valor a asignar dentro del modo configuración de interfaz

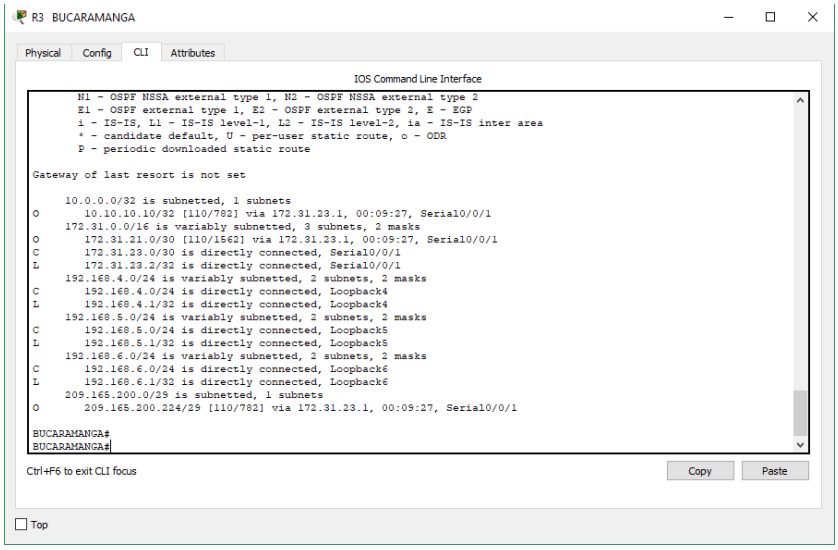
Verificar información de OSPF

• Visualizar tablas de enrutamiento y routers conectados por OSPFv2

Se pueden visualizar con el comando show iproute

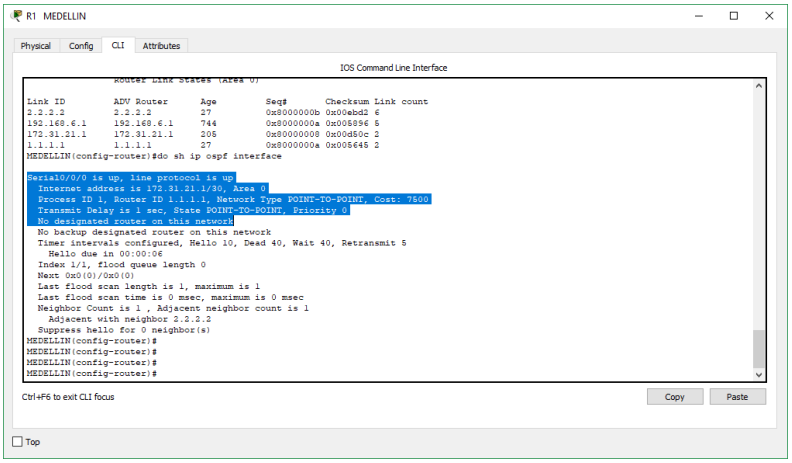


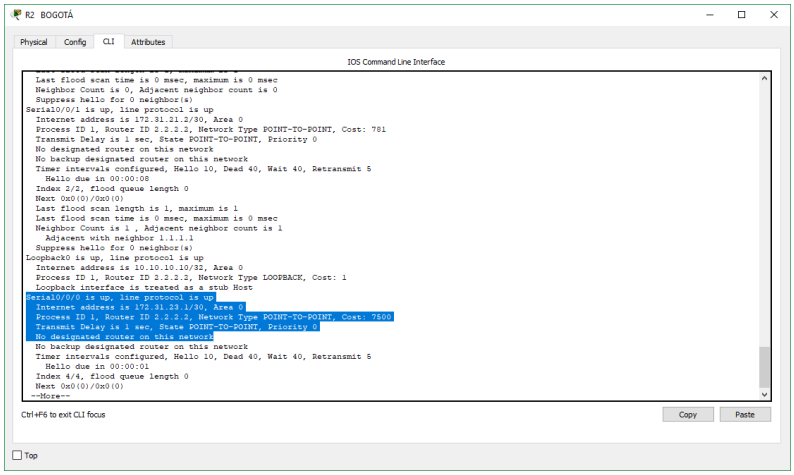


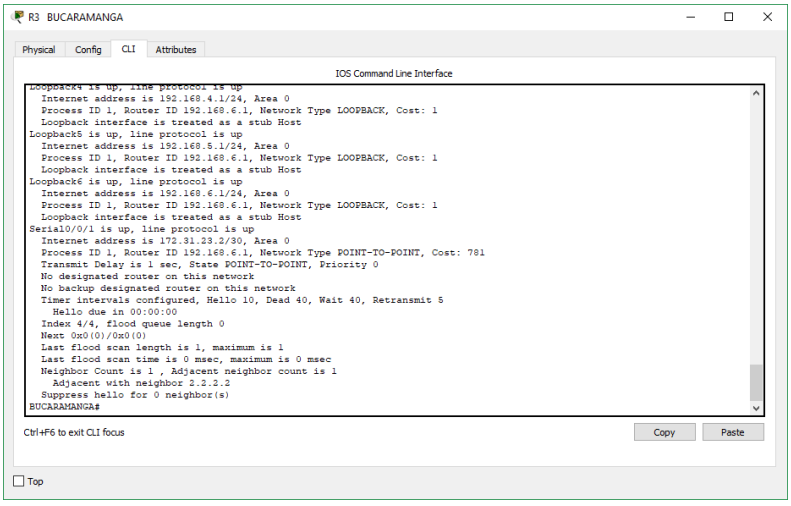


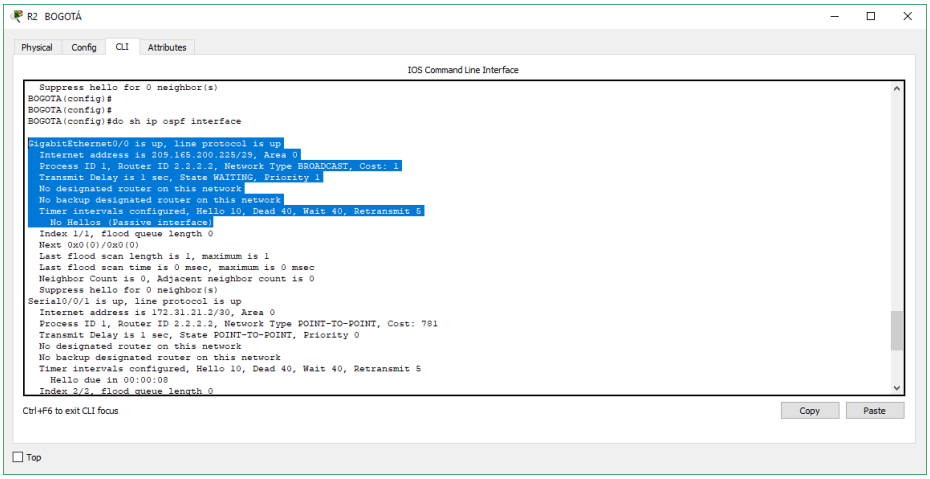
- Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface
- Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

Se puede realizar con el comando **show ipospf interface**


R1 MEDELLIN
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router Link States (Area 0)
Link ID ADV Router Age Seq# Checksum Link count
2.2.2.2 2.2.2.2 27 0x8000000b 0x00ebd2 6
192.168.6.1 192.168.6.1 744 0x8000000a 0x005896 5
172.31.21.1 172.31.21.1 205 0x80000008 0x00d50c 2
1.1.1.1 1.1.1.1 27 0x8000000a 0x005645 2
MEDELLIN(config-router)#do sh ip ospf interface
Serial0/0/0 is up, line protocol is up
Internet address is 172.31.21.1/30, Area 0
Process ID 1, Router ID 1.1.1.1, Network Type POINT-TO-POINT, Cost: 7500
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:06
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 2.2.2.2
Suppress hello for 0 neighbor(s)
MEDELLIN(config-router)#
MEDELLIN(config-router)#
MEDELLIN(config-router)#
MEDELLIN(config-router)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

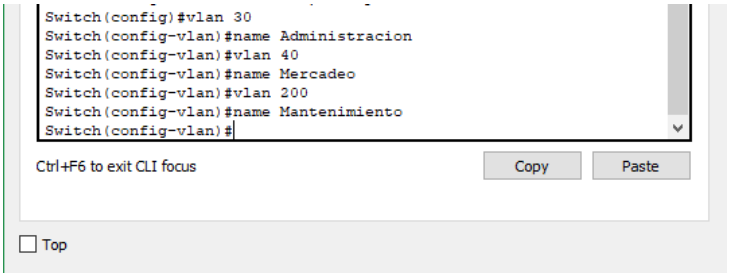

R2 BOGOTÁ
Physical
Config
CLI
Attributes
IOS Command Line Interface
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
Internet address is 172.31.21.2/30, Area 0
Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT, Cost: 781
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:08
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 1.1.1.1
Suppress hello for 0 neighbor(s)
Loopback0 is up, line protocol is up
Internet address is 10.10.10.10/32, Area 0
Process ID 1, Router ID 2.2.2.2, Network Type LOOPBACK, Cost: 1
Loopback interface is treated as a stub Host
Serial0/0/0 is up, line protocol is up
Internet address is 172.31.23.1/30, Area 0
Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT, Cost: 7500
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:01
Index 4/4, flood queue length 0
Next 0x0(0)/0x0(0)
--More--
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


R3 BUCARAMANGA
Physical
Config
CLI
Attributes
IOS Command Line Interface
Loopback4 is up, line protocol is up
Internet address is 192.168.4.1/24, Area 0
Process ID 1, Router ID 192.168.6.1, Network Type LOOPBACK, Cost: 1
Loopback interface is treated as a stub Host
Loopback5 is up, line protocol is up
Internet address is 192.168.5.1/24, Area 0
Process ID 1, Router ID 192.168.6.1, Network Type LOOPBACK, Cost: 1
Loopback interface is treated as a stub Host
Loopback6 is up, line protocol is up
Internet address is 192.168.6.1/24, Area 0
Process ID 1, Router ID 192.168.6.1, Network Type LOOPBACK, Cost: 1
Loopback interface is treated as a stub Host
Serial0/0/1 is up, line protocol is up
Internet address is 172.31.23.2/30, Area 0
Process ID 1, Router ID 192.168.6.1, Network Type POINT-TO-POINT, Cost: 781
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:00
Index 4/4, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 2.2.2.2
Suppress hello for 0 neighbor(s)
BUCARAMANGA#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

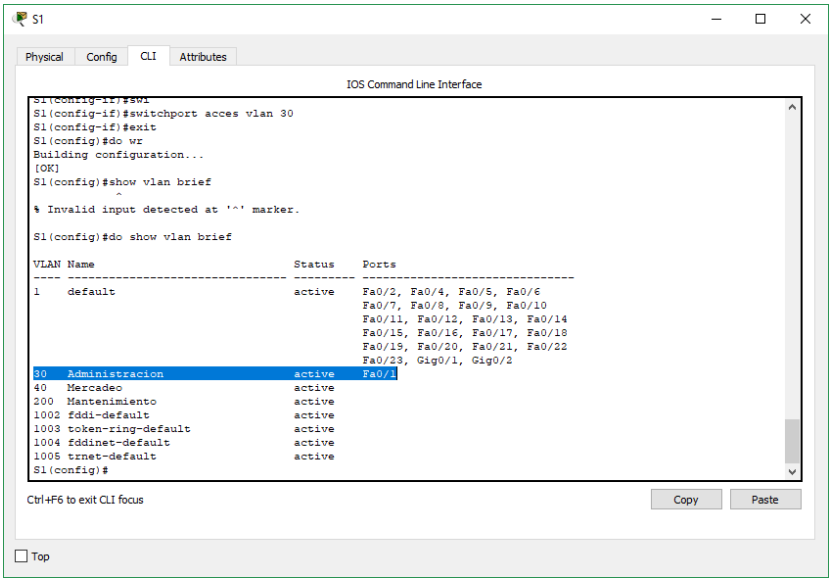


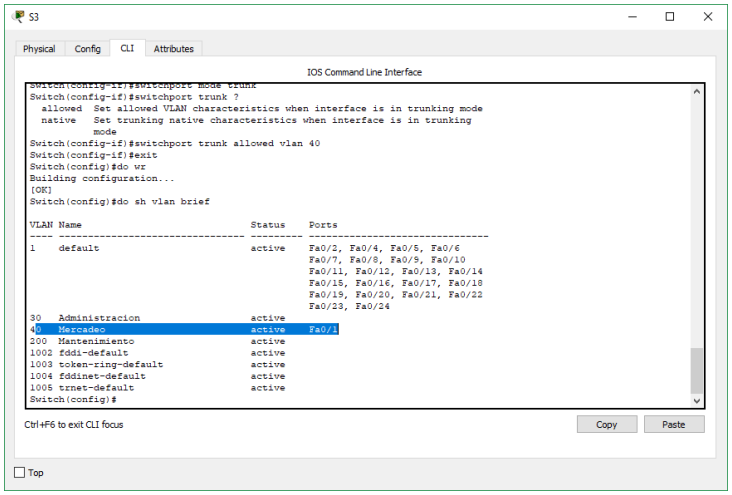
3. Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.

Creación VLANS



Verificación VLAN y puertos





Creación Encapsulación Dot1q

En el Router 1 – Medellin, se configura así:

MEDELLIN(config)#interface g0/0

MEDELLIN (config-if)#no shutdown

MEDELLIN (config-if)#exit

MEDELLIN (config)# interface g0/0.3

MEDELLIN (config-if)# encapsulation dot1Q 30

MEDELLIN (config-if)#ip address 192.168.30.1 255.255.255.0

exit

MEDELLIN (config)# interface g0/0.4

MEDELLIN (config-if)# encapsulation dot1Q 40

MEDELLIN (config-if)#ip address 192.168.40.1 255.255.255.0

exit

CreaciónIp de exclusión

MEDELLIN(config)#ipdhcp excluded-address 192.168.30.1

MEDELLIN(config)#ipdhcp excluded-address 192.168.40.1

MEDELLIN(config)#ipdhcp excluded-address 192.168.200.1

Configuración de seguridad en Routers y Switch

S1(config)#line console 0

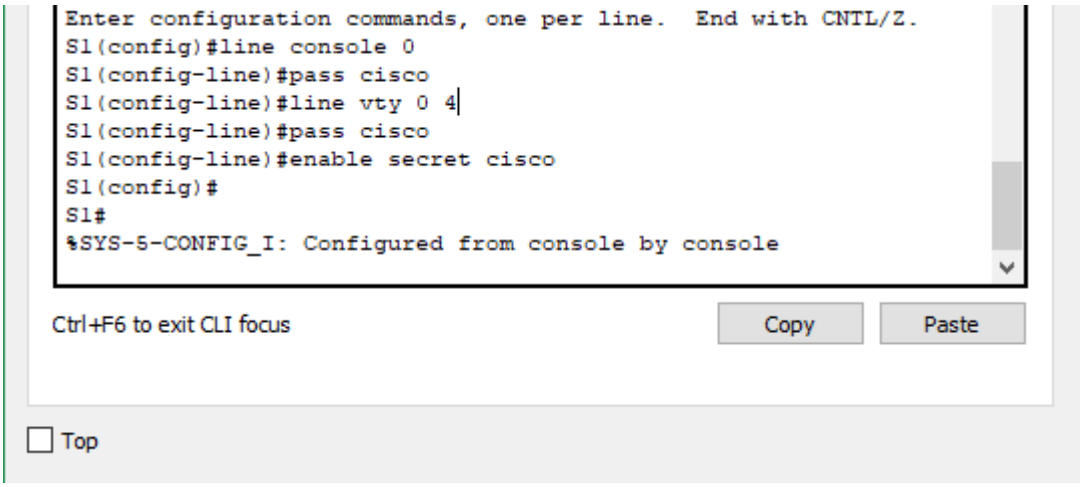
S1(config-line)#pass cisco

S1(config-line)#line vty 0 4

S1(config-line)#pass cisco

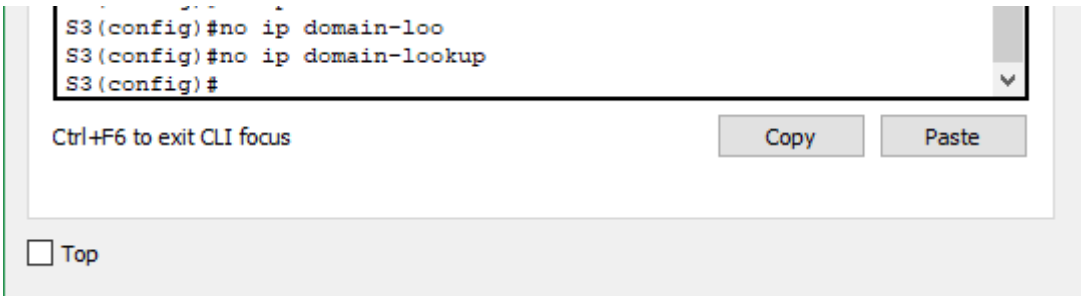
S1(config-line)#enable secret cisco

S1(config)#

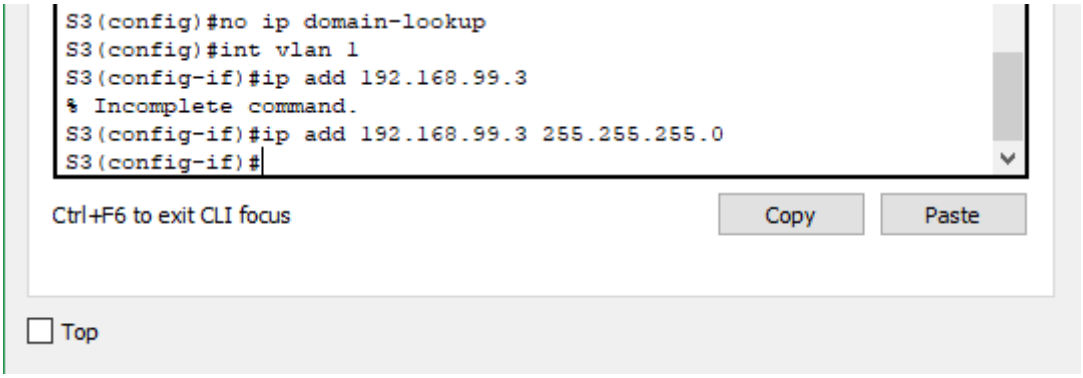


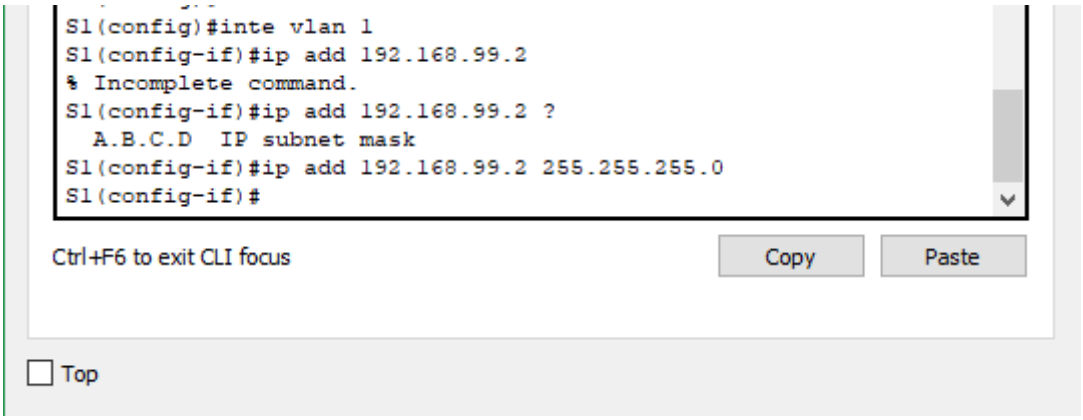
4. En el Switch 3 deshabilitar DNS lookup

Se realiza con el comando : no ipdomain-lookup



5. Asignar direcciones IP a los Switches acorde a los lineamientos.





6. Desactivar todas las interfaces que no sean utilizadas en el esquema de red.
7. Implement DHCP and NAT for IPv4
8. Configurar R1 como servidor DHCP para las VLANs 30 y 40.

Configuración DHCP

MEDELLIN(config)#ipdhcp pool vlan30

MEDELLIN(dhcp-config)#network 192.168.30.0 255.255.255.0

MEDELLIN(dhcp-config)#default-router 192.168.30.1

MEDELLIN(dhcp-config)#ipdhcp pool vlan40

MEDELLIN(dhcp-config)#network 192.168.40.0 255.255.255.0

MEDELLIN(dhcp-config)#default-router 192.168.40.1

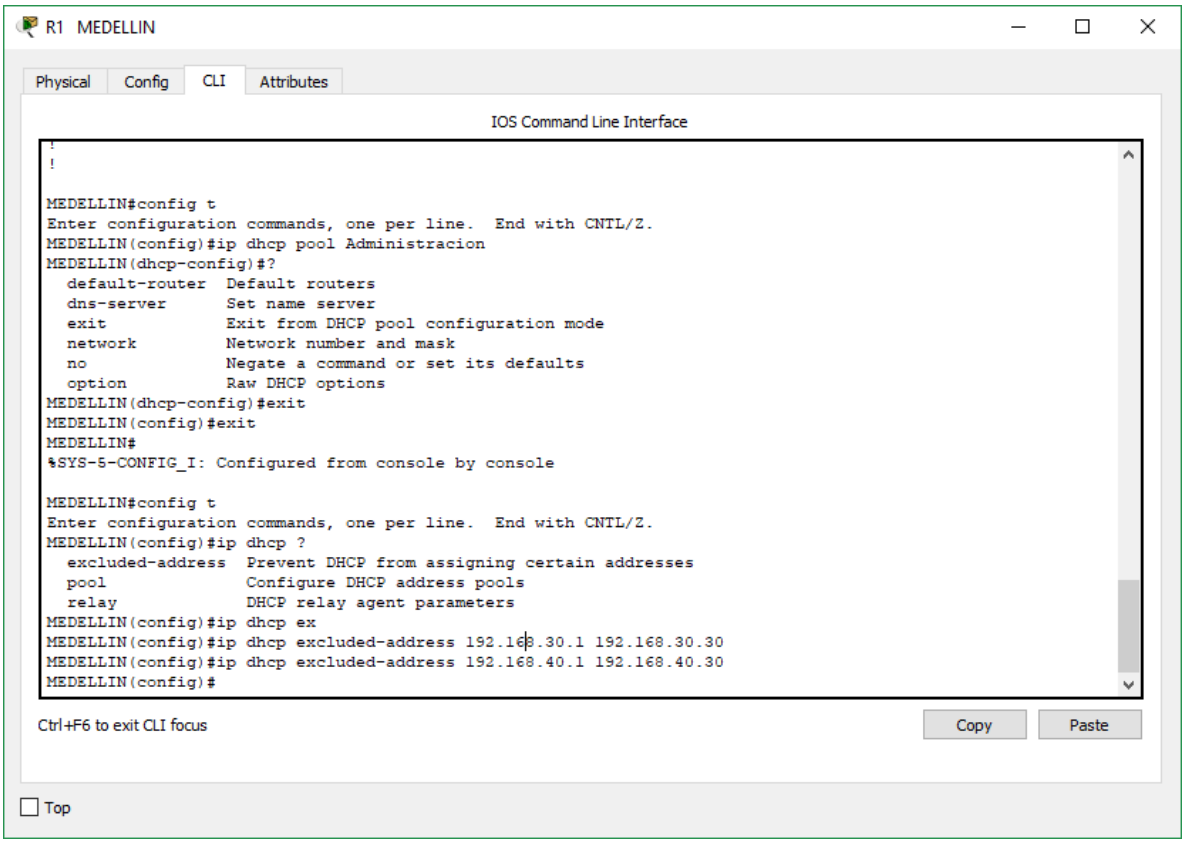
MEDELLIN(dhcp-config)#ipdhcp pool vlan200

MEDELLIN(dhcp-config)#network 192.168.200.0 255.255.255.0

MEDELLIN(dhcp-config)#default-router 192.168.200.1

9. Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

Exclusión de las 30 direcciones Ip para cada VLAN se realiza con el comando ipdhcpexcluded-address



10. Configurar NAT en R2 para permitir que los host puedan salir a internet

BOGOTA(config)#interface GigabitEthernet0/0

BOGOTA(config-if)#ipnat inside

BOGOTA(config-if)#int s0/0/0

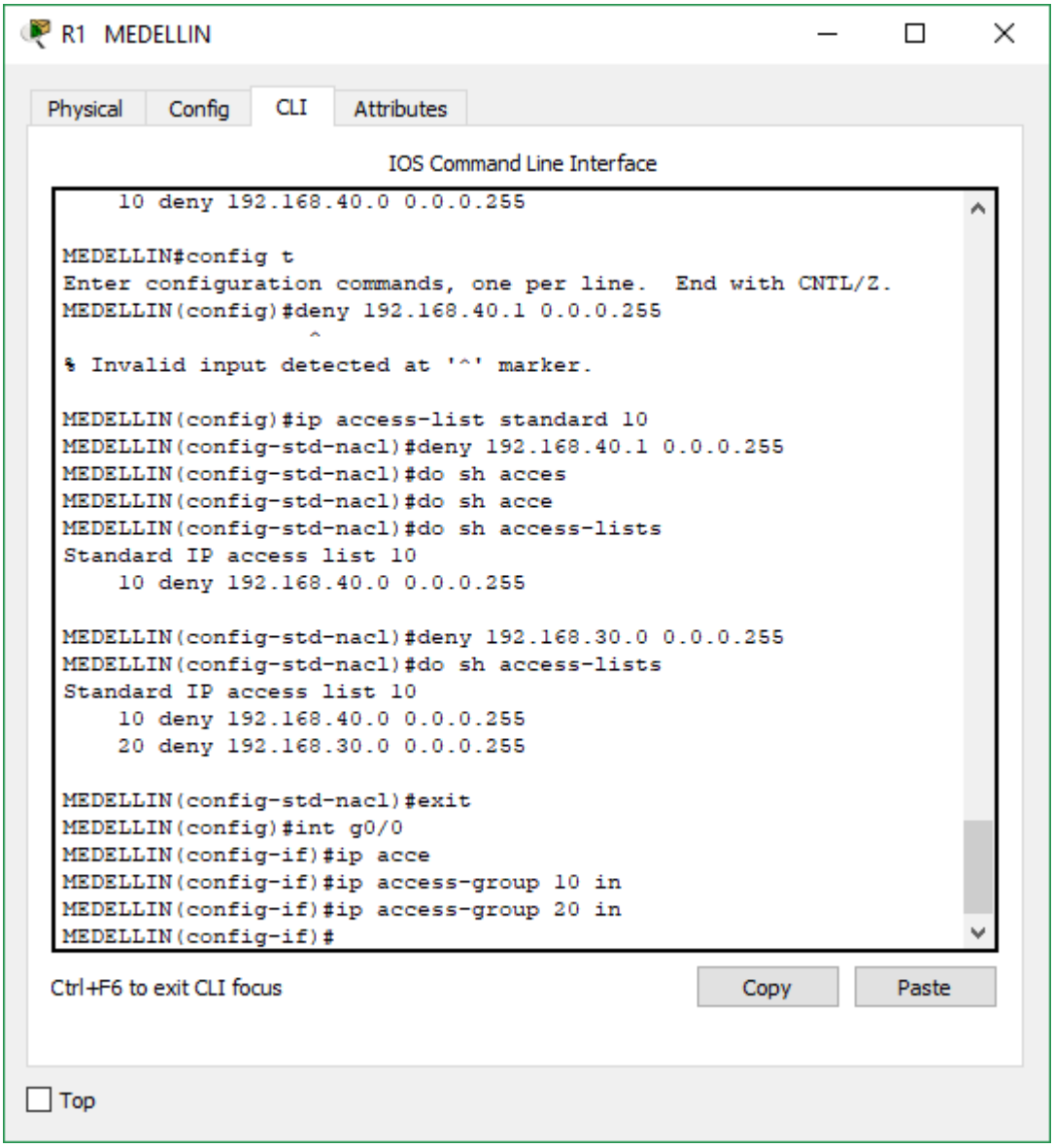
BOGOTA(config-if)#ipnat outside

BOGOTA(cint s0/0/0int s0/0/1

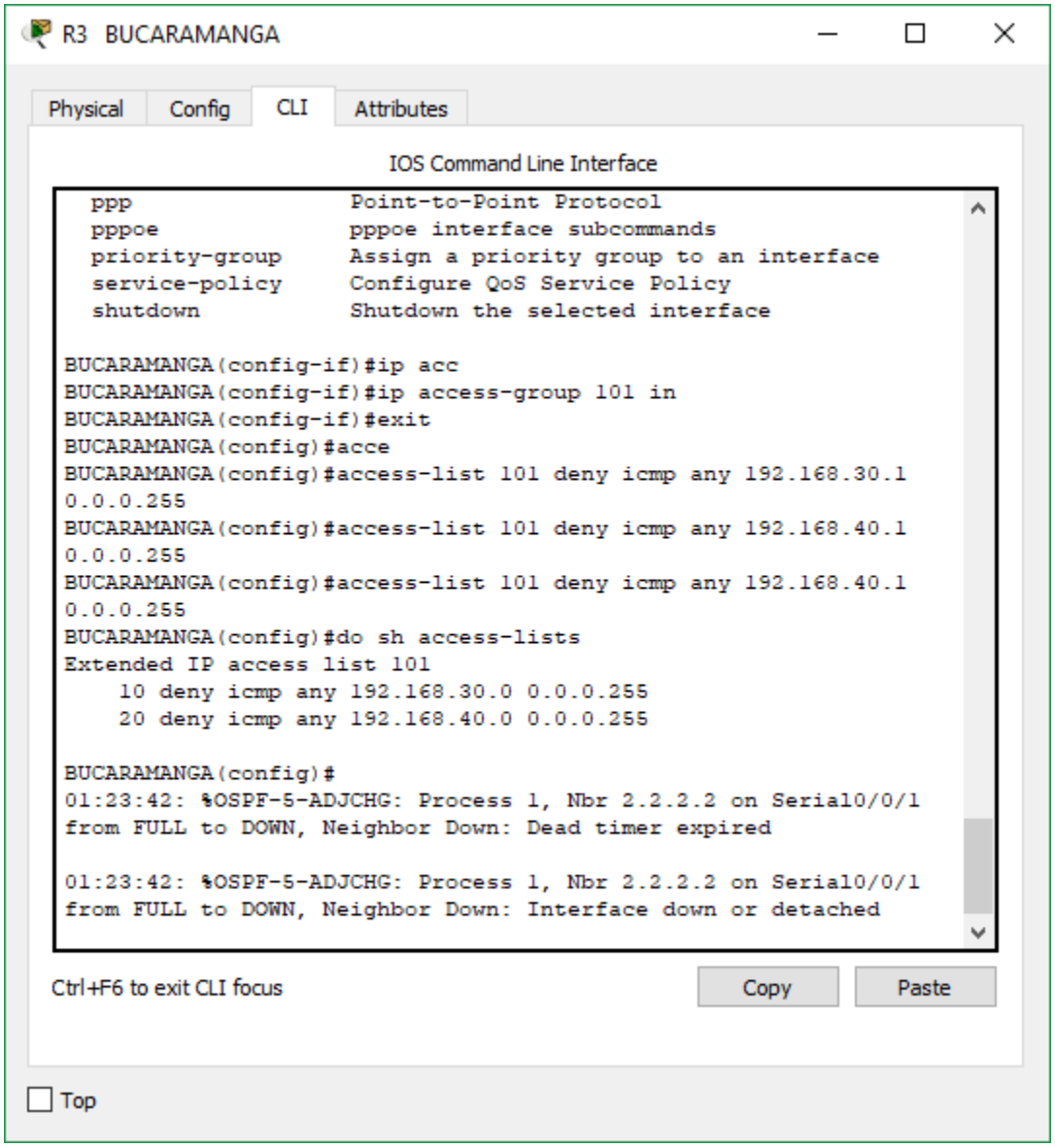
BOGOipnatoutsideipnat outside

BOGOTA(config-if)#exit

11. Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.



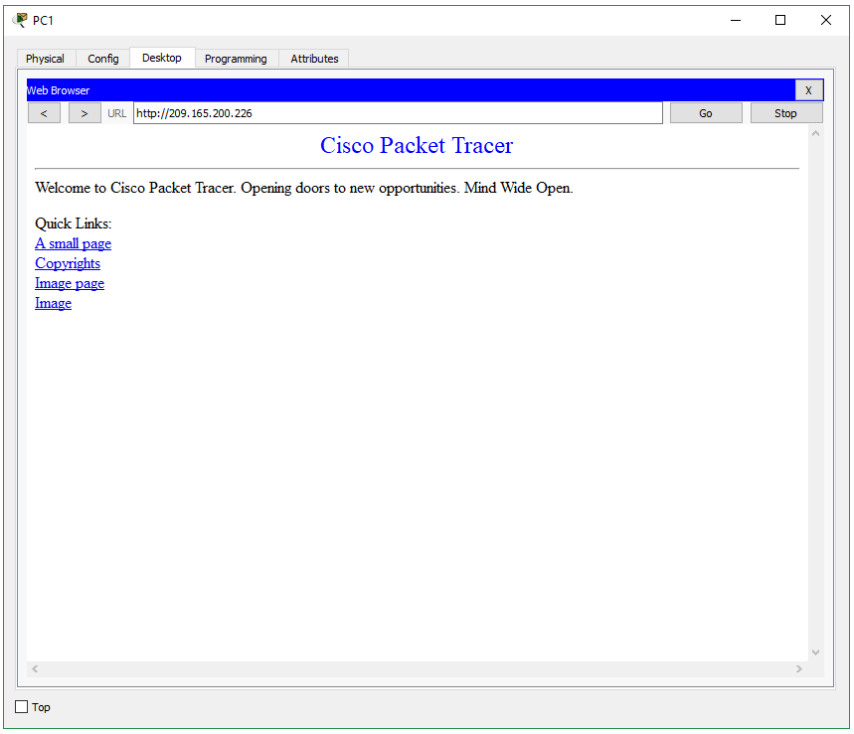
12. Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.


R3 BUCARAMANGA
Physical
Config
CLI
Attributes
IOS Command Line Interface
ppp Point-to-Point Protocol
pppoe pppoe interface subcommands
priority-group Assign a priority group to an interface
service-policy Configure QoS Service Policy
shutdown Shutdown the selected interface
BUCARAMANGA(config-if)#ip acc
BUCARAMANGA(config-if)#ip access-group 101 in
BUCARAMANGA(config-if)#exit
BUCARAMANGA(config)#acce
BUCARAMANGA(config)#access-list 101 deny icmp any 192.168.30.1
0.0.0.255
BUCARAMANGA(config)#access-list 101 deny icmp any 192.168.40.1
0.0.0.255
BUCARAMANGA(config)#access-list 101 deny icmp any 192.168.40.1
0.0.0.255
BUCARAMANGA(config)#do sh access-lists
Extended IP access list 101
10 deny icmp any 192.168.30.0 0.0.0.255
20 deny icmp any 192.168.40.0 0.0.0.255
BUCARAMANGA(config)#
01:23:42: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Dead timer expired
01:23:42: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Interface down or detached
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

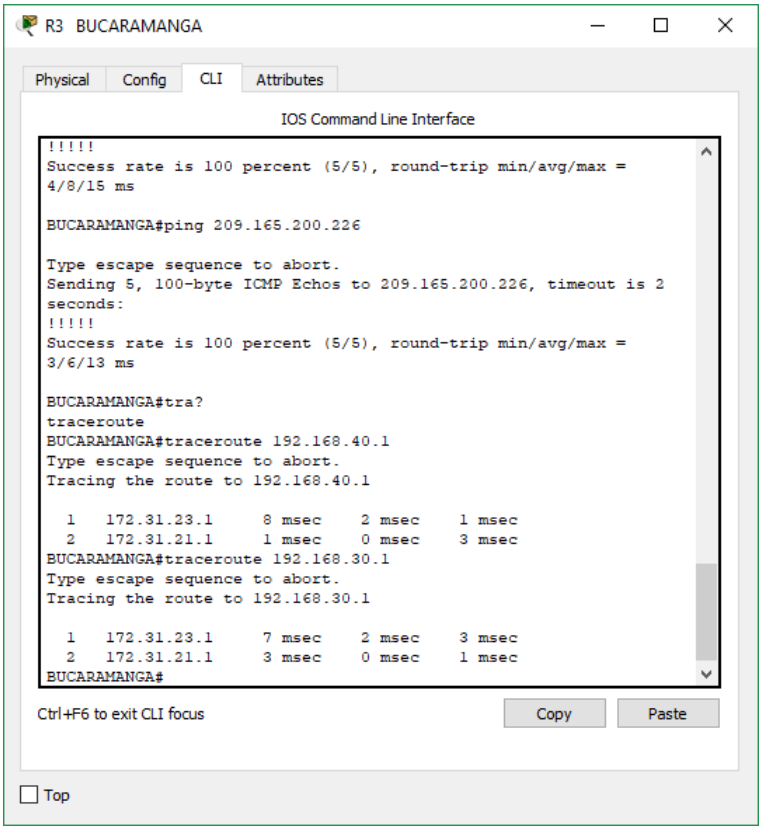
13. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

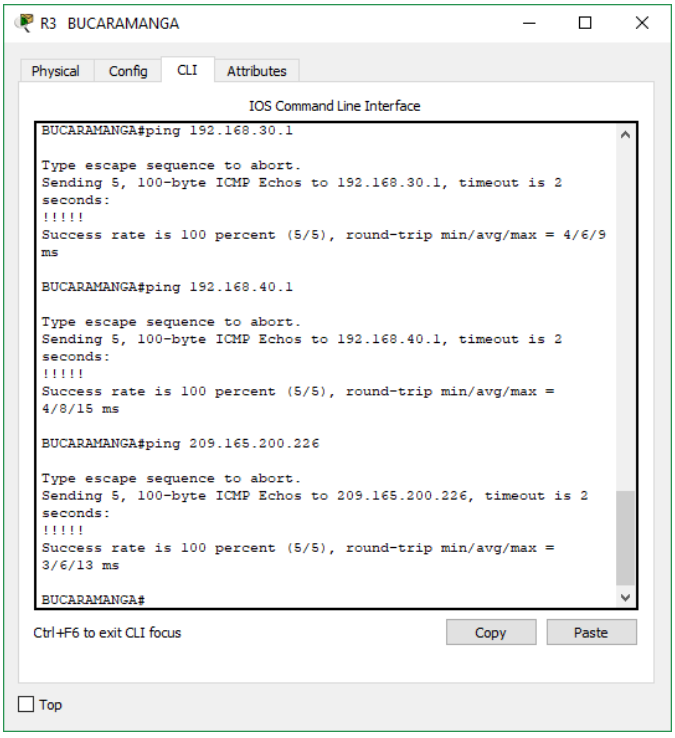
Pruebas de conectividad

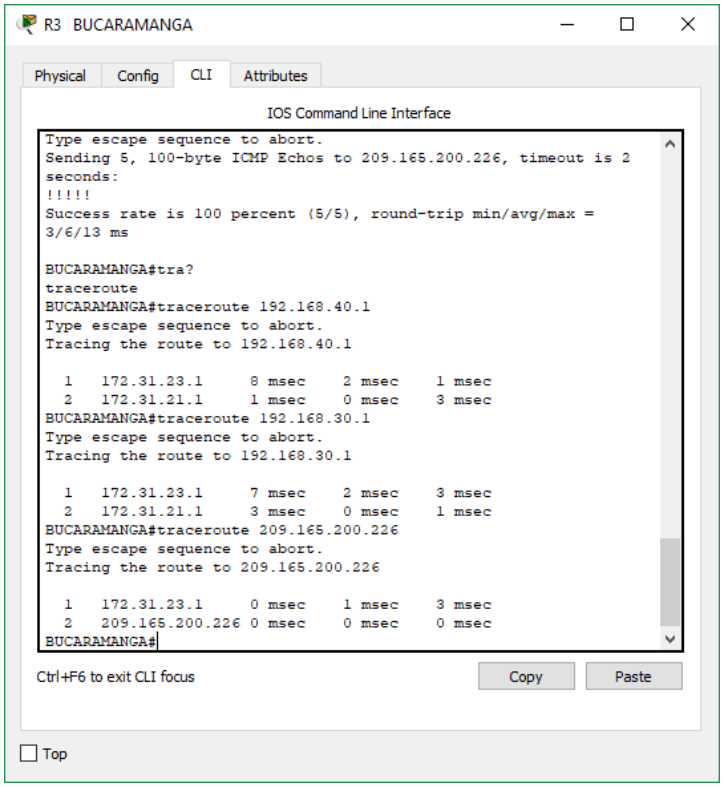
Desde PC1



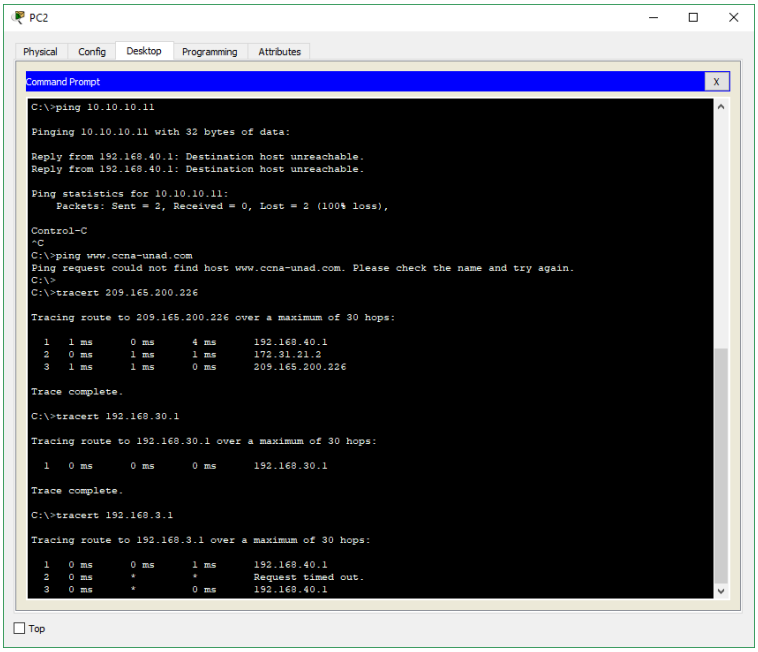
Desde Router 3

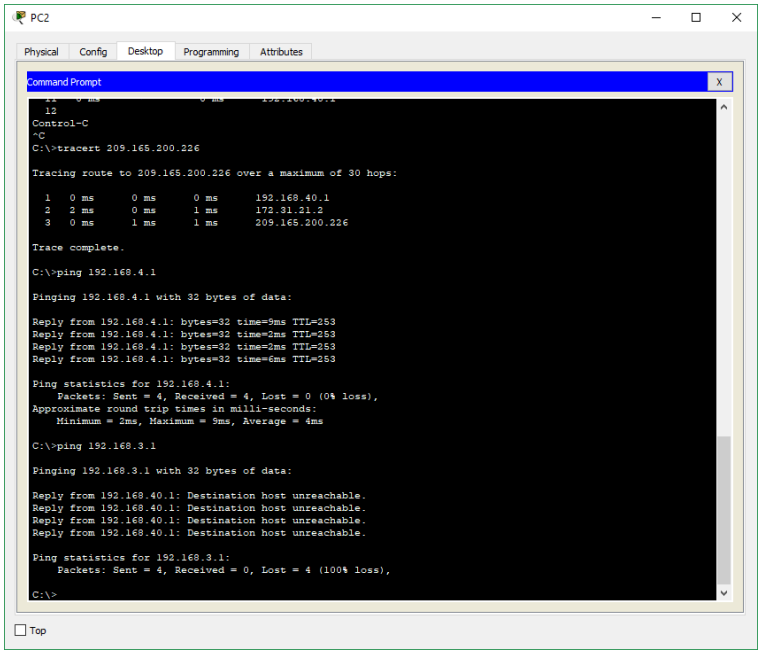





R3 BUCARAMANGA
Physical
Config
CLI
Attributes
IOS Command Line Interface
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/6/13 ms
BUCARAMANGA#tra?
traceroute
BUCARAMANGA#traceroute 192.168.40.1
Type escape sequence to abort.
Tracing the route to 192.168.40.1
1 172.31.23.1 8 msec 2 msec 1 msec
2 172.31.21.1 1 msec 0 msec 3 msec
BUCARAMANGA#traceroute 192.168.30.1
Type escape sequence to abort.
Tracing the route to 192.168.30.1
1 172.31.23.1 7 msec 2 msec 3 msec
2 172.31.21.1 3 msec 0 msec 1 msec
BUCARAMANGA#traceroute 209.165.200.226
Type escape sequence to abort.
Tracing the route to 209.165.200.226
1 172.31.23.1 0 msec 1 msec 3 msec
2 209.165.200.226 0 msec 0 msec 0 msec
BUCARAMANGA#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

Desde PC 2


PC2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
C:\>ping 10.10.10.11
Pinging 10.10.10.11 with 32 bytes of data:
Reply from 192.168.40.1: Destination host unreachable.
Reply from 192.168.40.1: Destination host unreachable.
Ping statistics for 10.10.10.11:
Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
^C
C:\>ping www.ccna-unad.com
Ping request could not find host www.ccna-unad.com. Please check the name and try again.
C:\>
C:\>tracert 209.165.200.226
Tracing route to 209.165.200.226 over a maximum of 30 hops:
1 1 ms 0 ms 4 ms 192.168.40.1
2 0 ms 1 ms 1 ms 172.31.21.2
3 1 ms 1 ms 0 ms 209.165.200.226
Trace complete.
C:\>tracert 192.168.30.1
Tracing route to 192.168.30.1 over a maximum of 30 hops:
1 0 ms 0 ms 0 ms 192.168.30.1
Trace complete.
C:\>tracert 192.168.3.1
Tracing route to 192.168.3.1 over a maximum of 30 hops:
1 0 ms 0 ms 1 ms 192.168.40.1
2 0 ms * * Request timed out.
3 0 ms * 0 ms 192.168.40.1
Top


PC2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
12
Control-C
^C
C:\>tracert 209.165.200.226
Tracing route to 209.165.200.226 over a maximum of 30 hops:
1 0 ms 0 ms 0 ms 192.168.40.1
2 2 ms 0 ms 1 ms 172.31.21.2
3 0 ms 1 ms 1 ms 209.165.200.226
Trace complete.
C:\>ping 192.168.4.1
Pinging 192.168.4.1 with 32 bytes of data:
Reply from 192.168.4.1: bytes=32 time=9ms TTL=253
Reply from 192.168.4.1: bytes=32 time=2ms TTL=253
Reply from 192.168.4.1: bytes=32 time=2ms TTL=253
Reply from 192.168.4.1: bytes=32 time=6ms TTL=253
Ping statistics for 192.168.4.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 9ms, Average = 4ms
C:\>ping 192.168.3.1
Pinging 192.168.3.1 with 32 bytes of data:
Reply from 192.168.40.1: Destination host unreachable.
Reply from 192.168.40.1: Destination host unreachable.
Reply from 192.168.40.1: Destination host unreachable.
Reply from 192.168.40.1: Destination host unreachable.
Ping statistics for 192.168.3.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Top

CONCLUSIONES

- Se configuró la topología de la red con routing OSPFv2, se cambió las asignaciones de ID de router, se configuro interfaces pasivas, se ajustó las métricas de OSPF y se utilizó varios comandos de CLI para ver y verificar la información de routing OSPF.

Bibliografía

Sciety, T. I. (1998). *internet protocol.* Obtenido de version 6: http://www.rfc-base.org/rfc-2460.html

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

UNAD (2014). Principios de Enrutamiento [OVA]. Recuperado de:

https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y

Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1