DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DILSON ERASMO BARRAGÁN NIÑO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA -ECBTI
INGENIERÍA ELECTRONICA
MITU
2020

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DILSON ERASMO BARRAGÁN NIÑO

Diplomado de opción de grado presentado para optar el título de
INGENIERO ELECTRONICO

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA -ECBTI
INGENIERÍA ELECRONICA
MITU
2020

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Mitú, 22 de Mayo de 2020

DEDICATORIA

Este trabajo es la terminación de un camino que se inició hace 5 años, el cual requirió esfuerzo, dedicación y sacrificio, los cuales me han llevado a obtener el gran don de la sabiduría. Hoy la meta se vislumbra más cerca, y es gracias al apoyo de mi familia, docentes y amigos, que ha sido posible alcanzar el objetivo, de esta manera, dedico a ellos el presente trabajo, muestra de mi gratitud y agradecimiento por el cumplimiento de este gran anhelo.

AGRADECIMIENTOS

A mis padres, así como a todas y cada una de las personas que de una u otra forma hicieron parte del viaje, con el convencimiento pleno de que este brindara las oportunidades de una mejor calidad de vida en un futuro, cada vez más cercano.

A la red de tutores y directores de las materias vistas en todo el proceso muchos de ellos fueron un ejemplo a seguir, otros motivaron ese deseo de aprender y ver que el éxito está en aquello que desconozco. A los compañeros que desde diferentes partes de la geografía colombiano dieron ejemplo de dedicación y esfuerzo motivando a seguir adelante en este viaje que hoy culmina.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

RED: Es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

VLAN: Es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local que no deberían intercambiar datos usando la red local.

SWITCH: Es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más host de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada ésta.

ROUTER: Es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes.

CCNP: Es el nivel intermedio de certificación de la compañía. Para obtener esta certificación, se han de superar varios exámenes, clasificados según la empresa en 3 módulos.

BGP: protocolo mediante el cual se intercambia información de enrutamiento entre sistemas autónomos

eBGP: sesiones externas de BGP

DTP:(Dynamic Trunking Protocol) es un protocolo creado por Cisco Systems que opera entre switches Cisco, el cual automatiza la configuración de trunking

VLAN:(Red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física

VTP:VLAN Trunking Protocol: Es un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco.

Interface Loopback: interfaz de red virtual, son usualmente utilizadas para probar la capacidad de la tarjeta interna si se están enviando datos BGP.

RESUMEN

Este proyecto consiste en desarrollar una serie de escenarios que permiten profundizar en el proceso de apropiación de las diferentes temáticas de Routing y Switching que se adquirieron durante el curso de profundización de CCNP, Junto con la aplicación práctica de dichos conocimientos para los módulos de CCNP ROUTE y CCNA SWITCH en ambientes de simulación lógica.

El principal objetivo es el incremento de las habilidades por parte del estudiante en un área de profundización del área de telecomunicaciones que le permita tener la capacidad de solucionar diferentes inconvenientes en su ejercicio profesional con un pensamiento crítico y la capacidad de análisis sobre plataforma de red, la solución de situaciones complicadas que se presentan en el mundo de las redes de datos.

Palabras Clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRAC

This project consists of developing a series of scenarios that allow to deepen the appropriation process of the different Routing and Switching themes that were acquired during the CCNP deepening course, along with the practical application of such knowledge for the CCNP ROUTE modules. and CCNA SWITCH in logical simulation environments.

The main objective is the increase of skills by the student in a deepening área of the telecommunications area that allows him to have the ability to solve different problems in his professional exercises with critical thinking and the ability to analyze on a network platform, solving complicated situations that arise in the world of data networks.

Keywords: CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

INTRODUCCIÓN

El presente documento presenta el desarrollo de la Prueba de Habilidades Practicas, las cuales forman parte de las actividades evaluativas del Diplomado de Profundización CCNP, y busca evaluar el grado de competencias y habilidades alcanzadas en el diplomado. Mediante los escenarios propuestos se busca poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

En el primer escenario veremos el proceso de enrutamiento a través del protocolo BGP con la creación de adyacencias en función de protocolo IPv4, del router ID e interface Loopback, buscando que todos los Router contengan en sus tablas de enrutamiento las rutas y saltos necesarios para el envió de paquetes en toda la red.

En el segundo escenario se configura una red de switches y PCs con enrutamiento IPv4, usando protocolo VTP Y DTP para lograr la comunicación entre los Switches, dentro de las configuraciones se crean las VLAN que simulan departamentos en una empresa, la configuración debe impedir que los equipos de un departamento puedan acceder a los equipos de los otros departamentos.

DESARROLLO DE LOS ESCENARIOS PROPUESTOS

ESCENARIO 1

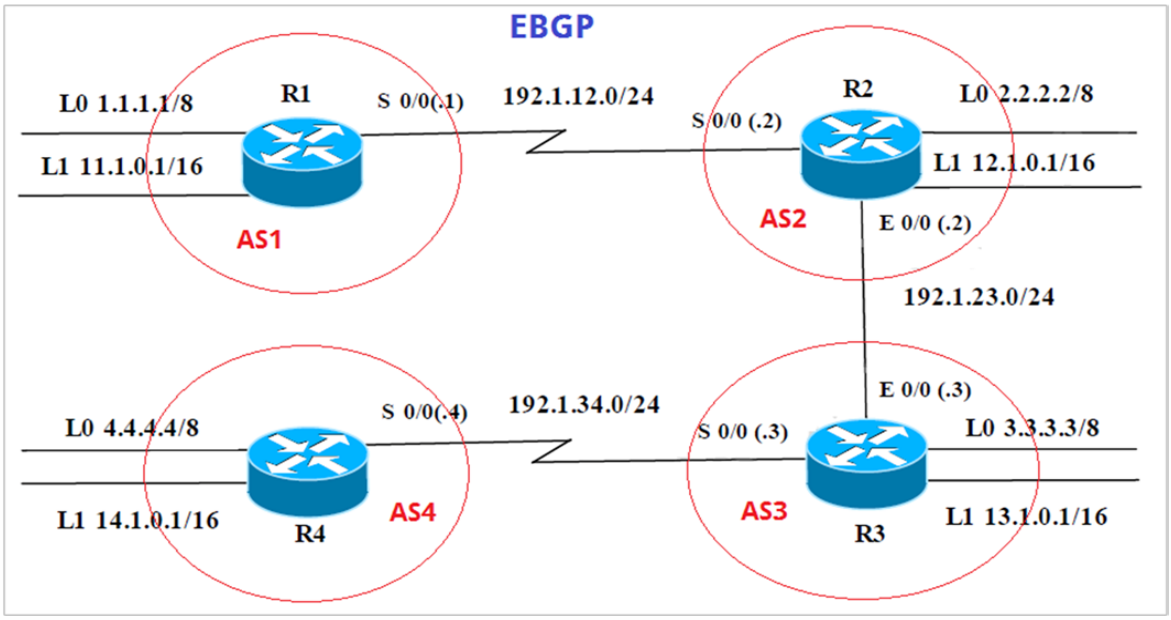

Figura 1. Diagrama escenario 1

Información para configuración de los Routers:

Router	Interfaz	Dirección IP	Mascara
R1	Loopback 0	1.1.1.1	255.0.0.0
	Loopback 1	11.1.0.1	255.255.0.0
	S0/1/0	192.1.12.1	255.255.255.0
R2	Loopback 0	2.2.2.2	255.0.0.0
	Loopback 1	12.1.0.1	255.255.0.0
	S0/1/0	192.1.12.2	255.255.255.0
	G0/1/0	192.1.23.2	255.255.255.0
R3	Loopback 0	3.3.3.3	255.0.0.0
	Loopback 1	13.1.0.1	255.255.0.0
	S0/1/0	192.1.34.3	255.255.255.0
	G0/1/0	192.1.23.3	255.255.255.0
R4	Loopback 0	4.4.4.4	255.0.0.0
	Loopback 1	14.1.0.1	255.255.0.0
	S0/1/0	192.1.34.4	255.255.255.0

Tabla 1. Configuración de Router escenario 1

1. Configuración inicial de cada Router

Antes de iniciar con la solución del Escenario se debe realizar la configuración inicial, básica de cada uno de los router en la que se debe configurar las interfaces con sus direcciones IP establecidas en el diagrama y las tablas entre otras configuraciones que garanticen la seguridad en cada Router

```
Router#configure terminal
Router(config)#Hostname R1
R1(config)#ENABLE SECRET class
R1(config)#LINE CONSOLE 0
R1(config-line)#PASSWORD cisco
R1(config-line)#LOGIN
R1(config-line)#EXIT
R1(config)#LINE VTY 0 15
R1(config-line)#PASSWORD cisco
R1(config-line)#LOGIN
R1(config-line)#EXIT
R1(config)#Service PASSWORD-ENCRYPTION
R1(config)#BANNER MOTD !EL ACCESO NO AUTORIZADO ESTA PROHIBIDO!
R1(config)#
```

Esta misma configuración se realiza para los demás dispositivos cambiando el **HOSTNAME** en cada uno.

Configuración de las direcciones IP en cada Router de acuerdo a la Tabla, como medida de seguridad se recomienda apagar los puertos que no se usan.

```
R1#CONFIGURE TERMINAL
R1(config)#INTERFACE SERIAL  0/1/0
R1(config-if)#IP ADDRESS 192.1.12.1 255.255.255.0
R1(config-if)#CLOCK RATE 2000000
R1(config-if)#NO SHUTDOWN
R1(config-if)#INTERFACE SERIAL  0/1/1
R1(config-if)#SHUTDOWN
R1(config-if)#EXIT
R1(config)#INTERFACE RANGE GIGABIT 0/0/0-2
R1(config-if-range)#SHUTDOWN
R1(config-if-range)#EXIT
R1(config)#INTERFACE LO 0
R1(config-if)#IP ADDRESS 1.1.1.1 255.0.0.0
R1(config-if)#INTERFACE LO 1
R1(config-if)#IP ADDRESS 11.1.0.1 255.255.0.0
R2#CONFIGURE TERMINAL
R2(config)#INTERFACE SERIAL 0/1/0
```

```
R2(config-if)#IP ADDRESS 192.1.12.2 255.255.255.0
R2(config-if)#NO SHUTDOWN
R2(config-if)#INTERFACE SERIAL 0/1/1
R2(config-if)#SHUTDOWN
R2(config-if)#EXIT
R2(config)#INTERFACE GIGABIT 0/0/0
R2(config-if)#IP ADDRESS 192.1.23.2 255.255.255.0
R2(config-if)#NO SHUTDOWN
R2(config-if)#EXIT
R2(config)#INTERFACE RANGE GIGABIT 0/0/1-2
R2(config-if-range)#SHUTDOWN
R2(config-if-range)#EXIT
R2(config)#INTERFACE LO 0
R2(config-if)#IP ADDRESS 2.2.2.2 255.0.0.0
R2(config-if)#INTERFACE LO 1
R2(config-if)#IP ADDRESS 12.1.0.1 255.255.0.0
R2(config-if)#EXIT

R3#CONFIGURE TERMINAL
R3(config)#INTERFACE SERIAL 0/1/0
R3(config-if)#IP ADDRESS 192.1.34.3 255.255.255.0
R3(config-if)#NO SHUTDOWN
R3(config-if)#CLOCK RATE 2000000
R3(config-if)#INTERFACE SERIAL 0/1/1
R3(config-if)#SHUTDOWN
R3(config-if)#EXIT
R3(config)#INTERFACE GIGABIT 0/0/0
R3(config-if)#IP ADDRESS 192.1.23.3 255.255.255.0
R3(config-if)#NO SHUTDOWN
R3(config-if)#EXIT
R3(config)#INTERFACE RANGE GIGABIT 0/0/1-2
R3(config-if-range)#SHUTDOWN
R3(config-if-range)#EXIT
R3(config)#INTERFACE LO 0
R3(config-if)#IP ADDRESS 3.3.3.3 255.0.0.0
R3(config-if)#INTERFACE LO 1
R3(config-if)#IP ADDRES 13.1.0.1 255.255.255.0
R3(config-if)#EXIT

R4#CONFIGURE TERMINAL
R4(config)#INTERFACE SERIAL 0/1/0
R4(config-if)#IP ADDRESS 192.1.34.4 255.255.255.0
R4(config-if)#NO SHUTDOWN
R4(config-if)#INTERFACE SERIAL 0/1/1
R4(config-if)#SHUTDOWN
```

```
R4(config-if)#EXIT
R4(config)#INTERFACE RANGE GIGABIT 0/0/0-2
R4(config-if-range)#SHUTDOWN
R4(config-if-range)#EXIT
R4(config)#INTERFACE LO 0
R4(config-if)#IP ADDRESS 4.4.4.4 255.0.0.0
R4(config-if)#INTERFACE LO 1
R4(config-if)#IP ADDRES 14.1.0.1 255.255.255.0
R4(config-if)#EXIT
```

2. Configure una relación de vecino BGP entre R1 y R2.

R1 debe estar en AS1 y R2 debe estar en AS2. Anuncie las direcciones de Loopback en BGP. Codifique los ID para los routers BGP como 22.22.22.22 para R1 y como 33.33.33.33 para R2. Presente el paso a paso con los comandos utilizados y la salida del comando **show ip route.**

Se procede a configurar el protocolo BGP en los router, declarando las redes a las que pertenece y declarando a su vez el vecino más cercano

```
R1#CONFIGURE TERMINAL
R1(config)#ROUTER BGP 1
R1(config-router)#BGP ROUTER-ID 22.22.22.22
R1(config-router)#NETWORK 1.0.0.0 MASK 255.0.0.0
R1(config-router)#NETWORK 192.1.12.0 MASK 255.255.255.0
R1(config-router)#NETWORK 11.1.0.0 MASK 255.255.0.0
R1(config-router)#NEIGHBOR 192.1.12.2 REMOTE-AS 2
R1(config-router)#END
```

```
R2#CONFIGURE TERMINAL
R2(config)#ROUTER BGP 2
R2(config-router)#BGP ROUTER-ID 33.33.33.33
R2(config-router)#NETWORK 192.1.12.0 MASK 255.255.255.0
R2(config-router)#NETWORK 2.0.0.0 MASK 255.0.0.0
R2(config-router)#NETWORK 12.1.0.0 MASK 255.255.255.0
R2(config-router)#NETWORK 192.1.23.0 MASK 255.255.255.0
R2(config-router)#NEIGHBOR 192.1.12.1 REMOTE-AS 1
R2(config-router)#NEIGHBOR 192.1.23.3 REMOTE-AS 3
R2(config-router)#END
```

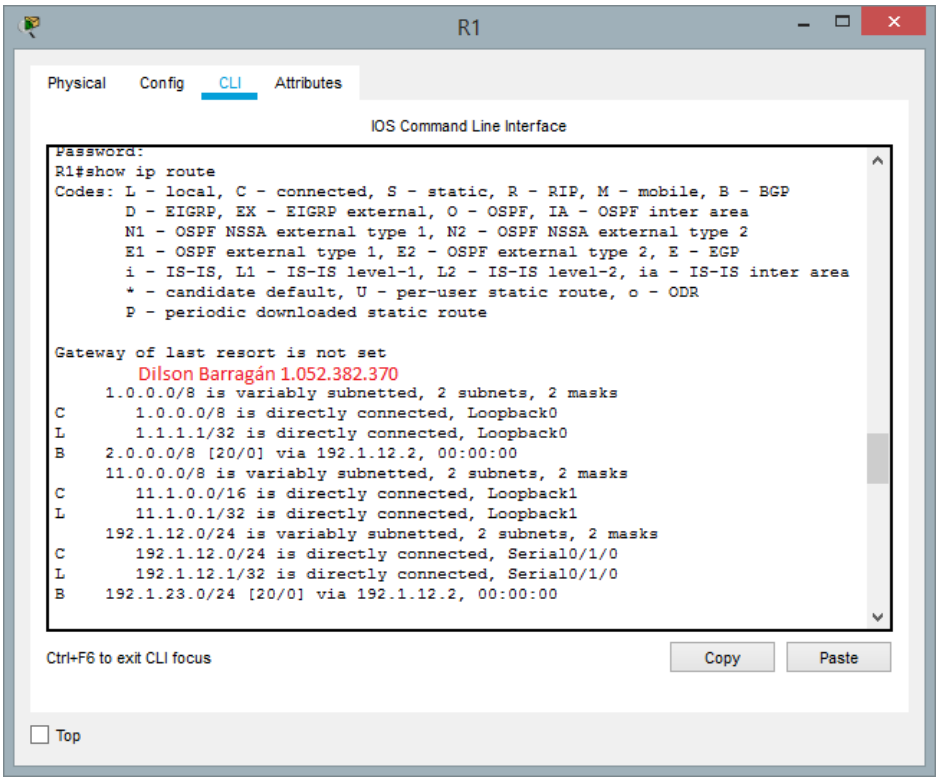

Figura 2. verificación de vecinos en R1

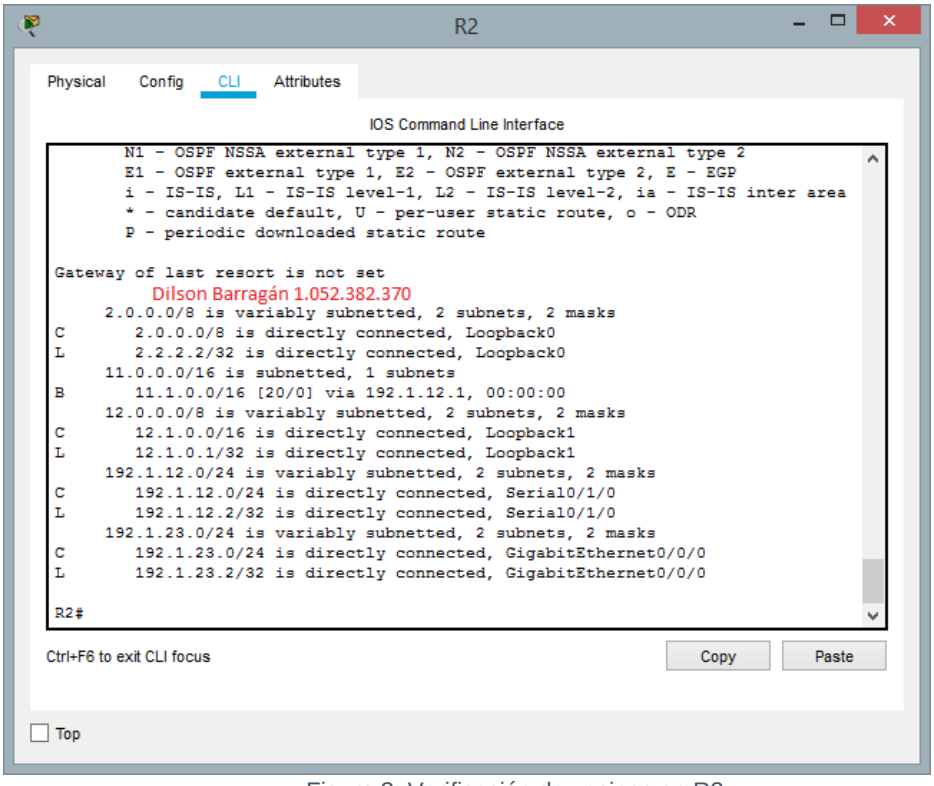

Figura 3. Verificación de vecinos en R2

3. Configure una relación de vecino BGP entre R2 y R3.

R2 ya debería estar configurado en **AS2** y R3 debería estar en **AS3**. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 44.44.44.44. Presente el paso a con los comandos utilizados y la salida del comando **show ip route.**

En el paso anterior se configuraron las redes vecinas en R2 por lo que se procede a realizar la configuración de vecinos en R3 con los parámetros dados.

```
R3#CONFIGURE TERMINAL
R3(config)#ROUTER BGP 3
R3(config-router)#BGP ROUTER-ID 44.44.44.44
R3(config-router)#NETWORK 192.1.34.0 MASK 255.255.255.0
R3(config-router)#NETWORK 192.1.23.0 MASK 255.255.255.0
R3(config-router)#NETWORK 13.1.0.0 MASK 255.255.0.0
R3(config-router)#NETWORK 3.0.0.0 MASK 255.0.0.0
R3(config-router)#NEIGHBOR 192.1.34.4 REMOTE-AS 4
R3(config-router)#NEIGHBOR 192.1.23.2 REMOTE-AS 2
R3(config-router)#END
```

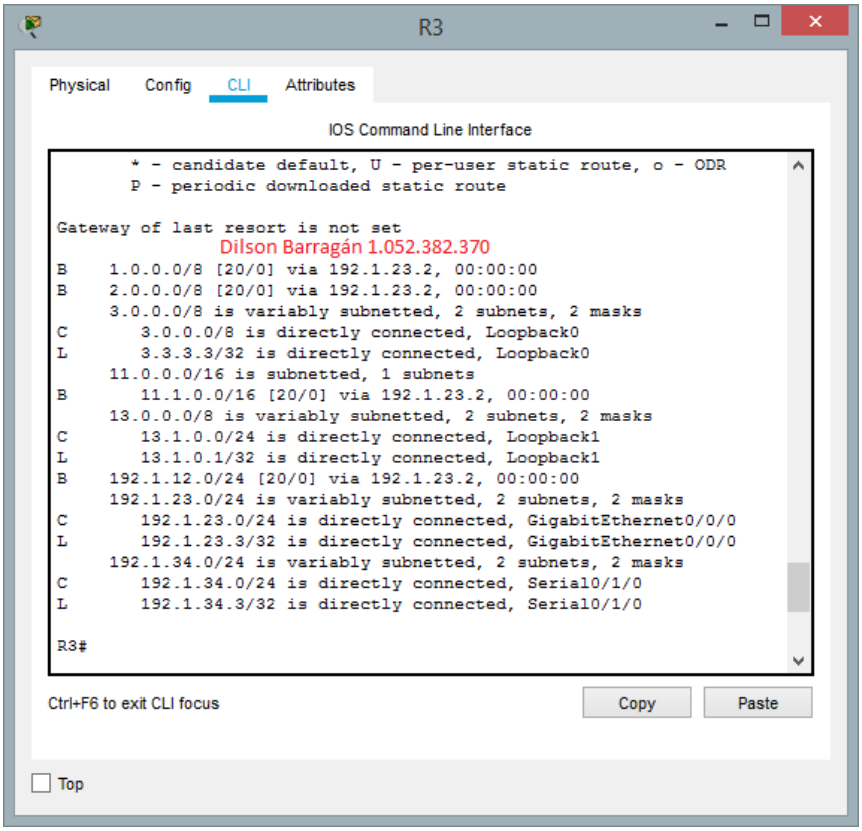

Figura 4. Verificación de vecinos en R3

4. Configure una relación de vecino BGP entre R3 y R4.

R3 ya debería estar configurado en **AS3** y R4 debería estar en **AS4**. Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como 66.66.66.66. Establezca las relaciones de vecino con base en las direcciones de Loopback 0. Cree rutas estáticas para alcanzar la Loopback 0 del otro router. No anuncie la Loopback 0 en BGP.

Anuncie la red Loopback de R4 en BGP. Presente el paso a con los comandos utilizados y la salida del comando **show ip route.**

R4#CONFIGURE TERMINAL
R4(config)#ROUTER BGP 4
R4(config-router)#BGP ROUTER-ID 66.66.66.66
R4(config-router)#NETWORK 192.1.34.0 MASK 255.255.255.0
R4(config-router)#NETWORK 14.1.0.0 MASK 255.255.0.0
R4(config-router)#NETWORK 4.0.0.0 MASK 255.0.0.0
R4(config-router)#NEIGHBOR 192.1.34.3 REMOTE-AS 3

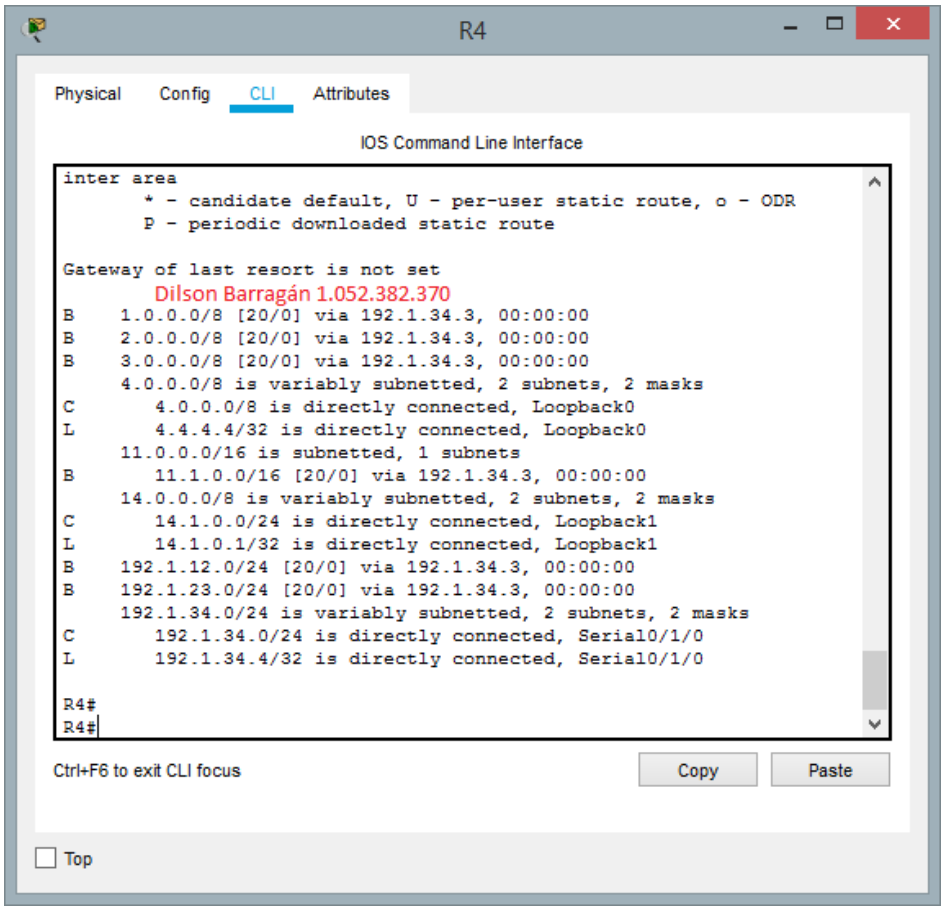

Figura 5. Verificación de vecinos en R4

Para validar las correcta configuración y que el protocolo BGP está correctamente funcionando se ejecuta el comando **show ip route** en R1 y desde este mismo dispositivo se realiza pin a las diferentes **loopback** de los demás equipos

Al ejecutar el comando Show ip route en R1 se evidencia que este ya tiene en su tabla las tablas y direcciones de los demás Routers

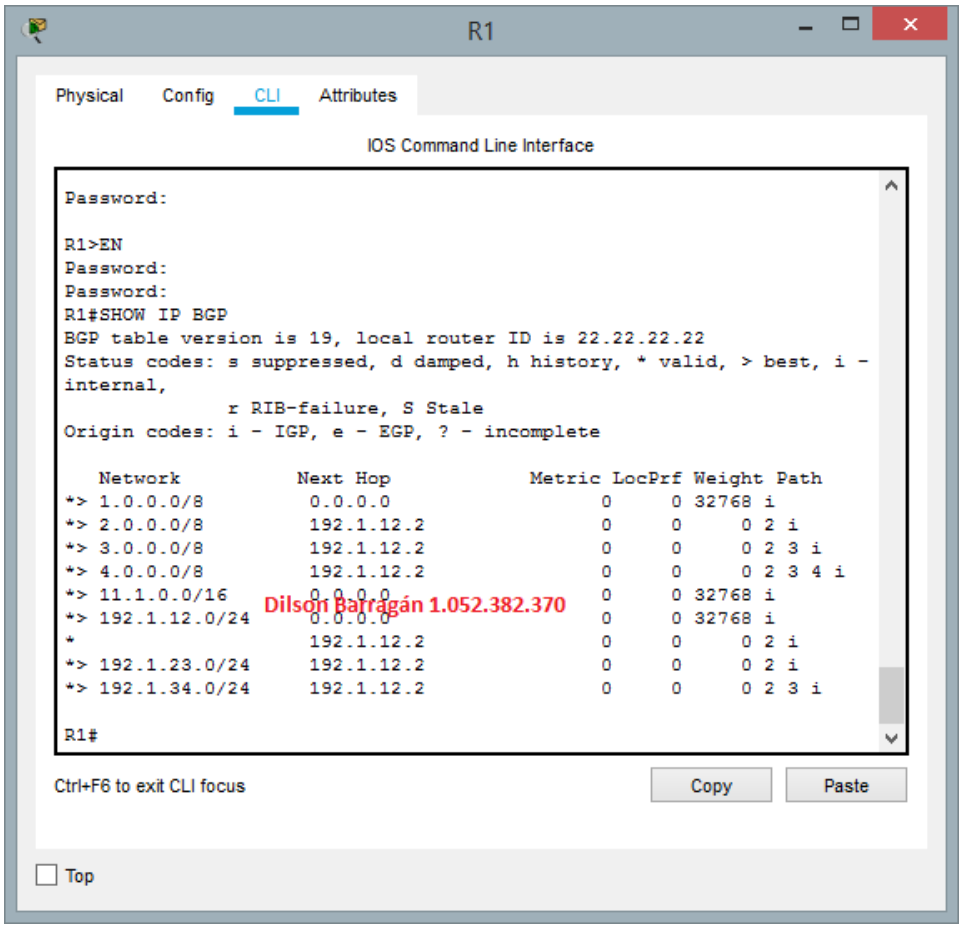

Figura 6. Verificación de Vecinos en R1

Al realizar ping a cada uno de las Loopback de cada router este es satisfactorio lo que garantiza la correcta comunicación de red.

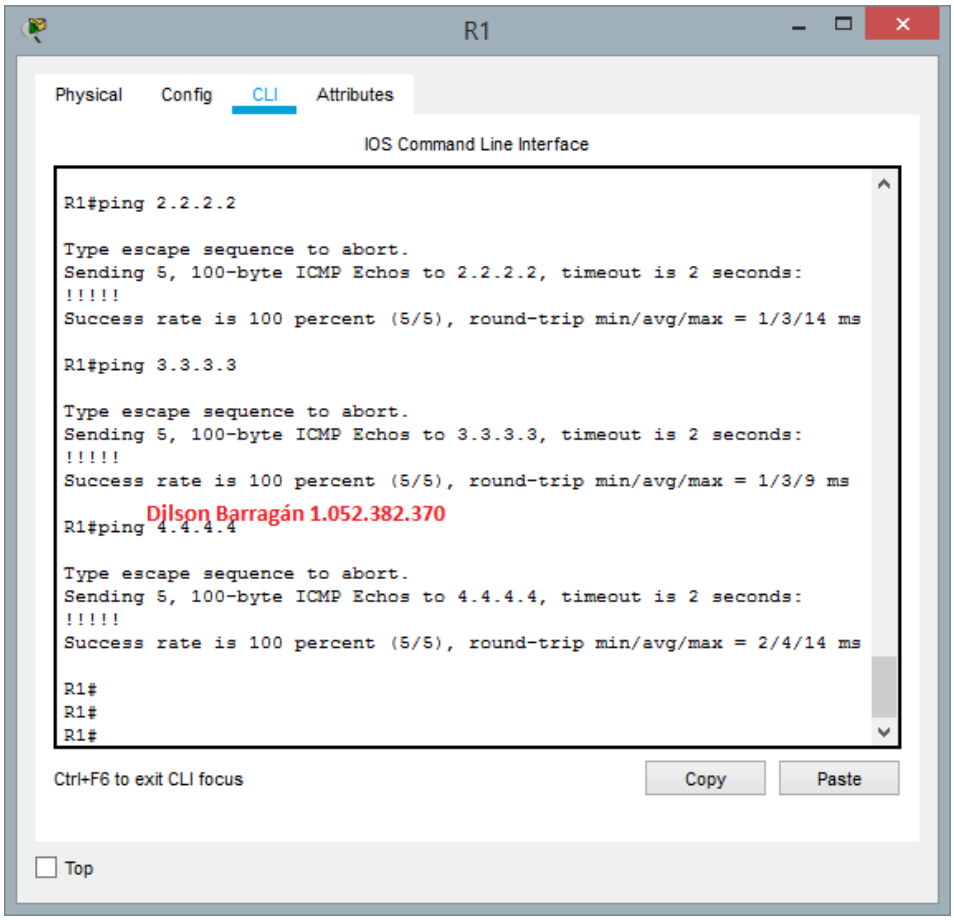

Figura 7. Ping a Loopback 0 de cada Router

ESCENARIO 2

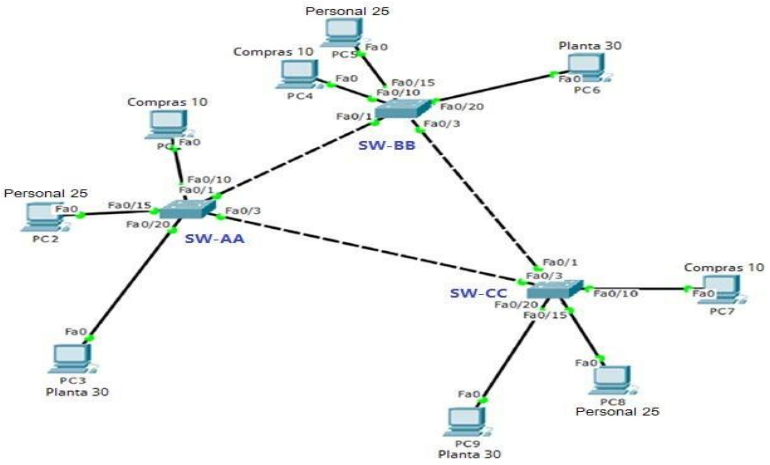

Figura 8. Diagrama Escenario 2

A. Configurar VTP

1. Todos los switches se configurarán para usar VTP para las actualizaciones de VLAN. El switch SW-BB se configurará como el servidor. Los switches SW-AA y SW-CC se configurarán como clientes. Los switches estarán en el dominio VPT llamado CCNP y usando la contraseña cisco.

```
Switch#CONFIGURE TERMINAL
Switch(config)#HOSTNAME SW-BB
SW-BB(config)#VTP MODE SERVER
SW-BB(config)#VTP DOMAIN CCNP
SW-BB(config)#VTP PASSWORD cisco
SW-BB(config)#END

Switch>ENABLE
Switch#CONFIGURE TERMINAL
Switch(config)#HOSTNAME SW-AA
SW-AA(config)#VTP MODE CLIENT
SW-AA(config)#VTP DOMAIN CCNP
SW-AA(config)#VTP PASSWORD cisco
SW-AA(config)#END

Switch>ENABLE
Switch#CONFIGURE TERMINAL
Switch(config)#VTP MODE CLIENT
Switch(config)#VTP DOMAIN CCNP
Switch(config)#VTP PASSWORD cisco
Switch(config)#END
```

2. Verifique las configuraciones mediante el comando **show vtp status**.

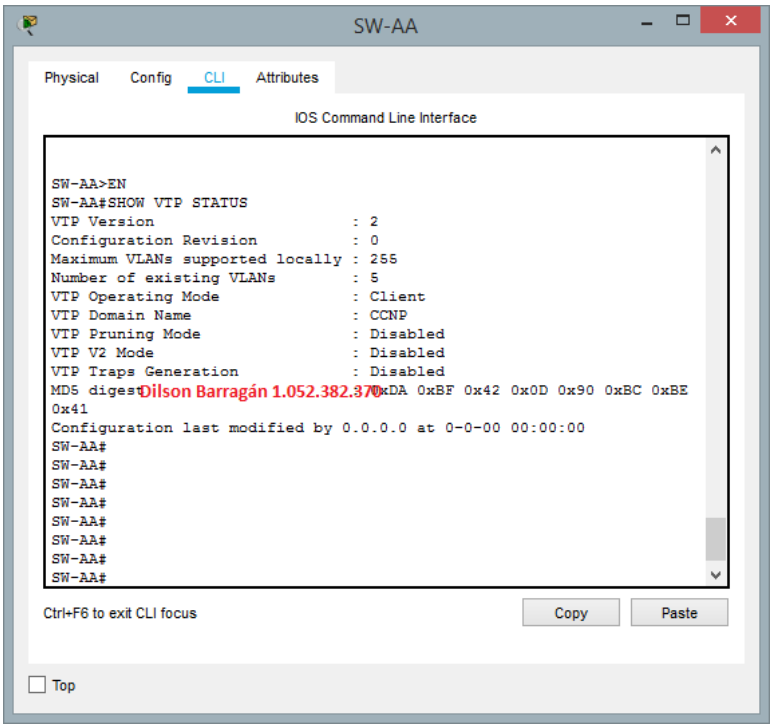

Figura 9. Comando Show Vtp Status en SW-AA

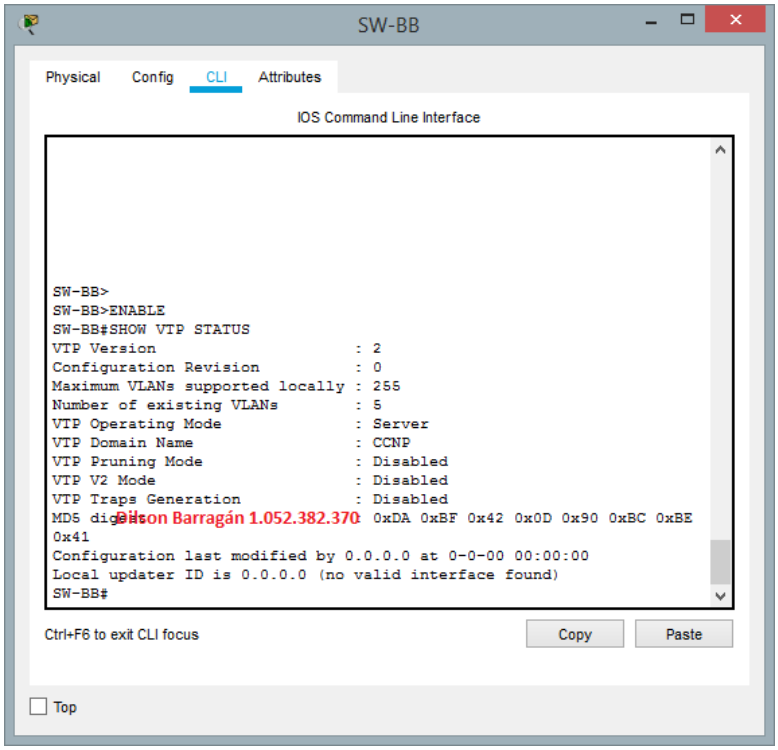

Figura 10. Comando Show Vtp Status en SW-BB

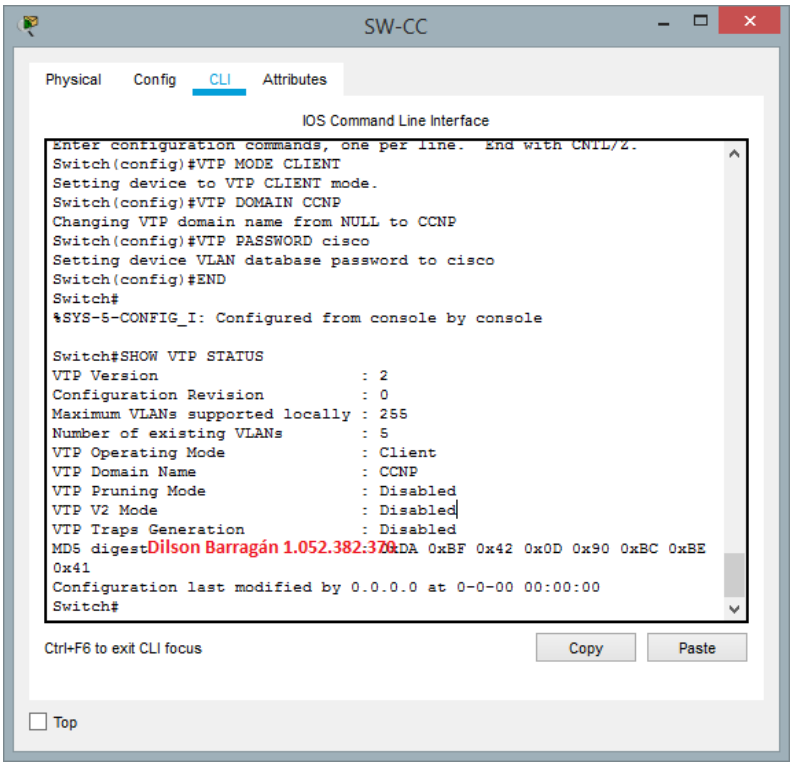

Figura11. Comando Show Vtp Status en SW-CC

B. Configurar DTP (Dynamic Trunking Protocol)

1. Configure un enlace troncal ("Trunk") dinámico entre SW-AA y SW-BB. Debido a que el modo por defecto es **dynamic auto**, solo un lado del enlace debe configurarse como **dynamic desirable**.

```
SW-BB#CONFIGURE TERMINAL
SW-BB(config)#INTERFACE GIGABIT 1/1
SW-BB(config-if)#SWITCH MODE DYNAMIC DESIRABLE
```

2. Verifique el enlace "Trunk" entre SW-AA y SW-BB usando el comando **show interfaces Trunk**.

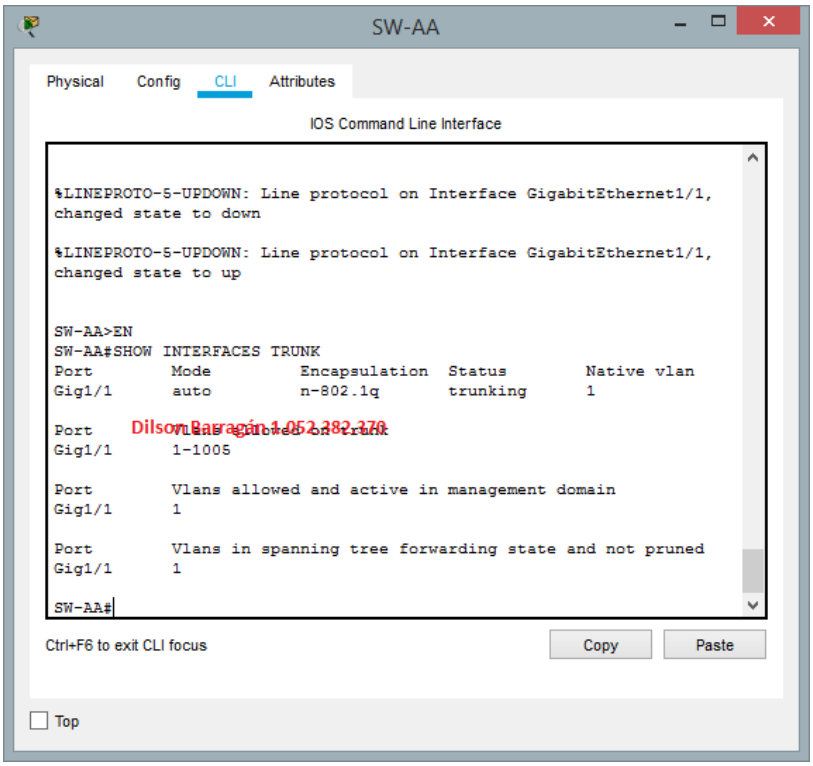

Figura 12. Verificación de enlace Trunk SW-AA

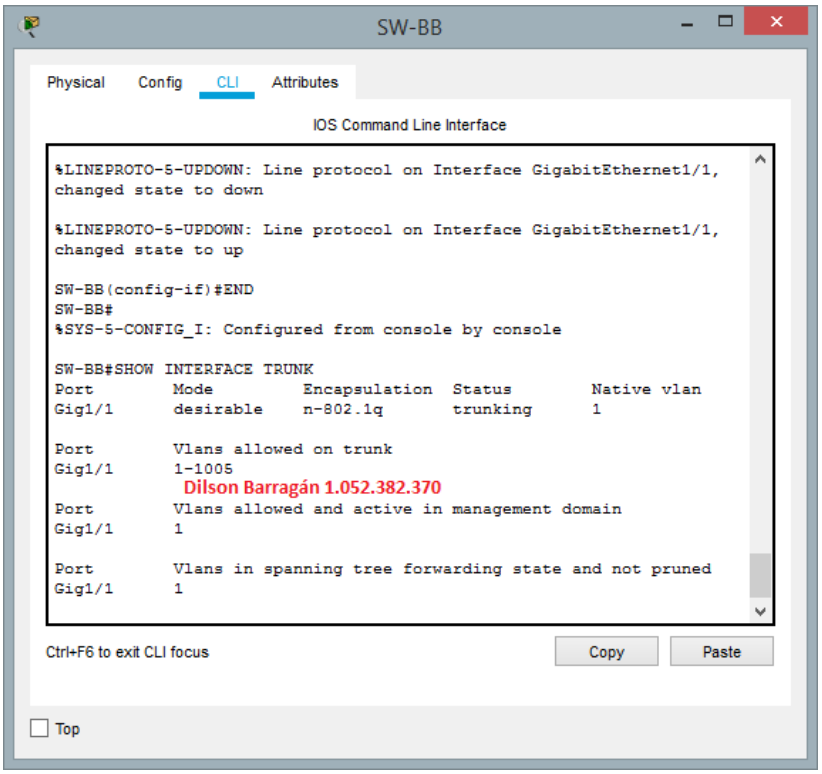

Figura 13. Verificación de enlace Trunk SW-BB

3. Entre SW-AA y SW-BB configure un enlace "trunk" estático utilizando el comando **switchport mode trunk** en la interfaz F0/3 de SW-AA

En el paso anterior se configuro un enlace dinámico entre estos dos switch, luego de analizar todo el inciso B se determina que posiblemente fue un Wrror al digitar la guía y se configura un enlace troncal en SW-AA y SW-CC a demás no se usa la interfaz serial F0/3, debido a que las interfaces usadas para esta ejercicios son interfaces Gigabit, esto como elemento diferenciador teniendo en cuenta además que el tipo de puerto no afecta el funcionamiento del protocolo.

```
SW-AA#CONFIGURE TERMINAL
SW-AA(config)#INTERFACE GIGABIT 0/1
SW-AA(config-if)#SWITCHPORT MODE TRUNK
SW-AA(config-if)#END
```

4. Verifique el enlace "Trunk" el comando **show interfaces Trunk** en SW-AA.

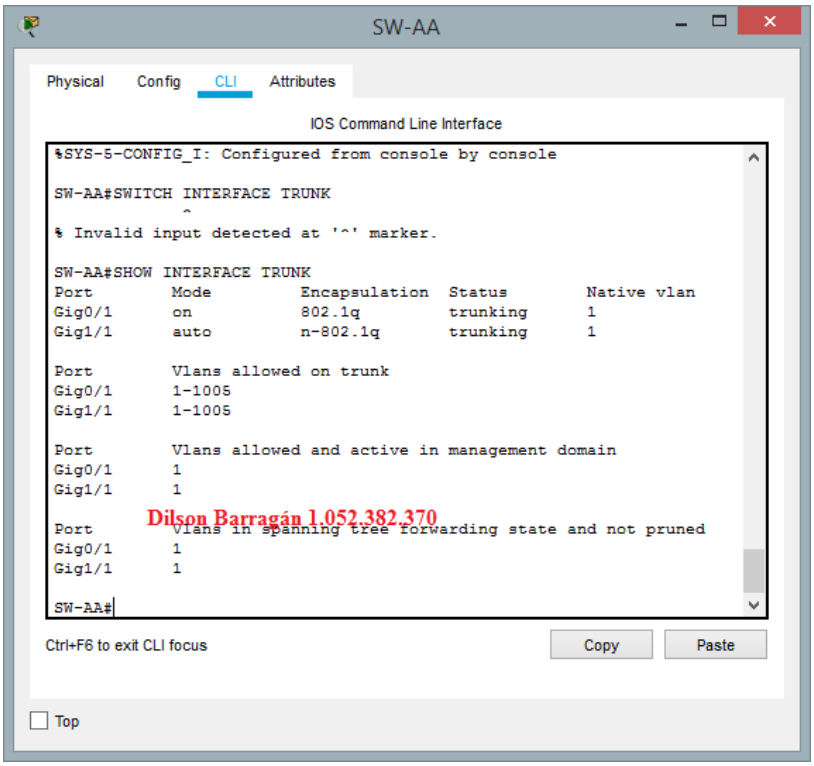

Figura 14. Verificación de enlace Trunk SW-AA

5. Configure un enlace "Trunk" permanente entre SW-BB y SW-CC.

```
SW-BB#CONFIGURE TERMINAL
SW-BB(config)#INTERFACE GIGABIT 0/1
SW-BB(config-if)#SWITCH MODE TRUNK
```

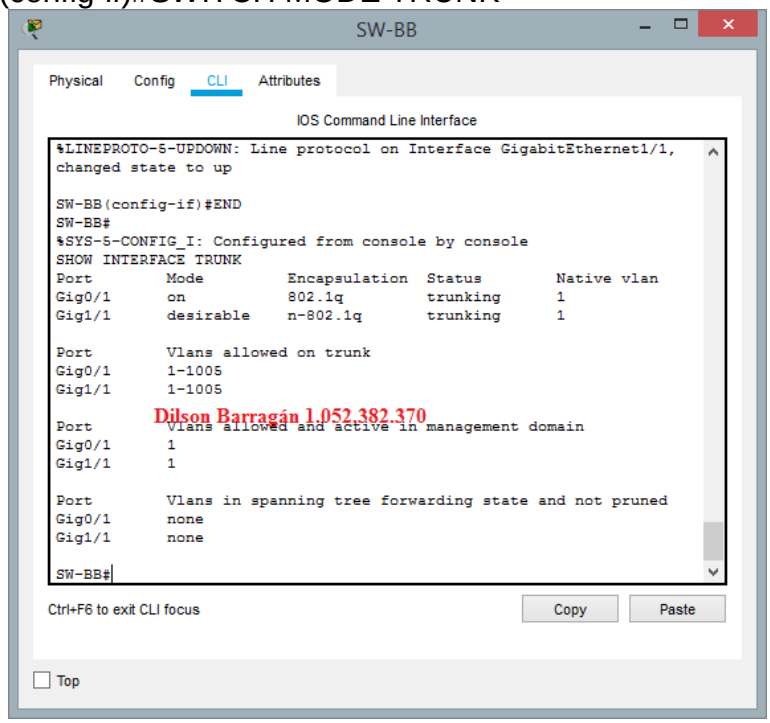

Figura 15. Verificación de enlace Trunk SW-BB

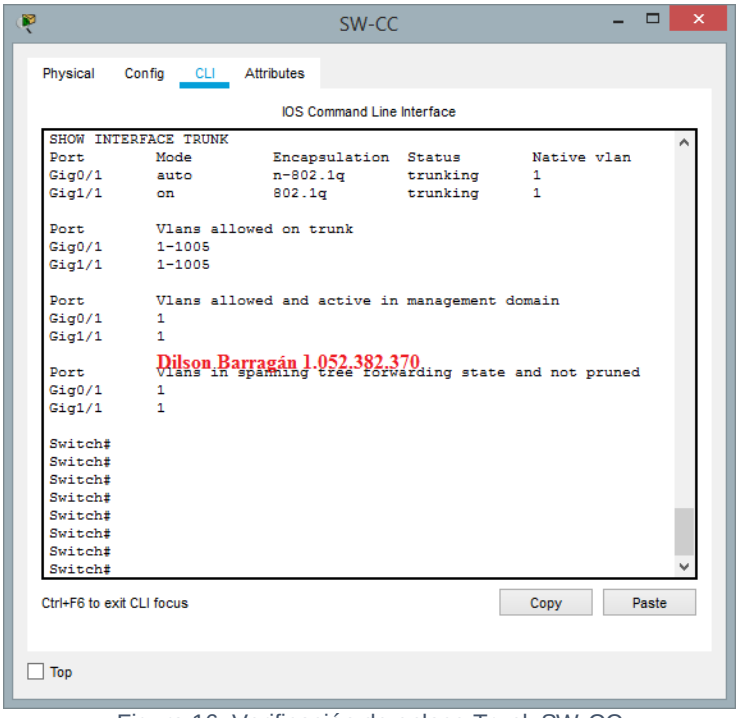

Figura 16. Verificación de enlace Trunk SW-CC

C. Agregar VLANs y asignar puertos.

1. En SW-AA agregue la VLAN 10. En SW-BB agregue las VLANS Compras (10), Personal (25), Planta (30) y Admon (99)

Configurar la VLAN 10 en SW-AA no se puede ya que este equipo esta me modo cliente

```
SW-BB#CONFIGURE TERMINAL
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#VLAN 10
SW-BB(config-vlan)#NAME Compras
SW-BB(config-vlan)#VLAN 20
SW-BB(config-vlan)#NAME Mercadeo
SW-BB(config-vlan)#VLAN 30
SW-BB(config-vlan)#NAME Planta
SW-BB(config-vlan)#VLAN 99
SW-BB(config-vlan)#NAME Admon
SW-BB(config-vlan)#exit
SW-BB(config)#
```

2. Verifique que las VLANs han sido agregadas correctamente.

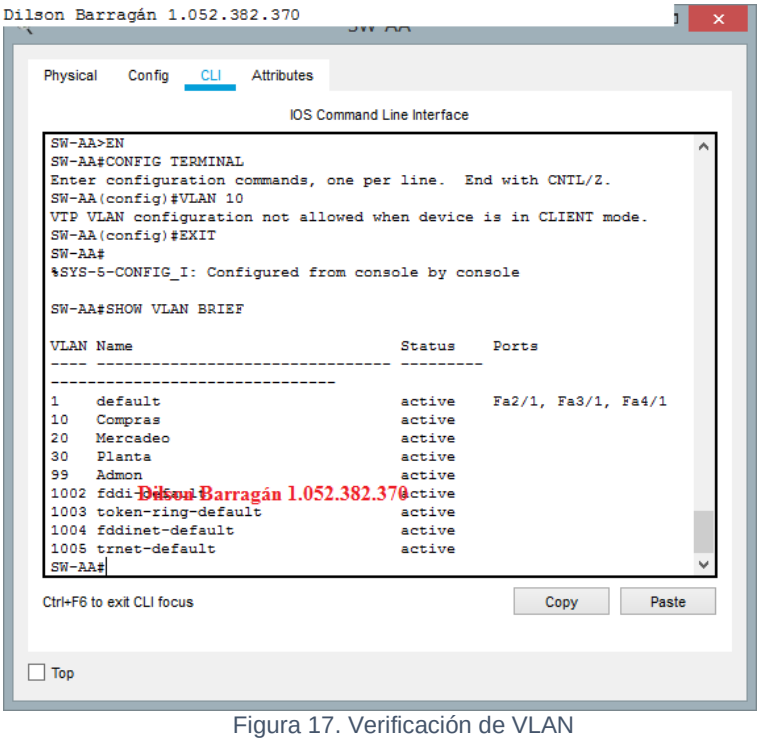

Figura 17. Verificación de VLAN

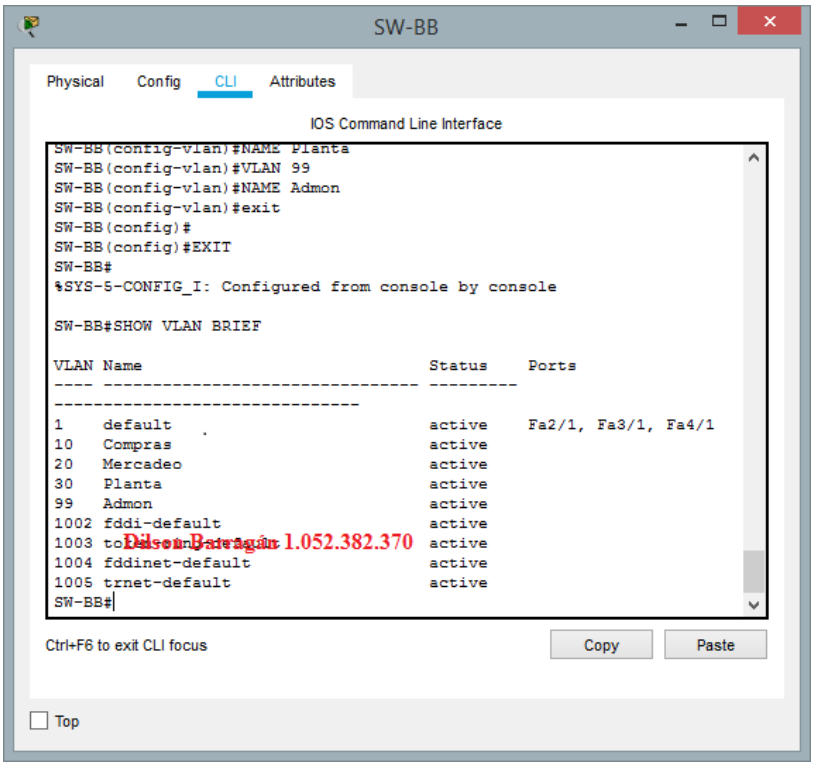

Figura 18. Verificación de VLAN en SW-BB

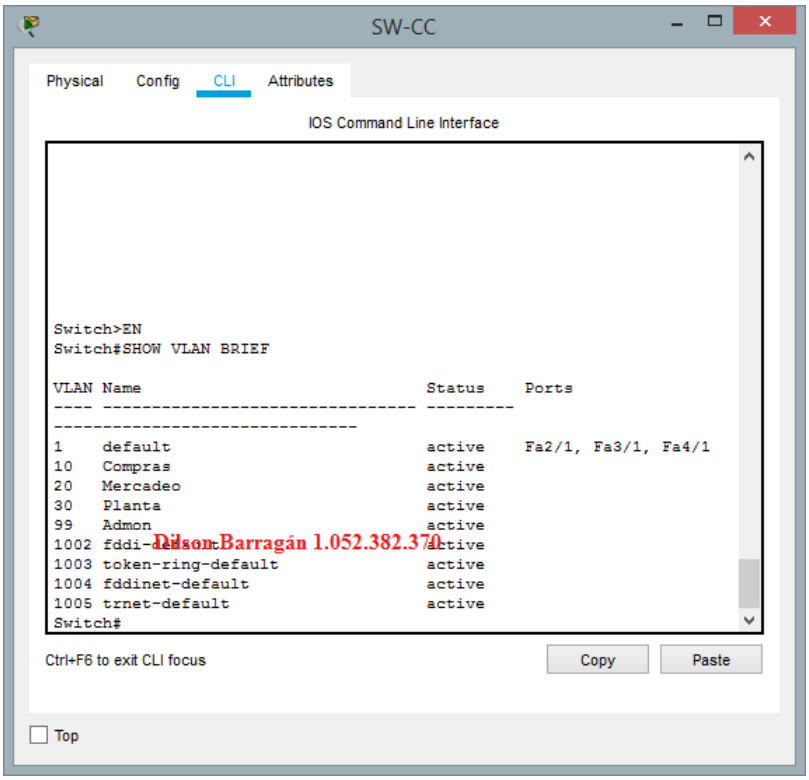

Figura 19. Verificación de VLAN en SW-CC

3. Asocie los puertos a las VLAN y configure las direcciones IP de acuerdo con la siguiente tabla.

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.X / 24
F0/15	VLAN 25	190.108.20.X /24
F0/20	VLAN 30	190.108.30.X /24

Tabla 2. Rango de Direcciones por Vlan

4. Configure el puerto F0/10 en modo de acceso para SW-AA, SW-BB y SW-CC y asígnelo a la VLAN 10.

5. Repita el procedimiento para los puertos F0/15 y F0/20 en SW-AA, SW-BB y SW-CC. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

```
SW-AA#CONFIGURE TERMINAL
SW-AA(config)#INTERFACE FASTETHERNET 2/1
SW-AA(config-if)#SWITCHPORT MODE ACCESS
SW-AA(config-if)#SWITCHPORT ACCESS VLAN 10
SW-AA(config-if)#INTERFACE FASTETHERNET 3/1
SW-AA(config-if)#SWITCHPORT MODE ACCESS
SW-AA(config-if)#SWITCHPORT ACCESS VLAN 20
SW-AA(config-if)#INTERFACE FASTETHERNET 4/1
SW-AA(config-if)#SWITCHPORT MODE ACCESS
SW-AA(config-if)#SWITCHPORT ACCESS VLAN 30
```

Se ejecutan los mismos comandos para los demás SWITCH las direcciones IP de cada PC se detallan en la siguiente tabla

PC	IP Address	Mascara
PC0	190.108.10.5	255.255.255.0
PC1	190.108.20.5	255.255.255.0
PC2	190.108.30.5	255.255.255.0
PC3	190.108.10.4	255.255.255.0
PC4	190.108.20.4	255.255.255.0
PC5	190.108.30.4	255.255.255.0
PC6	190.108.20.6	255.255.255.0
PC7	190.108.30.6	255.255.255.0
PC8	190.108.10.6	255.255.255.0

Tabla 3. Direcciones IP de cada PC

D. Configurar las direcciones IP en los Switches.

1. En cada uno de los Switches asigne una dirección IP al SVI (Switch Virtual Interface) para VLAN 99 de acuerdo con la siguiente tabla de direccionamiento y active la interfaz.

Equipo	Interfaz	Dirección IP	Máscara
SW-AA	VLAN 99	190.108.99.1	255.255.255.0
SW-BB	VLAN 99	190.108.99.2	255.255.255.0
SW-CC	VLAN 99	190.108.99.3	255.255.255.0

Tabla 4. Direcciones IP VLAN 99 para cada SWITCH

```
SW-AA(config)#INTERFACE VLAN 99
SW-AA(config-if)#IP ADDRESS 190.108.99.1 255.255.255.0

SW-BB(config)#INTERFACE VLAN 99
SW.BB(config-if)#IP ADDRESS 190.108.99.2 255.255.255.0

SW-CC(config)#INTERFACE VLAN 99
SW-CC(config-if)#IP ADDRESS 190.108.99.3 255.255.255.0
```

E. Verificar la conectividad Extremo a Extremo

1. Ejecute un Ping desde cada PC a los demás. Explique por qué el ping tuvo o no tuvo éxito.

Al realizar los ping hasta los diferentes solo resultan satisfactorios en los equipos que se encuentran dentro de la misma Vlan, los demás equipos no responden pues de esa manera fue configurada la red lo que se busca es que los usuarios de cada departamento no tengan acceso a los equipos e información de los demás departamentos

2. Ejecute un Ping desde cada Switch a los demás. Explique por qué el ping tuvo o no tuvo éxito.

El ping realizado entre los Switches fue exitosos, dado que las interfaces físicas que en rutan los datos enviados a través del protocolo ICMP entre los tres Switches están configuradas en modo troncal, y según se verifico mediante el comando show interfaces trunk, comparten el mismo tipo de encapsulamiento

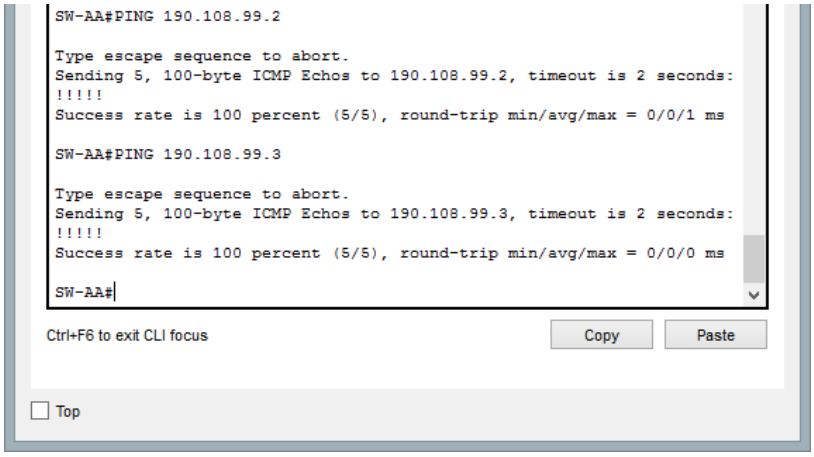

Figura 20. ping desde SW-AA a sus vecinos

3. Ejecute un Ping desde cada Switch a cada PC. Explique por qué el ping tuvo o no tuvo éxito.

El ping realizado entre los Switches y los PCs no tuvo éxito. Pues aunque se habilitaron las VLAN en cada uno de los Switches a través del protocolo VTP, no existe una configuración de enrutamiento IP para las VLAN 30, 20, 10 por lo que se hace necesario configurar dirección IP y mascara de red a la interface VLAN de los switches e interfaces nativas

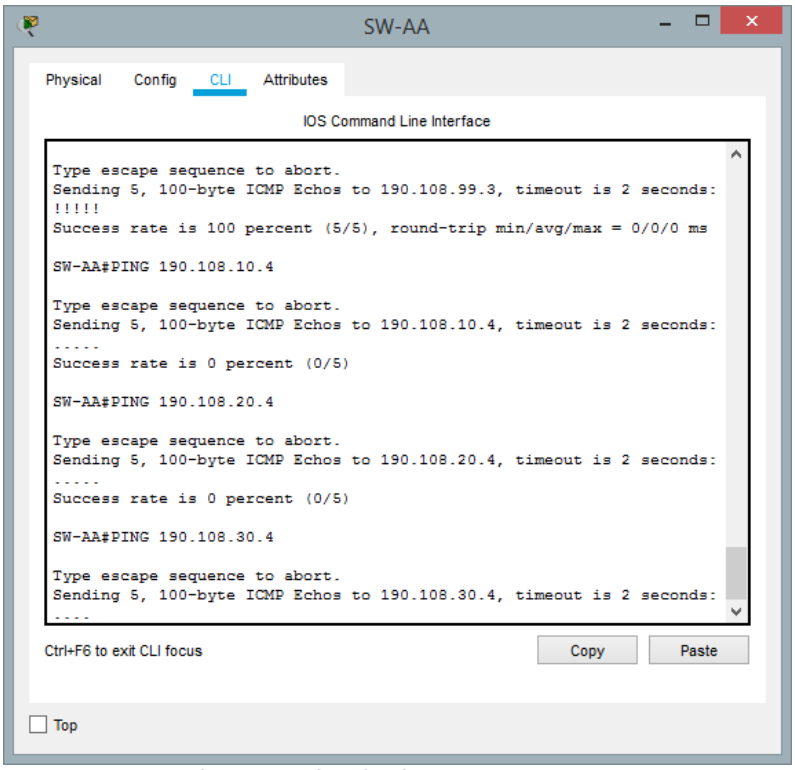

Figura 21. Ping desde SW-AA a sus PC

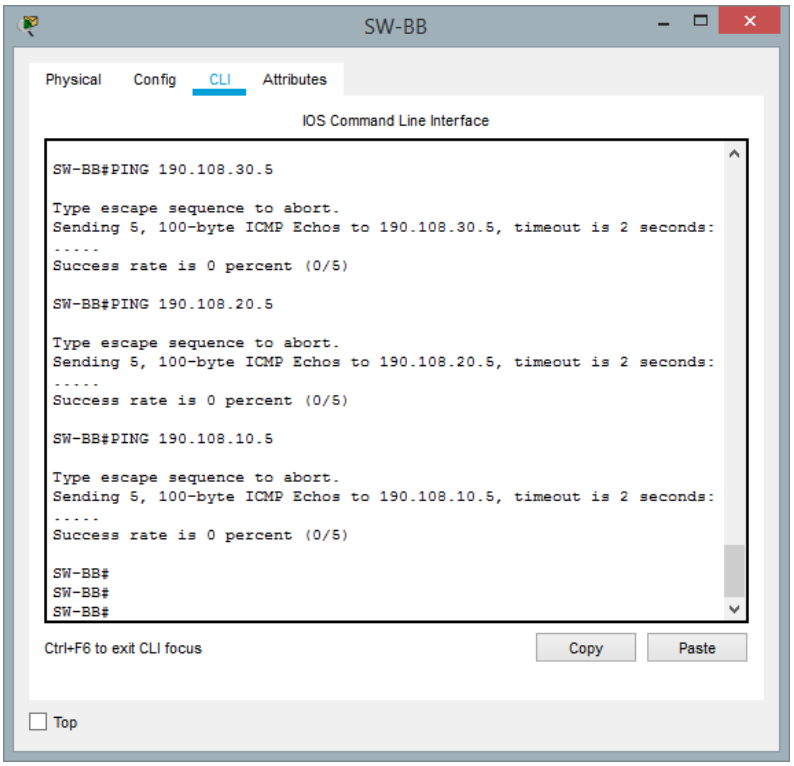

Figura 22. Ping desde SW-BB a sus PC

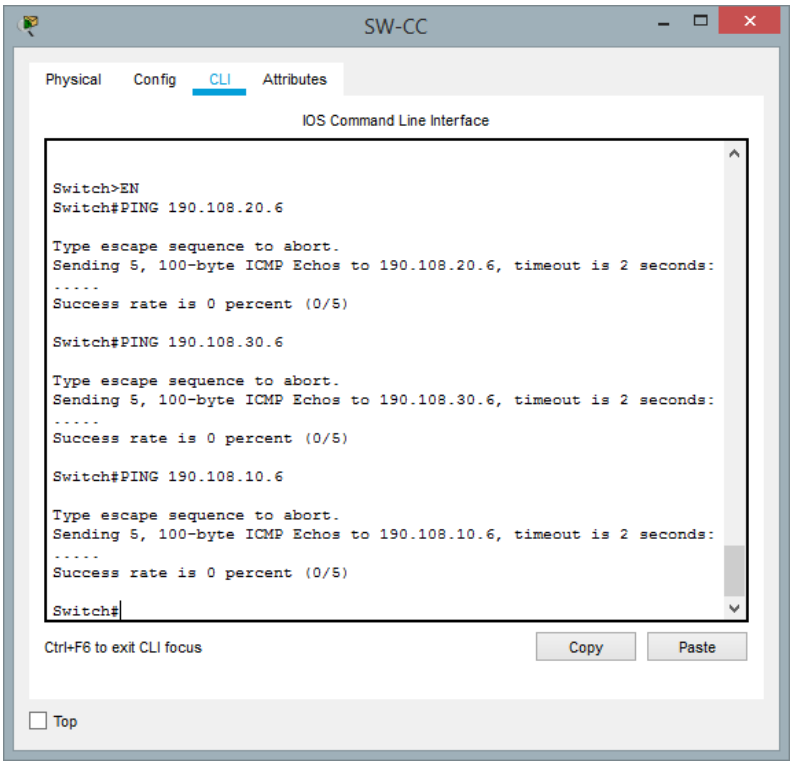

Figura 23. Ping desde SW-CC a sus PC

CONCLUSIONES

Tras completar las configuraciones requeridas para cada dispositivo de los diferentes escenarios, se logró afianzar los conocimientos adquiridos en el desarrollo del curso en especial sobre los requerimientos y métricas que se tienen en cuenta para el envió de tráfico a través de protocolo BGP, así como para la redistribución de rutas, creación de subredes, configuración del protocolo DTP (Dynamic Trunking Protocol) y del protocolo VTP. Estableciendo es este último caso, un dispositivo servidor a partir del cual se actualice la configuración de otros dispositivos, clientes, como parte del enrutamiento a través de redes de área local virtuales (Vlans).

Con el uso e implementación de las VLAN Como elemento de seguridad nos permite la segmentación adecuada de una red limitando de esta manera cualquier acceso no autorizado a los recursos de la red que no le sean necesarios y logrando una división basada en departamentos, servicios o localidades.

Se aplica el uso de la redistribución de protocolos de enrutamiento con el fin anunciar rutas que se aprenden por otros medios, como otro protocolo de enrutamiento, rutas estáticas o rutas directamente conectadas y al redistribuir a otro protocolo de enrutamiento, hay que tener presente las métricas de cada uno ya que juegan un papel importante en la redistribución. Cada protocolo utiliza diferentes métricas.

BIBLIOGRAFÍA

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

Froom, R., Frahim, E. (2015). CISCO Press (Ed). InterVLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing a Border Gateway Protocol (BGP) Solution for ISP Connectivity. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx