DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

GIOVANNY GUZMAN RAMIREZ

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

GIOVANNY GUZMAN RAMIREZ

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 ELECTRONICA
ZIPAQUIRA
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

ZIPAQUIRA, 22 de mayo de 2020

AGRADECIMIENTOS

Agradezco principalmente a Dios, quien ha constituido la fuerza de continuar siempre hacia adelante. También agradezco a mi familia, por su incondicional apoyo a mi vida durante este tiempo; especialmente a mi hijo, por ser mi motivación a crecer y no rendirme ante los obstáculos, así como por permanecer a mi lado aún en los momentos de dificultad. No puedo dejar de agradecer además a cada uno de los tutores de la Universidad Nacional Abierta y a Distancia por su acompañamiento, dedicación, paciencia, por compartir su conocimiento y por permitir que este modelo de estudio contribuya a la superación y crecimiento personal de los estudiantes.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

VLAN: Tecnología de red que permite la implementación de subredes dentro de una red conmutada de forma virtual. Cada VLAN es una subred diferente con direcciones IP asociadas.

NEIGHBOR: Relación de vecindad establecida entre dispositivos de red como routers debido a su adyacencia, la cual permite el intercambio de información.

NETWORKING: Definición de una red de computadoras u ordenadores conectados a algún medio físico que permite su comunicación para la transmisión de información. Por medio de esta red se envían y/o reciben ondas electromagnéticas, pulsos, señales digitales u otros medios que permiten el transporte de los datos.

ROUTER: Dispositivo de red que permite la interconexión de computadoras y equipos que operan en una interfase de red. Su función consiste en establecer la mejor ruta para que un paquete de información llegue a su destino de forma segura.

SWITCHING: Acción de enviar y recibir tramas realizada por un switch en un entorno de red, de acuerdo con el puerto de entrada y la dirección de destino. En una red LAN es común que el switch maneje internamente una tabla, mediante la cual establece el camino para reenviar la información.

VTP: Protocolo utilizado para la configuración de VLANs en una red de Cisco, permitiendo su creación y administración, así como simplificando su establecimiento en los diferentes nodos.

RESUMEN

Se presenta en esta prueba el análisis y posterior desarrollo a distintas configuraciones realizadas sobre 2 escenarios de red determinados, los cuales hacen parte de un ejercicio final del diplomado CCNP de CISCO, presentado para optar al título de ingeniería electrónica. Se establece el paso a paso para su desarrollo, identificando en el proceso el código implementado en cada uno de los dispositivos, mediante el cual fue posible alcanzar los objetivos propuestos en cada actividad.

En el primer escenario es configurado el debido enrutamiento, así como las relaciones de vecino BGP entre 4 routers y posteriormente constatadas mediante el comando show ip route. Por otro lado, en el segundo escenario es establecido el protocolo VTP en una interfaz de equipos, switches y VLANs determinados, estableciendo enlaces troncales, conmutación, y el debido direccionamiento de puertos en cada dispositivo que compone la red.

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

ABSTRACT

The analysis and subsequent development of different configurations carried out on 2 determined network stages are presented in this test, which are part of a final exercise of the CISCO CCNP diploma, presented to apply for the title of electronic engineering. The step by step for its development is established, identifying in the process the code implemented in each of the devices, through which it was possible to achieve the objectives proposed in each activity.

In the first stage, proper routing is configured, as well as the BGP neighbor relationships between 4 routers and subsequently verified using the show ip route command. On the other hand, in the second scenario, the VTP protocol is established in an interface of certain equipment, switches and VLANs, establishing trunks, switching, and the proper addressing of ports in each device that makes up the network.

Keywords: CISCO, CCNP, Routing, Swicthing, Network, Electronic.

INTRODUCCION

El mundo de las redes no se detiene, evolucionando cada día en razón de establecer protocolos seguros, medios más rápidos, en general, sistemas más sofisticados y eficientes. Es así como se torna indispensable para el administrador de una red el manejo y conocimiento de protocolos de enrutamiento en sistemas WAN, LAN, MAN VLAN, etc.

Uno de estos protocolos es el BGP, que surge como una opción de enrutamiento robusto y escalable cuyo objetivo es establecer el intercambio de información estable entre sistemas autónomos. Otro protocolo muy conocido y aplicado en el establecimiento de redes VLANs es el protocolo VTP, mediante el cual es posible simplificar la administración de redes VLAN en un solo switch.

En las siguiente páginas son presentadas las respectivas configuraciones aplicadas para el correcto establecimiento de protocolos tanto EBGP como VTP, en 2 escenarios de red establecidos y mediante herramientas de simulación en software como GNS3 y Packet tracer de Cisco. Tales ejercicios son desarrollados como actividad evaluativa de los conocimientos adquiridos en el diplomado de profundización CCNP de Cisco.

DESARROLLO DE LAS PRUEBAS

1. ESCENARIO 1

Figura 1. Escenario 1

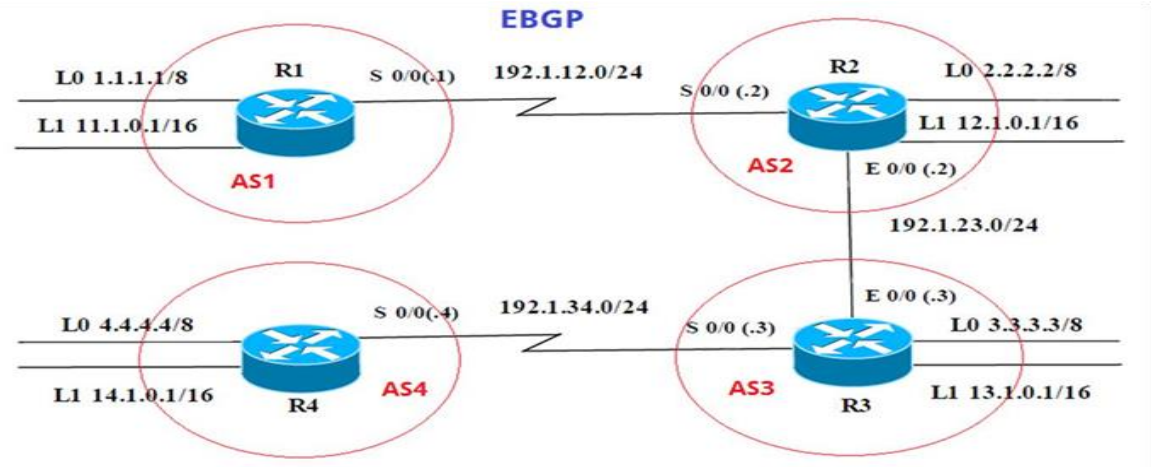


Figura 2. Simulación escenario 1 en GNS3

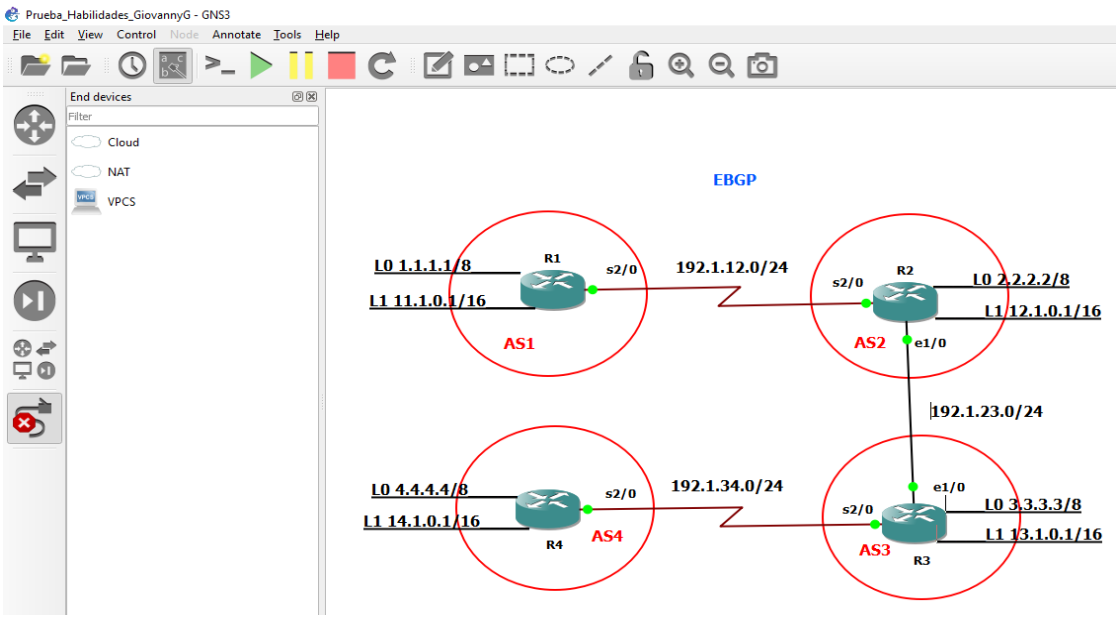


Tabla 1. Información para configuración de los Routers

	Interfaz	Dirección IP	Máscara
R1	Loopback 0	1.1.1.1	255.0.0.0
	Loopback 1	11.1.0.1	255.255.0.0
	S 2/0	192.1.12.1	255.255.255.0
	Interfaz	Dirección IP	Máscara
R2	Loopback 0	2.2.2.2	255.0.0.0
	Loopback 1	12.1.0.1	255.255.0.0
	S 2/0	192.1.12.2	255.255.255.0
	E 1/0	192.1.23.2	255.255.255.0
	Interfaz	Dirección IP	Máscara
R3	Loopback 0	3.3.3.3	255.0.0.0
	Loopback 1	13.1.0.1	255.255.0.0
	E 1/0	192.1.23.3	255.255.255.0
	S 2/0	192.1.34.3	255.255.255.0
	Interfaz	Dirección IP	Máscara
R4	Loopback 0	4.4.4.4	255.0.0.0
	Loopback 1	14.1.0.1	255.255.0.0
	S 2/0	192.1.34.4	255.255.255.0

1. 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 con los comandos utilizados y la salida del comando ***show ip route.***

Configuración relación de vecino BGP entre R1 y R2

```
R1#configure terminal
R1(config)#interface Loopback 0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#interface Loopback 1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#interface serial 2/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
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 11.1.0.0 mask 255.255.0.0
R1(config-router)#network 192.1.12.0 mask 255.255.255.0
R1(config-router)#neighbor 192.1.12.2 remote-as 2

R2#configure terminal
```

```
R2(config)#interface Loopback 0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#interface Loopback 1
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#interface serial 2/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#interface Ethernet 1/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router bgp 2
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#network 2.0.0.0 mask 255.0.0.0
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
R2(config-router)#network 192.1.12.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.12.1 remote-as 1
```

Figura 3. Configuración neighbors en R1

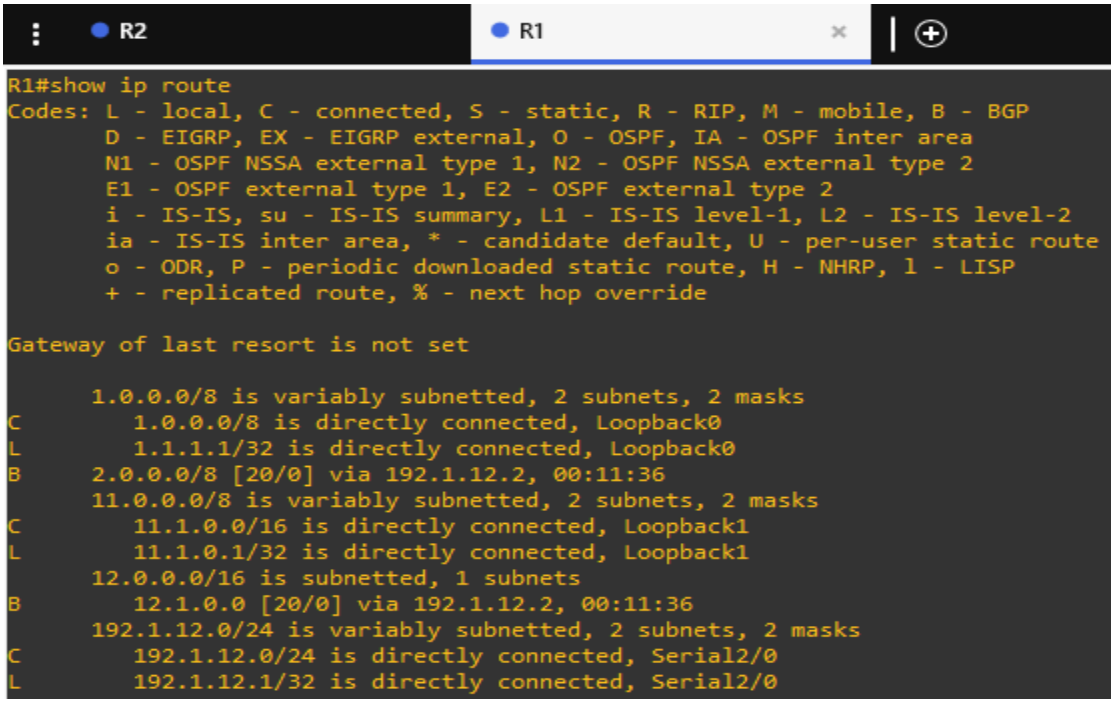
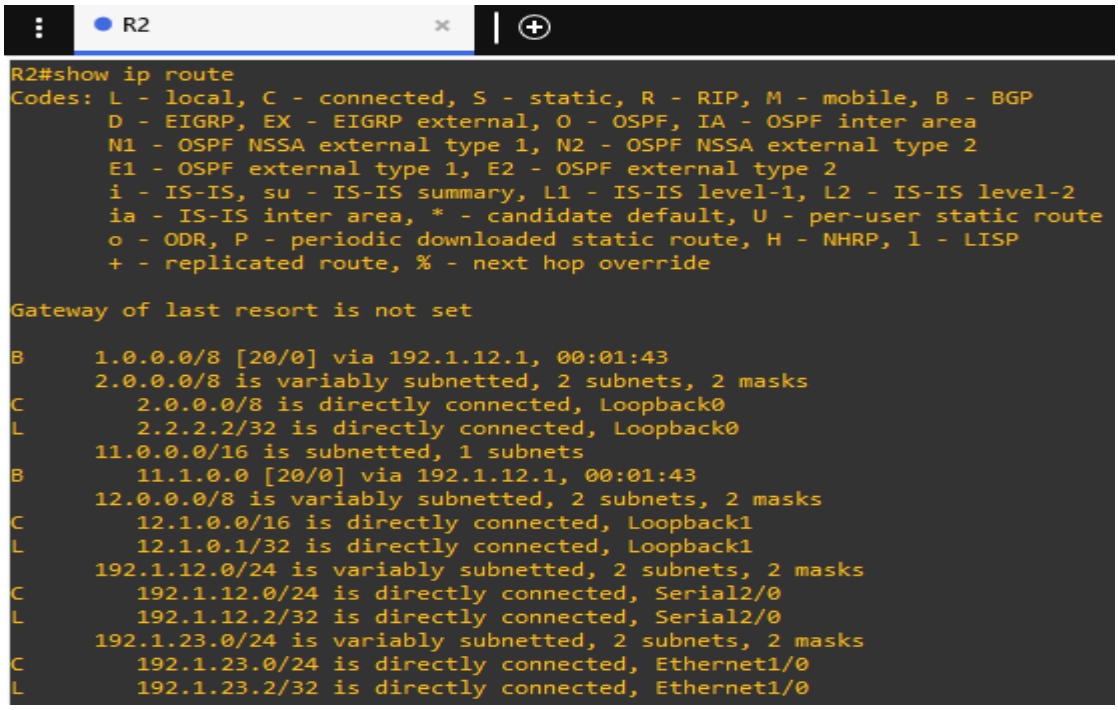


Figura 4. Configuración neighbors en R2



Se puede observar en las figuras 3 y 4 el resultado del comando **show ip route** en los routers R1 y R2 posterior a la configuración individual de las direcciones ip, direcciones Loopback, las direcciones de las redes de conexión directa y las interfaces vecinas correspondientes, de acuerdo a la tabla de direcciones establecida para cada router. Se observa también como ambos routers establecen comunicación mediante la red 192.1.12.0/24 mediante la interfaz serial 2/0.

2. 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.***

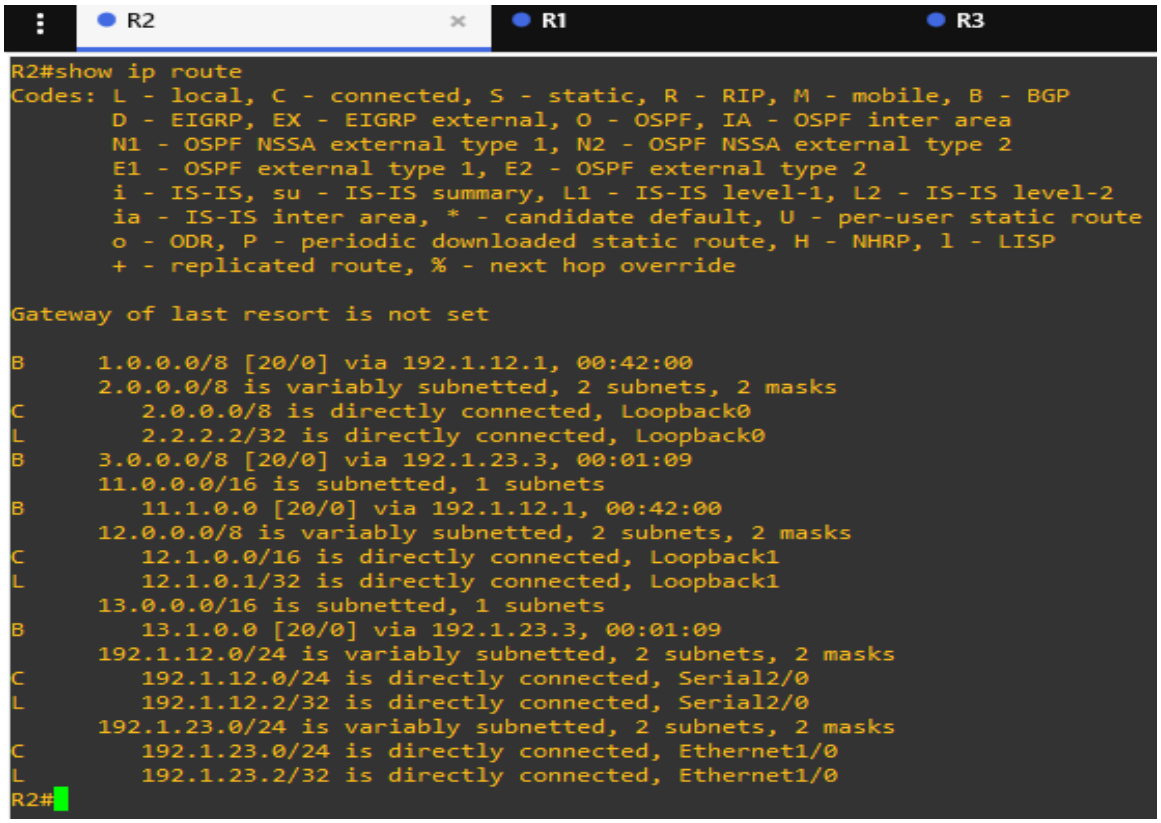
Configuración relación de vecino BGP entre R2 y R3

```
R2#configure terminal
R2(config)#router bgp 2
R2(config-router)#network 192.1.23.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.23.3 remote-as 3

R3#configure terminal
R3(config)#interface Loopback 0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#interface Loopback 1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
```

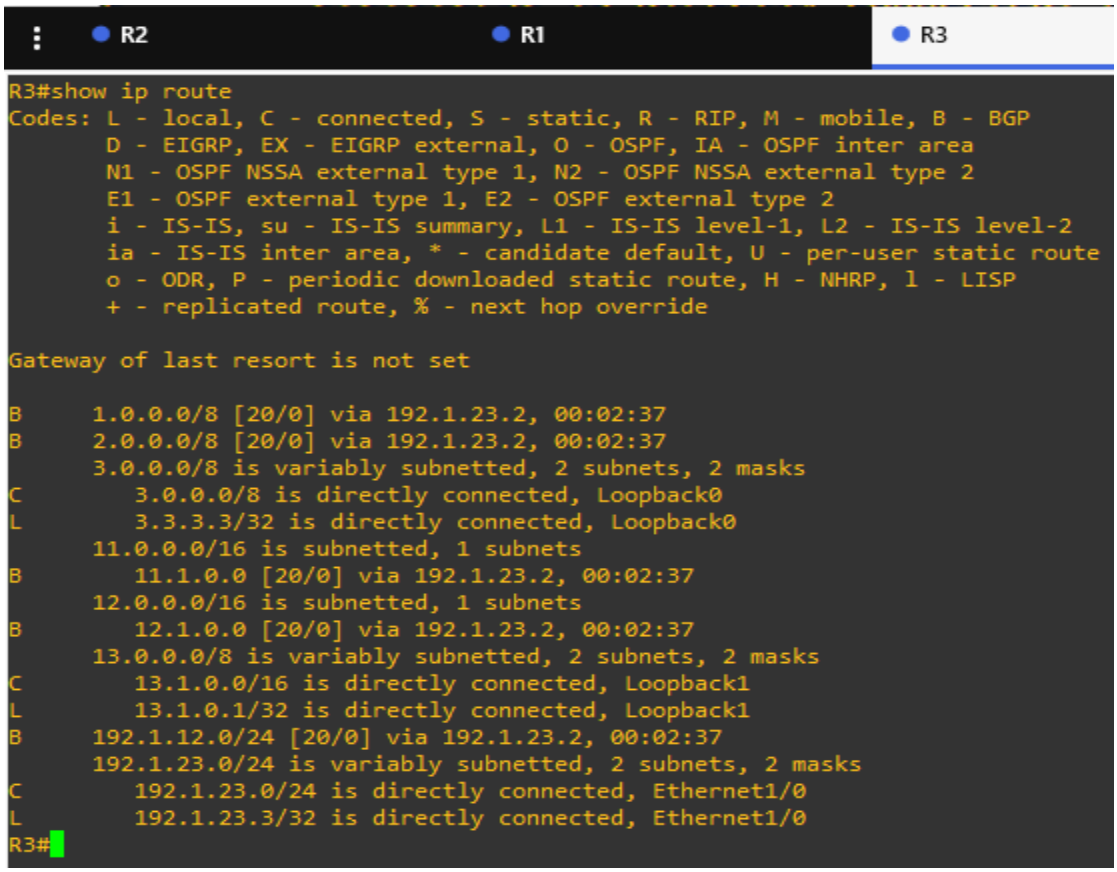
```
R3(config-if)#interface Ethernet 1/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#interface serial 2/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#network 3.0.0.0 mask 255.0.0.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3(config-router)#network 192.1.23.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.23.2 remote-as 2
```

Figura 5. Actualización neighbors en R2.



Se observa en la figura 5 que en el router R2 ahora aparecen las direcciones Loopback establecidas en R3, contando entonces con 4 rutas BGP reconocidas por la letra B en la columna izquierda.

Figura 6. Configuración neighbors en R3



En la figura 6 se visualiza la configuración realizada en R3 sobre sus interfaces Loopback, las interfaces Ethernet 1/0 y serial 2/0 mediante las cuales se comunica con R2 y R4. Es posible también observar en R3 la presentación de la dirección que comunica a R1 con R2 la cual obtuvo por medio de la configuración BGP.

3. 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.***

Configuración relación de vecino BGP entre R3 y R4

```
R3#configure terminal
R3(config)#router bgp 3
R3(config-router)#network 192.1.34.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.34.4 remote-as 4
```

```
R4#configure terminal
R4(config)#interface Loopback 0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#interface Loopback 1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#interface serial 2/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#router bgp 4
R4(config-router)#bgp router-id 66.66.66.66
R4(config-router)#network 4.0.0.0 mask 255.0.0.0
R4(config-router)#network 14.1.0.0 mask 255.255.0.0
R4(config-router)#network 192.1.34.0 mask 255.255.255.0
R4(config-router)#neighbor 192.1.34.3 remote-as 3
```

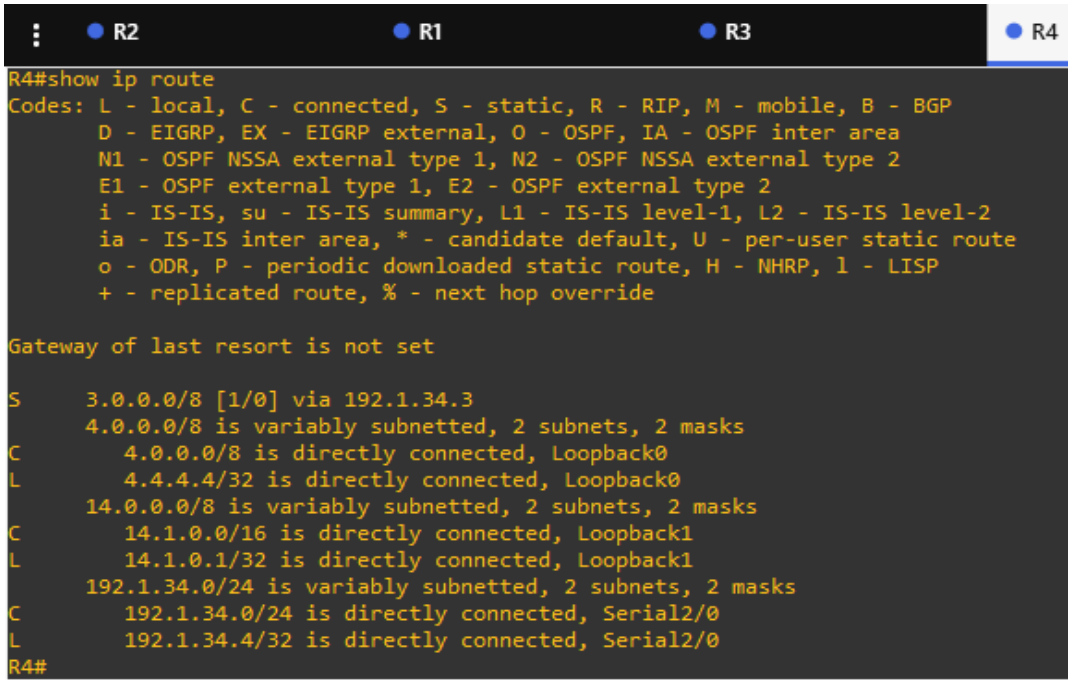
Para establecer las relaciones con base en la interfaz loopback se requiere configurar para que cualquier uso sea notificado. Se establece entonces la siguiente configuración:

```
R3#configure terminal
R3(config)#ip route 4.0.0.0 255.0.0.0 192.1.34.4
R3(config)#router bgp 3
R3(config-router)#no neighbor 192.1.34.4
R3(config-router)#no network 3.0.0.0 mask 255.0.0.0
R3(config-router)#neighbor 4.4.4.4 remote-as 4
R3(config-router)#neighbor 4.4.4.4 update-source loopback 0
R3(config-router)# neighbor 4.4.4.4 ebgp-multihop

R4(config)#ip route 3.0.0.0 255.0.0.0 192.1.34.3
R4(config)#router bgp 4
R4(config-router)#no neighbor 192.1.34.3
R4(config-router)#neighbor 3.3.3.3 remote-as 4
R4(config-router)#neighbor 3.3.3.3 update-source loopback 0
R4(config-router)# neighbor 3.3.3.3 ebgp-multihop
```

Figura 7. Actualización neighbors en R3

Figura 8. Configuración neighbors en R4



Se observa en la figura 7 la actualización de la información del router R3 donde se ve que su conexión con R4 ahora es por medio de la interfaz Loopback 0, que se presenta como estática. Dado que Loopback 0 es utilizada como dirección lógica, la red 192.1.4.0/24 continua como enlace físico.
Mientras tanto en el router R4, se evidencia el cambio en el enlace con los vecinos por medio ahora de la dirección Loopback 0 de R3.

2. ESCENARIO 2

Figura 9. Escenario 2

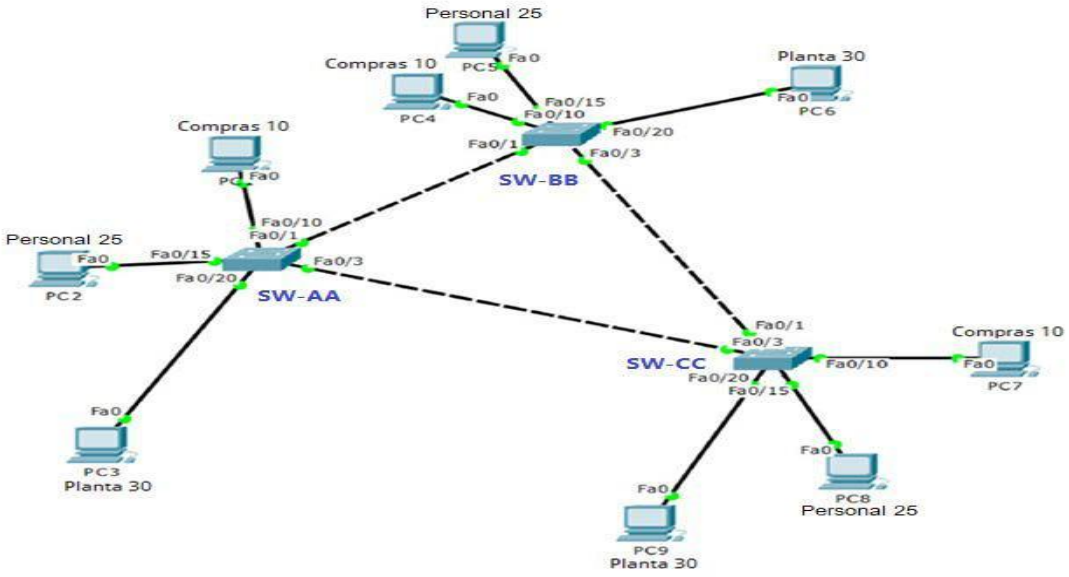
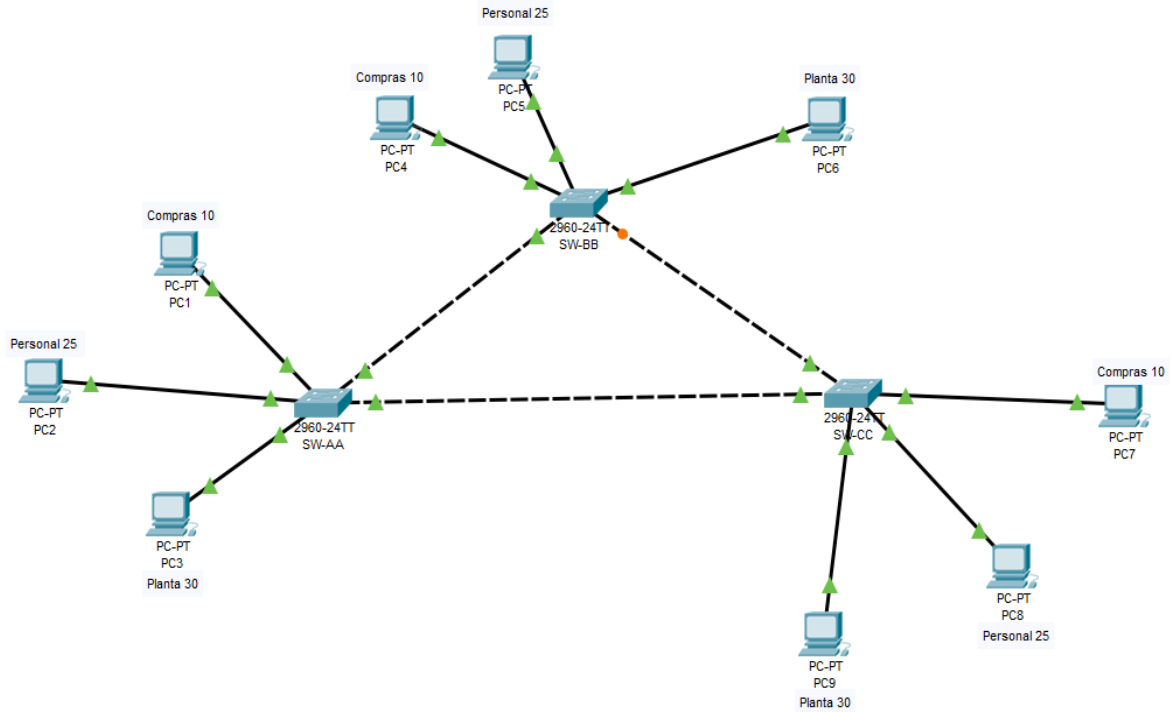


Figura 10. Simulación escenario 2 en Cisco Packet Tracer



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.

```
SW-AA#enable
SW-AA#config terminal
SW-AA(config)#vtp mode client
Setting device to VTP CLIENT mode
SW-AA(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-AA(config)#vtp version 2
SW-AA(config)#vtp password cisco
Setting device VLAN database password to cisco

SW-BB#enable
SW-BB#configure terminal
SW-BB(config)#vtp mode server
Device mode already to VTP SERVER
SW-BB(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-BB(config)#vtp version 2
SW-BB(config)#vtp password cisco
Setting device VLAN database password to cisco

SW-CC#enable
SW-CC#configure terminal
SW-CC(config)#vtp mode client
Setting device to VTP CLIENT mode
SW-CC(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-CC(config)#vtp version 2
SW-CC(config)#vtp password cisco
Setting device VLAN database password to cisco
```

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

Figura 11. Configuración VTP en SW-AA

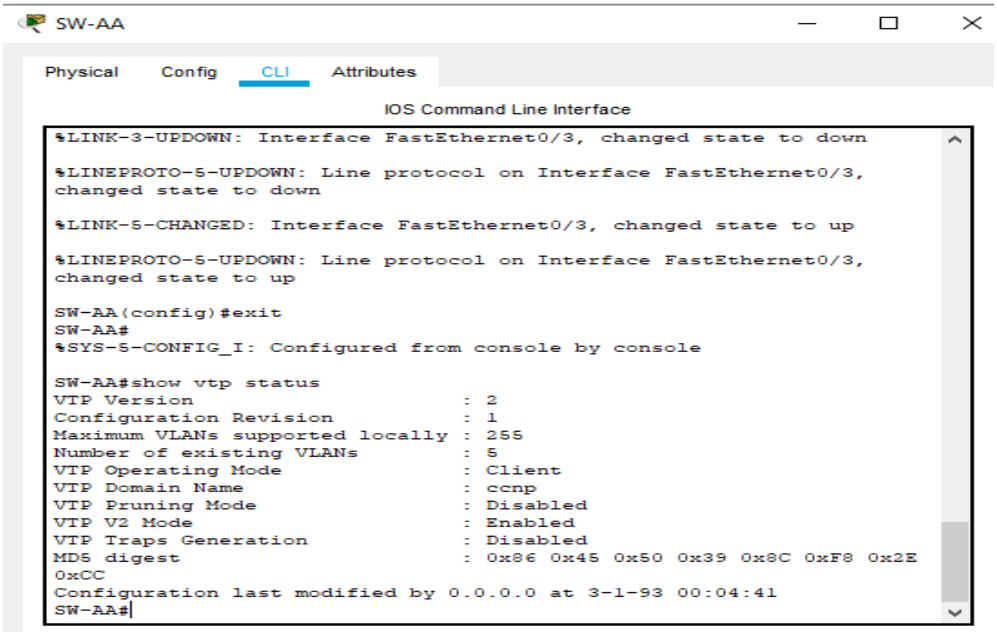


Figura 12. Configuración VTP en SW-BB

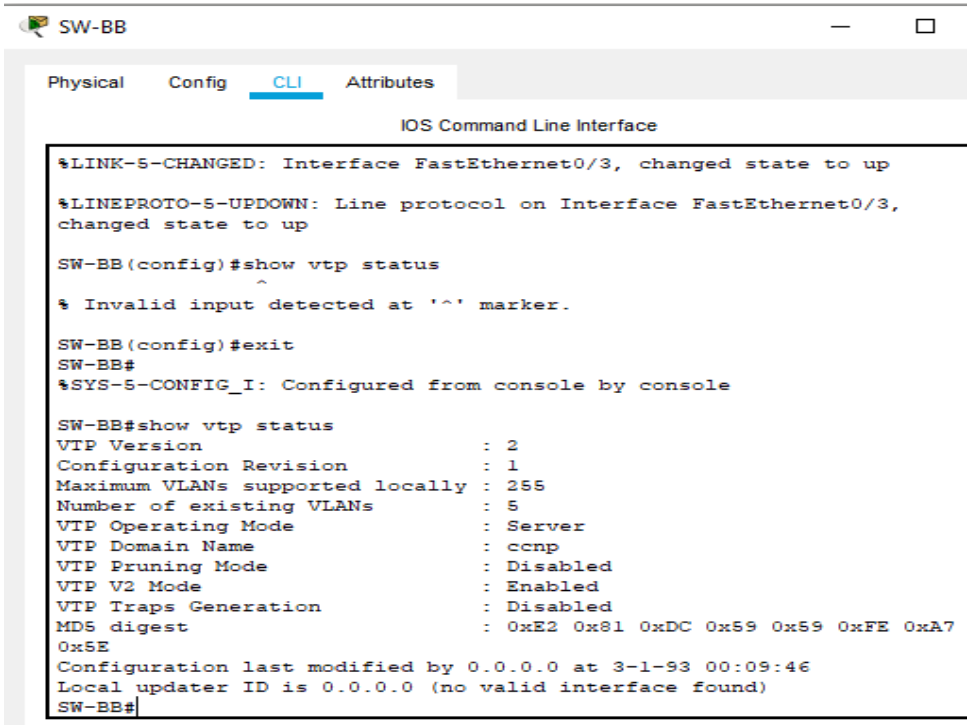
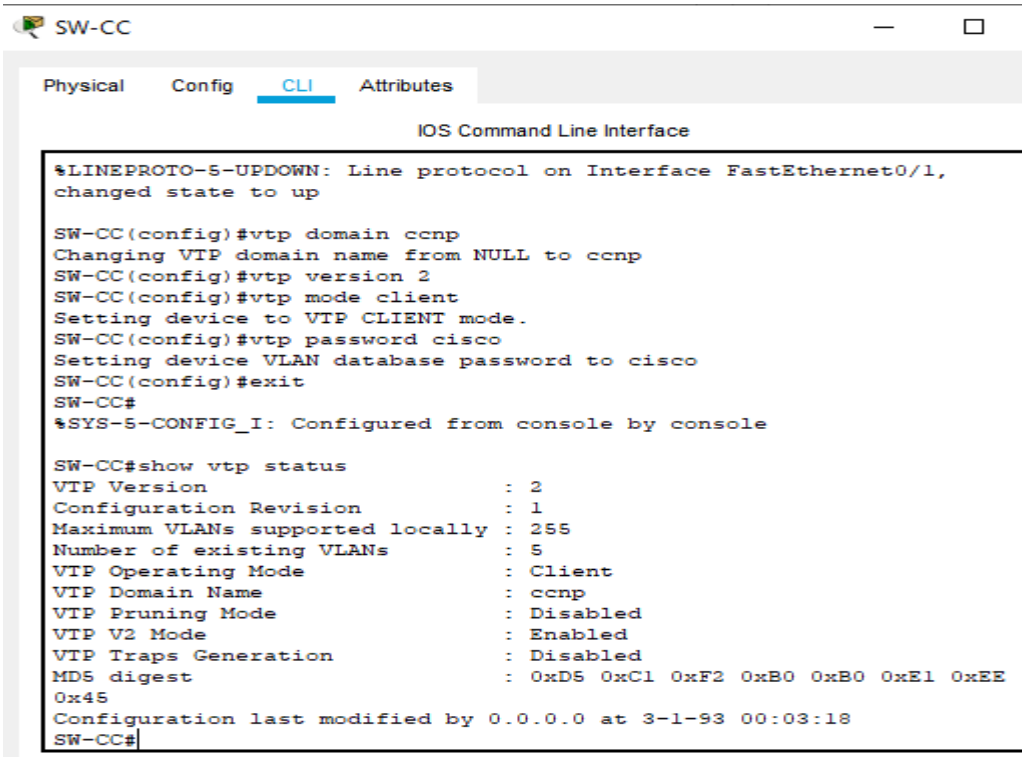


Figura 13. Configuración VTP en SW-CC



B. Configurar DTP (Dynamic Trunking Protocol)

4. 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-AA#configure terminal
SW-AA(config)#interface fastEthernet 0/1
SW-AA(config)#switchport mode trunk
SW-AA(config)#no shutdown

SW-BB#configure terminal
SW-BB(config)#interface fastEthernet 0/1
SW-BB(config)#switchport mode trunk
SW-BB(config-if)#switchport mode dynamic desirable
SW-BB(config)#no shutdown
```

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

Figura 14. Enlace trunk en SW-AA

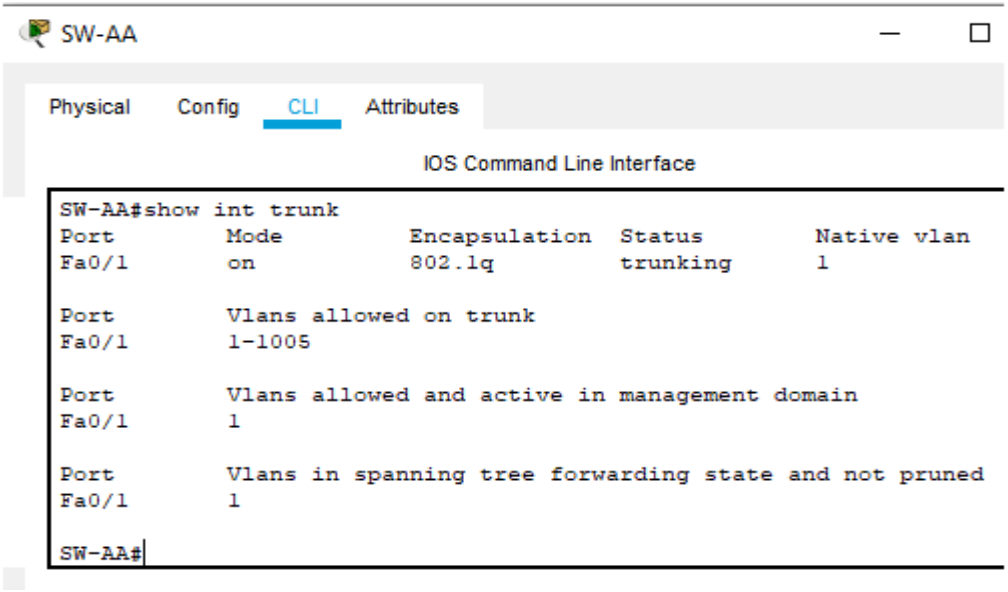
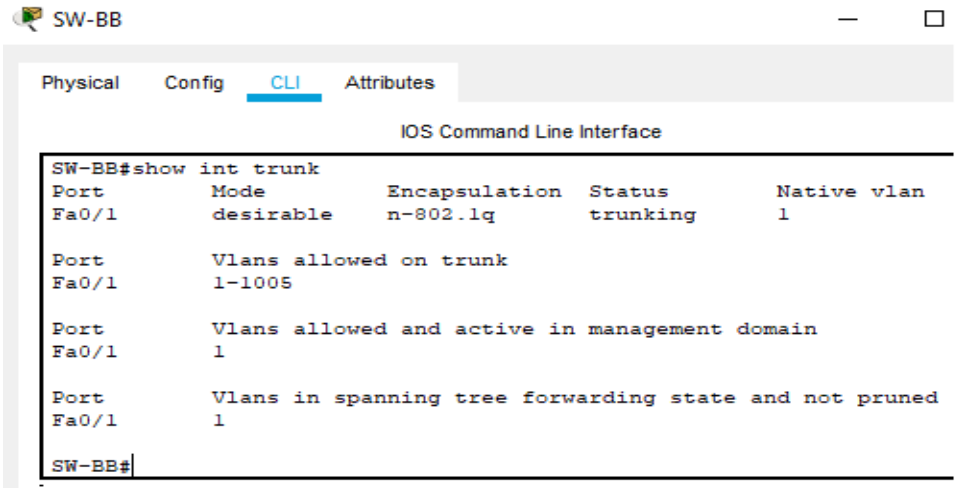


Figura 15. Enlace trunk en SW-BB

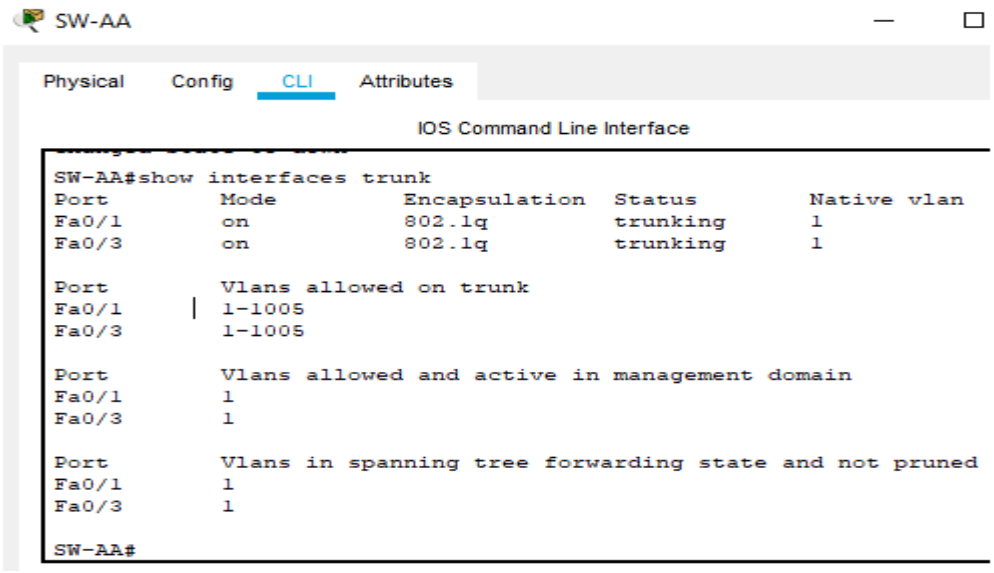


6. Entre SW-AA y SW-BB configure un enlace "trunk" estático utilizando el comando ***switchport mode trunk*** en la interfaz F0/3 de SW-AA

```
SW-AA#configure terminal
SW-AA(config)#interface fastEthernet 0/3
SW-AA(config-if)#switchport trunk encapsulation dot1q
SW-AA(config-if)#switchport mode trunk
SW-AA(config-if)#no shutdown
```

7. Verifique el enlace "trunk" el comando ***show interfaces trunk*** en SW-AA.

Figura 16. Verificación enlace trunk en SW-AA



8. Configure un enlace "trunk" permanente entre SW-BB y SW-CC.

```
SW-BB#configure terminal
SW-BB(config)#interface fastEthernet 0/3
SW-BB(config-if)#switchport mode trunk
SW-BB#no shutdown

SW-CC#configure terminal
SW-CC(config)#interface fastEthernet 0/1
SW-CC(config-if)#switchport mode trunk
SW-CC#no shutdown
```

Figura 17. Enlace trunk permanente configurado en SW-BB

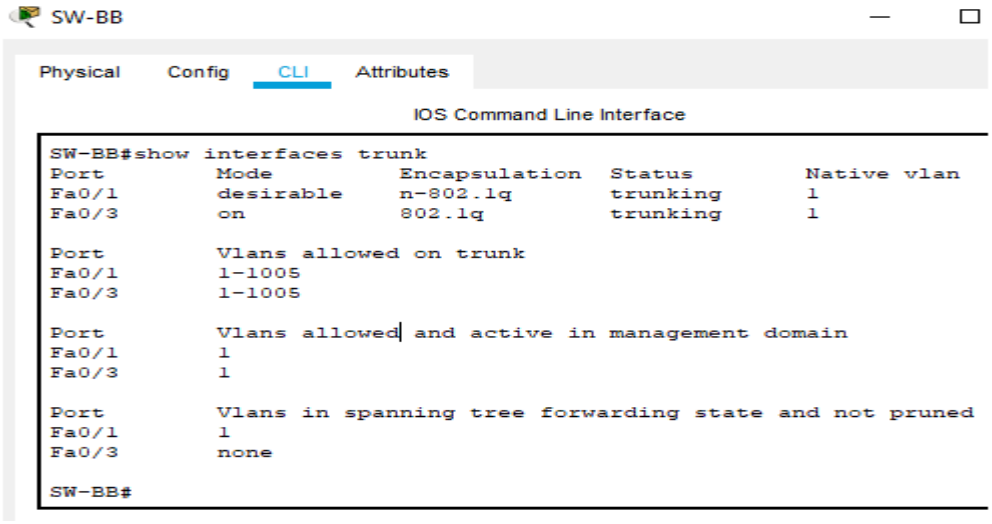
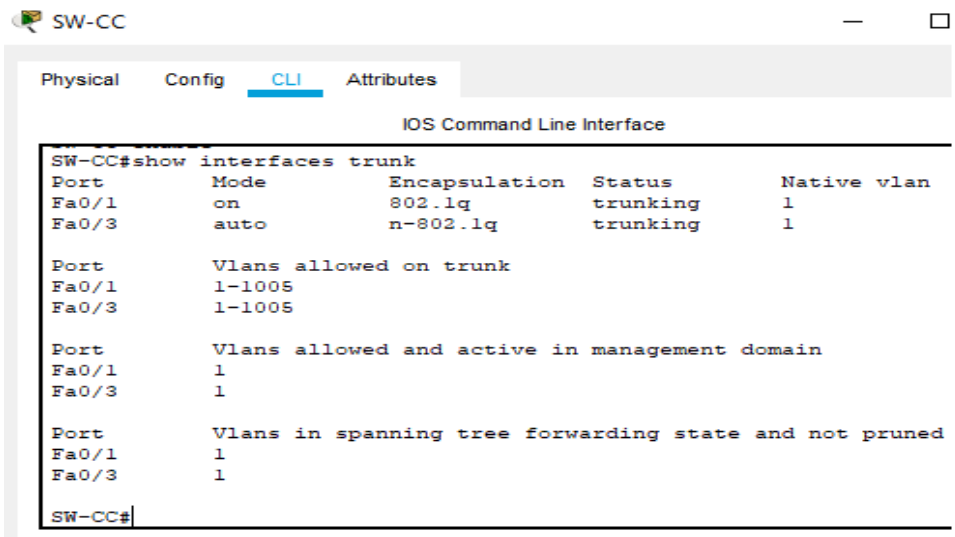


Figura 18. Enlace trunk permanente configurado en SW-CC

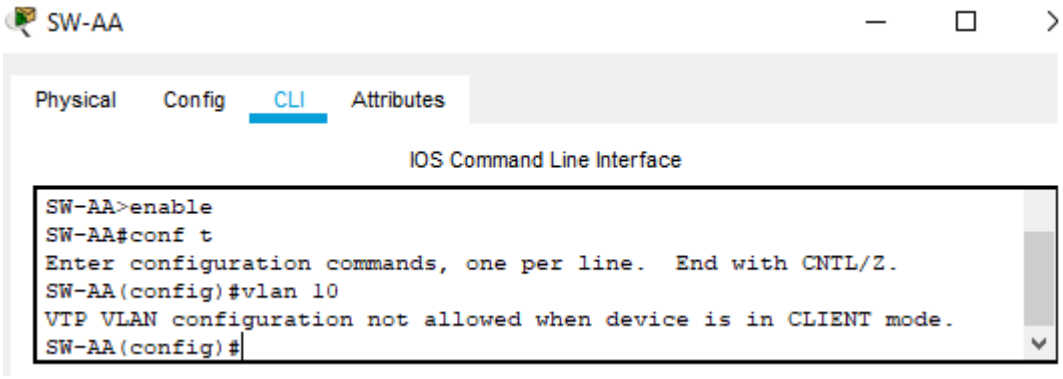


C. Agregar VLANs y asignar puertos.

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

```
SW-AA#configure terminal
SW-AA(config)#vlan 10
```

Figura 19. VLAN 10 en SW-AA




```
SW-BB#configure terminal
SW-BB(config)#vlan 10
SW-BB(config-vlan)#name Compras
SW-BB(config-vlan)#vlan 25
SW-BB(config-vlan)#name Personal
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
```

10. Verifique que las VLANs han sido agregadas correctamente.

Figura 20. Verificación de las VLANS agregadas en SW-AA

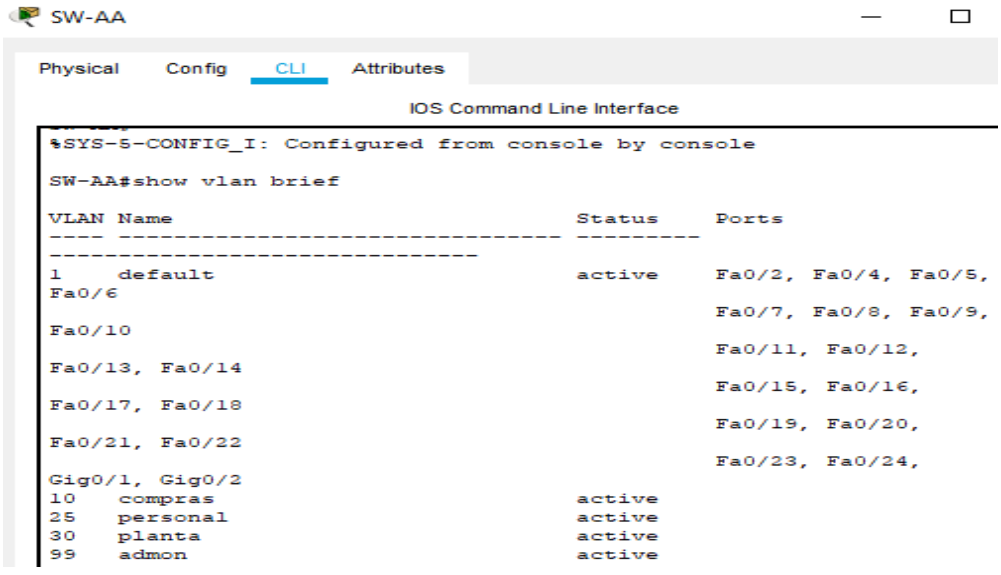


Figura 21. Verificación de las VLANS agregadas en SW-BB

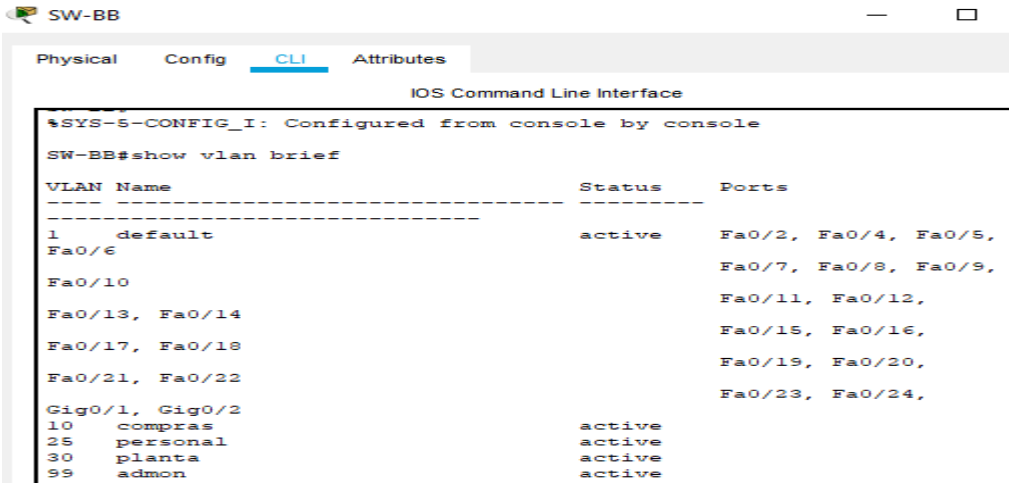
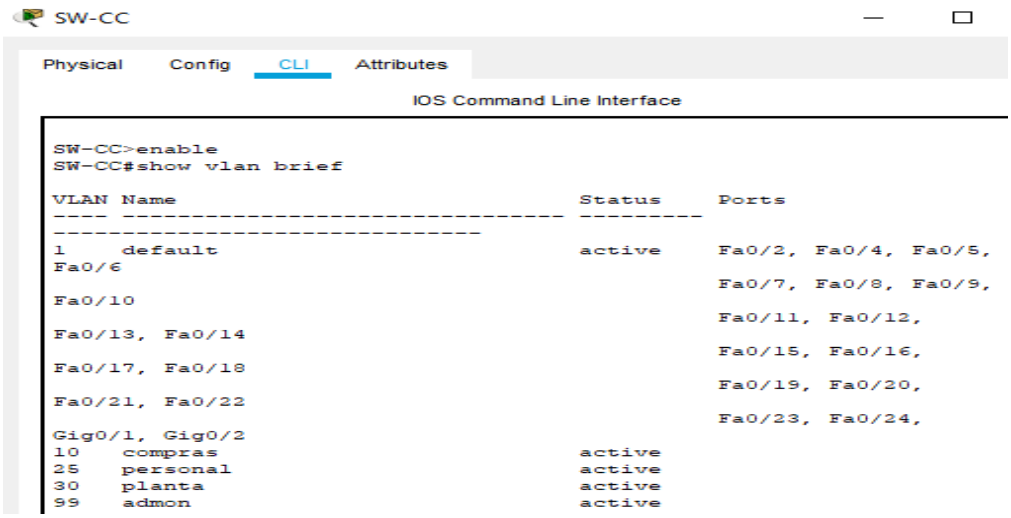


Figura 22. Verificación de las VLANS agregadas en SW-CC



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

Tabla 2. Puertos, VLAN y direcciones de los PCs

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

X = número de cada PC particular

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

13. 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 vlan 10
SW-AA config-if)#ip address 190.108.10.1 255.255.255.0
SW-AA(config-if)#exit
SW-AA(config)#interface vlan 25
SW-AA(config-if)#ip address 190.108.20.2 255.255.255.0
SW-AA(config-if)#exit
SW-AA(config)#interface vlan 30
SW-AA(config-if)#ip address 190.108.30.3 255.255.255.0
SW-AA(config-if)#exit

SW-BB#configure terminal
SW-BB(config)#interface vlan 10
SW-BB config-if)#ip address 190.108.10.4 255.255.255.0
SW-BB(config-if)#exit
SW-BB(config)#interface vlan 25
SW-BB(config-if)#ip address 190.108.20.5 255.255.255.0
SW-BB(config-if)#exit
SW-BB(config)#interface vlan 30
SW-BB(config-if)#ip address 190.108.30.6 255.255.255.0
SW-BB(config-if)#exit

SW-CC#configure terminal
SW-CC(config)#interface vlan 10
SW-CC config-if)#ip address 190.108.10.7 255.255.255.0
SW-CC(config-if)#exit
SW-CC(config)#interface vlan 25
SW-CC(config-if)#ip address 190.108.20.8 255.255.255.0
SW-CC(config-if)#exit
SW-CC(config)#interface vlan 30
SW-CC(config-if)#ip address 190.108.30.9 255.255.255.0
SW-CC(config-if)#exit
```

Tabla 3. Ubicación de los PCs en las Vlans y switches

Switch / Vlan	VLAN 10	VLAN 25	VLAN 30
SW - AA	190.108.10.1	190.108.20.2	190.108.30.3
SW - BB	190.108.10.4	190.108.20.5	190.108.30.6
SW - CC	190.108.10.7	190.108.20.8	190.108.30.9

```
PC1: ip 190.108.10.1 255.255.255.0
PC2: ip 190.108.20.2 255.255.255.0
PC3: ip 190.108.30.3 255.255.255.0
PC4: ip 190.108.10.4 255.255.255.0
PC5: ip 190.108.20.5 255.255.255.0
PC6: ip 190.108.30.6 255.255.255.0
PC7: ip 190.108.10.7 255.255.255.0
PC8: ip 190.108.20.8 255.255.255.0
PC9: ip 190.108.30.9 255.255.255.0
```

D. Configurar las direcciones IP en los Switches.

14. 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.

Tabla 4. Direcciones IP para los Switches

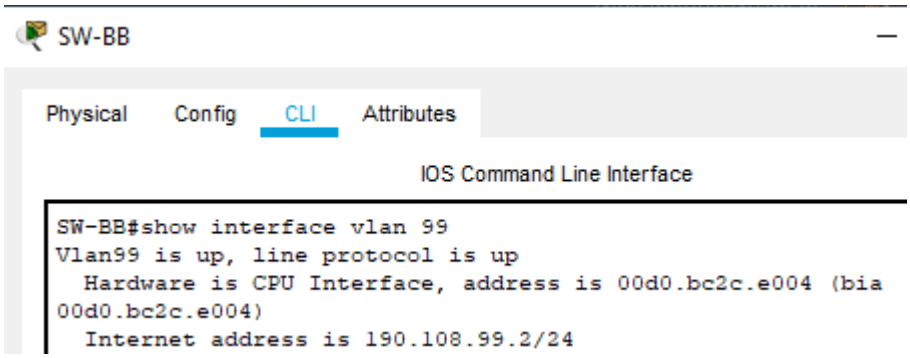
Equipo	Interfaz	Dirección IP	Máscara
SW-AA	VLAN 99	190.108.99.1	255.255.255.0
SW-BB	VLAN 99	190.108.99.2	255.255.255.0
SW-CC	VLAN 99	190.108.99.3	255.255.255.0

```
SW-AA#configure terminal
SW-AA(config)#interface vlan 99
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
```

Figura 23. Dirección IP configurada en SW-AA

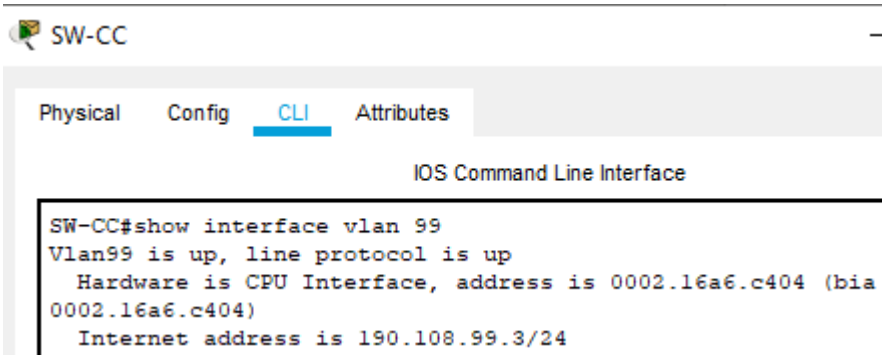

```
SW-BB#configure terminal
SW-BB(config)#interface vlan 99
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
```

Figura 24. Dirección IP configurada en SW-BB




```
SW-CC#configure terminal
SW-CC(config)#interface vlan 99
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0
```

Figura 25. Dirección IP configurada en SW-CC



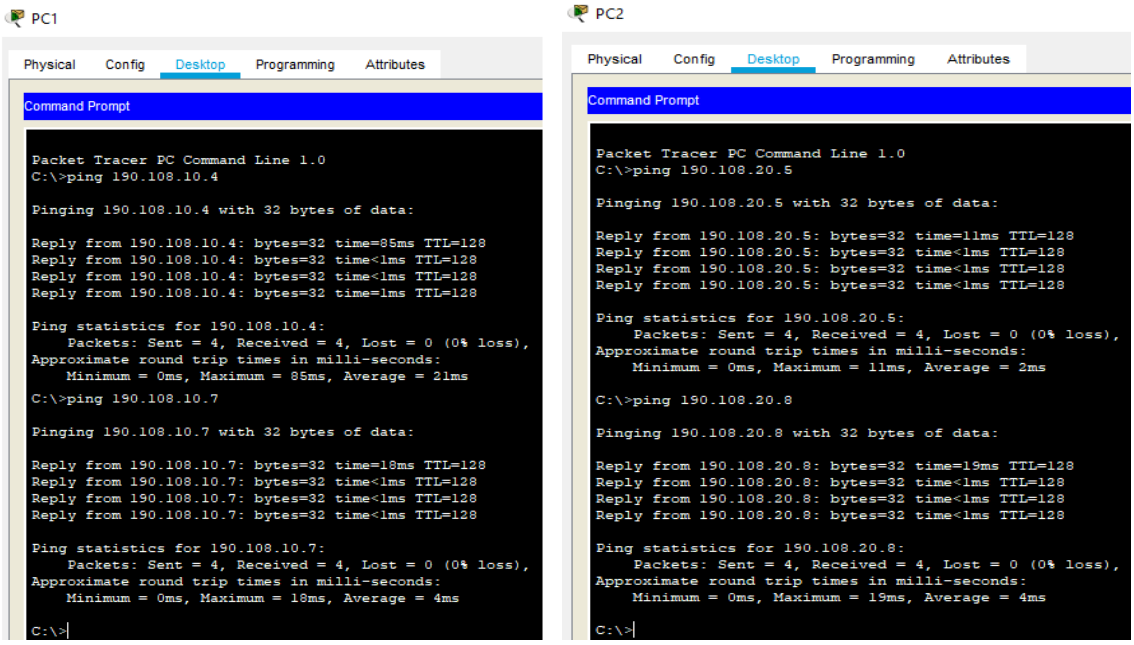
E. Verificar la conectividad Extremo a Extremo

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

Ping entre los Pcs de la Vlan 10 (compras), Ping entre los Pcs de la Vlan 25 (personal)

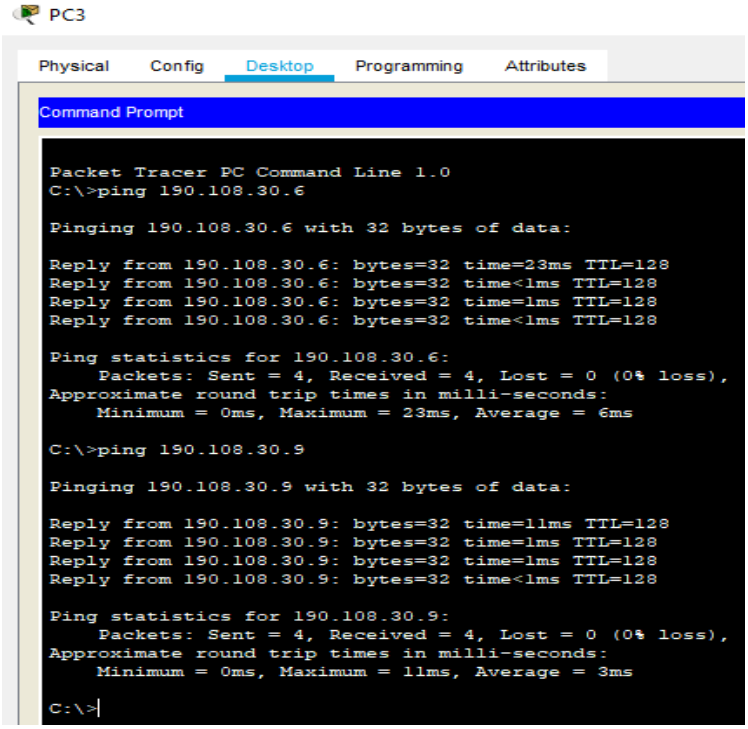
Se observó que los pings realizados entre los PCs pertenecientes a la misma VLAN fueron exitosos, mientras que los pings entre los equipos de diferentes VLANs no se completaron. Esto se debe a cada PC está ligado a una sección de red diferente. Una opción para poder comunicar estas hosts puede ser mediante el empleo de switches capa 3.

Figura 26. Ping exitoso entre los PCs de las VLANS 10 y 25



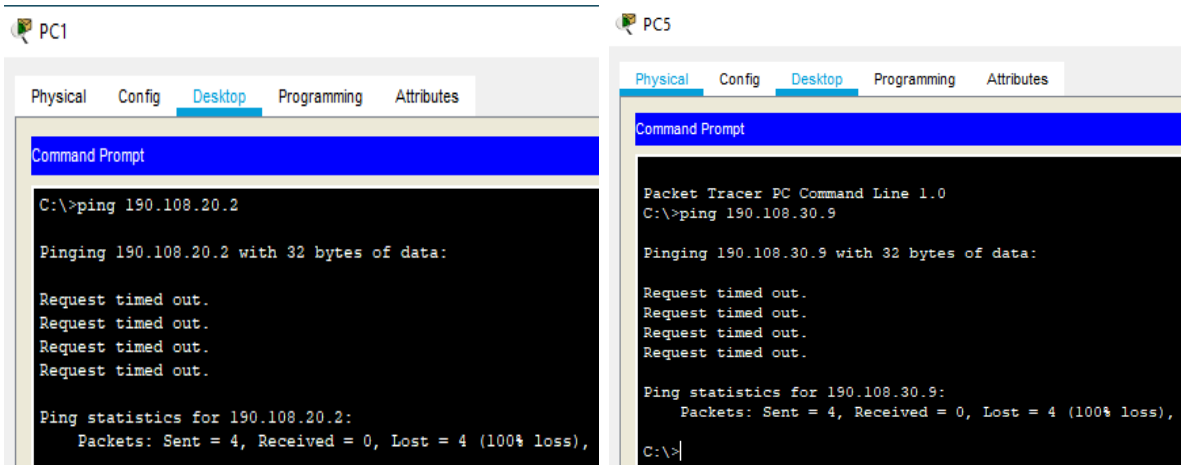
Ping entre los Pcs de la Vlan 30 (planta)

Figura 27. Ping exitoso entre los PCs de la VLAN 30



Ping entre PCs de vlans diferentes. PC1 a PC 2, PC5 a PC9.

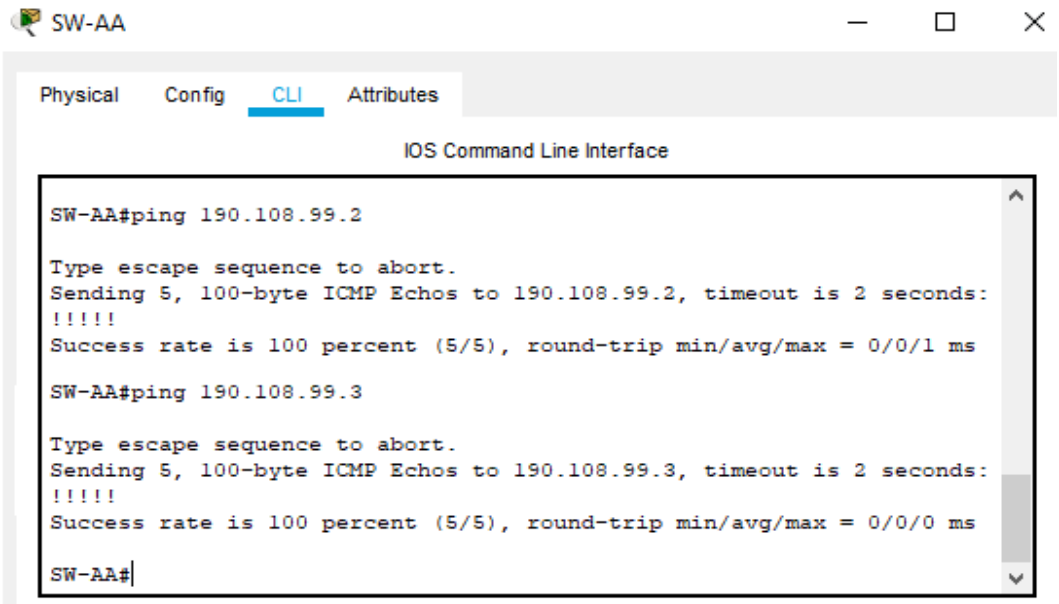
Figura 28. Ping entre PCs de VLANS distintas



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

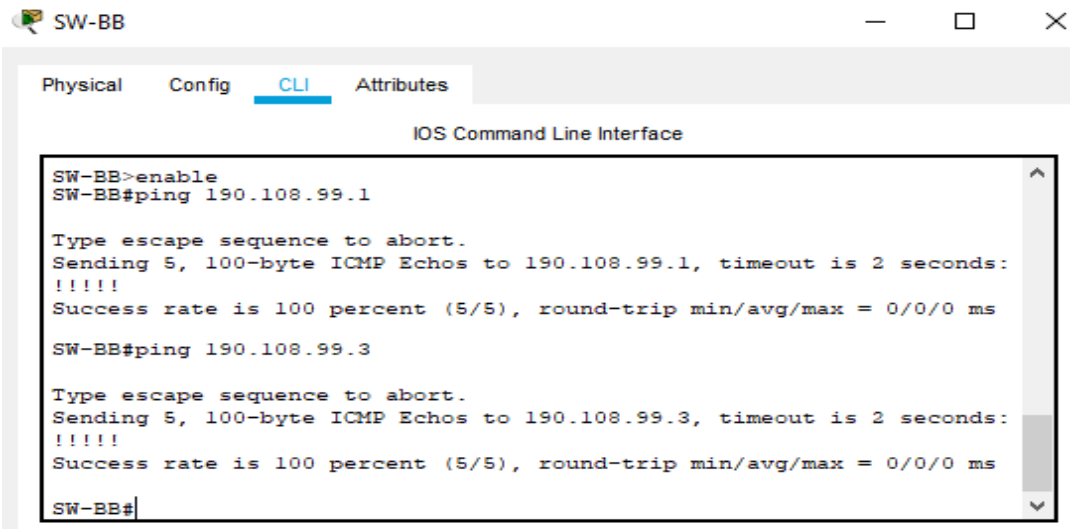
Ping de SW-AA a SW-BB y SW-CC

Figura 29. Ping desde SW-AA hacia los otros switches



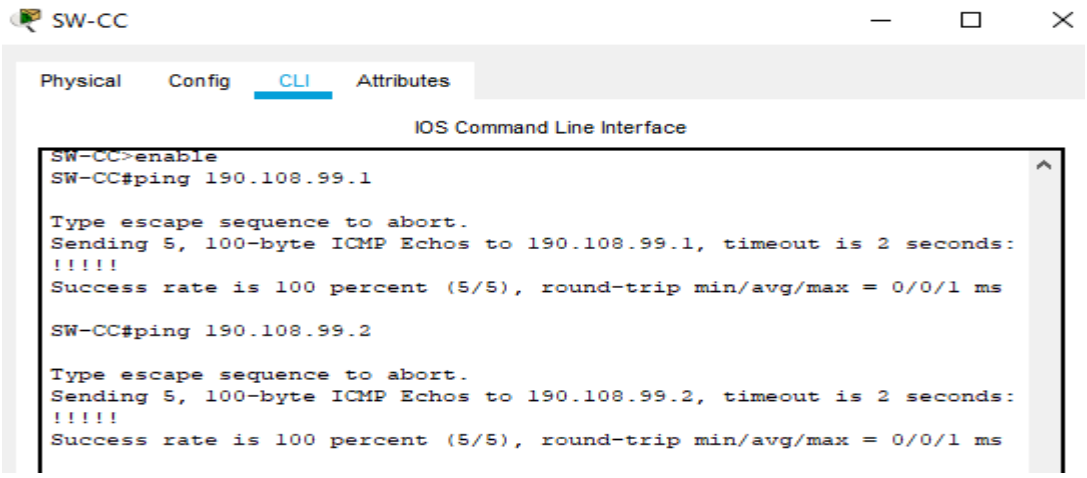
Ping de SW-BB a SW-AA y SW-CC

Figura 30. Ping desde SW-BB hacia los otros switches



Ping de SW-CC a SW-AA y SW-BB

Figura 31. Ping desde SW-CC hacia los otros switches

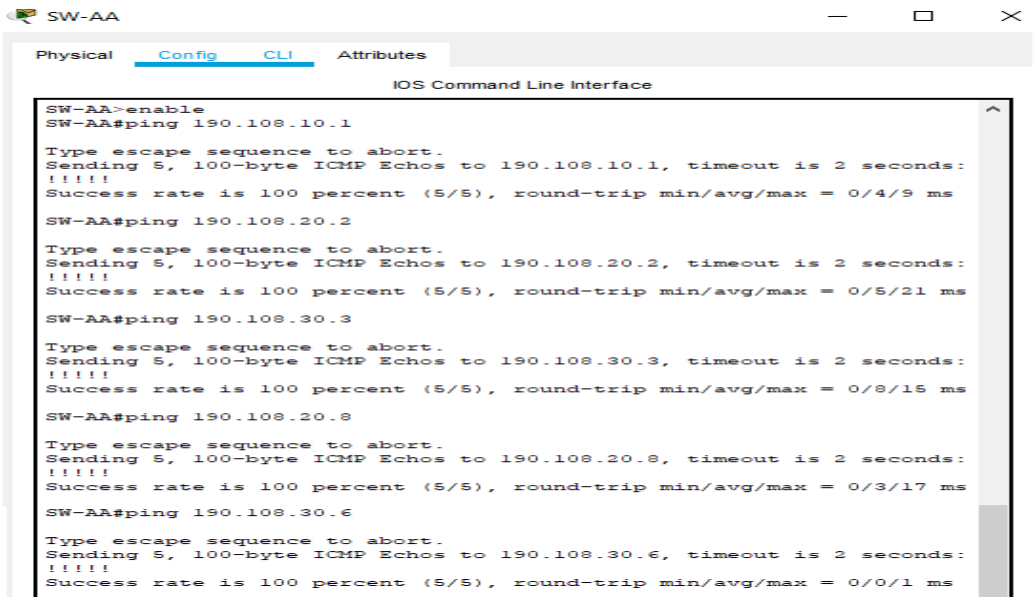


Entre los switches el ping realizado fue satisfactorio, esto debido a que la configuración de ruteo de información se hace por medio del protocolo ICMP, el cual se encuentra establecido en modo troncal.

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

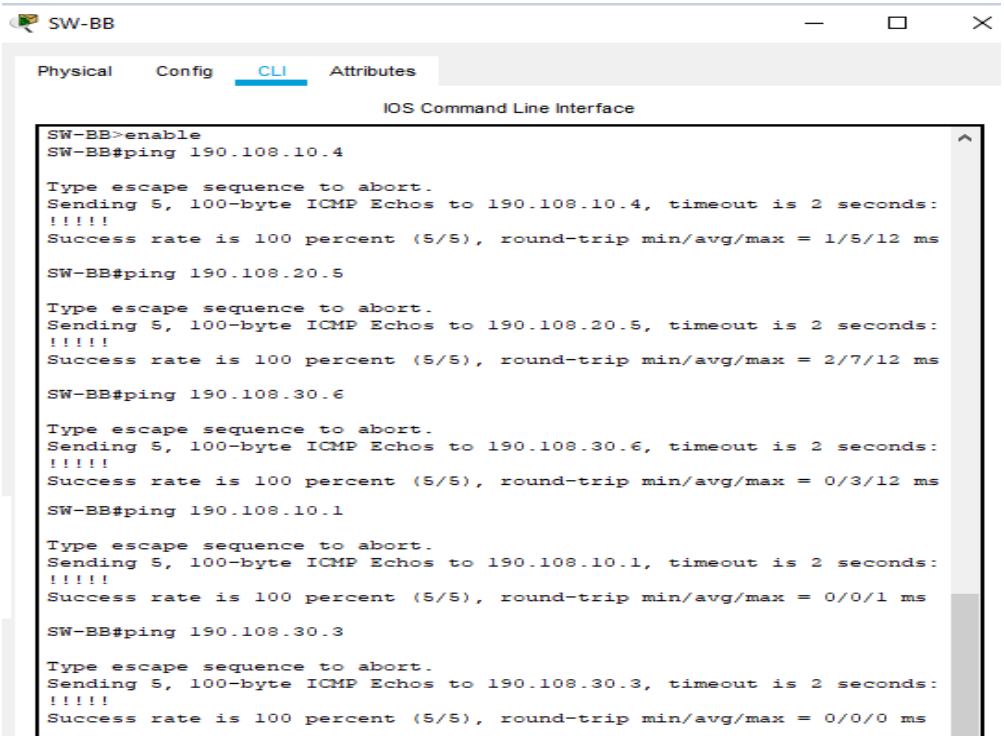
Ping desde switch SW-AA a cada PC

Figura 32. Ping desde switch SW-AA a cada PC



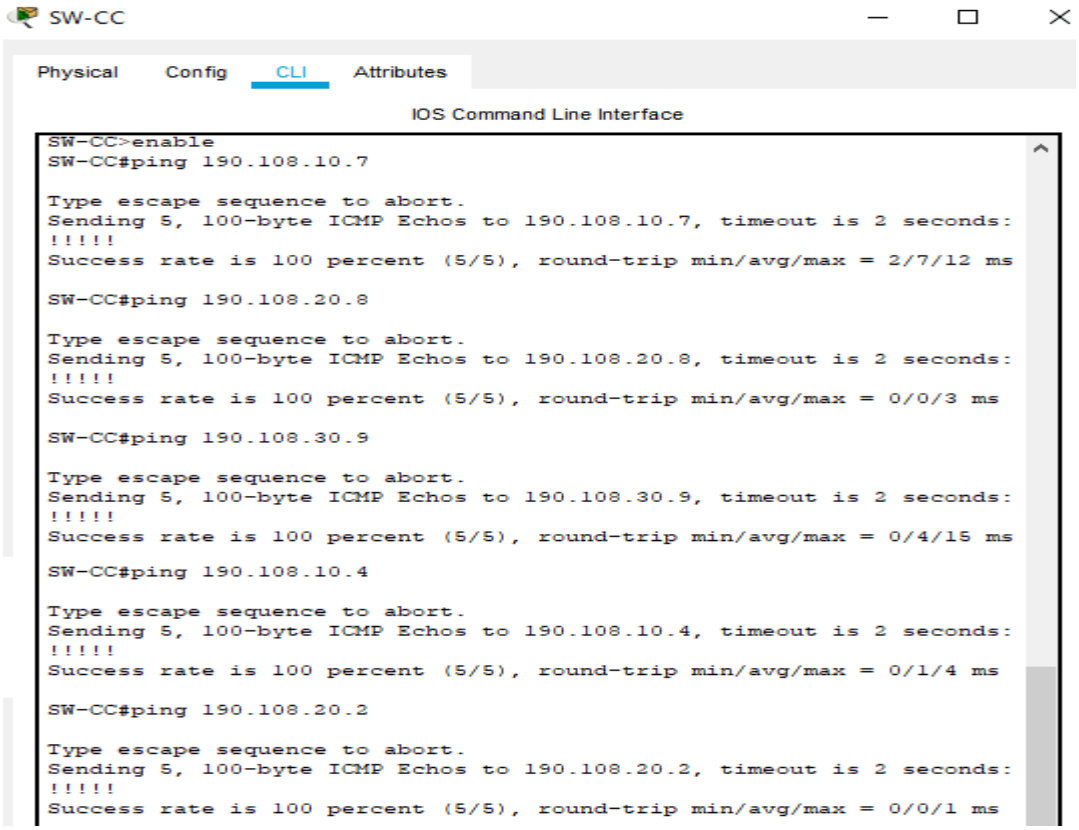
Ping desde switch SW-BB a cada PC

Figura 33. Ping desde switch SW-BB a cada PC



Ping desde switch SW-CC a cada PC

Figura 34. Ping desde switch SW-CC a cada PC



Se observa como los ping son exitosos tanto con los PCs conectados directamente a cada switch, como con los conectados a los otros switches. Esto fue posible gracias a la correcta configuración de las direcciones IP y máscaras de subred en las respectivas interfaces VLAN.

CONCLUSIONES

Se implementaron correctamente relaciones de vecinos BGP entre sistemas autónomos, estableciendo direcciones Loopback y determinando los comandos necesarios para establecer correctamente la configuración de cada uno de los enrutadores, de acuerdo con interfaces y direccionamiento IP establecido. Fueron fortalecidos además, conocimientos relacionados con el manejo y establecimiento de redes VLANs, protocolos VTP y activación de enlaces troncales.

Se demostraron así las competencias adquiridas en el diplomado CCNP de Cisco, mediante el análisis y configuración de dispositivos de Networking en escenarios de red establecidos, y mediante el manejo de software especializado en la simulación de estos entornos como es GNS3 y Packet Tracer.

Definitivamente, se puede decir que se desarrollaron competencias y habilidades necesarias en la implementación y solución de requerimientos de redes en entornos empresariales. Se puede decir también que el diplomado de profundización CCNP constituyó un medio mediante el cual se adquirieron y mejoraron las capacidades para el manejo profesional de protocolos de routing y switching.

BIBLIOGRAFIA

Donohue, D. (2017). CISCO Press (Ed). CCNP Quick Reference. Recuperado de https://1drv.ms/b/s!AgIGg5JUgUBthFt77ehzL5qp0OKD

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Fundamentals Review. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH. Recuperado de https://1drv.ms/b/s!AmIJYeiNT1IlnWR0hoMxgBNv1CJ

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE. Recuperado de https://1drv.ms/b/s!AmIJYeiNT1IlnMfy2rhPZHwEoWx

Wallace, K. (2015). CISCO Press (Ed). CCNP Routing and Switching ROUTE Official Cert Guide. Recuperado de https://1drv.ms/b/s!AgIGg5JUgUBthFx8WOxiq6LPJppl