DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JUAN FERNANDO CASTRO RODRIGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA TELECOMUNICACIONES
CHIA, CUNDINAMARCA
2020

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JUAN FERNANDO CASTRO RODRIGUEZ

Diplomado de opción de grado presentado para optar el
título de INGENIERO EN TELECOMUNICACIONES

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA TELECOMUNICACIONES
CHIA, CUNDINAMARCA
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

CHIA (CUNDINAMARCA), 22 de mayo de 2020

AGRADECIMIENTOS

Con este trabajo de grado quiero agradecer primeramente a **DIOS**, gracias a su voluntad pude llegar a este termino de mis estudios.

En segundo lugar, a mi esposa y mis hijos que son mi motor principal los que me motivan, mi esposa **Angelica Maria Fonseca** por su amor, su apoyo incondicional, su paciencia en este tiempo, cuando en algún momento pensé desfallecer , a mis dos hijos **Juan Sebastian y Andres Felipe** que ven en mi un ejemplo a seguir, ya escuchar de ellos decir yo quiero ser como mi papá un profesional, a mi madre **Maria Florinda Rodriguez** una mujer luchadora incansable que forjo en mi valores de responsabilidad, dedicación y que un día me dijo LO QUE SE INICIA SE TERMINA, y es así estoy terminando otro ciclo de mi vida que es llegando a obtener mi título profesional como Ingeniero en telecomunicaciones con mucho esfuerzo ya que no es fácil trabajar y estudiar, les agradezco por entenderme y en algunos momentos no compartir con ustedes tiempo ya que estaba realizando mis responsabilidades académicas.

A la universidad Nacional abierta y a distancia Unad la cual gracias a sus programas de educación a distancia me dieron esta gran oportunidad que de otra manera no habido sido posible ya que presencialmente no hubiese terminado.

Y por último a mis jefes y compañeros de trabajo de la CENCOSUD por su apoyo cuando necesitaba salir a una clase presencial.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

CCNP: Las siglas CCNP significan Cisco Certified Network Professional, es una certificación otorgada por la empresa Cisco Systems, esta certificación requiere mayor esfuerzo y conocimientos previos que el CCNA. Y nos indica que su titular posee conocimientos avanzados sobre redes que le permiten instalar, configurar y manejar redes LAN, WAN y servicios de acceso para organizaciones de 500 ordenadores aproximadamente.

Switch: un switch es un dispositivo de interconexión de redes informáticas. En informática de redes, un switch es el dispositivo analógico que permite la interconexión de redes operativas en la capa 2 o de nivel de enlace de datos según el modelo OSI.

Router: el router o enrutador es un dispositivo que opera en capa tres de nivel de 3. Así, permite que varias redes u ordenadores se conecten entre sí y, por ejemplo, compartan una misma conexión de Internet.

Ethernet: es una tecnología que conecta redes de área local (LAN) cableadas y permite que el dispositivo se comunique entre sí a través de un protocolo que es el lenguaje de red común. Esta LAN es una red de computadoras y otros dispositivos electrónicos que cubre un área pequeña en sus lugares como en la oficina, casa, habitación o edificio.

Firewall: Combinación de hardware y software la cual separa una red de área local (LAN)en dos o más partes con propósitos de seguridad. Su objetivo básico es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autentificación, etc.

RESUMEN

En la realización de este trabajo se describe los pasos correspondientes de Networking para la configuración de dos escenarios, mediante el protocolo de enrutamiento BGP y VTP los cuales corresponden a la prueba de habilidades del Diplomado de profundización Cisco CCNP ROUTE y CCNA SWITCH. El desarrollo tanto práctico como teórico nos permite entender los diferentes temas por medio de los escenarios propuesto durante el proceso de habilidades en el área de redes telecomunicaciones en el cual nos permita poseer una base práctica para el mejoramiento del pensamiento lógico y la capacidad de análisis.

Palabras claves: Cisco, CCNP, Redes, Enrutamiento

ABSTRACT

In carrying out this work, the corresponding Networking steps are described for the configuration of two scenarios, using the BGP and VTP routing protocol, which correspond to the skills test of the Cisco CCNP ROUTE and CCNA SWITCH deepening Diploma. Both practical and theoretical development allows us to understand the different topics through the scenarios proposed during the skills process in the area of telecommunications networks, which allows us to have a practical basis for improving logical thinking and analytical skills.

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

INTRODUCCIÓN

El programa de estudios Cisco CCNP está diseñado para alumnos que desean adquirir habilidades de gestión de redes orientadas hacia el mundo profesional y de nivel empresarial. CCNP ayuda a los alumnos a desarrollar las habilidades necesarias para complementar con éxito títulos universitarios relacionados con las TIC y para prepararse para la certificación Cisco CCNP. Ofrece una experiencia de aprendizaje con una gran carga tanto teórica como práctica que abarca habilidades avanzadas de Routing, Switching y resolución de problemas.

En el presente documento se desarrolla la prueba de habilidades Practicas, la cual hace parte de las actividades evaluativas del Diplomado de Profundización CCNP, con la realización de este trabajo busca identificar el grado de competencia y habilidad que se ha logrado adquirir a lo largo del diplomado, esto se realiza mediante 2 escenarios propuestos donde se realizan las respectivas configuraciones para dar solución a la conectividad planteada.

Para cumplir con el propósito mencionado se abordan temáticas como el enrutamiento a través del protocolo BGP y proceso de creación de adyacentes en función del protocolo IPV4 de Router ID e interfaces Loopback, también la configuración de una pequeña red basada en switches capa 2 y Pcs, donde se configura por enrutamiento IPv4 respectivo, se implementa protocolo VTP para las Vlans. A continuación, se encuentra el desarrollo paso a paso de la configuración de cada uno de los dispositivos de cada escenario con las especificaciones planteadas en la prueba de habilidades con sus respectivas validaciones tomadas de los simuladores de GNS3 y Packet Tracer.

DESARROLLO

Escenario 1

Figura 1: Topología escenario

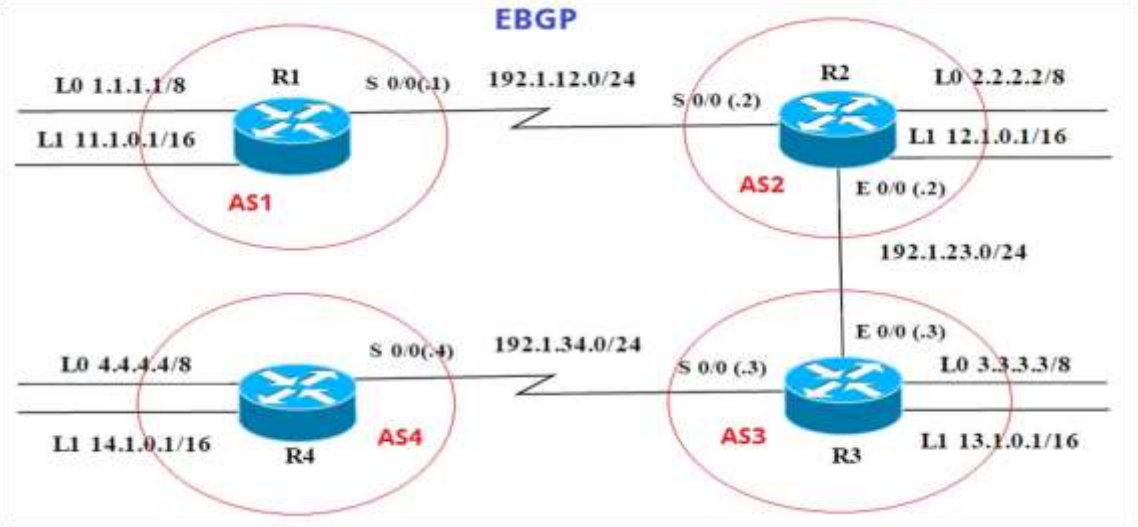
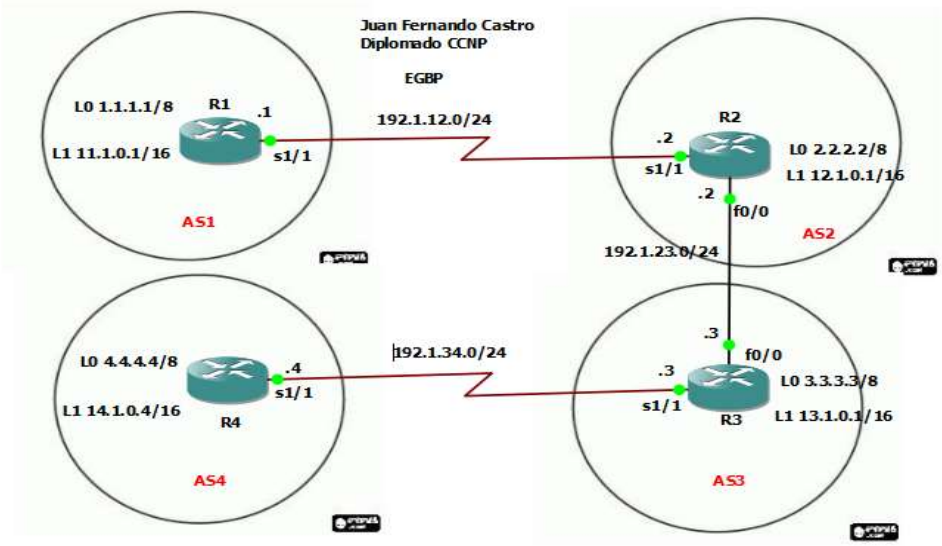


Figura 2: Topología escenario en gns3



Información para la configuración de los Routers

Tabla 1 Enrutamiento Router 1

R1

Interfaz	Dirección IP	Máscara
Loopback 0	1.1.1.1	255.0.0.0
Loopback 1	11.1.0.1	255.255.0.0
S 0/0	192.1.12.1	255.255.255.0

Tabla 2 Enrutamiento Router 2

R2

Interfaz	Dirección IP	Máscara
Loopback 0	2.2.2.2	255.0.0.0
Loopback 1	12.1.0.1	255.255.0.0
S 0/0	192.1.12.2	255.255.255.0
E 0/0	192.1.23.2	255.255.255.0

Tabla 3 enrutamiento Router 3

R3

Interfaz	Dirección IP	Máscara
Loopback 0	3.3.3.3	255.0.0.0
Loopback 1	13.1.0.1	255.255.0.0
E 0/0	192.1.23.3	255.255.255.0
S 0/0	192.1.34.3	255.255.255.0

Tabla 4 enrutamiento Router 4

R4

Interfaz	Dirección IP	Máscara
Loopback 0	4.4.4.4	255.0.0.0
Loopback 1	14.1.0.1	255.255.0.0
S 0/0	192.1.34.4	255.255.255.0

Configuración Router 1 y Router2

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.***

```
Router#configure terminal
R1(config)# interface Loopback 0
R1(config-if)# ip address 1.1.1.1 255.0.0.0
R1(config-if)# exit
R1(config)# interface Loopback 1
R1(config-if) # ip address 11.1.0.1 255.255.0.0
R1(config-if) # exit
R1(config)# interface Serial 1/1
R1(config-if)# description AS1 -> AS2
R1(config-if)# ip address 192.1.12.1 255.255.255.0
R1(config-if) # clock rate 128000
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) # exit
R2(config)# interface Loopback 1
R2(config-if) # ip address 12.1.0.1 255.255.0.0
R2(config-if) # exit
R2(config)# interface Serial 1/1
R2(config-if)# description AS2 -> AS1
R2(config-if) # ip address 192.1.12.2 255.255.255.0
R2(config-if) # clock rate 128000
R2(config-if) # no shutdown
R2(config-if) # exit
```

```
R2(config)# interface fastethernet 0/0
R2(config-if)# description AS2 -> AS3
R2(config-if) # ip address 192.1.23.2 255.255.255.0
R2(config-if) # no shutdow
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
```

A continuación, se presenta el resultado obtenido del comando ***show ip route***, donde el router R1 y R2 contienen en su tabla de enrutamiento las direcciones Loopback y las direcciones de las redes a las cuales se encuentran conectados de forma directa, también vemos las redes configuradas en las interfaces Loopback de su respectivo router vecino.

Estas redes se pueden identificar mediante el código **B** que las precede, estas redes son aprendidas a través del protocolo BGP, otro dato que se evidencia en esta tabla de enrutamiento de cada router es donde reconoce como vía para alcanzar esta ruta es la red 192.1.12.0/24 conectada a travez de la interface serial 1/1, donde este es el enlace físico que conecta a estos dos router.

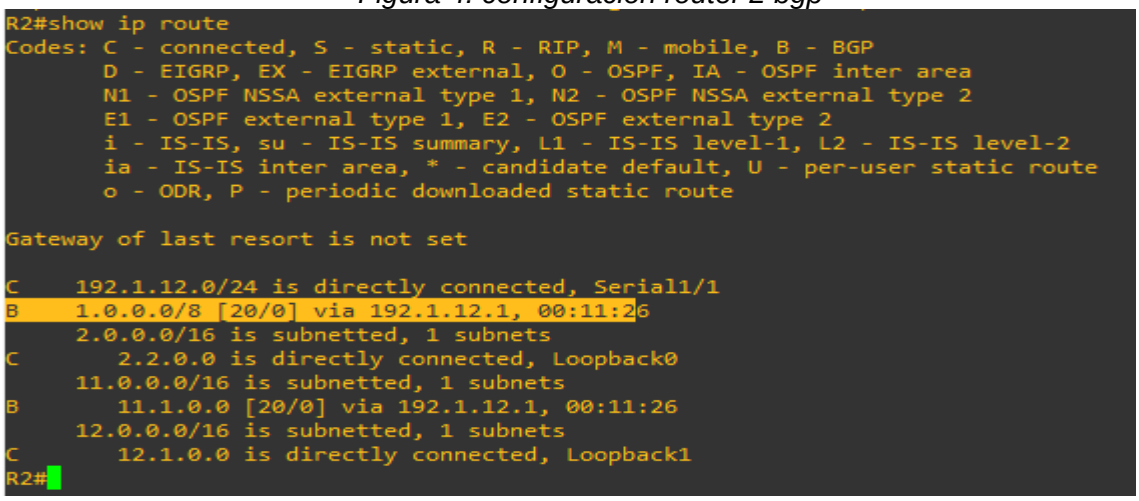
Figura 3: configuración router 1 bgp

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.1.12.0/24 is directly connected, Serial1/1
C    1.0.0.0/8 is directly connected, Loopback0
B    2.0.0.0/8 [20/0] via 192.1.12.2, 00:00:25
     11.0.0.0/16 is subnetted, 1 subnets
C       11.1.0.0 is directly connected, Loopback1
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.12.2, 00:00:25
R1#
```

Figura 4: configuración router 2 bgp



Configuración Router 2 a Router 3

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.***

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
R2(config-router)#exit
R2(config)#exit

R3# configure terminal
R3(config)# interface Loopback 0
R3(config-if) # ip address 3.3.3.3 255.0.0.0
R3(config-if) # exit
R3(config)# interface Loopback 1
R3(config-if) # ip address 13.1.0.1 255.255.0.0
R3(config-if) # exit
R3(config)# interface fastethernet 0/0
R3(config-if)# description AS3 -> AS2
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 Serial 1/1
R3(config-if)# description AS3 -> AS4

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

Realizada la configuración del R3 y la configuración de BGP en la R2 se puede evidenciar el resultado se obtiene con el comando Show ip route, donde el Router R2 se ha actualizado la tabla de enrutamiento y ahora vemos que tiene las direcciones de Loopback configuradas del router R3, por lo tanto, este dispositivo ha aprendido hasta este momento 4 rutas a través del protocolo BGP donde las cuales identifica se identifican con el código *B*.

El R3 contiene en su tabla de enrutamiento las redes que reconoce conectadas directamente, las interfaces Lookback y las redes que lo comunican con los routers R3 y R4 mediante las interfaces FasEthernet 0/0 y Serial 1/1 respectivamente, además este router (R3) se ha actualizado en su tabla de enrutamiento las direcciones de red correspondientes a las interfaces Lookback que se configuraron en R2 y R1, estas rutas las aprendió mediante el protocolo BGP estableciendo la relación adyacente con R2 y a que dichas redes se anunciaron en cada uno de los routers, en R3 también contiene la dirección de red que conecta los routers R1 y R2 la cual aprendió mediante el protocolo BGP con se evidencia en el código *B* el cual precede a la ip en la tabla de enrutamiento. Se evidencia que R3 tiene alcance a todas las redes a través de la interfaz FasEthernet 0/0.

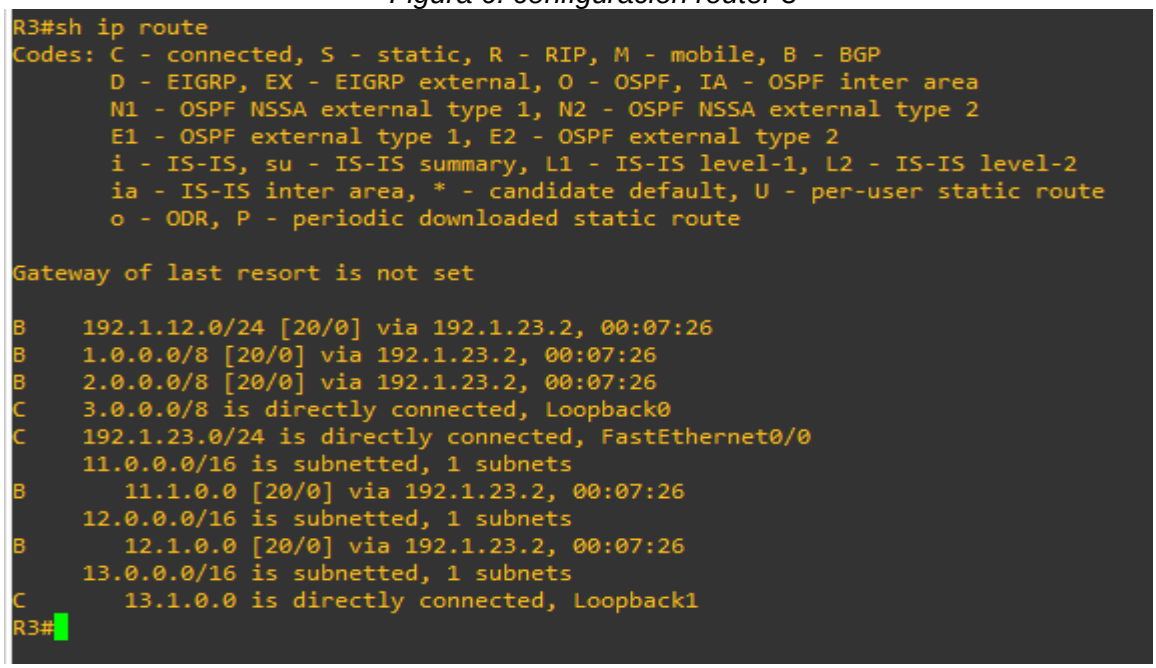
Figura 5: configuración router 2 bgp con rutas bgp router 3

```
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.1.12.0/24 is directly connected, Serial1/1
B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:14:37
C    2.0.0.0/8 is directly connected, Loopback0
B    3.0.0.0/8 [20/0] via 192.1.23.3, 00:02:09
C    192.1.23.0/24 is directly connected, FastEthernet0/0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.12.1, 00:14:37
     12.0.0.0/16 is subnetted, 1 subnets
C       12.1.0.0 is directly connected, Loopback1
     13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0 [20/0] via 192.1.23.3, 00:02:09
R2#
```

Figura 6: configuración router 3



Configuración Router 3 a Router 4

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*

```
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
R3(config-router) #exit
R3(config)#exit

R4#configure terminal
R4(config)# interface Loopback 0
R4(config-if) # ip address 4.4.4.4 255.0.0.0
R4(config-if) # exit
R4(config)# interface Loopback 1
R4(config-if) # ip address 14.1.0.1 255.255.0.0
R4(config-if) # exit
```

```
R4(config)# interface Serial 1/1
R4(config-if)# description AS4 -> AS3
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
R4(config-router) #exit
R4(config)#exit
```

Para establecer la relación de adyacentes utilizando las direcciones Loopback, del router vecino se necesita informar sobre el uso de cada una de estas interfaces en lugar de la interfaz física por tal razón se requiere una configuración adicional para establecer los vecinos esta configuración se realizar en R3 y R4.

```
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
R3(config-router) #exit
R3(config)#exit
```

```
R4#configure terminal
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 3
R4(config-router) # neighbor 3.3.3.3 update-source Loopback 0
R4(config-router) # neighbor 3.3.3.3 ebgp-multihop
R4(config-router) #exit
R4(config)#exit
```

Se presenta a continuación el resultado del comando *Show ip route*, donde el R3 ha actualizado su tabla de enrutamiento y la dirección de red que conecta este dispositivo con R4 ha cambiado tomando la dirección de Lookback 0, la cual

aparece como dirección estática, dado que así se estableció en la configuración que se realizó anteriormente, vemos que pese a que se usa la dirección lógica de la interface Loopback 0 para establecer la adyacencia, la vía de conexión física sigue siendo la red 192.1.4.0/24 correspondiente a la interfaz serial 1/1. También se puede identificar que la dirección de red de la interfaz Loopback 1 esta sigue aprendiendo mediante el protocolo BGP, pero no se alcanza mediante la interfaz Loopback 0 de R4 (4.4.4.4). en la tabla de enrutamiento los demás vecinos no sufrieron cambios, continúan los mismos vecinos.

La tabla de enrutamiento del router R4 se puede evidenciar que la dirección por la cual se comunica con sus vecinos BGP ha cambiado y ahora corresponde a la dirección de la interfaz Loopback 0 de R3.

Figura 7: configuración router 3 bgp con rutas hacia router 4

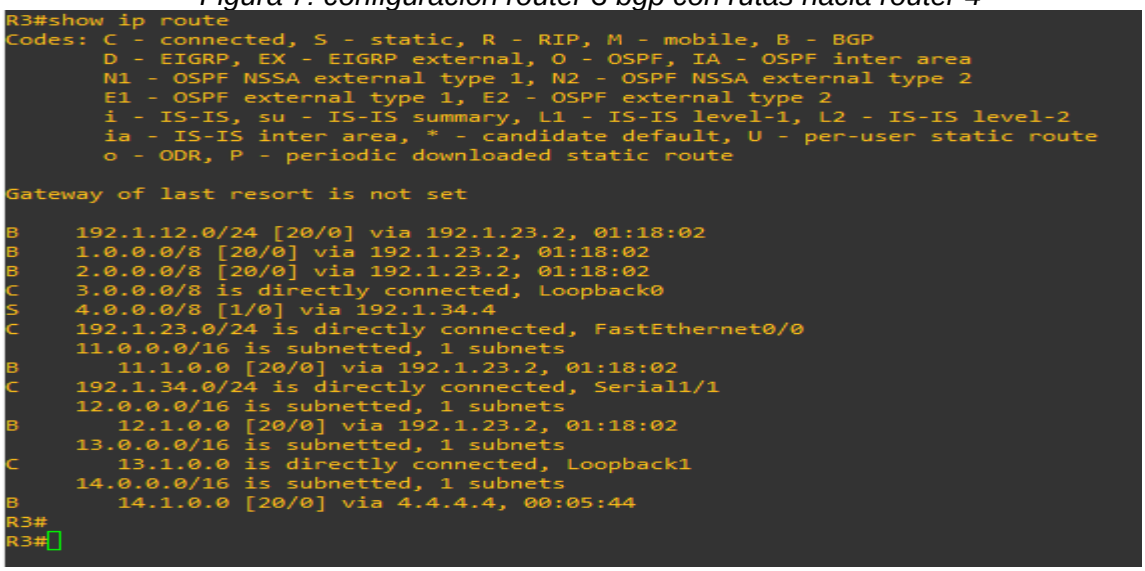
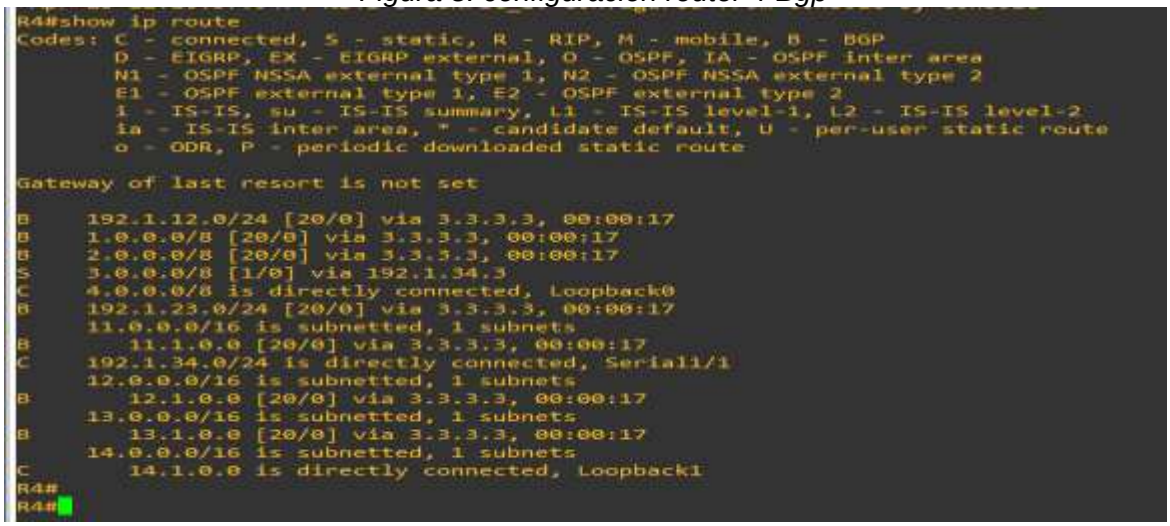


Figura 8: configuración router 4 Bgp



Escenario 2

Figura 9: Escenario 2

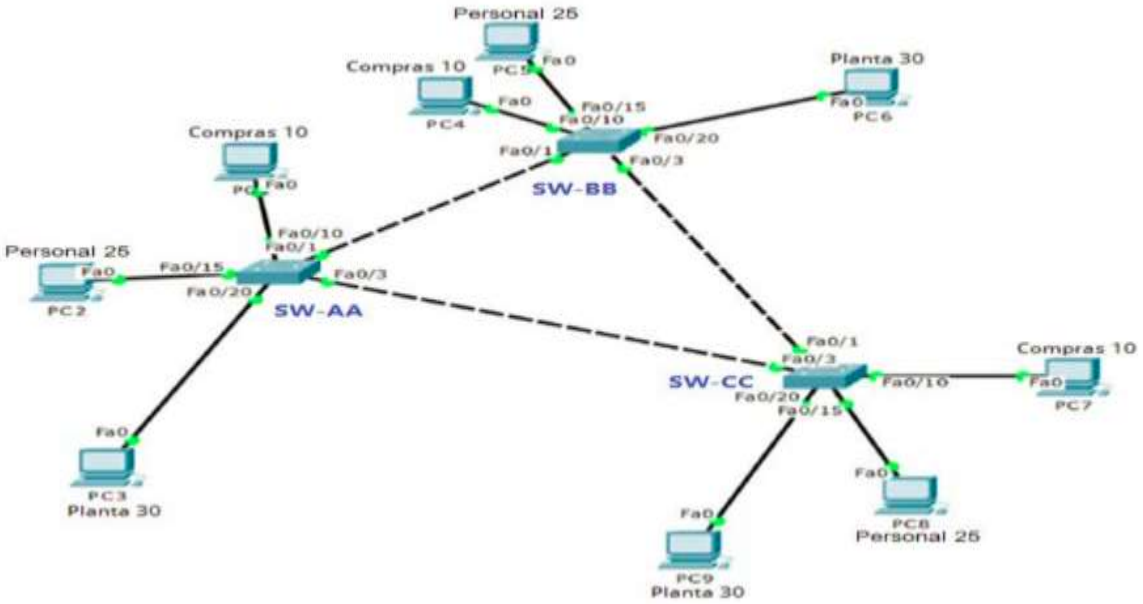
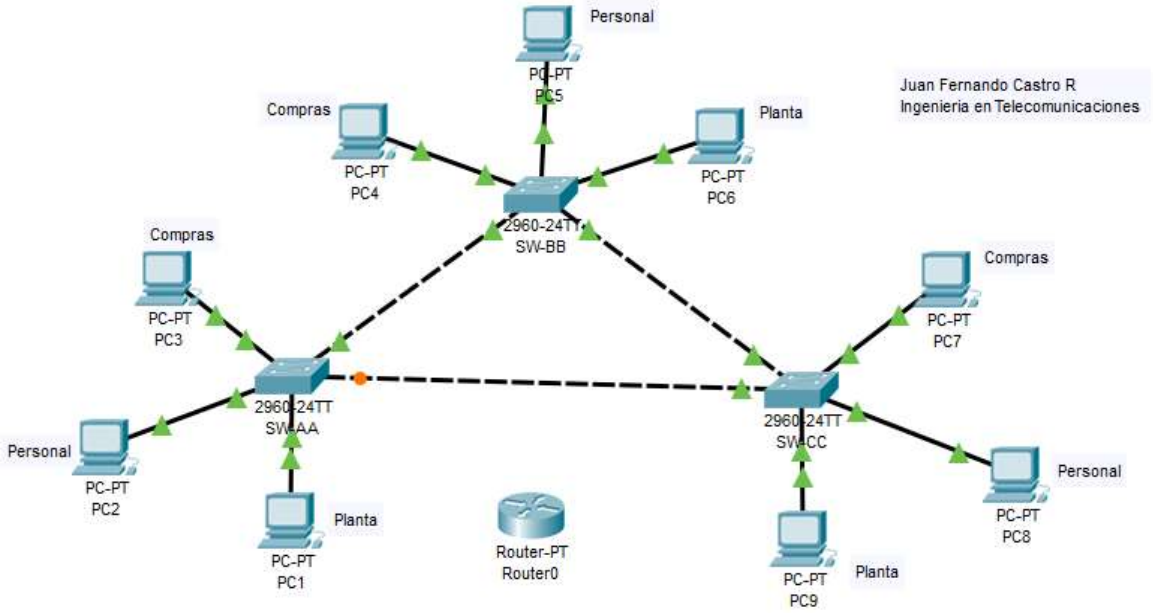


Figura 9: Topología Packet Tracer



Configuración 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#configure 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 Password cisco
Setting device VLAN database password to cisco
```

```
SW-BB> Enable
SW-BB#configure terminal
SW-BB(config)# vtp mode server
Setting device to VTP SERVER mode.
SW-BB(config)# vtp domain CCNP
Changing VTP domain name from NULL to CCNP
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 Password cisco
Setting device VLAN database password to cisco
```

2. Verificar las configuraciones mediante el comando *Show vtp status*

Figura 10: show vpt status switch SW-AA

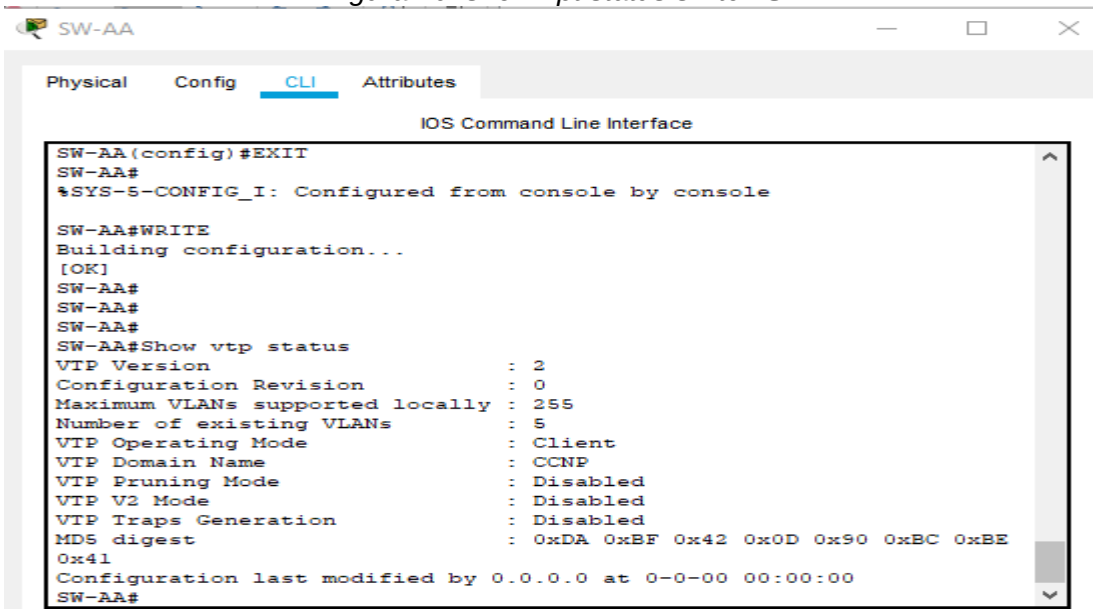


Figura 11: show vpt status switch SW-BB

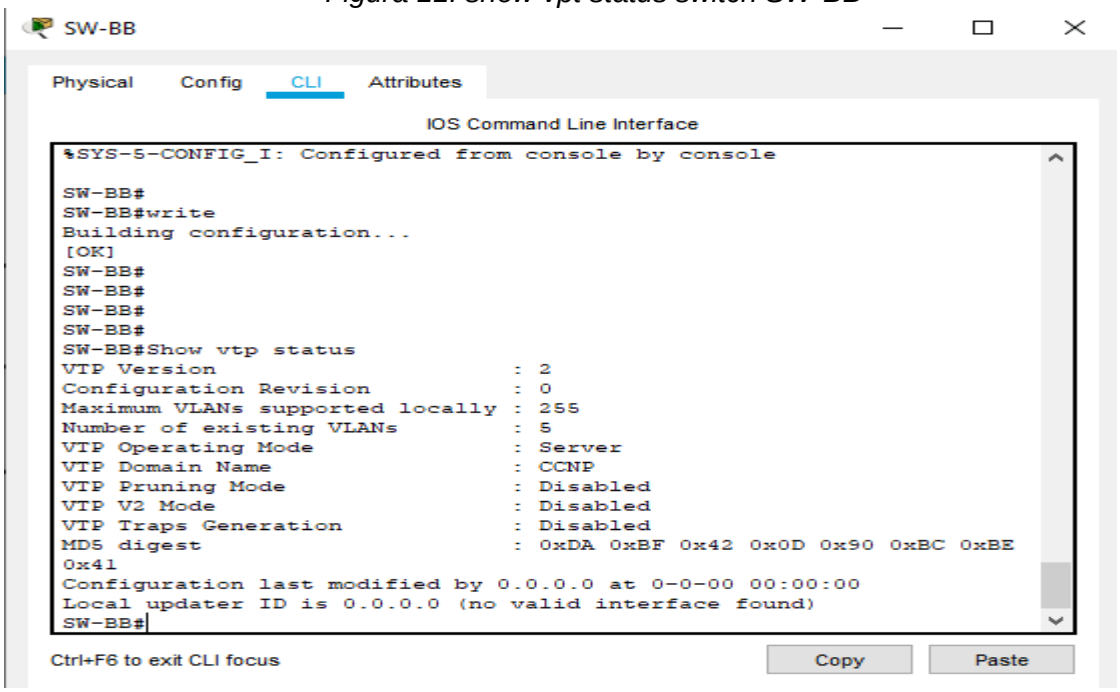
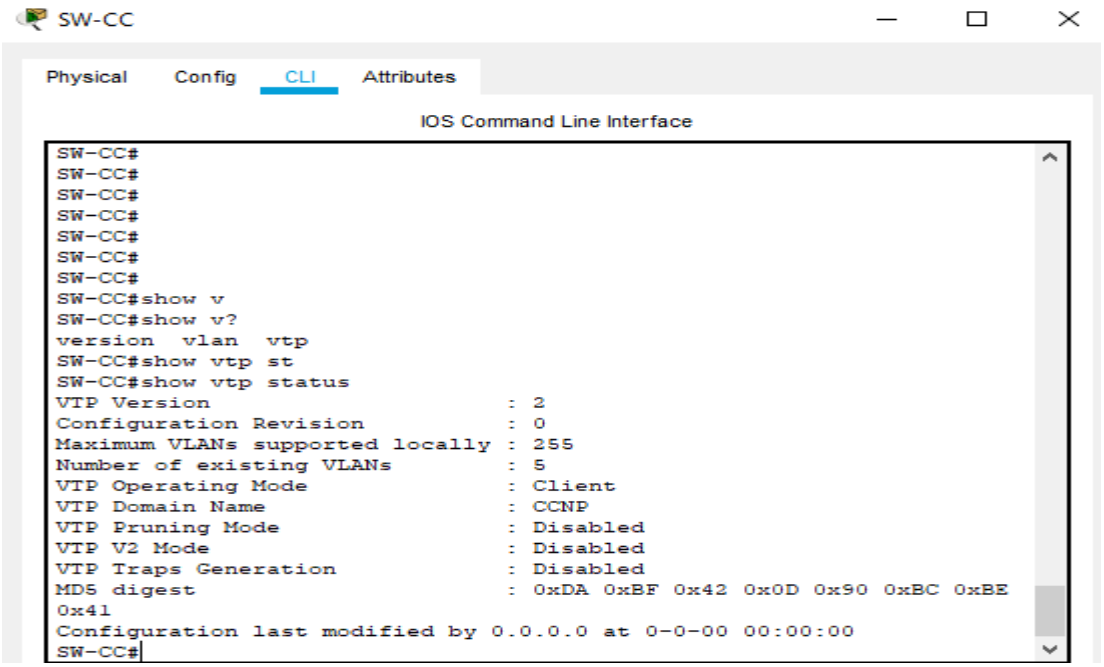


Figura 12: show vpt status switch SW-CC



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-BB> Enable
SW-BB#configure terminal
SW-BB(config)# interface fastEthernet 0/1
SW-BB(config-if)# switchport mode dynamic desirable
```

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

Figura 13: show interface trunk F0/1 SW-AA

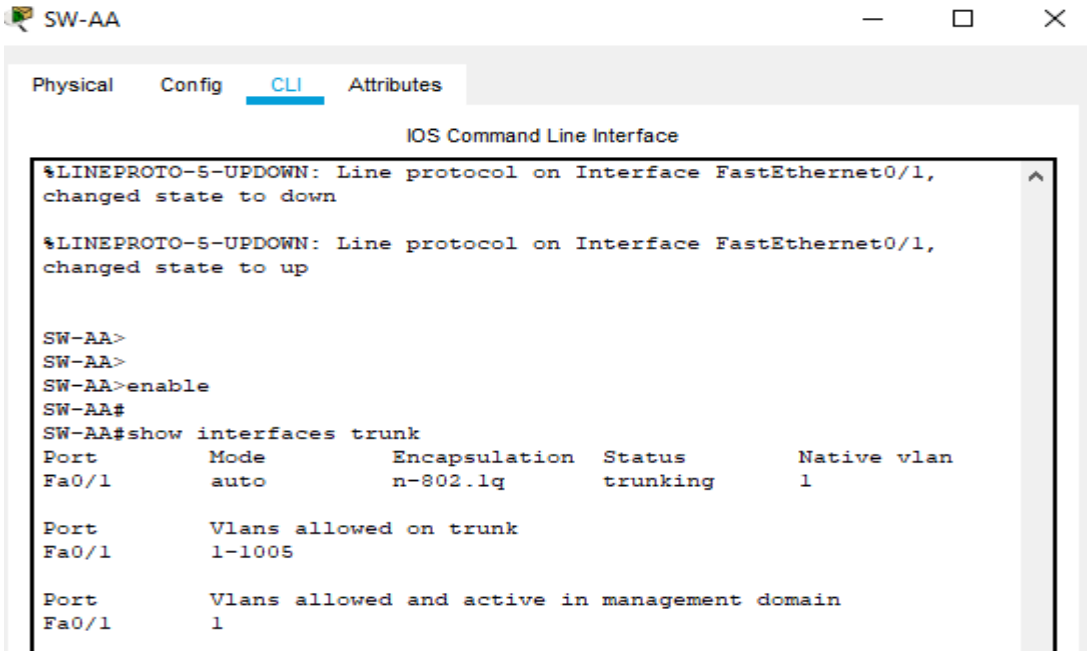
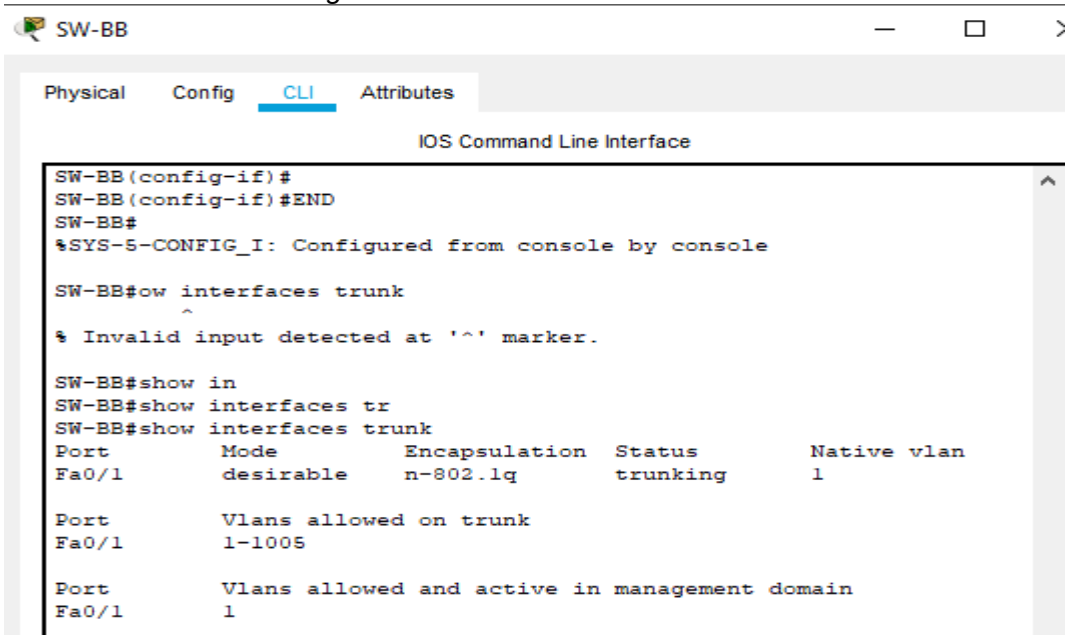


Figura 14: show interface trunk F 0/1 SW-BB

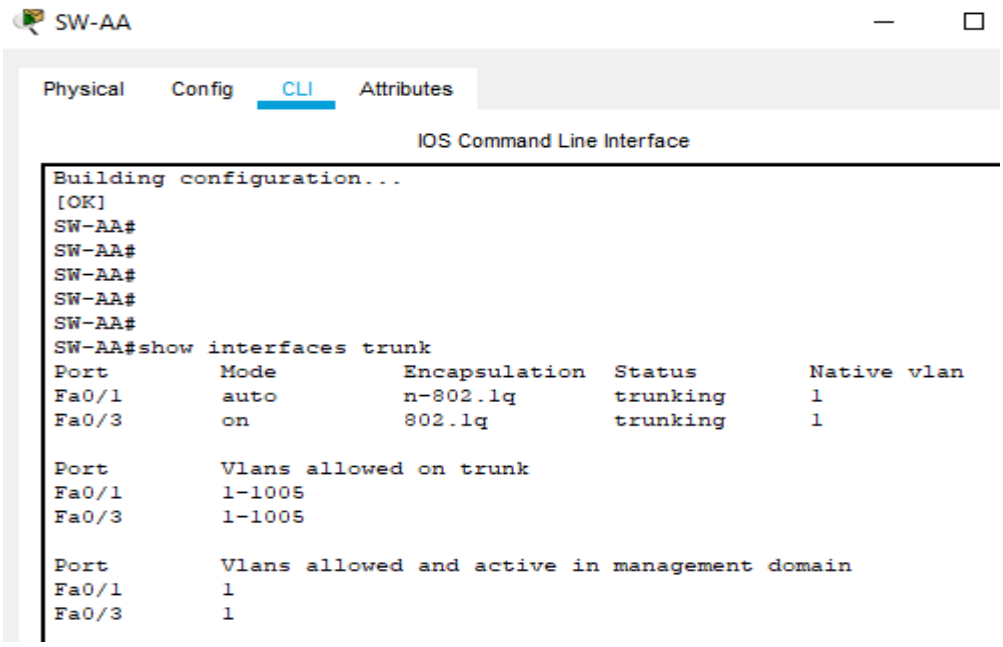


6. Entre SW-AA y SW-CC configure un enlace "trunk" estático utilizando el comando switchport *mode trunk* en la interfaz F0/3 de SW-AA.

```
SW-AA> Enable
SW-AA#configure terminal
SW-AA(config)# interface fastEthernet 0/3
SW-AA(config-if)# switchport mode trunk
```

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

Figura 15: show interface trunk F 0/3 SW-AA



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

```
SW-CC> Enable
SW-CC#configure terminal
SW-CC(config)# interface fastEthernet 0/1
SW-CC(config-if)# switchport mode trunk
```

Validación enlace “trunk” entre SW-BB y SW-CC

Figura 16: Validación modo trunk SW-BB

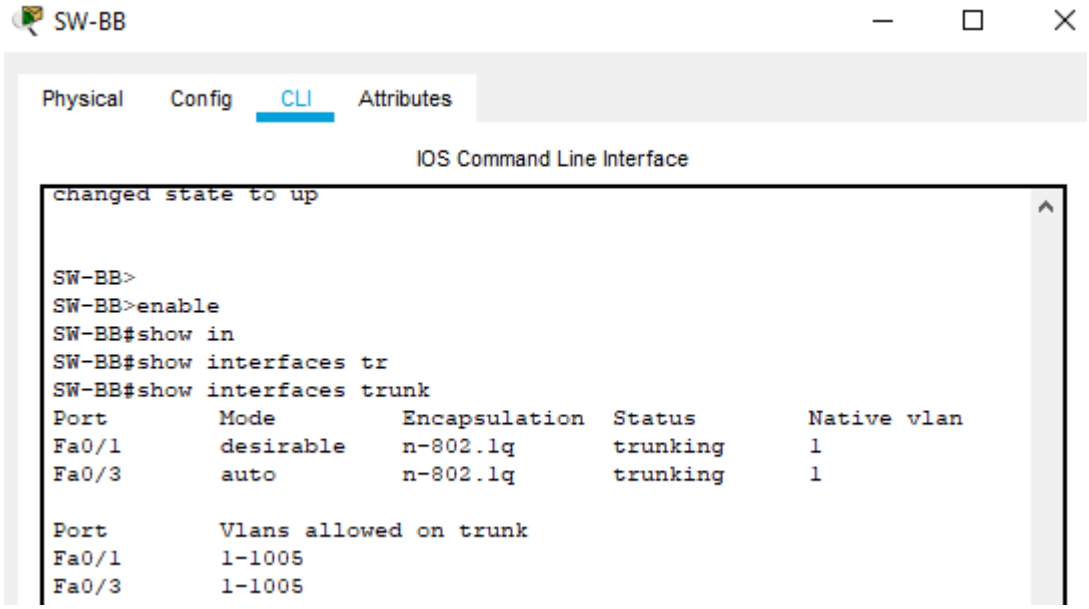
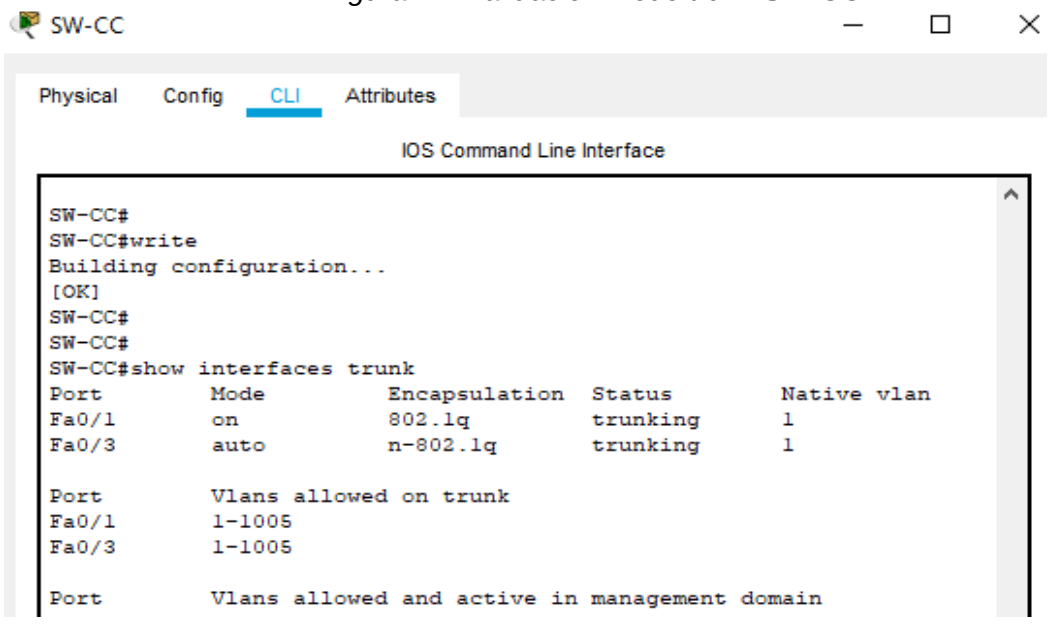


Figura 17: Validación modo trunk SW-CC



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> Enable
SW-AA#configure terminal
SW-AA(config)# vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode

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)#exit
SW-BB(config)#vlan 25
SW-BB(config-vlan)#name Personal
SW-BB(config-vlan)#exit
SW-BB(config)#vlan 30
SW-BB(config-vlan)#name planta
SW-BB(config-vlan)#exit
SW-BB(config)#vlan 99
SW-BB(config-vlan)#name Admon
SW-BB(config-vlan)#exit
SW-BB(config)#exit
```

10. Verifique que las VLANs han sido agregadas correctamente

Figura 18: Validación Creación de Vlans en SW-BB

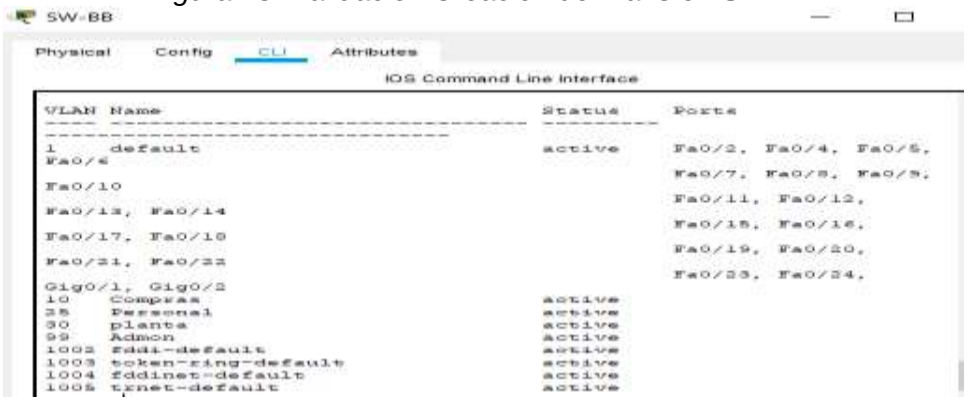


Figura 19: Validación Creación de Vlans en SW-AA

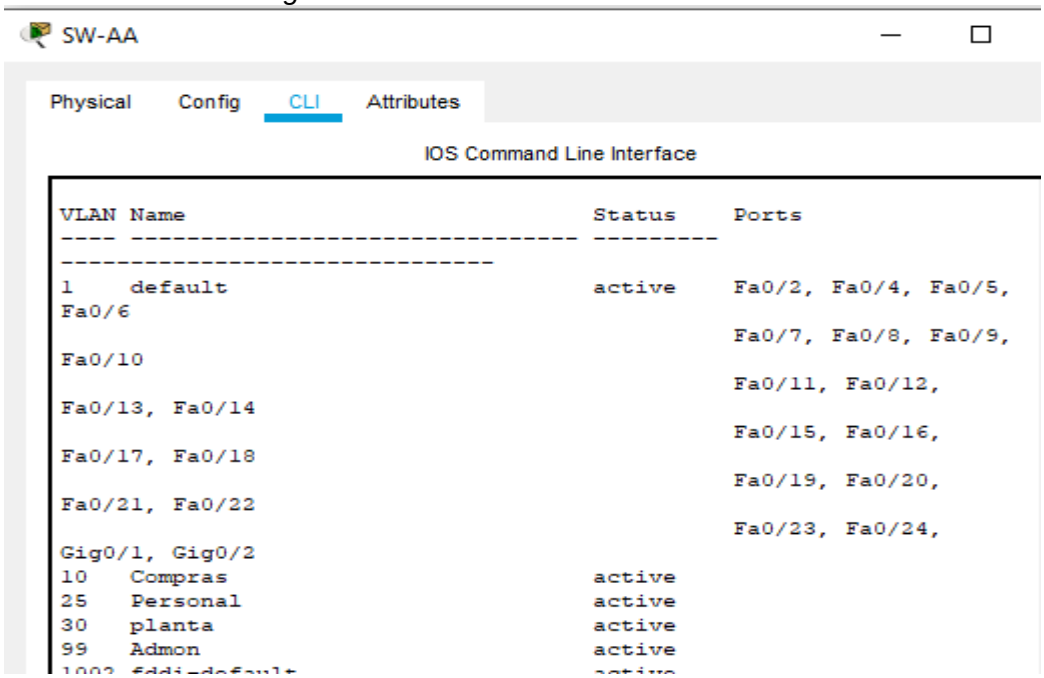
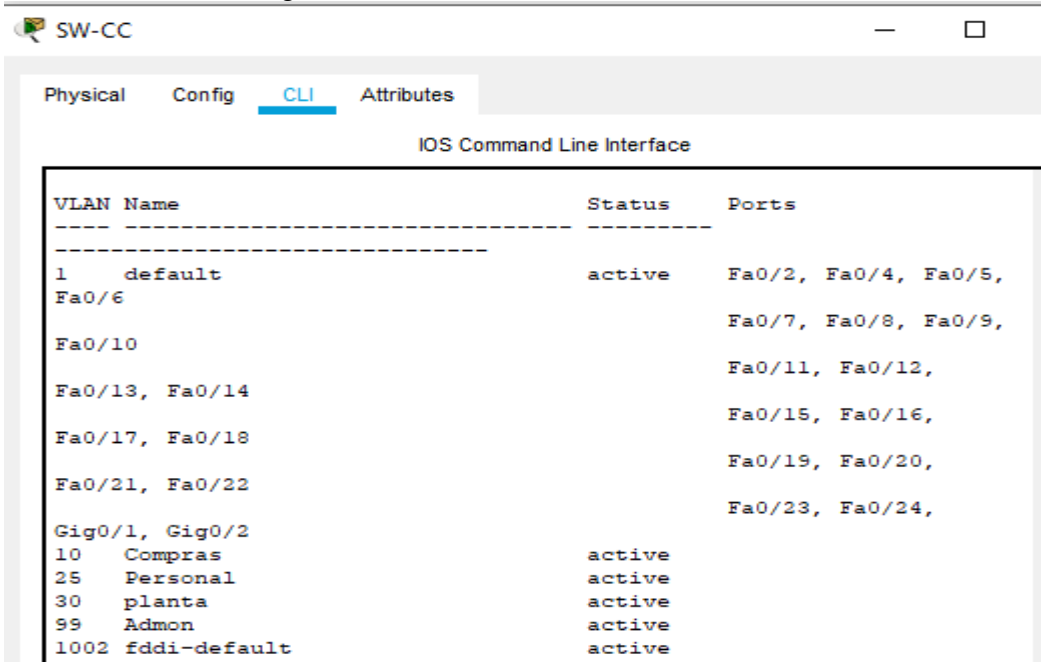


Figura 20: Validación Creación de Vlans en SW-CC



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

Tabla 5 enrutamiento PC

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 fastEthernet 0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10 / Compras
SW-AA(config-if)#exit
SW-AA(config)# interface fastEthernet 0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25 / Personal
SW-AA(config-if)#exit
SW-AA(config)# interface fastEthernet 0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30 / Planta
SW-AA(config)#end
```

```
SW-BB#configure terminal
SW-BB(config)#interface fastEthernet 0/10
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10 / Compras
SW-BB(config-if)#exit
SW-BB(config)# interface fastEthernet 0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25 / Personal
```

```
SW-BB(config-if)#exit
SW-BB(config)# interface fastEthernet 0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30 / Planta
SW-BB(config)#end

SW-CC#configure terminal
SW-CC(config)#interface fastEthernet 0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10 / Compras
SW-CC(config-if)#exit
SW-CC(config)# interface fastEthernet 0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25 / Personal
SW-CC(config-if)#exit
SW-CC(config)# interface fastEthernet 0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30 / Planta
SW-CC(config)#end
```

Direccionamiento de los pc

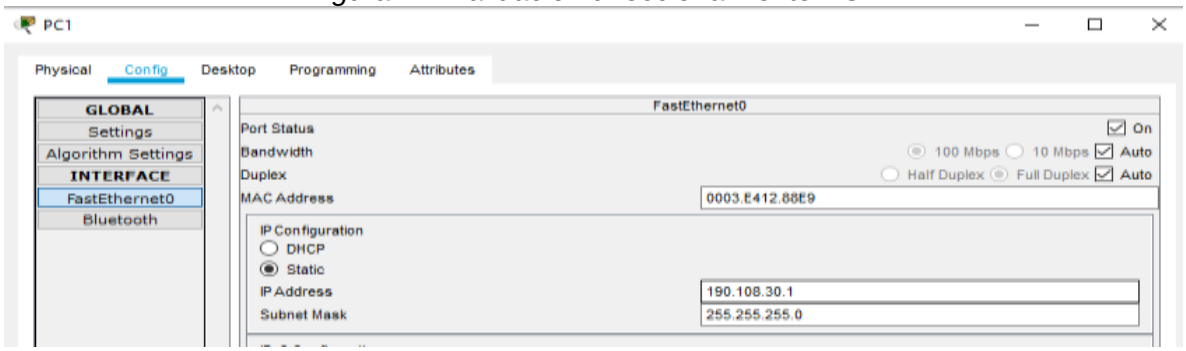
Tabla 6 enrutamiento PC según Vlan

Interfaz	VLAN	N pc	Direcciones IP de los PCs
F0/10	VLAN 10	3	190.108.10.1 / 24
		4	190.108.10.2 / 24
		7	190.108.10.3 / 24
F0/15	VLAN 25	2	190.108.20.1 /24
		5	190.108.20.2 /24
		8	190.108.20.3 /24
F0/20	VLAN 30	1	190.108.30.1 /24
		6	190.108.30.2 /24
		9	190.108.30.3 /24

SW-AA

Pc 1 Planta

Figura 21: Validación direccionamiento PC1

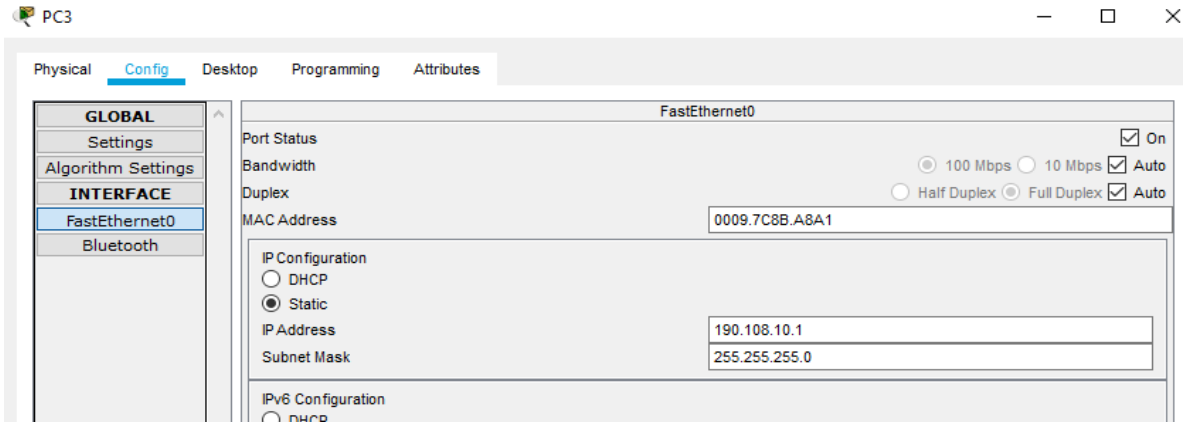


Pc 2 Personal

Figura 22: Validación direccionamiento PC2

Pc 3 Compras

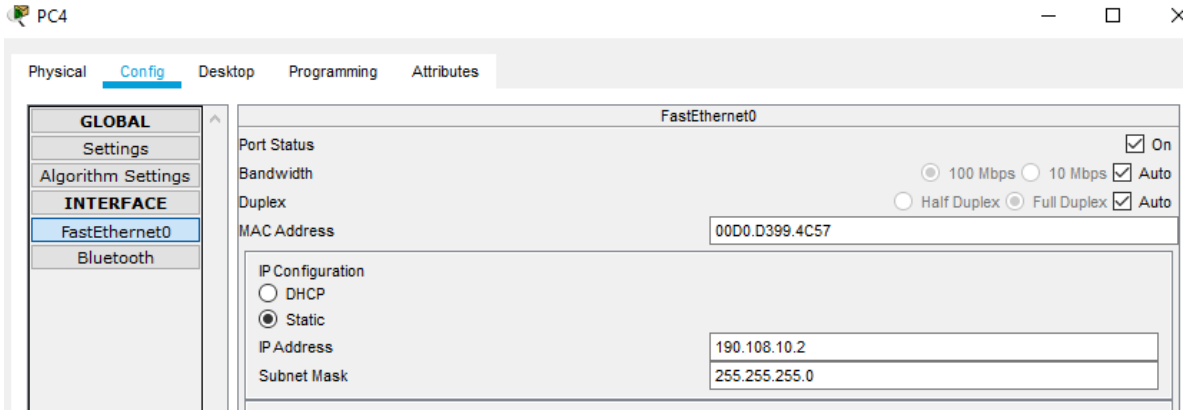
Figura 23: Validación direccionamiento PC3



SW-BB

Pc 4 Compras

Figura 24: Validación direccionamiento PC4

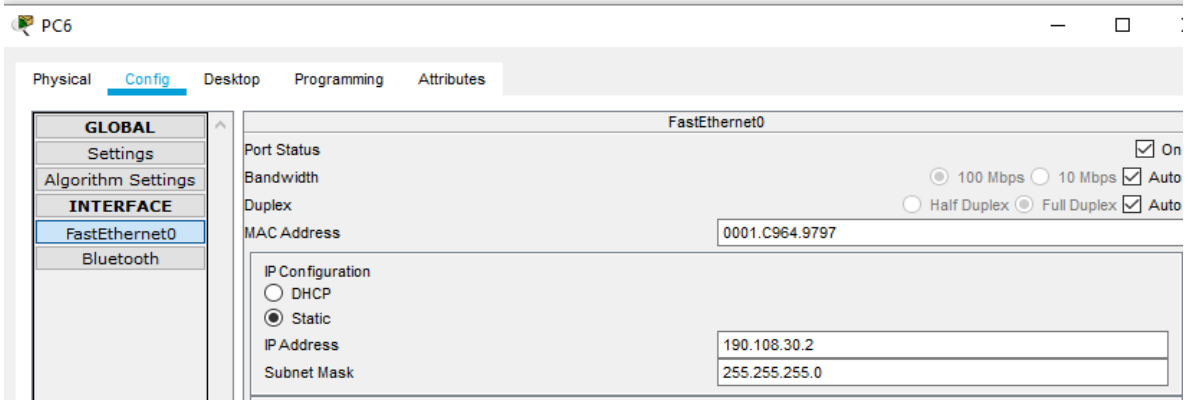


Pc 5 Personal

Figura 25: Validación direccionamiento PC5

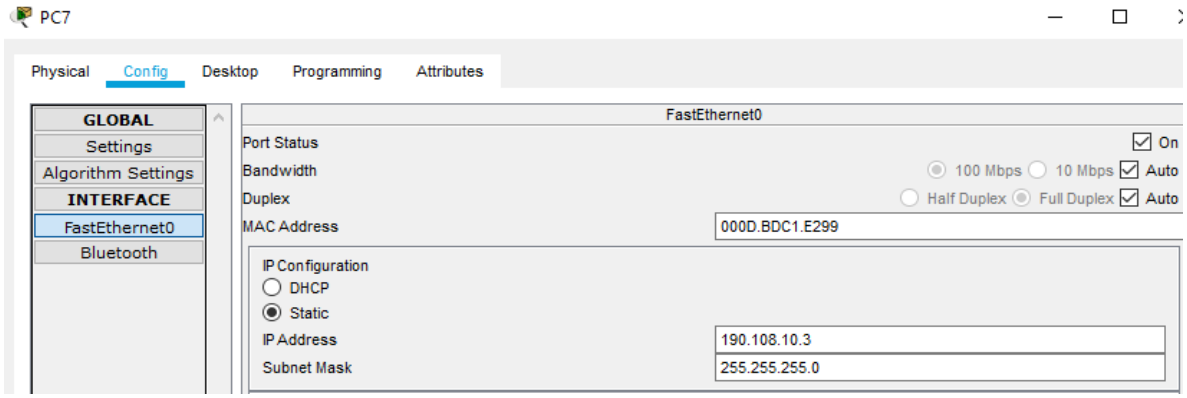
Pc 6 Planta

Figura 26: Validación direccionamiento PC6



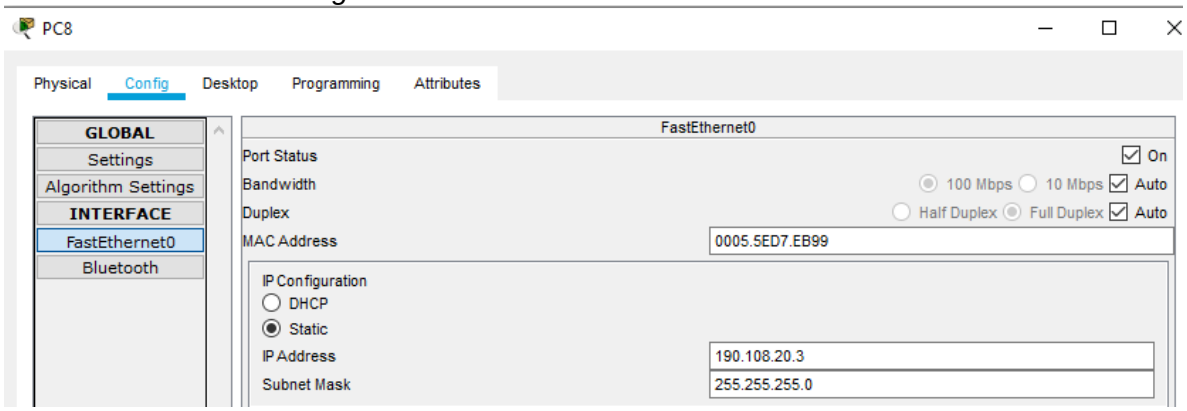
Pc 7 Compras

Figura 27: Validación direccionamiento PC7



Pc 8 Personal

Figura 28: Validación direccionamiento PC8



Pc 9 Planta

Figura 29: Validación direccionamiento PC9

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.

15. Tabla 7 enrutamiento 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>
SW-AA# configure terminal
SW-AA(config)# interface vlan 99
SW-AA(config-if)# ip address 190.108.99.1 255.255.255.0
SW-AA(config-if)# exit

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

SW-CC>
SW-CC# configure terminal
SWT3(config)# interface vlan 99
SW-CC(config-if)# ip address 190.108.99.3 255.255.255.0
SW-CC(config-if)# exit.
```

Verificación de conectividad Extremo a Extremo

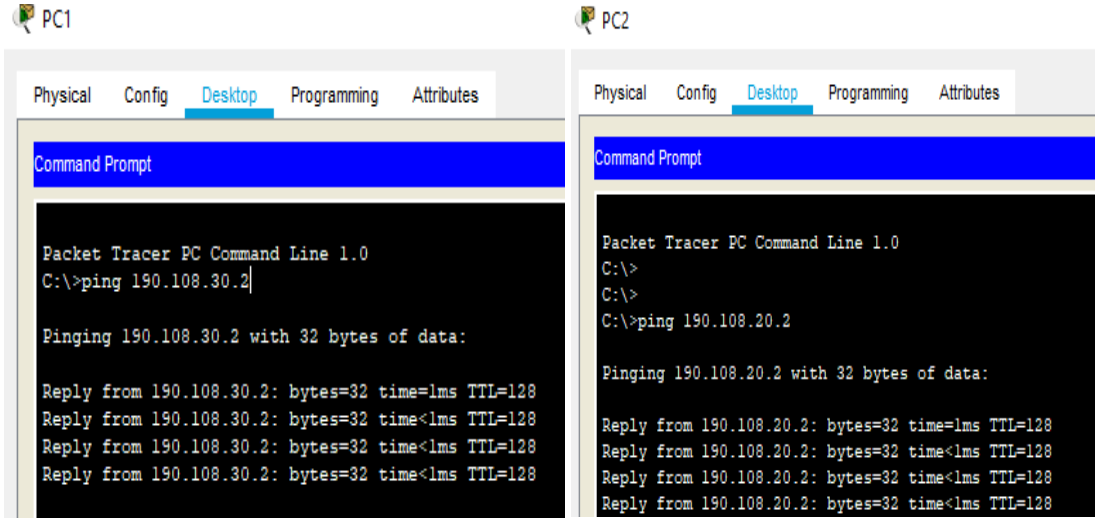
15. Ejecute un Ping desde cada PC a los demás. Explique por qué el ping tuvo o no tuvo éxito.

En la realización del ping entre los PCs pertenecientes a diferentes Vlans no tuvo éxito, al realizar ping entre los PCs de la misma Vlan este si tiene éxito, la no realización de ping entre todos los PCs y diferentes Vlans se presenta ya que cada PC pertenece a un segmento de red diferente que está

configurado por en las Vlans. Para lograr establecer comunicación con todas las Vlan y los PC se necesitaría agregar a la topología un switch de capa 3 el cual brindaría la función de enrutador entre las Vlans configuradas, así se lograría comunicar todo el tráfico ICMP generado en la red.

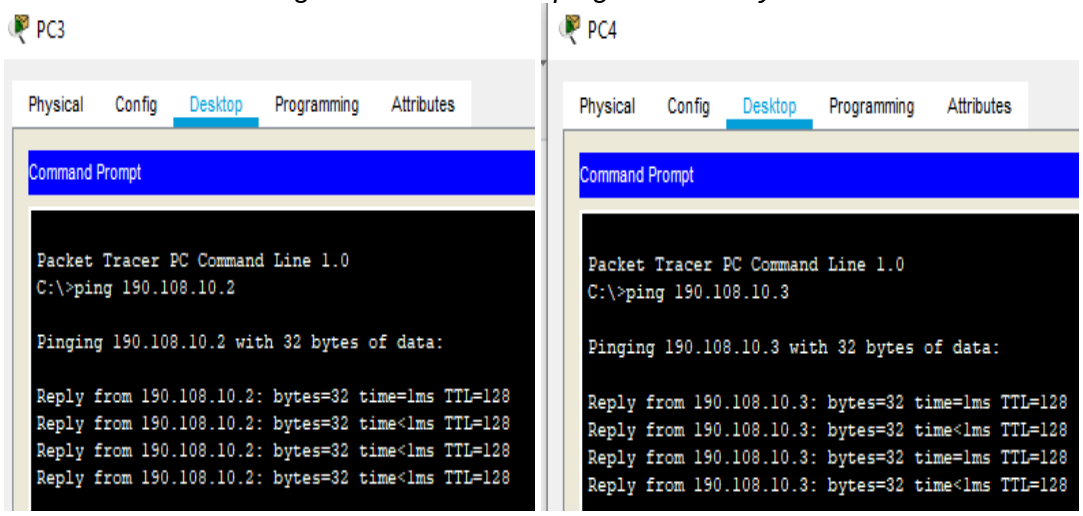
Ping de PC1 a PC 6 Ping de PC2 a PC5

Figura 30: Validación ping PC1 a Pc 6 y Pc2 a Pc5



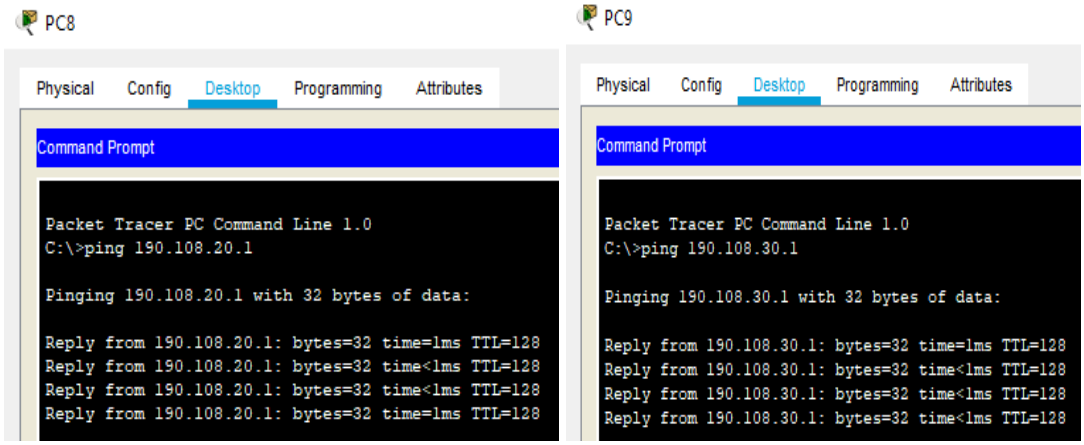
Ping de PC3 a PC 4 Ping de PC4 a PC7

Figura 30: Validación ping Pc3 a Pc4 y Pc4 a Pc7



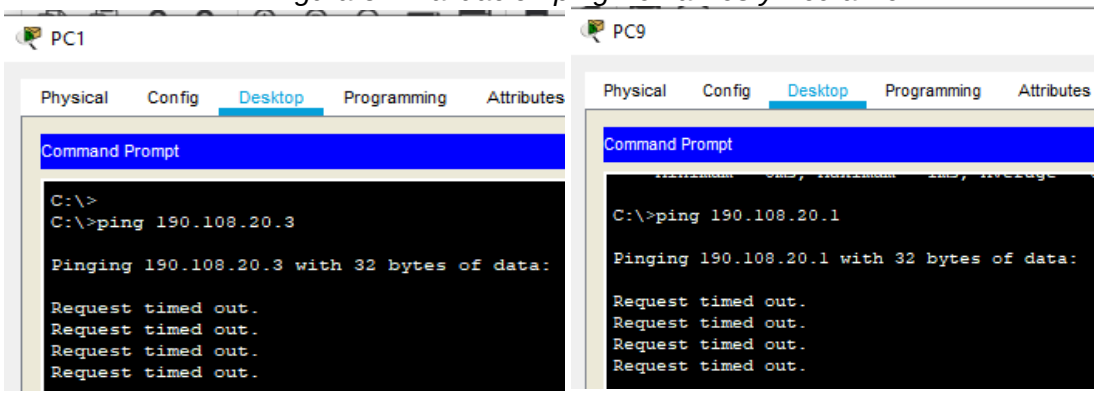
Ping de PC8 a PC 2 Ping de PC9 a PC1

Figura 31: Validación ping Pc8 a Pc2 y Pc9 a Pc1



Ping de PC1 a PC 8 Ping de PC9 a PC2

Figura 32: Validación ping Pc1 a Pc8 y Pc9 a Pc2



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

Al realizar ping entre los Switches es exitoso, dado que las interfaces físicas por estas se envían los datos al switch destino del ping este los recibe a través del protocolo ICMP, entre los Switches están configuradas en modo troncal, estas comparten el mismo tipo de encapsulamiento donde se validó con el comando *show interfaces trunk* y estas se encuentran en modo compatible.

Figura 33: Validación ping SW-AA a SW-BB y SW-CC

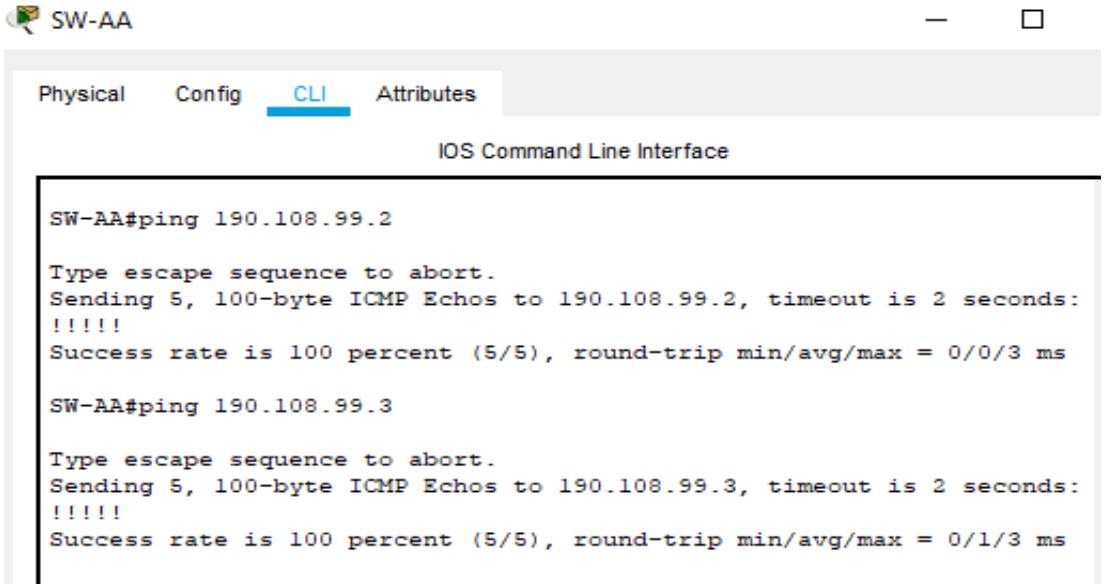


Figura 34: Validación ping SW-BB a SW-AA y SW-CC

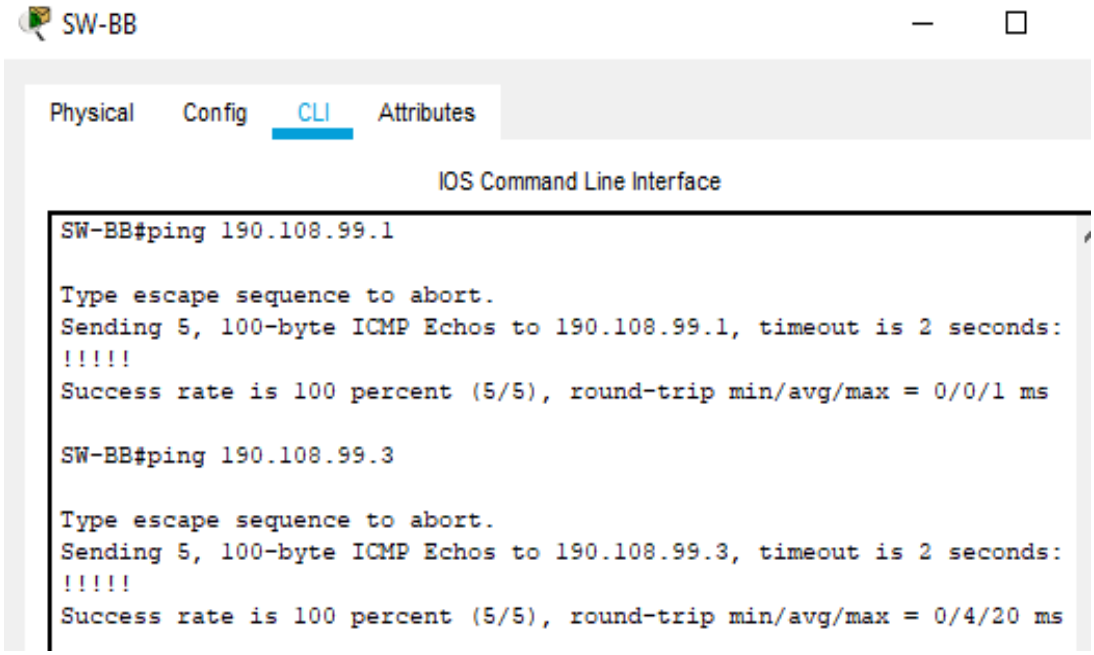
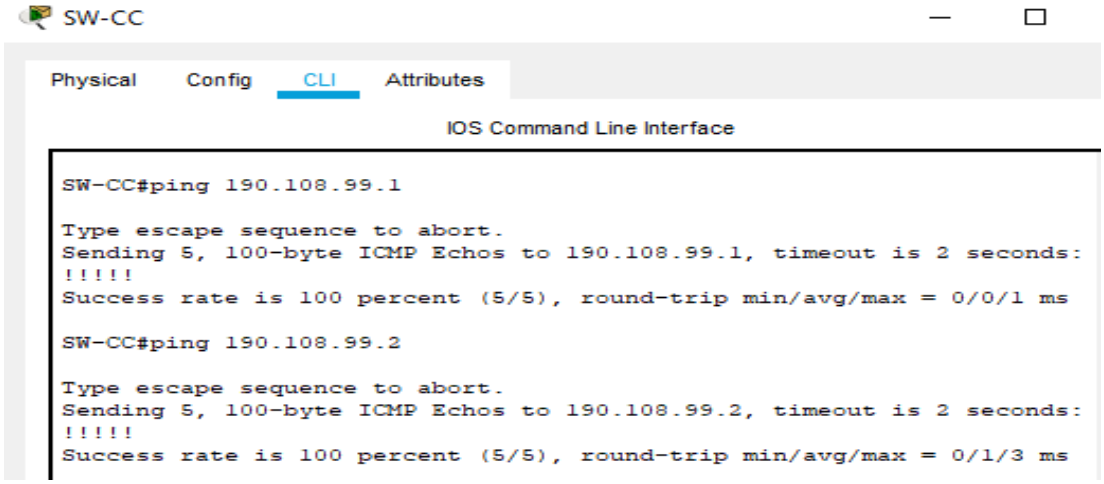


Figura 35: Validación ping SW-CC a SW-AA y SW-BB



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

Al realizar ping desde los switches a los PC este no es exitoso, esto se debe a que no se tiene configurada una dirección ip y una máscara de subred en cada una de las interfaces Vlan de los switches, para esto que el ping sea éxitos se debe realizar esta asignación a cada una de las Vlans con una dirección ip del mismo segmento a la cual está conectada el pc y definir la Valn nativa de dichas interfaces.

Figura 36: Validación ping SW-AA a Pc 1-Pc2 y Pc3

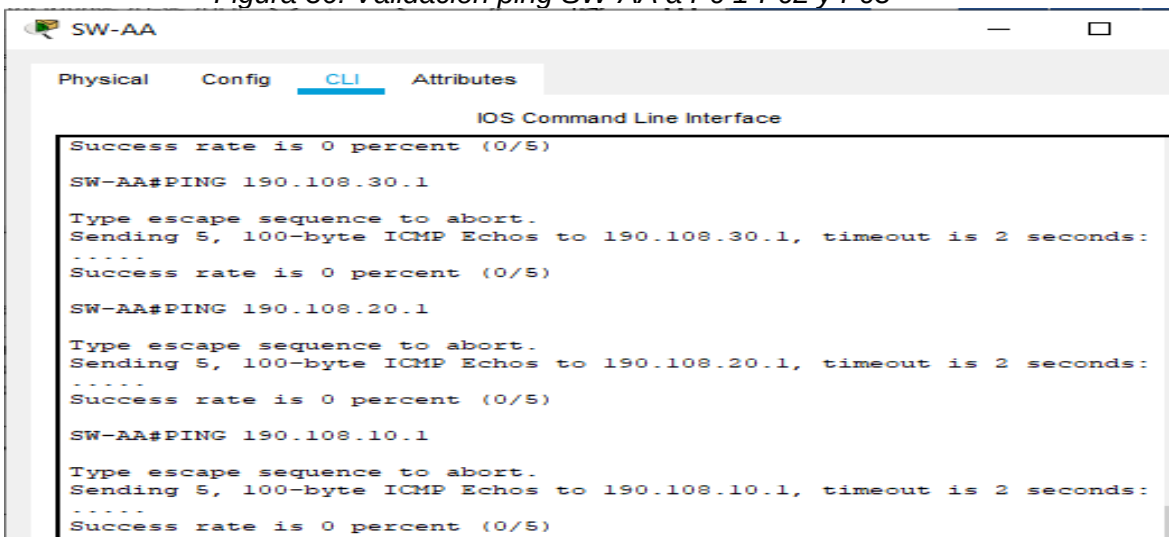


Figura 37: Validación ping SW-BB a Pc 1-Pc2 y Pc3

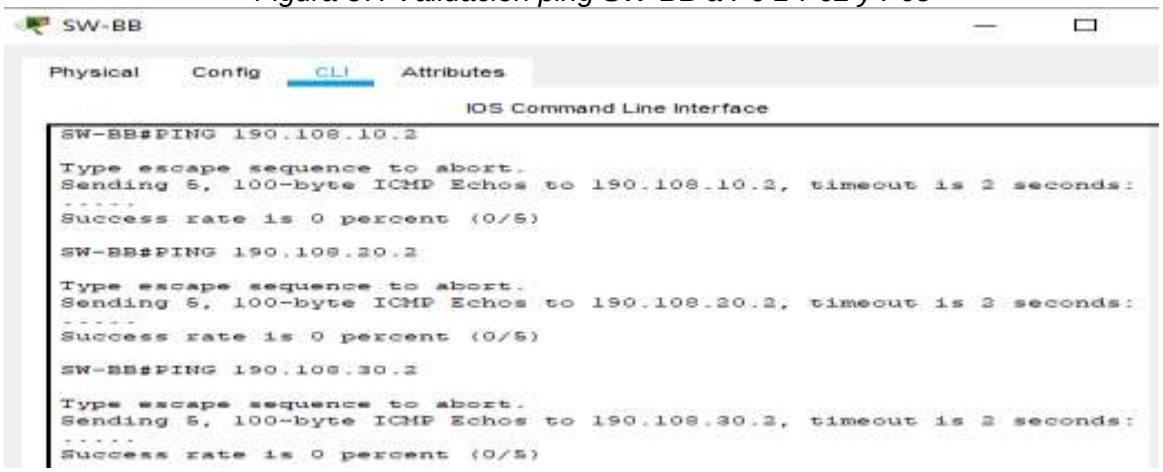
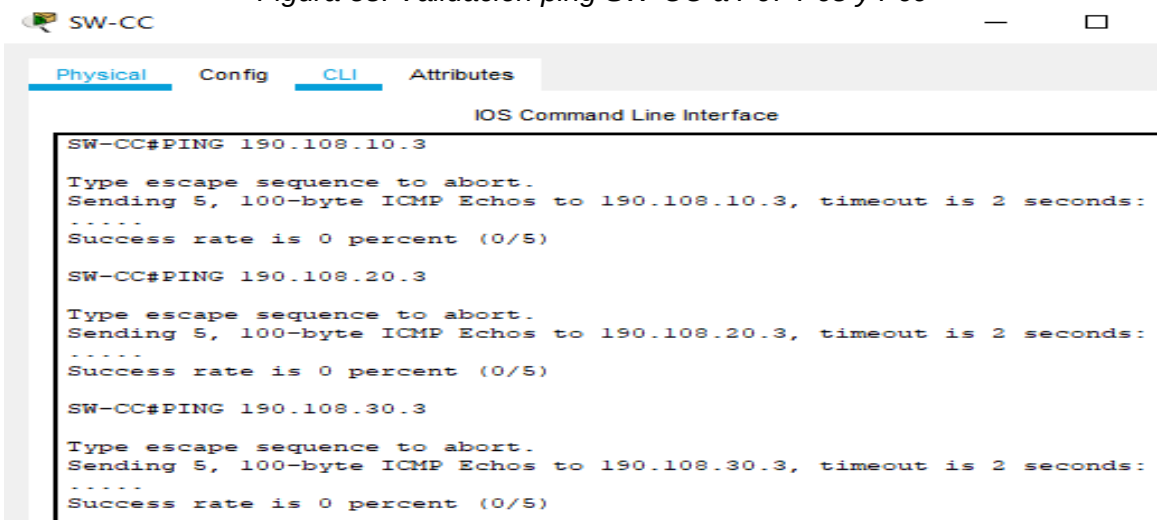


Figura 38: Validación ping SW-CC a Pc7-Pc8 y Pc9



CONCLUSIONES

En la realización de los dos escenarios propuestos como parte de la evaluación final del curso, se logró contextualizar los conocimientos teóricos y las habilidades practicas adquiridas a través del curso desarrollando estas mediante software como son GNS3 y Packet Tracer de cisco, en cuanto al contexto de la configuración del protocolo de configuración BGP se dejó en claro en funcionamiento de esté y su utilización en una red de enrutadores, se realizó la configuración de enrutamiento IPv4 en las interfaces Seriales, FastEthernet y Loopback de los dispositivos de enrutamiento, conmutación y accesos a la red por parte de usuarios finales. Se logró identificar fallas y dar solución a estos aplicando las habilidades adquiridas en este diplomado, se valida la existencia de conexiones lógicas entre los dispositivos de las redes propuestas.

En la verificación final de conectividad de extremo a extremos en el segundo escenario propuesto se constata los conocimientos obtenidos tras el cumplimiento del curso sobre estas temáticas, donde al tener que analizar los posibles causas de fallas de conectividad entre los diferentes dispositivos mediante la realización de ping donde vemos que en la una red física mediante Vlans podemos segmentar el tráfico a diferentes áreas de una compañía, este escenario en nuestra vida profesional nos vamos a enfrentar a la solución y configuraciones de estos y este diplomado nos da las bases para realizar nuestro trabajo de la mejor manera.

Tras completar las configuraciones requeridas para cada dispositivo, se logró contrastar los conocimientos adquiríos a lo largo del curso en referencia a los requerimientos y métricas que se tienen en cuenta para él envió de tráfico a través de 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).

BIBLIOGRAFIA

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Switch Fundamentals Review. 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). Network Design Fundamentals. 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). Campus Network Architecture. 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). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx

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

UNAD (2015). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm