# DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

**MARIA XIMENA RAMIREZ LOPEZ**

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

**MARIA XIMENA RAMIREZ LOPEZ**

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTÁ DC, 22 de mayo de 2020

AGRADECIMIENTOS

Con el presente quiero dar gracias a mi familia, por ser el pilar que motiva día tras día a salir adelante, a mis compañeros que me apoyaron en este proceso y juntos logramos mediante pruebas identificar errores y superarlos, asimismo al grupo docente en especial a mi tutor por su orientación, acompañamiento, consejos y grandes experiencias que fueron muy importantes y de gran valor para el desarrollo de las actividades.

## CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

## GLOSARIO

BGP Border Gateway Protocol: Es un protocolo tipo path-vector, aunque mantiene muchas características comunes con los de vector-distancia, diseñando para ser escalable y poder utilizarse en grandes redes creando rutas estables entre las organizaciones. Las rutas son registradas de acuerdo con los sistemas autónomos por donde está pasando y los bucles son evitados rechazando aquellas rutas que tienen el mismo número de sistema autónomo al cual están llegando

VTP Trunking Protocol: es un protocolo propietario de Cisco de capa 2 que nos permite intercambiar información sobre VLANs entre trunks de forma que los switches de la red tengan la base de datos de VLANs sincronizadas en todo momento desde un punto central de la red.

Loopback Es una interfaz de red virtual las cuales señalan que las direcciones del rango 127.0.0.0 son direcciones de loopback. Mayor mente se utiliza la 127.0.0.1 al ser la primera del rango. Son redefinidas en los dispositivos incluso en las direcciones IP públicas por ejemplo los routers realizan este tipo de actividades siempre

VLAN Es una red de área local virtual y sirve para crear redes lógicas independientes dentro de una misma red física. Esto significa que podemos tener varias redes virtuales separadas entre sí en un mismo switch físico.

Enrutamiento: se refiere al proceso en el que los enrutadores aprenden sobre redes remotas, encuentran todas las rutas posibles para llegar a ellas y luego escogen las mejores rutas (las más rápidas) para intercambiar datos entre las mismas.

## RESUMEN

Con la elaboración y desarrollo de las siguientes actividades del diplomado de Cisco CCNP se diseñaron topologías de conmutación y enrutamiento que mediante la configuración de direccionamiento y protocolo de BGP se logra intercambiar información mediante el establecimiento de una sesión de comunicación entre los router, permitiendo estabilidad de las redes donde los router se pueden adaptar rápido para enviar paquetes mediante una nueva conexión y en la segunda actividad se ve el funcionamiento del protocolo VTP el cual centraliza y simplifica la administración en un dominio de VLAN donde reduce la necesidad de configurar la misma VLAN en todos los switch operando en tres modos distintos el servidor (modo por defecto), cliente y transparente.



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



## ABSTRACT

With the elaboration and development of the following activities of the Cisco CCNP diploma, switching and routing topologies were designed that through the configuration of addressing and BGP protocol, it is possible to exchange information by establishing a communication session between the routers, allowing stability of networks where routers can quickly adapt to send packets over a new connection and in the second activity we see the operation of the VTP protocol which centralizes and simplifies administration in a VLAN domain where it reduces the need to configure the same VLAN in all switches operating in three different modes: server (default mode), client and transparent..



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

## INTRODUCCION

El presente trabajo tiene como objetivo poner en práctica los conocimientos adquiridos en el trascurso del estudio de las unidades del diplomado de profundización CCNP (prueba de habilidades practicas), el cual consta de dos escenarios uno que comprende la configuración correspondiente a routing mediante la implementación de protocolos como BGP y el otro enfocado a switching donde se configurara protocolo VTP y así validar el funcionamiento de cada uno de ellos mediante el uso de comandos show como show vtp status y ping entre otros.

## DESARROLLO

1. ESCENARIO 1

Figura 1.Escenario 1

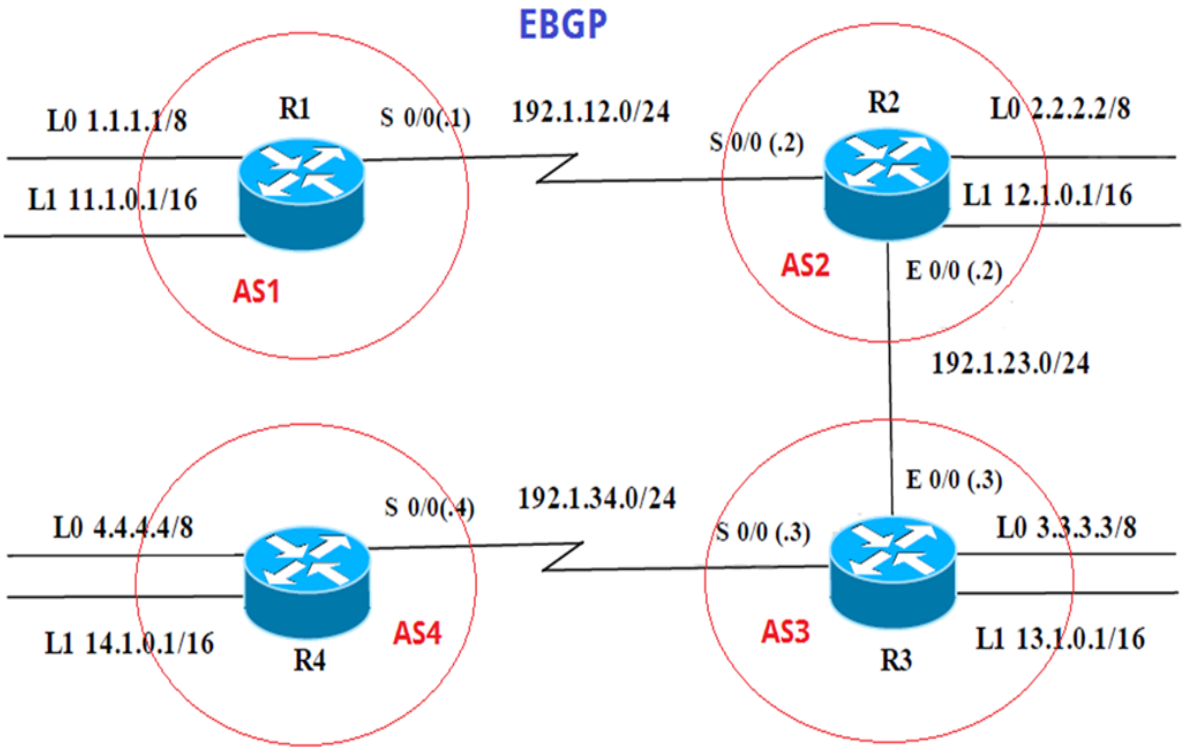
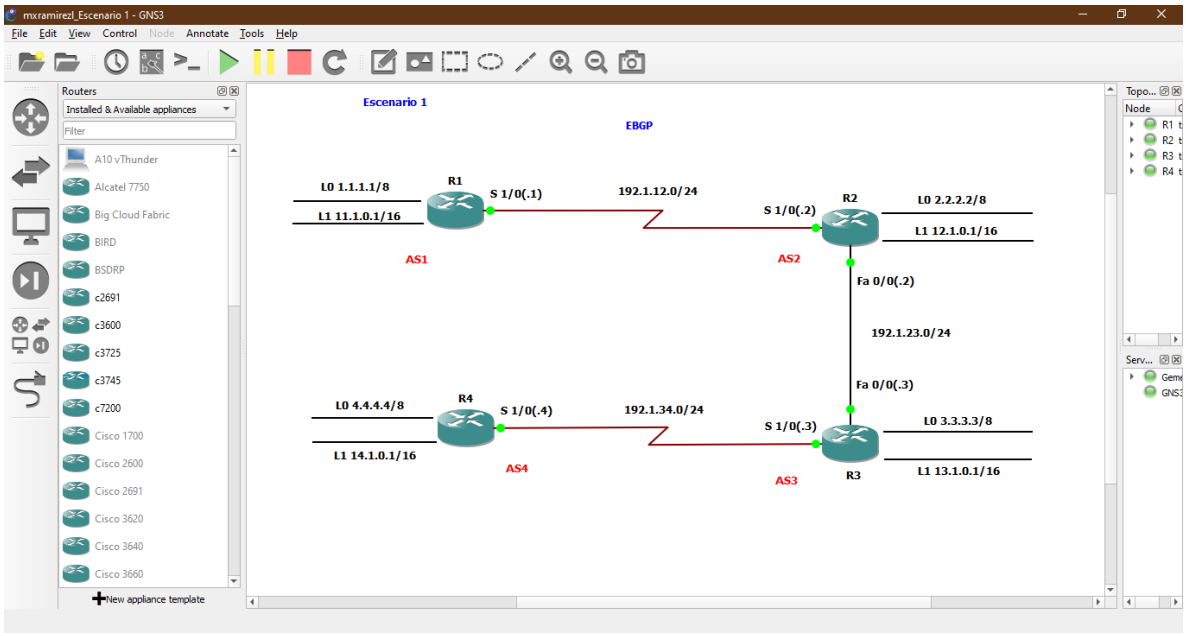


Figura 2.Simulación de escenario 1




Información para configuración de los Routers

Tabla 1.Direccionamiento R1

**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.Direccionamiento R2

**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.Direccionamiento R3

**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.Direccionamiento R4

**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 |

Para la elaboración del primer escenario se trabajara por medio del simulador GNS3 donde antes de iniciar con la ejecución de los puntos se dará inicio con la configuración de direccionamiento correspondiente a las interfaces de los cuatro Routers.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface Loopback 0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#
R1(config-if)#interface Loopback 1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#
R1(config-if)#interface serial 1/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit

R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface Loopback 0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#
R2(config-if)#interface Loopback 1
R2(config-if)#ip address 12.1.0.1 255.255.0.0
```

```
R2(config-if)#
R2(config-if)#interface serial 1/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#
R2(config-if)#interface fastEthernet 0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit

R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface Loopback 0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#
R3(config-if)#interface Loopback 1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#
R3(config-if)#interface fastEthernet 0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#
R3(config-if)#interface serial 1/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit

R4#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#interface Loopback 0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#
R4(config-if)#interface Loopback 1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#
R4(config-if)#interface serial 1/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
```

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.***

Se realiza configuración del protocolo BGP entre R1 y R2, donde se realiza anuncio de las direcciones loopback.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router bgp 1
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
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)#neighbor 192.1.12.2 remote-as 2
R1(config-router)#end
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router bgp 2
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
R2(config-router)#network 2.0.0.0 mask 255.0.0.0
R2(config-router)#network 192.1.12.0 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
```

Por medio del comando ***show ip route (***comando que permite visualizar tabla de enrutamiento**)**, se realiza verificación de los comandos ingresados anteriormente tanto en R1 y R2, logrando evidenciar que juntos routers tienen en la tabla de enrutamiento las direcciones loopback como las direcciones de las redes directamente conectadas.

Figura 3.Ejecución comando show ip router R1

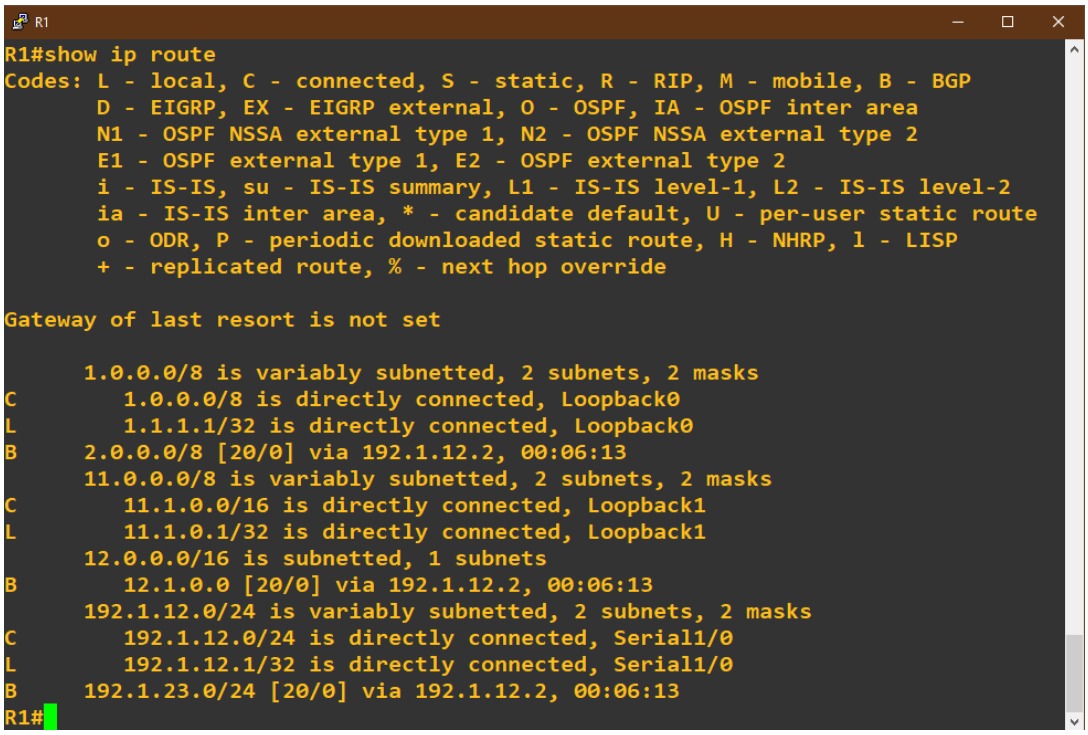
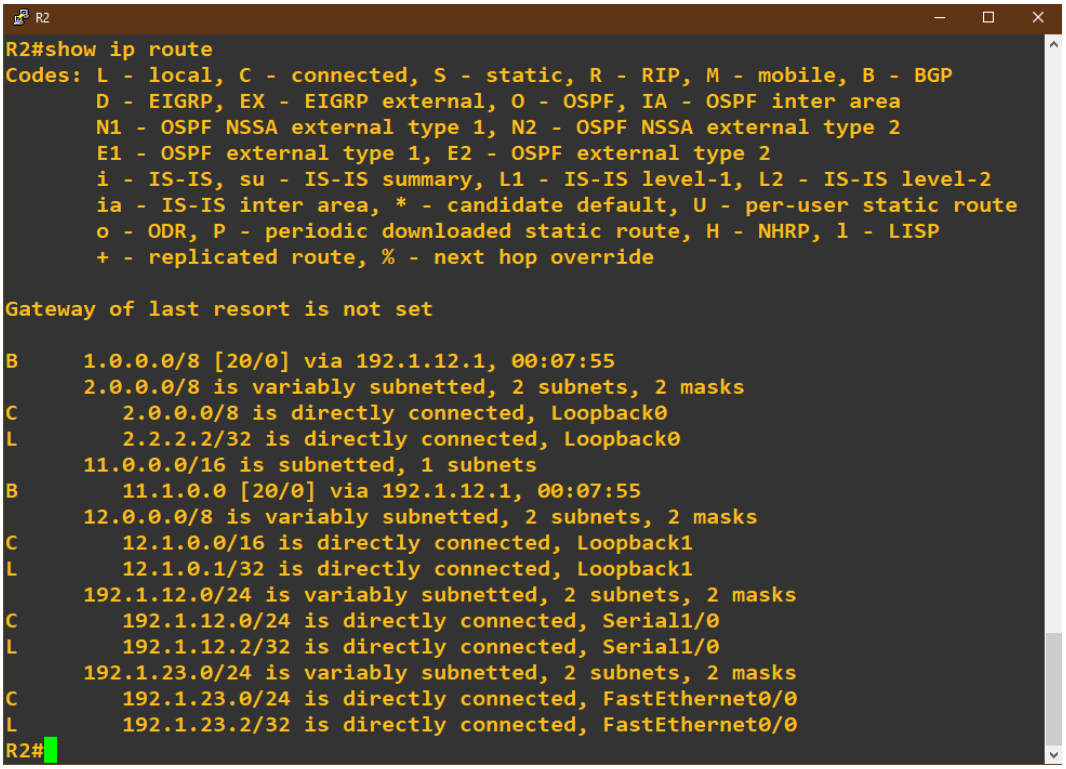



Figura 4.Ejecución comando show ip router R2



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.***

Se realiza configuración de BGP sobre R3 ya que en el anterior paso se realizó sobre R2, se realiza anuncio de las direcciones loopback de las direcciones de las interfaces y se codifica el ID del router R3.

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
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)#network 192.1.34.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#end
```

A continuación de emite el comando ***show ip route,*** donde se puede evidenciar que la tabla de enrutamiento fue actualizada sobre R2 con las direcciones de Loopback ingresadas en el R3 y al emitir este mismo comando sobre el R3 se visualiza que su tabla de enrutamiento contiene las redes directamente conectadas.

Figura 5.Ejecución comando show ip router R2

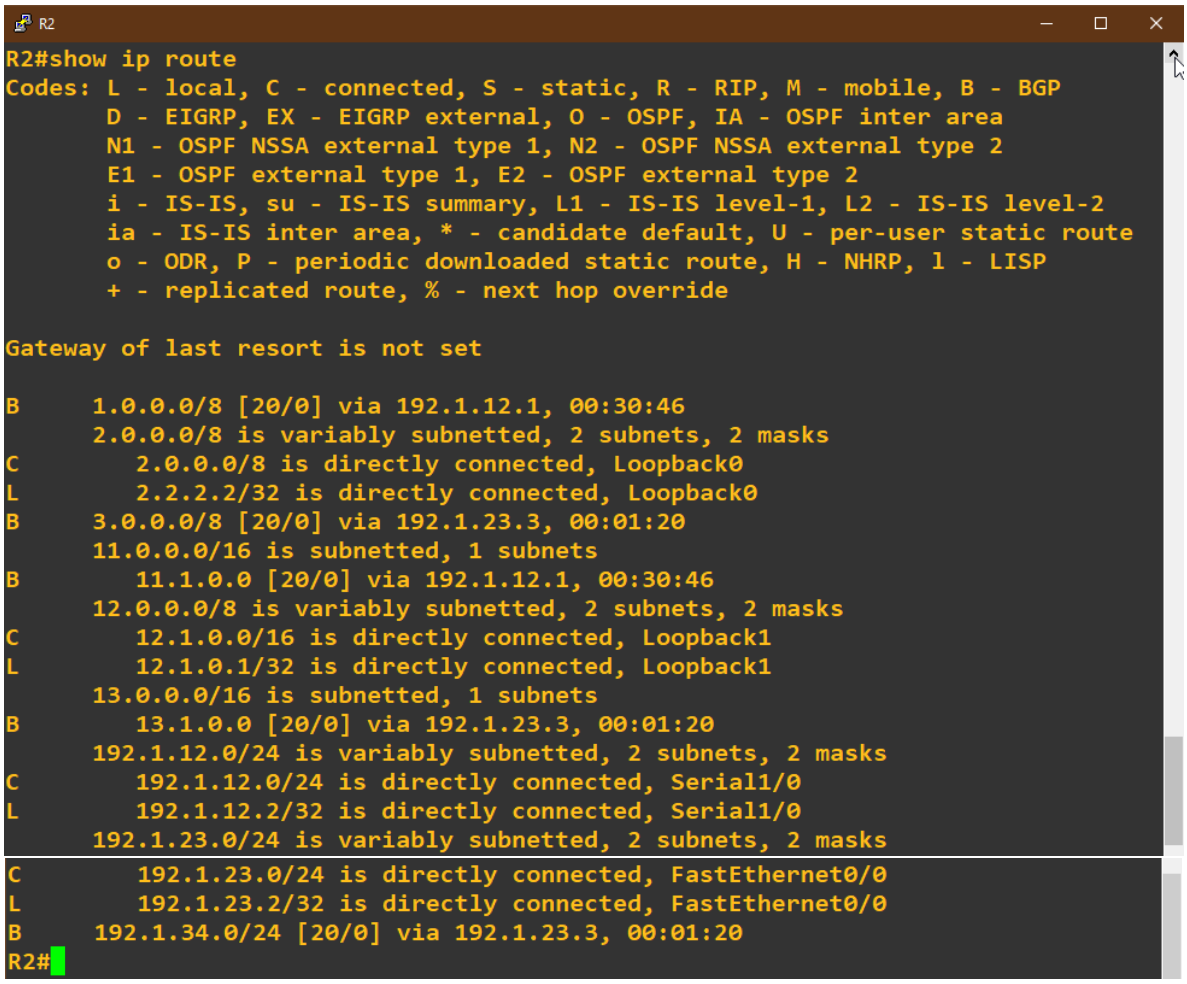
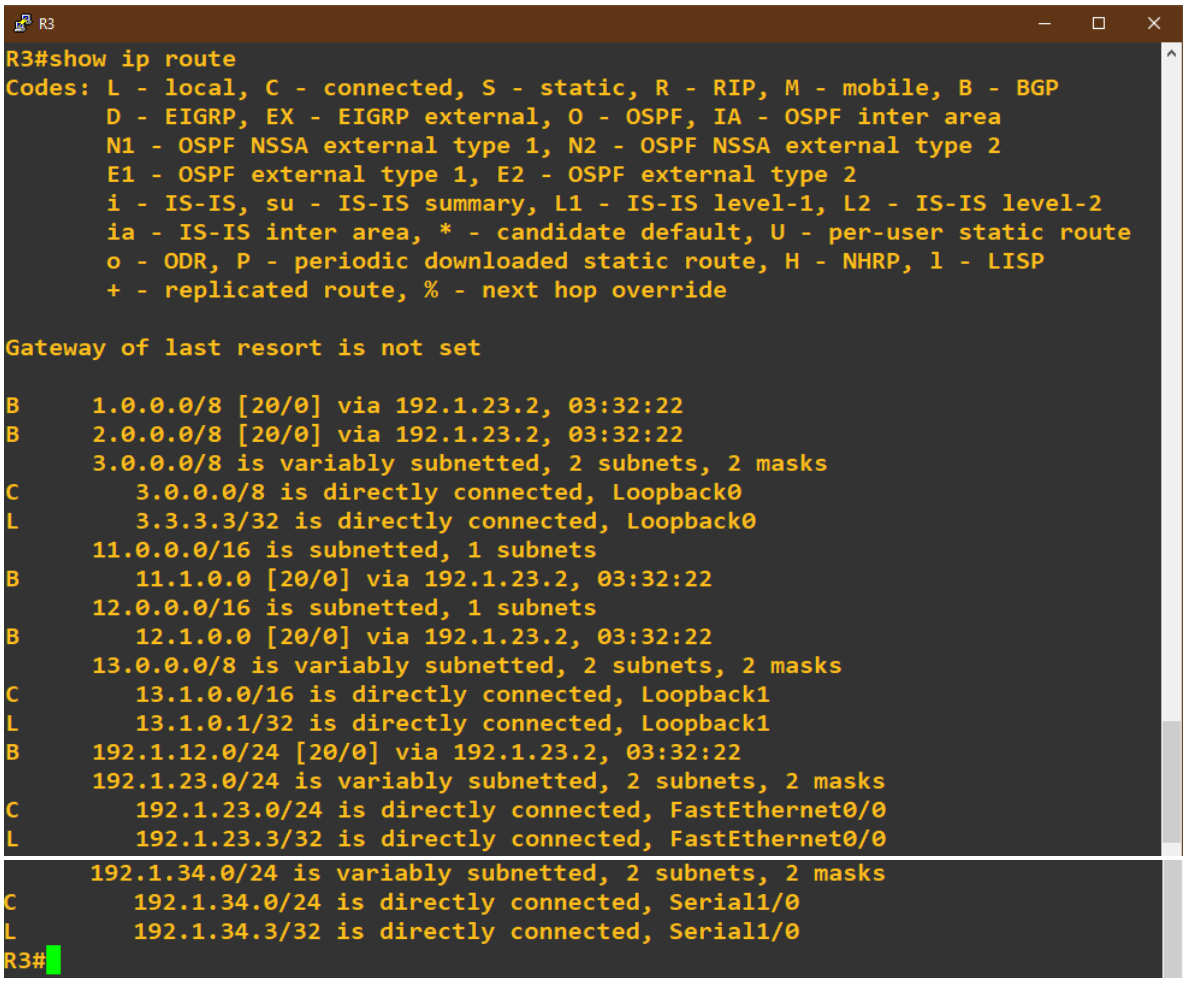


Figura 6.Ejecución comando show ip router R3




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.***

Se realiza configuración de BGP entre R3 y R4, donde se anuncian las direcciones Loopback y las direcciones de las interfaces en BGP, de igual manera se codifica ID del R4.

R4#configure terminal

```
Enter configuration commands, one per line.  End with CNTL/Z.
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)#end
```

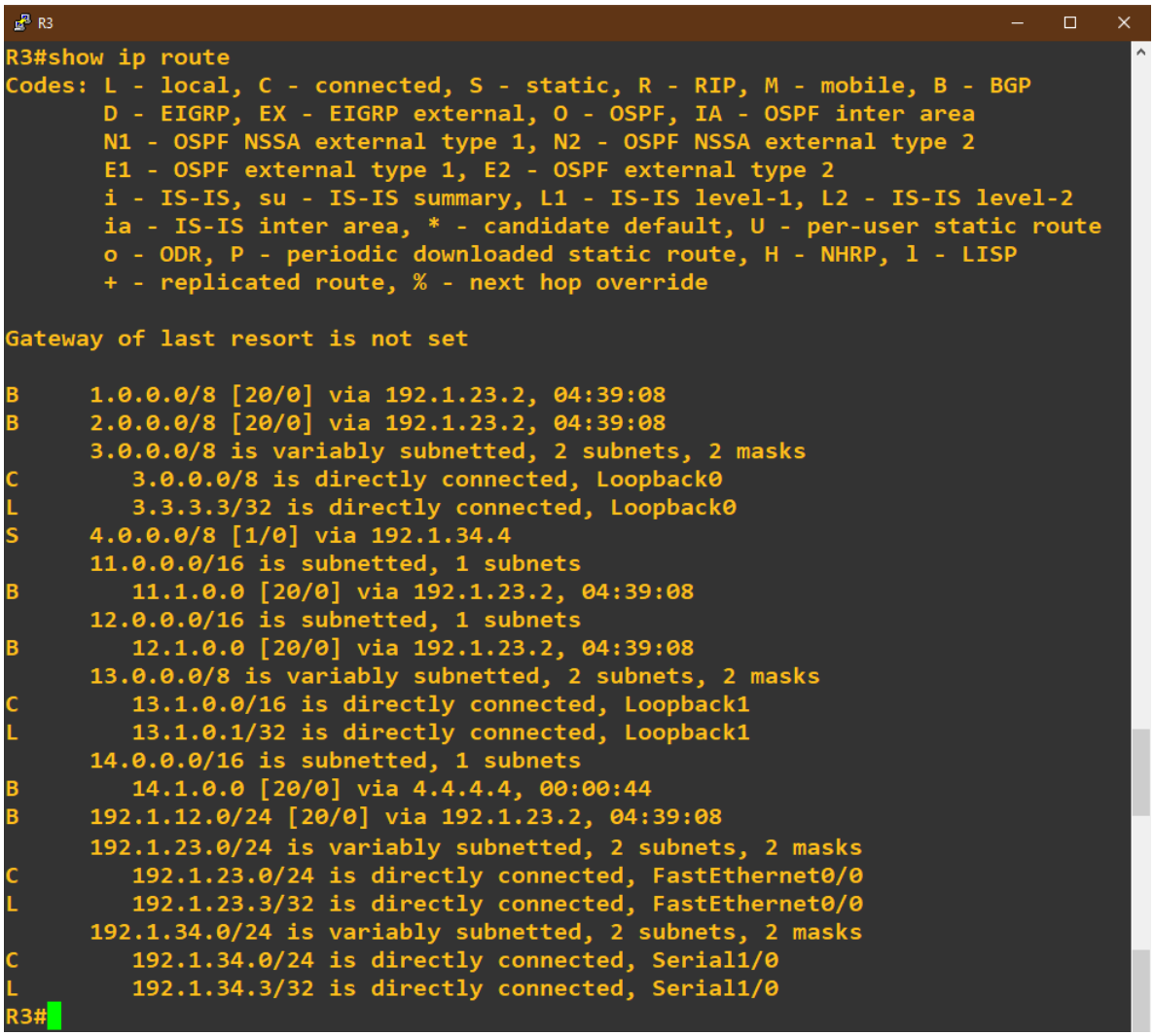
Se realiza configuración para establecer las adyacencias por medio de las direcciones de Loopback.

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
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)#end
```

```
R4#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
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)#end
```

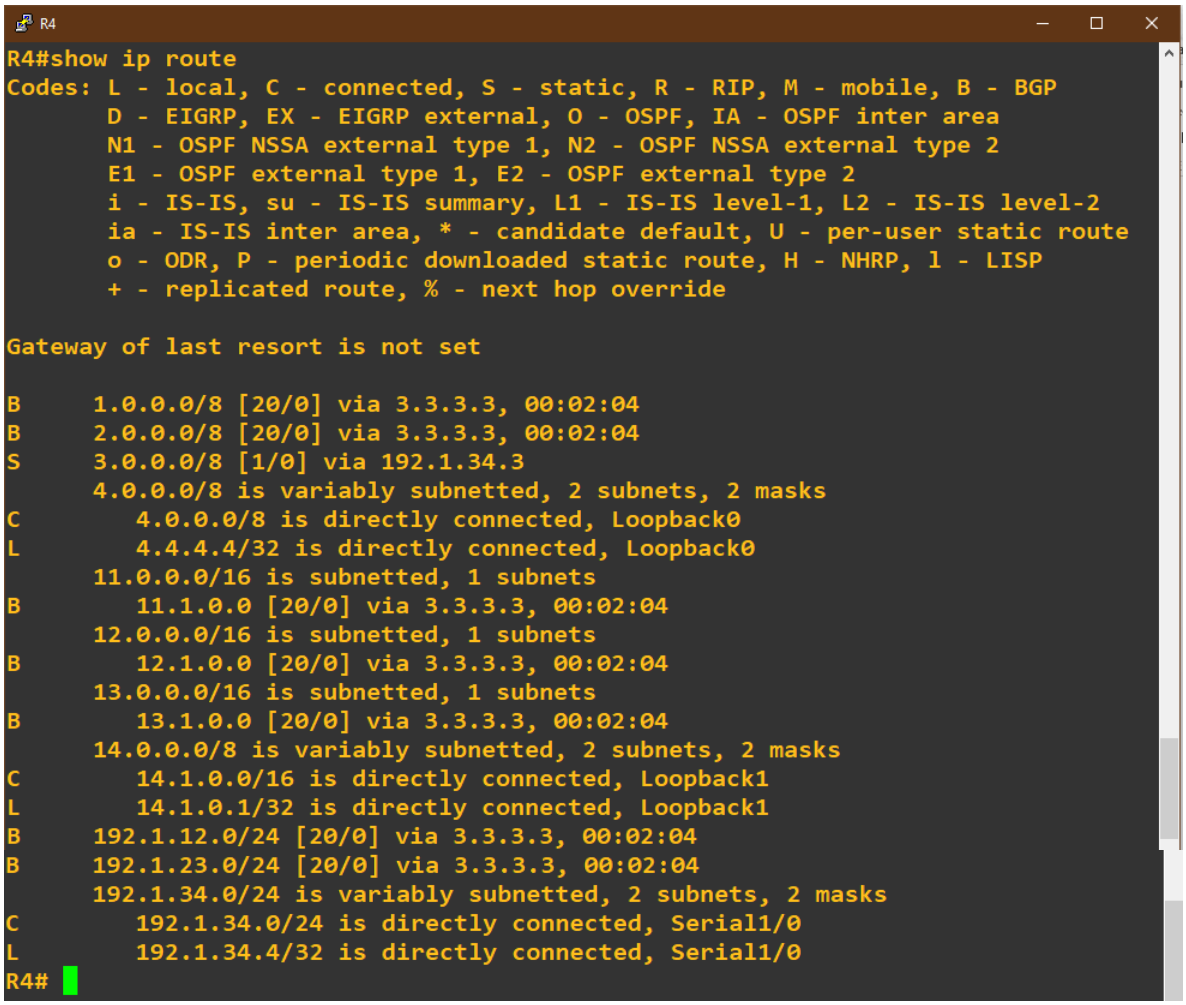
Se emite el comando ***show ip route,*** donde se puede evidenciar que la tabla de enrutamiento fue actualizada donde en R3 la dirección de red que conecta a R4 ahora es la Loopback 0 que se encuentra como ruta estática de acuerdo a la configuración anterior.

Figura 7.Ejecución comando show ip router R3




Se verica actualizacion de la tabla de enrutamiento sobre R4 por medio del comando ***show ip route*** donde se evidencia que ahora se comunica con los vecinos por medio de la interface Loopback 0 de R3.

Figura 8.Ejecución comando show ip router R3



2. ESCENARIO 2

Figura 9.Escenario 2

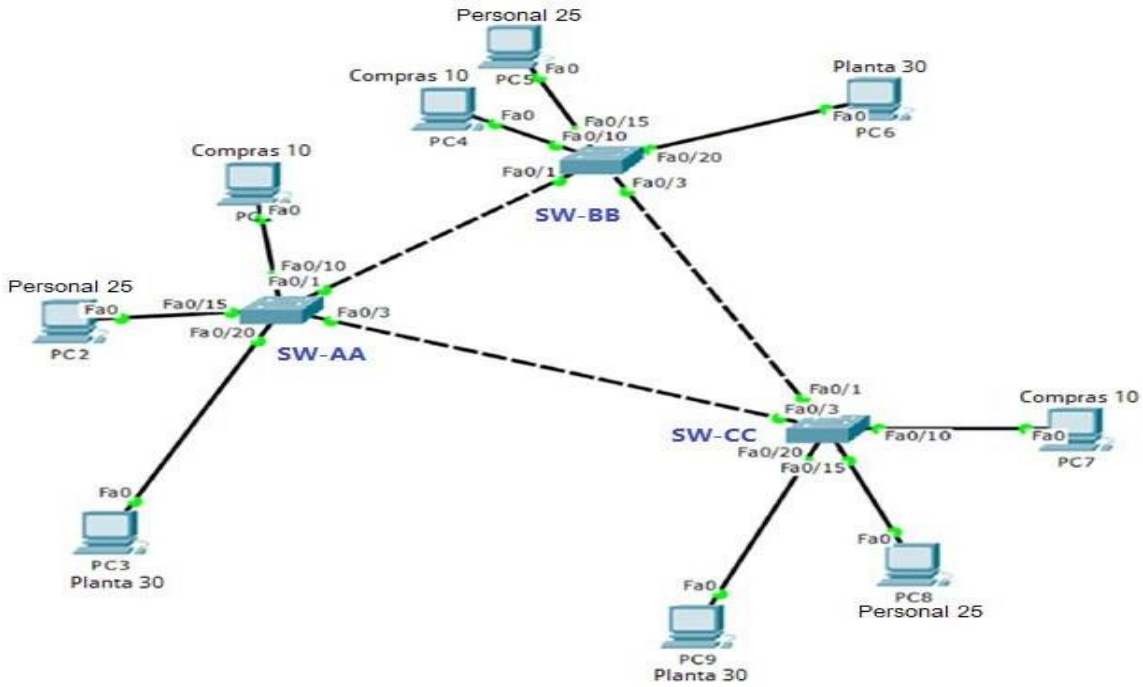
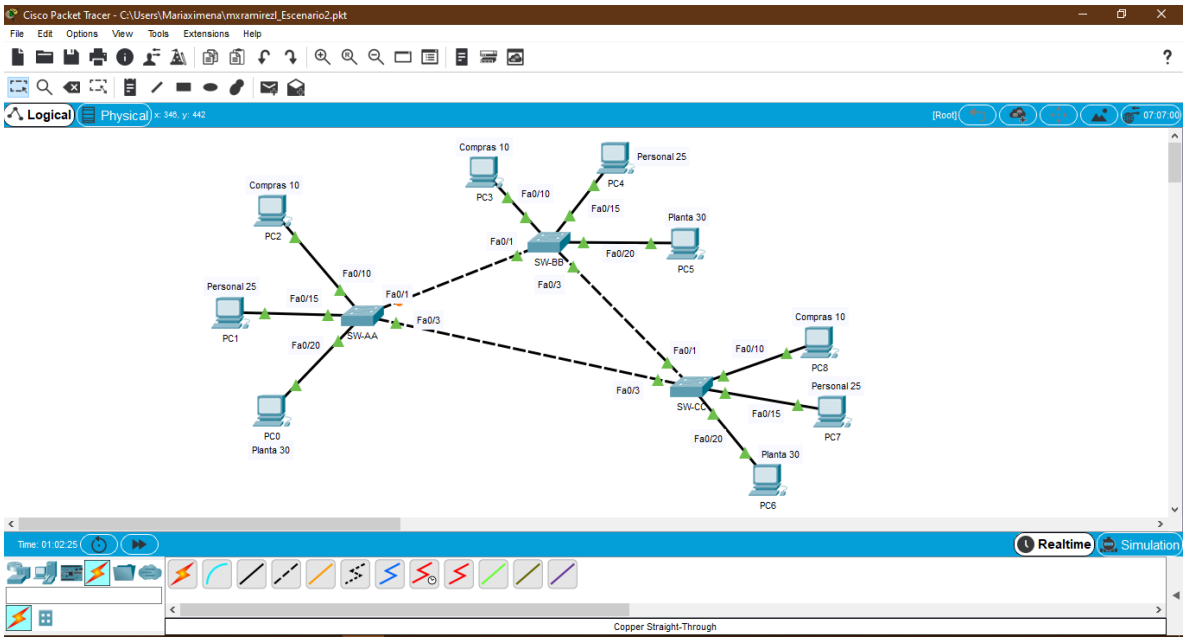



Figura 10.Simulación de escenario 2



## 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.

Por medio de los siguientes comandos se realizara la configuración del protocolo VTP el cual será aplicado sobre los tres sw en donde un será servidor y los otros dos cumplirá la función de cliente.

```
SW-BB#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-BB(config)#vtp mode server
Device mode already VTP SERVER.
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-BB(config)#exit

SW-AA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
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-AA(config)#exit

SW-CC#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
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
SW-CC(config)#exit
```

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

Por medio del comando **show vtp status** permite observar el estado de vtp al igual que proporciona información del dominio configurado anteriormente.

Figura 11.Salida comando show vtp status SW-BB

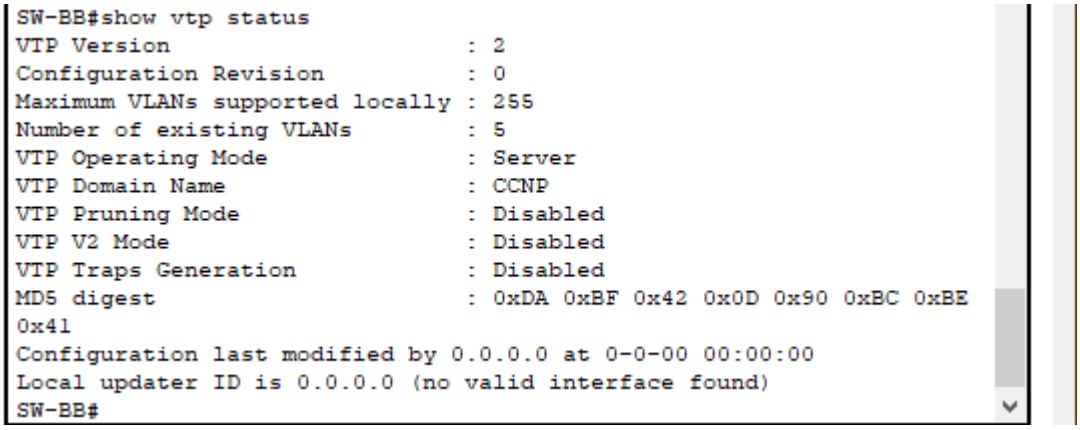



Figura 12.Salida comando show vtp status SW-AA

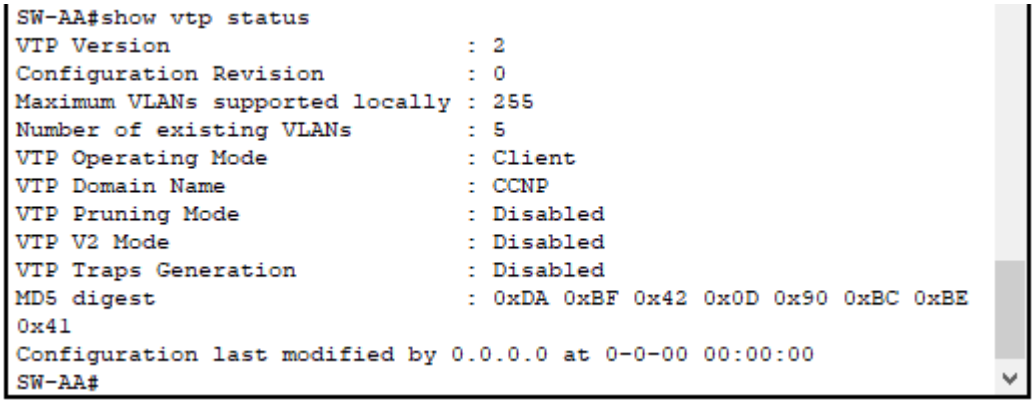
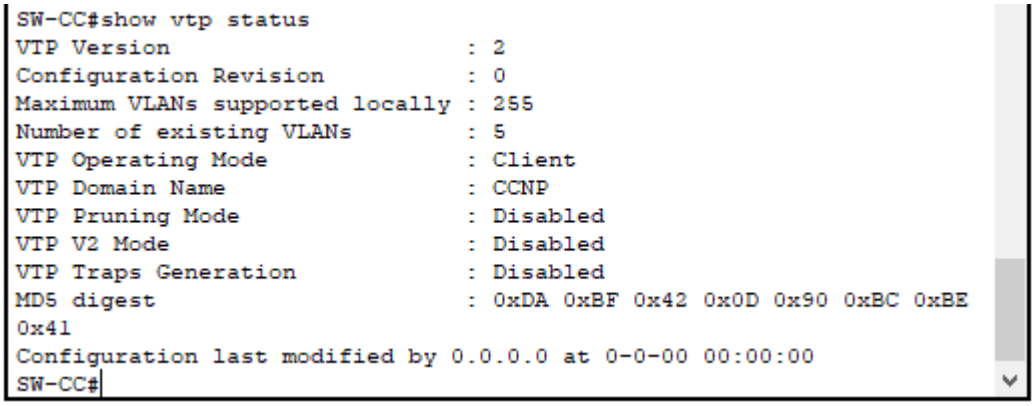



Figura 13.Salida comando show vtp status SW-CC



## 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***.

Se realiza configuración del enlace troncal entre SW-AA y SW-BB en donde se realizara configuración del puerto sobre el SWW-BB este se dejara como dynamic desirable.

SW-BB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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***.

Ahora se ejecuta el comando **show interfaces trunk** en juntos swhitch el cual nos permitirá verificar la configuración de los puertos troncales.

Figura 14.Salida comando show interfaces trunk SW-BB

```
SW-BB#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       desirable    n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1

SW-BB#
```

Figura 15.Salida comando show interfaces trunk SW-AA

```
SW-AA#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       none

SW-AA#
```

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

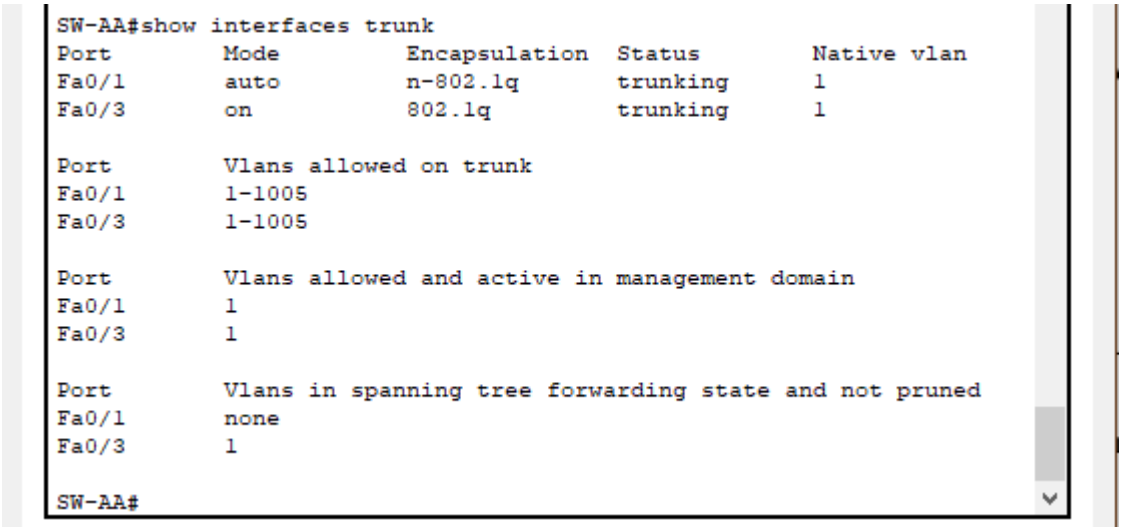
Se realiza configuración en modo troncal sobre la interface fa0/3 del SW-AA.

SW-AA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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.

Se realiza verificación del enlace troncal por medio del comando show interfaces trunk, en donde será ejecutado sobre el SW-AA.

Figura 16.Salida comando show interfaces trunk SW-AA




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

Se realiza configuración del enlace troncal entre el SW-BB y SW-CC sobre la interface fa0/1.

SW-CC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#interface fastethernet 0/1
SW-CC(config-if)#switchport mode trunk

**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)

Se realiza configuración de la VLAN 10 sobre el SW-BB debido a que como el SW-AA se encuentra en modo cliente no es posible realizar esta agregación, de igual manera se realiza configuración de las vlan siguientes.

```
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 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.

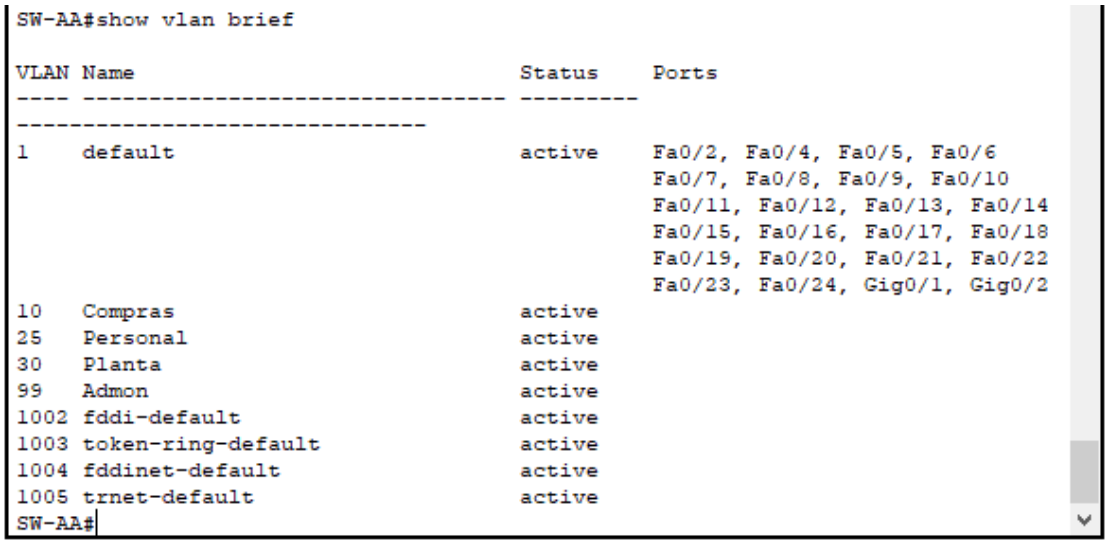
Por medio del comando show vlan brief se realiza verificación de las vlan agregadas en los switches esto es posible debido a que el modo servidor se encarga de crear modificar y eliminar sobre todo el dominio de vtp mientras que el modo cliente permite sincroniza la configuración propagada por el servidor.

Figura 17.Ejecución show vlan brief SW-BB

```
SW-BB#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   Compras                          active
25   Personal                         active
30   Planta                           active
99   Admon                            active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SW-BB#
```

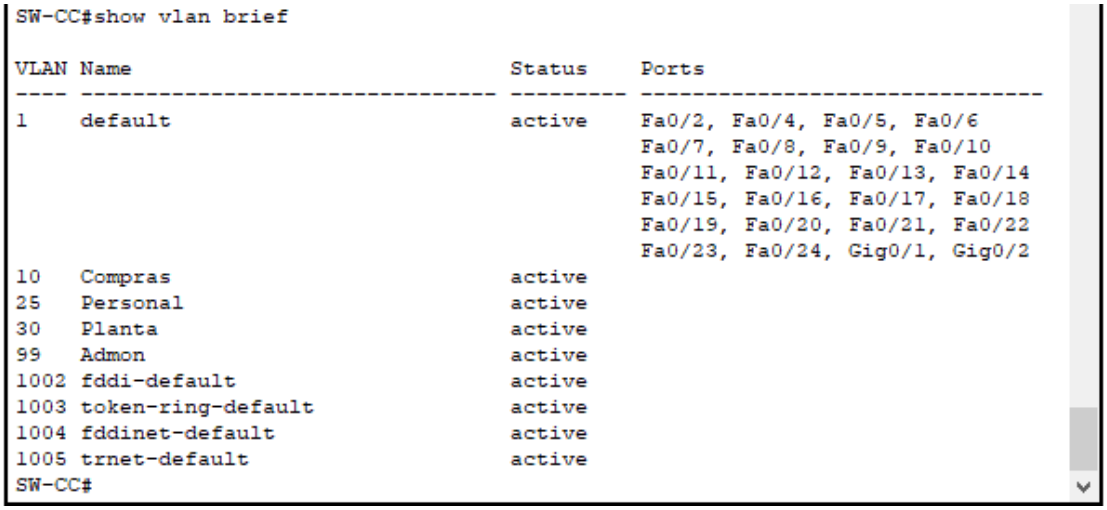
Figura 18.Ejecución show vlan brief SW-AA



```
SW-AA#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   Compras                           active
25   Personal                          active
30   Planta                            active
99   Admon                             active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
SW-AA#
```

Figura 19.Ejecución show vlan brief SW-CC



```
SW-CC#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   Compras                           active
25   Personal                          active
30   Planta                            active
99   Admon                             active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
SW-CC#
```

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

Tabla 5.Direccionamiento IP VLAN

| 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.

Se realiza la siguiente configuración sobre el puerto Fa0/10 donde se convierte en modo acceso sobre los tres switches.

```
SW-AA(config)#interface fastEthernet 0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10

SW-BB(config)#interface fastEthernet 0/10
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10

SW-CC(config)#interface fastEthernet 0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access 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.

Se realiza la siguiente configuración sobre el puerto Fa0/15 y Fa0/20 donde se convierte en modo acceso y se configura la vlan correspondiente sobre los tres switches.

```
SW-AA(config)#interface fastEthernet 0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#
SW-AA(config-if)#interface fastEthernet 0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30

SW-BB(config)#interface fastEthernet 0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#
SW-BB(config-if)#interface fastEthernet 0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30

SW-CC(config)#interface fastEthernet 0/15
SW-CC(config-if)#switchport mode access
```

SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#
SW-CC(config-if)#interface fastEthernet 0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30

Ahora se muestra configuración realizada sobre los PCs asignando la IP de acuerdo a la tabla.

Figura 20.Configuración IP PCs del SW-AA

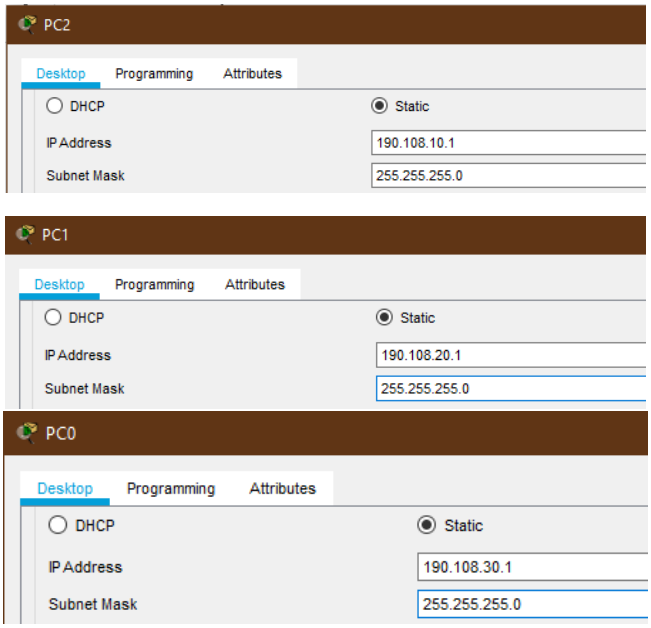
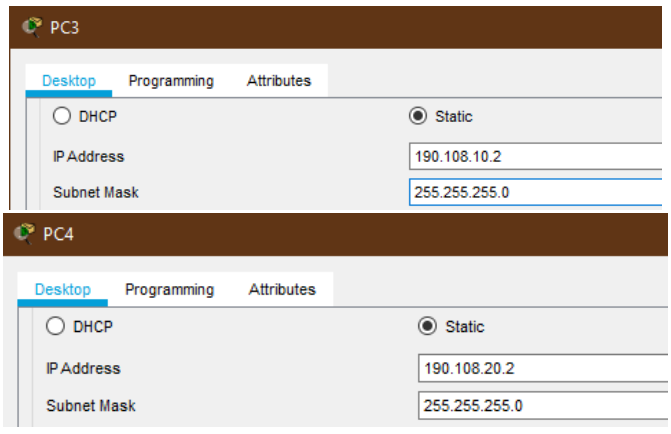



Figura 21.Configuración IP PCs del SW-BB



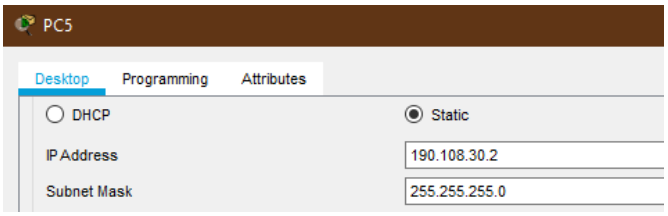
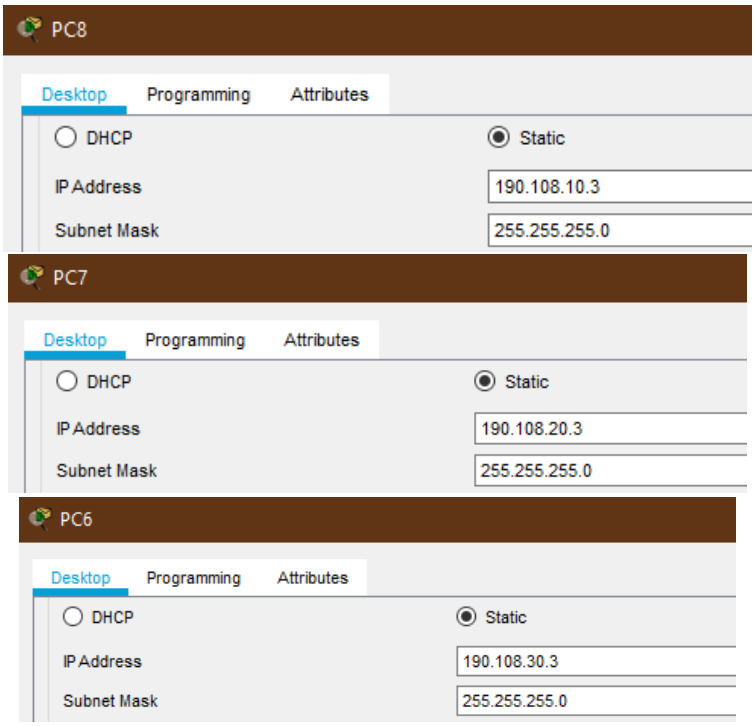



Figura 22.Configuración IP PCs del SW-CC




## 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 6.Direccionamiento IP VLAN 99

| 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 |

Se realiza configuración sobre cada uno de los switches donde se configura la interface VLAN 99 con la ip respectiva de acuerdo a la tabla de direcciones anteriormente indicada.

SW-AA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface vlan 99
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0

SW-BB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#interface vlan 99
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0

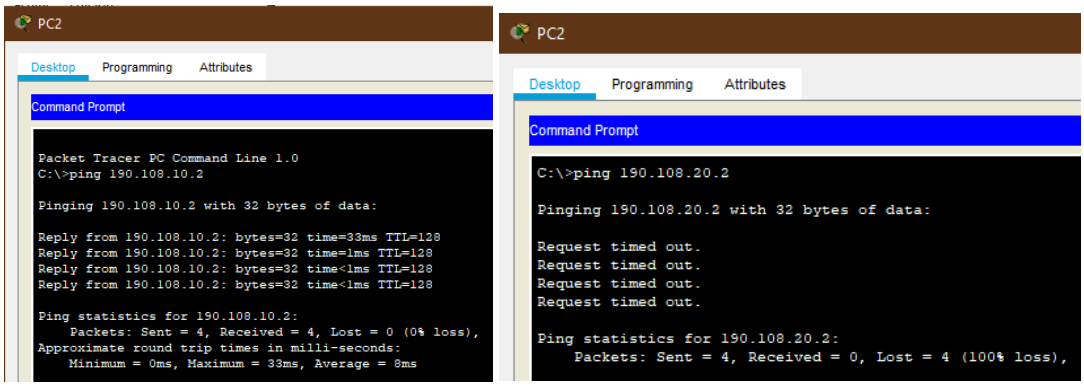
SW-CC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#interface vlan 99
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0

### E. Verificar la conectividad Extremo a Extremo

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

Se logra tener ping exitoso sobre los PCs que se encuentran en la misma VLAN, sin embargo el ping no fue exitoso sobre los PCs que se encuentran en diferentes VLAN esto debido a para que tengan comunicación es necesario un router el cual tiene la función de realizar el enrutamiento de VLAN.

Figura 23.Ping PC2 a PC3, PC4 y PC5



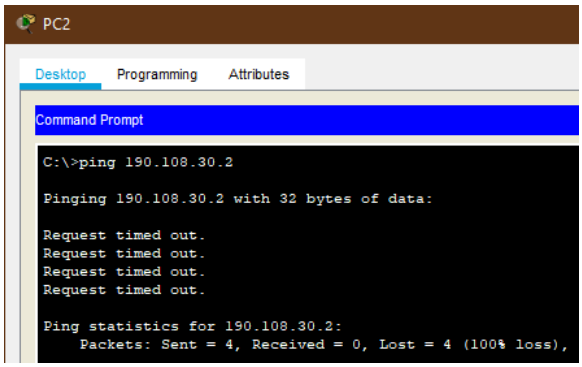
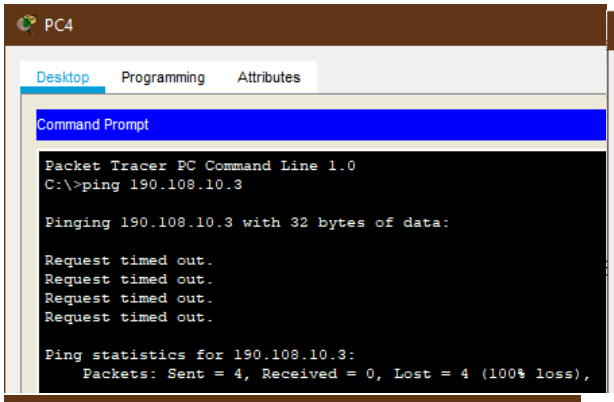
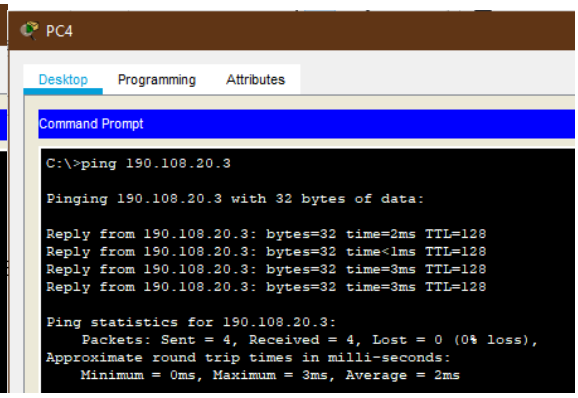



Figura 24.Ping PC4 a PC6, PC7 y PC8



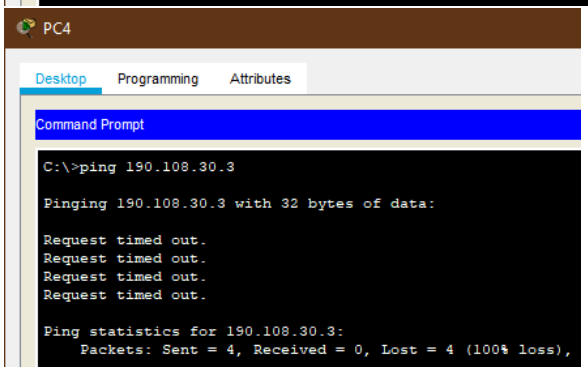
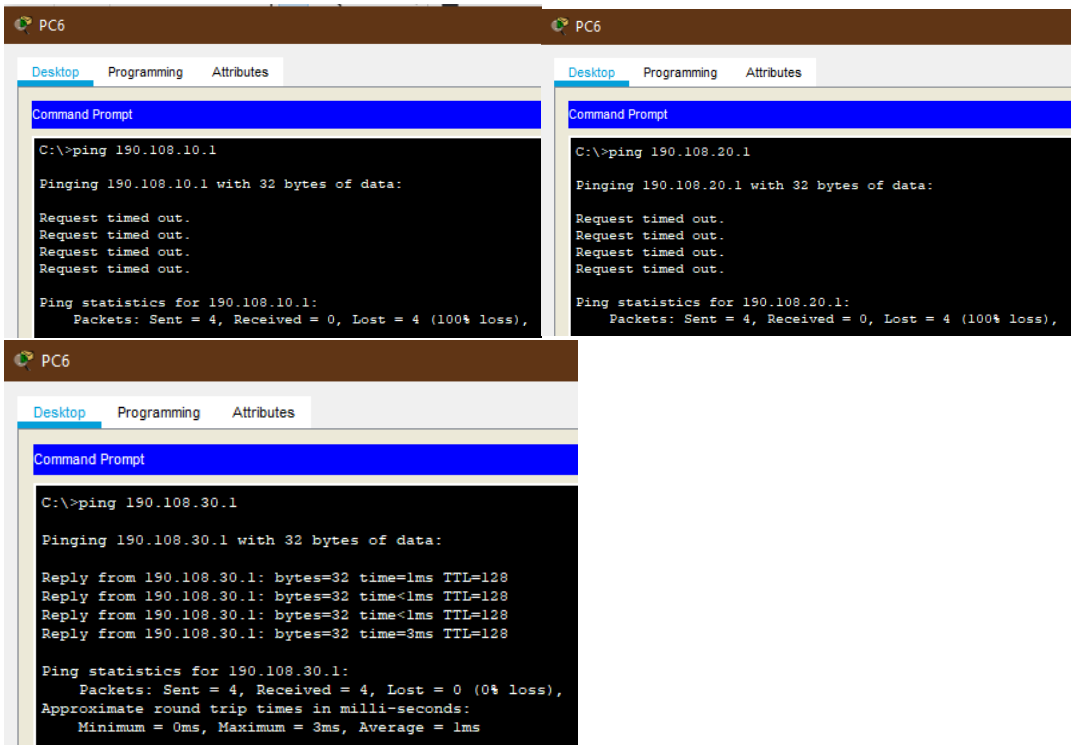



Figura 25.Ping PC6 a PC2, PC1 y PC0




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

Se logra tener ping exitoso sobre desde cada uno de los switch a los demás debido a que las interfaces físicas se encuentran en modo troncal, de igual manera se determinó una VLAN nativa para dichas interfaces con su correspondiente dirección IP.

Figura 26.Ping SW-AA a SW-BB y SW-CC

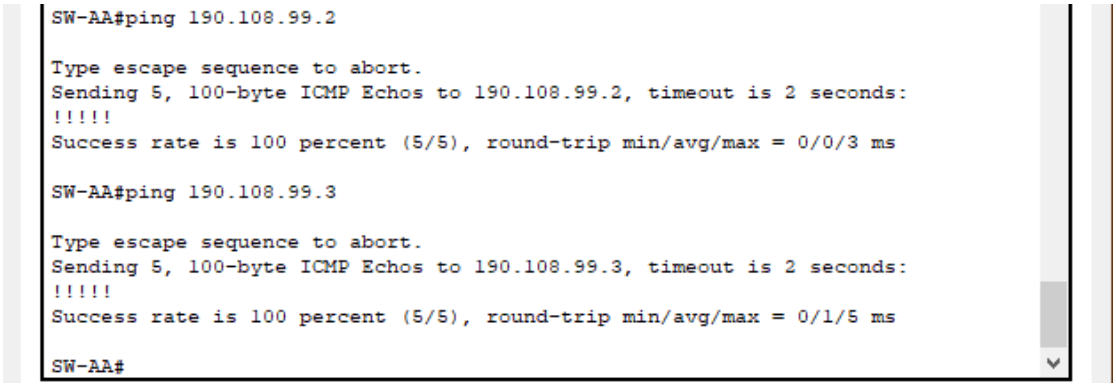


Figura 27.Ping SW-BB a SW-AA y SW-CC

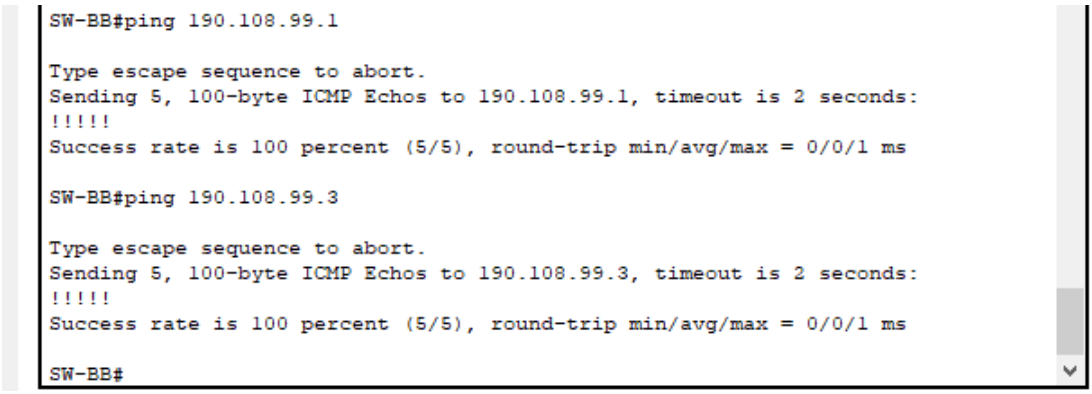
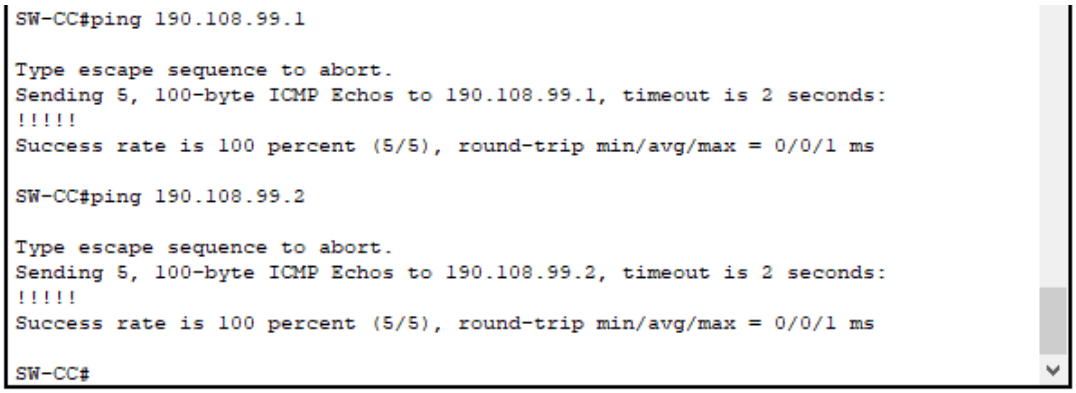



Figura 28.Ping SW-CC a SW-AA y SW-BB




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

No se logra tener ping exitoso de switch a PCs debido a que es necesario el enrutamiento IP entre las VLAN creadas, configurando una dirección IP y una mascaras de subred sobre cada una de las interface VLAN de los switches de tal manera que pertenezcan al mismo segmento de red en el que se encuentran los PC de cada VLAN.

Figura 29.Ping SW-AA a PC0, PC1 y PC2

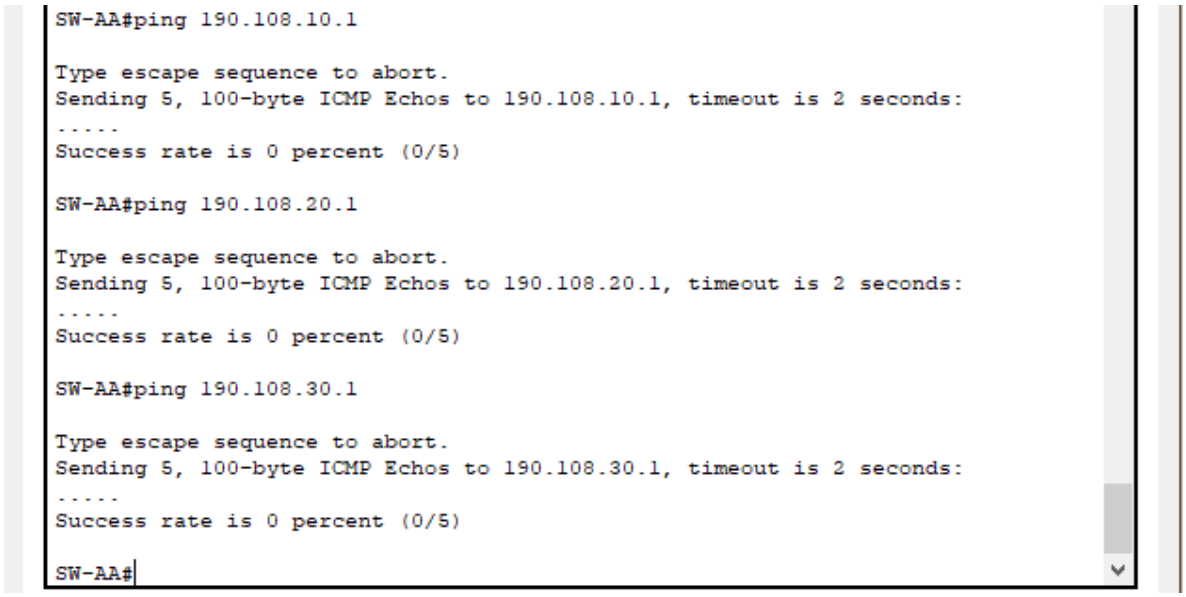



Figura 30.Ping SW-BB a PC3, PC4 y PC5

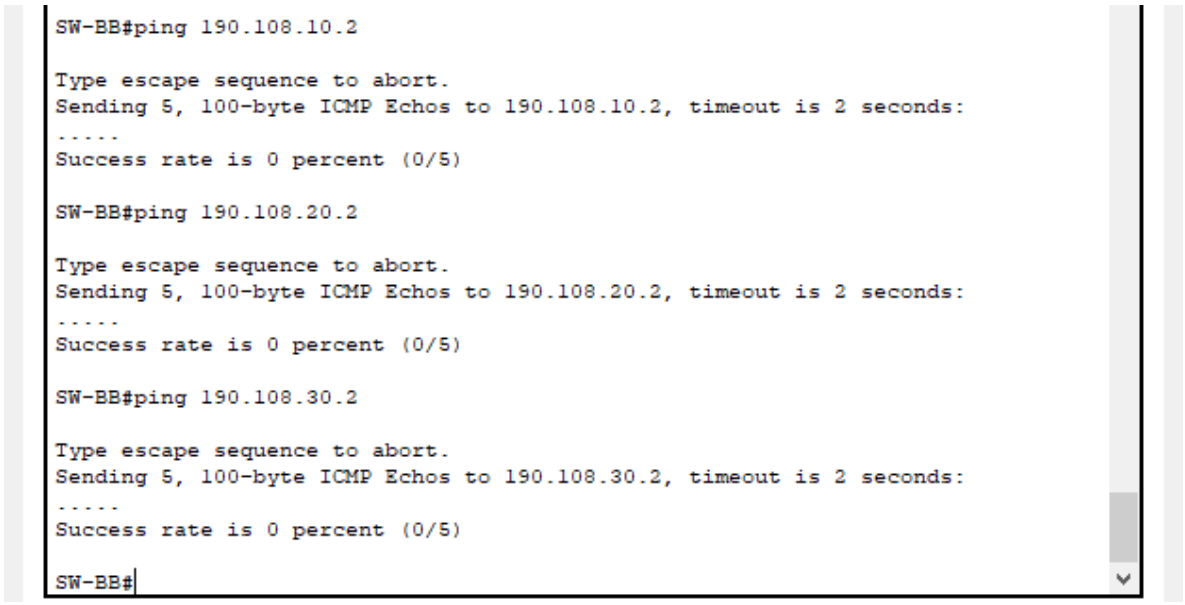
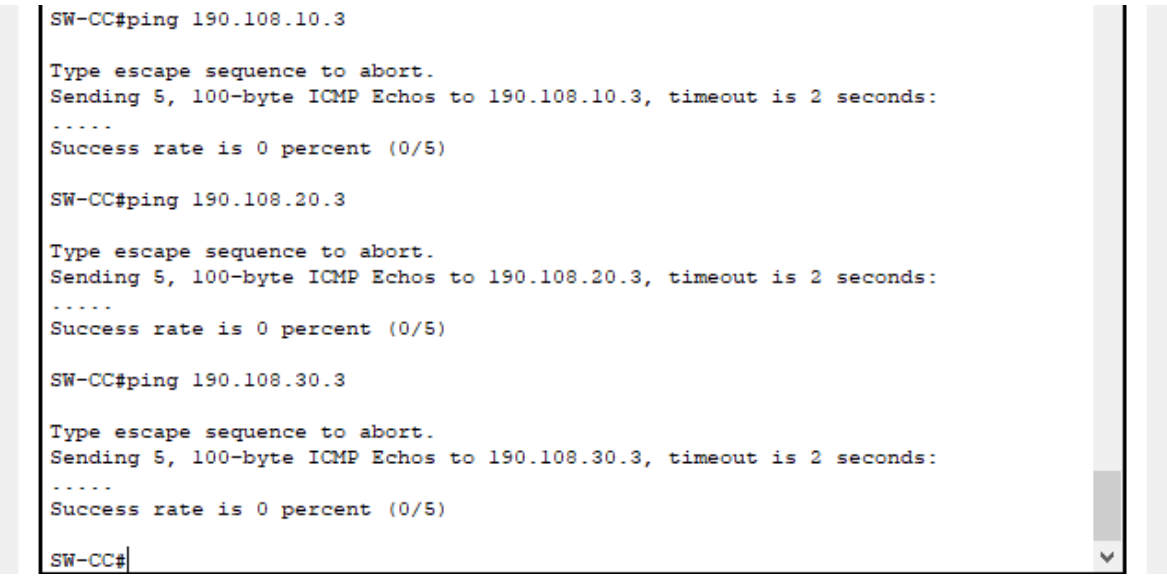


Figura 31.Ping SW-CC a PC6, PC7 y PC8



## CONCLUSIONES

Se aplican los conocimientos teóricos y las habilidades practicas propuestas mediante el uso de herramientas como GNS3 y Packet tracer, donde se realiza configuración de protocolos de enrutamiento como BGP y de mensajería como VTP

Mediante el uso y configuración del protocolo VTP se centralizo y amplifico la administración a un dominio de VLAN, por lo que no fue necesario realizar la configuración de forma manual en cada uno de los switches.

Se realiza configuración de uno de los tres modos en el que opera el protocolo de mensajera VTP el cual fue cliente, este sincroniza la información basándose en los menajes VTP que son recibidos de los servidores que están en el mismo dominio.

## BIBLIOGRAFIA


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

Kent, S., Lynn, C., & Seo, K. (2000). Secure Border Gateway Protocol (S-BGP). IEEE Journal on Selected Areas in Communications, 18(4), 582-592. https://doi.org/10.1109/49.839934

Rey, L. C., Quiñones, T. O. L., & García, W. B. (2014). Protocolos de enrutamiento aplicables a redes MANET. Revista Telemática, 13(3), 59-74.

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