DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ANDREA PAOLA 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

ANDREA PAOLA 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

Quiero agradecer a mi familia, y amigos que me acompañaron y apoyaron a lo largo de este proceso, que aportaron a mi formación tanto profesional como ser humano.

De manera especial a mi tutor y compañeros que con su acompañamiento y orientación hicieron que fuera posible el desarrollo a cabalidad de cada una de las prácticas planteadas, por compartir sus conocimientos y experiencias a lo largo del diplomado.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

BGP Border Gateway Protocol: Es el sistema que utilizan los grandes nodos de Internet para comunicarseentre ellos y transferir una gran cantidad de información entre dos puntos de la Red. Su misión es encontrar elcamino más eficiente entre los nodos para propiciar una correcta circulación de la información en Internet.

VTP Trunking Protocol: un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite centralizar y simplificar la administración en un domino de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos.

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

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

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

RESUMEN

Con el desarrollo de los escenarios correspondientes al diplomado CCNP se tiene como objetivo la implementación de protocolos como BGP que mediante su configuración ayuda para el enrutamiento de los paquetes IP y así identificar los vecinos directamente conectados en las redes, adicional en el desarrollo del segundo escenario se crea una topología de conmutación donde se usara el protocolo VTP propietario de CISCO, el cual mediante su configuración centraliza en un switch la administración de las VLAN, reduciendo la complejidad de la administración y su tráfico, se logra realizar mediante los estados de servidor, el cual permite la creación, eliminación, modificación, anuncia y sincroniza la configuración de los switch, estado cliente solo sincroniza y transparente no participa en VTP.

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

ABSTRACT

With the development of the environments corresponding to the CCNP diploma, the objective is to implement protocols such as BGP, which through its configuration helps to route IP packets and thus identify the neighbors directly connected in the networks, additionally in the development of the second scenario A switching topology is created where the CISCO proprietary VTP protocol is used, which through its centralized configuration in a switch, manages the VLANs, reducing the complexity of the administration and its traffic, it is possible to achieve through the server states, Which allows the creation, allows, modification, announces and synchronizes the configuration of the switches, client state only synchronizes and transparent does not participate in VTP.

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

INTRODUCCION

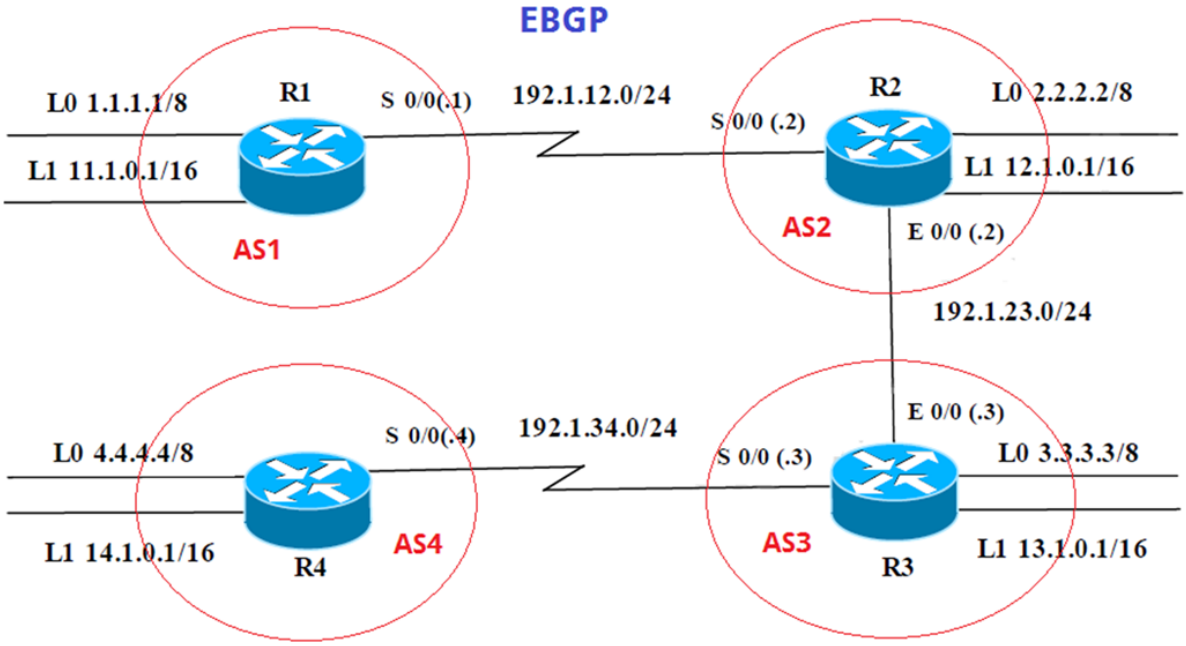
En el presente trabajo se realizara y dará solución a dos escenarios donde se abarcaran temas estudiados durante la presentación del diplomado de profundización CCNP (prueba de habilidades practicas), mediante el desarrollo de prácticas enfocadas al routing y switching poniendo a prueba la comprensión y solución que se le de cada uno de ellos con la aplicación de los conocimientos adquiridos en el transcurso de las unidades vistas.

Posterior a las configuraciones realizadas se hace la verificación del correcto funcionamiento de la topología mediante los comando show y ping.

DESARROLLO

1. ESCENARIO 1

Figura 1.Escenario 1



Información para configuración de los Routers

Tabla 1.Configuracion IP 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.Configuracion IP 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

R2

S 0/0	192.1.12.2	255.255.255.0
E 0/0	192.1.23.2	255.255.255.0

Tabla 3.Configuracion IP R3

R3

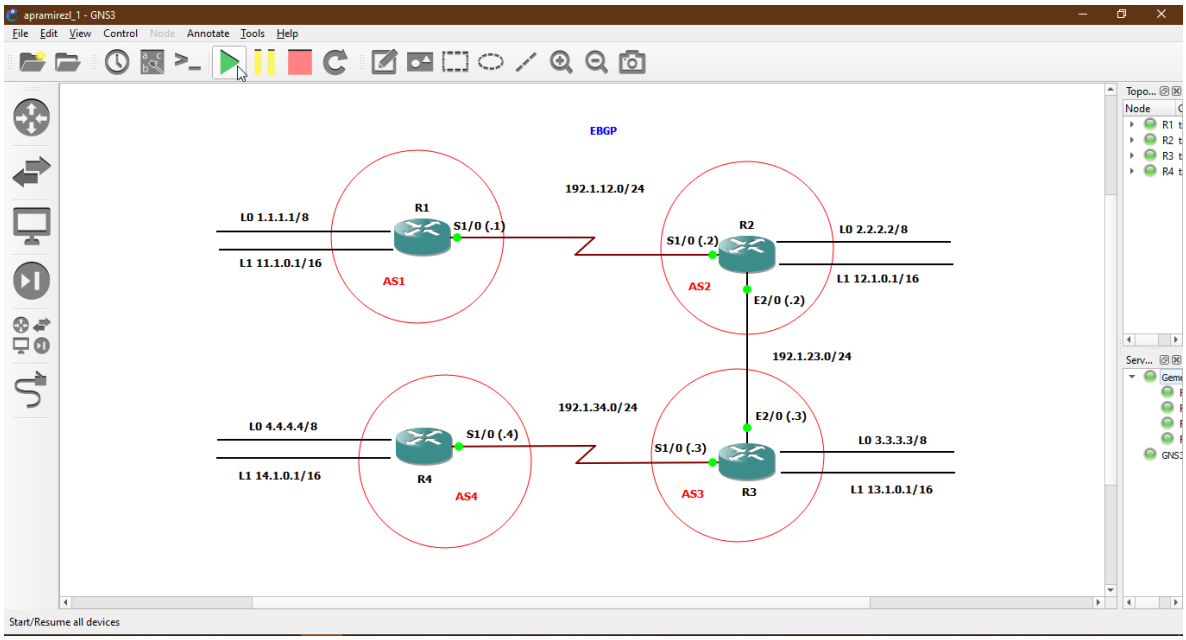
Interfaz	Dirección IP	Máscara
Loopback 0	3.3.3.3	255.0.0.0
Loopback 1	13.1.0.1	255.255.0.0
E 0/0	192.1.23.3	255.255.255.0
S 0/0	192.1.34.3	255.255.255.0

Tabla 4.Configuracion IP 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

Figura 2.Simulación Escenario 1



Antes de dar inicio al desarrollo de los puntos es necesario realizar configuración de cada una de las interfaces en los router de acuerdo a la información de cada una de las tablas.

```
R1(config)#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
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

R2(config)#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)#exit
R2(config)#interface Ethernet 2/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface 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

R3(config)#interface Ethernet 2/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface 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
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
```

```
R4(config)#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
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
```

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 de BGP entre R1 y R2 donde se anuncian direcciones Loopback los ID para R1 y R2, por medio de los siguientes comandos.

```
R1(config)#router bgp 22
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#network 192.1.12.0 mask 255.255.255.0
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)#neighbor 192.1.12.2 remote-as 33
R1(config-router)#exit

R2(config)#router bgp 33
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#network 192.1.12.0 mask 255.255.255.0
R2(config-router)#network 2.0.0.0 mask 255.0.0.0
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
R2(config-router)#neighbor 192.1.12.1 remote-as 22
R2(config-router)#exit
```

Se verifica actualización de las tablas de enrutamiento por medio de las salida del comando show ip route de esta manera se logra evidenciar que tanto R1 y R2 contienen las rutas directamente conectadas y las interfaces Loopback del router vecino.

Figura 3.Verificacion show ip route R1

```
R1#show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.0.0.0/8 is directly connected, Loopback0
L        1.1.1.1/32 is directly connected, Loopback0
B     2.0.0.0/8 [20/0] via 192.1.12.2, 00:05:17
      11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        11.1.0.0/16 is directly connected, Loopback1
L        11.1.0.1/32 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, 00:05:17
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial1/0
L        192.1.12.1/32 is directly connected, Serial1/0
R1#
```

Figura 4.Verificación show ip route R2

```
R2#show ip route
Codes: L - local, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B     1.0.0.0/8 [20/0] via 192.1.12.1, 00:07:58
      2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        2.0.0.0/8 is directly connected, Loopback0
L        2.2.2.2/32 is directly connected, Loopback0
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.12.1, 00:07:58
      12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        12.1.0.0/16 is directly connected, Loopback1
L        12.1.0.1/32 is directly connected, Loopback1
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial1/0
L        192.1.12.2/32 is directly connected, Serial1/0
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, Ethernet2/0
L        192.1.23.2/32 is directly connected, Ethernet2/0
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 relación vecino BGP sobre R2 hacia R3

```
R2(config)#router bgp 33
R2(config-router)#network 192.1.23.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.23.3 remote-as 44
R2(config-router)#exit
```

Ahora se procede a realizar configuración sobre R3 donde se anuncian las direcciones Loopback y se codifica el ID de router

```
R3(config)#router bgp 44
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#network 192.1.23.0 mask 255.255.255.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3(config-router)#network 3.0.0.0 mask 255.0.0.0
R3(config-router)#neighbor 192.1.23.2 remote-as 33
R3(config-router)#exit
```

Se emite nuevamente el comando show ip route donde se observa que las tablas de enrutamiento fueron actualizadas observando que R2 ya contiene las direcciones de Loopback del R3 y en R3 se evidencia sus vecinos directamente conectados.

Figura 5.Verificación show ip route R2

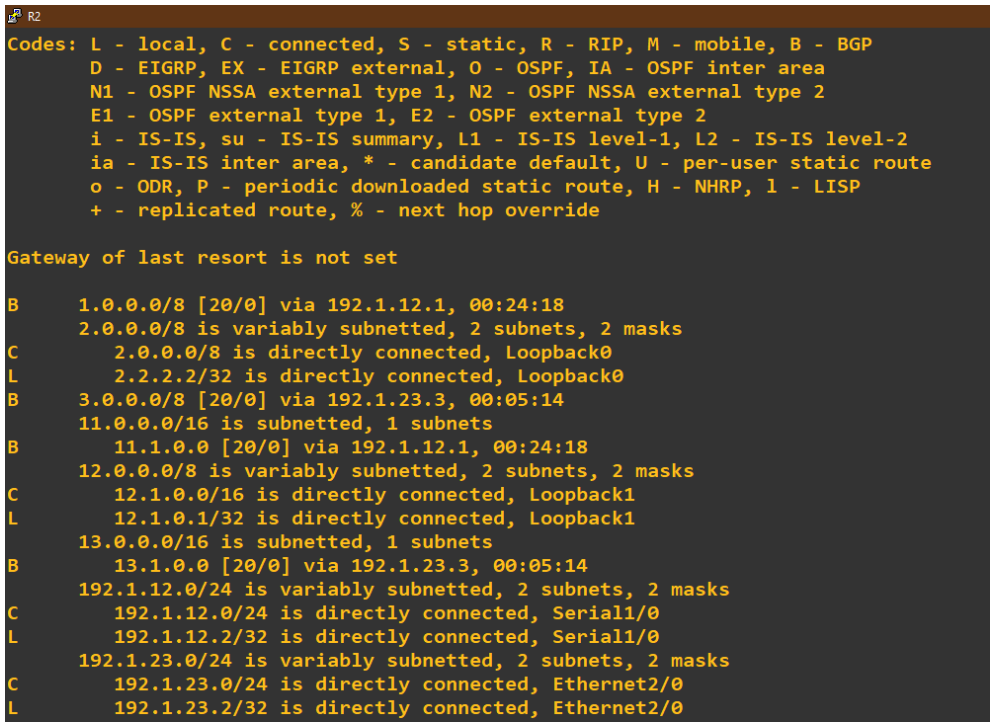
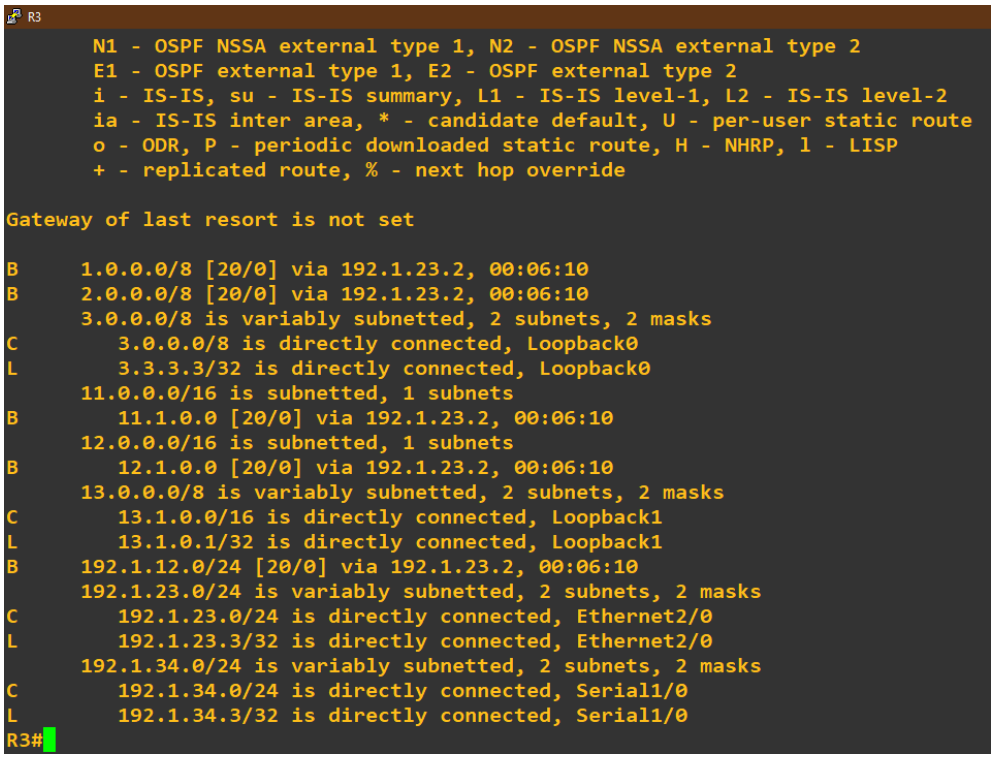


Figura 6.Verificación show ip route R3



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 relación vecino BGP sobre R3 hacia R4

```
R3(config)#router bgp 44
R3(config-router)#network 192.1.34.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.34.4 remote-as 66
R3(config-router)#exit
```

Ahora se realiza configuración sobre R4 donde se anuncian las direcciones Loopback y se codifica el ID de router.

```
R4(config)#router bgp 66
R4(config-router)#bgp router-id 66.66.66.66
R4(config-router)#network 192.1.34.0 mask 255.255.255.0
R4(config-router)#network 14.1.0.0 mask 255.255.0.0
R4(config-router)#network 4.0.0.0 mask 255.0.0.0
R4(config-router)#neighbor 192.1.34.3 remote-as 44
```

Ahora con la siguiente configuración se establecerá las relaciones de vecino en base a las direcciones de Loopback por medio de rutas estáticas.

```
R3(config)#ip route 4.0.0.0 255.0.0.0 192.1.34.4
R3(config)#router bgp 44
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 66
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 66
R4(config-router)#no neighbor 192.1.34.3
R4(config-router)#neighbor 3.3.3.3 remote-as 44
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

A continuación se verifica actualización de las tablas de enrutamiento por medio de la salida del comando show ip route donde se observa que las tablas de enrutamiento fueron actualizadas observando que R3 ahora se conecta hacia R4 por medio de la dirección Loopback 0 configurada como ruta estática y en R4 se evidencia se comunica con los router vecinos por medio de la Loopback de R3.

Figura 7.Verificación show ip route en R3

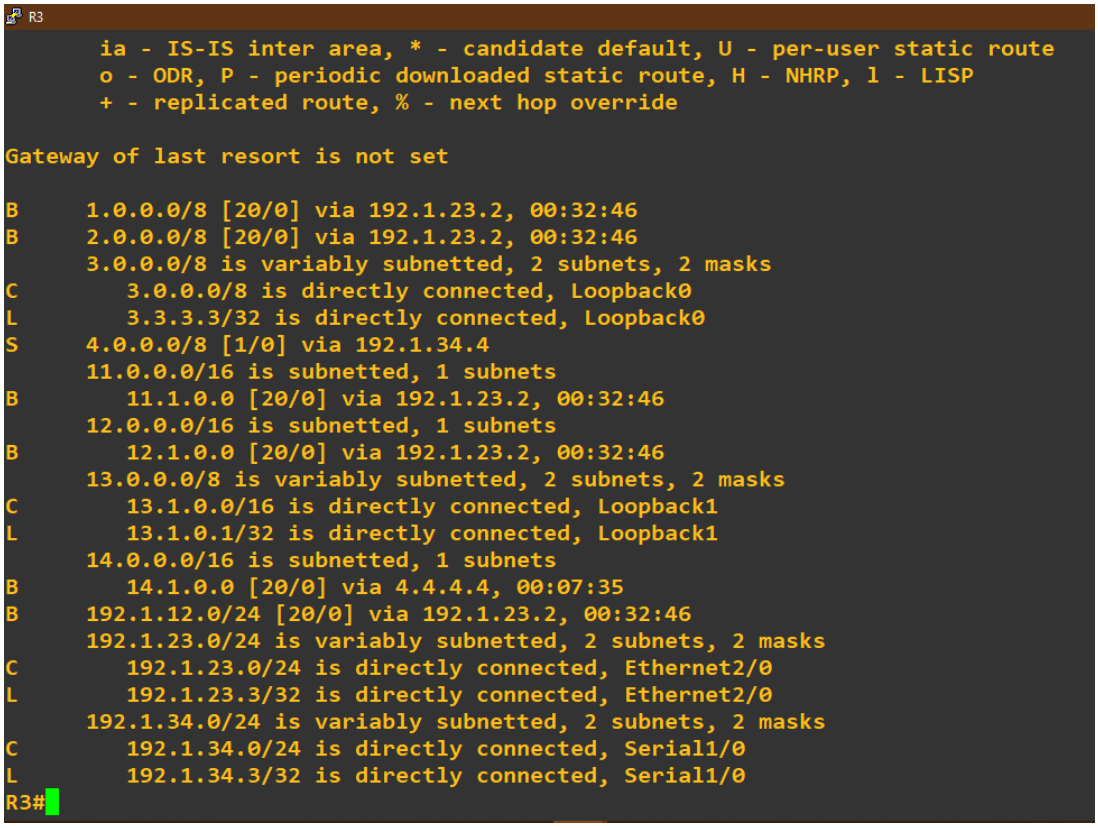
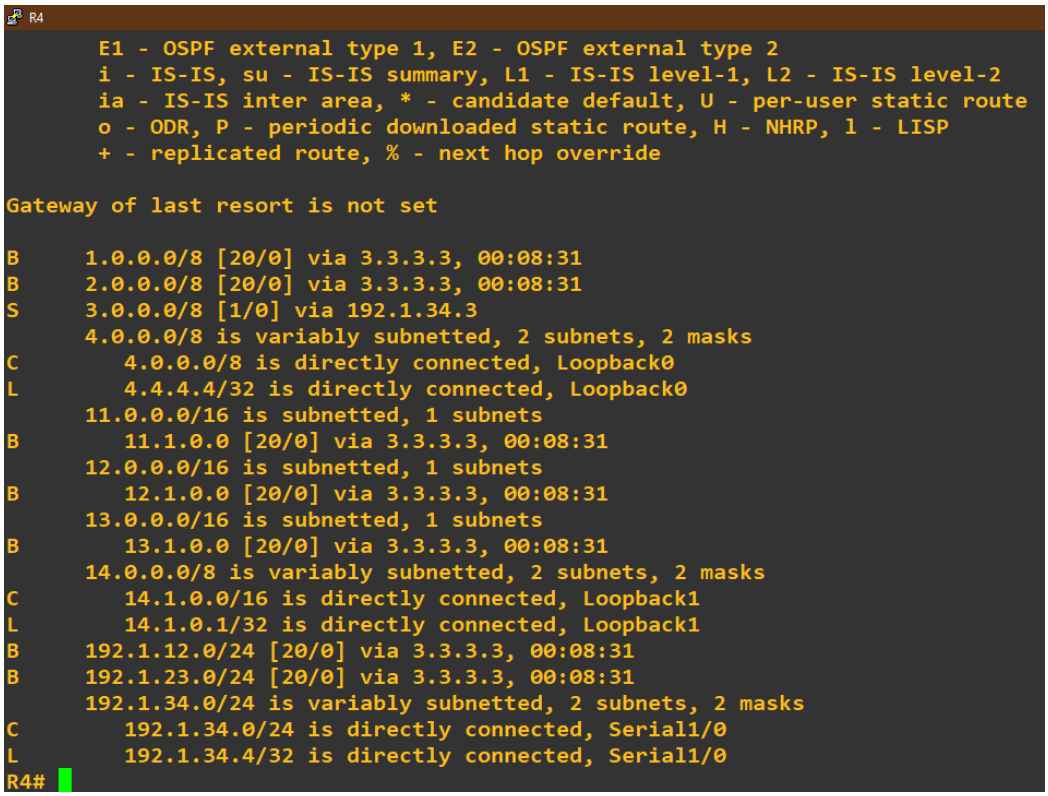


Figura 8.Verificación show ip route en R3



Por medio del comando show ip bgp se mostrara el contenido de la tabla de enrutamiento BGP de igual manera se realiza verificación de la codificación del ID correspondiente para este caso se tomara el R3 y R4.

Figura 9.Salida comando show ip bgp en R3

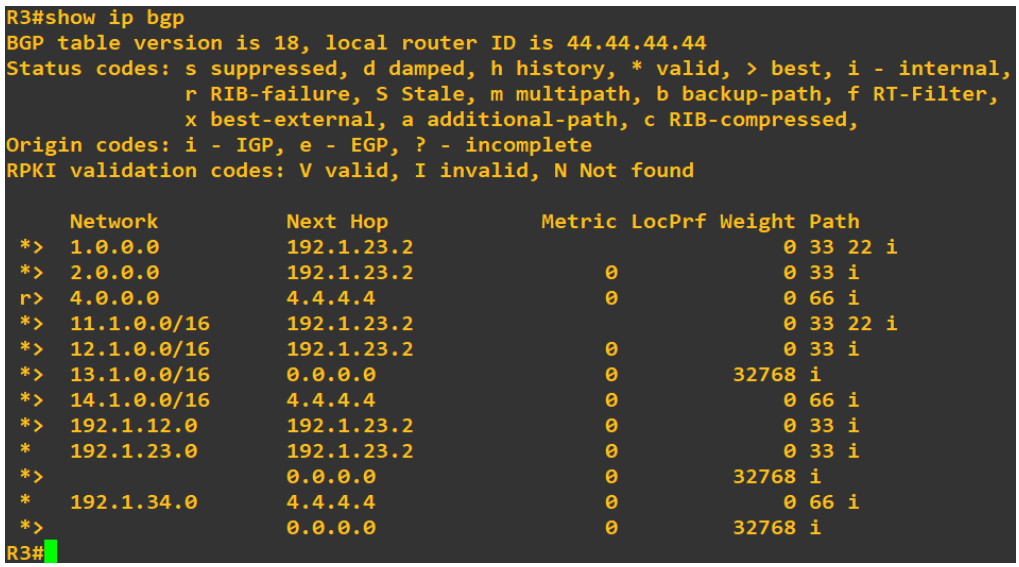
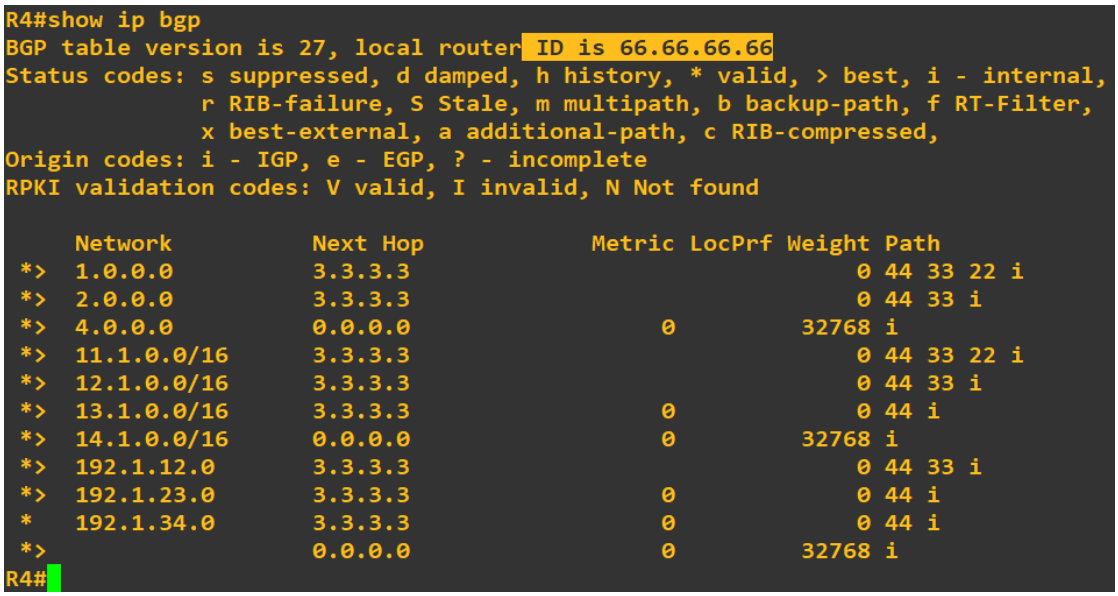


Figura 10.Salida comando show ip bgp en R4



2. ESCENARIO 2

Figura 11.Escenario 2

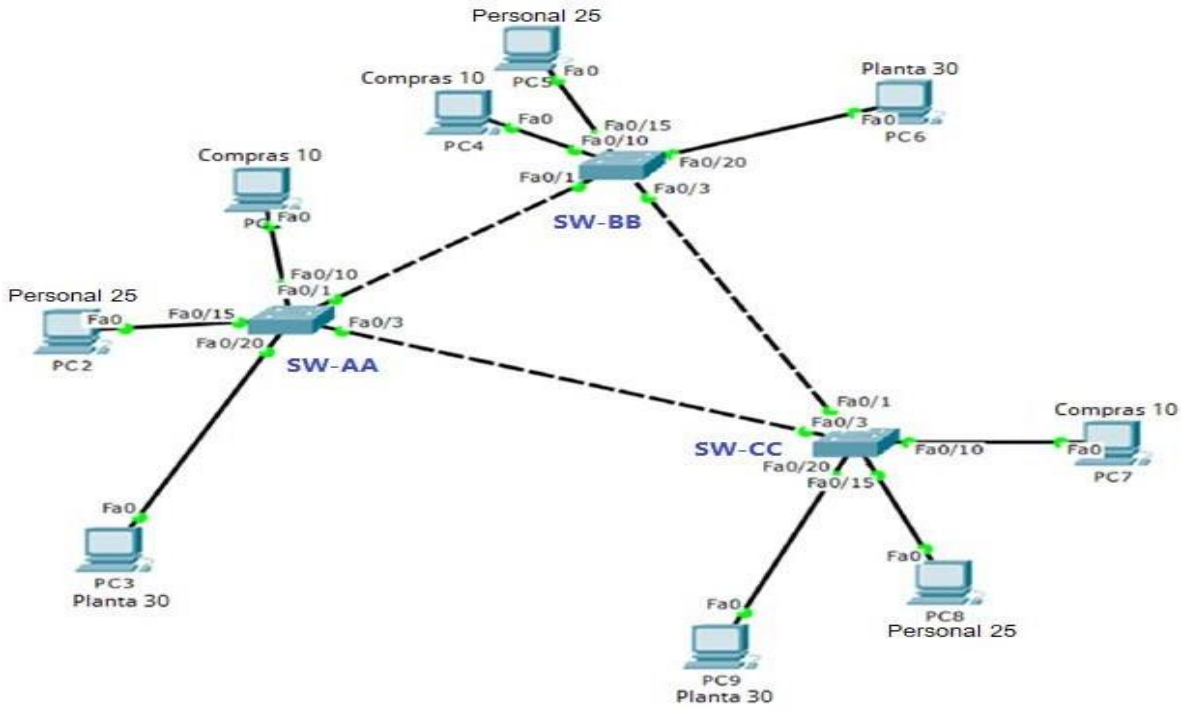
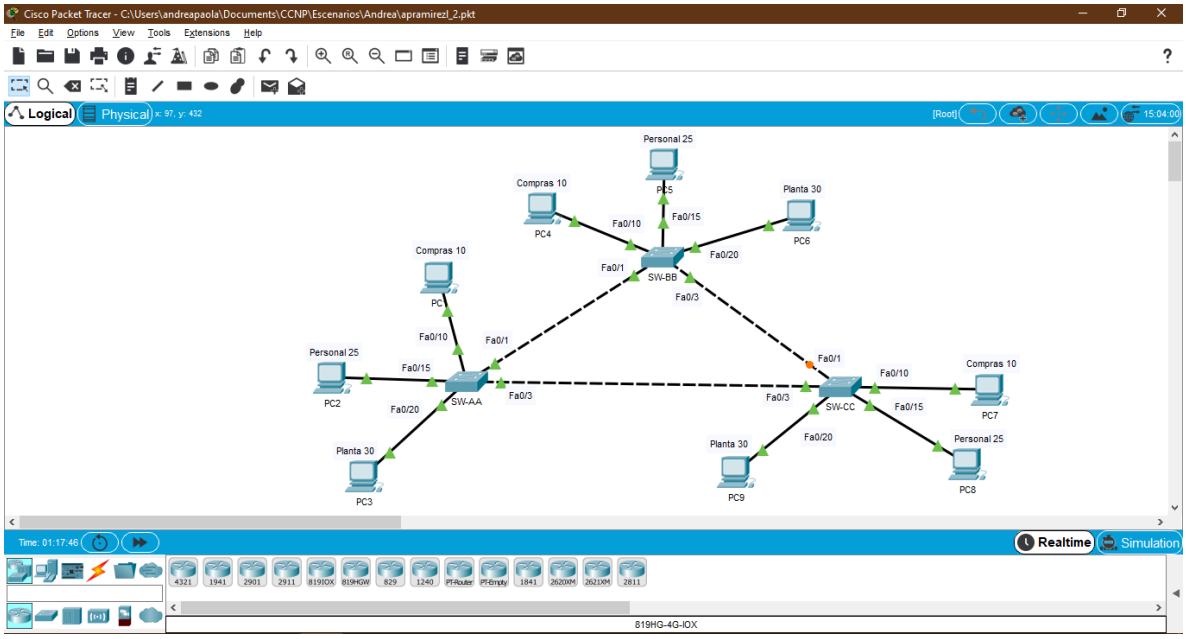


Figura 12.Simulación escenario 2



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 la siguiente línea de comandos se realizara la configuración de VTP en donde el SW-BB trabajara en modo servidor y los otros dos switch trabajaran en modo cliente, de igual manera se realiza configuración del domino indicado.

```
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-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-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 de la salida del comando show vtp status se verifica el estado de la configuración vtp realizada anteriormente en cada uno de los switches.

Figura 13.Salida comando show vtp status SW-AA

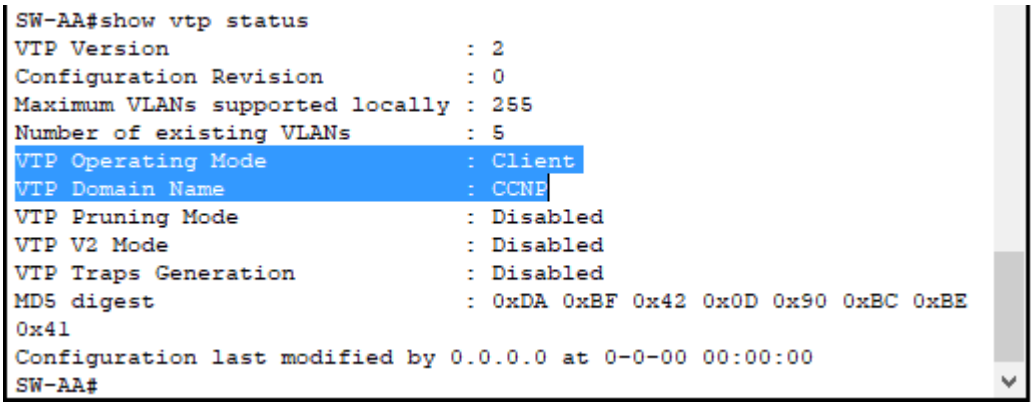


Figura 14.Salida comando show vtp status SW-BB

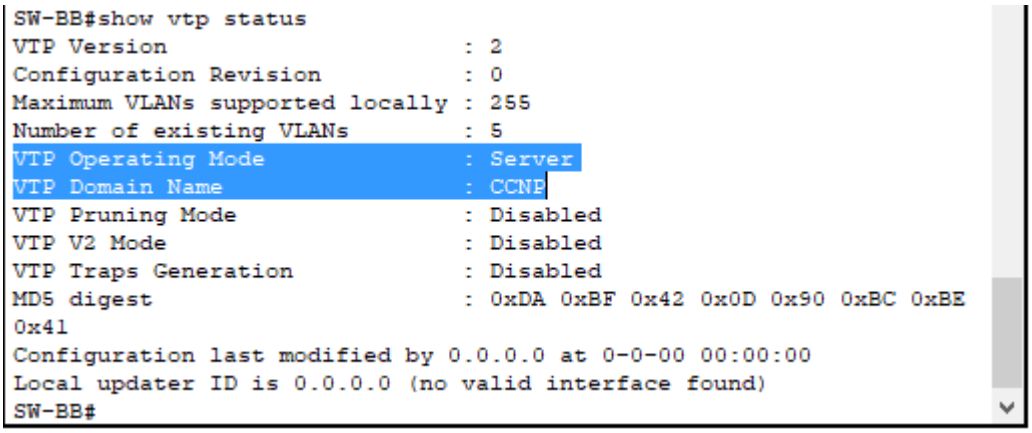
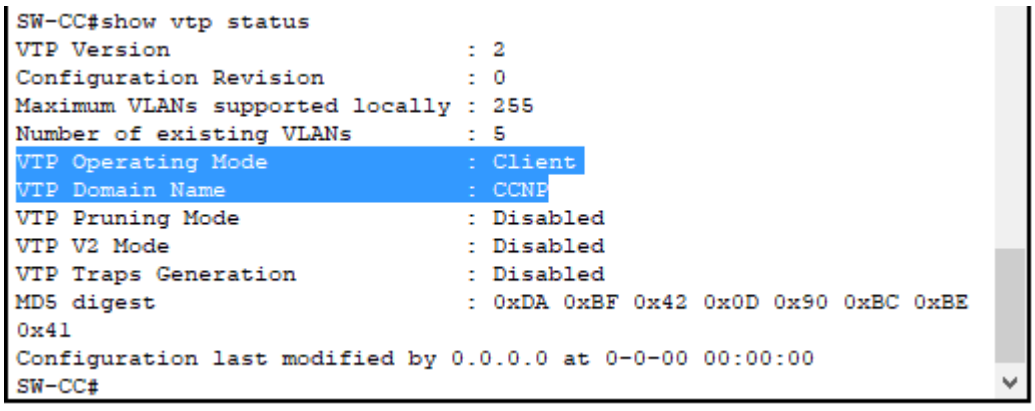


Figura 15.Salida comando show vtp status SW-CC



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***.

Por medio de la siguiente línea de comando se realiza configuración del enlace troncal entre SW-AA y SW-BB.

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***.

Por medio de la salida del comando show interfaces trunk se observara como se encuentra el enlace o interface troncal en SW-AA y SW-BB.

Figura 16.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       1

SW-AA#
```

Figura 17.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#
```

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

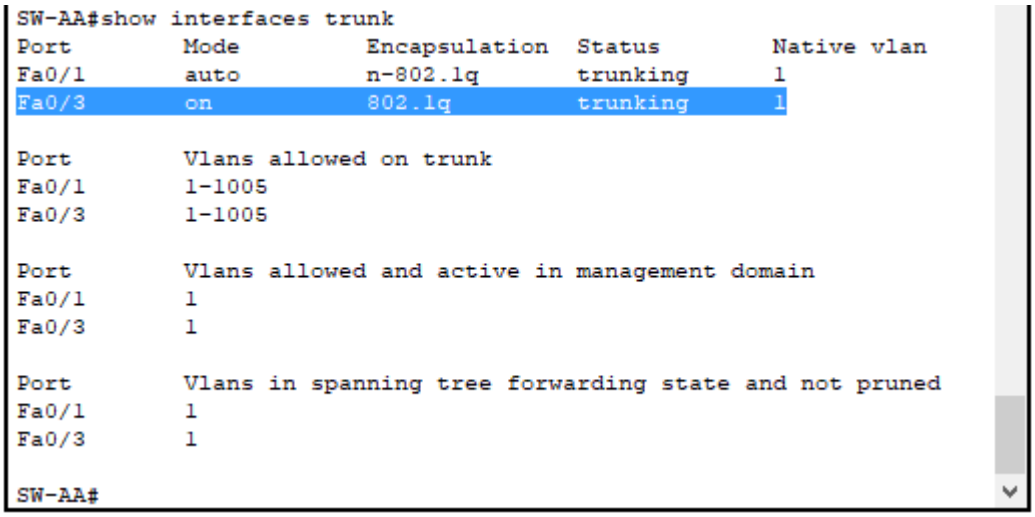
Con la siguiente línea de comando se realizara configuración del enlace troncal sobre la interface Fa0/3 del SW-AA.

```
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.

Ahora se realiza verificación de los enlaces troncales sobre SW-AA para verificar la configuración realizada en el punto anterior por medio del comando show interface trunk.

Figura 18.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
Fa0/3       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/3       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1
Fa0/3       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
Fa0/3       1

SW-AA#
```

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

Se realiza configuración sobre la Fa0/1 del SW-CC configurándolo como enlace troncal por medio de la siguiente línea de comandos.

```
SW-CC(config)#interface fastEthernet 0/1
SW-CC(config-if)#switchport mode trunk
SW-CC(config-if)#exit
```

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 intento de agregación de la VLAN 10 sobre el SW-AA, sin embargo no es posible dado que este switch se encuentra en modo cliente por lo que no permite crear o cambiar la configuración de las VLAN.

```
SW-AA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
SW-AA(config)#exit
```

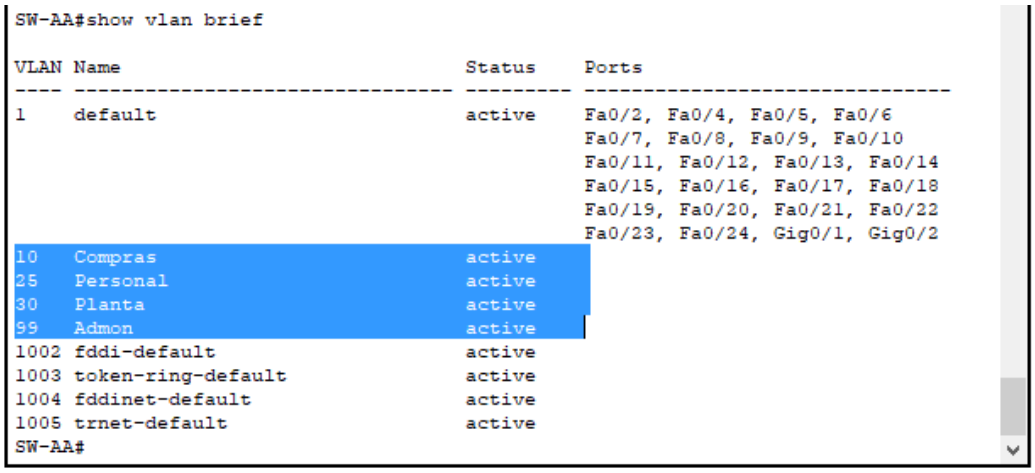
De acuerdo a lo anterior es necesario realizar la configuración de las VLAN sobre el switch que se encuentra en modo servidor que de acuerdo a las configuraciones realizadas de VTP corresponde al SW-BB, debido a que este modo permite la creación, modificación y propagación de la configuración de VLAN.

```
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)#
```

10. Verifique que las VLANs han sido agregadas correctamente.

Por medio de la salida del comando show vlan brief es posible realizar la verificación de la configuración y propagación de las vlan en los switches.

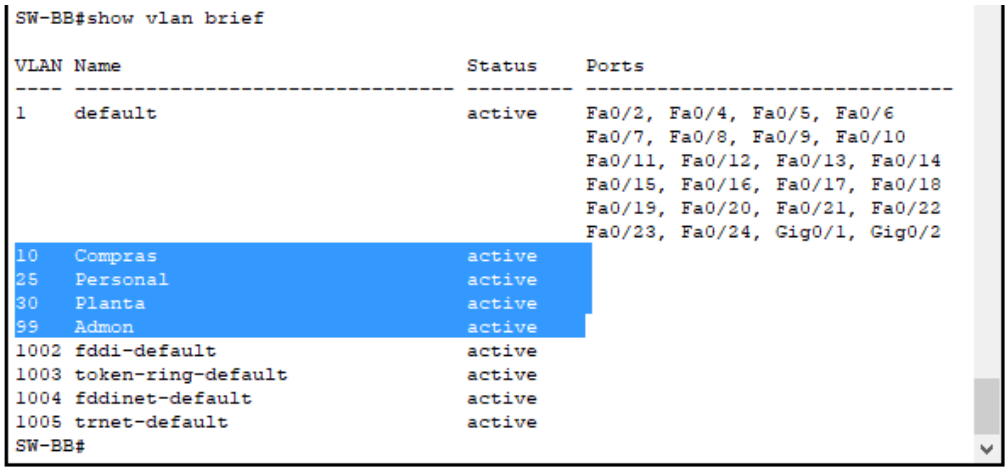
Figura 19.Salida comando show vlan brief SW-AA



```
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#
```

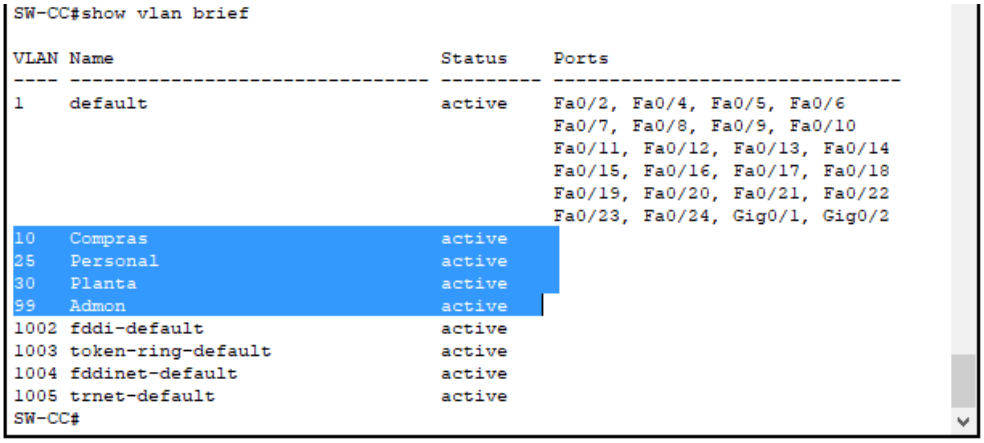
Figura 20.Salida comando show vlan brief SW-BB



```
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 21.Salida comando 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.Direccion 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 configuración del puerto en modo acceso por medio de la siguiente línea de comando sobre los tres swintch.

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

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

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

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 configuración sobre los puertos Fa0/15 y Fa0/20 para los tres switches donde se pasan a modo acceso y se realiza asignación de VLAN correspondientes.

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

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

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

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

Se realiza configuración de IP sobre cada uno de los PC de acuerdo a las VLAN asignadas.

Figura 22.Configuración PC1

Figura 23.Configuración PC2

Figura 24.Configuración PC3

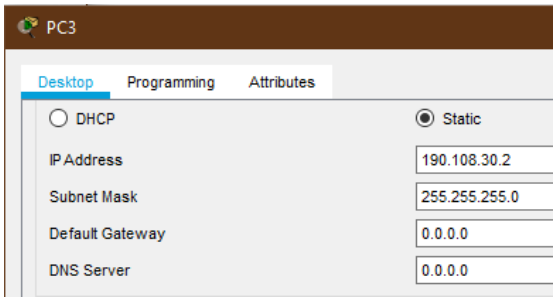


Figura 25.Configuración PC4

Figura 26.Configuración PC5

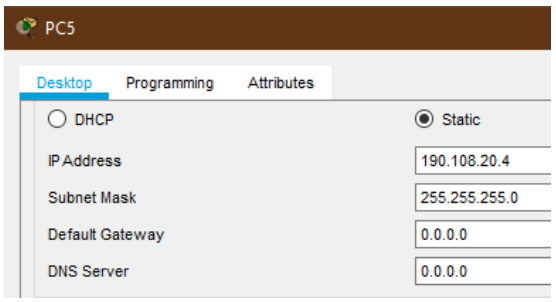


Figura 27.Configuración PC6

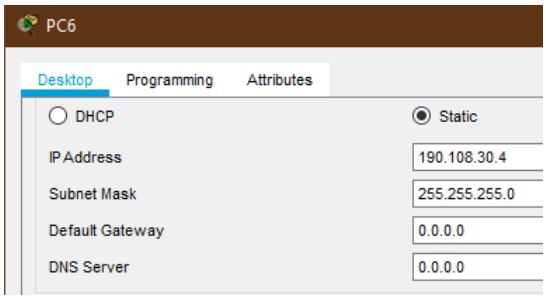


Figura 28.Configuración PC7

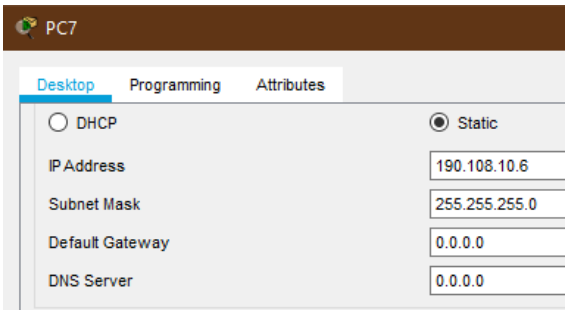


Figura 29.Configuración PC8

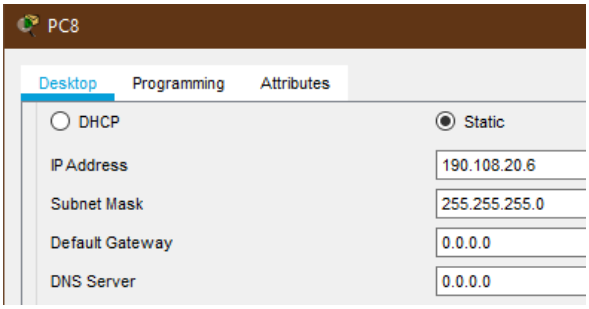
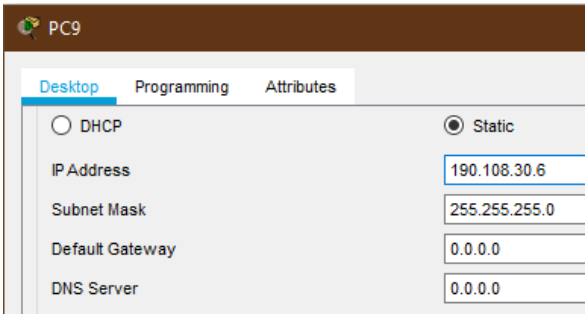


Figura 30.Configuración PC9



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.Dirección 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 de la VLAN 99 con la siguiente línea de comando donde se asigna respectiva IP y se activa la interface.

```
SW-AA#conf t
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-AA(config-if)#exit

SW-BB#conf t
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-BB(config-if)#exit

SW-CC#conf t
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
SW-CC(config-if)#exit
```

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.

Solo se tiene ping con los equipos que comparten la misma VLAN ya que pertenecen a un mismo segmento y requieren sean enrutadas, mientras que para que se tenga comunicación entre VLAN diferentes es necesario la implementación de router el cual tiene la funcionalidad de enrutarlas.

Figura 31.Ping PC1 a PC4

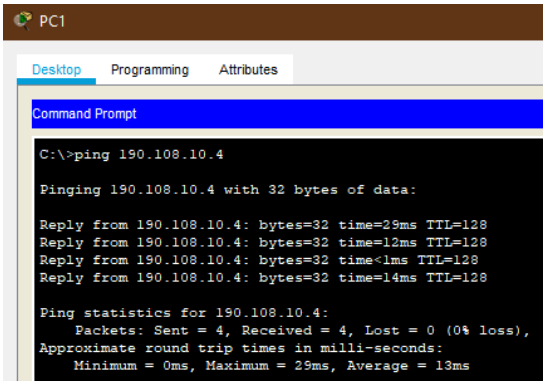


Figura 32.Ping PC2 a PC9

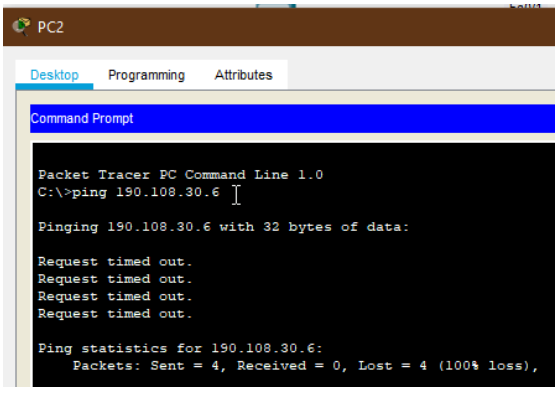


Figura 33.Ping PC3 a PC5

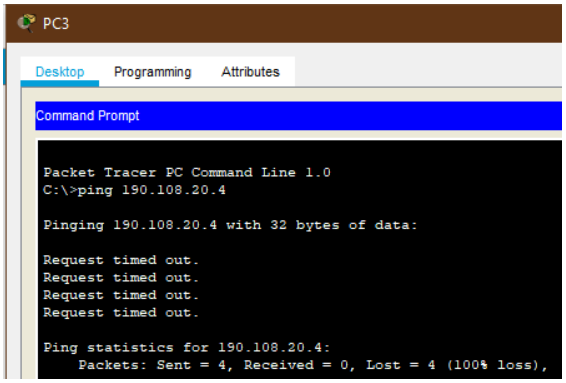
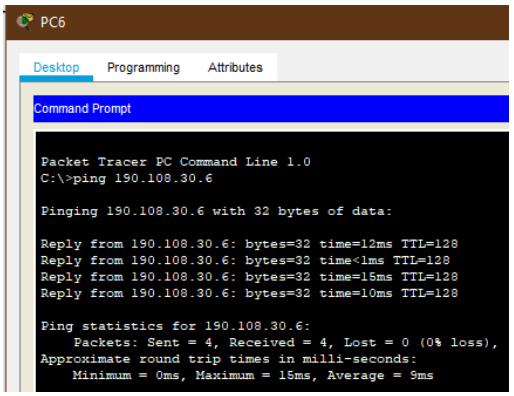


Figura 34.Ping PC6 a PC9



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

Figura 35.Ping SW-AA a SW-BB y SW-CC

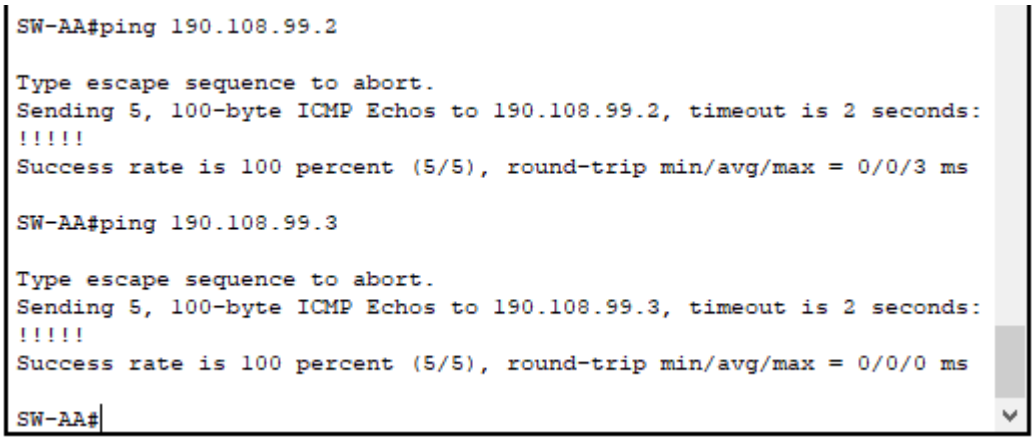


Figura 36.Ping SW-BB a SW-AA y SW-CC

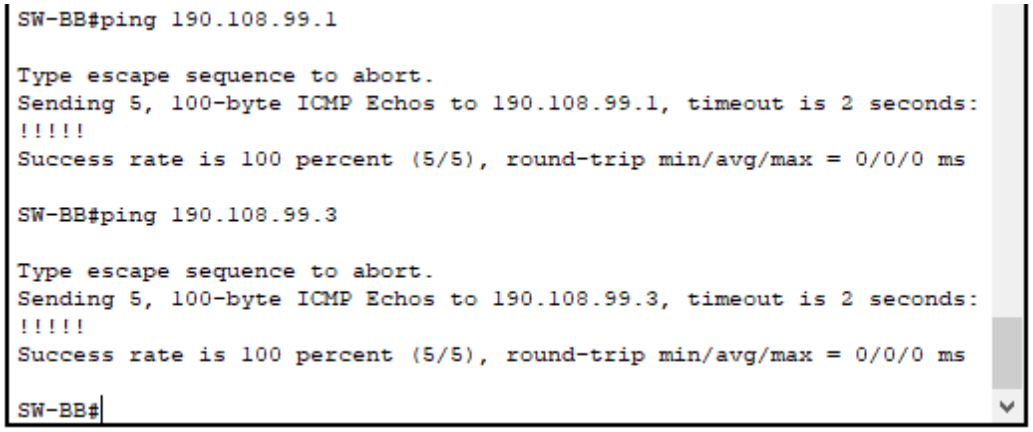
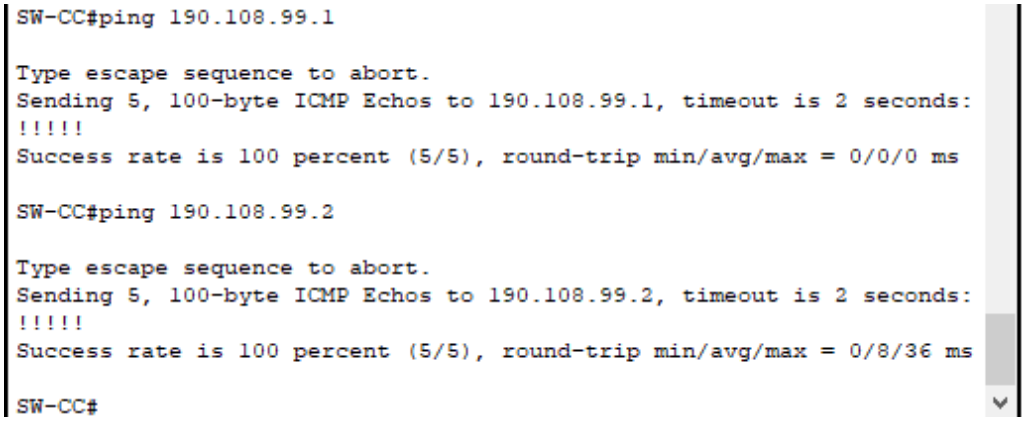


Figura 37.Ping SW-CC a SW-AA y SW-BB



Se presenta ping debido a que anteriormente fueron configuradas las interfaces que conecta a los switches en modo troncal de igual manera se realizó configuración de la VLAN con la que se comunicaran entre ellos.

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

Figura 38.Ping SW-AA a PC1, PC2 y PC3

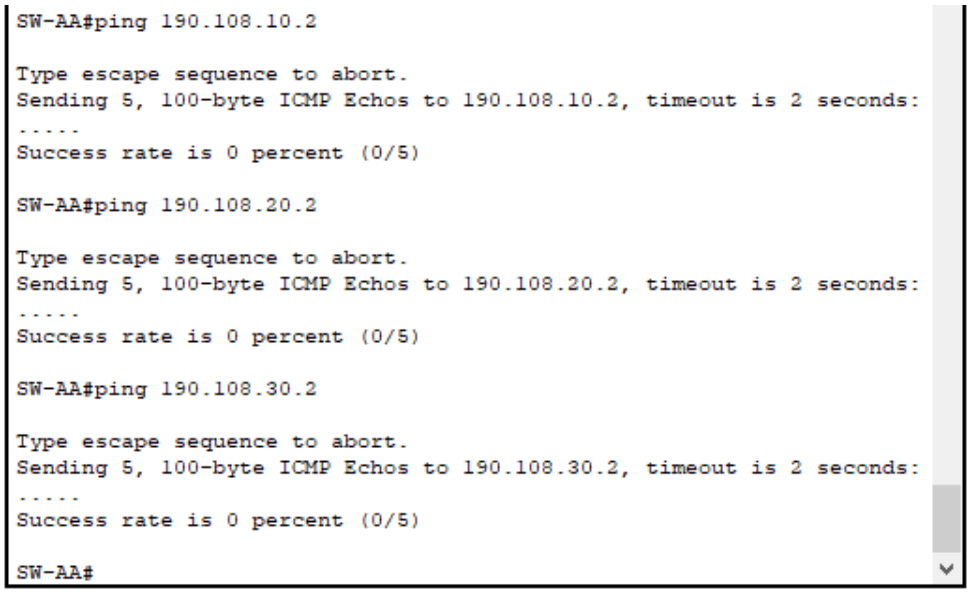


Figura 39.Ping SW-BB a PC5, PC4 y PC6

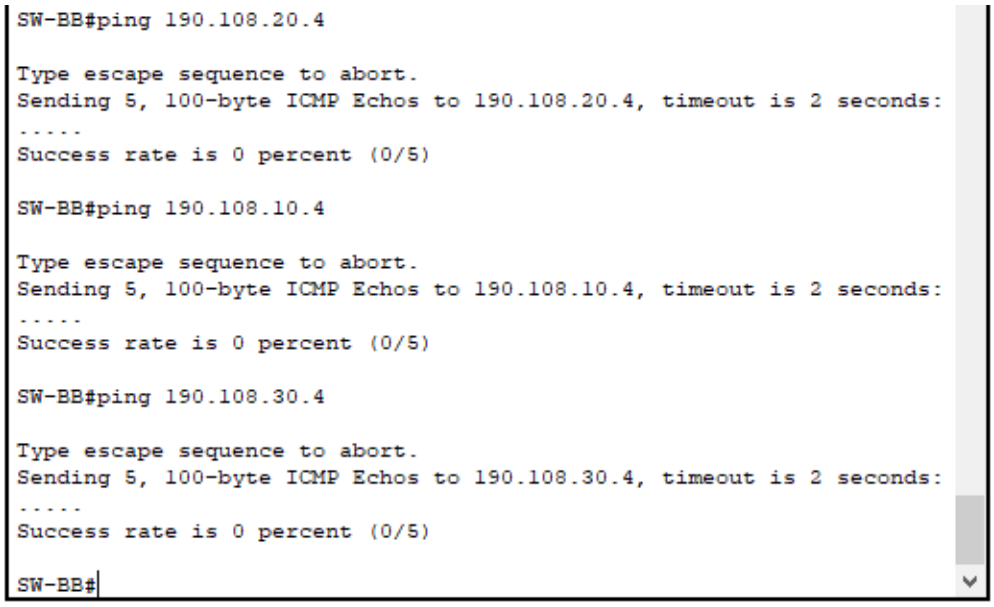
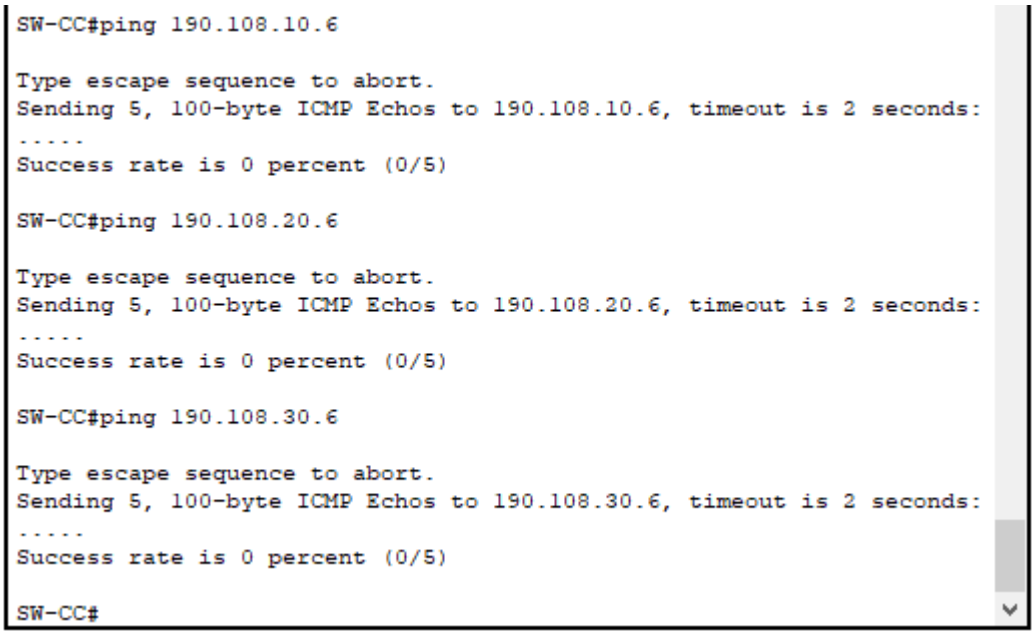


Figura 40.Ping SW-CC a PC7, PC8 y PC9



Los pines no son exitosos debido a que falta realizar la configuración de enrutamiento IP en las VLAN, ya que para esto es necesario habilitar las interfaces de cada VLAN con su dirección IP y mascara subred correspondiente.

CONCLUSIONES

Con las configuraciones realzadas se logra aplica los conocimiento adquiridos durante el curso en cuanto a métricas y requerimientos a tener en cuenta en él envió de tráfico a través de BGP el cual es un protocolo escalable donde crea rutas estables entre las organizaciones, este soporta VLSM, CIDR y sumarización.

Una vez realizada la configuración de VPT se logra validar el funcionamiento de uno de los modos en el que opera este protocolo siendo este el de servidor el cual crea, elimina y modifica VLAN, este anuncia la configuración al resto de los switches que están en el mismo dominio de VTP.

Se logaron identificar fallos mediante la validación de la configuración de los dispositivos de la red, con el uso de los comandos como show running-config, show interface trunk, show vtp status, show ip route entre otros y de eta forma dar solución a los errores.

BIBLIOGRAFIA

4105.pdf. (s. f.). Recuperado 15 de mayo de 2020, de http://www.sistemamid.com/panel/uploads/biblioteca/1/619/672/673/675/4105.pdf

Rabie, S., Aboul-Magd, O., & Mohan, D. (2013). VLAN support of differentiated services (United States Patent N.o US8422500B2). https://patents.google.com/patent/US8422500B2/en

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

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