

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICA CCNP

EDWIN HUMBERTO MASMELA ZAPATA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIA BASICAS, TECNOLOGIA E INGENIERIA – ECBTI
INGENIERIA DE TELECOMUNICACIONES
MEDELLIN
2020

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICA CCNP

EDWIN HUMBERTO MASMELA ZAPATA

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIA BASICAS, TECNOLOGIA E INGENIERIA – ECBTI
INGENIERIA DE TELECOMUNICACIONES
MEDELLIN
2020

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

MEDELLIN, 22 de mayo de 2020

AGRADECIMIENTOS

En primera medida agradecer a Dios por darme la salud y licencia de culminar mis estudios, también dale gracias a mis padres por el apoyo que me brindaron a lo largo de este proceso de formación ya que sin este tal vez me hubiera quedado en el camino y por ultimo pero, no en importancia agradecer a los tutores que brindaron su orientación y acompañamiento en cada uno de los cursos del programa académico, siendo su ayuda de vital importancia para cumplir con las actividades y requisitos exigidos en cada uno de estos.

CONTENIDO

AGRADECIMIENTOS.....	4
LISTA DE TABLAS	7
LISTA DE FIGURAS	8
GLOSARIO	10
RESUMEN.....	12
ABSTRACT.....	12
INTRODUCCIÓN	13
DESARROLLO	14
Escenario 1.....	14
Configuración de interfaces en el router (R1)	16
Configuración de interfaces en el router (R2)	16
Configuración de interfaces en el router (R3)	16
Configuración de interfaces para el router (R4).....	17
Configuración BGP en R1	18
Configuración BGP en R2	18
Relación de vecino entre R1 y R2	19
Configuración BGP en R4	23
Enrutamiento estático en R4	24
Enrutamiento estático en R3	24
Enrutamiento estático en R2.	25
Enrutamiento estático en R1	25
ESCENARIO 2	27
Configurar VTP.....	28
Configuración VTP en SW-AA.....	29
Configuración VTP en SW-BB.....	29
Configuración VTP en SW-BB.....	29
Configurar DTP (Dynamic Trunking Protocol)	31
Configuración de VLAN'S y Asignación de Puertos	33
Configuración de direcciones IP en los switches	36

Verificación de conectividad extremo a extremo	36
Ping entre los PC del Switches.....	36
CONCLUSIONES	45
BIBLIOGRAFÍA.....	46

LISTA DE TABLAS

Tabla 1. Direccionamiento para el Router (R1).....	15
Tabla 2. Direccionamiento para el Router (R2).....	15
Tabla 3. Direccionamiento para el Router (R3).....	15
Tabla 4. Direccionamiento para el Router (R4).....	15
Tabla 5. Información de puertos vlan´s y direccionamiento de host´s	34
Tabla 6. Direccionamiento IP para las SVI asociadas a la VLAN 99 Admon	36
Tabla 7. Direccionamiento IP de SVI en la Vlan 10,25 y 30 para cada switch	38

LISTA DE FIGURAS

Figura 1. Topología del escenario 1	14
Figura 2. Montaje en GNS3 de la topología del escenario 1	14
Figura 3. Ping desde R1 hacia R2	17
Figura 4. Ping desde R2 hacia R1	17
Figura 5. Ping desde R2 hacia R3	17
Figura 6. Ping desde R3 hacia R2	18
Figura 7. Ping desde R3 hacia R4	18
Figura 8. Ping desde R4 hacia R3	18
Figura 9. Tabla de enrutamiento R1	19
Figura 10. Tabla de enrutamiento de R2	19
Figura 11. Relación de vecindad entre R1 y R2.....	20
Figura 12. Relación de vecindad entre R2 y R1.....	20
Figura 13. Tabla de enrutamiento R2	21
Figura 14. Tabla de R3	22
Figura 15. Relación de vecindad entre R2 y R3.....	22
Figura 16. Relación de vecindad entre R3 y R2.....	23
Figura 17. Prueba ping desde R1 hacia interfaces Loopback (R2, R3, R4).....	25
Figura 18. Prueba ping desde R4 hacia interfaces Loopback (R1, R2, R3).....	26
Figura 19. Tabla de enrutamiento de R3	26
Figura 20. Tabla de enrutamiento de R4	27
Figura 21. Topología del escenario 2.....	27
Figura 22. Montaje en GNS3 del escenario 2	28
Figura 23. Verificación configuración VTP SW-AA	30
Figura 24. verificación configuración VTP SW-BB.....	30
Figura 25. Verificación de configuración SW-CC.....	30
Figura 26. Enlace troncal dinámico SW-AA y SW-BB.....	31
Figura 27. Enlace troncal estático entre SW-AA y SW-CC	32
Figura 28. Enlace troncal estático entre SW-BB y SW-CC	32
Figura 29. Verificación de configuración VLAN en SW-BB	33
Figura 30. Propagación de Vlan's por VTP desde SW-BB hacia SW-AA y SW-CC	34
Figura 31. Verificación de asignación de puertos en (SW-AA, SW-BB y SW-CC).35	
Figura 32. Ping entre PC del SW-AA.....	36
Figura 33. Ping entre PC del SW-BB.....	37
Figura 34. Ping entre PC del SW-CC.....	37
Figura 35. Ping 2 Corrección de conectividad entre PC SW-AA.....	39
Figura 36. Ping 2 Corrección de conectividad entre PC SW-BB.....	40

Figura 37. Ping 2 corrección de conectividad entre PC SW-CC	40
Figura 38. Ping entre PC Vlan 10	41
Figura 39. Ping entre PC Vlan 25	41
Figura 40. Ping entre PC Vlan 30	42
Figura 41. Pin entre switch SVI Vlan´s 99.....	42
Figura 42. Ping desde SW-AA hacia PC1, 2 y 3.....	43
Figura 43. Ping desde SW-BB hacia PC4, 5 y 6.....	43
Figura 44. Ping desde SW-CC hacia PC7, 8 y 9.....	43

GLOSARIO

Vlan: Las LANs virtuales (VLANs) son agrupaciones, definidas por software, de estaciones LAN que se comunican entre si como si estuvieran conectadas al mismo cable, incluso estando situadas en segmentos diferentes de una red de edificio o de campus. Es decir, la red virtual es la tecnología que permite separar la visión lógica de la red de su estructura física mediante el soporte de comunidades de intereses, con definición lógica, para la colaboración en sistemas informáticos de redes. Este concepto fácilmente asimilable a grandes trazos implica en la práctica, sin embargo, todo un conjunto de cuestiones tecnológicas. Quizás, por ello, los fabricantes de comunicación LAN se están introduciendo a este nuevo mundo a través de caminos diferentes, complicando aún más su divulgación entre los usuarios. (Castillo Porturas, 2015, pág. 30)

STP (spanning tree protocol): es un protocolo de red operando sobre la capa de enlace del modelo OSI que permite a redes en anillo evitar loops, a la vez, que administra de forma automática las rutas o caminos alternos para alcanzar un destino; ofrece mayor fiabilidad a la red por medio de redundancia de sus rutas de transmisión ante la falla de una de estas rutas. Esto lo hace por medio de cálculos que realiza STP para establecer en la red enlaces únicos libre de loops entre los dispositivos de red, pero manteniendo los enlaces alternos desactivados como reserva, con el fin de activarlos en caso de fallo. El cálculo para establecer los enlaces principales ocurre cada vez que un enlace en la red presenta un cambio de estado. (Bojorquez, 2017, pág. 43)

BGP (Border Gateway Protocol): es un protocolo de enrutamiento cuya función principal es establecer un intercambio de información entre diferentes AS, dicha información incluye una lista de los dominios por los cuales la información transita, la cual es suficiente para construir grafos de conectividad entre los AS, además de hacer cumplir las políticas de administración que se hayan implementado. (Delgado Vallejo, 2010, pág. 9)

DTP(Dynamic Trunking Protocol): protocolo desarrollado por cisco systems que opera entre switches cisco el cual automatiza la configuracion de trunking.

HSRP(Hot Standby Router Protocol): Los protocolos de redundancia permiten configurar una única puerta de enlace predeterminada, haciendo que la configuración del cliente y la comunicación sea más fácil, ya que el host puede utilizar sus protocolos estándar para comunicarse. HSRP cumple esta función a través de un router virtual para todos los hosts, esto se logra usando una ip virtual compartida entre cada uno de los hosts como puerta de enlace. Dicho router virtual cuenta con sus propias direcciones ip y mac. Cuando un host realiza una petición ARP la dirección mac virtual se anuncia. Para los hosts es indiferente el router que los atiende, ellos solo reenvían el tráfico. (Carpio, 2018, pág. 15)

RESUMEN

En el transcurso del proceso de aprendizaje y del desarrollo de las actividades para el programa de telecomunicaciones de la UNAD, se desarrollaron los módulos de cisco correspondiente a CCNA (introducción a las redes, Rutas y conexiones esenciales, escalabilidad de redes y conectividad de redes); llegando de esta manera al diplomando de CCNP el cual tiene como objetivo configurar y resolver los fallos presentes en dos escenarios planteados, enfocados a el routing y switching, aplicando los conocimientos adquiridos en los módulos ya mencionados y haciendo uso de herramientas de simulación como Packet tracer, GNS3 y Smartab las cuales permiten una emulación de situaciones que se pueden presentar en el campo profesional y en el desarrollo de nuestras actividades cotidianas como ingenieros en telecomunicaciones.

Lo anterior nos ayudara a generar la destreza para la solución de problemas en redes de área local LAN o de área extendida WAN otorgándonos experiencia necesaria a nivel de laboratorios para afrontar los requerimientos de posibles clientes o empresas que requieran del servicio profesional de un ingeniero de telecomunicaciones.

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

ABSTRACT

In the course of the learning process and the development of activities for the UNAD telecommunication program, the cisco modules for CCNA (Introduction to Networks, Essential Routes and Connections, Network Scalability and Network Connectivity) were developed; reaching in this way the CCNP diploma which aims to configure and solve the failures present in two proposed scenarios, focused on routing and switching, applying the knowledge acquired in the modules already mentioned and making use of simulation tools such as Packet tracer, GNS3 and Smartab which allow an emulation of situations that may occur in the professional field and in the development of our daily activities as telecommunications engineers.

This will help us to generate the skills for the solution of problems in local area networks LAN or extended area WAN giving us the necessary experience at laboratory level to face the requirements of possible clients or companies that require the professional service of a telecommunication engineer.

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

INTRODUCCIÓN

Con el desarrollo de los escenarios propuestos para el presente diplomado de profundización se pretende abordar los temas concernientes a routing y switching entre dispositivos cisco, siguiendo la línea de los laboratorios propuestos a lo largo de los módulos (Route y Switch), presentando el paso a paso de las configuraciones para dar solución a cada uno de los puntos solicitados para el escenario 1 y 2.

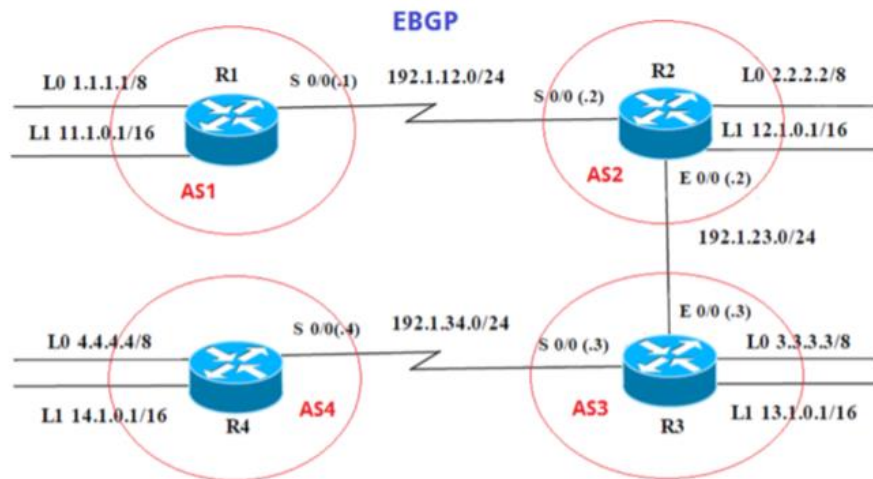
De igual manera a medida que se desarrollen y apliquen las configuraciones se irán sustentando los resultados obtenidos haciendo uso de los comandos de verificación “**show**” y pruebas de conectividad vía ping entre los dispositivos, cada una de las pruebas y verificaciones tendrá previamente consignados los comandos empleados para la configuración de los equipos.

Una vez realizadas las pruebas solicitadas en la guía para el avance del paso a paso de cada uno de los escenarios, y si estas no arrojan los resultados esperados de acuerdo a las configuraciones realizadas, se verificarán las mismas aplicando los ajustes necesarios para llegar a la solución de posibles problemas consignando nuevamente las pruebas y sustentando el efecto de los cambios efectuados y el motivo del éxito o no de dichas pruebas.

DESARROLLO

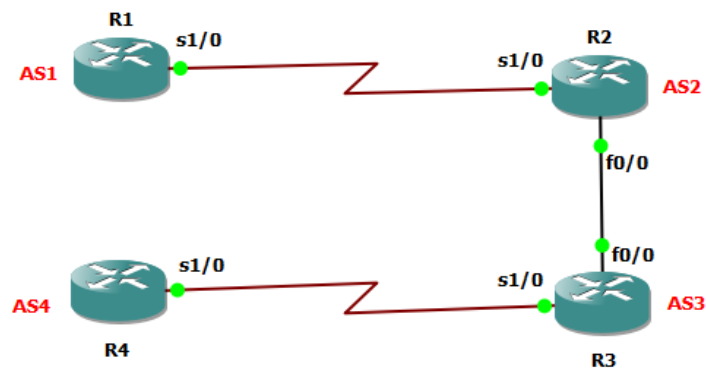
Escenario 1

Figura 1. Topología del escenario 1



Para desarrollar el escenarios se trabajara con el software de simulación GNS3 v.3 y routers C7200 a continuación el ilustra el resultado de la topología obtenida en este simulador para el escenario 1.

Figura 2. Montaje en GNS3 de la topología del escenario 1



La etiqueta de las interfaces seriales cambia debido a la referencia del router utilizado; a continuación se muestra la información para la configuración inicial de los routers.

Tabla 1. Direccionamiento para el Router (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 1/0	192.1.12.1	255.255.255.0

Tabla 2. Direccionamiento para el Router (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 1/0	192.1.12.2	255.255.255.0
E 0/0	192.1.23.2	255.255.255.0

Tabla 3. Direccionamiento para el Router (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 1/0	192.1.34.3	255.255.255.0

Tabla 4. Direccionamiento para el Router (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 1/0	192.1.34.4	255.255.255.0

Antes de iniciar con el desarrollo y la configuración de BGP entre los sistemas autónomos AS que se muestran en las topologías es necesario aplicar la configuración de direccionamiento de acuerdo a las tablas anteriormente

relacionadas y suministradas para el presente escenario para lo cual se emplearon al siguiente serie de comandos en cada uno de los router.

Configuración de interfaces en el router (R1)

```
R1# configure terminal
R1(config)#interface s1/0
R1(config if)# ip address 192.1.12.1 255.255.255.0
R1(config if)# no sh
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
```

Configuración de interfaces en el router (R2)

```
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 s1/0
R2(config if)#ip address 192.1.12.2 255.255.255.0
R2(config if)#no sh
R2(config if)#exit
R2(config)#interface fastEthernet 0/0
R2(config if)#ip address 192.1.23.2 255.255.255.0
R2(config if)#no sh
R2(config if)#exit
R2(config)#
```

Configuración de interfaces en el router (R3)

```
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)#ip address 192.1.23.3 255.255.255.0
R3(config if)#no sh
```



```

R3(config if)#exit
R3(config)#interface s1/0
R3(config if)#ip address 192.1.34.3 255.255.255.0
R3(config if)#no sh
R3(config if)#exit
R3(config)#

```

Configuración de interfaces para el router (R4)

```

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 s1/0
R4(config if)# ip address 192.1.34.4 255.255.255.0
R4(config if)#no sh
R4(config if)#exit
R4(config)#

```

Para verificar que la configuración es correcta se realizan pruebas de conectividad vía ping entre las conexiones directas de los routers.

Figura 3. Ping desde R1 hacia R2

```

R1#ping 192.1.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.12.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/31/56 ms
R1#

```

Figura 4. Ping desde R2 hacia R1

```

R2#ping 192.1.12.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.12.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/51/88 ms
R2#

```

Figura 5. Ping desde R2 hacia R3

```

R2#ping 192.1.23.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.23.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/74/188 ms
R2#

```

Figura 6. Ping desde R3 hacia R2

```
R3#ping 192.1.23.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.23.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/55/136 ms
R3#
```

Figura 7. Ping desde R3 hacia R4

```
R3#ping 192.1.34.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.34.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/42/48 ms
R3#
```

Figura 8. Ping desde R4 hacia R3

```
R4#ping 192.1.34.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.34.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/46/88 ms
R4#
```

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

Configuración BGP en R1

Para la configuración de BGP en R1 es necesario aplicar la siguiente serie de comandos.

```
R1#configure terminal
R1(config)#router bgp 1
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#network 1.0.0.0
R1(config-router)#network 11.1.0.0
R1(config-router)#network 192.1.12.0 255.255.255.0
```

Configuración BGP en R2

```
R2#configure terminal
```

```

R2(config)#router bgp 2
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#network 2.0.0.0
R2(config-router)#network 12.1.0.0
R2(config-router)#network 192.1.12.0

```

Relación de vecino entre R1 y R2

Para establecer una relación de vecino entre estos dos dispositivos se deben ejecutar los siguientes comandos en R1 y R2 respectivamente:

```

R1#configure terminal
R1(config)#router bgp 1
R1(config-router)#neighbor 192.1.12.2 remote-as 2
-----
R2#configure terminal
R2(config)#router bgp 2
R2(config-router)#neighbor 192.1.12.1 remote-as 1

```

Se verifica que se hayan establecido las adyacencias de vecindad entre los dos router revisando la información de la tabla de enrutamiento en cada uno de ellos empleando el comando **show ip route** y **show ip bgp neighbors**

Figura 9. Tabla de enrutamiento 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, I - ISIS
       + - 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, 00:00:20
B    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
C    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

```

Figura 10. Tabla de enrutamiento de 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, I - ISIS
       + - 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, 00:00:40
B    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
C    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
C    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
C    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks

```

Nótese como tanto R1 como R2 anuncian las redes de las direcciones de loopback en la información de las tablas de enrutamiento lo cual nos permite certificar que se ha establecido las adyacencias y las relaciones de vecindad BGP entre los dos routers.

Figura 11. Relación de vecindad entre R1 y R2

```
R1#show ip bgp neighbors
BGP neighbor is 192.1.12.2, remote AS 2, external link
BGP version 4, remote router ID 33.33.33.33
BGP state = Established, up for 00:00:44
Last read 00:00:44, last write 00:00:44, hold time is 180, keepalive interval is 60 seconds
Neighbor sessions:
  1 active, is not multisession capable (disabled)
Neighbor capabilities:
  Route refresh: advertised and received(new)
  Four-octets ASN Capability: advertised and received
  Address family IPv4 Unicast: advertised and received
  Enhanced Refresh Capability: advertised and received
  Multisession Capability:
  Stateful switchover support enabled: NO for session 1
Message statistics:
  InQ depth is 0
  OutQ depth is 0

             Sent       Rcvd
Opens:         1         1
Notifications:  0         0
Updates:        0         0
Keepalives:     1         1
Route Refresh:  0         0
Total:          2         2
Default minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
Session: 192.1.12.2
BGP table version 27, neighbor version 23/27
Output queue size : 0
Index 3, Advertise bit 0
3 update-group member
Slow-peer detection is disabled
Slow-peer split-update-group dynamic is disabled
```

Figura 12. Relación de vecindad entre R2 y R1

```
R2#show ip bgp neighbors
BGP neighbor is 192.1.12.1, remote AS 1, external link
BGP version 4, remote router ID 22.22.22.22
BGP state = Established, up for 00:10:45
Last read 00:00:16, last write 00:00:15, hold time is 180, keepalive interval is 60 seconds
Neighbor sessions:
  1 active, is not multisession capable (disabled)
Neighbor capabilities:
  Route refresh: advertised and received(new)
  Four-octets ASN Capability: advertised and received
  Address family IPv4 Unicast: advertised and received
  Enhanced Refresh Capability: advertised and received
  Multisession Capability:
  Stateful switchover support enabled: NO for session 1
Message statistics:
  InQ depth is 0
  OutQ depth is 0

             Sent       Rcvd
Opens:         1         1
Notifications:  0         0
Updates:        4         2
Keepalives:    22        22
Route Refresh:  0         0
Total:         29        25
Default minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
Session: 192.1.12.1
BGP table version 13, neighbor version 13/0
Output queue size : 0
Index 1, Advertise bit 0
1 update-group member
Slow-peer detection is disabled
Slow-peer split-update-group dynamic is disabled
~More~
             Sent       Rcvd
For address family: IPv4 Unicast
Session: 192.1.12.1
BGP table version 13, neighbor version 13/0
Output queue size : 0
Index 1, Advertise bit 0
1 update-group member
Slow-peer detection is disabled
Slow-peer split-update-group dynamic is disabled
```

De la salida del comando **show ip bgp neighbors**, destacamos información importante como la dirección ip de la interface del vecino, su router ID y el número del sistema autónomo al cual pertenece; además se tiene la versión de la tabla BGP y el estado de la sesión BGP que para este caso se encuentra activa.

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**.

Como R2 ya se ha configurado para que ejecute un proceso de BGP dentro del sistema autónomo 2 (AS2) y como se ilustra en las figuras 9 y 10 también anuncia las redes para las interfaces de loopback, no quedaría sino por establecer la relación de vecino en R2 hacia R3, y en este punto la configuración se centra en el R3 para que inicie los procesos BGP y establezca las relaciones de vecindad con R2. A continuación se presentan los comandos necesarios para que R3 ejecute BGP:

```
R2#conf t
R2(config)#router bgp 2
R2(config-router)#network 192.1.23.0
R2(config-router)#neighbor 192.1.23.3 remote-as 3
-----
R3#config t
R3(config)#router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#network 3.0.0.0
R3(config-router)#network 13.1.0.0
R3(config-router)#neighbor 192.1.23.2 remote-as 2
```

Se verifica para este caso nuevamente la relación de vecino entre R2->R3 y viceversa haciendo uso del comando **show ip route** y **show ip bgp neighbors**:

Figura 13. Tabla de enrutamiento R2

```
R2#sh ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       O - OSPF, EX - OSPF 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, I - 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, 00:49:49
C    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
B    3.0.0.0/8 [20/0] via 192.1.23.3, 00:03:07
L    12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    12.1.0.0/16 is directly connected, Loopback1
C    12.1.0.1/32 is directly connected, Loopback1
C    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
C    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, FastEthernet0/0
L    192.1.23.2/32 is directly connected, FastEthernet0/0
R2#
```

Figura 14. Tabla de R3

```
R3#sh ip rout
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 192.1.23.2, 00:17:38
B 2.0.0.0/8 [20/0] via 192.1.23.2, 00:17:38
  3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   3.0.0.0/8 is directly connected, Loopback0
L   3.3.3.3/32 is directly connected, Loopback0
  13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   13.1.0.0/16 is directly connected, Loopback1
L   13.1.0.1/32 is directly connected, Loopback1
B 192.1.12.0/24 [20/0] via 192.1.23.2, 00:17:38
  192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.1.23.0/24 is directly connected, FastEthernet0/0
L   192.1.23.3/32 is directly connected, FastEthernet0/0
  192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.1.34.0/24 is directly connected, Serial1/0
L   192.1.34.3/32 is directly connected, Serial1/0
```

Del resultado de la configuración podemos concluir que aunque se anuncian las redes a las cuales pertenecen las interfaces de loopbak 11.1.0.1, 12.1.0.1, 13.1.0.1 por BGP de los router R1,R2 y R3 respectivamente esta no son anunciadas en las tablas de enrutamiento esto se debe a que se es necesario emplear rutas estáticas para que sean alcanzadas.

Figura 15. Relación de vecindad entre R2 y R3

```
BGP neighbor is 192.1.23.3, remote AS 3, external link
BGP version 4, remote router ID 44.44.44.44
BGP state = Established, up for 00:38:17
Last read 00:00:22, last write 00:00:03, hold time is 180, keepalive interval is 60 seconds
Neighbor sessions:
  1 active, is not multisession capable (disabled)
Neighbor capabilities:
  Route refresh: advertised and received(new)
  Four-octets ASN Capability: advertised and received
  Address family IPv4 Unicast: advertised and received
  Enhanced Refresh Capability: advertised and received
  Multisession Capability:
  Stateful switchover support enabled: NO for session 1
Message statistics:
  InQ depth is 0
  OutQ depth is 0

           Sent         Rcvd
Opens:           1           1
Notifications:    0           0
Updates:         10          10
Keepalives:       40          40
Route Refresh:     0           0
Total:           51          51
Default minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
Session: 192.1.23.3
BGP table version 13, neighbor version 13/0
Output queue size : 0
Index 1, Advertise bit 0
1 update-group member
Slow-peer detection is disabled
Slow-peer split-update-group dynamic is disabled
```

Figura 16. Relación de vecindad entre R3 y R2

```
BGP neighbor is 192.1.23.2, remote AS 2, external link
BGP version 4, remote router ID 33.33.33.33
BGP state = Established, up for 01:10:33
Last read 00:00:12, last write 00:00:48, hold time is 180, keepalive interval is 60 seconds
Neighbor sessions:
  1 active, is not multisession capable (disabled)
Neighbor capabilities:
  Route refresh: advertised and received(new)
  Four-octets ASN Capability: advertised and received
  Address family IPv4 Unicast: advertised and received
  Enhanced Refresh Capability: advertised and received
  Multisession Capability:
  Stateful switchover support enabled: NO for session 1
Message statistics:
  InQ depth is 0
  OutQ depth is 0

      Sent          Rcvd
Opens:          1           1
Notifications:  0           0
Updates:        10          10
Keepalives:     75          75
Route Refresh:  0           0
Total:          86          86
Default minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
Session: 192.1.23.2
BGP table version 13, neighbor version 13/0
Output queue size : 0
Index 1, Advertise bit 0
1 update-group member
Slow-peer detection is disabled
Slow-peer split-update-group dynamic is disabled

      Sent          Rcvd
Prefix activity:  ----
Prefixes Current: 6           4 (Consumes 320 bytes)
```

Al igual que entre R1 y R2 se resaltan los datos de importancia de la salida del comando **show ip bgp neighbors**.

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

Configuración BGP en R4

Para configurar el BGP en R4 se siguen los mismos comandos empleados en los demás router lo único que varia son el numero para el sistema autónomo, el id del router y las redes que se anuncian:

```
R2#configure terminal
R2(config)#router bgp 4
```

```
R2(config-router)#bgp router-id 66.66.66.66
R2(config-router)#network 14.1.0.0
R2(config-router)#network 192.1.34.0
```

Adicionalmente se debe configurar la relación de vecino BGP desde R4 hacia R3 y viceversa lo cual se logra con la ejecución de los siguientes comandos.

```
R3#configure terminal
R3(config)#router bgp 3
R3(config-router)#neighbor 192.1.34.4 remote-as 4
-----
R4#configure terminal
R4(config)#router bgp 4
R4(config-router)#neighbor 192.1.34.3 remote-as 3
```

Tal como se indica se deben garantizar la conectividad entre las direcciones de loopback para los cual como ya se había mencionado es necesarios establecer rutas estáticas en los diferentes routers continuación se describe el procedimiento empleado con los comandos necesarios para tal fin.

Enrutamiento estático en R4

Para la configuración de enrutamiento estático en R4 fue necesario emplear los siguientes comandos.

```
R4#configure terminal
R4(config)#ip route 11.1.0.0 255.255.0.0 192.1.34.3
R4(config)#ip route 12.1.0.0 255.255.0.0 192.1.34.3
R4(config)#ip route 13.1.0.0 255.255.0.0 192.1.34.3
```

Se anuncian de estáticamente las redes 11.1.0.0, 12.1.0.0, 13.1.0.0 correspondientes a las redes de loopback de R1, R2, R3 respectivamente.

Enrutamiento estático en R3

Al igual que en R4 se anuncian las redes de loopback de R1, R2 y R4 haciendo uso la misma cadena de comandos que en el caso anterior, con la diferencia de que se crea una ruta estática predeterminada hacia el R4 con el fin de que todo el trafico que vaya hacia este sea dirigido a través de la interface seria 1/0.

```
R3#configure terminal
R3(config)#ip route 0.0.0.0 0.0.0.0 serial 1/0
R3(config)#ip route 11.1.0.0 255.255.0.0 192.1.23.2
```



```
R3(config)#ip route 12.1.0.0 255.255.0.0 192.1.23.3
```

Enrutamiento estático en R2.

Se sigue el mismo procedimiento para las rutas estáticas hacia las redes de loopback de los demás router.

```
R2#configure terminal
R2(config)#ip route 0.0.0.0 0.0.0.0 192.1.12.1
R2(config)#ip route 13.1.0.0 255.255.0.0 192.1.23.3
R2(config)#ip route 14.1.0.0 255.255.0.0 192.1.23.3
```

Enrutamiento estático en R1

Una vez configuradas las rutas estáticas en R4, R3 y R2 no queda sino configurar en R1 una ruta estática predeterminada para concluir de esta manera la conectividad de extremo a extremo de la siguiente manera.

```
R2#configure terminal
R2(config)#ip route 0.0.0.0 0.0.0.0 serial 1/0
```

Para finalizar se realizan pruebas de conectividad vía ping desde R1 hacia R4 y viceversa hacia la interfaces loopback.

Figura 17. Prueba ping desde R1 hacia interfaces Loopback (R2, R3, R4)

```
R1#ping 12.1.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.1.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/39/80 ms
R1#ping 13.1.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 13.1.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/73/104 ms
R1#ping 14.1.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.1.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/128/164 ms
R1#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/50/60 ms
R1#ping 3.3.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/42/80 ms
R1#ping 4.4.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#
```

Todos los ping tienen respuesta excepto el de la interface Loopback 4.4.4.4 del router R4 lo cual se debe a que esta red no fue anunciada en la configuración BGP por los requerimientos del laboratorio.

Figura 18. Prueba ping desde R4 hacia interfaces Loopback (R1, R2, R3)

```
R4#ping 11.1.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.1.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/87/180 ms
R4#ping 12.1.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.1.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/57/84 ms
R4#ping 13.1.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 13.1.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/42/64 ms
R4#ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/120/168 ms
R4#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/64/72 ms
R4#ping 3.3.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/28/40 ms
R4#
```

Comprobamos las tablas de enrutamiento y la relación de vecino entre R3 y R4.

Figura 19. Tabla de enrutamiento de R3

```
R3#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, I - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 is directly connected, Serial1/0
B 1.0.0.0/8 [20/0] via 192.1.23.2, 01:57:43
B 2.0.0.0/8 [20/0] via 192.1.23.2, 02:16:38
C 3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 3.0.0.0/8 is directly connected, Loopback0
L 3.3.3.3/32 is directly connected, Loopback0
L 11.0.0.0/16 is subnetted, 1 subnets
S 11.1.0.0 [1/0] via 192.1.23.2
S 12.0.0.0/16 is subnetted, 1 subnets
S 12.1.0.0 [1/0] via 192.1.23.2
C 13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 13.1.0.0/16 is directly connected, Loopback1
L 13.1.0.1/32 is directly connected, Loopback1
B 192.1.12.0/24 [20/0] via 192.1.23.2, 02:00:41
L 192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.1.23.0/24 is directly connected, FastEthernet0/0
L 192.1.23.3/32 is directly connected, FastEthernet0/0
C 192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.1.34.0/24 is directly connected, Serial1/0
L 192.1.34.3/32 is directly connected, Serial1/0
R3#
R3#
```

Figura 20. Tabla de enrutamiento de R4

```
R4#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 - OOR, P - periodic downloaded static route, H - NHRP, I - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

R
  1.0.0.0/8 [20/0] via 192.1.34.3, 02:01:49
R
  2.0.0.0/8 [20/0] via 192.1.34.3, 02:20:17
R
  3.0.0.0/8 [20/0] via 192.1.34.3, 02:20:48
R
  4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C
  4.0.0.0/8 is directly connected, Loopback0
L
  4.4.4.4/32 is directly connected, Loopback0
S
  11.0.0.0/16 is subnetted, 1 subnets
S
  11.1.0.0 [1/0] via 192.1.34.3
S
  12.0.0.0/16 is subnetted, 1 subnets
S
  12.1.0.0 [1/0] via 192.1.34.3
S
  13.0.0.0/16 is subnetted, 1 subnets
S
  13.1.0.0 [1/0] via 192.1.34.3
R
  14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C
  14.1.0.0/16 is directly connected, Loopback1
L
  14.1.0.1/32 is directly connected, Loopback1
R
  192.1.12.0/24 [20/0] via 192.1.34.3, 02:04:48
R
  192.1.23.0/24 [20/0] via 192.1.34.3, 02:20:17
R
  192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C
  192.1.34.0/24 is directly connected, Serial1/0
L
  192.1.34.4/32 is directly connected, Serial1/0
```

Se identifican las rutas anunciadas por BGP, las aprendidas por estáticamente teniendo de esta manera una convergencia en la red.

ESCENARIO 2

Figura 21. Topología del escenario 2

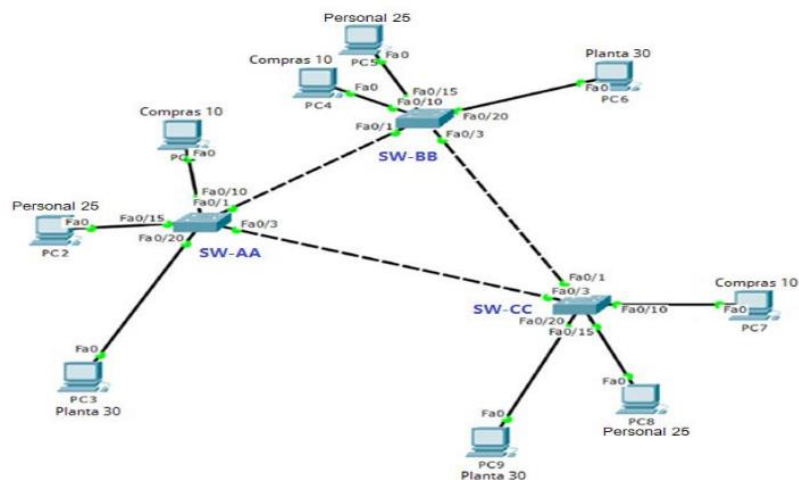
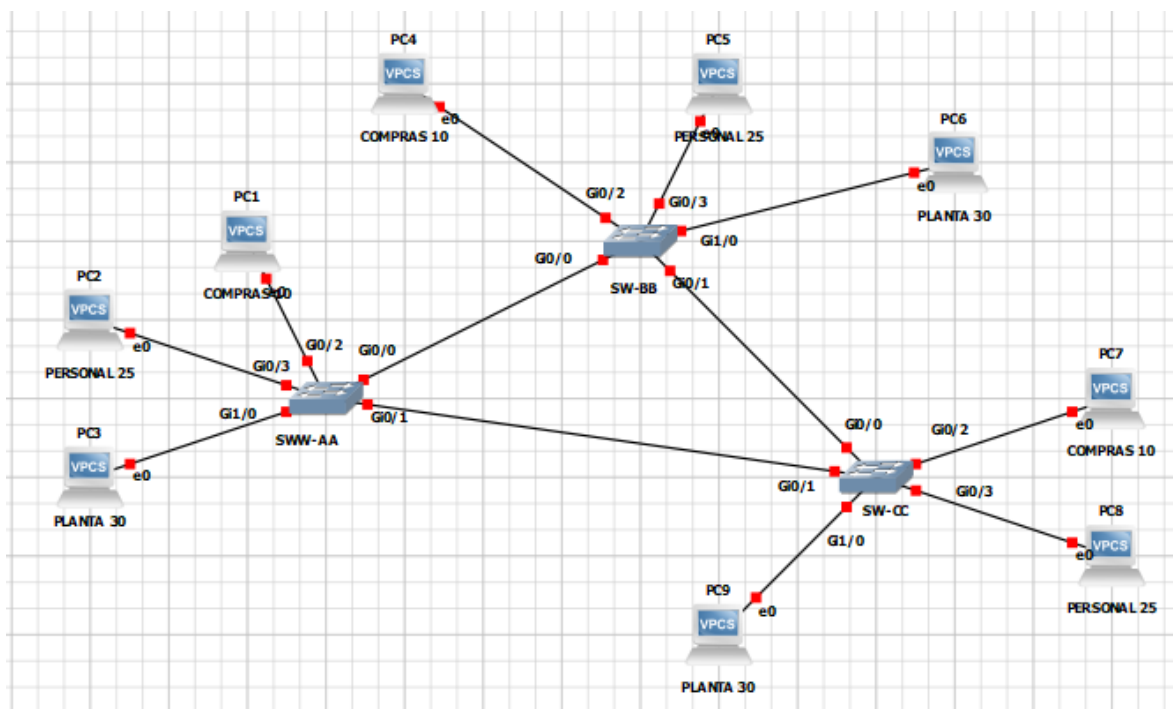


Figura 22. Montaje en GNS3 del escenario 2



Antes de aplicar las configuraciones que se solicitan para el presente escenario a los switches se realizara una configuración preliminar general la cual aplicar para cada uno de los conmutadores de la topología:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-BB
SW-BB(config)#no ip domain lookup
SW-BB(config)#line con 0
SW-BB(config-line)#logging synchronous
SW-BB(config-line)#exec-timeout 0 0
SW-BB(config-line)#exit
```

Se aplica los mismos comandos para los switches SW-AA y SW-CC modificando el nombre del dispositivo según corresponda.

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 defecto los switches cisco se encuentran en modo server para ejecutar los procesos de VTP por lo cual y según se indica se requiere cambiar SW-AA y SW-CC al modo cliente y configurar el dominio para que reciban las actualizaciones de VLAN desde el SW-BB que quedaría como server de la siguiente manera.

Configuración VTP en SW-AA

```
SW-AA(config)#vtp version 2
SW-AA(config)#vtp mode client
SW-AA(config)#vtp domain CCNP
SW-AA(config)#vtp password cisco
```

Configuración VTP en SW-BB

```
SW-BB(config)#vtp version 2
SW-BB(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-BB(config)#vtp password cisco
Setting device VTP password to cisco
SW-BB(config)#exit
*May 11 22:48:35.242: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name
changed to CCNP.
```

Configuración VTP en SW-CC

```
SW-CC(config)#vtp version 2
SW-CC(config)#vtp mode client
Setting device to VTP Client mode for VLANs.
SW-CC(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-CC(config)#vtp password cisco
Setting device VTP password to cisco
SW-CC(config)#exit
*May 11 22:51:41.850: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name
changed to CCNP.
SW-CC(config)#exit
```

Se evidencia en los mensajes de notificación de los switches que se configuró vtp y se ha cambiado del modo en los conmutadores que requerían pasar de modo server a cliente, para verificar estos cambios emite el comando **show vtp status** en cada switch.

Figura 23. Verificación configuración VTP SW-AA

```
SW-AA#show vtp status
VTP Version capable      : 1 to 3
VTP version running      : 2
VTP Domain Name          : CCNP
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 0c04.208d.8000
Configuration last modified by 0.0.0.0 at 5-11-20 22:43:11

Feature VLAN:
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs : 5
Configuration Revision    : 1
MD5 digest               : 0xCD 0xB9 0x92 0xF5 0xA9 0xB3 0x9E 0xD8
                        : 0x94 0x66 0x40 0x3E 0xEB 0xF9 0x99 0xB9

SW-AA#
```

Figura 24. verificación configuración VTP SW-BB

```
SW-BB#show vtp status
VTP Version capable      : 1 to 3
VTP version running      : 2
VTP Domain Name          : CCNP
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 0c04.2063.8000
Configuration last modified by 0.0.0.0 at 5-11-20 22:48:34
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
-----
VTP Operating Mode       : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 5
Configuration Revision    : 1
MD5 digest               : 0xCD 0xB9 0x92 0xF5 0xA9 0xB3 0x9E 0xD8
                        : 0x94 0x66 0x40 0x3E 0xEB 0xF9 0x99 0xB9

SW-BB#
```

Figura 25. Verificación de configuración SW-CC

```
SW-CC#show vtp status
VTP Version capable      : 1 to 3
VTP version running      : 2
VTP Domain Name          : CCNP
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : 0c04.203c.8000
Configuration last modified by 0.0.0.0 at 5-11-20 22:51:40

Feature VLAN:
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs : 5
Configuration Revision    : 1
MD5 digest               : 0xCD 0xB9 0x92 0xF5 0xA9 0xB3 0x9E 0xD8
                        : 0x94 0x66 0x40 0x3E 0xEB 0xF9 0x99 0xB9

SW-CC#
```

Se resalta la información relevante de la salida del comando para la configuración de VTP como la versión, dominio y modo en el cual se encuentra el swiche.

Configurar DTP (Dynamic Trunking Protocol)

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 aplicara la configuración en le SW-BB a la interface g0/0 para establecer el enlace troncal dinámico aplicando los siguientes comandos.

```
SW-BB(config)#interface g0/0
SW-BB(config-if)#switchport mode dynamic desirable
SW-BB(config-if)#no shutdown

SW-AA(config)#interface g0/0
SW-AA(config-if)#no shutdown
```

Se verifica que se haya establecido el enlace troncal entre los las interfaces g0/0 de los dos swiches empleando el comando; *show interfaces trunk*.

Figura 26. Enlace troncal dinámico SW-AA y SW-BB

Port	Mode	Encapsulation	Status	Native vlan
Gi0/0	auto	n-isl	trunking	1

Port	Mode	Encapsulation	Status	Native vlan
Gi0/0	desirable	n-isl	trunking	1

Both screenshots also show the following information for Gi0/0:

- Vlans allowed on trunk: 1-4094
- Vlans allowed and active in management domain: 1
- Vlans in spanning tree forwarding state and not pruned: none

A continuación se configurara un enlace troncal estático entre SW-AA y SW-CC cambiando el modo de las interfaces g0/1 en ambos a trunk.

```
SW-AA(config)#interface g0/1
SW-AA(config-if)#switchport trunk encapsulation dot1q
SW-AA(config-if)#switchport mode trunk
SW-AA(config-if)#no shutdown

SW-CC(config)#interface g0/1
SW-CC(config-if)#switchport trunk encapsulation dot1q
SW-CC(config-if)#switchport mode trunk
```

```
SW-CC(config-if)#no shutdown
```

Nuevamente empujando el comando **show interface trunk** verificamos que se haya establecido el enlace troncal esta vez entre SW-AA y SW-CC.

Figura 27. Enlace troncal estático entre SW-AA y SW-CC

SW-AA#sh int trunk					SW-CC(config-if)#do sh int trunk				
Port	Mode	Encapsulation	Status	Native vlan	Port	Mode	Encapsulation	Status	Native vlan
Gi0/0	auto	n-isl	trunking	1	Gi0/1	on	802.1q	trunking	1
Gi0/1	on	802.1q	trunking	1					
Port Vlans allowed on trunk					Port Vlans allowed on trunk				
Gi0/0	1-4094				Gi0/1	1-4094			
Gi0/1	1-4094								
Port Vlans allowed and active in management domain					Port Vlans allowed and active in management domain				
Gi0/0	1				Gi0/1	1			
Gi0/1	1								
Port Vlans in spanning tree forwarding state and not pruned					Port Vlans in spanning tree forwarding state and not pruned				
Gi0/0	none				Gi0/1	1			
Gi0/1	1				SW-CC(config-if)#				

En el SW-AA se tienen establecidos ya dos enlaces troncales uno a través de DTP y otro establecido de manera manual o estática, y SW-CC se estableció el enlace troncal con SW-AA a través de la interface g0/1.

Procedo de la misma manera para establecer el enlace troncal entre SW-BB y SW-CC a la interfaces g0/1 y g0/0 respectivamente.

```
SW-BB(config)#interface g0/1
SW-BB(config-if)#switchport trunk encapsulation dot1q
SW-BB(config-if)#switchport mode trunk
SW-BB(config-if)#no shutdown

SW-CC(config)#interface g0/0
SW-CC(config-if)#switchport trunk encapsulation dot1q
SW-CC(config-if)#switchport mode trunk
SW-CC(config-if)#no shutdown
```

Se realiza la respectiva verificación del enlace entre los switches.

Figura 28. Enlace troncal estático entre SW-BB y SW-CC

SW-BB(config-if)#do sh int trunk					SW-CC(config-if)#do sh int trunk				
Port	Mode	Encapsulation	Status	Native vlan	Port	Mode	Encapsulation	Status	Native vlan
Gi0/0	desirable	n-isl	trunking	1	Gi0/0	on	802.1q	trunking	1
Gi0/1	on	802.1q	trunking	1	Gi0/1	on	802.1q	trunking	1
Port Vlans allowed on trunk					Port Vlans allowed on trunk				
Gi0/0	1-4094				Gi0/0	1-4094			
Gi0/1	1-4094				Gi0/1	1-4094			
Port Vlans allowed and active in management domain					Port Vlans allowed and active in management domain				
Gi0/0	1				Gi0/0	1			
Gi0/1	1				Gi0/1	1			
Port Vlans in spanning tree forwarding state and not pruned					Port Vlans in spanning tree forwarding state and not pruned				
Gi0/0	1				Gi0/0	1			
Gi0/1	1				Gi0/1	1			

Configuración de VLAN'S y Asignación de Puertos

Como los switches se configuraron para que ejecuten VTP versión 2 basta con realizar la configuración de las VLAN en el SW-BB el cual esta en modo server y una vez configuradas las VLAN este propagara la información hacia los otros dos switches que se encuentran en modo server; a continuación se detallan los comando utilizados para dicha configuración.

```
SW-BB# configure terminal
SW-BB(config)#vlan 10
SW-BB(config-vlan)#name Compras
SW-BB(config-vlan)#no shutdown
SW-BB(config-vlan)#exit
SW-BB(config)#vlan 25
SW-BB(config-vlan)#name Personal
SW-BB(config-vlan)#no shutdown
SW-BB(config-vlan)#exit
SW-BB(config)#vlan 30
SW-BB(config-vlan)#name Planta
SW-BB(config-vlan)#no shutdown
SW-BB(config-vlan)#exit
SW-BB(config)#vlan 99
SW-BB(config-vlan)#name AdmonS
SW-BB(config-vlan)#no shutdown
SW-BB(config-vlan)#exit
```

Una vez coniguradas las VLAN en el SW-BB el cual es el servidor para los procesos VTP en la red verificamos esta configuración emitiendo el comando `show vlan` en los tres switches ya los SW-AA y SW-CC deben tener la información de las vlan configurada gracias a la propagación VTP.

Figura 29. Verificación de configuración VLAN en SW-BB

```
SW-BB#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Gi0/2, Gi0/3, Gi1/0, Gi1/1 Gi1/2, Gi1/3, Gi2/0, Gi2/1 Gi2/2, Gi2/3, Gi3/0, Gi3/1 Gi3/2, Gi3/3
10	Compras	active	
25	Personal	active	
30	Planta	active	
99	Admon	active	
1002	fddi-default	act/unsup	
1003	trcrf-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trbrf-default	act/unsup	

Figura 30. Propagación de Vlan's por VTP desde SW-BB hacia SW-AA y SW-CC

SW-AA#show vlan				SW-CC#show vlan			
VLAN Name		Status	Ports	VLAN Name		Status	Ports
1	default	active	Gi0/2, Gi0/3, Gi1/0, Gi1/1 Gi1/2, Gi1/3, Gi2/0, Gi2/1 Gi2/2, Gi2/3, Gi3/0, Gi3/1 Gi3/2, Gi3/3	1	default	active	Gi0/2, Gi0/3, Gi1/0, Gi1/1 Gi1/2, Gi1/3, Gi2/0, Gi2/1 Gi2/2, Gi2/3, Gi3/0, Gi3/1 Gi3/2, Gi3/3
10	Compras	active		10	Compras	active	
25	Personal	active		25	Personal	active	
30	Planta	active		30	Planta	active	
99	Admon	active		99	Admon	active	
1002	fddi-default	act/unsup		1002	fddi-default	act/unsup	
1003	trcrf-default	act/unsup		1003	trcrf-default	act/unsup	
1004	fddinet-default	act/unsup		1004	fddinet-default	act/unsup	
1005	trbrf-default	act/unsup		1005	trbrf-default	act/unsup	

Como se muestra en las capturas de la salida del comando show vlan ya los tres switches tienen creadas las vlan pero no se les ha asociado puertos a estas por lo cual en el siguiente paso se detallaran los comandos necesarios para la asignación de puertos en a estas vlan teniendo en cuenta la siguiente tabla.

Tabla 5. Información de puertos vlan's y direccionamiento de host's

Interfaz	VLAN	Direcciones IP de los PCs
G0/2	VLAN 10	190.108.10.X / 24
G0/3	VLAN 25	190.108.20.X / 24
G1/0	VLAN 30	190.108.30.X / 24

X = número de cada PC particular

```
SW-AA(config)#int g0/2
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#no shutdown
SW-AA(config-if)#exit
SW-AA(config)#int g0/3
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#no shutdown
SW-AA(config-if)#exit
SW-AA(config)#int g1/0
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
SW-AA(config-if)#no shutdown
SW-AA(config-if)#exit
```

```

SW-BB(config)#int g0/2
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#no shutdown
SW-BB(config-if)#exit
SW-BB(config)#int g0/3
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#no shutdown
SW-BB(config-if)#exit
SW-BB(config)#int g1/0
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30
SW-BB(config-if)#no shutdown
SW-BB(config-if)#exit

SW-CC(config)#int g0/2
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#no shutdown
SW-CC(config-if)#exit
SW-CC(config)#int g0/3
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#no shutdown
SW-CC(config-if)#exit
SW-CC(config)#int g1/0
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30
SW-CC(config-if)#no shutdown
SW-CC(config-if)#exit

```

Verificamos la asignación de puertos a las vlan con el comando **show vlan**.

Figura 31. Verificación de asignación de puertos en (SW-AA, SW-BB y SW-CC)

SW-AA(config)#do sh vlan				SW-BB#show vlan			
VLAN Name	Status	Ports		VLAN Name	Status	Ports	
1 default	active	Gi1/1, Gi1/2, Gi1/3, Gi2/0 Gi2/1, Gi2/2, Gi2/3, Gi3/0 Gi3/1, Gi3/2, Gi3/3		1 default	active	Gi1/1, Gi1/2, Gi1/3, Gi2/0 Gi2/1, Gi2/2, Gi2/3, Gi3/0 Gi3/1, Gi3/2, Gi3/3	
10 Compras	active	Gi0/2		10 Compras	active	Gi0/2	
25 Personal	active	Gi0/3		25 Personal	active	Gi0/3	
30 Planta	active	Gi1/0		30 Planta	active	Gi1/0	
99 Admon	active			99 Admon	active		
1002 fddi-default	act/unsup			1002 fddi-default	act/unsup		
1003 trcrf-default	act/unsup			1003 trcrf-default	act/unsup		
1004 fddinet-default	act/unsup			1004 fddinet-default	act/unsup		
1005 trbrf-default	act/unsup			1005 trbrf-default	act/unsup		

SW-CC#show vlan			
VLAN Name	Status	Ports	
1 default	active	Gi1/1, Gi1/2, Gi1/3, Gi2/0 Gi2/1, Gi2/2, Gi2/3, Gi3/0 Gi3/1, Gi3/2, Gi3/3	
10 Compras	active	Gi0/2	
25 Personal	active	Gi0/3	
30 Planta	active	Gi1/0	
99 Admon	active		
1002 fddi-default	act/unsup		
1003 trcrf-default	act/unsup		
1004 fddinet-default	act/unsup		
1005 trbrf-default	act/unsup		

Configuración de direcciones IP en los switches

Debemos configurar la dirección ip para la administración de los switches a través de la vlan 99 (Admon) siguiendo las indicaciones de la siguiente tabla.

Tabla 6. Direccionamiento IP para las SVI asociadas a la VLAN 99 Admon

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(config)#int vlan 99
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
SW-AA(config-if)#no shutdown
```

```
SW-BB(config)#int vlan 99
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
SW-BB(config-if)#no shutdown
```

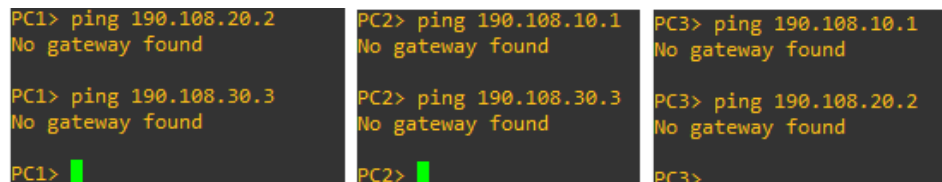
```
SW-CC(config)#int vlan 99
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0
SW-CC(config-if)#no shutdown
```

Verificación de conectividad extremo a extremo

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

Ping entre los PC del Switches

Figura 32. Ping entre PC del SW-AA



```
PC1> ping 190.108.20.2
No gateway found

PC1> ping 190.108.30.3
No gateway found

PC1>

PC2> ping 190.108.10.1
No gateway found

PC2> ping 190.108.30.3
No gateway found

PC2>

PC3> ping 190.108.10.1
No gateway found

PC3> ping 190.108.20.2
No gateway found

PC3>
```

Figura 33. Ping entre PC del SW-BB

```
PC4> ping 190.108.20.5
host (190.108.10.3) not reachable

PC4> ping 190.108.30.6
host (190.108.10.3) not reachable

PC4> █

PC5> ping 190.108.10.4
host (190.108.20.4) not reachable

PC5> ping 190.108.30.6
host (190.108.20.4) not reachable

PC5> █

PC6> ping 190.108.10.4
host (190.108.30.2) not reachable

PC6> ping 190.108.20.5
host (190.108.30.2) not reachable

PC6> █
```

Figura 34. Ping entre PC del SW-CC

```
PC7> ping 190.108.20.8
190.108.20.8 icmp_seq=1 timeout
190.108.20.8 icmp_seq=2 timeout
190.108.20.8 icmp_seq=3 timeout
190.108.20.8 icmp_seq=4 timeout
190.108.20.8 icmp_seq=5 timeout

PC7> ping 190.108.30.9
190.108.30.9 icmp_seq=1 timeout
190.108.30.9 icmp_seq=2 timeout
190.108.30.9 icmp_seq=3 timeout
190.108.30.9 icmp_seq=4 timeout
190.108.30.9 icmp_seq=5 timeout

PC7> █

PC8> ping 190.108.10.7
190.108.10.7 icmp_seq=1 timeout
190.108.10.7 icmp_seq=2 timeout
190.108.10.7 icmp_seq=3 timeout
190.108.10.7 icmp_seq=4 timeout
190.108.10.7 icmp_seq=5 timeout

PC8> ping 190.108.30.9
190.108.30.9 icmp_seq=1 timeout
190.108.30.9 icmp_seq=2 timeout
190.108.30.9 icmp_seq=3 timeout
190.108.30.9 icmp_seq=4 timeout
190.108.30.9 icmp_seq=5 timeout

PC8> █

PC9> ping 190.108.10.7
190.108.10.7 icmp_seq=1 timeout
190.108.10.7 icmp_seq=2 timeout
190.108.10.7 icmp_seq=3 timeout
190.108.10.7 icmp_seq=4 timeout
190.108.10.7 icmp_seq=5 timeout

PC9> ping 190.108.20.8
190.108.20.8 icmp_seq=1 timeout
190.108.20.8 icmp_seq=2 timeout
190.108.20.8 icmp_seq=3 timeout
190.108.20.8 icmp_seq=4 timeout
190.108.20.8 icmp_seq=5 timeout

PC9> █
```

El ping no es exitoso entre los PC conectados a los switches de manera local ya que como se muestra en la tabla 6 se da la información de direccionamiento para configurar la SVI de la Vlan 99 para las demás Vlan no se tiene parámetros para la configuración ip por lo tanto se tienen los mensajes (no Gateway found, host no reachable y timeout), en SW-AA, SW-BB y SW-CC respectivamente que aparecen al intentar realizar las solicitudes de ICMP a través del comando ping, esto se debe a que no se tiene la configuración de direccionamiento ya mencionada en las SVI para las VLAN 10, 25 y 30. Debido a esto el ping entre los PC de los switch tampoco será exitoso; por lo cual se realiza la configuración de estas teniendo en cuenta la siguiente tabla.

Tabla 7. Direcccionamiento IP de SVI en la Vlan 10,25 y 30 para cada switch

SWITCH	IP	MASCARA	VLAN
SW-AA	190.108.10.2	255.255.255.0	10
SW-AA	190.108.20.3	255.255.255.0	25
SW-AA	190.108.30.1	255.255.255.0	30
SW-BB	190.108.10.3	255.255.255.0	10
SW-BB	190.108.20.4	255.255.255.0	25
SW-BB	190.108.30.2	255.255.255.0	30
SW-CC	190.108.10.4	255.255.255.0	10
SW-CC	190.108.20.5	255.255.255.0	25
SW-CC	190.108.30.3	255.255.255.0	30

A continuación se listan los comandos aplicados en cada switch para la configuración del direccionamiento IP en las vlan según la tabla anterior:

```
SW-AA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#int vlan 10
SW-AA(config-if)#ip address 190.108.10.2 255.255.255.0
SW-AA(config-if)#no shutdown
SW-AA(config-if)#exit
SW-AA(config)#int vlan 25
SW-AA(config-if)#ip address 190.108.20.3 255.255.255.0
SW-AA(config-if)#no shutdown
SW-AA(config-if)#exit
SW-AA(config)#int vlan 30
SW-AA(config-if)#ip address 190.108.30.1 255.255.255.0
SW-AA(config-if)#no shutdown
SW-AA(config-if)#exit
```

```
SW-BB#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#int vlan 10
SW-BB(config-if)#ip address 190.108.10.3 255.255.255.0
SW-BB(config-if)#no shutdown
SW-BB(config-if)#exit
SW-BB(config)#int vlan 25
SW-BB(config-if)#ip address 190.108.20.4 255.255.255.0
SW-BB(config-if)#no shutdown
SW-BB(config-if)#exit
SW-BB(config)#int vlan 30
SW-BB(config-if)#ip address 190.108.30.2 255.255.255.0
SW-BB(config-if)#no shutdown
SW-BB(config-if)#exit
```

```

SW-CC#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-CC(config)#int vlan 10
SW-CC(config-if)#ip address 190.108.10.4 255.255.255.0
SW-CC(config-if)#no shutdown
SW-CC(config-if)#exit
SW-CC(config)#int vlan 25
SW-CC(config-if)#ip address 190.108.20.5 255.255.255.0
SW-CC(config-if)#no shutdown
SW-CC(config-if)#exit
SW-CC(config)#int vlan 30
SW-CC(config-if)#ip address 190.108.30.3 255.255.255.0
SW-CC(config-if)#no shutdown
SW-CC(config-if)#exit

```

Una vez aplicados estos cambios en los switch de la topología realizamos pruebas de conectividad via ping entre los PC de cada conmutador y adicionalmente verificamos la conectividad ping entre los equipos de cada vlan para garantizar de esta manera conectividad de extremo a extremo.

Figura 35. Ping 2 Corrección de conectividad entre PC SW-AA

```

PC1> ping 190.108.20.2
84 bytes from 190.108.20.2 icmp_seq=1 ttl=63 time=13.447 ms
84 bytes from 190.108.20.2 icmp_seq=2 ttl=63 time=8.722 ms
84 bytes from 190.108.20.2 icmp_seq=3 ttl=63 time=7.322 ms
84 bytes from 190.108.20.2 icmp_seq=4 ttl=63 time=8.465 ms
84 bytes from 190.108.20.2 icmp_seq=5 ttl=63 time=12.642 ms

PC1> ping 190.108.30.3
84 bytes from 190.108.30.3 icmp_seq=1 ttl=255 time=40.716 ms
84 bytes from 190.108.30.3 icmp_seq=2 ttl=255 time=23.105 ms
84 bytes from 190.108.30.3 icmp_seq=3 ttl=255 time=27.419 ms
84 bytes from 190.108.30.3 icmp_seq=4 ttl=255 time=76.043 ms
84 bytes from 190.108.30.3 icmp_seq=5 ttl=255 time=54.421 ms

PC1>

PC2> ping 190.108.10.1
84 bytes from 190.108.10.1 icmp_seq=1 ttl=63 time=15.223 ms
84 bytes from 190.108.10.1 icmp_seq=2 ttl=63 time=11.201 ms
84 bytes from 190.108.10.1 icmp_seq=3 ttl=63 time=20.096 ms
84 bytes from 190.108.10.1 icmp_seq=4 ttl=63 time=24.434 ms
84 bytes from 190.108.10.1 icmp_seq=5 ttl=63 time=15.744 ms

PC2> ping 190.108.30.3
84 bytes from 190.108.30.3 icmp_seq=1 ttl=255 time=153.282 ms
84 bytes from 190.108.30.3 icmp_seq=2 ttl=255 time=24.319 ms
84 bytes from 190.108.30.3 icmp_seq=3 ttl=255 time=29.795 ms
84 bytes from 190.108.30.3 icmp_seq=4 ttl=255 time=30.499 ms
84 bytes from 190.108.30.3 icmp_seq=5 ttl=255 time=46.980 ms

PC2>

PC3> ping 190.108.10.1
84 bytes from 190.108.10.1 icmp_seq=1 ttl=63 time=13.836 ms
84 bytes from 190.108.10.1 icmp_seq=2 ttl=63 time=12.340 ms
84 bytes from 190.108.10.1 icmp_seq=3 ttl=63 time=20.660 ms
84 bytes from 190.108.10.1 icmp_seq=4 ttl=63 time=14.944 ms
84 bytes from 190.108.10.1 icmp_seq=5 ttl=63 time=15.755 ms

PC3> ping 190.108.20.2
84 bytes from 190.108.20.2 icmp_seq=1 ttl=63 time=17.459 ms
84 bytes from 190.108.20.2 icmp_seq=2 ttl=63 time=17.814 ms
84 bytes from 190.108.20.2 icmp_seq=3 ttl=63 time=33.195 ms
84 bytes from 190.108.20.2 icmp_seq=4 ttl=63 time=10.523 ms
84 bytes from 190.108.20.2 icmp_seq=5 ttl=63 time=8.667 ms

PC3>

```

Figura 36. Ping 2 Corrección de conectividad entre PC SW-BB

```
PC4> ping 190.108.20.5
190.108.20.5 icmp_seq=1 timeout
190.108.20.5 icmp_seq=2 timeout
84 bytes from 190.108.20.5 icmp_seq=3 ttl=63 time=18.477 ms
84 bytes from 190.108.20.5 icmp_seq=4 ttl=63 time=6.356 ms
84 bytes from 190.108.20.5 icmp_seq=5 ttl=63 time=12.574 ms

PC4> ping 190.108.30.6
190.108.30.6 icmp_seq=1 timeout
84 bytes from 190.108.30.6 icmp_seq=2 ttl=63 time=6.545 ms
84 bytes from 190.108.30.6 icmp_seq=3 ttl=63 time=21.213 ms
84 bytes from 190.108.30.6 icmp_seq=4 ttl=63 time=4.393 ms
84 bytes from 190.108.30.6 icmp_seq=5 ttl=63 time=13.141 ms

PC4> █

PC5> ping 190.108.10.4
84 bytes from 190.108.10.4 icmp_seq=1 ttl=255 time=23.479 ms
84 bytes from 190.108.10.4 icmp_seq=2 ttl=255 time=21.052 ms
84 bytes from 190.108.10.4 icmp_seq=3 ttl=255 time=50.655 ms
84 bytes from 190.108.10.4 icmp_seq=4 ttl=255 time=22.387 ms
84 bytes from 190.108.10.4 icmp_seq=5 ttl=255 time=20.625 ms

PC5> ping 190.108.30.6
84 bytes from 190.108.30.6 icmp_seq=1 ttl=63 time=19.814 ms
84 bytes from 190.108.30.6 icmp_seq=2 ttl=63 time=3.171 ms
84 bytes from 190.108.30.6 icmp_seq=3 ttl=63 time=4.745 ms
84 bytes from 190.108.30.6 icmp_seq=4 ttl=63 time=10.333 ms
84 bytes from 190.108.30.6 icmp_seq=5 ttl=63 time=19.339 ms

PC5> █

PC6> ping 190.108.20.5
84 bytes from 190.108.20.5 icmp_seq=1 ttl=255 time=21.597 ms
84 bytes from 190.108.20.5 icmp_seq=2 ttl=255 time=22.081 ms
84 bytes from 190.108.20.5 icmp_seq=3 ttl=255 time=26.680 ms
84 bytes from 190.108.20.5 icmp_seq=4 ttl=255 time=252.228 ms
84 bytes from 190.108.20.5 icmp_seq=5 ttl=255 time=30.919 ms

PC6> ping 190.108.10.4
84 bytes from 190.108.10.4 icmp_seq=1 ttl=255 time=79.280 ms
84 bytes from 190.108.10.4 icmp_seq=2 ttl=255 time=46.443 ms
84 bytes from 190.108.10.4 icmp_seq=3 ttl=255 time=45.335 ms
84 bytes from 190.108.10.4 icmp_seq=4 ttl=255 time=39.000 ms
84 bytes from 190.108.10.4 icmp_seq=5 ttl=255 time=25.261 ms

PC6> █
```

Figura 37. Ping 2 corrección de conectividad entre PC SW-CC

```
PC7> ping 190.108.20.8
84 bytes from 190.108.20.8 icmp_seq=1 ttl=63 time=9.912 ms
84 bytes from 190.108.20.8 icmp_seq=2 ttl=63 time=9.003 ms
84 bytes from 190.108.20.8 icmp_seq=3 ttl=63 time=7.349 ms
84 bytes from 190.108.20.8 icmp_seq=4 ttl=63 time=24.040 ms
84 bytes from 190.108.20.8 icmp_seq=5 ttl=63 time=7.627 ms

PC7> ping 190.108.30.9
84 bytes from 190.108.30.9 icmp_seq=1 ttl=63 time=5.951 ms
84 bytes from 190.108.30.9 icmp_seq=2 ttl=63 time=7.206 ms
84 bytes from 190.108.30.9 icmp_seq=3 ttl=63 time=14.010 ms
84 bytes from 190.108.30.9 icmp_seq=4 ttl=63 time=8.806 ms
84 bytes from 190.108.30.9 icmp_seq=5 ttl=63 time=6.511 ms

PC7> █

PC8> ping 190.108.10.7
84 bytes from 190.108.10.7 icmp_seq=1 ttl=63 time=14.803 ms
84 bytes from 190.108.10.7 icmp_seq=2 ttl=63 time=16.290 ms
84 bytes from 190.108.10.7 icmp_seq=3 ttl=63 time=16.461 ms
84 bytes from 190.108.10.7 icmp_seq=4 ttl=63 time=15.300 ms
84 bytes from 190.108.10.7 icmp_seq=5 ttl=63 time=11.303 ms

PC8> ping 190.108.30.9
84 bytes from 190.108.30.9 icmp_seq=1 ttl=63 time=19.450 ms
84 bytes from 190.108.30.9 icmp_seq=2 ttl=63 time=7.512 ms
84 bytes from 190.108.30.9 icmp_seq=3 ttl=63 time=13.202 ms
84 bytes from 190.108.30.9 icmp_seq=4 ttl=63 time=4.703 ms
84 bytes from 190.108.30.9 icmp_seq=5 ttl=63 time=6.876 ms

PC8> █

PC9> ping 190.108.10.7
84 bytes from 190.108.10.7 icmp_seq=1 ttl=63 time=10.969 ms
84 bytes from 190.108.10.7 icmp_seq=2 ttl=63 time=16.596 ms
84 bytes from 190.108.10.7 icmp_seq=3 ttl=63 time=24.868 ms
84 bytes from 190.108.10.7 icmp_seq=4 ttl=63 time=6.264 ms
84 bytes from 190.108.10.7 icmp_seq=5 ttl=63 time=18.012 ms

PC9> ping 190.108.20.8
84 bytes from 190.108.20.8 icmp_seq=1 ttl=63 time=27.976 ms
84 bytes from 190.108.20.8 icmp_seq=2 ttl=63 time=35.226 ms
84 bytes from 190.108.20.8 icmp_seq=3 ttl=63 time=8.730 ms
84 bytes from 190.108.20.8 icmp_seq=4 ttl=63 time=34.246 ms
84 bytes from 190.108.20.8 icmp_seq=5 ttl=63 time=15.983 ms

PC9> █
```

Como se puede observar se ha solucionado el problema de conectividad entre los host conectados a los conmutadores, ahora se realizara prueba ping entre los equipos que se encuentran asociados a las VLAN.

Figura 38. Ping entre PC Vlan 10

```
PC1> ping 190.108.10.4
84 bytes from 190.108.10.4 icmp_seq=1 ttl=64 time=25.262 ms
84 bytes from 190.108.10.4 icmp_seq=2 ttl=64 time=46.356 ms
84 bytes from 190.108.10.4 icmp_seq=3 ttl=64 time=40.086 ms
84 bytes from 190.108.10.4 icmp_seq=4 ttl=64 time=34.579 ms
84 bytes from 190.108.10.4 icmp_seq=5 ttl=64 time=38.792 ms

PC1> ping 190.108.10.7
84 bytes from 190.108.10.7 icmp_seq=1 ttl=64 time=34.813 ms
84 bytes from 190.108.10.7 icmp_seq=2 ttl=64 time=23.137 ms
84 bytes from 190.108.10.7 icmp_seq=3 ttl=64 time=28.119 ms
84 bytes from 190.108.10.7 icmp_seq=4 ttl=64 time=15.872 ms
84 bytes from 190.108.10.7 icmp_seq=5 ttl=64 time=14.830 ms

PC1> █

PC4> ping 190.108.10.1
84 bytes from 190.108.10.1 icmp_seq=1 ttl=64 time=21.988 ms
84 bytes from 190.108.10.1 icmp_seq=2 ttl=64 time=24.377 ms
84 bytes from 190.108.10.1 icmp_seq=3 ttl=64 time=31.758 ms
84 bytes from 190.108.10.1 icmp_seq=4 ttl=64 time=34.119 ms
84 bytes from 190.108.10.1 icmp_seq=5 ttl=64 time=55.200 ms

PC4> ping 190.108.10.7
84 bytes from 190.108.10.7 icmp_seq=1 ttl=64 time=40.944 ms
84 bytes from 190.108.10.7 icmp_seq=2 ttl=64 time=26.250 ms
84 bytes from 190.108.10.7 icmp_seq=3 ttl=64 time=23.830 ms
84 bytes from 190.108.10.7 icmp_seq=4 ttl=64 time=49.767 ms
84 bytes from 190.108.10.7 icmp_seq=5 ttl=64 time=18.514 ms

PC4> █

PC7> ping 190.108.10.1
84 bytes from 190.108.10.1 icmp_seq=1 ttl=64 time=53.778 ms
84 bytes from 190.108.10.1 icmp_seq=2 ttl=64 time=25.089 ms
84 bytes from 190.108.10.1 icmp_seq=3 ttl=64 time=16.752 ms
84 bytes from 190.108.10.1 icmp_seq=4 ttl=64 time=22.062 ms
84 bytes from 190.108.10.1 icmp_seq=5 ttl=64 time=23.072 ms

PC7> ping 190.108.10.4
84 bytes from 190.108.10.4 icmp_seq=1 ttl=64 time=32.580 ms
84 bytes from 190.108.10.4 icmp_seq=2 ttl=64 time=22.278 ms
84 bytes from 190.108.10.4 icmp_seq=3 ttl=64 time=27.927 ms
84 bytes from 190.108.10.4 icmp_seq=4 ttl=64 time=71.207 ms
84 bytes from 190.108.10.4 icmp_seq=5 ttl=64 time=18.710 ms

PC7> █
```

Figura 39. Ping entre PC Vlan 25

```
PC2> ping 190.108.20.5
84 bytes from 190.108.20.5 icmp_seq=1 ttl=255 time=40.929 ms
84 bytes from 190.108.20.5 icmp_seq=2 ttl=255 time=18.618 ms
84 bytes from 190.108.20.5 icmp_seq=3 ttl=255 time=86.926 ms
84 bytes from 190.108.20.5 icmp_seq=4 ttl=255 time=20.312 ms
84 bytes from 190.108.20.5 icmp_seq=5 ttl=255 time=18.769 ms

PC2> ping 190.108.20.8
84 bytes from 190.108.20.8 icmp_seq=1 ttl=64 time=56.577 ms
84 bytes from 190.108.20.8 icmp_seq=2 ttl=64 time=19.774 ms
84 bytes from 190.108.20.8 icmp_seq=3 ttl=64 time=36.469 ms
84 bytes from 190.108.20.8 icmp_seq=4 ttl=64 time=18.250 ms
84 bytes from 190.108.20.8 icmp_seq=5 ttl=64 time=40.421 ms

PC2> █

PC5> ping 190.108.20.2
84 bytes from 190.108.20.2 icmp_seq=1 ttl=64 time=46.365 ms
84 bytes from 190.108.20.2 icmp_seq=2 ttl=64 time=49.758 ms
84 bytes from 190.108.20.2 icmp_seq=3 ttl=64 time=48.474 ms
84 bytes from 190.108.20.2 icmp_seq=4 ttl=64 time=29.005 ms
84 bytes from 190.108.20.2 icmp_seq=5 ttl=64 time=26.910 ms

PC5> ping 190.108.20.8
84 bytes from 190.108.20.8 icmp_seq=1 ttl=64 time=33.122 ms
84 bytes from 190.108.20.8 icmp_seq=2 ttl=64 time=34.456 ms
84 bytes from 190.108.20.8 icmp_seq=3 ttl=64 time=25.951 ms
84 bytes from 190.108.20.8 icmp_seq=4 ttl=64 time=56.936 ms
84 bytes from 190.108.20.8 icmp_seq=5 ttl=64 time=33.372 ms

PC5> █

PC8> ping 190.108.20.2
84 bytes from 190.108.20.2 icmp_seq=1 ttl=64 time=19.998 ms
84 bytes from 190.108.20.2 icmp_seq=2 ttl=64 time=28.612 ms
84 bytes from 190.108.20.2 icmp_seq=3 ttl=64 time=30.176 ms
84 bytes from 190.108.20.2 icmp_seq=4 ttl=64 time=16.917 ms
84 bytes from 190.108.20.2 icmp_seq=5 ttl=64 time=27.140 ms

PC8> ping 190.108.20.5
84 bytes from 190.108.20.5 icmp_seq=1 ttl=255 time=39.078 ms
84 bytes from 190.108.20.5 icmp_seq=2 ttl=255 time=12.614 ms
84 bytes from 190.108.20.5 icmp_seq=3 ttl=255 time=29.434 ms
84 bytes from 190.108.20.5 icmp_seq=4 ttl=255 time=11.887 ms
84 bytes from 190.108.20.5 icmp_seq=5 ttl=255 time=8.915 ms

PC8> █
```

Figura 40. Ping entre PC Vlan 30

```

PC3> ping 190.108.30.6
84 bytes from 190.108.30.6 icmp_seq=1 ttl=64 time=21.099 ms
84 bytes from 190.108.30.6 icmp_seq=2 ttl=64 time=105.073 ms
84 bytes from 190.108.30.6 icmp_seq=3 ttl=64 time=41.982 ms
84 bytes from 190.108.30.6 icmp_seq=4 ttl=64 time=64.211 ms
84 bytes from 190.108.30.6 icmp_seq=5 ttl=64 time=49.575 ms

PC3> ping 190.108.30.9
84 bytes from 190.108.30.9 icmp_seq=1 ttl=64 time=28.254 ms
84 bytes from 190.108.30.9 icmp_seq=2 ttl=64 time=55.188 ms
84 bytes from 190.108.30.9 icmp_seq=3 ttl=64 time=49.041 ms
84 bytes from 190.108.30.9 icmp_seq=4 ttl=64 time=21.182 ms
84 bytes from 190.108.30.9 icmp_seq=5 ttl=64 time=24.915 ms

PC3>

PC6> ping 190.108.30.3
84 bytes from 190.108.30.3 icmp_seq=1 ttl=255 time=37.096 ms
84 bytes from 190.108.30.3 icmp_seq=2 ttl=255 time=50.959 ms
84 bytes from 190.108.30.3 icmp_seq=3 ttl=255 time=70.911 ms
84 bytes from 190.108.30.3 icmp_seq=4 ttl=255 time=75.001 ms
84 bytes from 190.108.30.3 icmp_seq=5 ttl=255 time=64.357 ms

PC6> ping 190.108.30.9
84 bytes from 190.108.30.9 icmp_seq=1 ttl=64 time=48.471 ms
84 bytes from 190.108.30.9 icmp_seq=2 ttl=64 time=33.786 ms
84 bytes from 190.108.30.9 icmp_seq=3 ttl=64 time=25.239 ms
84 bytes from 190.108.30.9 icmp_seq=4 ttl=64 time=26.548 ms
84 bytes from 190.108.30.9 icmp_seq=5 ttl=64 time=17.808 ms

PC6>

PC9> ping 190.108.30.3
84 bytes from 190.108.30.3 icmp_seq=1 ttl=255 time=82.124 ms
84 bytes from 190.108.30.3 icmp_seq=2 ttl=255 time=9.506 ms
84 bytes from 190.108.30.3 icmp_seq=3 ttl=255 time=7.845 ms
84 bytes from 190.108.30.3 icmp_seq=4 ttl=255 time=5.938 ms
84 bytes from 190.108.30.3 icmp_seq=5 ttl=255 time=7.565 ms

PC9> ping 190.108.30.6
84 bytes from 190.108.30.6 icmp_seq=1 ttl=64 time=33.247 ms
84 bytes from 190.108.30.6 icmp_seq=2 ttl=64 time=16.902 ms
84 bytes from 190.108.30.6 icmp_seq=3 ttl=64 time=39.327 ms
84 bytes from 190.108.30.6 icmp_seq=4 ttl=64 time=14.001 ms
84 bytes from 190.108.30.6 icmp_seq=5 ttl=64 time=19.833 ms

```

El ping es exitoso entre los PC que están en las vlan y en los diferentes switches esto es gracias a que la configuración de los puertos troncales, los host están conectados a puertos asociados a estas vlan y a que se aplicó la configuración en las SVI de las vlan 10, 25 y 30 la cual no se suministro para el desarrollo del presente escenario.

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

Esta prueba se realizara ejecutando el ping hacia las SVI de la vlan 99 de cada switch.

Figura 41. Pin entre switch SVI Vlan's 99

```

SW-AA#ping 190.108.99.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 19/27/47 ms
SW-AA#ping 190.108.99.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 13/17/20 ms
SW-AA#

SW-BB#ping 190.108.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/31/44 ms
SW-BB#ping 190.108.99.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 11/23/29 ms
SW-BB#

SW-CC#ping 190.108.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/35/66 ms
SW-CC#ping 190.108.99.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/33/100 ms
SW-CC#

```

El ping es exitoso gracias a que se tiene una configuración correcta se los puertos troncales y el direccionamiento esta bien configurado.

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

Se realizara prueba de ping desde cada switch hacia los PC conectados en sus interfaces.

Figura 42. Ping desde SW-AA hacia PC1, 2 y 3

```
SW-AA#ping 190.108.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/10/25 ms
SW-AA#ping 190.108.20.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/16/33 ms
SW-AA#ping 190.108.30.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/18/53 ms
SW-AA#
```

Figura 43. Ping desde SW-BB hacia PC4, 5 y 6

```
SW-BB#ping 190.108.10.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 5/6/9 ms
SW-BB#ping 190.108.20.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.5, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 9/16/22 ms
SW-BB#ping 190.108.30.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/7/21 ms
SW-BB#
```

Figura 44. Ping desde SW-CC hacia PC7, 8 y 9

```
SW-CC#ping 190.108.10.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.7, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/12/32 ms
SW-CC#ping 190.108.20.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/28/97 ms
SW-CC#ping 190.108.30.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.9, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/28/88 ms
SW-CC#
```

El ping es exitoso gracias a los ajustes realizados en las pruebas iniciales al encontrar el fallo de que las SVI de las Vlan 10, 25 y 30 no se habían configurado ya que no se tenía los parámetros de direccionamiento estos se configuraron y eligieron a criterio propio escogiendo ip dentro del mismo segmento de las configuradas en los PC, estas direcciones fueron el punto de partida para elegir el direccionamiento ip para las interfaces virtuales de las Vlan en mención.

CONCLUSIONES

Se aplican los conocimientos obtenidos en el desarrollo del diplomado y los adquiridos en los módulos de CCNP (route y switch)para la configuración de router y switches cisco especialmente la configuración de los puertos para establecer enlaces troncales y las distintas maneras de realizarlo como son los son de manera automática empleando DTP o manualmente estableciendo los puertos en modo trunk.

Se afianzan los conocimientos a cerca de las formas de configurar enrutamiento en una red que este compuesta por dispositivos de capa 3, dichas técnicas de enrutamiento van desde el enrutamiento estático, en el cual se añaden las rutas de manera manual hasta el uso de protocolos de enrutamiento dinámico que dependiendo de su estructura algorítmica establecen adyacencias de vecindad con los equipos que ejecuten este tipo de protocolos y estén en la misma red.

Se identifican los diferencias de los protocolos de enrutamiento los cuales pueden ser de Gateway interior (IBG) o de Gateway exterior (EGP), y los entornos en los que se pueden aplicar cada uno de ellos teniendo en cuenta sus características.

Empleando la configuración de VLAN se disminuye el trafico de difusión comprendiendo de esta manera que se puede optimizar la red y se facilita su administración a través de la implementación de este tipo de interfaces lógicas virtuales.

BIBLIOGRAFÍA

- Bojorquez, M. (2017). *Analisis de la Factibilidad Tecnica y Economica para la Migracion de una red Metro-Ethernet en STP a EAPS*. Tesis, UNIVERSIDAD DE SAN CARLOS DE GUATEMALA , Guatemala.
- Carpio, C. (2018). *Implementacion de un Esquema de Redundancia en la Red de Gestion de Americatel, Mediante el uso del Protocolo HSRP y SLA, en la Sede Principal Olguin*. Lima.
- Castillo Porturas, A. N. (2015). *Implementación de redes virtuales utilizando Vlan para reducir el tamaño del dominio de difusión de la red en el Inabib*. UCH UNIVERSIDAD DE CIENCIAS Y HUMANIDADES , Tesis, Lima . Obtenido de Repositorio UHC.
- Delgado Vallejo, S. S. (2010). *Adaptacion del protocolo BGP-4 para Reducir la Congestion en Redes IP*. Tesis, Popayan.