

**DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP**

DAIRO JOSE SANCHEZ RICARDO

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECBTI
INGENIERÍA ELECTRÓNICA
BARRANQUILLA
2020**

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DAIRO JOSE SANCHEZ RICARDO

Diplomado de opción de grado presentado para optar el
título de INGENIERO ELECTRONICO

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ECBTI
INGENIERÍA ELECTRÓNICA
BARRANQUILLA
2020

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Barranquilla, 22 de mayo de 2020

AGRADECIMIENTOS

A Dios por ayudarme en este camino, por la vida que me ha dado, por la sabiduría para enfrentar los retos del día a día, y la capacidad de entendimiento para salir adelante y cumplir mis metas.

A mi amada esposa por su entereza y paciencia, y por ese gran apoyo que me ha brindado.

A mis padres Adolfo Sánchez y Candelaria Sampayo, por enseñarme a valerme por sí mismo, en búsqueda de mi futuro profesional y el gran esfuerzo que siempre dedicaron para que logre superarme, mil gracias por todo.

A la Universidad Nacional Abierta y a Distancia, a los tutores y directores de curso que hicieron parte del conocimiento que he adquirido y el cual pondré al servicio de mi país, muchas gracias.

CONTENIDO

AGRADECIMIENTOS	4
CONTENIDO	5
LISTA DE TABLAS	6
LISTA DE FIGURAS	7
GLOSARIO	9
RESUMEN	10
ABSTRACT	10
INTRODUCCIÓN	11
DESARROLLO	11
1. Escenario 1	13
1.1 Configuración relación de vecino BGP router R1 y R2	14
1.2 Configuración de interfaz loopback R1 y R2.....	15
1.3 Configuración de interfaz loopback R2 y R3.....	17
1.4 Configuración de interfaz loopback R3 y R4.....	20
2. Escenario 2	22
2.1 Configurar VTP	23
2.2 Configurar DTP (Dynamic Trunking Protocol).....	26
2.3 Agregar VLANs y asignar puertos.....	30
2.4 Configurar las direcciones IP en los Switches.....	36
2.4 Verificar la conectividad Extremo a Extremo.....	37
CONCLUSIONES	46
BIBLIOGRAFÍA.....	47

LISTA DE TABLAS

Tabla 1. Interfaces loopback para crear R1.....	13
Tabla 2. Interfaces loopback para crear R2.....	13
Tabla 3. Interfaces loopback para crear R3.....	14
Tabla 4. Interfaces loopback para crear R4.....	14
Tabla 5. Configuración direcciones IP.....	32
Tabla 6. Configurar las direcciones IP en los switch.....	37

LISTA DE FIGURAS

Figura 1. Escenario 1 -----	12
Figura 2. Simulación de escenario 1-----	12
Figura 3. Ejecución comando show ip route en R1 -----	17
Figura 4. Ejecución comando show ip route en R2-----	17
Figura 5. Ejecución comando show ip route en R2-----	19
Figura 6. Ejecución comando show ip route en R3-----	19
Figura 7. Ejecución comando show ip route en R3-----	21
Figura 8. Ejecución comando show ip route en R4-----	22
Figura 9. Escenario 2 -----	22
Figura 10. Simulación del escenario 2 -----	23
Figura 11. Ejecución comando show vtp status en SW-AA -----	24
Figura 12. Ejecución comando show vtp status en SW-BB -----	25
Figura 13. Ejecución comando show vtp status en SW-CC -----	25
Figura 14. Ejecución comando show interfaces trunk desde SW-AA-----	27
Figura 15. Ejecución comando show interfaces trunk -----	27
Figura 16. Ejecución comando show interfaces trunk desde SW-AA-----	28
Figura 17. Ejecución comando show interfaces trunk en SW-BB-----	29
Figura 18. Ejecución comando show interfaces trunk en SW-CC -----	30
Figura 19. VLANs agregadas en SW-AA. -----	31
Figura 20. VLANs agregadas en SW-BB-----	32
Figura 21. Configuración dirección IP en PC1 -----	32
Figura 22. Configuración dirección IP en PC2 -----	33
Figura 23. Configuración dirección IP en PC3 -----	33
Figura 24. Configuración dirección IP en PC4 -----	35
Figura 25. Configuración dirección IP en PC5 -----	35
Figura 26. Configuración dirección IP en PC6 -----	35
Figura 27. Configuración dirección IP en PC7 -----	36
Figura 28. Configuración dirección IP en PC8-----	36

LISTA DE FIGURAS

Figura 29. Configuración dirección IP en PC9 -----	36
Figura 30. Ping exitoso desde PC1 a PC4, PC7 -----	38
Figura 31. Ping exitoso desde PC4 a PC1, PC7 -----	38
Figura 32. Ping exitoso desde PC7 a PC1, PC4 -----	39
Figura 33. Ping no exitoso desde PC1 a PC5, PC9 -----	39
Figura 34. Ping desde PC9 a PC4, PC6 -----	40
Figura 35. Ping desde PC5 a PC3, PC8 -----	40
Figura 36. Ping desde SW-AA a SW-BB, SW-CC -----	41
Figura 37. Ping desde SW-BB a SW-AA, SW-CC -----	41
Figura 38. Ping desde SW-CC a SW-AA, SW-BB -----	42
Figura 39. Ping desde SW-AA a PCs -----	43
Figura 40. Ping desde SW-BB a PCs -----	44
Figura 41. Ping desde SW-CC a PCs -----	45

GLOSARIO

BGP: de sus siglas en inglés Border Gateway Protocol, es un protocolo que administra cómo se enrutan los paquetes a través de Internet a través del intercambio de información de enrutamiento y accesibilidad entre enrutadores de borde.

DTP: de sus siglas en inglés Dynamic Trunking Protocol, es un protocolo de enlace dinámico se utiliza para negociar la formación de un enlace troncal entre dos dispositivos Cisco. Este protocolo provoca un aumento del tráfico y está habilitado de forma predeterminada, pero puede deshabilitarse.

IP: de sus siglas en inglés Internet Protocol, es un protocolo para la comunicación de datos a través de una red de paquetes conmutados. Una dirección IP es una secuencia de números única que identifica un dispositivo y le permite comunicarse con otros dentro de una red que utiliza el protocolo IP.

Loopback: La interfaz de bucle invertido es una interfaz virtual que se puede crear en los enrutadores. Como es virtual, no depende de ninguna interfaz física y, por lo tanto, siempre está activa.

SVI: de sus siglas en inglés Switch Virtual Interface, es una interface virtual, como su nombre lo indica. Funciona como una interfaz Capa 2 y Capa 3 y generalmente son la puerta de enlace para los usuarios que pertenecen a este dominio de broadcast (vlan).

VLAN: Las redes de área local virtual o VLAN son una de las tecnologías de red más recientes y geniales desarrolladas en los últimos años, aunque solo recientemente han comenzado a ganar reconocimiento

VTP: de sus siglas en inglés VLAN Trunk Protocol, Sirve para centralizar en un solo switch la administración de todas las VLANs.

RESUMEN

En este trabajo se presentará la implementación y ejecución práctica de dos escenarios diferentes, los cuales serán configurados de acuerdo con las competencias adquiridas durante el estudio de las infraestructuras de redes de comunicaciones, aprendidas durante las actividades evaluativas del diplomado de profundización CISCO CCNP, también se pondrá en práctica las competencias aprendidas durante el desarrollo de las pruebas realizadas, teniendo en cuenta las topologías de dos escenarios diferentes, en donde configuraremos el enrutamiento de redes, y la conmutación de dispositivos electrónicos para la administración de información dentro de una misma red. También conoceremos los protocolos de comunicación de redes que implementaremos, así como su evaluación en simuladores de redes como es GNS3 y CISCO Packet Tracer, en donde conectaremos y configuraremos los diferentes módulos de red para su correcta conectividad y así poder establecer los diferentes servicios administrativos, los cuales nos permitirán establecer comunicación, control y monitoreo de la redes locales y globales, buscando de esta manera beneficios y seguridad a los usuarios finales.

Palabras Clave: CISCO, CCNP, GNS3, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

In this work, the implementation and practical execution of two different scenarios will be presented, which will be configured in accordance with the skills acquired during the study of communication network infrastructures, learned during the evaluative activities of the CISCO CCNP deepening diploma course. will put into practice the skills learned during the development of the tests carried out, considering the topologies of two different scenarios, where we will configure the routing of networks, and the switching of electronic devices for the administration of information within the same network. We will also know the network communication protocols that we will implement, as well as their evaluation in network simulators such as GNS3 and CISCO Packet Tracer, where we will connect and configure the different network modules for their correct connectivity and thus be able to establish the different administrative services, which will allow us to establish communication, control and monitoring of local and global networks, thus seeking benefits and security for end users.

Keywords: CISCO, CCNP, GNS3, Routing, Switching, Networking, Electronics.

INTRODUCCIÓN

El diplomado profesional en redes CISCO CCNP, tiene como objetivo principal preparar profesionales idóneos para implementar tecnologías adecuadas para la construcción de infraestructura de redes basados en dispositivos como routers, y switches entre los sistemas de intercambio de información WANs, relacionadas con el diseño de topologías de redes y sistemas de enrutamiento, logrando mejorar el tráfico de información, la seguridad, y el rendimiento de los sistemas LANs, así como también la creación de intranets locales y globales.

En el primer escenario se presentará los pasos para habilitar el encaminamiento con el protocolo BGP, teniendo en cuenta la topología del escenario uno, en el cual se desarrollará ejecutando líneas de comandos específicos e implementados para la correcta configuración de los routers que veremos en esta prueba, así como la configuración de interfaz de red virtual Loopback, y el acceso entre la relación de vecinos BGP, para el intercambio de información entre los enrutadores del sistema.

En el segundo escenario veremos cómo centralizar las VLANs entre cada conmutador de la red, y configurar enlaces troncales dinámicos y estáticos en cada uno de los switches según cada situación presentada para su correcta configuración, y los accesos entre VLANs creadas según los requerimientos del problema presentado; aquí ejecutaremos comandos que nos ayudarán a establecer comunicación entre las redes de área local virtual o VLAN, y rutas troncales para la interconexión de redes a través de dispositivos electrónicos de comunicación como son los switches, estas tecnologías de redes nos ayudan a tener mejor y más conectividad de datos para el usuario final, ya que nos permitirá facilidad y seguridad en la transferencia de datos entre diferentes VLANs.

DESARROLLO

1. ESCENARIO 1

Figura 1. Escenario 1

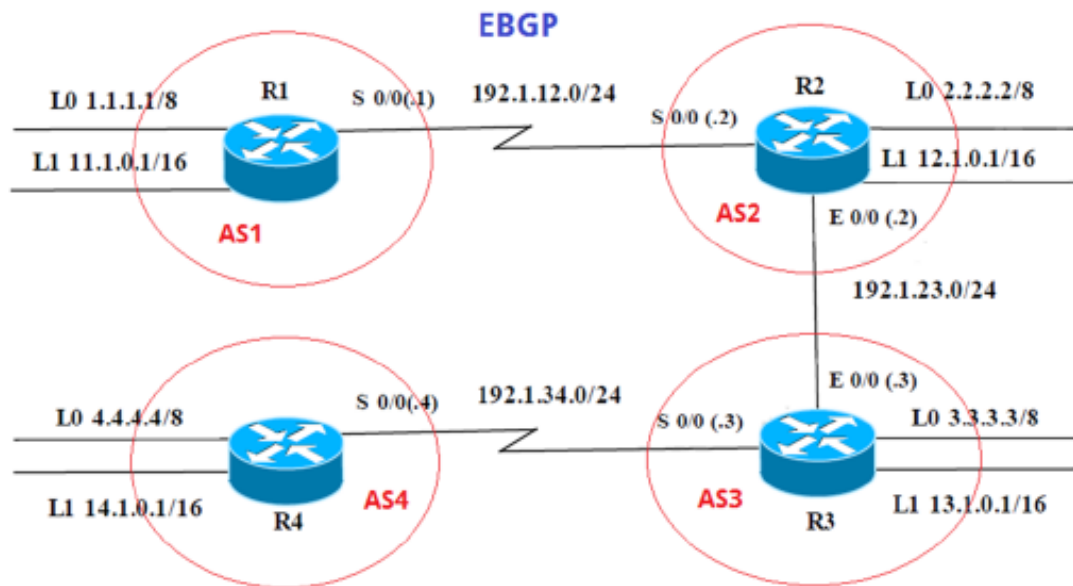
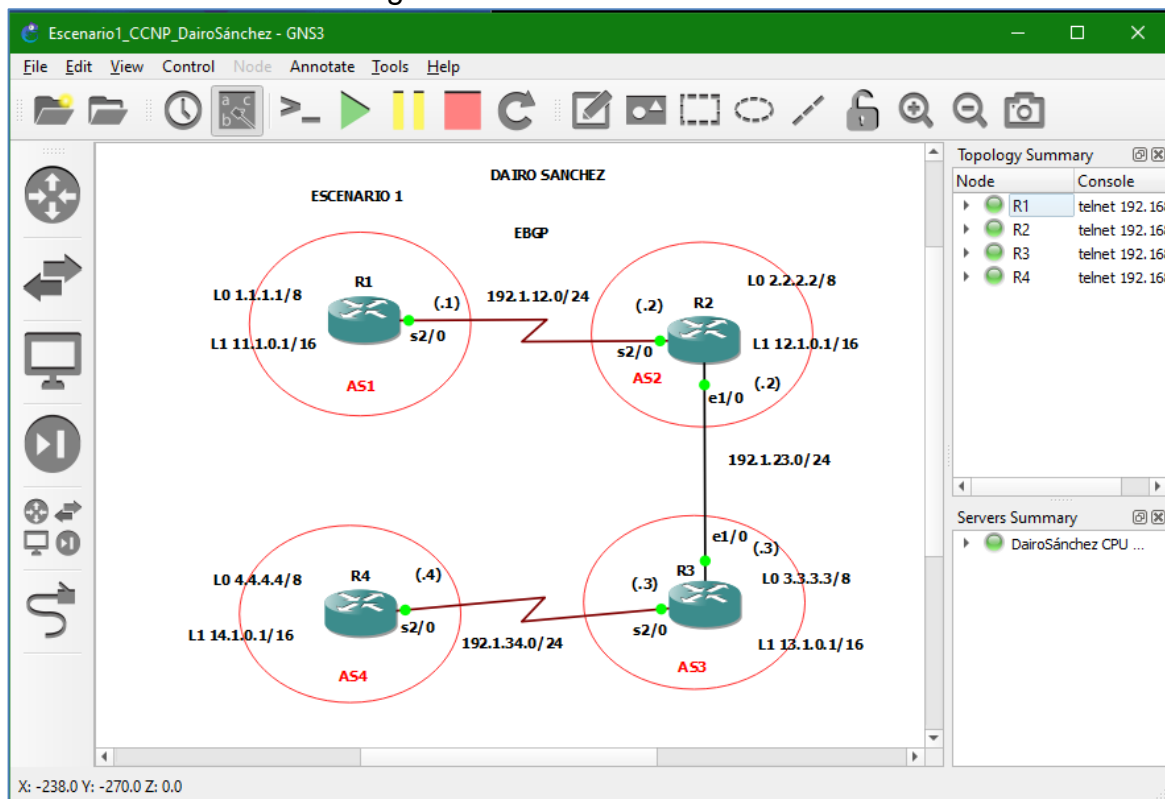


Figura 2. Simulación de escenario 1



Información para configuración de los Routers

Tabla 1. Interfaces loopback para crear 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
	S2/0	192.1.12.1	255.255.255.0

Tabla 2. Interfaces loopback para crear R2

R2	Interfaz	Dirección IP	Máscara
	Loopback 0	2.2.2.2	255.0.0.0
	Loopback 1	12.1.0.1	255.255.0.0
	S2/0	192.1.12.2	255.255.255.0
	E1/0	192.1.23.2	255.255.255.0

Tabla 3. Interfaces loopback para crear R3

	Interfaz	Dirección IP	Máscara
R3	Loopback 0	3.3.3.3	255.0.0.0
	Loopback 1	13.1.0.1	255.255.0.0
	E1/0	192.1.23.3	255.255.255.0
	S2/0	192.1.34.3	255.255.255.0

Tabla 4. Interfaces loopback para crear R4

	Interfaz	Dirección IP	Máscara
R4	Loopback 0	4.4.4.4	255.0.0.0
	Loopback 1	14.1.0.1	255.255.0.0
	S2/0	192.1.34.4	255.255.255.0

1. Configure una relación de vecino BGP entre R1 y R2. R1 debe estar en AS1 y R2 debe estar en AS2. Anuncie las direcciones de Loopback en BGP. Codifique los ID para los routers BGP como 22.22.22.22 para R1 y como 33.33.33.33 para R2. Presente el paso a con los comandos utilizados y la salida del comando *show ip route*.

Desarrollo paso a paso

Para el desarrollo de este primer escenario se realizará las configuraciones básicas de cada interfaz dispuesta la tabla de direccionamiento para cada router en el simulador de redes gráfico GNS3.

A continuación, se establecen las configuraciones de acuerdo con las tablas de direccionamiento y sus respectivas interfaz.

Router R1

```
R1#config term
R1(config)#
R1(config)#
R1(config)#int Lo0
R1(config-if)# ip address 1.1.1.1 255.0.0.0
R1(config-if)# int Lo1
R1(config-if)# ip address 11.1.0.1 255.255.0.0
R1(config-if)# int s2/0
R1(config-if)# ip address 192.1.12.1 255.255.255.0
R1(config-if)# no shut
```

```
R1(config-if)# exit
R1(config)#exit
R1#wr
```

Router R2

```
R2#config term
R2(config)#
R2(config)#
R2(config)#int Lo0
R2(config-if)# ip address 2.2.2.2 255.0.0.0
R2(config-if)# int Lo1
R2(config-if)# ip address 12.1.0.1 255.255.0.0
R2(config-if)# int e1/0
R2(config-if)# ip address 192.1.23.2 255.255.255.0
R2(config-if)# no shut
R2(config-if)# int s2/0
R2(config-if)# ip address 192.1.12.2 255.255.255.0
R2(config-if)# no shut
R2(config-if)# exit
R2(config)#exit
R2#wr
```

Router R3

```
R3#config term
R3(config)#
R3(config)#
R3(config)#int Lo0
R3(config-if)# ip address 3.3.3.3 255.0.0.0
R3(config-if)# int Lo1
R3(config-if)# ip address 13.1.0.1 255.255.0.0
R3(config-if)# int e1/0
R3(config-if)# ip address 192.1.23.3 255.255.255.0
R3(config-if)# no shut
R3(config-if)# int s2/0
R3(config-if)# ip address 192.1.34.3 255.255.255.0
R3(config-if)# no shut
R3(config-if)# exit
R3(config)#exit
R3#wr
```

Router R4

```
R4#config term
R4(config)#int Lo0
R4(config-if)# ip address 4.4.4.4 255.0.0.0
R4(config-if)# int Lo1
R4(config-if)# ip address 14.1.0.1 255.255.0.0
R4(config-if)# int s2/0
R4(config-if)# ip address 192.1.34.4 255.255.255.0
R4(config-if)# no shut
R4(config-if)# exit
R4(config)#exit
R4#wr
```

Ahora que ya sean configurado las direcciones IP en cada una de sus interfaces, se procede con la configuración del protocolo BGP teniendo en cuenta la codificación ID suministrada en el punto número 1.

Configuración de la relación de vecino entre R1 y R2.

Router R1

```
R1(config)#
R1(config)#router bgp 1
R1(config-router)# bgp router-id 22.22.22.22
R1(config-router)# neighbor 192.1.12.2 remote-as 2
R1(config-router)# network 1.0.0.0
R1(config-router)# network 11.1.0.0
R1(config-router)# network 192.1.12.0
R1(config-router)#exit
R1(config)#exit
R1#wr
```

Configuración de la relación de vecino entre R2 y R1.

Router R2

```
R2#config term
R2(config)#router bgp 2
R2(config-router)# bgp router-id 33.33.33.33
R2(config-router)# neighbor 192.1.12.1 remote-as 1
R2(config-router)# network 2.0.0.0
R2(config-router)# network 12.1.0.0
R2(config-router)# network 192.1.12.0
R2(config-router)# exit
R2(config)#exit
```


R2#wr

```
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, 00:00:40
  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
  192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.12.0/24 is directly connected, Serial2/0
L    192.1.12.1/32 is directly connected, Serial2/0
R1#
```

Figura 3. Ejecución comando show ip route

```
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, 00:01:51
  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
  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, Serial2/0
L    192.1.12.2/32 is directly connected, Serial2/0
R2#
```

Figura 4. Ejecución comando show ip route

2. Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en AS2 y R3 debería estar en AS3. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 44.44.44.44. Presente el paso a con los comandos utilizados y la salida del comando *show ip route*.

Configuración de la relación de vecino entre R2 y R3.

Router R2

```
R2#config term
R2(config)#router bgp 2
R2(config-router)# network 192.1.23.0 mask 255.255.255.0
R2(config-router)# neighbor 192.1.23.3 remote-as 3
R2(config-router)# end
R2#wr
```

Configuración de la relación de vecino entre R3 y R2.

Router R3

```
R3#config term
R3(config)#router bgp 3
R3(config-router)# bgp router-id 44.44.44.44
R3(config-router)# network 3.0.0.0 mask 255.0.0.0
R3(config-router)# network 13.1.0.0 mask 255.255.0.0
R3(config-router)# network 192.1.23.0 mask 255.255.255.0
R3(config-router)# neighbor 192.1.23.2 remote-as 2
R3(config-router)#exit
R3(config)#exit
R3#wr
```

Ahora se configura R3 para establecer la relación con los vecinos y su identificación

Router R3

```
R3#config term
R3(config)#router bgp 3
R3(config-router)# network 192.1.34.0 mask 255.255.255.0
R3(config-router)# neighbor 192.1.34.4 remote-as 4
R3(config-router)# end
R3#wr
```

```

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, 00:50:37
     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
L    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
L    192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.12.0/24 is directly connected, Serial2/0
L    192.1.12.2/32 is directly connected, Serial2/0
L    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, Ethernet1/0
L    192.1.23.2/32 is directly connected, Ethernet1/0
R2#

```

Figura 5. Ejecución comando show ip route

Como podemos observar R2 restablece los enrutamientos y nos muestra las direcciones Loopback configuradas en el router R3, lo que nos indica que ha asimilado las rutas con el protocolo BGP.

```

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, 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, 00:00:11
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:00:11
     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    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, 00:00:11
     192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, Ethernet1/0
L    192.1.23.3/32 is directly connected, Ethernet1/0
     192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial2/0
L    192.1.34.3/32 is directly connected, Serial2/0
R3#

```

Figura 6. Ejecución comando show ip route

El enrutador R3 ha actualizado su direcciones, las cuales ha reconocidos directamente gracias al protocolo BGP, y que fueron anunciadas en cada uno de los routers.

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 configura la relación de vecino BGP entre R3 y R4.

Router R3

```
R3#config term
R3(config)#router bgp 3
R3(config-router)# network 192.1.34.0 mask 255.255.255.0
R3(config-router)# neighbor 192.1.34.4 remote-as 4
R3(config-router)# end
R3#wr
```

Se configura la relación de vecino BGP entre R4 y R3 y se ejecutan los siguientes comandos:

Router R4

```
R4#config term
R4(config)#router bgp 4
R4(config-router)# bgp router-id 66.66.66.66
R4(config-router)# network 4.0.0.0 mask 255.0.0.0
R4(config-router)# network 14.1.0.0 mask 255.255.0.0
R4(config-router)# network 192.1.34.0 mask 255.255.255.0
R4(config-router)# neighbor 192.1.34.3 remote-as 3
R4(config-router)# exit
R4(config)#exit
R4#wr
```

Para establecer las relaciones de vecindad mediante las direcciones de Loopback, el router vecino necesita anunciar sobre el uso de esta interfaz en lugar de una interfaz física y, por tanto, se requiere una configuración para establecer los vecinos

Router R3

```
R3#config term
R3(config)#
R3(config)#ip route 4.0.0.0 255.0.0.0 192.1.34.4
```

```

R3(config)#router bgp 3
R3(config-router)# no neighbor 192.1.34.4
R3(config-router)# no network 3.0.0.0 mask 255.0.0.0
R3(config-router)# neighbor 4.4.4.4 remote-as 4
R3(config-router)# neighbor 4.4.4.4 update-source I0
R3(config-router)# neighbor 4.4.4.4 ebgp-multihop
R3(config-router)# end
R3#wr

```

Router R4

```

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

```

```

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, 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, 00:34:21
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:34:21
     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
S    4.0.0.0/8 [1/0] via 192.1.34.4
     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, 00:34:21
     192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, Ethernet1/0
L    192.1.23.3/32 is directly connected, Ethernet1/0
     192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial2/0
L    192.1.34.3/32 is directly connected, Serial2/0
R3#

```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved

Figura 7. Ejecución comando show ip route

```

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 - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

S    3.0.0.0/8 [1/0] via 192.1.34.3
C    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
C    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
C    192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial1/1
L    192.1.34.4/32 is directly connected, Serial1/1
R4#

```

Figura 8. Ejecución comando show ip route

Como se puede observar los resultados obtenidos con el comando show ip route, el enrutador R3 ha actualizado su direccionamiento y la dirección de red que conecta este dispositivo con R4, además ha cambiado su acceso con el enlace de R3, ahora corresponde a la dirección de Loopback 0, la cual aparece como una dirección estática.

2. ESCENARIO 2

Figura 9. Escenario 2

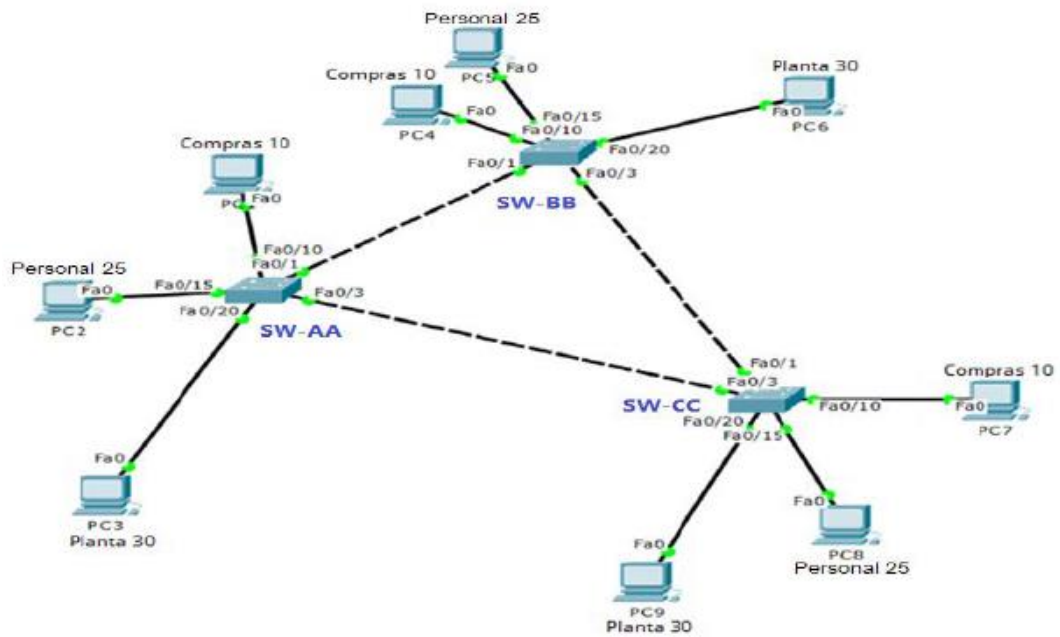
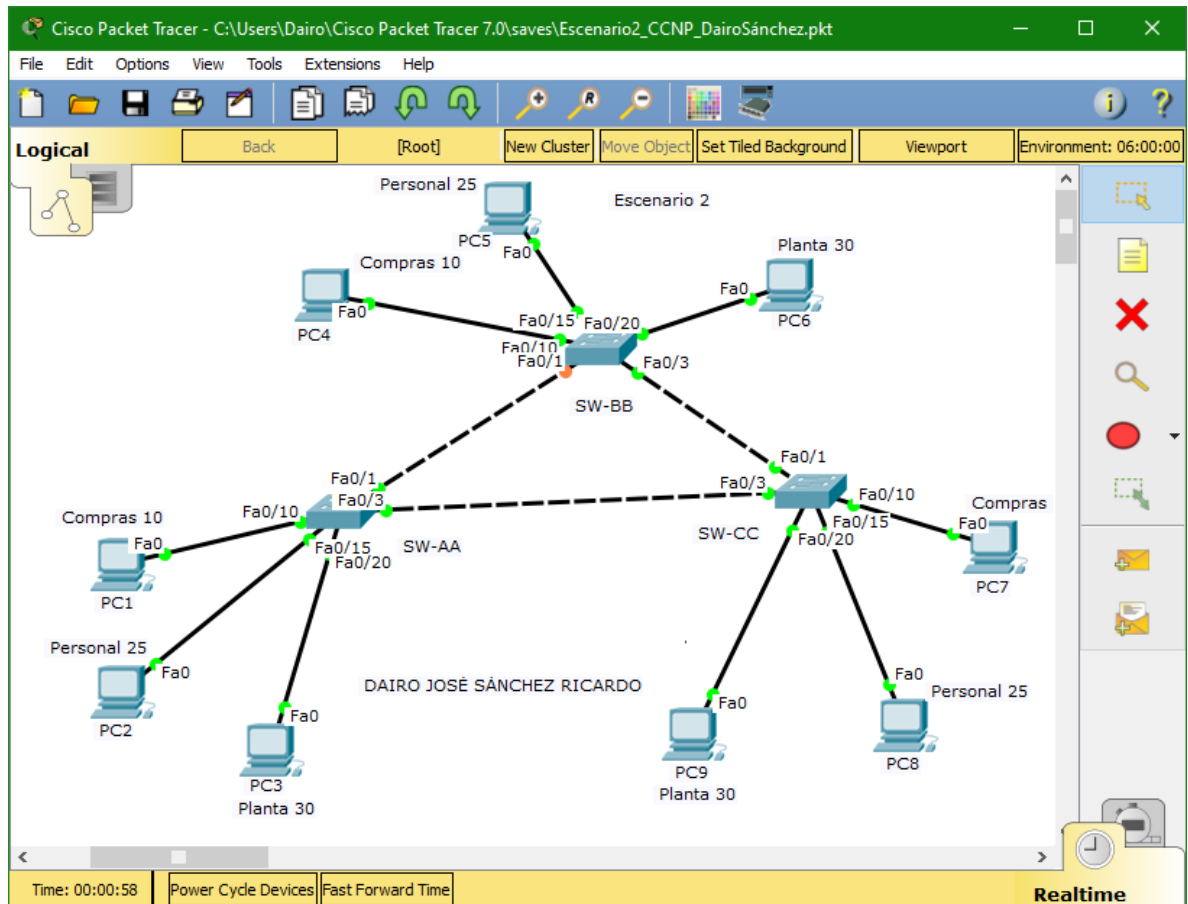


Figura 10. Simulación del escenario 2



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.

SWITCH SW-AA

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

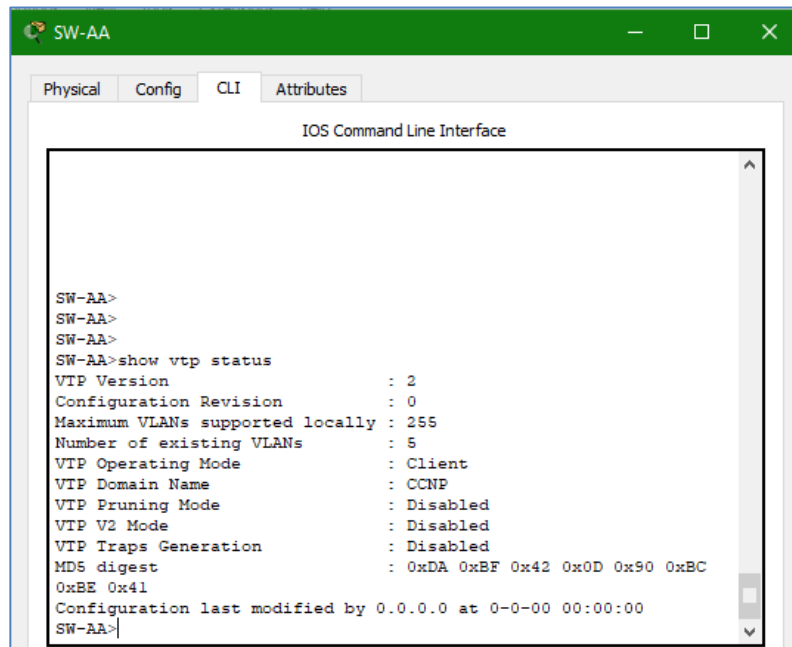
SWITCH SW-BB

```
Switch>ena
Switch#config term
Switch(config)#hostname SW-BB
SW-BB(config)#vtp mode server
SW-BB(config)#vtp domain CCNP
SW-BB(config)#vtp password cisco
SW-BB(config)#vtp version 2
SW-BB(config)#exit
SW-BB#wr
```

SWITCH SW-CC

```
Switch>ena
Switch#config term
Switch(config)#hostname SW-CC
SW-CC(config)#vtp domain CCNP
SW-CC(config)#vtp mode client
SW-CC(config)#vtp password cisco
SW-CC(config)#vtp version 2
SW-CC(config)#exit
SW-CC#wr
```

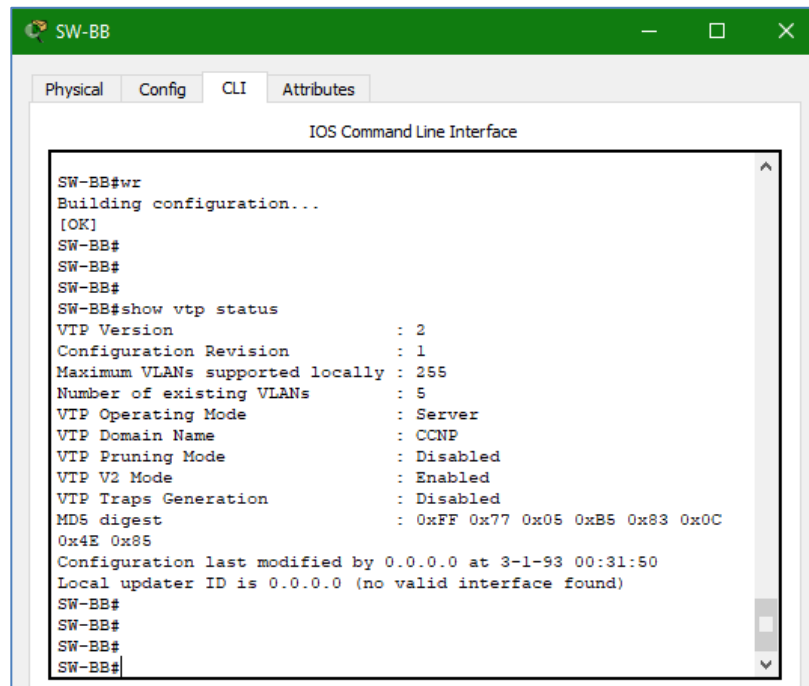
3. Verifique las configuraciones mediante el comando *show vtp status*.



```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface

SW-AA>
SW-AA>
SW-AA>
SW-AA>show vtp status
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode : Client
VTP Domain Name : CCNP
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xDA 0xBF 0x42 0x0D 0x90 0xBC
0xBE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SW-AA>
```

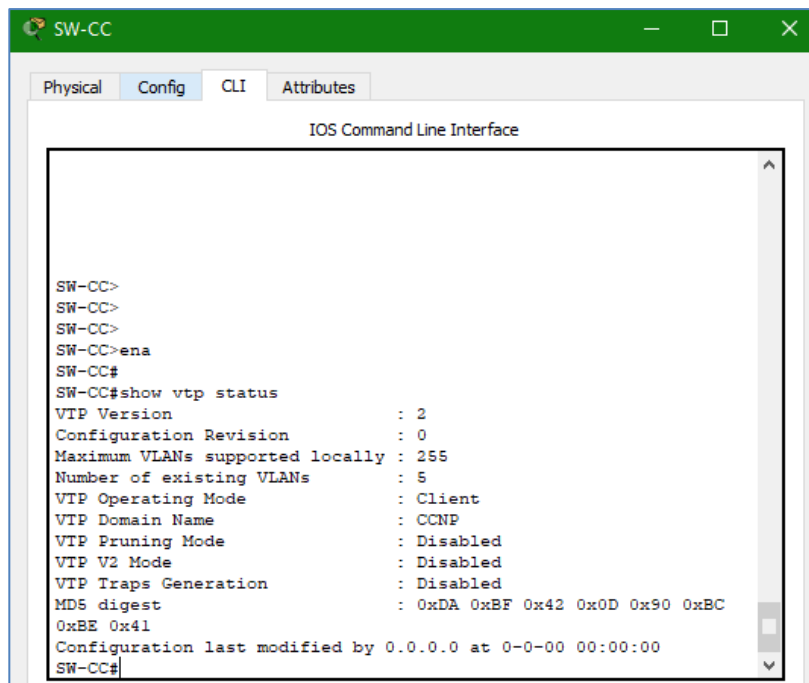
Figura 11. Ejecución comando *show vtp status* en SW-AA



The screenshot shows a terminal window for SW-BB with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the following text:

```
SW-BB#wr
Building configuration...
[OK]
SW-BB#
SW-BB#
SW-BB#
SW-BB#show vtp status
VTP Version : 2
Configuration Revision : 1
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode : Server
VTP Domain Name : CCNP
VTP Pruning Mode : Disabled
VTP V2 Mode : Enabled
VTP Traps Generation : Disabled
MD5 digest : 0xFF 0x77 0x05 0xB5 0x83 0x0C
0x4E 0x85
Configuration last modified by 0.0.0.0 at 3-1-93 00:31:50
Local updater ID is 0.0.0.0 (no valid interface found)
SW-BB#
SW-BB#
SW-BB#
SW-BB#
```

Figura 12. Ejecución comando show vtp status en SW-BB



The screenshot shows a terminal window for SW-CC with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the following text:

```
SW-CC>
SW-CC>
SW-CC>
SW-CC>ena
SW-CC#
SW-CC#show vtp status
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode : Client
VTP Domain Name : CCNP
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xDA 0xBF 0x42 0x0D 0x90 0xBC
0xBE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SW-CC#
```

Figura 13. Ejecución comando show vtp status en SW-CC

B. Configurar DTP (Dynamic Trunking Protocol)

4. Configure un enlace troncal ("trunk") dinámico entre SW-AA y SW-BB. Debido a que el modo por defecto es *dynamic auto*, solo un lado del enlace debe configurarse como *dynamic desirable*.

Se configura el switch SW-AA en modo Dynamic desirable

SWITCH SW-AA

```
SW-AA(config)#int f0/1
SW-AA(config-if)#switchport mode trunk
SW-AA(config-if)# switchport mode dynamic desirable
SW-AA(config-if)# exit
```

Se configura el switch SW-AA en modo trunk

SWITCH SW-BB

```
SW-BB#config term
SW-BB(config)#int f0/1
SW-BB(config-if)#switchport mode trunk
SW-BB(config-if)#exit
SW-BB(config)#
```

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

```
SW-AA>
SW-AA>
SW-AA>ena
SW-AA#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-AA#
```

Figura 14. Ejecución comando show interfaces trunk desde SW-AA

```
SW-BB(config)#int f0/1
SW-BB(config-if)#switchport mode trunk
SW-BB(config-if)#exit
SW-BB(config)#
SW-BB(config)#exit
SW-BB#
%SYS-5-CONFIG_I: Configured from console by console

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

Port      Vlans allowed on trunk
Fa0/1     1-1005

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

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

SW-BB#
```

Figura 15. Ejecución comando show interfaces trunk

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

SWITCH SW-AA

```
SW-AA#config term
SW-AA(config)#int f0/3
SW-AA(config-if)#switchport mode trunk
SW-AA(config-if)#exit
SW-AA(config)#
```

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

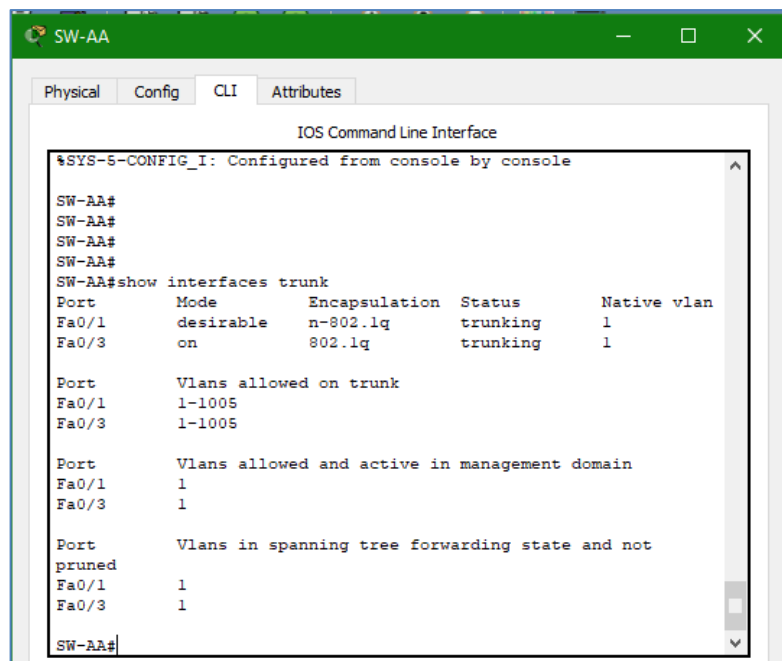


Figura 16. Ejecución comando show interfaces trunk desde SW-AA

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

```
switchport mode trunk
```

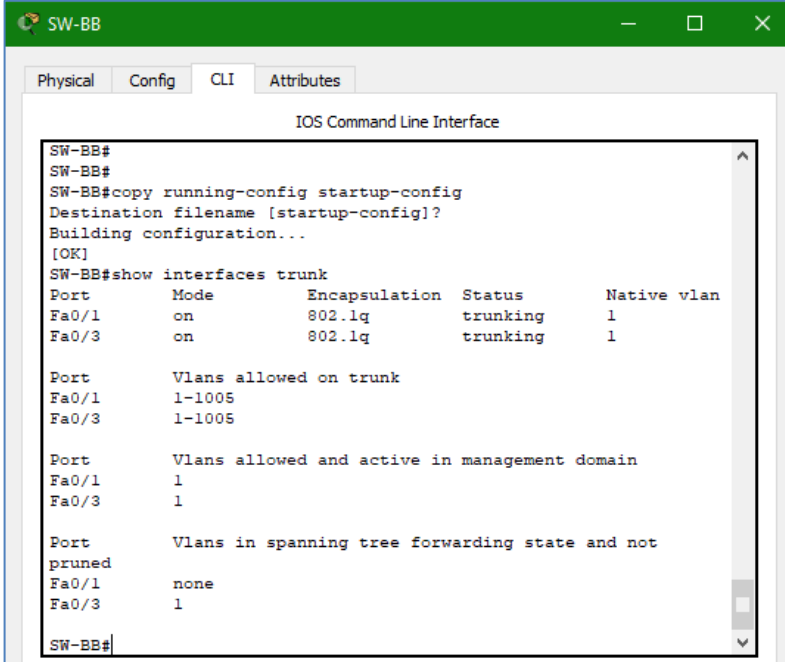
SWITCH SW-BB

```
SW-BB#config term
SW-BB(config)#int f0/3
SW-BB(config-if)#switchport mode trunk
```

```
SW-BB(config-if)#exit
SW-BB(config)#exit
SW-BB#wr
```

SWITCH SW-CC

```
SW-CC#
SW-CC#config term
SW-CC(config)#int f0/1
SW-CC(config-if)#switchport mode trunk
SW-CC(config-if)#exit
SW-CC(config)#exit
SW-CC#wr
```



```
SW-BB
Physical Config CLI Attributes
IOS Command Line Interface
SW-BB#
SW-BB#
SW-BB#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW-BB#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     on        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     none
Fa0/3     1
SW-BB#
```

Figura 17. Ejecución comando show interfaces trunk en SW-BB.

```

SW-CC#
SW-CC#
SW-CC#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
SW-CC#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     on        802.1q         trunking    1
Fa0/3     auto      n-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-CC#

```

Figura 18. Ejecución comando show interfaces trunk en SW-CC.

C. Agregar VLANs y asignar puertos.

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

Se crea la VLAN 10 en SW-AA

SWITCH SW-AA

```

SW-AA>en
SW-AA#config term
SW-AA(config)#vlan 10
SW-AA(config)#

```

Se configuran las VLANs en SW-BB

SWITCH SW-BB

```

SW-BB#config term
SW-BB(config)#vlan 10
SW-BB(config-vlan)#name Compras
SW-BB(config-vlan)#vlan 25

```

```
SW-BB(config-vlan)#name Personal
SW-BB(config-vlan)#vlan 30
SW-BB(config-vlan)#name Planta
SW-BB(config-vlan)#vlan 99
SW-BB(config-vlan)#name Admon
SW-BB(config-vlan)#exit
SW-BB(config)#exit
SW-BB#wr
```

10. Verifique que las VLANs han sido agregadas correctamente.

Se ejecuta el comando show vlan brief para verificar la creación de las VLANs.

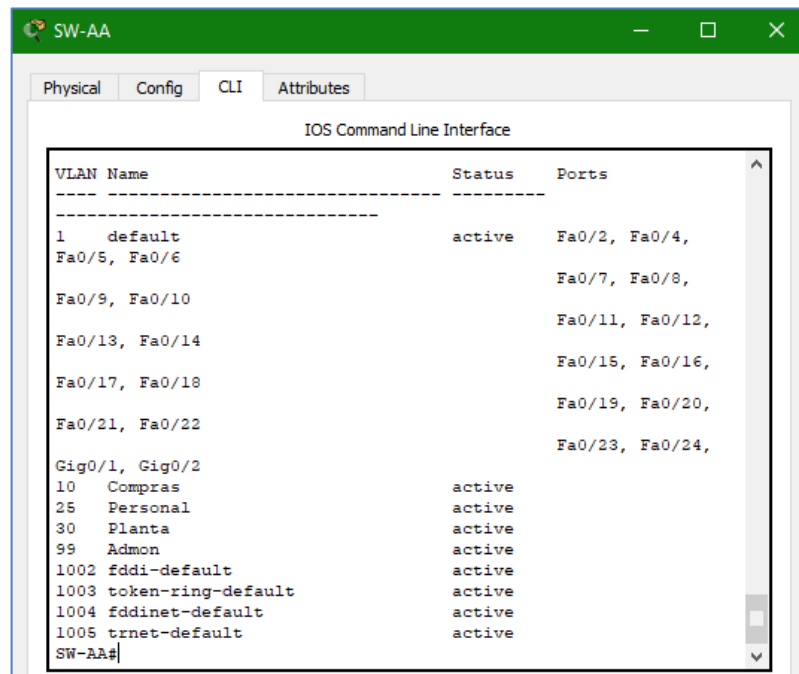


Figura 19. VLANs agregadas en SW-AA.

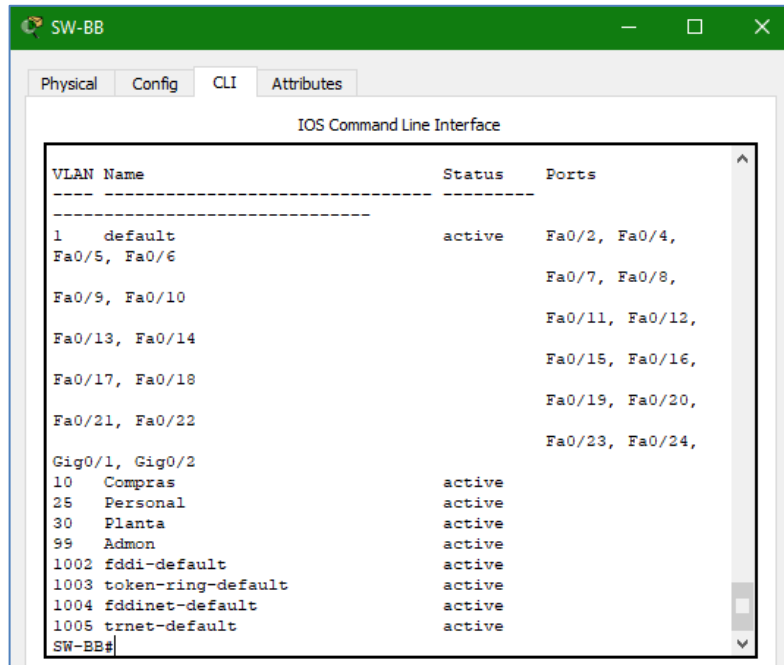


Figura 20. VLANs agregadas en SW-BB.

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

Tabla 5. Configuración direcciones IP

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.1 / 24
F0/15	VLAN 25	190.108.25.2 / 24
F0/20	VLAN 30	190.108.30.3 / 24

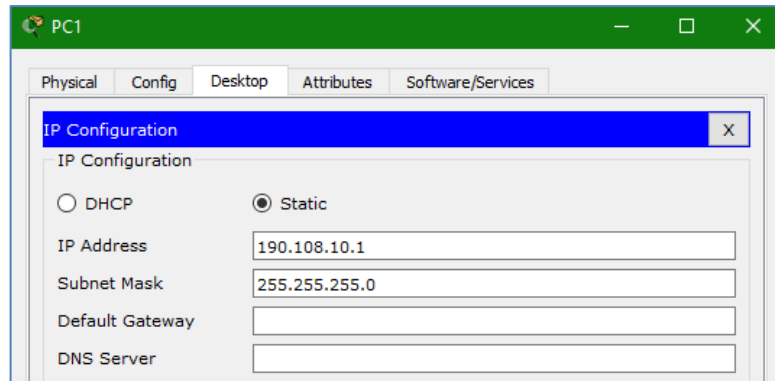


Figura 21: Configuración dirección IP en PC1

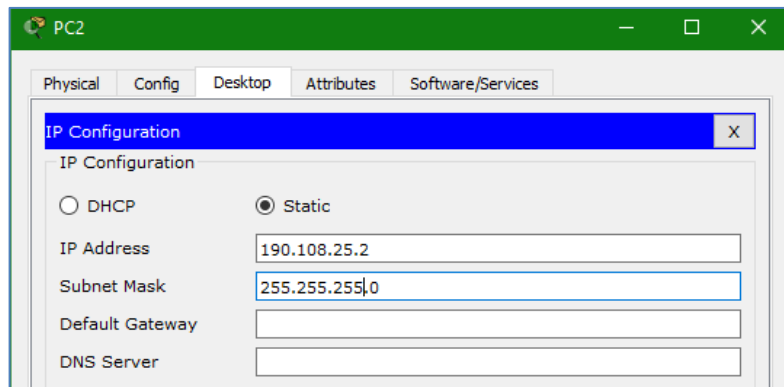


Figura 22: Configuración dirección IP en PC2

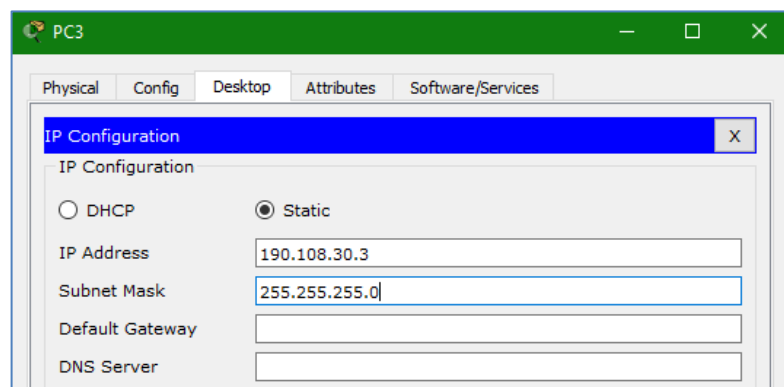


Figura 23: Configuración dirección IP en PC3

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

SWITCH SW-AA

```
SW-AA>en
SW-AA#config term
SW-AA(config)#interface f0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
```

SWITCH SW-BB

```
SW-BB>en
SW-BB#config term
SW-BB(config)#interface f0/10
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
```

SWITCH SW-CC

```
SW-CC>en
SW-CC#config term
SW-CC(config)#interface f0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
```

13. Repita el procedimiento para los puertos F0/15 y F0/20 en SW-AA, SW-BB y SW-CC. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

SWITCH SW-AA

```
SW-AA(config-if)#
SW-AA(config-if)#interface f0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#
SW-AA(config-if)#interface f0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
SW-AA(config-if)#
SW-AA#
```

SWITCH SW-BB

```
SW-BB(config-if)#interface f0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#interface f0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30
SW-BB(config-if)#
```

SWITCH SW-CC

```
SW-CC(config-if)#interface f0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#interface f0/20
```

```
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30
SW-CC(config-if)#
```

Ahora se configuran las direcciones IP en los demás PCs de la red.

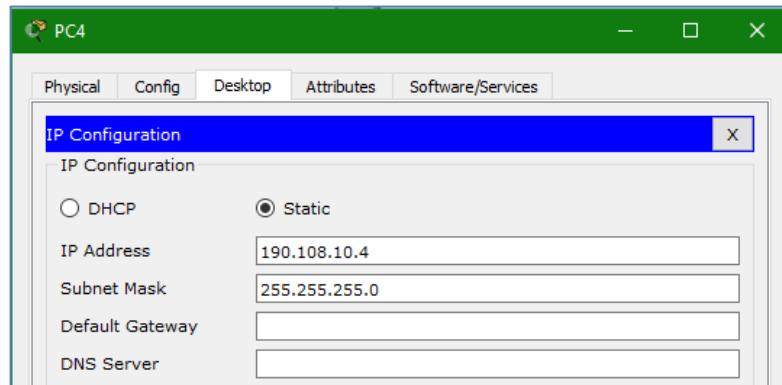


Figura 24: Configuración dirección IP en PC4

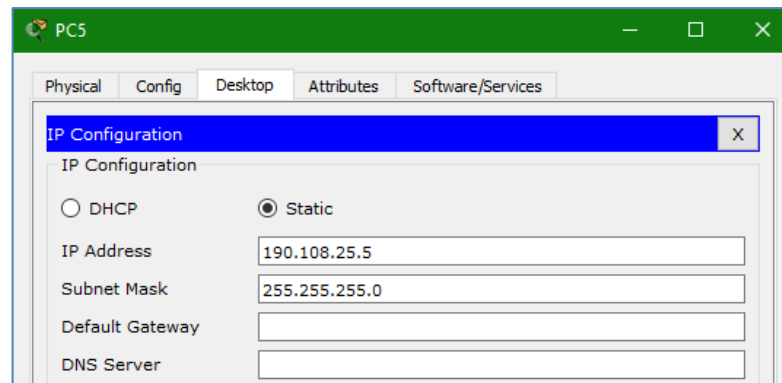


Figura 25: Configuración dirección IP en PC5

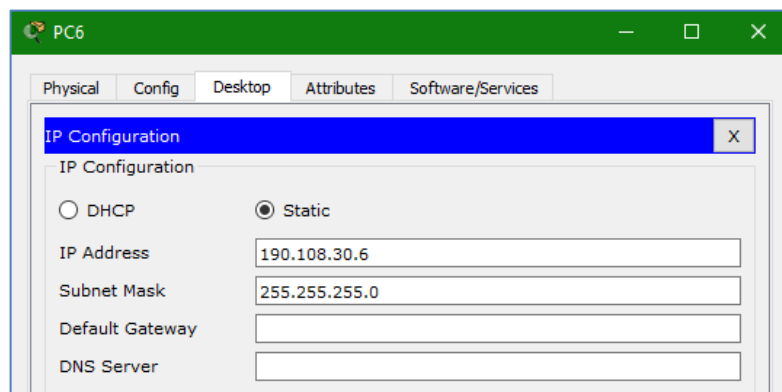


Figura 26: Configuración dirección IP en PC6

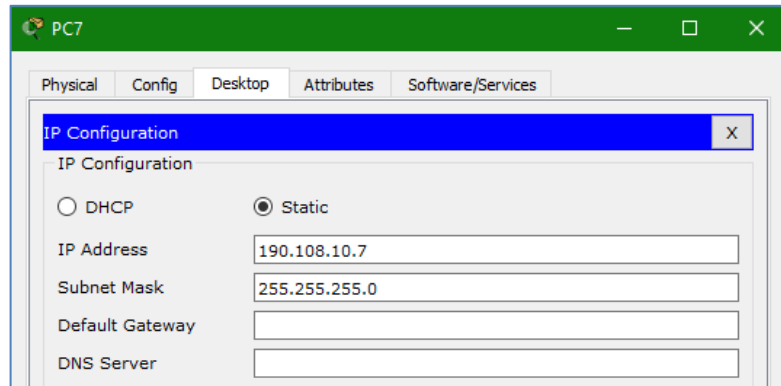


Figura 27: Configuración dirección IP en PC7

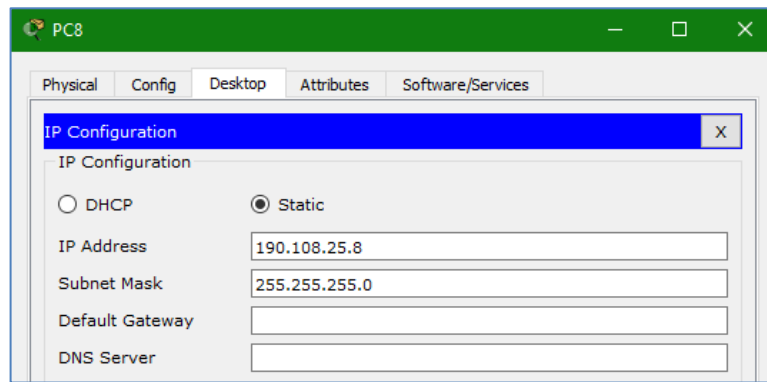


Figura 28: Configuración dirección IP en PC8

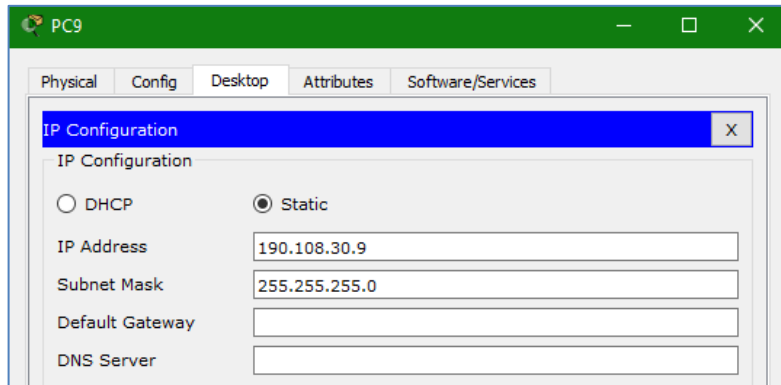


Figura 29: Configuración dirección IP en PC9

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. Configurar las direcciones IP en los switch

Equipo	Interfaz	Direcciones 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 configuran las direcciones IP al SVI de la VLAN 99, se procede de la siguiente manera:

SWITCH SW-AA

```
SW-AA>en
SW-AA#config term
SW-AA(config)#interface vlan 99
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
SW-AA(config-if)#no shutdown
```

SWITCH SW-BB

```
SW-BB>en
SW-BB#config term
SW-BB(config)#interface vlan 99
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
SW-BB(config-if)#no shutdown
```

SWITCH SW-CC

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

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.

```
PC1
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 190.108.10.4

Pinging 190.108.10.4 with 32 bytes of data:

Reply from 190.108.10.4: bytes=32 time<1ms TTL=128
Reply from 190.108.10.4: bytes=32 time<1ms TTL=128
Reply from 190.108.10.4: bytes=32 time<1ms TTL=128
Reply from 190.108.10.4: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 190.108.10.7

Pinging 190.108.10.7 with 32 bytes of data:

Reply from 190.108.10.7: bytes=32 time<1ms TTL=128
Reply from 190.108.10.7: bytes=32 time<1ms TTL=128
Reply from 190.108.10.7: bytes=32 time<1ms TTL=128
Reply from 190.108.10.7: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.10.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figura 30. Ping exitoso desde PC1 a PC4, PC7

```
PC4
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 190.108.10.1

Pinging 190.108.10.1 with 32 bytes of data:

Reply from 190.108.10.1: bytes=32 time<1ms TTL=128
Reply from 190.108.10.1: bytes=32 time<1ms TTL=128
Reply from 190.108.10.1: bytes=32 time<1ms TTL=128
Reply from 190.108.10.1: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 190.108.10.7

Pinging 190.108.10.7 with 32 bytes of data:

Reply from 190.108.10.7: bytes=32 time=2ms TTL=128
Reply from 190.108.10.7: bytes=32 time=1ms TTL=128
Reply from 190.108.10.7: bytes=32 time<1ms TTL=128
Reply from 190.108.10.7: bytes=32 time=3ms TTL=128

Ping statistics for 190.108.10.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

Figura 31. Ping exitoso desde PC4 a PC1, PC7

```
PC7
Physical Config Desktop Attributes Software/Services
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 190.108.10.1

Pinging 190.108.10.1 with 32 bytes of data:

Reply from 190.108.10.1: bytes=32 time<1ms TTL=128
Reply from 190.108.10.1: bytes=32 time<1ms TTL=128
Reply from 190.108.10.1: bytes=32 time<1ms TTL=128
Reply from 190.108.10.1: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 190.108.10.4

Pinging 190.108.10.4 with 32 bytes of data:

Reply from 190.108.10.4: bytes=32 time=1ms TTL=128
Reply from 190.108.10.4: bytes=32 time<1ms TTL=128
Reply from 190.108.10.4: bytes=32 time<1ms TTL=128
Reply from 190.108.10.4: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figura 32. Ping exitoso desde PC7 a PC1, PC4

```
PC1
Physical Config Desktop Attributes Software/Services
Command Prompt
C:\>ping 190.108.25.5

Pinging 190.108.25.5 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.25.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.30.9

Pinging 190.108.30.9 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.30.9:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 33. Ping no exitoso desde PC1 a PC5, PC9

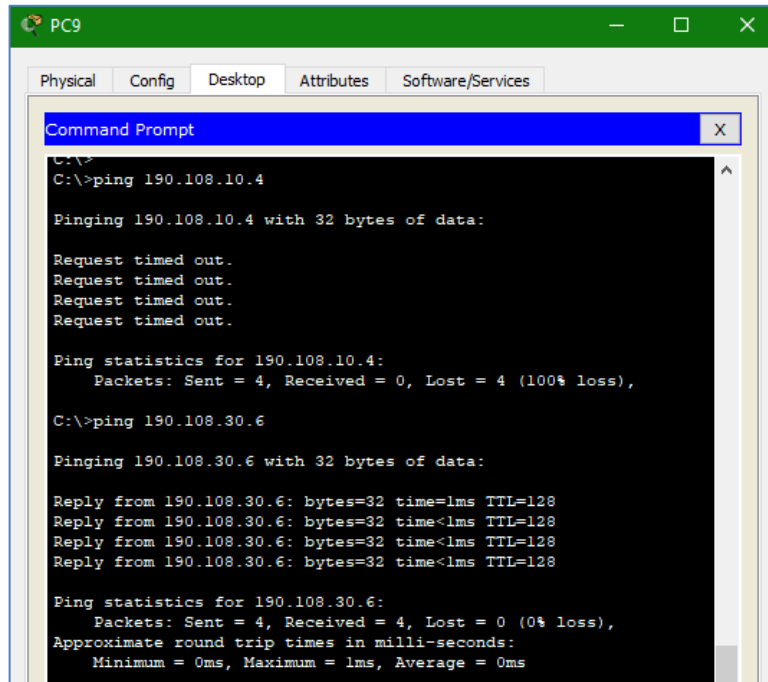


Figura 34. Ping desde PC9 a PC4, PC6

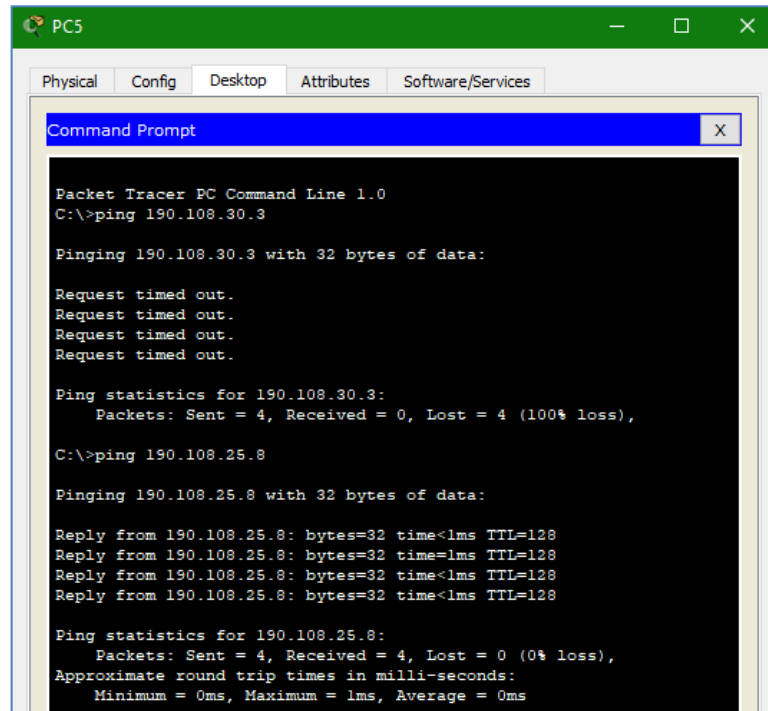
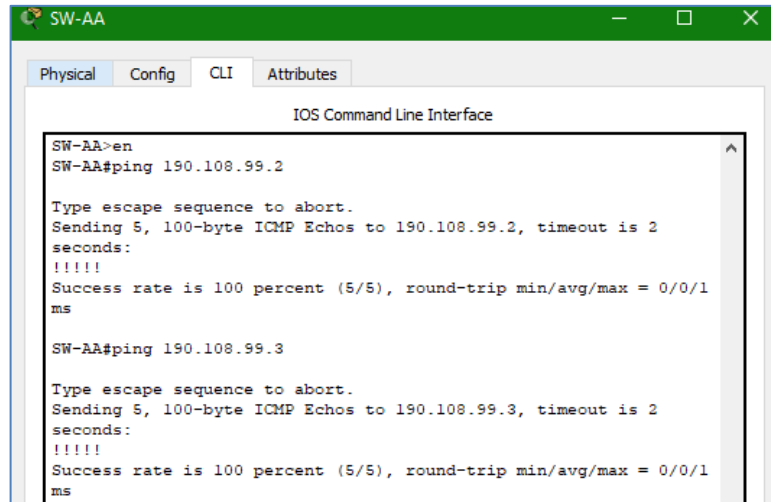


Figura 35. Ping desde PC5 a PC3, PC8

Como resultado de la prueba de conectividad entre cada PCs, se observa que la comunicación de datos es exitosa si pertenecen a la misma red VLAN asignada,

de lo contrario no se puede establecer comunicación ya que solo puede ser administradas desde las vlans asociadas a cada departamento, en este caso en particular no se puede cruzar la información entre las diferentes vlans.

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



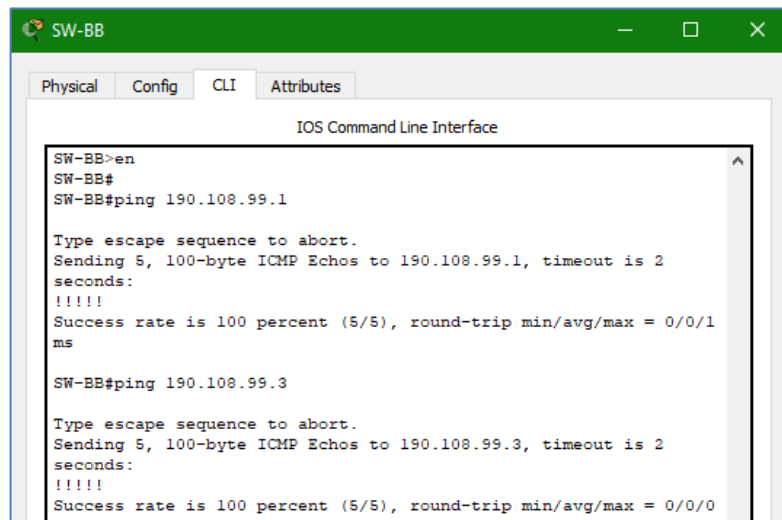
```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
SW-AA>en
SW-AA#ping 190.108.99.2

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 = 0/0/1
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 100 percent (5/5), round-trip min/avg/max = 0/0/1
ms
```

Figura 36. Ping desde SW-AA a SW-BB, SW-CC



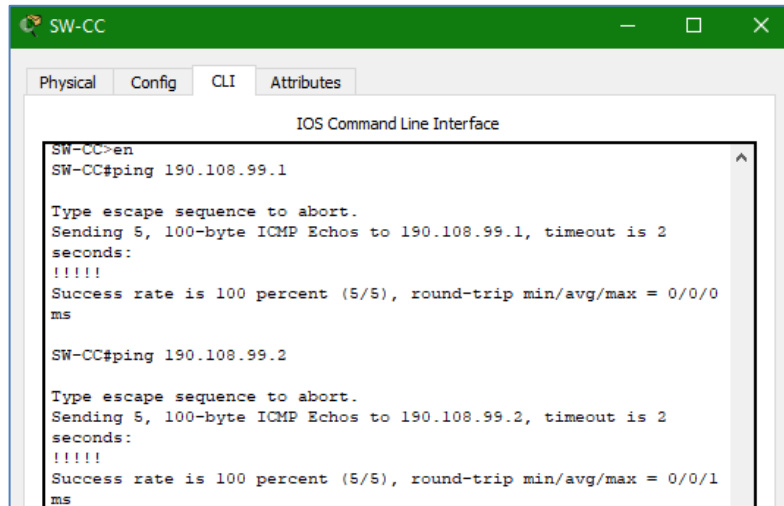
```
SW-BB
Physical Config CLI Attributes
IOS Command Line Interface
SW-BB>en
SW-BB#
SW-BB#ping 190.108.99.1

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 = 0/0/1
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 100 percent (5/5), round-trip min/avg/max = 0/0/0
```

Figura 37. Ping desde SW-BB a SW-AA, SW-CC



```
SW-CC
Physical Config CLI Attributes
IOS Command Line Interface
SW-CC>en
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 = 0/0/0
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 = 0/0/1
ms
```

Figura 38. Ping desde SW-CC a SW-AA, SW-BB

Como resultado de la prueba de ping entre los conmutadores se puede observar que existe una verificación de estado exitosa entre cada conmutador, ya que cada uno de éstos ha sido configurado con enlaces troncales, y sus respectivas vlans, las cuales permiten el paso de información en estos enlaces.

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

```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
SW-AA>en
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 0 percent (0/5)

SW-AA#ping 190.108.25.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.2, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

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 0 percent (0/5)

SW-AA#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 0 percent (0/5)

SW-AA#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:
```

Figura 39. Ping desde SW-AA a PCs

```
SW-BB
Physical Config CLI Attributes
IOS Command Line Interface
SW-BB>en
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 0 percent (0/5)

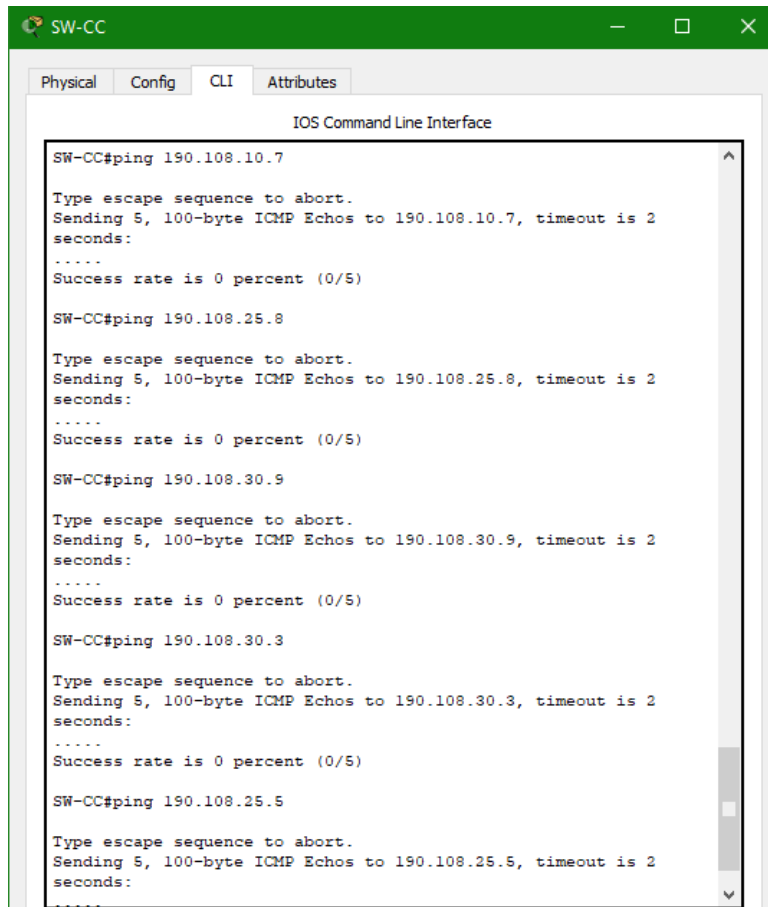
SW-BB#ping 190.108.25.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.5, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

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 0 percent (0/5)

SW-BB#ping 190.108.25.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.2, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#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:
```

Figura 40. Ping desde SW-BB a PCs



```
SW-CC
Physical Config CLI Attributes
IOS Command Line Interface
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 0 percent (0/5)

SW-CC#ping 190.108.25.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.8, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

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 0 percent (0/5)

SW-CC#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 0 percent (0/5)

SW-CC#ping 190.108.25.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.5, timeout is 2
seconds:
.....
```

Figura 41. Ping desde SW-CC a PCs

Los resultados obtenidos con el comando ping en cada uno de switches no fueron exitosos, porque las direcciones IP y las puertos de enlace de cada Host no han sido configuradas en las VLANs ya creadas en cada uno de los conmutadores de red.

CONCLUSIONES

En esta prueba de habilidades se ha puesto en práctica las competencias adquiridas durante el desarrollo del curso de profundización CISCO CCNP, en el cual se ha logrado aplicar y comprender los conceptos sobre la creación de rutas por medio protocolos BGP, aplicando relaciones de vecino entre enrutadores, y los cuales han sido configurados para el envío de datos de acuerdo topologías de red desarrollado en el escenario uno; también se ha llevado a la práctica la ejecución comandos específicos en cada uno de los escenarios presentados, y con el cual se ha implementado códigos o líneas de comando para cada escenario, relacionados con el enrutamiento básico y avanzado en la programación de redes de comunicación de datos, y las configuraciones de enlaces troncales y creación de VLANs, aprendidos durante el curso de profundización CISCO CCNP.

En el primer escenario se ha logrado configurar de manera correcta el encaminamiento BGP, o una relación de vecinos entre los router que comparten una red o enlace para el intercambio de información de encaminamiento, y en el cual se especifica al sistema autónomo, este protocolo de enrutamiento nos permite transferir grandes cantidades de información entre dos puntos de la red, su importancia es que nos proporcionar el camino más eficientes entre los nodos de la red de enlace configurada, ayudando así a proporcionar un mejor tránsito de información en internet.

Para el segundo escenario se ha configurado de manera correcta el protocolo VTP, el cual nos ayuda a centralizar en solo switch la administración de todas las VLANs creadas, y la cual nos ayuda a transferir la información de forma automática en otras VLANs de distintos swich; también se ha creado enlaces troncales para la actualización de redes de área local virtual VLANs, las cuales han sido configuradas en el sistema según la topología presentada, y posteriormente se les ha asignado el direccionamiento IP, para la conmutación de información con los PCS pertenecientes a sus misma VLANs; estas redes de área local virtual han sido configuradas para centralizar cada departamento en la red del sistema de comunicación de datos y suministrar de manera optima la transferencia de datos a cada departamento. Para la verificación de envío de paquetes, se realizan ping en cada dispositivo de la red, la cual nos da como resultado la independencia de trafico de información entre las VLANs pertenecientes a un mismo departamento.

BIBLIOGRAFÍA

Documentation: The official GNS3 Documentation, (2020).
<https://www.gns3.com/support/docs>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1IlnWR0hoMxgBNv1CJ>

Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de <http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1IlnMfy2rhPZHwEoWx>

Wallace, K. (2015). CISCO Press (Ed). CCNP Routing and Switching ROUTE 300-101 Official Cert Guide. Recuperado de <https://1drv.ms/b/s!AglGg5JUgUBthFx8WOxiq6LPJppI>