

DIPLOMADO CCNP - CISCO PRUEBA DE HABILIDADES CCNP

JOSE MANUEL GOMEZ MORA

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

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JOSE MANUEL GOMEZ MORA

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

DIRECTOR:  
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN:

---

---

---

---

---

---

---

---

Firma del presidente del jurado

---

Firma del jurado

---

Firma del jurado

Bogotá, 22 de mayo 2020

## **AGRADECIMIENTO**

Te agradezco a ti Dios, por ayudarme a terminar mis proyectos, por darme la fuerza y el coraje para hacer mi sueño realidad, por estar conmigo en cada momento de mi vida.

A mi familia, por su compañía, aliento, por darme fuerza y enseñarme a no rendirme a pesar de las adversidades. Por ser mi principal motivación para ser cada día mejor no solo en el ámbito profesional sino el personal.

También agradezco a la Universidad quien por medio de todos los docentes con que interactúe me ayudaron a no desmotivarme y continuar la búsqueda de este anhelo tan esperado y necesario en este mundo tan tecnológico.

## TABLA DE CONTENIDO

AGRADECIMIENTO .....	4
LISTA DE TABLAS .....	6
LISTA DE ILUSTRACIONES .....	7
GLOSARIO .....	8
RESUMEN.....	9
ABSTRACT .....	10
INTRODUCCION.....	11
DESARROLLO DE LOS ESCENARIOS.....	12
Escenario 1 .....	12
Relación de vecino BGP entre R1 y R2 .....	13
Relación de vecino BGP entre R2 y R3 .....	15
Escenario 2.....	20
CONCLUSIONES .....	39
BIBLIOGRAFIA.....	40

## LISTA DE TABLAS

Tabla 1. Interfaz, dirección IP y máscara .....	12
Tabla 2. Tabla de direcciones para PCS.....	29
Tabla 3. Tabla de direccionamiento de los switch.....	31

## LISTA DE ILUSTRACIONES

Ilustración 1: Escenario 1 .....	12
Ilustración 2: Rutas vecinas entre R1 y R2. ....	14
Ilustración 3: Rutas vecinas entre R1 y R2. ....	15
Ilustración 4: Rutas vecinas entre R2 y R3. ....	16
Ilustración 5: Rutas vecinas entre R2 y R3. ....	17
Ilustración 6: Rutas vecinas entre R3 y R4. ....	19
Ilustración 7: Rutas vecinas entre R3 y R4. ....	19
Ilustración 8: Escenario 2.....	20
Ilustración 9: Status del SW-AA en VTP. ....	22
Ilustración 10: Status del SW-BB en VTP. ....	22
Ilustración 11: Status del SW-CC en VTP.....	23
Ilustración 12: Modo trunk de los puertos. ....	24
Ilustración 13: Modo trunk de los puertos. ....	25
Ilustración 14: Modo trunk de los puertos. ....	26
Ilustración 15: Modo trunk de los puertos. ....	26
Ilustración 16: Error en creación de VLAN.....	27
Ilustración 17: VLAN creadas en el SW-BB. ....	28
Ilustración 18: VLAN creadas por VTP en SW-AA.....	28
Ilustración 19: VLAN creadas por VTP en SW-CC. ....	29
Ilustración 20: Prueba de conectividad 1. ....	32
Ilustración 21: Prueba de conectividad 2. ....	33
Ilustración 22: Prueba de conectividad 3. ....	33
Ilustración 23: Prueba de conectividad 4. ....	34
Ilustración 24: Prueba de conectividad 5. ....	35
Ilustración 25: Prueba de conectividad 6. ....	36
Ilustración 26: Prueba de conectividad 7. ....	37
Ilustración 27: Prueba de conectividad 8. ....	38

## GLOSARIO

**Enrutador (del inglés Router):** Dispositivo hardware o software de interconexión de redes de computadores que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red. El router toma decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirige los paquetes hacia el segmento y el puerto de salida adecuados.

**Gateway:** Un gateway (puerta de enlace) es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

**Red de área amplia (WAN):** Una red que interconecta recursos de computadoras que están geográficamente ampliamente separadas (usualmente a más de 100 km). Esto incluye pueblos, ciudades, estados y condados. Un WAN cubre generalmente un área mayor que 5 millas (8 km) y puede considerarse que consiste en una colección de LANs.

**Switch:** Dispositivo de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconnection). Un switch interconecta dos o más segmentos de red, pasando datos de un segmento a otro, de acuerdo con la dirección de destino de los datagramas en la red. Un switch en el centro de una red en estrella. Los switches se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs.

**UDP:** (del Inglés User Datagram Protocol, protocolo de datagrama de usuario). Protocolo del nivel de transporte basado en el intercambio de datagramas. No tiene confirmación, ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco sabemos si ha llegado correctamente, ya que no hay confirmación de entrega o de recepción. Su uso principal es para protocolos como DHCP, BOOTP, DNS.

**VPN:** (Virtual Private Network/Red Privada Virtual). Una conexión IP entre dos sitios sobre una red pública IP que tiene su tráfico de carga útil codificada de manera que sólo los nodos fuente y destino pueden descifrar los paquetes de tráfico. Una VPN permite a una red públicamente accesible será usada para transmisiones de datos altamente confidenciales, dinámicas y seguras.



## **RESUMEN**

El presente escrito se realiza como trabajo final del diplomado de profundización CCNP CISCO como rama importante de la electrónica sin la cual no existirían las telecomunicaciones. Para lo anterior se utilizarán como herramientas principales el software de simulación de Redes Packet Tracer, Usando VTP, cada switch publica en sus puertos troncales su dominio de administración, las VLANs que conoce y determinados parámetros para cada VLAN conocida. Todos los dispositivos en el mismo dominio de administración reciben información de Enrutamiento acerca de cualquier nueva VLAN que se haya configurado en el dispositivo transmisor y conmutan entre sí. Se debe crear y configurar una nueva VLAN en un solo dispositivo del dominio de administración. Los demás dispositivos reciben automáticamente la información.

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

## **ABSTRACT**

This document is carried out as the final work of the CCNP CISCO deepening diploma as an important branch of electronics without which telecommunications would not exist. For the above, the simulation software of Packet Tracer Networks will be used as main tool. Using VTP, each switch publishes its management domain, the VLANs it knows and certain parameters for each known VLAN on its trunk ports. All devices in the same management domain receive Routing information about any new VLANs that have been configured on the transmitting device and switch between them. A new VLAN must be created and configured on a single device in the management domain. The other devices automatically receive the information.

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

## INTRODUCCION

En el presente trabajo se expone la evidencia de las habilidades adquiridas a través del diplomado realizado; para lo anteriormente descrito se plantean dos situaciones en las cuales como ingenieros capacitados en Routing y Switching, realizamos la configuración de los equipos dispuestos en dos (2) escenarios para cumplir su objetivo dentro de la red diseñada.

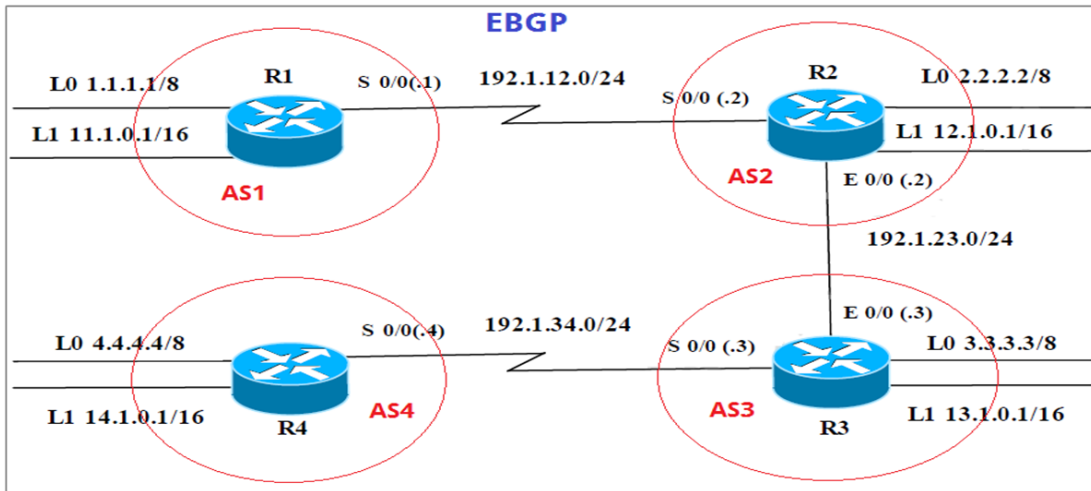
En el primer escenario se plantea una red compuesta con 4 Routers a la cual se le deberá configurar las relaciones requeridas para lograr la redistribución de rutas a través de protocolos BGP, OSPF y EIGPR; para este caso se utilizará el software de simulación GSN3.

En el segundo escenario se cuenta con una red compleja la cual consta de tres (3) Switch interconectados y 9 Pcs; en esta red se busca configurar entre los Switch AA-BB y CC-BB una conexión Cliente-servidor, establecer rutas troncales dentro de ellos y a sus vez crear segmentaciones Vlan que permitan limitar la interacción única con el segmento establecido; para este escenario se utilizará el Software Packet tracer.

## DESARROLLO DE LOS ESCENARIOS

### Escenario 1

Ilustración 1: Escenario 1



Fuente: Prueba de habilidades CCNP 2020, Cisco Academy.

Tabla 1. Tabla interfaz, dirección IP y máscara.

Interfaz	Dirección IP	Máscara
Loopback 0	1.1.1.1	255.0.0.0
Loopback 1	11.1.0.1	255.255.0.0
S 0/0	192.1.12.1	255.255.255.0
Interfaz	Dirección IP	Máscara
Loopback 0	2.2.2.2	255.0.0.0
Loopback 1	12.1.0.1	255.255.0.0
S 0/0	192.1.12.2	255.255.255.0
E 0/0	192.1.23.2	255.255.255.0
Interfaz	Dirección IP	Máscara
Loopback 0	3.3.3.3	255.0.0.0
Loopback 1	13.1.0.1	255.255.0.0
E 0/0	192.1.23.3	255.255.255.0
S 0/0	192.1.34.3	255.255.255.0

Interfaz	Dirección IP	Máscara
Loopback 0	4.4.4.4	255.0.0.0
Loopback 1	14.1.0.1	255.255.0.0
S 0/0	192.1.34.3	255.255.255.0

Fuente: Prueba de habilidades CCNP 2020, Cisco Academy.

## Relación de vecino BGP entre R1 y R2

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.

```
R1(config)#hostname R1 R1(config)#interface Loopback 0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#interface Loopback 1
R1(config-if)#ip address 11.1.0.1 255.255.0.0 R1(config-if)#interface serial
0/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0 R1(config-if)#no
shutdown
R1(config-if)#exit R1(config)#router bgp 1
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#network 1.0.0.0 mask 255.0.0.0
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router)#network 192.1.12.0 mask 255.255.255.0
R1(config-router)#neighbor 192.1.12.2 remote-as 2 R1(config-router)#exit
R1(config)#do wr Building configuration...
```

```
R2(config)#hostname R2 R2(config)#interface Loopback 0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#interface Loopback 1
```

```
R2(config-if)#ip address 12.1.0.1 255.255.0.0 R2(config-if)#interface serial 0/0
```

```
R2(config-if)#ip address 192.1.12.2 255.255.255.0 R2(config-if)#no shutdown
```

```
R2(config-if)#interface e1/0
```

```
R2(config-if)#ip address 192.1.23.2 255.255.255.0 R2(config-if)#no shutdown
```

```
R2(config-if)#exit R2(config)#router bgp 2
```

```
R2(config-router)#bgp router-id 33.33.33.33
```

```
R2(config-router)#network 2.0.0.0 mask 255.0.0.0
```

Ilustración 2: Rutas vecinas entre R1 y R2.

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

Gateway of last resort is not set

C    192.1.12.0/24 is directly connected, Serial0/0
C    1.0.0.0/8 is directly connected, Loopback0
B    2.0.0.0/8 [20/0] via 192.1.12.2, 00:01:44
     11.0.0.0/16 is subnetted, 1 subnets
C       11.1.0.0 is directly connected, Loopback1
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.12.2, 00:01:44
R1#
```

Fuente: Elaboración propia.

### Ilustración 3: Rutas vecinas entre R1 y R2.

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

Gateway of last resort is not set

C    192.1.12.0/24 is directly connected, Serial0/0
B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:02:53
C    2.0.0.0/8 is directly connected, Loopback0
C    192.1.23.0/24 is directly connected, Ethernet1/0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.12.1, 00:02:53
     12.0.0.0/16 is subnetted, 1 subnets
C       12.1.0.0 is directly connected, Loopback1
R2#
```

Fuente: Elaboración propia.

### Relación de vecino BGP entre R2 y R3

Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en AS2 y R3 debería estar en AS3. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 44.44.44.44.

Presente el paso a con los comandos utilizados y la salida del comando `show ip route`.

```
R2(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)#do wr
```

```
Building configuration...
```

```
R3(config)#hostname R3 R3(config)#interface Loopback 0
```

```
R3(config-if)#ip address 3.3.3.3 255.0.0.0
```

```
R3(config-if)#interface Loopback 1
```

```
R3(config-if)#ip address 13.1.0.1 255.255.0.0 R3(config-if)#interface e1/0
```

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

shutdown

R3(config-if)#interface serial 0/0

R3(config-if)#ip address 192.1.34.3 255.255.255.0 R3(config-if)#no shutdown

R3(config-if)#exit R3(config)#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

Ilustración 4: Rutas vecinas entre R2 y R3.

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

Gateway of last resort is not set

C    192.1.12.0/24 is directly connected, Serial0/0
B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:06:17
C    2.0.0.0/8 is directly connected, Loopback0
B    3.0.0.0/8 [20/0] via 192.1.23.3, 00:00:23
C    192.1.23.0/24 is directly connected, Ethernet1/0
B    11.0.0.0/16 is subnetted, 1 subnets
     11.1.0.0 [20/0] via 192.1.12.1, 00:06:17
B    12.0.0.0/16 is subnetted, 1 subnets
     12.1.0.0 is directly connected, Loopback1
C    13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0 [20/0] via 192.1.23.3, 00:00:25
R2#
```

Fuente: Elaboración propia.



## Ilustración 5: Rutas vecinas entre R2 y R3.

```
R3#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:01:06
B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:01:06
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:01:06
C    3.0.0.0/8 is directly connected, Loopback0
C    192.1.23.0/24 is directly connected, Ethernet1/0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.23.2, 00:01:06
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.23.2, 00:01:06
     13.0.0.0/16 is subnetted, 1 subnets
C       13.1.0.0 is directly connected, Loopback1
R3#
```

Fuente: Elaboración propia.

## Relación de vecino BGP entre R3 y R4

Configure una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en AS3 y R4 debería estar en AS4. Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como 66.66.66.66. Establezca las relaciones de vecino con base en las direcciones de Loopback 0. Cree rutas estáticas para alcanzar la Loopback 0 del otro router. No anuncie la Loopback 0 en BGP. Anuncie la red Loopback de R4 en BGP. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

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

```
R3(config)#router bgp 3
```

```
R3(config-router)#no neighbor 192.1.34.4
```

```
R3(config-router)#no network 3.0.0.0 mask 255.0.0.0
```

```
R3(config-router)#neighbor 4.4.4.4 remote-as 4
R3(config-router)#neighbor 4.4.4.4 update-source loopback 0 R3(config-
router)# neighbor 4.4.4.4 ebgp-multihop

R4(config)#hostname R4 R4(config)#interface Loopback 0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#interface Loopback 1
R4(config-if)#ip address 14.1.0.1 255.255.0.0 R4(config-if)#interface serial
0/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0 R4(config-if)#no
shutdown
R4(config-if)#exit R4(config)#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)#ip route 3.0.0.0 255.0.0.0 192.1.34.3
R4(config)#router bgp 4
R4(config-router)#no neighbor 192.1.34.3
R4(config-router)#neighbor 3.3.3.3 remote-as 4
R4(config-router)#neighbor 3.3.3.3 update-source loopback 0 R4(config-
router)# neighbor 3.3.3.3 ebgp-multihop R4(config-router)#do wr
Building configuration...
```

Ilustración 6: Rutas vecinas entre R3 y R4.

```
R3#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:05:51
B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:05:51
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:05:51
C    3.0.0.0/8 is directly connected, Loopback0
S    4.0.0.0/8 [1/0] via 192.1.34.4
C    192.1.23.0/24 is directly connected, Ethernet1/0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.23.2, 00:05:51
C    192.1.34.0/24 is directly connected, Serial0/0
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.23.2, 00:05:52
     13.0.0.0/16 is subnetted, 1 subnets
C       13.1.0.0 is directly connected, Loopback1
R3#
```

Fuente: Elaboración propia.

Ilustración 7: Rutas vecinas entre R3 y R4.

```
R4#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

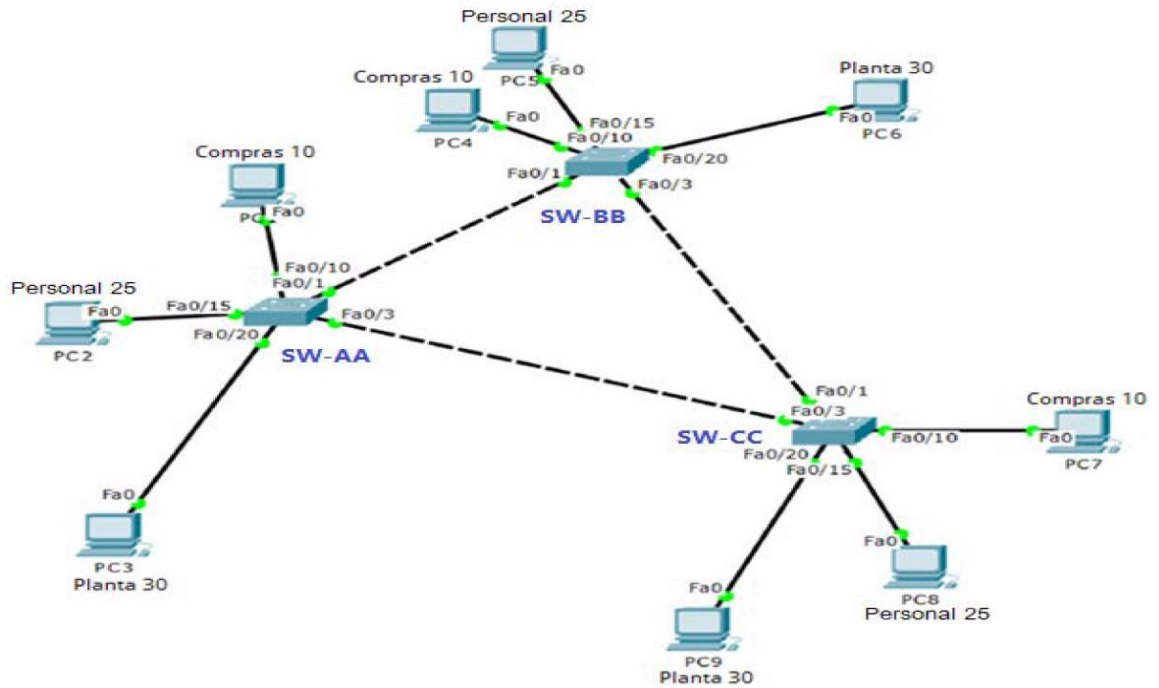
Gateway of last resort is not set

B    192.1.12.0/24 [20/0] via 3.3.3.3, 00:46:50
B    1.0.0.0/8 [20/0] via 3.3.3.3, 00:46:50
B    2.0.0.0/8 [20/0] via 3.3.3.3, 00:46:50
S    3.0.0.0/8 [1/0] via 192.1.34.3
C    4.0.0.0/8 is directly connected, Loopback0
B    192.1.23.0/24 [20/0] via 3.3.3.3, 00:46:50
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 3.3.3.3, 00:46:50
C    192.1.34.0/24 is directly connected, Serial1/0
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 3.3.3.3, 00:46:50
     13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0 [20/0] via 3.3.3.3, 00:46:50
     14.0.0.0/16 is subnetted, 1 subnets
C       14.1.0.0 is directly connected, Loopback1
R4#
```

Fuente: Elaboración propia.

## Escenario 2

Ilustración 8: Escenario 2.



Fuente: Prueba de habilidades CCNP 2020, Cisco Academy.

### Configurar VTP

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 1

```
Switch#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname SW-AA

SW-AA(config)#vtp mode client Setting device to VTP CLIENT mode. SW-AA(config)#vtp domain CCNP Domain name already set to CCNP. SW-AA(config)#vtp password cisco Password already set to cisco

Switch 2 Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname SW-BB

SW-BB(config)#vtp mode server Device mode already VTP SERVER. SW-BB(config)#vtp domain CCNP

Changing VTP domain name from NULL to CCNP SW-BB(config)#vtp password cisco

Setting device VLAN database password to cisco

Switch 3 Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#hostname SW-CC

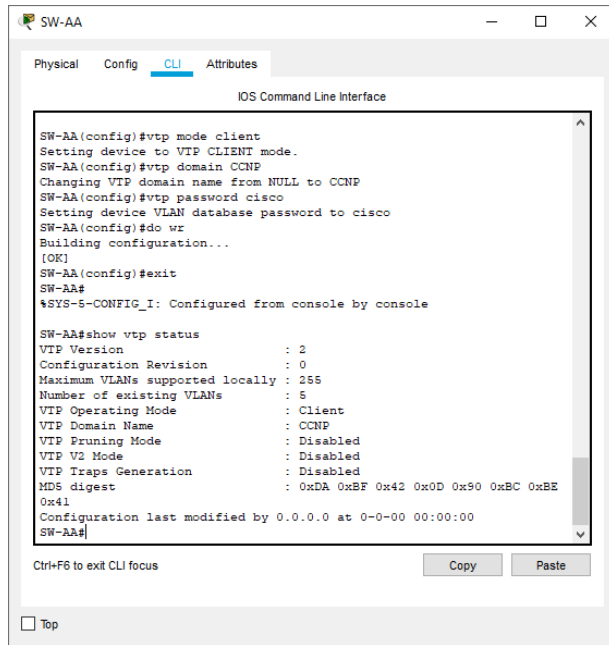
SW-CC(config)#vtp mode client Setting device to VTP CLIENT mode. SW-CC(config)#vtp domain CCNP

Changing VTP domain name from NULL to CCNP SW-CC(config)#vtp password cisco

Setting device VLAN database password to cisco

Verifique las configuraciones mediante el comando show vtp status.

Ilustración 9: Status del SW-AA en VTP.



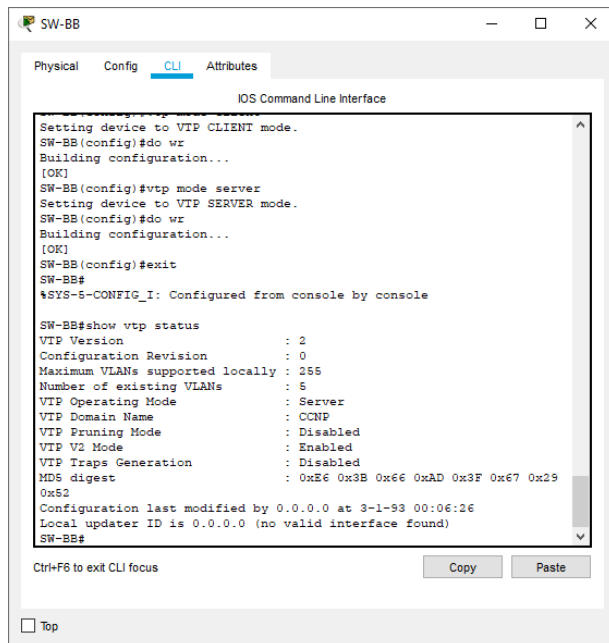
```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface

SW-AA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-AA(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-AA(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-AA(config)#do wr
Building configuration...
[OK]
SW-AA(config)#exit
SW-AA#
*SYS-5-CONFIG_I: Configured from console by console

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
MDS 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#
```

Fuente: Elaboración propia.

Ilustración 10: Status del SW-BB en VTP.



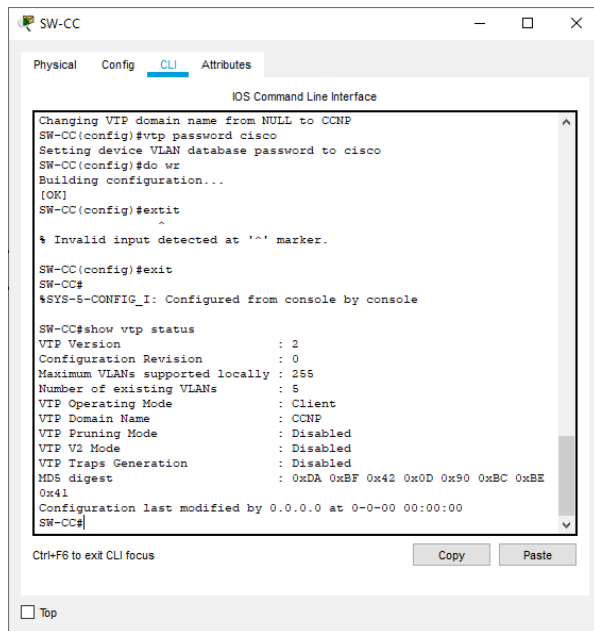
```
SW-BB
Physical Config CLI Attributes
IOS Command Line Interface

Setting device to VTP CLIENT mode.
SW-BB(config)#do wr
Building configuration...
[OK]
SW-BB(config)#vtp mode server
Setting device to VTP SERVER mode.
SW-BB(config)#do wr
Building configuration...
[OK]
SW-BB(config)#exit
SW-BB#
*SYS-5-CONFIG_I: Configured from console by console

SW-BB#show vtp status
VTP Version          : 2
Configuration Revision : 0
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
MDS digest          : 0xE6 0x3B 0x66 0xAD 0x3F 0x67 0x29
0x52
Configuration last modified by 0.0.0.0 at 3-1-93 00:06:26
Local updater ID is 0.0.0.0 (no valid interface found)
SW-BB#
```

Fuente: Elaboración propia.

Ilustración 11: Status del SW-CC en VTP.



```
SW-CC
Physical Config CLI Attributes
IOS Command Line Interface
Changing VTP domain name from NULL to CCNP
SW-CC(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-CC(config)#do wr
Building configuration...
[OK]
SW-CC(config)#exit
^
% Invalid input detected at '^' marker.
SW-CC(config)#exit
SW-CC#
%SYS-5-CONFIG_I: Configured from console by console

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
MDS 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#
```

Fuente: Elaboración propia.

## Configurar DTP (Dynamic Trunking Protocol)

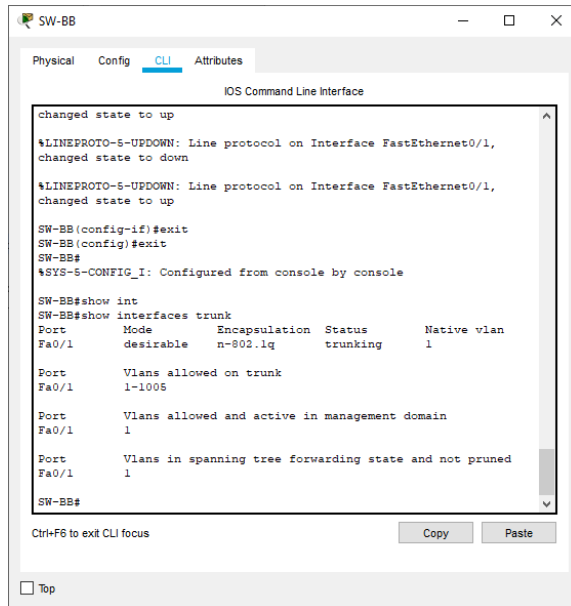
Configure un enlace troncal ("trunk") dinámico entre SW-AA y SW-BB. Debido a que el modo por defecto es dynamic auto, solo un lado del enlace debe configurarse como dynamic desirable.

```
SW-BB(config)#interface fastEthernet 0/1
```

```
SW-BB(config-if)#switchport mode dynamic desirable
```

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

Ilustración 12: Modo trunk de los puertos.



```
SW-BB
Physical Config CLI Attributes
IOS Command Line Interface
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
SW-BB(config-if)#exit
SW-BB(config)#exit
SW-BB#
%SYS-5-CONFIG_I: Configured from console by console
SW-BB#show int
SW-BB#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     desirable n-802.1q       trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005

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

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1
SW-BB#
```

Ctrl+F6 to exit CLI focus    Copy    Paste

Top

Fuente: Elaboración propia.

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

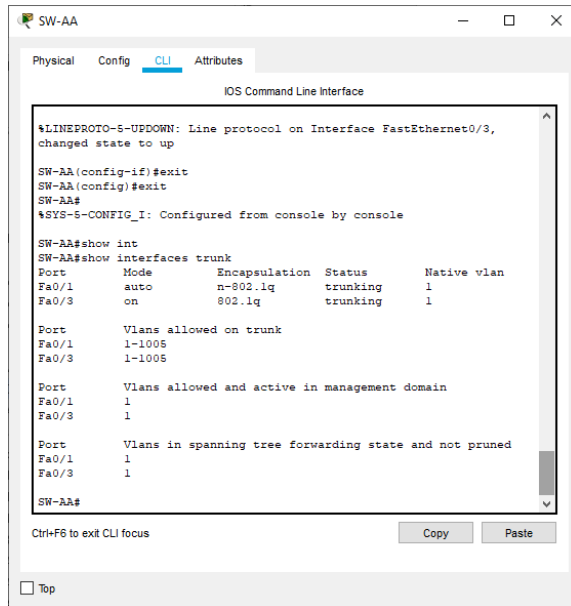
```
SW-AA(config)#interface fastEthernet 0/3
```

```
SW-AA(config-if)#switchport mode trunk
```

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



Ilustración 13: Modo trunk de los puertos.



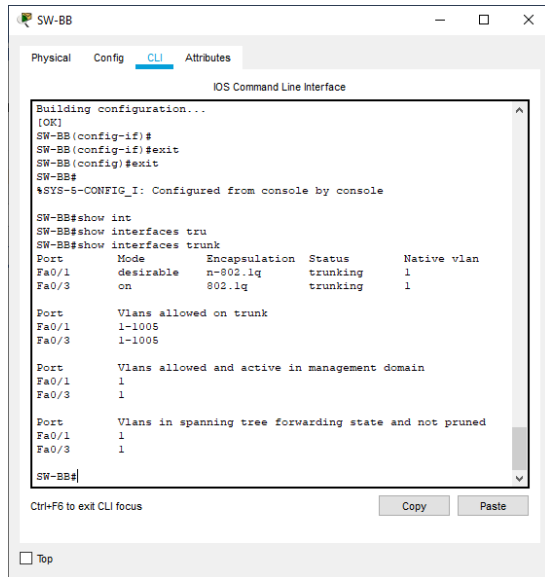
Fuente: Elaboración propia.

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

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

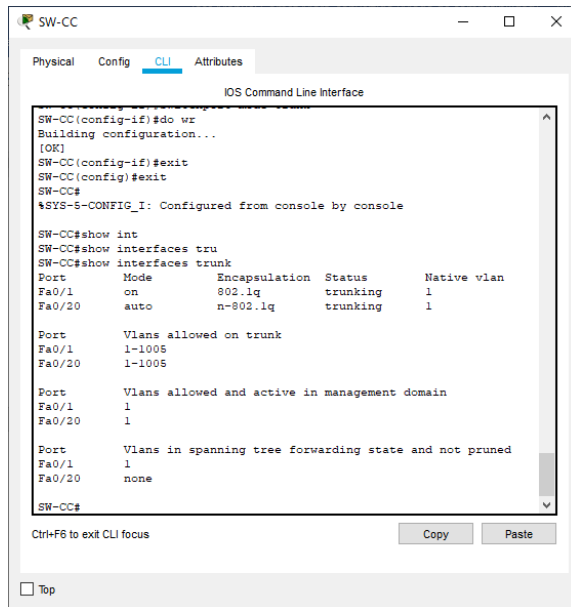
```
SW-BB(config)#interface fastEthernet 0/3 SW-BB(config-if)#switchport mode
trunk
```

Ilustración 14: Modo trunk de los puertos.



Fuente: Elaboración propia.

Ilustración 15: Modo trunk de los puertos.



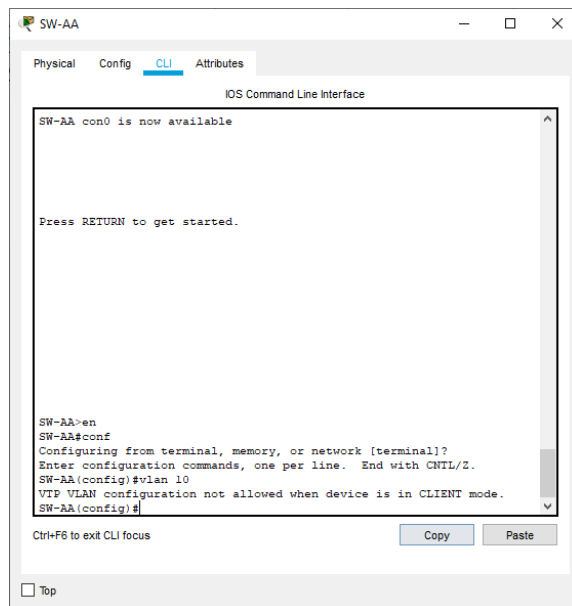
Fuente: Elaboración propia.

Agregar VLANs y asignar puertos.

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

```
SW-AA(config)#vlan 10
```

Ilustración 16: Error en creación de VLAN.



Fuente: Elaboración propia.

```
SW-BB#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z. SW-BB(config)#vlan 10
```

```
SW-BB(config-vlan)#name Compras SW-BB(config-vlan)#vlan 25
```

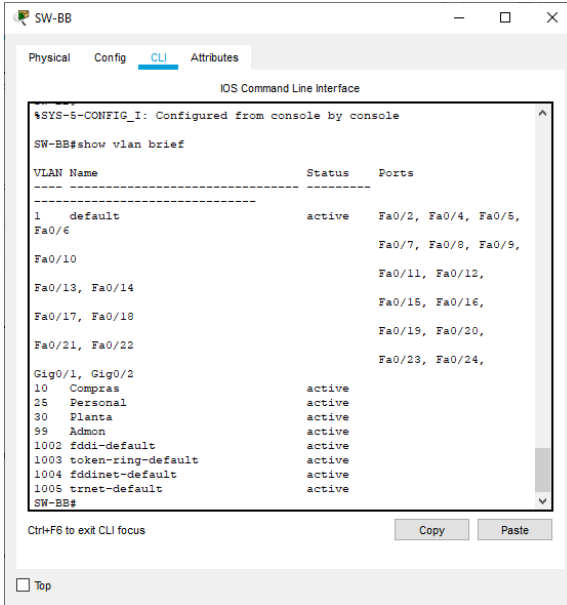
```
SW-BB(config-vlan)#name Personal SW-BB(config-vlan)#vlan 30
```

```
SW-BB(config-vlan)#name Planta SW-BB(config-vlan)#vlan 99
```

```
SW-BB(config-vlan)#name Admon SW-BB(config-vlan)#exit
```

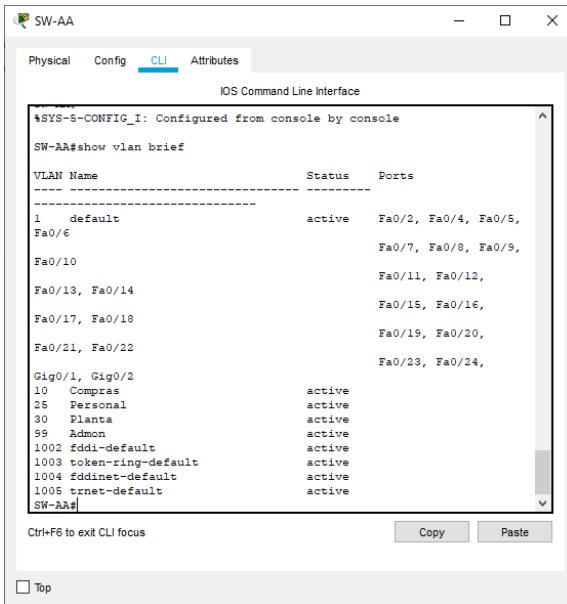
Verifique que las VLANs han sido agregadas correctamente.

Ilustración 17: VLAN creadas en el SW-BB.



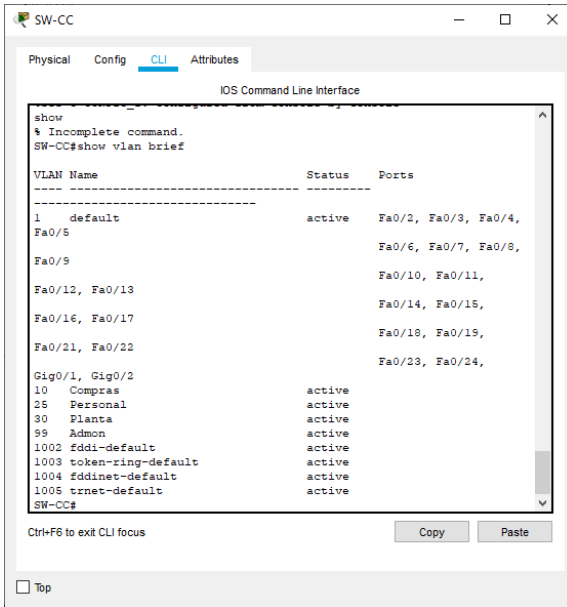
Fuente: Elaboración propia.

Ilustración 18: VLAN creadas por VTP en SW-AA.



Fuente: Elaboración propia.

Ilustración 19: VLAN creadas por VTP en SW-CC.



Fuente: Elaboración propia.

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

Tabla 2. Tabla de direcciones para PCS.

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.X /24
F0/15	VLAN 25	190.108.20.X /24
F0/20	VLAN 30	190.108.30.X /24

Fuente: Prueba de habilidades CCNP 2020, Cisco Academy.

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

```
SW-AA#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z. SW-AA(config)#interface fastEthernet 0/10
```

```
SW-AA(config-if)#switchport mode access SW-AA(config-if)#switchport access vlan 10
```

```
SW-AA(config)#interface fastEthernet 0/15
```

```
SW-AA(config-if)#switchport mode access
```

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

```
SW-AA(config-if)#switchport mode access
```

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

```
SW-BB#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z. SW-BB(config)#interface fastEthernet 0/10
```

```
SW-BB(config-if)#switchport mode access SW-BB(config-if)#switchport access vlan 10
```

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

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

```
SW-BB(config-if)#switchport mode access
```

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

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

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

```
SW-CC(config-if)#switchport mode access SW-CC(config-if)#switchport access vlan 25
```

```

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

```

Configurar las direcciones IP en los Switches.

1. 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 3. Tabla de direccionamiento de los switch.

Equipo	Interfaz	Dirección IP	Máscara
SW-AA	VLAN 99	190.108.99.1	255.255.255.
SW-BB	VLAN 99	190.108.99.2	255.255.255.
SW-CC	VLAN 99	190.108.99.3	255.255.255.

Fuente: Elaboración propia.

```

SW-AA(config)#interface vlan 99
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
SW-BB(config)#interface vlan 99
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
W-CC(config)#interface vlan 99

```

```
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0
```

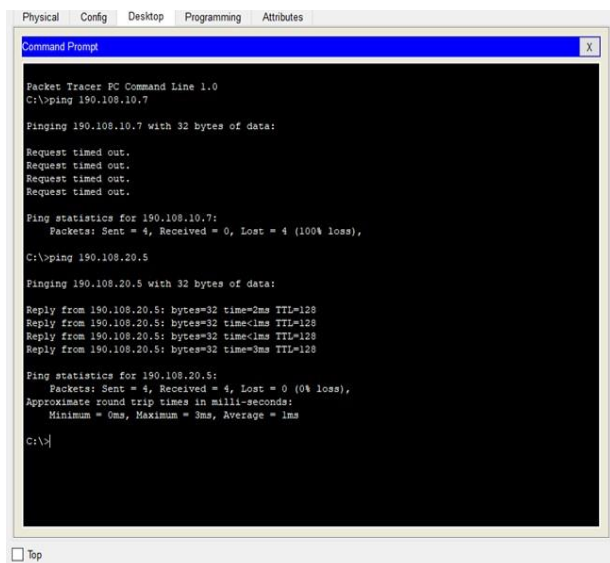
Verificar la conectividad Extremo a Extremo

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

Debido a la configuración establecida en la red de trabajo se evidencia que solo se tienen pings satisfactorios con los PCs que se encuentran dentro del mismo segmento; los pings realizados hacia los PCs que están fuera de la dependencia creada nunca van a establecerse.

Ping de PC6 a PC3 y PC4

Ilustración 20: Prueba de conectividad 1.



```
Physical  Config  Desktop  Programming  Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 190.108.10.7

Pinging 190.108.10.7 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.10.7:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.20.5

Pinging 190.108.20.5 with 32 bytes of data:
Reply from 190.108.20.5: bytes=32 time=2ms TTL=128
Reply from 190.108.20.5: bytes=32 time<1ms TTL=128
Reply from 190.108.20.5: bytes=32 time<1ms TTL=128
Reply from 190.108.20.5: bytes=32 time=3ms TTL=128

Ping statistics for 190.108.20.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

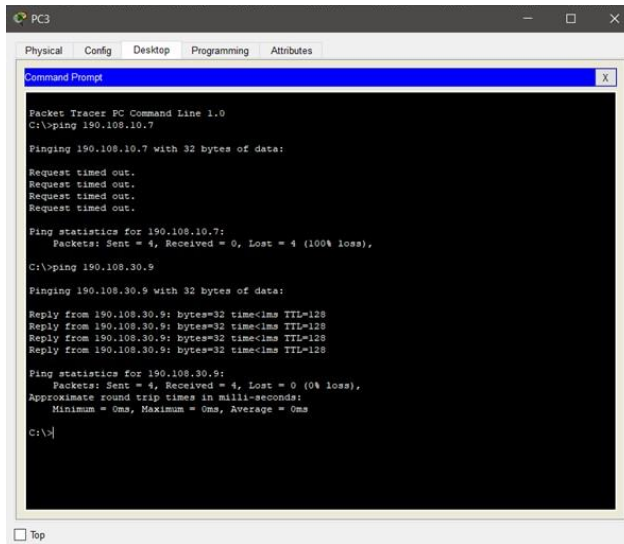
C:\>
```

Fuente: Elaboración propia.



## Ping de PC7 a PC3 y PC9

Ilustración 21: Prueba de conectividad 2.



```
Packet Tracer PC Command Line 1.0
C:\>ping 190.108.10.7

Pinging 190.108.10.7 with 32 bytes of data:

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

Ping statistics for 190.108.10.7:
    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:

Reply from 190.108.30.9: bytes=32 time<1ms TTL=128
Reply from 190.108.30.9: bytes=32 time<1ms TTL=128
Reply from 190.108.30.9: bytes=32 time<1ms TTL=128
Reply from 190.108.30.9: bytes=32 time<1ms TTL=128

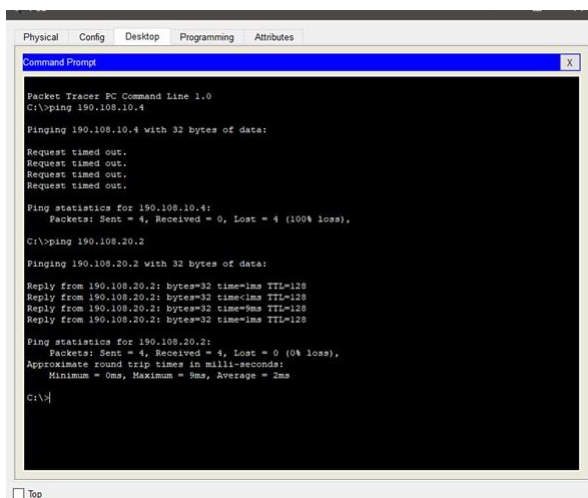
Ping statistics for 190.108.30.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Elaboración propia.

## Ping de PC8 a PC4 y PC2

Ilustración 22: Prueba de conectividad 3.



```
Packet Tracer PC Command Line 1.0
C:\>ping 190.108.10.4

Pinging 190.108.10.4 with 32 bytes of data:

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

Ping statistics for 190.108.10.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.20.2

Pinging 190.108.20.2 with 32 bytes of data:

Reply from 190.108.20.2: bytes=32 time<1ms TTL=128
Reply from 190.108.20.2: bytes=32 time<1ms TTL=128
Reply from 190.108.20.2: bytes=32 time=9ms TTL=128
Reply from 190.108.20.2: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 9ms, Average = 2ms

C:\>
```

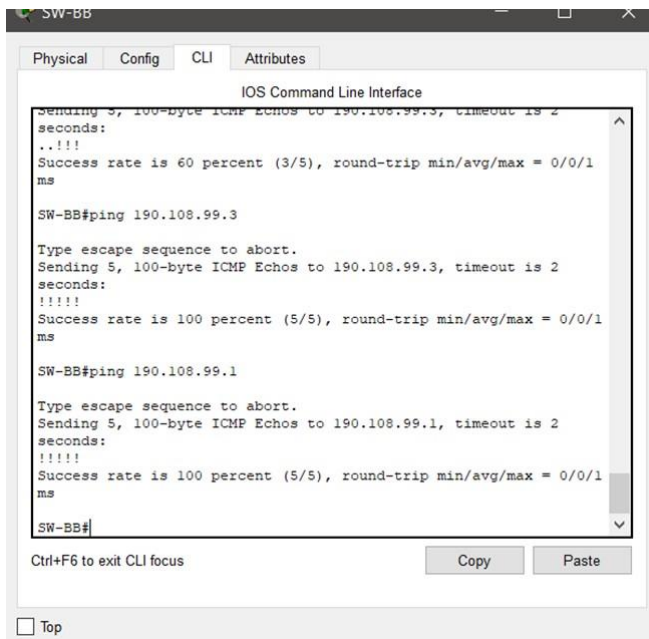
Fuente: Elaboración propia.

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

Bajo la configuración establecida de cada uno de los switch si es posible tener comunicación entre cada uno de ellos debido a que al tener configurada una vlan común o de administración se va a tener comunicación exitosa.

## Ping de SW-BB a SW-AA Y SW-CC

Ilustración 23: Prueba de conectividad 4.



```
SW-BB#
Physical  Config  CLI  Attributes
IOS Command Line Interface
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2
seconds:
..!!!
Success rate is 60 percent (3/5), 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 = 0/0/1
ms

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#
```

Ctrl+F6 to exit CLI focus

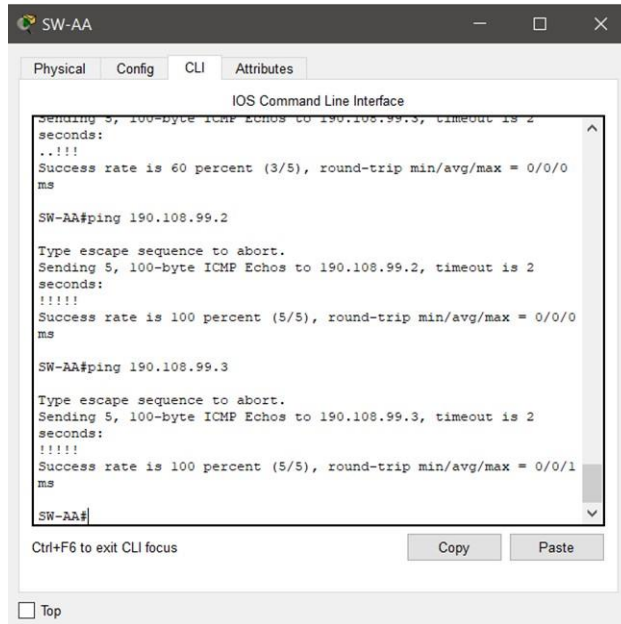
Copy Paste

Top

Fuente: Elaboración propia.

## Ping de SW-AA a SW-BB Y SW-CC

Ilustración 24: Prueba de conectividad 5.



```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2
seconds:
.....
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0
ms
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 = 0/0/0
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
SW-AA#
```

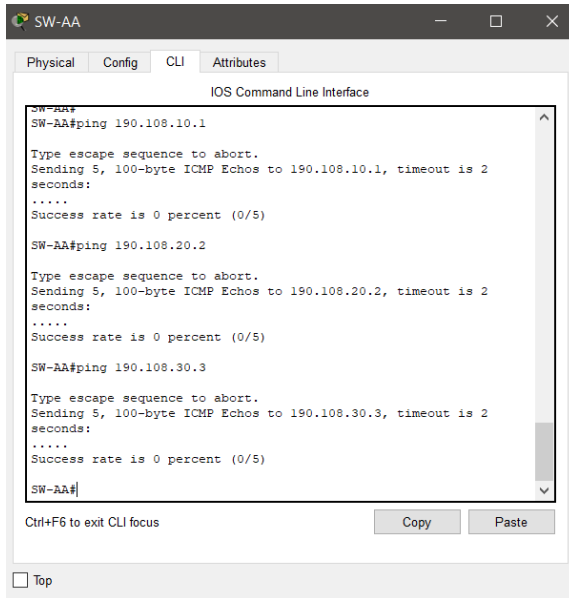
Fuente: Elaboración propia.

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

Dispositivos como sw y pcs no tienen la capacidad de enrutarse a otras redes sin dispositivos físicos y protocolos, también hay que tener en cuenta que a los pcs no tienen configuradas IPs y puertos de enlace y sin eso no es imposible conectarse con otras redes.

## Ping de SW-AA a PC1-PC2 y PC3

Ilustración 25: Prueba de conectividad 6.

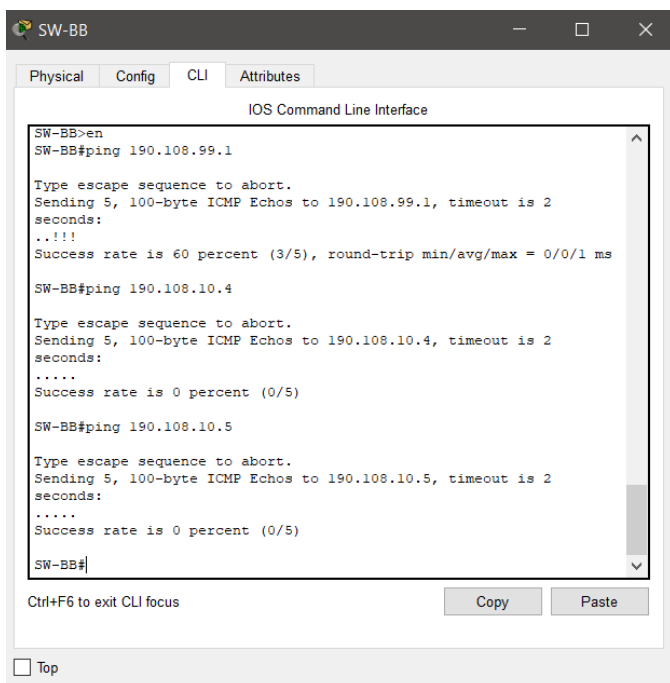


```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
SW-AA#ping 190.108.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.1, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#ping 190.108.20.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.2, timeout is 2
seconds:
.....
Success rate is 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#
Ctrl+F6 to exit CLI focus Copy Paste
Top
```

Fuente: Elaboración propia.

## Ping de SW-BB a PC4-PC5 y PC6

## Ilustración 26: Prueba de conectividad 7.



```
SW-BB>en
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 60 percent (3/5), round-trip min/avg/max = 0/0/1 ms

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 190.108.10.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.5, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#
```

Ctrl+F6 to exit CLI focus

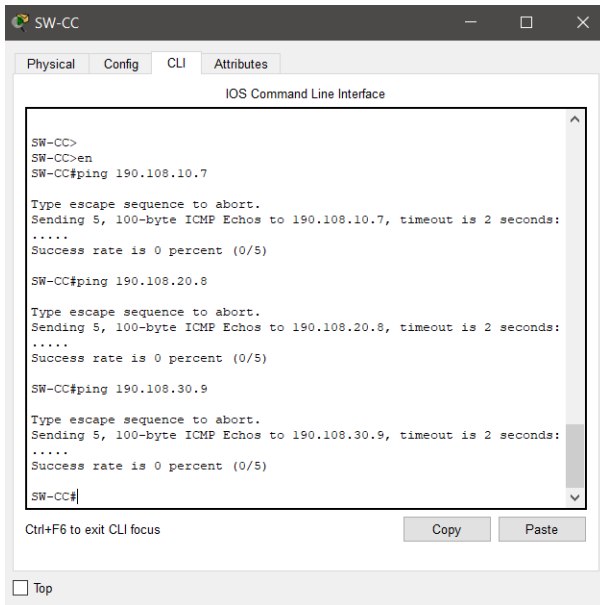
Copy Paste

Top

Fuente: Elaboración propia

## Ping de SW-CC a PC7-PC8 y PC9

Ilustración 27: Prueba de conectividad 8.



```
SW-CC
SW-CC>en
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 190.108.20.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.8, timeout is 2 seconds:
.....
Success rate is 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#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Fuente: Elaboración propia.

## CONCLUSIONES

Durante el desarrollo de la presente actividad se logra exponer la práctica del aprendizaje adquirido a lo largo del curso y aplicar de manera hábil las competencias en cada uno de los escenarios planteados.

El protocolo de OSPF permite configurar de manera sencilla la creación de grandes redes ayudando a establecer rutas eficientes que permitan la transmisión de la información de manera bidireccional; lo que conlleva a tener un desempeño de red más rápido y reducción de pérdida de paquetes.

Se evidencia el funcionamiento del protocolo de enrutamiento BGP que a pesar de tener un nivel de dificultad alto a la hora de configurarlo su funcionamiento es muy simple, fiable y es la mejor manera de establecer las rutas mas eficientes acorde a la topología diseñada.

En la temática relacionada con el Switching fue realmente interesante aprender del potencial que tiene el Switch a nivel de red y sus funciones, como es el caso del protocolo VTP el cual permite administrar las Vlan de una red, dividirla o segmentarla y crear rutas troncales.

El éxito de una implementación por protocolo VTP radica en la configuración de un dominio para toda la red y que dicha parametrización este replicada en cada uno de los Switch que la conforman.

## BIBLIOGRAFIA

Donohue, D. CISCO Press (Ed). CCNP Quick Reference. {En Linea}. 2017. {Consultado el 16 Mayo 2020}. Recuperado de <https://1drv.ms/b/s!AgIGg5JUgUBthFt77ehzL5qp0OKD>

García, V. S. Diseño de Redes con BGP. {En Linea}. 2017. {Consultado el 18 Mayo 2020}. Obtenido de Universitat Politècnica de València: <https://riunet.upv.es/bitstream/handle/10251/91691/S%C3%81NCHEZ%20-%20Dise%C3%B1o%20de%20redes%20con%20BGP.pdf?sequence=1>

Hucaby, D. CISCO Press (Ed). CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. {En Linea}. 2015. {Consultado el 18 Mayo 2020}. Recuperado de <https://onedrive.live.com/?authkey=%21AHpFYJKwJmd8OjY&cid=6D40815492830602&id=6D40815492830602%21605&parId=6D40815492830602%21602&o=OneUp>

Teare, Diane. CISCO Press (Ed). ImplementingCiscoIPRouting. {En Linea}. 2014. {Consultado el 16 Mayo 2020}. Recuperado de <https://1drv.ms/b/s!AgIGg5JUgUBthFt77ehzL5qp0OKD>

Tecnologías, S., Estudios De Caso BGP, N. {En Linea}. 2020. {Consultado el 15 Mayo 2020}. Cisco. Recuperado de: [https://www.cisco.com/c/es\\_mx/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html](https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html)