

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

LUIS ALFONSO MENDIETA SALGADO

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

INGENIERÍA ELECTRONICA

GIRARDOT

2020

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

LUIS ALFONSO MENDIETA SALGADO

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
INGENIERÍA ELECTRONICA

GIRARDOT

2020

NOTA DE ACEPTACIÓN

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Girardot, 15 de mayo de 2020

AGRADECIMIENTOS

A mi familia, gestora de un proyecto de vida, de una razón, motivo de mi lucha incansable.

A la Universidad Nacional Abierta y a Distancia – UNAD. Institución de educación superior, por darme la oportunidad de desarrollarme en mi plano educacional.

CONTENIDO

LISTA DE TABLAS.....	6
LISTA DE FIGURAS.....	7
GLOSARIO.....	8
RESUMEN.....	9
ABSTRACT.....	9
INTRODUCCION.....	10
DESARROLLO DE LOS ESCENARIOS	11
Escenario 2	11
Relación de vecino BGP entre R1 y R2.....	12
Relación de vecino BGP entre R2 y R3.....	14
Relación de vecino BGP entre R3 y R4.....	16
Escenario 3	19
A. Configurar VTP.....	19
B. Configurar DTP (Dynamic Trunking Protocol).....	22
C. Agregar VLANs y asignar puertos.....	25
D. Configurar las direcciones IP en los Switches.	30
E. Verificar la conectividad Extremo a Extremo.....	31
CONCLUSIONES.....	37
BIBLIOGRAFIA.....	38

LISTA DE TABLAS

Tabla 1. interfaz, dirección IP y máscara.	12
Tabla 2. Tabla de direcciones para PCS.....	28
Tabla 3. Tabla de direccionamiento de PC.	30
Tabla 4. Tabla de direccionamiento de los switch.....	30

LISTA DE FIGURAS

Figura 1. Escenario 2.	11
Figura 2. Rutas vecinas entre R1 y R2.....	13
Figura 3. Rutas vecinas entre R1 y R2.....	13
Figura 4. Rutas vecinas entre R2 y R3.....	15
Figura 5. Rutas vecinas entre R2 y R3.....	16
Figura 6. Rutas vecinas entre R3 y R4.....	17
Figura 7. Rutas vecinas entre R3 y R4.....	18
Figura 8. Escenario 3.	19
Figura 9. Status del SW en VTP.....	21
Figura 10. Status del SW en VTP.....	21
Figura 11. Status del SW en VTP.....	22
Figura 12. Modo trunk de los puertos.....	23
Figura 13. Modo trunk de los puertos.....	24
Figura 14. Modo trunk de los puertos.....	24
Figura 15. Modo trunk de los puertos.....	25
Figura 16. Error en creación de VLAN.	26
Figura 17. VLAN creadas en el SW.....	27
Figura 18. VLAN creadas por VTP en SW.	27
Figura 19. VLAN creadas por VTP en SW.	28
Figura 20. Prueba de conectividad.....	31
Figura 21. Prueba de conectividad.....	32
Figura 22. Prueba de conectividad.....	32
Figura 23. Prueba de conectividad.....	33
Figura 24. Prueba de Conectividad.....	34
Figura 25. Prueba de conectividad.....	35
Figura 26. Prueba de conectividad.....	35
Figura 27. Prueba de conectividad.....	36

GLOSARIO

Red LAN: es una sigla que refiere a Local Area Network (Red de Área Local). Estas redes vinculan computadoras que se hallan en un espacio físico pequeño, como una oficina o un edificio. La interconexión se realiza a través de un cable o de ondas.

Red WAN: es la sigla de Wide Area Network (“**Red** de Área Amplia”). El concepto se utiliza para nombrar a la **red** de computadoras que se extiende en una gran franja de territorio, ya sea a través de una ciudad, un país o, incluso, a nivel mundial. Un ejemplo de **red WAN** es la propia Internet.

Router: es un comando que muestra y modifica las entradas en la tabla de enrutamiento IP. Usado sin parámetros, muestra la ruta de ayuda.

Spoofing: es el uso de técnicas de suplantación de identidad generalmente para usos maliciosos. Se pueden clasificar sus ataques en función de la tecnología utilizada. Entre ellos el más extendido es el IP spoofing, aunque también existe el ARP spoofing, DNS spoofing, Web spoofing o email spoofing.

Switch: un switch o conmutador es un dispositivo de interconexión de redes informáticas. En computación y en informática de redes, un switch es el dispositivo analógico que permite interconectar redes operando en la capa 2 o de nivel de enlace de datos del modelo OSI u Open Systems Interconnection.

RESUMEN

En el presente trabajo se describen los pasos correspondientes a la configuración de tres diferentes escenarios propuestos en la prueba de habilidades prácticas del diplomado de profundización Cisco CCNP.

Se brinda solución a las situaciones planteadas mostrando a través de tablas e imágenes el desarrollo aplicando los conocimientos adquiridos en el diplomado y durante la carrera de ingeniería electrónica en conmutación, enrutamiento dinámico y los diferentes protocolos como VLAN Trunking Protocol así como configuración de redes basada en switches; todo esto para dar solución a problemas que se relacionan con diversos aspectos de networking y que nos van a ser muy útiles aplicándolos a nuestra profesión.

.

ABSTRACT

In this paper, the steps corresponding to the configuration of three different scenarios proposed in the practical skills test of the Cisco CCNP.

Solution to the situations presented is shown showing through tables and images the development applying the knowledge acquired in the diploma course and during the career of electronic engineering in switching, dynamic routing and the different protocols such as VLAN Trunking Protocol as well as networking based configuration on switches; all this to solve problems that are related to various aspects of networking and that will be very useful to us applying them to our profession.

INTRODUCCION

El presente documento contiene el desarrollo de la Prueba de Habilidades Practicas, la cual forma parte de las actividades evaluativas del Diplomado de Profundización CCNP, y busca identificar el grado de desarrollo de competencias y habilidades que logramos adquirir a lo largo del diplomado. Mediante los 3 escenarios propuestos se busca poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

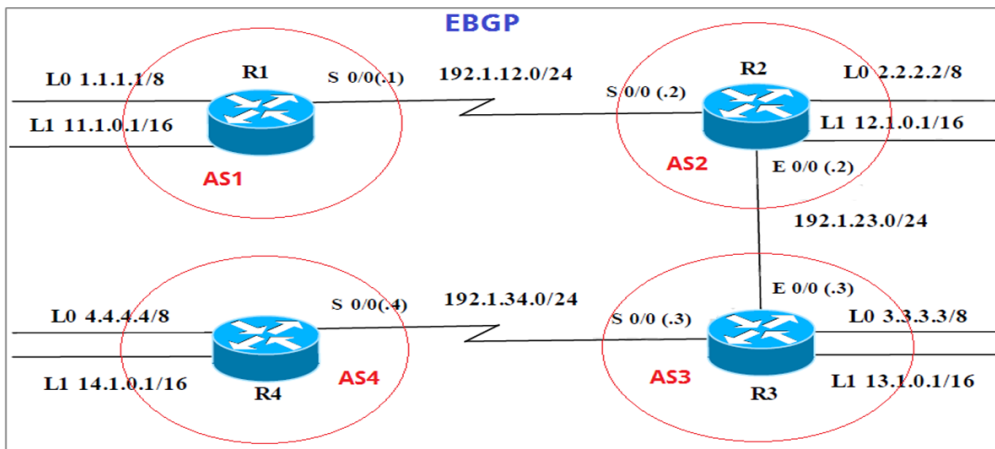
Para cumplir con los propósitos mencionados, se abordan temáticas como el enrutamiento dinámico a través de los protocolos OSPF y EIGRP, así como la configuración de áreas y sistemas autónomos respectivamente, el enrutamiento a través del protocolo BGP y el proceso de creación de adyacenticas en función del protocolo IPv4, del Router ID e interfaces Loopback.

Por último, se evidencia la configuración de una pequeña red basada en Switches capa 2 y PCs, en la cual se configura el enrutamiento IPv4 respectivo, se implementa protocolos como VLAN Trunking Protocol y Dynamic Trunking Protocol, así como una parte inicial del enrutamiento InterVLAN.

DESARROLLO DE LOS ESCENARIOS

Escenario 1

Figura 1. Escenario 2.



Fuente: Prueba de habilidades CCNP 2020, Cisco Academy.

Tabla 1. interfaz, dirección IP y máscara.

R1	Interfaz	Dirección IP	Máscara
	Loopback 0	1.1.1.1	255.0.0.0
	Loopback 1	11.1.0.1	255.255.0.0
	S 0/0	192.1.12.1	255.255.255.0
R2	Interfaz	Dirección IP	Máscara
	Loopback 0	2.2.2.2	255.0.0.0
	Loopback 1	12.1.0.1	255.255.0.0
	S 0/0	192.1.12.2	255.255.255.0
	E 0/0	192.1.23.2	255.255.255.0
R3	Interfaz	Dirección IP	Máscara
	Loopback 0	3.3.3.3	255.0.0.0
	Loopback 1	13.1.0.1	255.255.0.0
	E 0/0	192.1.23.3	255.255.255.0
	S 0/0	192.1.34.3	255.255.255.0
R4	Interfaz	Dirección IP	Máscara
	Loopback 0	4.4.4.4	255.0.0.0
	Loopback 1	14.1.0.1	255.255.0.0
	S 0/0	192.1.34.3	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
```

Figura 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.

Figura 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

```

Figura 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
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.12.1, 00:06:17
     12.0.0.0/16 is subnetted, 1 subnets
C       12.1.0.0 is directly connected, Loopback1
     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.

Figura 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...

```

Figura 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.

Figura 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

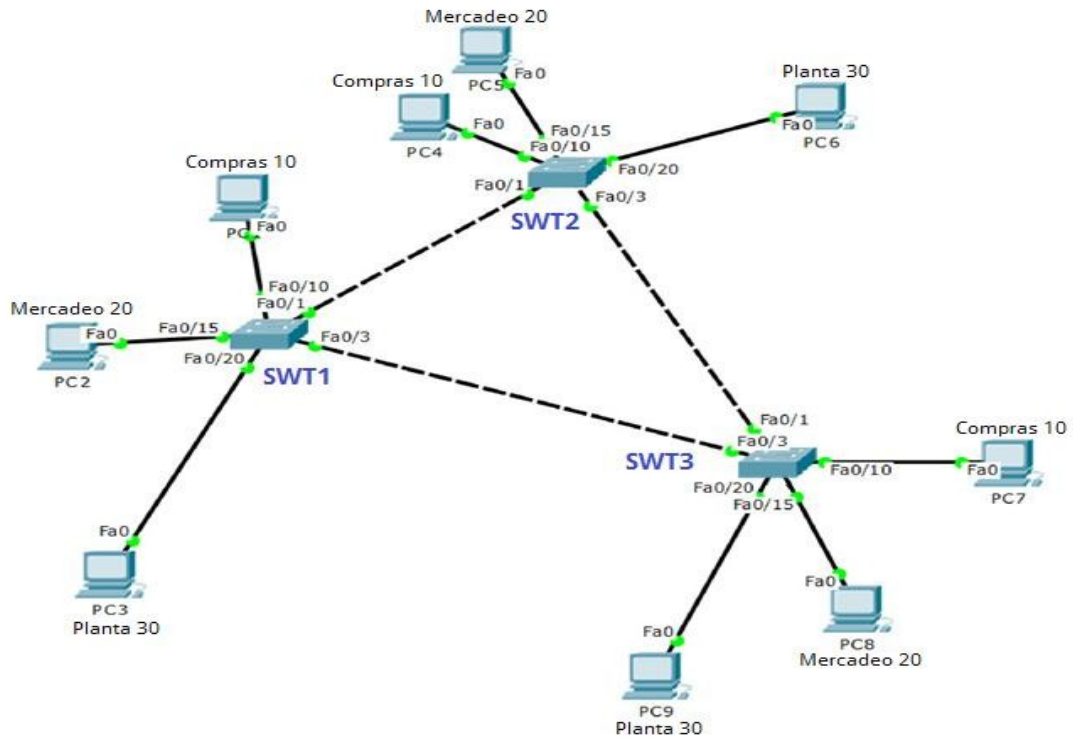
Gateway of last resort is not set

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
```

Fuente: Elaboración propia.

Escenario 2

Figura 8. Escenario 3.



Fuente: Prueba de habilidades CCNP 2020, Cisco Academy.

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 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

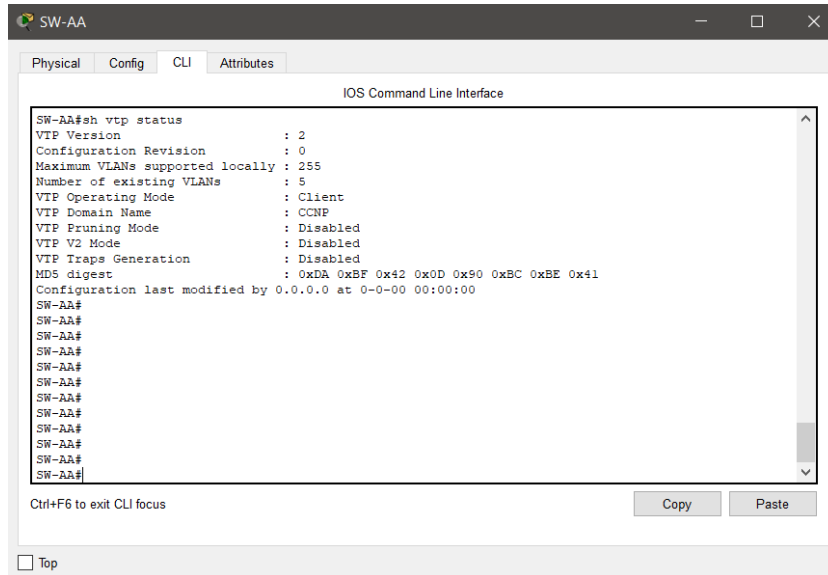
```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-BB
SW-BB(config)#vtp mode server
Device mode already VTP SERVER.
SW-BB(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-BB(config)#vtp password cisco
Setting device 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
```

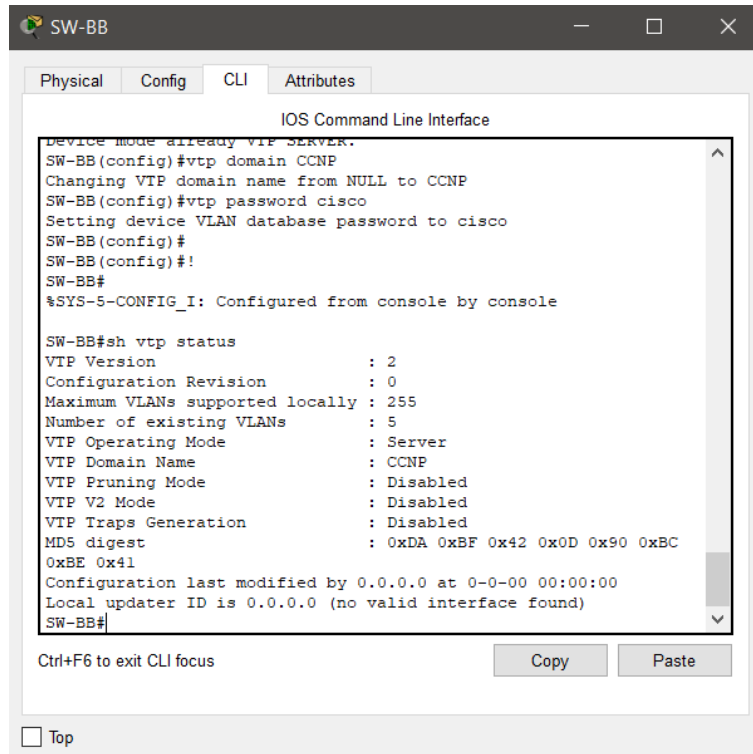
2. Verifique las configuraciones mediante el comando show vtp status.

Figura 9. Status del SW en VTP.



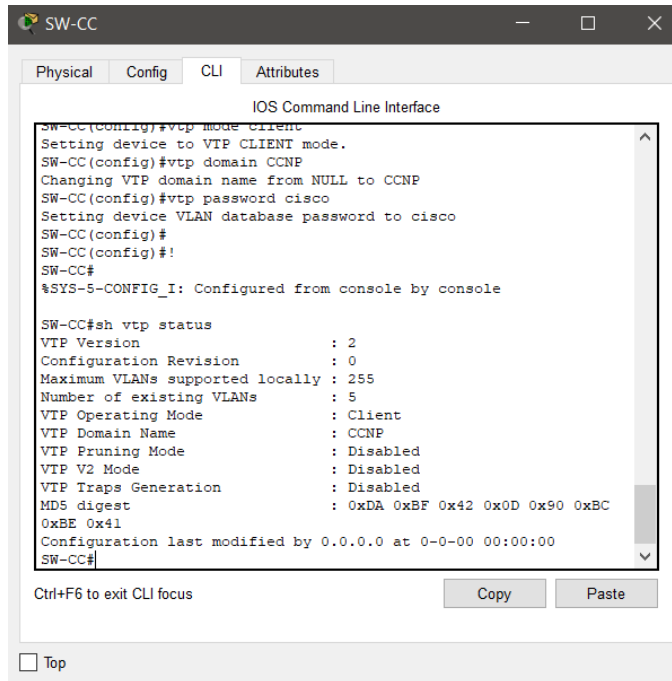
Fuente: Elaboración propia.

Figura 10. Status del SW en VTP.



Fuente: Elaboración propia.

Figura 11. Status del SW en VTP.



```
SW-CC
Physical Config CLI Attributes
IOS Command Line Interface
SW-CC(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-CC(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-CC(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-CC(config)#
SW-CC(config)#!
SW-CC#
%SYS-5-CONFIG_I: Configured from console by console

SW-CC#sh 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.

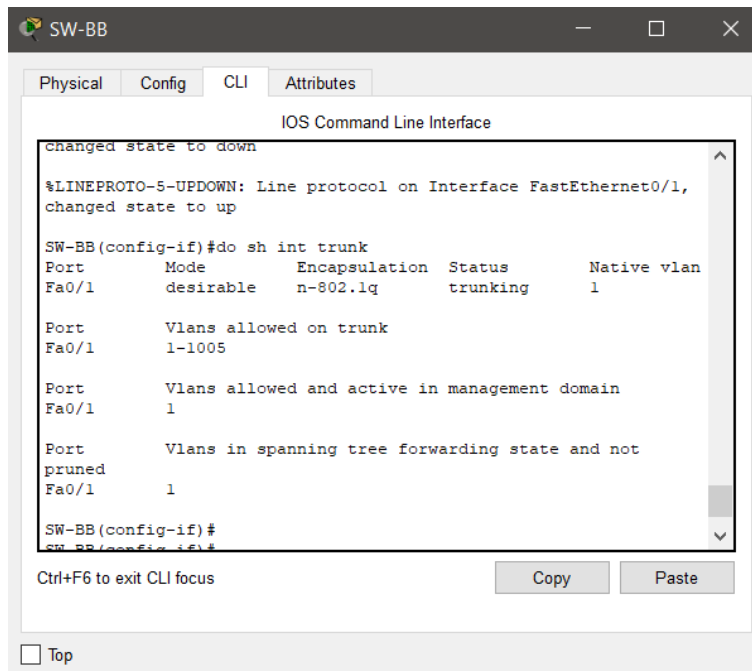
B. Configurar DTP (Dynamic Trunking Protocol)

1. 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
```

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

Figura 12. Modo trunk de los puertos.



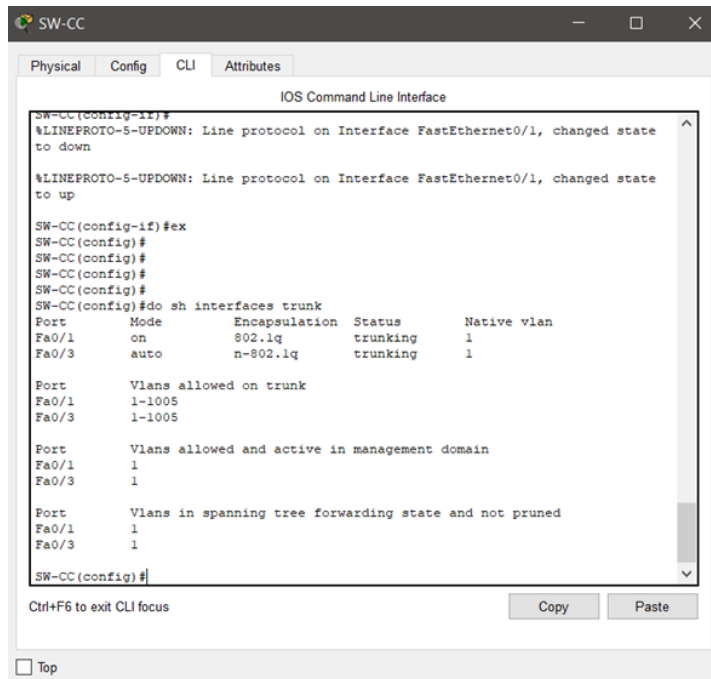
Fuente: Elaboración propia.

3. 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
```

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

Figura 15. Modo trunk de los puertos.



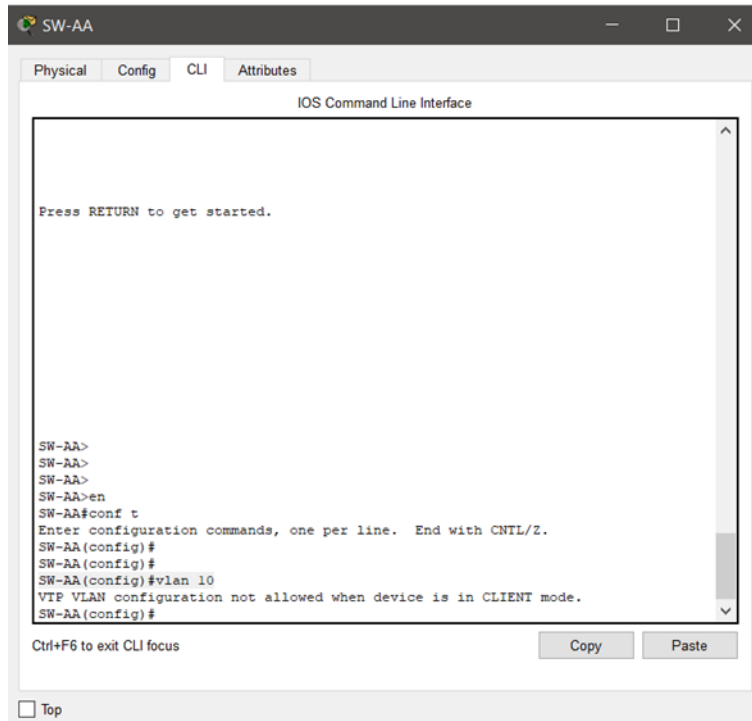
Fuente: Elaboración propia.

C. Agregar VLANs y asignar puertos.

1. En STW1 agregue la VLAN 10. En STW2 agregue las VLANs Compras (10), Personal (20), Planta (30) y Admon (99).

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

Figura 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
```

2. Verifique que las VLANs han sido agregadas correctamente.

Figura 17. VLAN creadas en el SW.

```
SW-BB(config-vlan)#exit
SW-BB(config)#
SW-BB(config)#
SW-BB(config)#
SW-BB(config)#!!
SW-BB#
%SYS-5-CONFIG_I: Configured from console by console

SW-BB#
SW-BB#
SW-BB#
SW-BB#sh vlan brief
```

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

SW-BB#

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Fuente: Elaboración propia.

Figura 18. VLAN creadas por VTP en SW.

```
SW-AA(config)#
SW-AA(config)#
SW-AA(config)#
SW-AA(config)#!
SW-AA#
%SYS-5-CONFIG_I: Configured from console by console

SW-AA#
SW-AA#
SW-AA#
SW-AA#sh vlan br
SW-AA#sh vlan brief
```

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

SW-AA#

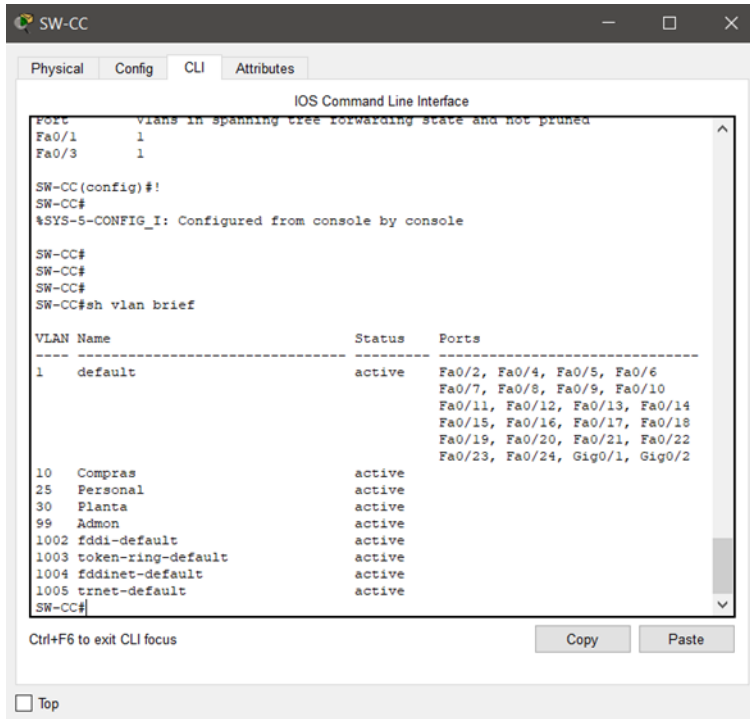
Ctrl+F6 to exit CLI focus

Copy Paste

Top

Fuente: Elaboración propia.

Figura 19. VLAN creadas por VTP en SW.



Fuente: Elaboración propia.

3. 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

X = número de cada PC particular

Fuente: Prueba de habilidades CCNP 2020, Cisco Academy.

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

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

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

```
SW-CC(config)#interface fastEthernet 0/10
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-if)#interface fastEthernet 0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30
```

Tabla 3. Tabla de direccionamiento de PC.

Pc	Vlan	Ip	Mascara
1	10	190.108.10.1	255.255.255.0
4	10	190.108.10.2	255.255.255.0
7	10	190.108.10.3	255.255.255.0
2	20	190.108.20.4	255.255.255.0
5	20	190.108.20.5	255.255.255.0
8	20	190.108.20.6	255.255.255.0
3	30	190.108.30.7	255.255.255.0
6	30	190.108.30.8	255.255.255.0
9	30	190.108.30.9	255.255.255.0

Fuente: Elaboración propia.

D. 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 4. 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
```

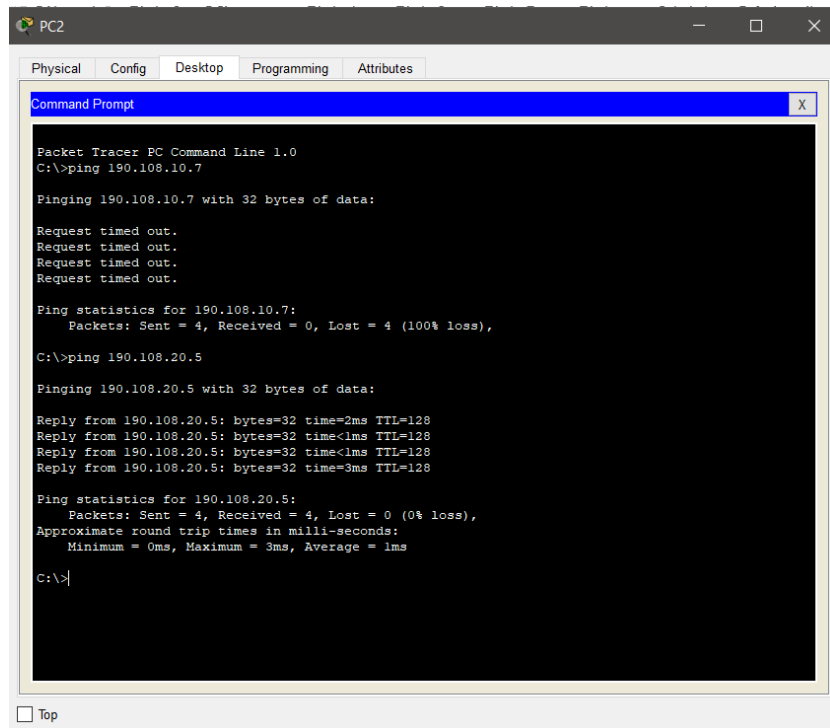
```
W-CC(config)#interface vlan 99
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0
```

E. Verificar la conectividad Extremo a Extremo

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

Ping de PC2 a PC5 y PC7

Figura 20. Prueba de conectividad.



```
PC2
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

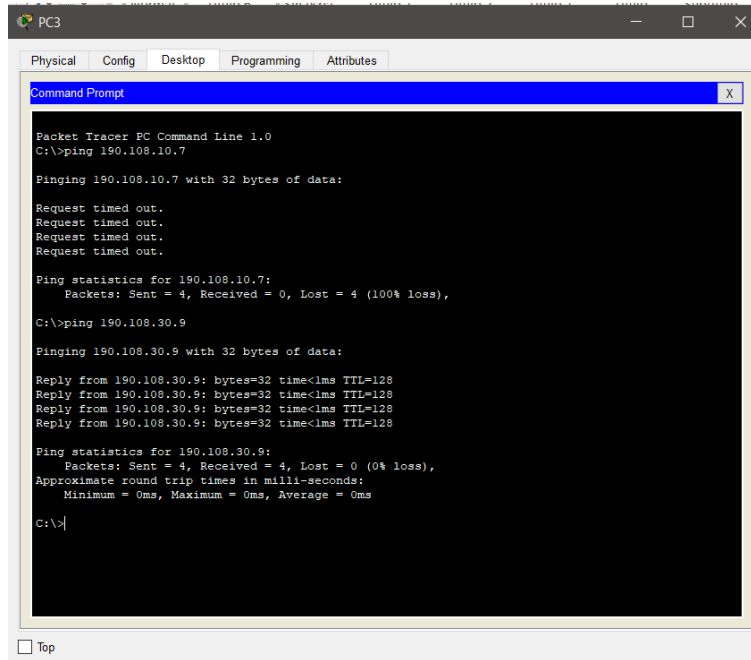
Ping statistics for 190.108.20.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>
```

Fuente: Elaboración propia.

Ping de PC3 a PC7 y PC9

Figura 21. Prueba de conectividad.



```
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

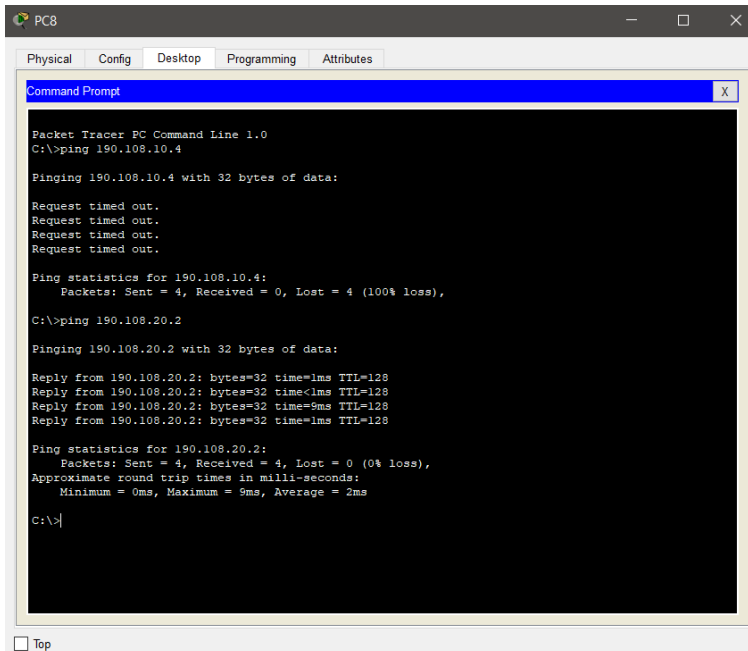
Ping statistics for 190.108.30.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Fuente: Elaboración propia.

Ping de PC8 a PC4 y PC2

Figura 22. Prueba de conectividad.



```
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:\>
```

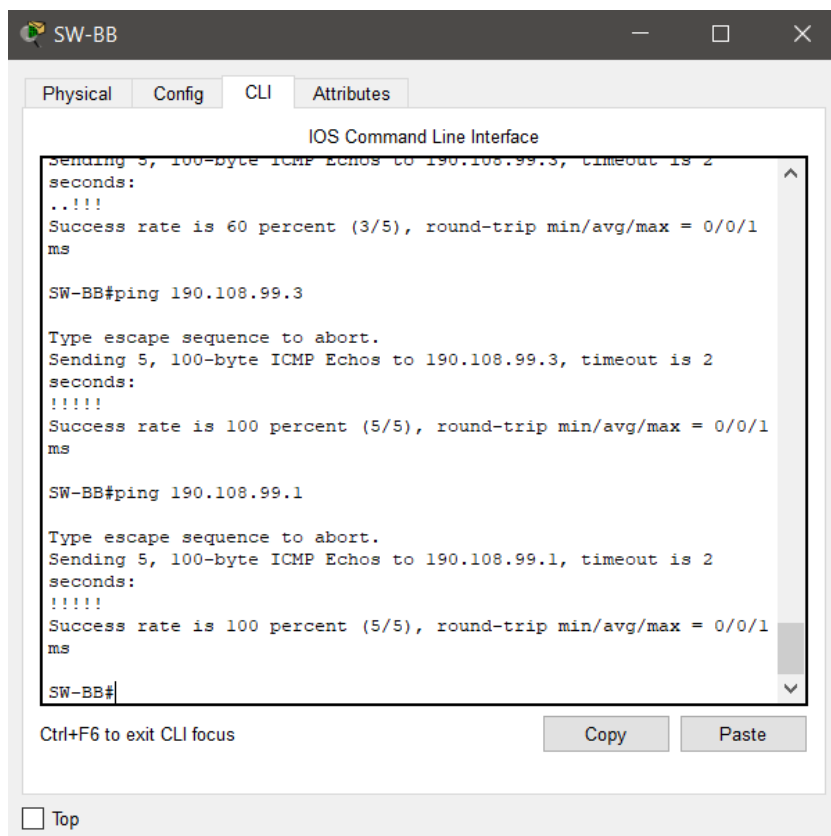
Fuente: Elaboración propia.

La conectividad entre las mismas vlan funciona de forma adecuada, no funciona entre vlan de diferente id ya que el ejercicio no contiene enrutamiento y no tiene como redireccionar el proceso entre redes diferentes

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

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

Figura 23. Prueba de conectividad.



```
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#
```

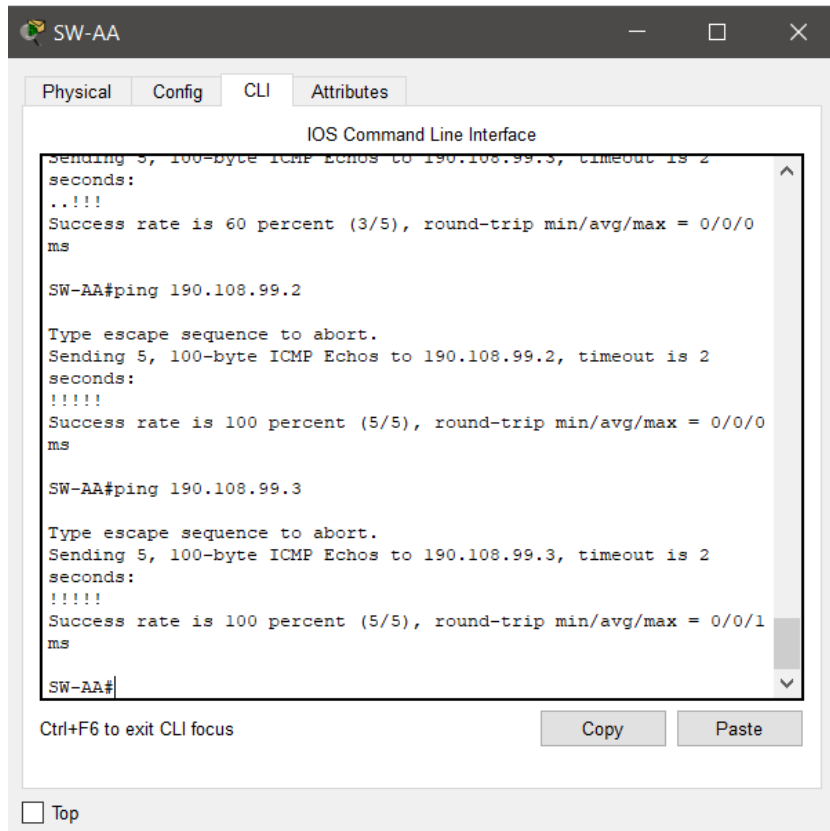
Ctrl+F6 to exit CLI focus Copy Paste

Top

Fuente: Elaboración propia.

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

Figura 24. Prueba de Conectividad.



The screenshot shows a window titled "SW-AA" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The output shows three ping tests:

```
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#
```

At the bottom of the CLI window, there is a "Ctrl+F6 to exit CLI focus" instruction, "Copy" and "Paste" buttons, and a "Top" button.

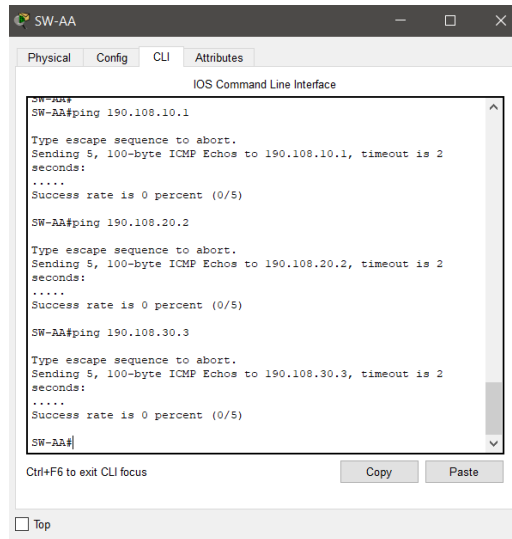
Fuente: Elaboración propia.

El ping entre los sw funciona de forma adecuada ya que sus direcciones están en la misma vlan y no tienen problema de comunicaciones entre ellos

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

Ping de SW-AA a PC1-PC2 y PC3

Figura 25. Prueba de conectividad.

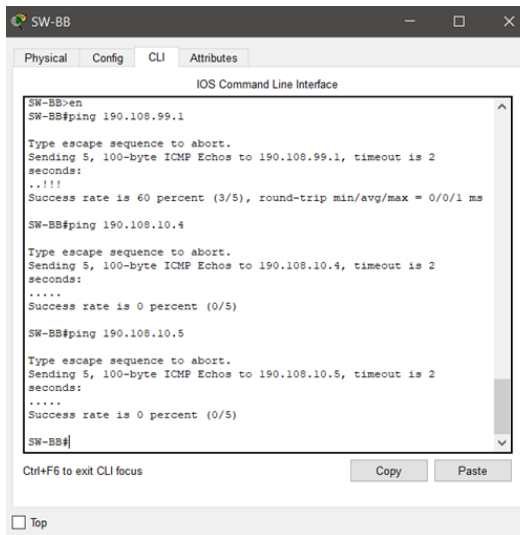


```
SW-AA#ping 190.108.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.1, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#ping 190.108.20.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.2, timeout is 2
seconds:
.....
Success 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#
```

Fuente: Elaboración propia.

Ping de SW-BB a PC4-PC5 y PC6

Figura 26. Prueba de conectividad.

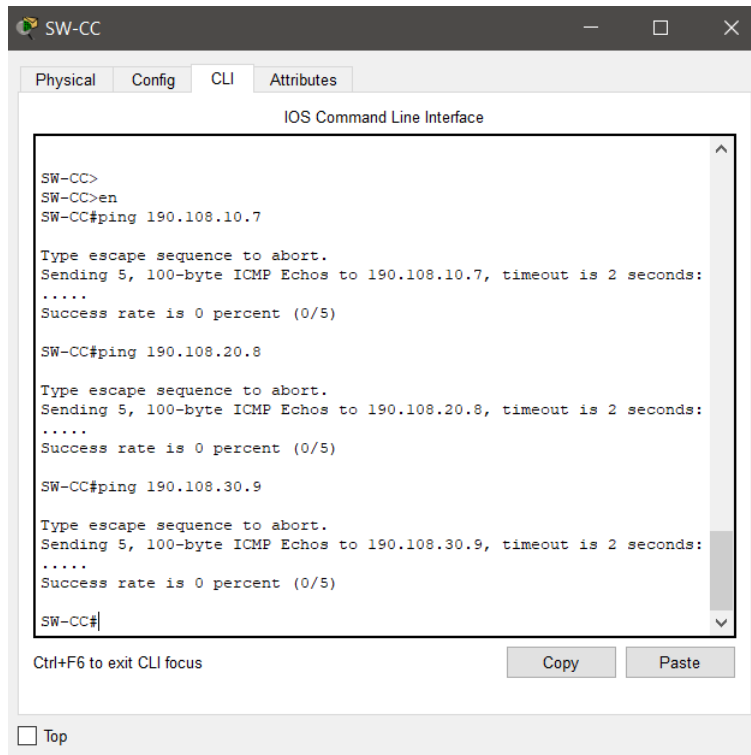


```
SW-BB>en
SW-BB#ping 190.108.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2
seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/1 ms
SW-BB#ping 190.108.10.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 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#
```

Fuente: Elaboración propia.

Ping de SW-CC a PC7-PC8 y PC9

Figura 27. Prueba de conectividad.



```
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#|
```

Fuente: Elaboración propia.

Es el mismo caso presentado anteriormente, al no estar conectadas en la misma VLAN los pcs no pueden comunicarse entre ellos, se necesita un router que realice las comunicaciones entre redes diferentes ya que el protocolo vtp lo único que hace es duplicar las vlan en los sw client

CONCLUSIONES

Durante el desarrollo de los escenarios propuestos en la prueba, pudimos afianzar los conocimientos adquiridos sobre protocolos de enrutamiento, como BGP y distribución de vlan en switc con VTP, y realizar la implementación de ellos en los simuladores Packet tracer y GNS3, es raro ver como una propuesta de cisco no se puede desarrollar completa en su propio simulador y debimos acudir a simuladores alternos.

Una vez configurados los dispositivos solicitados pude apreciar la importancia de cada uno de ellos, y ver cual son los ítems a tener en cuenta cuando puedan llegar a presentar errores de conectividad, aprovechar la información que arrojan los comando show es muy crucial para desarrollar un trobleshooting real

Mediante la práctica se aplicaron los conocimientos en enrutamiento y configuración de redes para dar solución a los escenarios planteados, configuración y administración de los dispositivos por lo cual se comprende la importancia del enrutamiento para ser aplicados en el ámbito laboral y profesional.

BIBLIOGRAFIA

Casos Prácticos de BGP. (30 de Octubre de 2008). Obtenido de Cisco: https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html

Froom, R., Frahim, E. (2015). CISCO Press (Ed). *Fundamentals Review. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115*. Recuperado de: <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). *Campus Network Design Fundamentals. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115*. Recuperado de: <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). *Campus Network Architecture*.

Froom, R., Frahim, E. (2015). CISCO Press (Ed). *InterVLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115*. Recuperado de: <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>

García, V. S. (04 de Julio de 2017). *Diseño de Redes con BGP*. Obtenido de Universitat Politècnica de València: <https://riunet.upv.es/bitstream/handle/10251/91691/S%C3%81NCHEZ%20->

Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de: <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>