

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JHONNATAN ORDOÑEZ PIAMBA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE TELECOMUNICACIONES
Santiago de Cali
2020

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JHONNATAN ORDOÑEZ PIAMBA

Diplomado para opción de grado presentado para optar el
título de INGENIERO DE TELECOMUNICACIONES.

DIRECTOR
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA DE TELECOMUNICACIONES
Santiago de Cali
2020

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Santiago de Cali, 22 de mayo de 2020

AGRADECIMIENTOS

Durante el proceso académico en la universidad pasé por momentos difíciles el cual tuve que aplazar mis estudios, pasaron años para volver a retomar y durante ese tiempo ya no tenía la perseverancia, los ánimos y tampoco querer culminar la carrera.

Es por eso que, durante ese tiempo algunas personas importantes en mi vida como mi familia, amigos de infancia y esos amigos que se ganan en la universidad a través de los cinco años, estuvieron para no dejarme desfallecer ante todas las dificultades. También reconocer a todos los docentes, directores de curso que permitieron llegar a esta fase final ya que, sin sus conocimientos, apoyos, orientación esto sería aún más difícil

Gracias por permitirme seguir adelante y conseguir este logro, para así seguir conquistando mis metas.

CONTENIDO

AGRADECIMIENTOS	4
CONTENIDO	5
LISTAS DE TABLAS	6
LISTA DE FIGURAS	7
GLOSARIO	9
RESUMEN	10
ABSTRACT	11
INTRODUCCIÓN	12
DESARROLLO	13
Escenario 1	13
Escenario 2	24
CONCLUSIONES	44
BIBLIOGRAFÍA	45

LISTAS DE TABLAS

Tabla 1 , Configuración Router R1	13
Tabla 2 , Configuración Router R2	13
Tabla 3 , Configuración Router R3	14
Tabla 4 , Configuración Router R4	14
Tabla 5 , Configuración de Puertos a las VLANs y direcciones IP	32
Tabla 6 , Asignar IP en los switch para la VLAN 99	38

LISTA DE FIGURAS

Ilustración 1 , Escenario EBGp	13
Ilustración 2 , Show IP Route en R1	17
Ilustración 3 , Show IP Route en R2	18
Ilustración 4 , Show IP Route en R2	19
Ilustración 5 , Show IP Route en R3	20
Ilustración 6 , Show IP Route en R3	21
Ilustración 7 , Show IP Route en R4	21
Ilustración 8 , Show IP Route R3	23
Ilustración 9 , Show IP Route R4	23
Ilustración 10 , Escenario Switch	24
Ilustración 11 , Comando show VTP status en SW-AA Client.....	25
Ilustración 12 , Comando show VTP status en SW-BB Server	26
Ilustración 13 , Comando show VTP status en SW-CC Client	26
Ilustración 14 , Verificación del puerto en SW-AA.....	27
Ilustración 15 , Verificación de la interfaz en SW-AA	27
Ilustración 16 , Verificación del puerto en SW-BB.....	27
Ilustración 17 , Verificación de la interfaz en SW-BB	28
Ilustración 18 , Comando show interface trunk en SW-AA.....	28
Ilustración 19 , Mode trunk en switchport SW-AA	29
Ilustración 20 , Mode trunk en SW-CC.....	29
Ilustración 21 , Comando show interface trunk en switchport SW-CC	29
Ilustración 22 , Mode Trunk en SW-CC.....	30
Ilustración 23 , Mode Trunk en SW-BB	30
Ilustración 24 , Show vlan brief en SW-AA.....	32
Ilustración 25 , Show vlan brief en SW-BB.....	32
Ilustración 26 , Configuración IP en PC 1.....	35
Ilustración 27 , Configuración IP en PC2.....	35
Ilustración 28 , Configuración IP en PC3.....	36

Ilustración 29 , Configuración IP en PC4.....	36
Ilustración 30 , Configuración IP en PC5.....	36
Ilustración 31, Configuración IP en PC6	37
Ilustración 32 , Configuración IP en PC7.....	37
Ilustración 33 , Configuración IP en PC8.....	37
Ilustración 34 , Configuración IP en PC9.....	38
Ilustración 35 , Ping desde el PC1 a los otros 8 PC	39
Ilustración 36 , Ping desde el PC2 a los otros 8 PC.....	40
Ilustración 37 , Ping desde el PC3 a los otros 8 PC	40
Ilustración 38 , Ping desde el SW-AA a los otros Switch.....	41
Ilustración 39 , Ping desde el SW-BB a los otros Switch.....	41
Ilustración 40 , Ping desde el SW-CC a los otros Switch	41
Ilustración 41 , Ping desde SW-AA a los 9 PCs	42
Ilustración 42 , Ping desde SW-BB a los 9 PCs	43
Ilustración 43 , Ping desde SW-CC a los 9 PCs.....	43

GLOSARIO

GNS3: GNS3 es un simulador gráfico de red lanzado en 2008, que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos, permitiendo la combinación de dispositivos tanto reales como virtuales.

CCNP: (Cisco Certified Network Professional) es el nivel intermedio de certificación de la compañía. Para obtener esta certificación, se han de superar varios exámenes, clasificados según la empresa en 3 módulos.

VLAN: acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.

Protocolos de enrutamiento: especifica cómo los enrutadores se comunican entre sí para distribuir información que les permite seleccionar rutas entre dos nodos en una red informática.

BGP: El protocolo de puerta de enlace de frontera o BGP es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos.

Switching: Se utiliza para conectar varios dispositivos a través de la misma red dentro de una misma oficina o edificio. Se utiliza el switching cuando queremos transportar datos de un sitio a otro con la capacidad de tener menos colisiones posibles dentro de la misma red.

RESUMEN

El desarrollo de este documento aplica fundamentos en la solución de problemas en la red bajo la supervisión de Cisco, desarrollando las actividades del programa de CCNP, a través de protocolos de enrutamiento y configuraciones de aprendizaje en los dispositivos de interconexión.

Por lo tanto, se necesita tener conocimientos de redes, básicamente haber realizado el curso de Cisco en el programa de CCNA.

Palabras Clave: Cisco, Redes, Protocolos, CCNP.

ABSTRACT

The development of this document applies foundations in the solution of problems in the network under the supervision of Cisco, developing the activities of the CCNP program, through routing protocols and learning configurations in the interconnection devices.

Therefore, you need to have networking knowledge, having taken the Cisco course in the CCNA program.

Keywords: Cisco, Networks, Protocols, CCNP.

INTRODUCCIÓN

Hoy en día la telecomunicación es muy esencial para el mundo, para la actualización de información, comunicación, negocios entre otras cosas, pero para garantizar una buena conexión se deben de tener buenas prácticas y a través de este Diplomado de Cisco en CCNP se adquirieron conocimientos y habilidades necesarias para analizar y configurar los dispositivos según las necesidades.

En este trabajo se desarrollan dos escenarios el cual permite aplicar los conocimientos a través del curso, estos ejercicios se desarrollaron con la aplicación de GNS3 y una maquina virtual en VMware Workstation de GNS3VM.

También todas las capturas de pantallas son propias del autor del documento para mostrar la evidencia de los resultados de los protocolos de configuración en todos los dispositivos.

DESARROLLO

Escenario 1

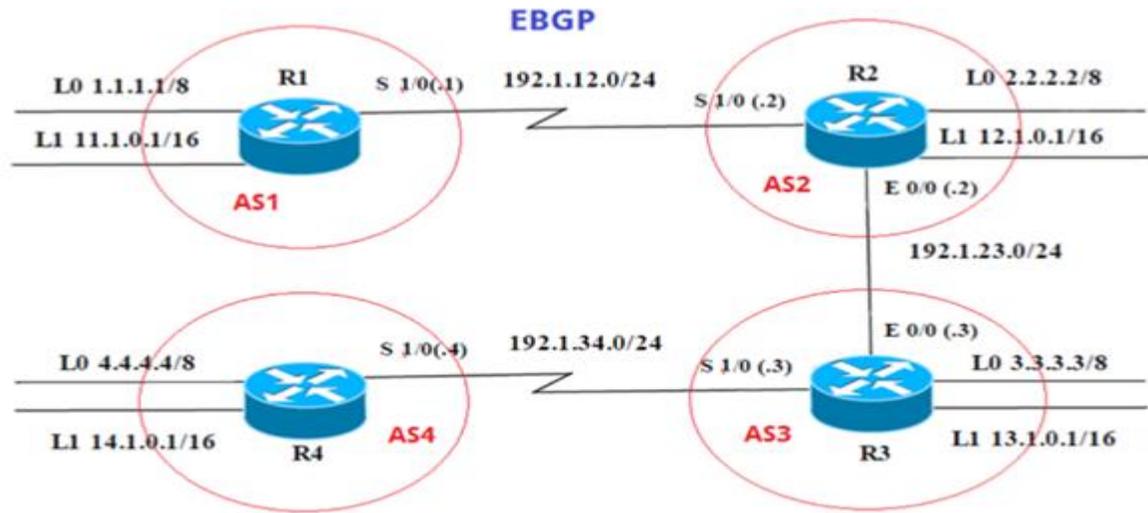


Ilustración 1, Escenario EBGP

Información para configuración de los Routers

R1		
Interfaz	Dirección IP	Máscara
Lookback 0	1.1.1.1	255.0.0.0
Lookback 1	11.1.0.1	255.255.0.0
S 1/0	192.1.12.1	255.255.255.0

Tabla 1, Configuración Router R1

R2		
Interfaz	Dirección IP	Máscara
Lookback 0	2.2.2.2	255.0.0.0
Lookback 1	12.1.0.1	255.255.0.0
S 1/0	192.1.12.2	255.255.255.0
GE 0/0	192.1.23.2	255.255.255.0

Tabla 2, Configuración Router R2

R3		
Interfaz	Dirección IP	Máscara
Lookback 0	3.3.3.3	255.0.0.0
Lookback 1	13.1.0.1	255.255.0.0
S 1/0	192.1.34.3	255.255.255.0
GE 0/0	192.1.23.3	255.255.255.0

Tabla 3, Configuración Router R3

R4		
Interfaz	Dirección IP	Máscara
Lookback 0	4.4.4.4	255.0.0.0
Lookback 1	14.1.0.1	255.255.0.0
S 1/0	192.1.34.4	255.255.255.0

Tabla 4, Configuración Router R4

Primero realizaremos la configuración de las interfaces de los dispositivos para lograr unas buenas prácticas y se maneja una velocidad de sincronización de 56000 ya que este valor es habitual en los laboratorios de redes.

Configuración de interfaces R1.

R1(config)#int loopback0

R1(config-if)#ip add 1.1.1.1 255.0.0.0

R1(config-if)#exit

R1(config)#int loopback1

R1(config-if)#ip add 11.1.0.1 255.255.0.0

R1(config-if)#exit

R1(config)#int s1/0

R1(config-if)#ip add 192.1.12.1 255.255.255.0

R1(config-if)#clock rate 56000

R1(config-if)#no shut

R1(config-if)#exit

Configuración de interfaces R2

R2(config)#int loopback0

R2(config-if)#ip add 2.2.2.2 255.0.0.0

R2(config-if)#exit

R2(config)#int loopback1

R2(config-if)#ip add 12.1.0.1 255.255.0.0

R2(config-if)#exit

R2(config)#int s1/0

R2(config-if)#ip add 192.1.12.2 255.255.255.0

R2(config-if)#clock rate 56000

R2(config-if)#no shut

R2(config-if)#exit

R2(config)#int gigabitEthernet0/0

R2(config-if)#ip add 192.1.23.2 255.255.255.0

R2(config-if)#no shut

R2(config-if)#exit

Configuración de interfaces R3

R3(config)#int loopback0

R3(config-if)#ip add 3.3.3.3 255.0.0.0

R3(config-if)#exit

R3(config)#int loopback1

R3(config-if)#ip add 13.1.0.1 255.255.0.0

R3(config-if)#exit

R3(config)#int s1/0

R3(config-if)#ip add 192.1.34.3 255.255.255.0

R3(config-if)#clock rate 56000

R3(config-if)#no shut

```
R3(config-if)#exit
R3(config)#int gigabitEthernet0/0
R3(config-if)#ip add 192.1.23.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
```

Configuración de interfaces R4

```
R4(config)#int loopback0
R4(config-if)#ip add 4.4.4.4 255.0.0.0
R4(config-if)#exit
R4(config)#int loopback1
R4(config-if)#ip add 14.1.0.1 255.255.0.0
R4(config-if)#exit
R4(config)#int s1/0
R4(config-if)#ip add 192.1.34.4 255.255.255.0
R4(config-if)#clock rate 56000
R4(config-if)#no shut
R4(config-if)#exit
```

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

Se configura el protocolo BGP en los dispositivos R1 y R2, se describen las rutas de loopback y por último se establece la red y el direccionamiento del puerto de R2.

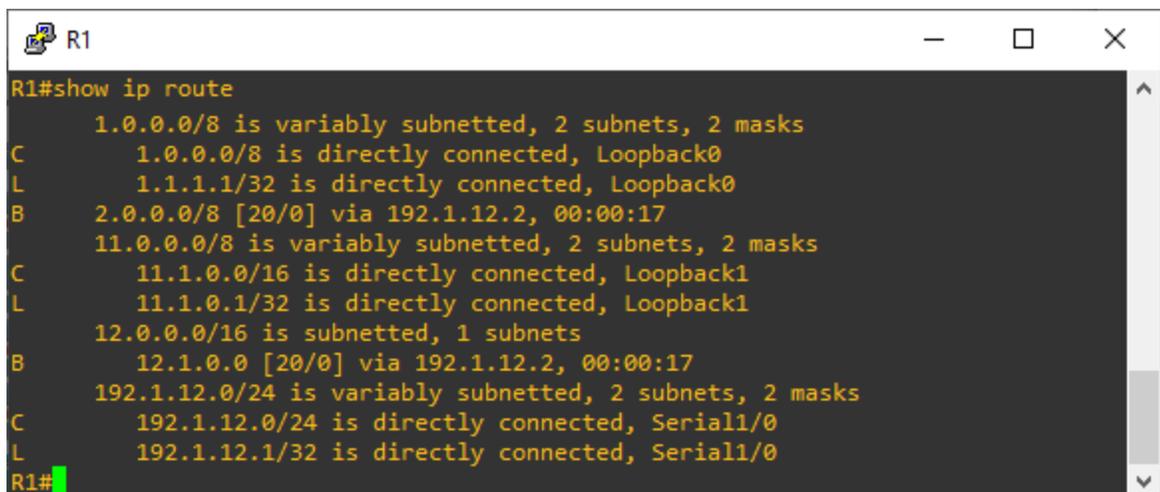
Configuración BGP en R1

```
R1(config)#router bgp 1
R1(config-router)#bgp router-id 11.11.11.11
```

```
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
```

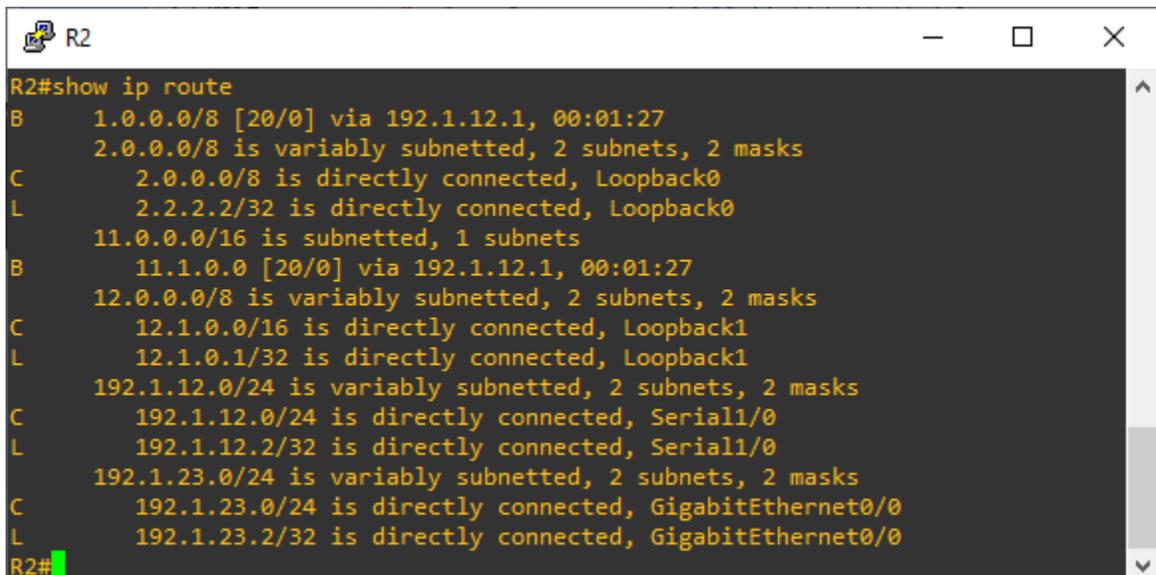
Configuración BGP en R2

```
R2(config)#router bgp 2
R2(config-router)#bgp router-id 22.22.22.22
R2(config-router)#network 2.0.0.0 mask 255.0.0.0
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
R2(config-router)#network 192.1.12.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#exit
```



```
R1#show ip route
 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, 00:00:17
 11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    11.1.0.0/16 is directly connected, Loopback1
L    11.1.0.1/32 is directly connected, Loopback1
 12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 192.1.12.2, 00:00:17
 192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.12.0/24 is directly connected, Serial1/0
L    192.1.12.1/32 is directly connected, Serial1/0
R1#
```

Ilustración 2, Show IP Route en R1



```
R2#show ip route
B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:01:27
     2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    2.0.0.0/8 is directly connected, Loopback0
L    2.2.2.2/32 is directly connected, Loopback0
     11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 192.1.12.1, 00:01:27
     12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    12.1.0.0/16 is directly connected, Loopback1
L    12.1.0.1/32 is directly connected, Loopback1
     192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.12.0/24 is directly connected, Serial1/0
L    192.1.12.2/32 is directly connected, Serial1/0
     192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, GigabitEthernet0/0
L    192.1.23.2/32 is directly connected, GigabitEthernet0/0
R2#
```

Ilustración 3, Show IP Route en R2

2. Configure una relación de vecino BGP entre R2 y R3, R2 ya debería de estar configurado en AS2 y R3 debería estar en AS3. Anuncie las direcciones Lookback 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.

De acuerdo a la ilustración 3 el dispositivo R2 se encuentra en la configuración AS2, por lo tanto, en este paso vamos a agregar la configuración para comunicarnos con AS3.

Configuración de BGP en R2

R2(config)#router bgp 2

R2(config-router)#neighbor 192.1.23.3 remote-as 3

R2(config-router)#exit

Configuración de BGP en R3

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

```
R3(config-router)#bgp router-id 33.33.33.33
```

```
R3(config-router)#network 3.0.0.0 mask 255.0.0.0
```

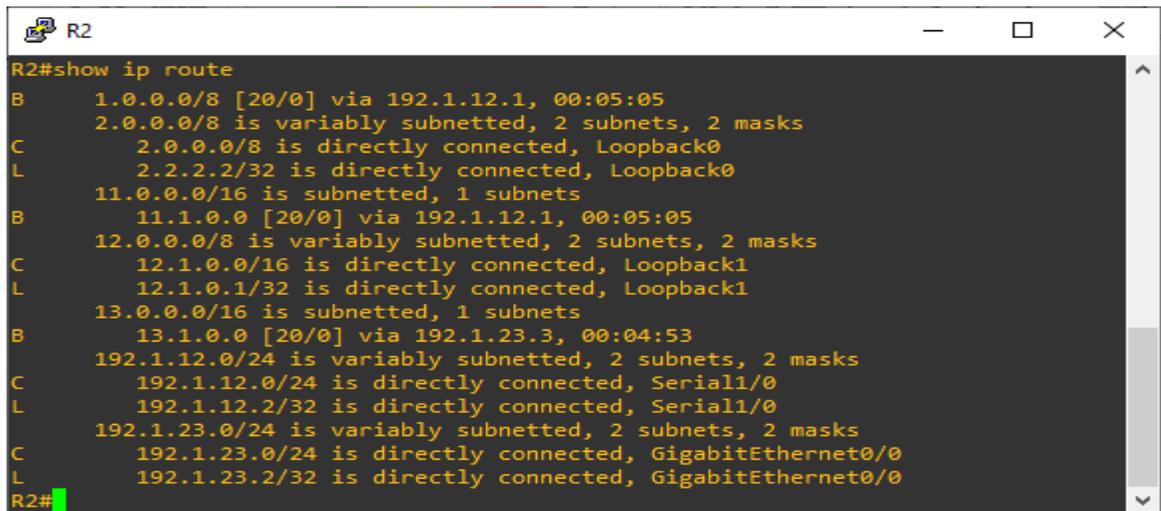
```
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
```

```
R3(config-router)#network 192.1.23.0 mask 255.255.255.0
```

```
R3(config-router)#neighbor 192.1.23.2 remote-as 2
```

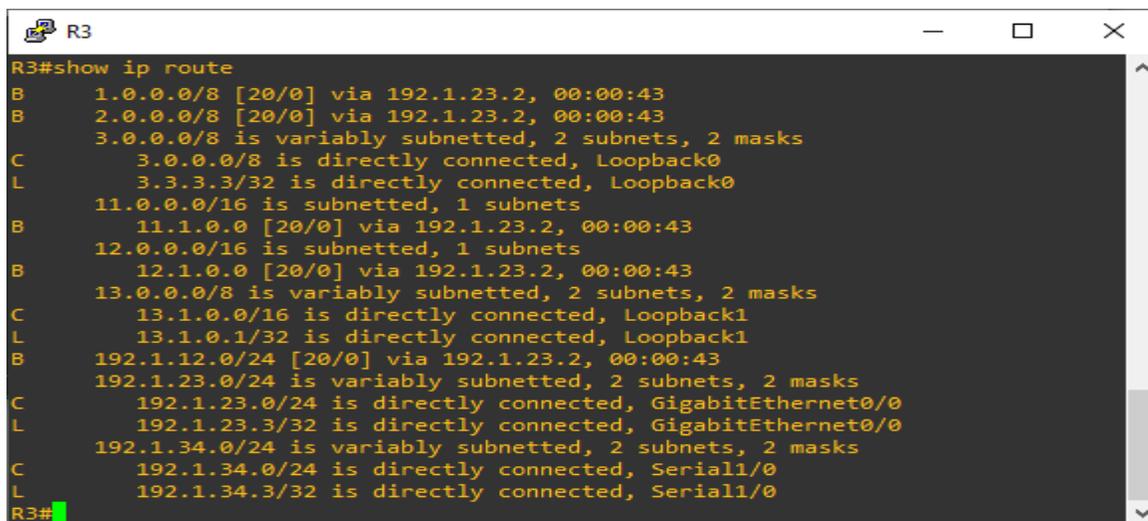
```
R3(config-router)#exit
```

Se observa todo el enrutamiento de los dispositivos R2 y R3



```
R2
R2#show ip route
B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:05:05
     2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    2.0.0.0/8 is directly connected, Loopback0
L    2.2.2.2/32 is directly connected, Loopback0
     11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 192.1.12.1, 00:05:05
     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
     13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0 [20/0] via 192.1.23.3, 00:04:53
     192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.12.0/24 is directly connected, Serial1/0
L    192.1.12.2/32 is directly connected, Serial1/0
     192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, GigabitEthernet0/0
L    192.1.23.2/32 is directly connected, GigabitEthernet0/0
R2#
```

Ilustración 4, Show IP Route en R2



```
R3#show ip route
B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:00:43
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:00:43
    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
    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 192.1.23.2, 00:00:43
    12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 192.1.23.2, 00:00:43
    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, 00:00:43
    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, GigabitEthernet0/0
L    192.1.23.3/32 is directly connected, GigabitEthernet0/0
    192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial1/0
L    192.1.34.3/32 is directly connected, Serial1/0
R3#
```

Ilustración 5, Show IP Route en R3

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

Por último, se configura el BGP en los dispositivos R3 y R4 para su respectiva comunicación.

Configuración BGP en R3

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

```
R3(config-router)#neighbor 192.1.34.4 remote-as 4
```

```
R3(config-router)#exit
```

Configuración BGP en R4

```
R4(config)#router bgp 4
```

```
R4(config-router)#bgp router-id 44.44.44.44
```

```
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

```

Tabla de enrutamiento de los dispositivos R3 y R4 para su comunicación.

```

R3#show ip route
B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:04:16
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:04:16
B    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
B    4.0.0.0/8 [20/0] via 192.1.34.4, 00:00:50
B    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 192.1.23.2, 00:04:16
B    12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 192.1.23.2, 00:04:16
B    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    14.0.0.0/16 is subnetted, 1 subnets
B    14.1.0.0 [20/0] via 192.1.34.4, 00:00:50
B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:04:16
B    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, GigabitEthernet0/0
L    192.1.23.3/32 is directly connected, GigabitEthernet0/0
B    192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial1/0
L    192.1.34.3/32 is directly connected, Serial1/0
R3#

```

Ilustración 6, Show IP Route en R3

```

R4#show ip route
B    1.0.0.0/8 [20/0] via 192.1.34.3, 00:03:01
B    2.0.0.0/8 [20/0] via 192.1.34.3, 00:03:01
B    3.0.0.0/8 [20/0] via 192.1.34.3, 00:03:01
B    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
B    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 192.1.34.3, 00:03:01
B    12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 192.1.34.3, 00:03:01
B    13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0 [20/0] via 192.1.34.3, 00:03:01
B    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
B    192.1.12.0/24 [20/0] via 192.1.34.3, 00:03:01
B    192.1.23.0/24 [20/0] via 192.1.34.3, 00:03:01
B    192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial1/0
L    192.1.34.4/32 is directly connected, Serial1/0
R4#

```

Ilustración 7, Show IP Route en R4

Se establecen las relaciones de adyacencia por medio de las direcciones lookback para crear rutas estáticas y alcanzar la loopback 0 del dispositivo vecino.

A continuación, se configura la ruta estática para la conexión con el dispositivo vecino, no se anuncian las interfaces S1/0 y loopback 0, se establece conexión por la loopback 0 por el dominio 4 y por ultimo solo los clientes registrados se pueden comunicar por la ruta estática.

Configuración de ruta estática y BGP en R3

```
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 loopback 0
```

```
R3(config-router)#neighbor 4.4.4.4 ebgp-multihop
```

```
R3(config-router)#exit
```

Configuración de ruta estática y BGP en R4

```
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 3
```

```
R4(config-router)#neighbor 3.3.3.3 update-source loopback 0
```

```
R4(config-router)#neighbor 3.3.3.3 ebgp-multihop
```

Tabla de enrutamiento de los dispositivos R3 y R4 para su comunicación.

```
R3#show ip route
B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:10:52
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:10:52
S    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
    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 192.1.23.2, 00:10:52
    12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 192.1.23.2, 00:10:52
    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
    14.0.0.0/16 is subnetted, 1 subnets
B    14.1.0.0 [20/0] via 4.4.4.4, 00:01:26
B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:10:52
    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, GigabitEthernet0/0
L    192.1.23.3/32 is directly connected, GigabitEthernet0/0
    192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial1/0
L    192.1.34.3/32 is directly connected, Serial1/0
R3#
```

Ilustración 8, Show IP Route R3

```
R4#show ip route
B    1.0.0.0/8 [20/0] via 3.3.3.3, 00:02:26
B    2.0.0.0/8 [20/0] via 3.3.3.3, 00:02:26
S    3.0.0.0/8 [1/0] via 192.1.34.3
    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
    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 3.3.3.3, 00:02:26
    12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 3.3.3.3, 00:02:26
    13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0 [20/0] via 3.3.3.3, 00:02:26
    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
B    192.1.12.0/24 [20/0] via 3.3.3.3, 00:02:26
B    192.1.23.0/24 [20/0] via 3.3.3.3, 00:02:26
    192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial1/0
L    192.1.34.4/32 is directly connected, Serial1/0
R4#
```

Ilustración 9, Show IP Route R4

Escenario 2

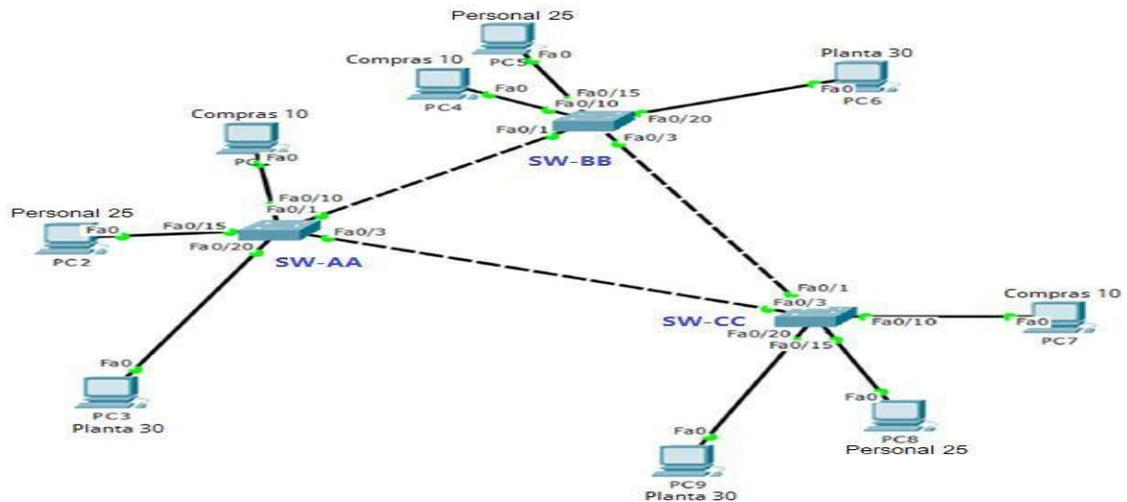


Ilustración 10, Escenario Switch

A. Configurar VTP 1.

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.

Para este ejercicio trabajaremos con la versión 2 de VTP para poder usar rangos en las VLANs.

Configuración de VTP versión 2 en SW-AA

```
SW-AA(config)#vtp version 2
```

```
SW-AA(config)#vtp mode client
```

```
SW-AA(config)#vtp domain CCNP
```

```
SW-AA(config)#vtp password cisco
```

Configuración de VTP versión 2 en SW-BB

```
SW-BB(config)#vtp version 2
```

```
SW-BB(config)#vtp mode server
```

```
SW-BB(config)#vtp domain CCNP
```

```
SW-BB(config)#vtp password cisco
```

Configuración de VTP versión 2 en SW-CC

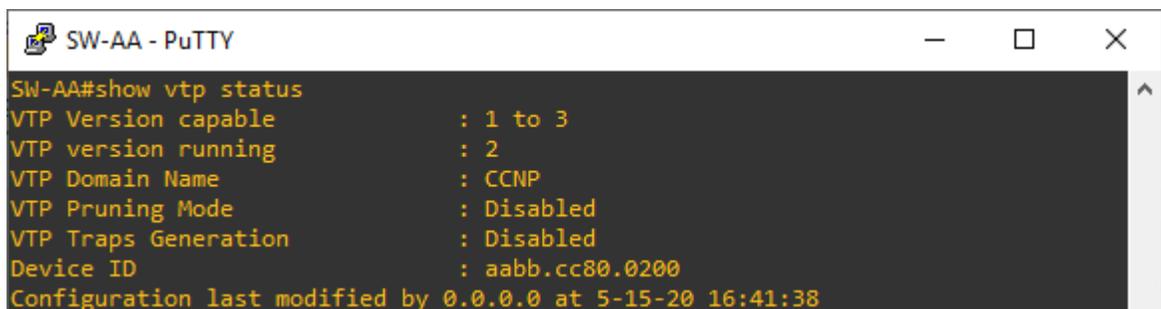
```
SW-CC(config)#vtp version 2
```

```
SW-CC(config)#vtp mode client
```

```
SW-CC(config)#vtp domain CCNP
```

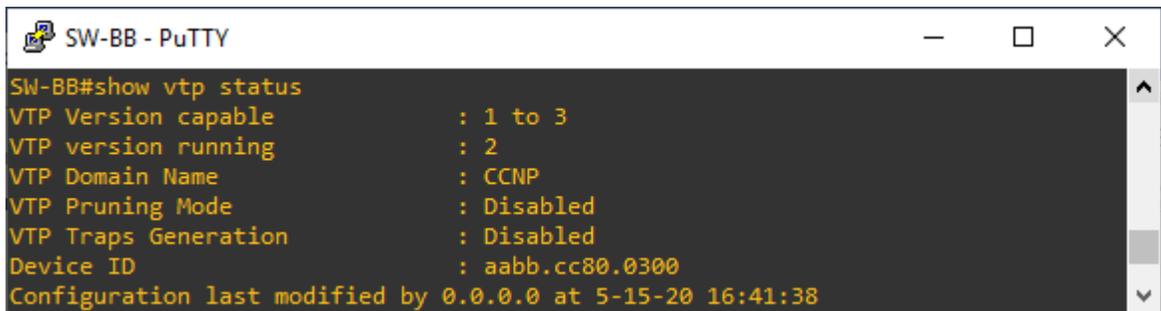
```
SW-CC(config)#vtp password cisco
```

2. Verifique las configuraciones mediante el comando show vtp status



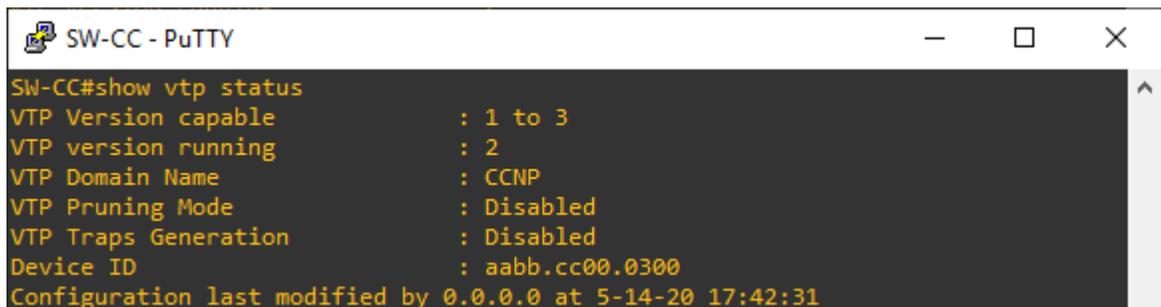
```
SW-AA - PuTTY
SW-AA#show vtp status
VTP Version capable      : 1 to 3
VTP version running     : 2
VTP Domain Name         : CCNP
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID               : aabb.cc80.0200
Configuration last modified by 0.0.0.0 at 5-15-20 16:41:38
```

Ilustración 11, Comando show VTP status en SW-AA Client



```
SW-BB#show vtp status
VTP Version capable      : 1 to 3
VTP version running      : 2
VTP Domain Name          : CCNP
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : aabb.cc80.0300
Configuration last modified by 0.0.0.0 at 5-15-20 16:41:38
```

Ilustración 12, Comando show VTP status en SW-BB Server



```
SW-CC#show vtp status
VTP Version capable      : 1 to 3
VTP version running      : 2
VTP Domain Name          : CCNP
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : aabb.cc00.0300
Configuration last modified by 0.0.0.0 at 5-14-20 17:42:31
```

Ilustración 13, Comando show VTP status en SW-CC Client

B. Configurar DTP (Dynamic Trunking Protocol)

3. 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 puerto Eth0/0 como dynamic desirable en el dispositivo SW-AA para lograr un modo troncal y el extremo opere en modo trunk automáticamente.

```
SW-AA(config)#int eth0/0
```

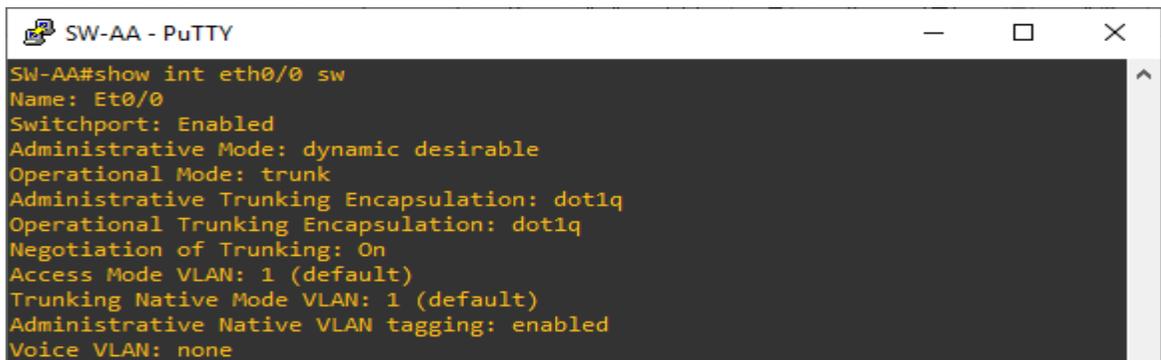
```
SW-AA(config-if)#sw trunk encapsulation dot1q
```

```
SW-AA(config-if)#sw mo dynamic desirable
```

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

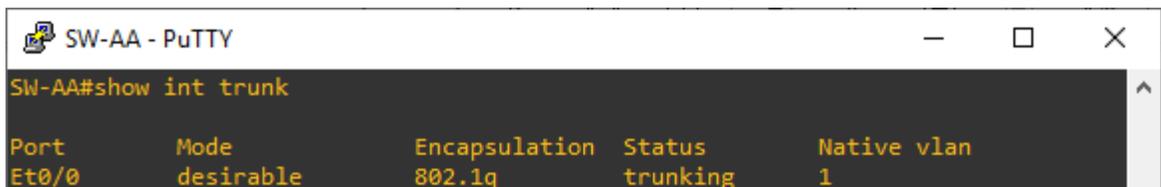
4. Verifique el enlace "trunk" entre SW-AA y SW-BB usando el comando show interfaces trunk.

Con la verificación de la configuración anterior se puede observar el modo Dynamic Desirable activado y funcionando en los dispositivos SW-AA y SW-BB.



```
SW-AA#show int eth0/0 sw
Name: Et0/0
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

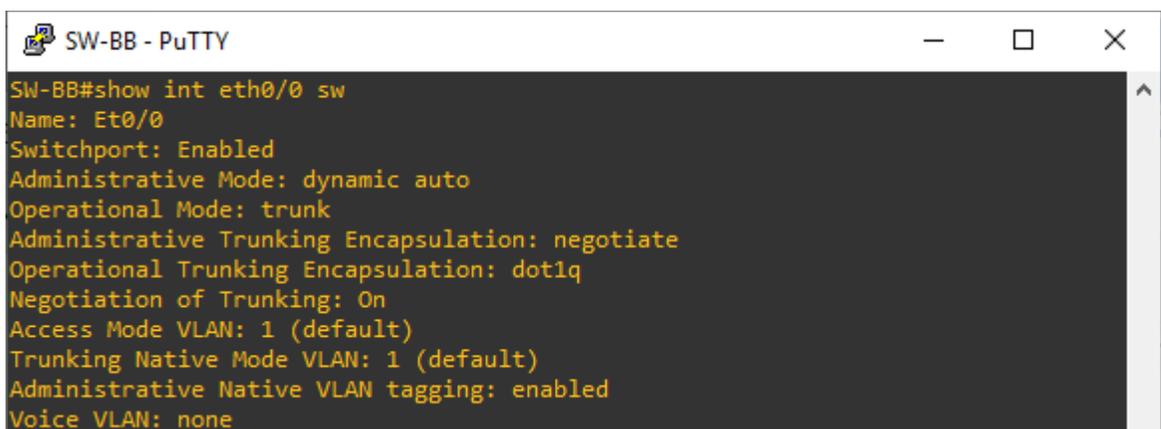
Ilustración 14, Verificación del puerto en SW-AA



```
SW-AA#show int trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Et0/0	desirable	802.1q	trunking	1

Ilustración 15, Verificación de la interfaz en SW-AA



```
SW-BB#show int eth0/0 sw
Name: Et0/0
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

Ilustración 16, Verificación del puerto en SW-BB

```
SW-BB#show inter trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Et0/0	auto	n-802.1q	trunking	1

Ilustración 17, Verificación de la interfaz en SW-BB

- Entre SW-AA y SW-BB configure un enlace "trunk" estático utilizando el comando switchport mode trunk en la interfaz Eth0/0 de SW-AA

Configuración modo Trunk

SW-AA(config)#int eth0/2

SW-AA(config-if)#sw trunk encapsulation dot1q

SW-AA(config-if)#sw mo trunk

SW-AA(config-if)#exit

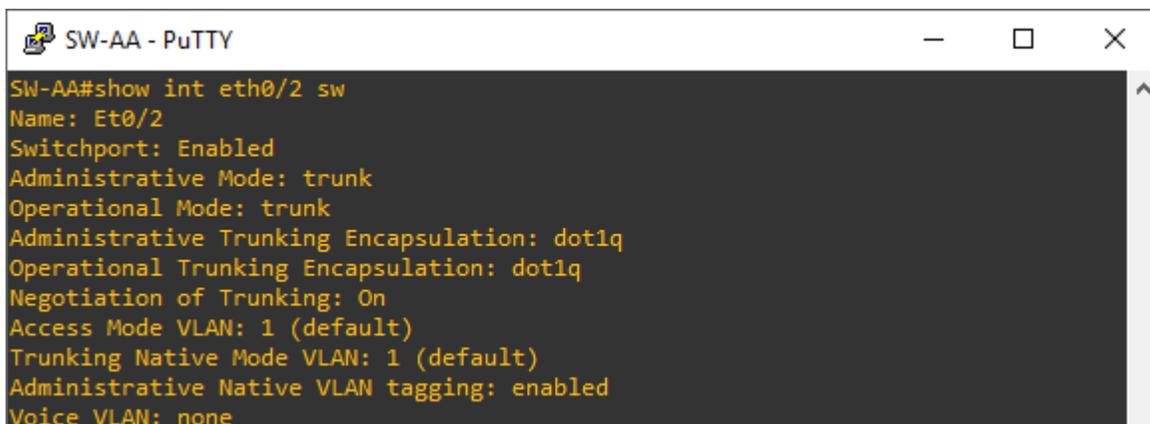
- Verifique el enlace "trunk" el comando show interfaces trunk en SW-AA.

Con la verificación de la configuración anterior se puede observar el modo Trunk activado y funcionando en el dispositivo SW-AA.

```
SW-AA#show int trunk
```

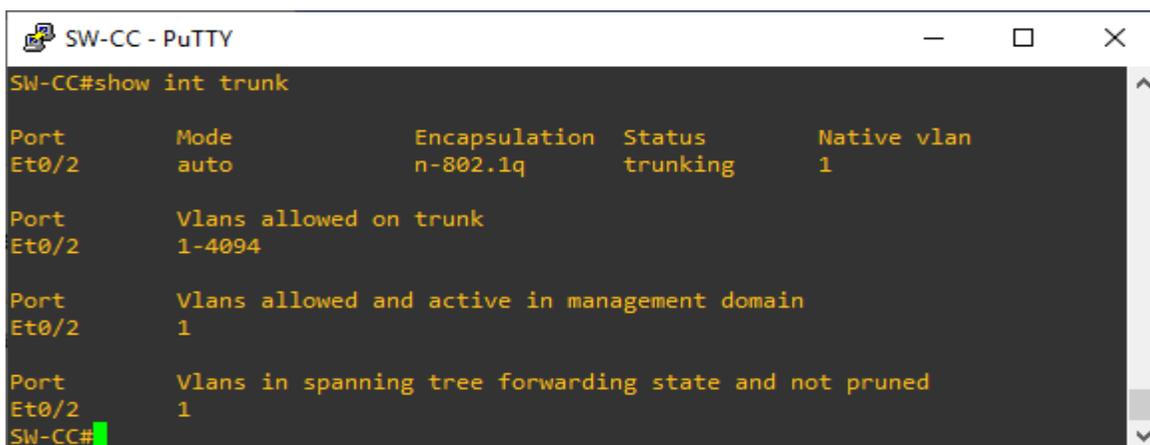
Port	Mode	Encapsulation	Status	Native vlan
Et0/0	desirable	802.1q	trunking	1
Et0/2	on	802.1q	trunking	1

Ilustración 18, Comando show interface trunk en SW-AA



```
SW-AA#show int eth0/2 sw
Name: Et0/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

Ilustración 19, Mode trunk en switchport SW-AA



```
SW-CC#show int trunk

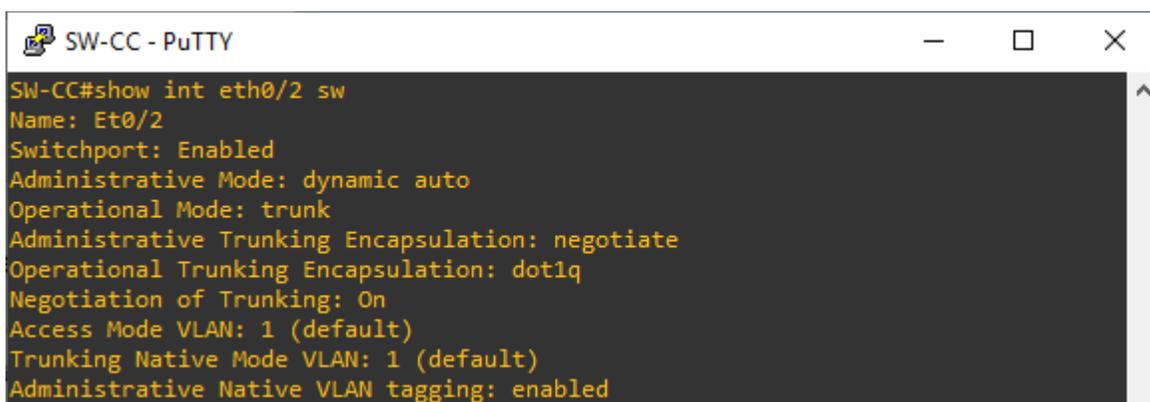
Port      Mode           Encapsulation  Status        Native vlan
Et0/2     auto           n-802.1q       trunking      1

Port      Vlans allowed on trunk
Et0/2     1-4094

Port      Vlans allowed and active in management domain
Et0/2     1

Port      Vlans in spanning tree forwarding state and not pruned
Et0/2     1
SW-CC#
```

Ilustración 20, Mode trunk en SW-CC



```
SW-CC#show int eth0/2 sw
Name: Et0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
```

Ilustración 21, Comando show interface trunk en switchport SW-CC

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

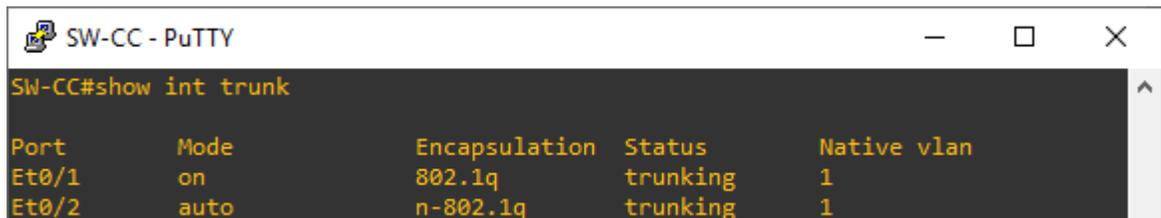
Para habilitar el modo troncal primero se debe habilitar el protocolo de encapsulación dot1q y este estado permanecerá permanente.

SW-CC(config)#int eth0/1

SW-CC(config-if)#sw trunk encapsulation dot1q

SW-CC(config-if)#sw mo trunk

SW-CC(config-if)#exit



```
SW-CC#show int trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Et0/1	on	802.1q	trunking	1
Et0/2	auto	n-802.1q	trunking	1

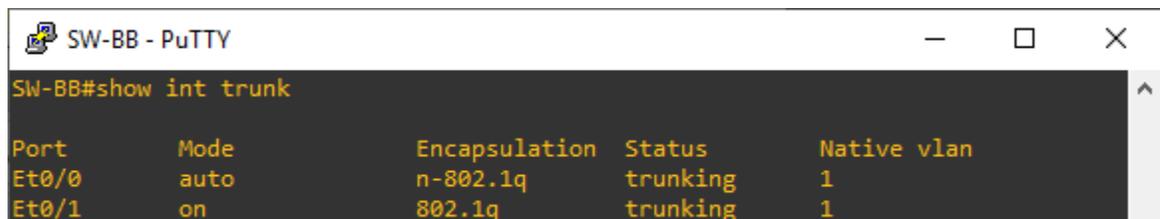
Ilustración 22, Mode Trunk en SW-CC

SW-BB(config)#int eth0/1

SW-BB(config-if)#sw trunk encapsulation dot1q

SW-BB(config-if)#sw mo trunk

SW-BB(config-if)#exit



```
SW-BB#show int trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Et0/0	auto	n-802.1q	trunking	1
Et0/1	on	802.1q	trunking	1

Ilustración 23, Mode Trunk en SW-BB

C. Agregar VLANs y asignar puertos.

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

Debido a que el dispositivo SW-AA está configurado en modo cliente, no permitirá crear la VLAN 10, es por eso que para poder crearla se permitieron los permisos adecuados y luego asignarla.

Configuración de VLAN 10 en SW-AA

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

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

Configuración de VLANs en SW-BB

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

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

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

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

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

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

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

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

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

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

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

9. Verifique que las VLANs han sido agregadas correctamente.

```

SW-AA - PuTTY
SW-AA#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Et0/1, Et0/3, Et1/0, Et1/1
                    Et1/2, Et1/3, Et2/0, Et2/1
                    Et2/2, Et2/3, Et3/0, Et3/1
                    Et3/2, Et3/3

10   VLAN0010              active
1002 fddi-default         act/unsup
1003 trcrf-default      act/unsup
1004 fddinet-default    act/unsup
1005 trbrf-default     act/unsup
SW-AA#
  
```

Ilustración 24, Show vlan brief en SW-AA

```

SW-BB - PuTTY
SW-BB#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Et0/2, Et0/3, Et1/0, Et1/1
                    Et1/2, Et1/3, Et2/0, Et2/1
                    Et2/2, Et2/3, Et3/0, Et3/1
                    Et3/2, Et3/3

10   Compras                active
25   Personal              active
30   Planta                active
99   Admon                  active
1002 fddi-default         act/unsup
1003 trcrf-default      act/unsup
1004 fddinet-default    act/unsup
1005 trbrf-default     act/unsup
SW-BB#
  
```

Ilustración 25, Show vlan brief en SW-BB

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

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

Tabla 5, Configuración de Puertos a las VLANs y direcciones IP

11. Configure el puerto Eth1/0 en modo de acceso para SW-AA, SW-BB y SW-CC y asígnelo a la VLAN 10.

Configuración del puerto en SW-AA

```
SW-AA(config)#int eth1/0
```

```
SW-AA(config-if)#sw mo access
```

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

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

Configuración del puerto en SW-BB

```
SW-BB(config)#int eth1/0
```

```
SW-BB(config-if)#sw mo access
```

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

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

Configuración del puerto en SW-CC

```
SW-CC(config)#int eth1/0
```

```
SW-CC(config-if)#sw mo access
```

```
SW-CC(config-if)#sw access vlan 10
```

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

12. 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.

Configuración de los puertos en SW-AA

SW-AA(config)#int eth1/1

SW-AA(config-if)#sw mo access

SW-AA(config-if)#sw access vlan 25

SW-AA(config-if)#exit

SW-AA(config)#int eth1/2

SW-AA(config-if)#sw mo access

SW-AA(config-if)#sw access vlan 30

SW-AA(config-if)#exit

Configuración de los puertos en SW-BB

SW-BB(config)#int eth1/1

SW-BB(config-if)#sw mo access

SW-BB(config-if)#sw access vlan 25

SW-BB(config-if)#exit

SW-BB(config)#int eth1/2

SW-BB(config-if)#sw mo access

SW-BB(config-if)#sw access vlan 30

SW-BB(config-if)#exit

Configuración de los puertos en SW-CC

SW-CC(config)#int eth1/1

SW-CC(config-if)#sw mo access

SW-CC(config-if)#sw access vlan 25

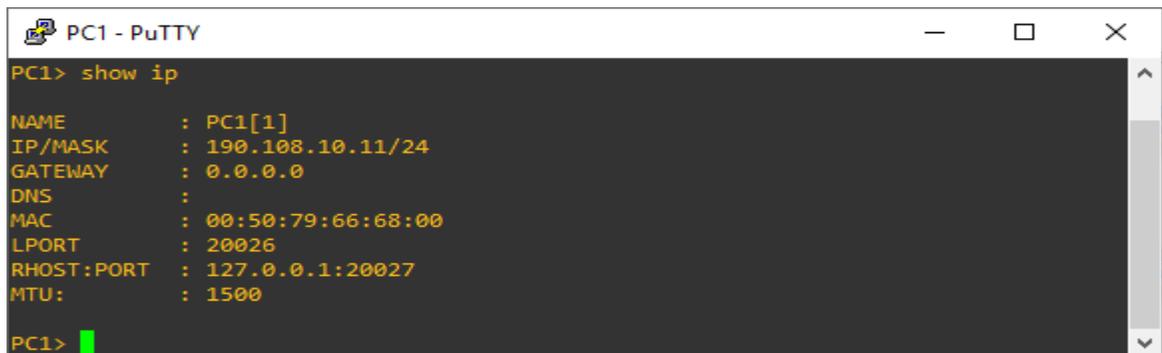
SW-CC(config-if)#exit

SW-CC(config)#int eth1/2

SW-CC(config-if)#sw mo access

SW-CC(config-if)#sw access vlan 30

SW-CC(config-if)#exit



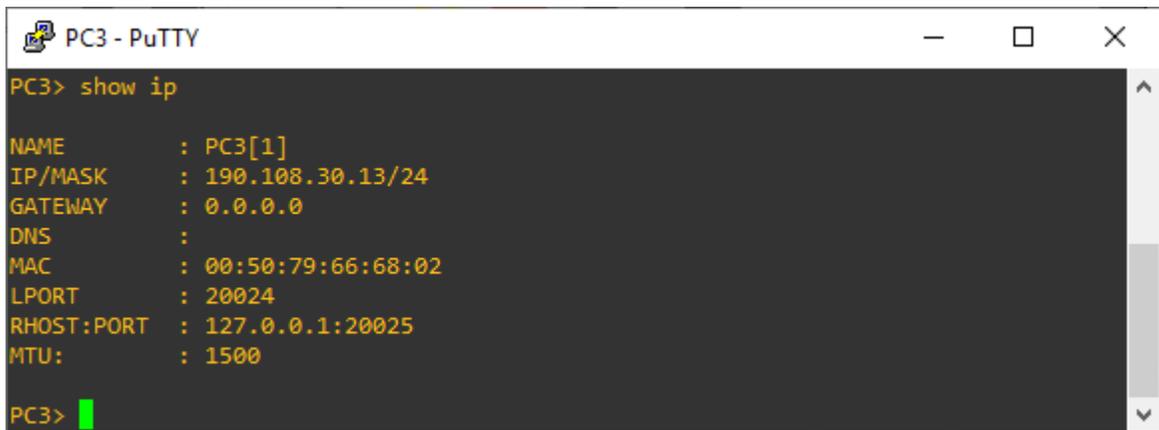
```
PC1 - PuTTY
PC1> show ip
NAME       : PC1[1]
IP/MASK    : 190.108.10.11/24
GATEWAY    : 0.0.0.0
DNS        :
MAC        : 00:50:79:66:68:00
LPORT     : 20026
RHOST:PORT : 127.0.0.1:20027
MTU        : 1500
PC1>
```

Ilustración 26, Configuración IP en PC 1



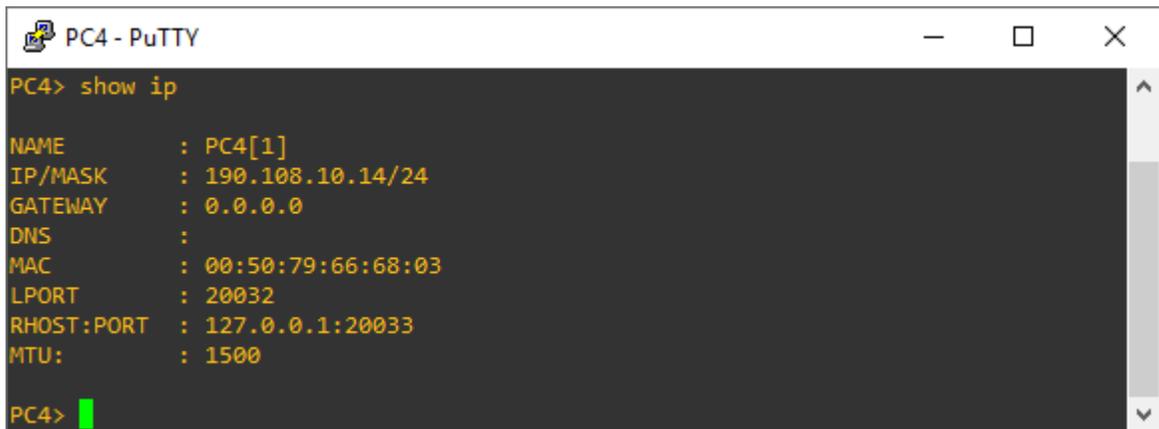
```
PC2 - PuTTY
PC2> show ip
NAME       : PC2[1]
IP/MASK    : 190.108.20.12/24
GATEWAY    : 0.0.0.0
DNS        :
MAC        : 00:50:79:66:68:01
LPORT     : 20028
RHOST:PORT : 127.0.0.1:20029
MTU        : 1500
PC2>
```

Ilustración 27, Configuración IP en PC2



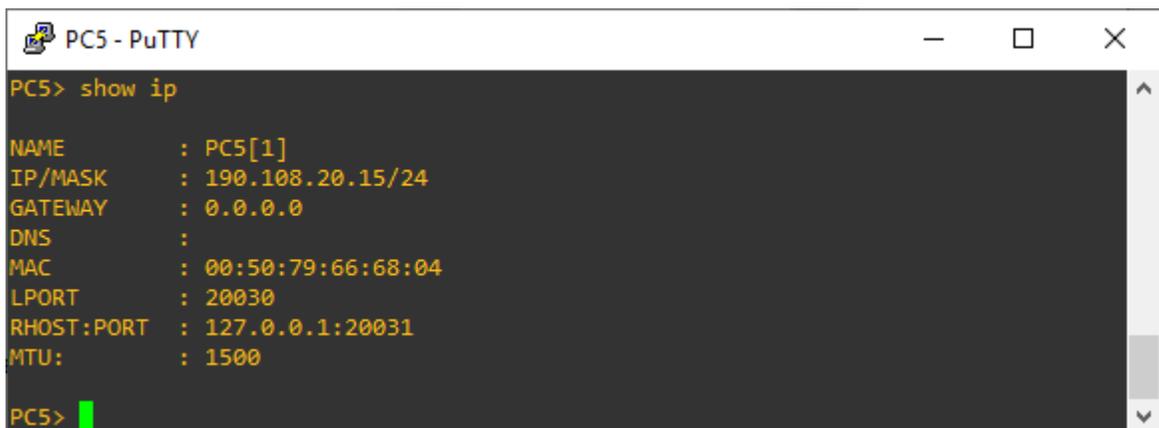
```
PC3 - PuTTY
PC3> show ip
NAME       : PC3[1]
IP/MASK    : 190.108.30.13/24
GATEWAY    : 0.0.0.0
DNS        :
MAC        : 00:50:79:66:68:02
LPORT     : 20024
RHOST:PORT : 127.0.0.1:20025
MTU        : 1500
PC3> █
```

Ilustración 28, Configuración IP en PC3



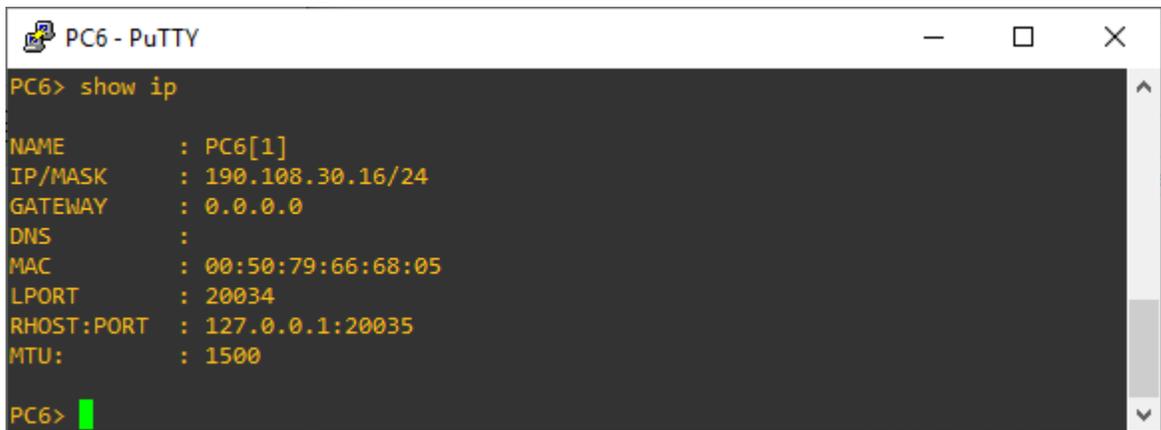
```
PC4 - PuTTY
PC4> show ip
NAME       : PC4[1]
IP/MASK    : 190.108.10.14/24
GATEWAY    : 0.0.0.0
DNS        :
MAC        : 00:50:79:66:68:03
LPORT     : 20032
RHOST:PORT : 127.0.0.1:20033
MTU        : 1500
PC4> █
```

Ilustración 29, Configuración IP en PC4



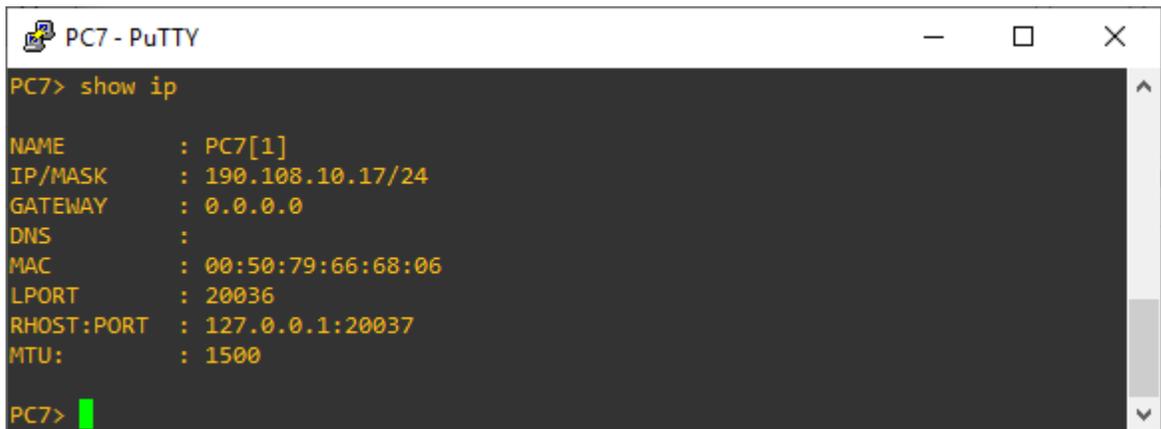
```
PC5 - PuTTY
PC5> show ip
NAME       : PC5[1]
IP/MASK    : 190.108.20.15/24
GATEWAY    : 0.0.0.0
DNS        :
MAC        : 00:50:79:66:68:04
LPORT     : 20030
RHOST:PORT : 127.0.0.1:20031
MTU        : 1500
PC5> █
```

Ilustración 30, Configuración IP en PC5



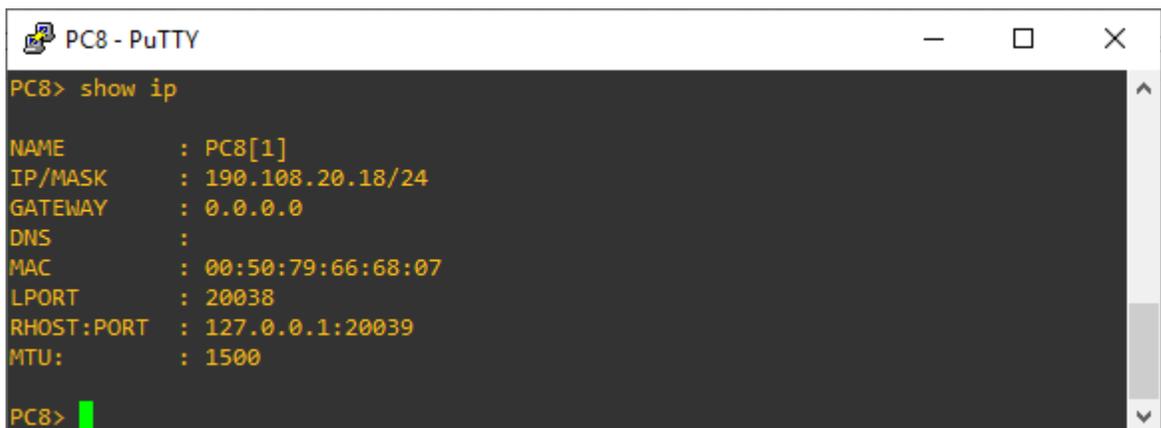
```
PC6 - PuTTY
PC6> show ip
NAME       : PC6[1]
IP/MASK    : 190.108.30.16/24
GATEWAY    : 0.0.0.0
DNS        :
MAC        : 00:50:79:66:68:05
LPORT     : 20034
RHOST:PORT : 127.0.0.1:20035
MTU       : 1500
PC6>
```

Ilustración 31, Configuración IP en PC6



```
PC7 - PuTTY
PC7> show ip
NAME       : PC7[1]
IP/MASK    : 190.108.10.17/24
GATEWAY    : 0.0.0.0
DNS        :
MAC        : 00:50:79:66:68:06
LPORT     : 20036
RHOST:PORT : 127.0.0.1:20037
MTU       : 1500
PC7>
```

Ilustración 32, Configuración IP en PC7



```
PC8 - PuTTY
PC8> show ip
NAME       : PC8[1]
IP/MASK    : 190.108.20.18/24
GATEWAY    : 0.0.0.0
DNS        :
MAC        : 00:50:79:66:68:07
LPORT     : 20038
RHOST:PORT : 127.0.0.1:20039
MTU       : 1500
PC8>
```

Ilustración 33, Configuración IP en PC8

```

PC9 - PuTTY
PC9> show ip

NAME       : PC9[1]
IP/MASK    : 190.108.30.19/24
GATEWAY    : 0.0.0.0
DNS        :
MAC        : 00:50:79:66:68:08
LPORT     : 20040
RHOST:PORT : 127.0.0.1:20041
MTU       : 1500

PC9>

```

Ilustración 34, Configuración IP en PC9

D. Configurar las direcciones IP en los Switches.

13. 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.

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

Tabla 6, Asignar IP en los switch para la VLAN 99

Configuración VLAN 99

SW-AA(config)#interface vlan 99

SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0

SW-AA(config-if)#exit

Configuración VLAN 99

SW-BB(config)#interface vlan 99

SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0

Configuración VLAN 99

SW-CC(config)#interface vlan 99

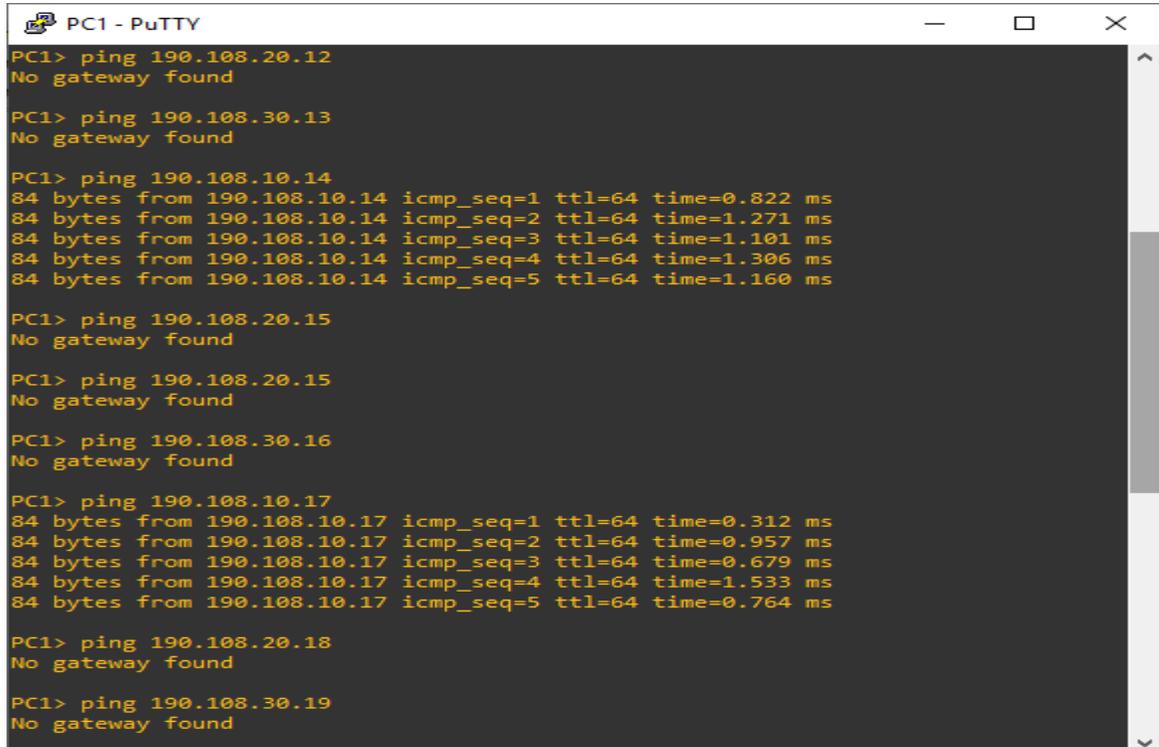
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0

SW-CC(config-if)#exit

E. Verificar la conectividad Extremo a Extremo

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

Con las pruebas realizadas a continuación se observa que los grupos de equipos que pertenecen a la misma VLAN (PC1, PC4, PC7) (PC2, PC5, PC8) (PC3, PC6, PC9) si tienen éxito y esto se debe a la configuración de los puertos, pero no se tiene éxito al tratar de hacer ping a equipos que están por fuera de este grupo.



```
PC1 - PuTTY
PC1> ping 190.108.20.12
No gateway found

PC1> ping 190.108.30.13
No gateway found

PC1> ping 190.108.10.14
84 bytes from 190.108.10.14 icmp_seq=1 ttl=64 time=0.822 ms
84 bytes from 190.108.10.14 icmp_seq=2 ttl=64 time=1.271 ms
84 bytes from 190.108.10.14 icmp_seq=3 ttl=64 time=1.101 ms
84 bytes from 190.108.10.14 icmp_seq=4 ttl=64 time=1.306 ms
84 bytes from 190.108.10.14 icmp_seq=5 ttl=64 time=1.160 ms

PC1> ping 190.108.20.15
No gateway found

PC1> ping 190.108.20.15
No gateway found

PC1> ping 190.108.30.16
No gateway found

PC1> ping 190.108.10.17
84 bytes from 190.108.10.17 icmp_seq=1 ttl=64 time=0.312 ms
84 bytes from 190.108.10.17 icmp_seq=2 ttl=64 time=0.957 ms
84 bytes from 190.108.10.17 icmp_seq=3 ttl=64 time=0.679 ms
84 bytes from 190.108.10.17 icmp_seq=4 ttl=64 time=1.533 ms
84 bytes from 190.108.10.17 icmp_seq=5 ttl=64 time=0.764 ms

PC1> ping 190.108.20.18
No gateway found

PC1> ping 190.108.30.19
No gateway found
```

Ilustración 35, Ping desde el PC1 a los otros 8 PC

```
PC2 - PuTTY
PC2> ping 190.108.10.11
No gateway found

PC2> ping 190.108.30.13
No gateway found

PC2> ping 190.108.10.14
No gateway found

PC2> ping 190.108.20.15
84 bytes from 190.108.20.15 icmp_seq=1 ttl=64 time=0.294 ms
84 bytes from 190.108.20.15 icmp_seq=2 ttl=64 time=4.089 ms
84 bytes from 190.108.20.15 icmp_seq=3 ttl=64 time=0.442 ms
84 bytes from 190.108.20.15 icmp_seq=4 ttl=64 time=1.227 ms
84 bytes from 190.108.20.15 icmp_seq=5 ttl=64 time=0.919 ms

PC2> ping 190.108.30.16
No gateway found

PC2> ping 190.108.10.17
No gateway found

PC2> ping 190.108.20.18
84 bytes from 190.108.20.18 icmp_seq=1 ttl=64 time=0.407 ms
84 bytes from 190.108.20.18 icmp_seq=2 ttl=64 time=0.820 ms
84 bytes from 190.108.20.18 icmp_seq=3 ttl=64 time=0.752 ms
84 bytes from 190.108.20.18 icmp_seq=4 ttl=64 time=0.682 ms
84 bytes from 190.108.20.18 icmp_seq=5 ttl=64 time=0.795 ms

PC2> ping 190.108.30.19
No gateway found

PC2>
```

Ilustración 36, Ping desde el PC2 a los otros 8 PC

```
PC3 - PuTTY
PC3> ping 190.108.10.11
No gateway found

PC3> ping 190.108.20.12
No gateway found

PC3> ping 190.108.10.14
No gateway found

PC3> ping 190.108.20.15
No gateway found

PC3> ping 190.108.30.16
84 bytes from 190.108.30.16 icmp_seq=1 ttl=64 time=0.404 ms
84 bytes from 190.108.30.16 icmp_seq=2 ttl=64 time=0.774 ms
84 bytes from 190.108.30.16 icmp_seq=3 ttl=64 time=1.023 ms
84 bytes from 190.108.30.16 icmp_seq=4 ttl=64 time=0.895 ms
84 bytes from 190.108.30.16 icmp_seq=5 ttl=64 time=0.582 ms

PC3> ping 190.108.10.17
No gateway found

PC3> ping 190.108.20.18
No gateway found

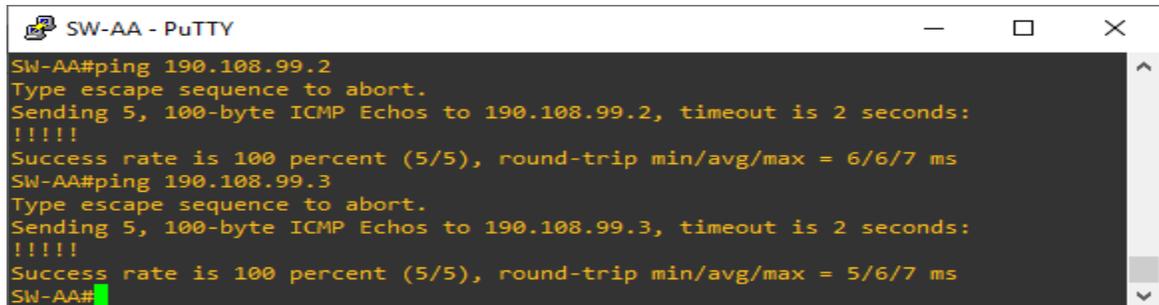
PC3> ping 190.108.30.19
84 bytes from 190.108.30.19 icmp_seq=1 ttl=64 time=1.444 ms
84 bytes from 190.108.30.19 icmp_seq=2 ttl=64 time=4.007 ms
84 bytes from 190.108.30.19 icmp_seq=3 ttl=64 time=1.288 ms
84 bytes from 190.108.30.19 icmp_seq=4 ttl=64 time=0.821 ms
84 bytes from 190.108.30.19 icmp_seq=5 ttl=64 time=0.736 ms

PC3>
```

Ilustración 37, Ping desde el PC3 a los otros 8 PC

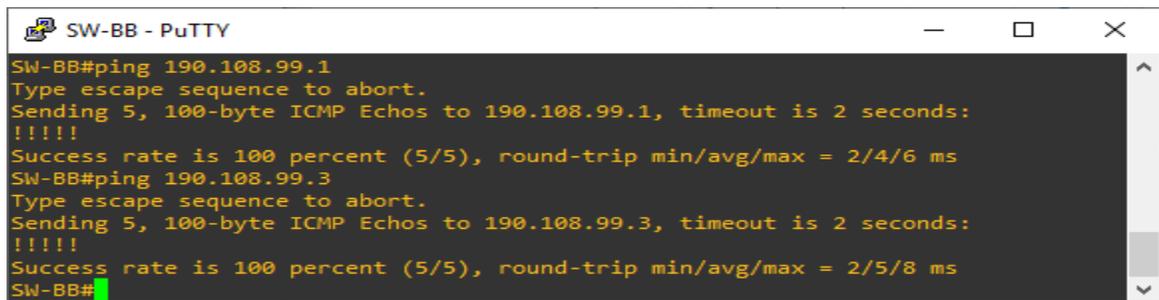
15. Ejecute un Ping desde cada Switch a los demás. Explique por qué el ping tuvo o no tuvo éxito

Con las pruebas realizadas a continuación se observa que los Switch tienen éxito en su comunicación, esto se debe a la configuración de los puertos en modo troncal y la compatibilidad del encapsulamiento.



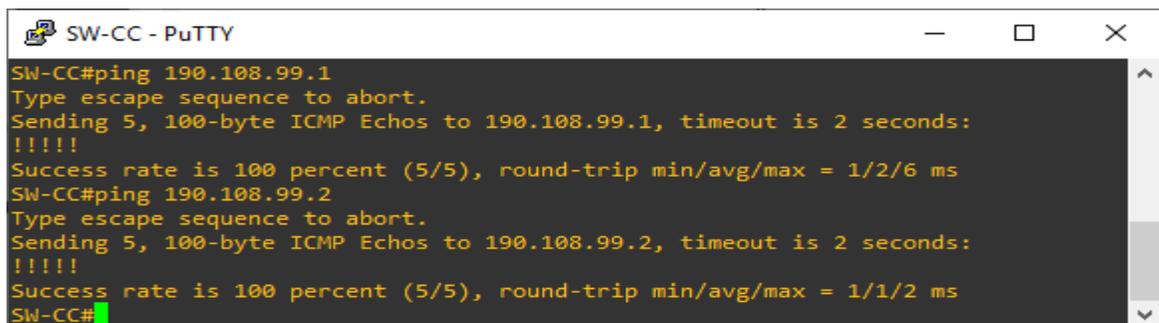
```
SW-AA#ping 190.108.99.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/7 ms
SW-AA#ping 190.108.99.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/6/7 ms
SW-AA#
```

Ilustración 38, Ping desde el SW-AA a los otros Switch



```
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 = 2/4/6 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 = 2/5/8 ms
SW-BB#
```

Ilustración 39, Ping desde el SW-BB a los otros Switch

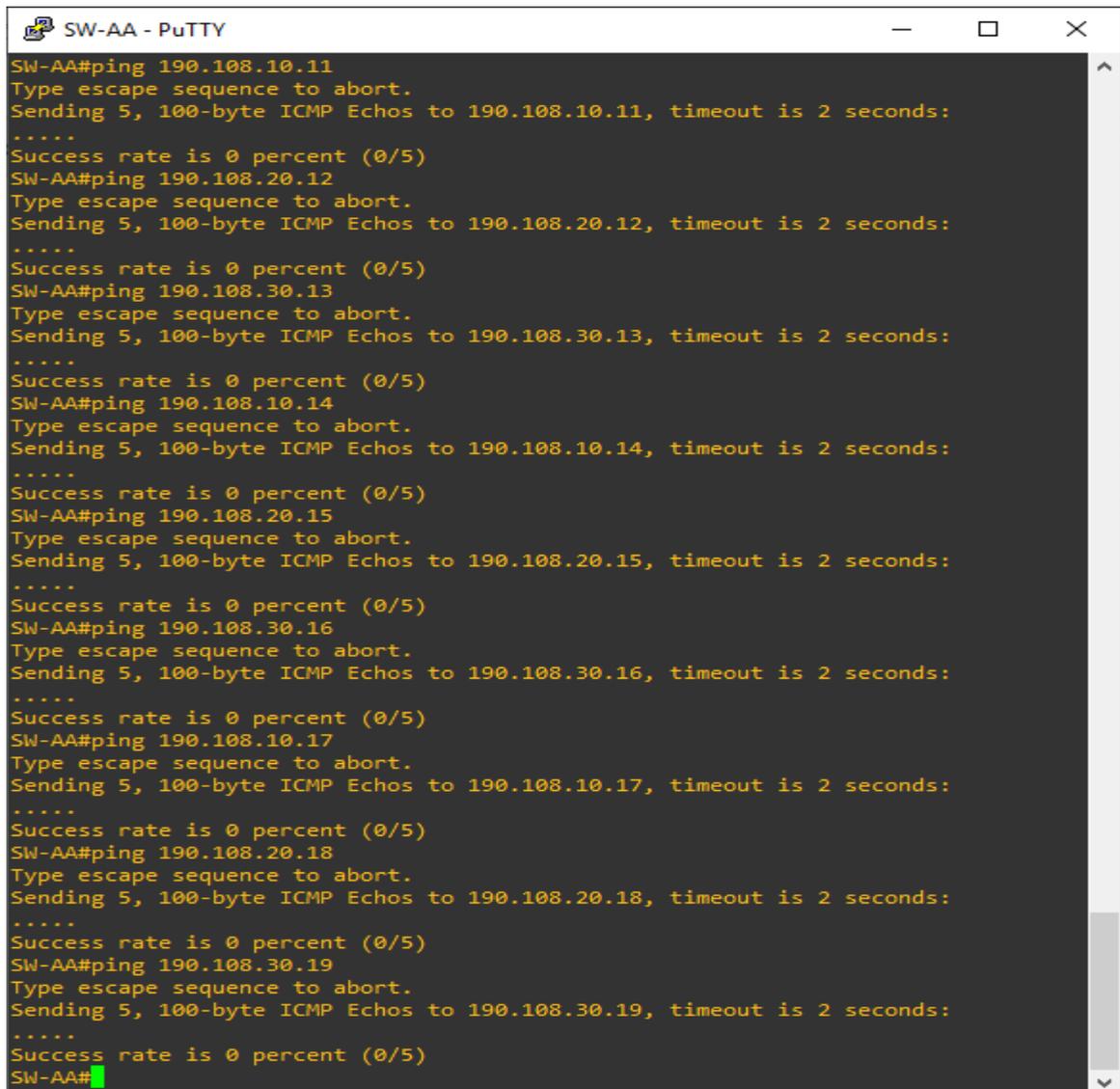


```
SW-CC#ping 190.108.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6 ms
SW-CC#ping 190.108.99.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
SW-CC#
```

Ilustración 40, Ping desde el SW-CC a los otros Switch

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

Con las pruebas realizadas a continuación se observa que ningún Switch tuvo éxito en el Ping hacia los PCs ya que la configuración de estos esta administrado por el protocolo VTP a través de las VLANs. Los Switch están trabajando por la VLAN 99 y los equipos trabajan por otras.



```
SW-AA#ping 190.108.10.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.11, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#ping 190.108.20.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.12, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#ping 190.108.30.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.13, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#ping 190.108.10.14
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.14, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#ping 190.108.20.15
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.15, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#ping 190.108.30.16
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.16, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#ping 190.108.10.17
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.17, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#ping 190.108.20.18
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.18, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#ping 190.108.30.19
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.19, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#
```

Ilustración 41, Ping desde SW-AA a los 9 PCs

```
SW-BB - PuTTY
SW-BB#ping 190.108.10.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.11, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#ping 190.108.20.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.12, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#ping 190.108.30.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.13, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#ping 190.108.10.14
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.14, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#ping 190.108.20.15
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.15, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#ping 190.108.30.16
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.16, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#ping 190.108.10.17
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.17, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#ping 190.108.20.18
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.18, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#ping 190.108.30.19
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.19, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#
```

Ilustración 42, Ping desde SW-BB a los 9 PCs

```
SW-CC - PuTTY
SW-CC#ping 190.108.10.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.11, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-CC#ping 190.108.20.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.12, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-CC#ping 190.108.30.13
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.13, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-CC#ping 190.108.10.14
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.14, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-CC#ping 190.108.20.15
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.15, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-CC#ping 190.108.30.16
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.16, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-CC#ping 190.108.10.17
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.17, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-CC#ping 190.108.20.18
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.18, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-CC#ping 190.108.30.19
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.19, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-CC#
```

Ilustración 43, Ping desde SW-CC a los 9 PCs

CONCLUSIONES

La elaboración de estos ejercicios en GNS3 permitió profundizar en todos los temas vistos en el curso ya que estos escenarios manejan un ámbito real.

La línea de Cisco nos permite conocer como está conectado el mundo entre sí, al igual que nos prepara para entender, analizar, configurar y sacar conclusiones de los casos de redes que podamos presenciar.

A parte de estos conocimientos, también se debe de conocer las preferencias del software que se está utilizando para tener unas buenas prácticas, ya que se obtuvieron algunos errores y atrasaba el procedimiento del desarrollo de los escenarios por no saber posibles configuraciones del software.

BIBLIOGRAFÍA

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!AmlJYei-NT1InWR0hoMxgBNv1CJ>

Switch CISCO - Procedimientos de instalación y configuración del IOS [OVA]. Recuperado de <https://1drv.ms/u/s!AmlJYei-NT1IlyYRohwtwPUV64dg>

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-NT1InMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing a Border Gateway Protocol (BGP). Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmlJYei-NT1InMfy2rhPZHwEoWx>

UNAD (2015). Introducción a la configuración de Switches y Routers [OVA]. Recuperado de <https://1drv.ms/u/s!AmlJYei-NT1IhgL9QChD1m9EuGqC>

UNAD (2015). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmlJYei-NT1IhgOyiWeh6timi_Tm