

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CARLOS ARTURO ROJAS GUAZA

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CARLOS ARTURO ROJAS GUAZA

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTÁ, 22 de mayo de 2020

AGRADECIMIENTOS

Agradezco a Dios por bendecirme y guiar mis pasos, a mi esposa y mi familia quienes son el motor de mi vida y han creído en mí siempre, mostrándome el camino hacia la superación.

CONTENIDO

AGRADECIMIENTOS.....	4
CONTENIDO.....	5
LISTA DE TABLAS	6
LISTA DE FIGURAS	7
GLOSARIO	8
RESUMEN.....	9
ABSTRACT.....	9
INTRODUCCIÓN.....	10
DESARROLLO	11
1. Escenario 1	11
2. Escenario 2	19
CONCLUSIONES.....	31
BIBLIOGRAFÍA.....	32

LISTA DE TABLAS

Tabla 1. Configuración de R1 -----	11
Tabla 2. Configuración de R2 -----	11
Tabla 3. Configuración de R3-----	12
Tabla 4. Configuración de R4 -----	12
Tabla 5. Configuración de los puertos y direccionamiento de la Vlan -----	25
Tabla 6. Asignación de dirección IP al SVI -----	27

LISTA DE FIGURAS

Figura 1. Topología del escenario1 -----	11
Figura 2. Topología en GNS3 -----	12
Figura 3. Tabla de enrutamiento -----	14
Figura 4. Tabla de enrutamiento -----	15
Figura 5. Tabla de enrutamiento -----	16
Figura 6. Tabla de enrutamiento -----	16
Figura 7. Tabla de enrutamiento -----	17
Figura 8. Tabla de enrutamiento -----	18
Figura 9. Topología del escenario 2 -----	19
Figura 10. Topología en Packet Tracer -----	19
Figura 11. Se verifica VTP -----	20
Figura 12. Se verifica VTP -----	21
Figura 13. Se verifica VTP -----	21
Figura 14. Se verifica el enlace troncal -----	22
Figura 15. Se verifica el enlace troncal -----	22
Figura 16. Se verifica el enlace troncal -----	22
Figura 17. Se verifica el enlace troncal -----	23
Figura 18. Se verifica el enlace troncal -----	23
Figura 19. Se verifica las Vlan agregadas -----	24
Figura 20. Se verifica las Vlan agregadas -----	25
Figura 21. Se verifica las Vlan agregadas -----	25
Figura 22. Ping desde PC1 a PC2, PC9 y PC4 -----	28
Figura 23. Comando Ping en los Switches -----	29
Figura 24. Comando Ping en los Switches -----	29
Figura 25. Comando Ping en los Switches -----	29
Figura 26. Ping desde SW AA a PC1, PC2, PC3 -----	30

GLOSARIO

Dirección ip: una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz de un dispositivo dentro de una red que utilice el protocolo IP.

Enlace troncal: un enlace troncal es un enlace punto a punto, entre dos dispositivos de red, que transporta más de una VLAN.

Interfaz: una interfaz de router suministra la conexión física entre el router y un tipo de medio físico de la red.

Máscara: una máscara wildcard es una máscara de bits que indica qué partes de una dirección de IP son relevantes para la ejecución de una determinada acción.

Vlan: método para crear redes lógicas independientes dentro de una misma red física.

RESUMEN

Por medio de esta actividad se coloca en práctica el desarrollo de escenarios en diferentes herramientas de simulación, con el fin de configurar adecuadamente los dispositivos, en estos escenarios se aplicaran protocolos de enrutamiento BGP, protocolo de administración como el VTP, se crearan VLANS, se configuraran los enlaces troncales, se configuraran las direcciones IP correspondiente y para verificar cada uno de los procedimientos se utilizaran comandos como Show ip route para verificar las configuraciones.

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

ABSTRACT

Through this activity, the development of scenarios is put into practice in different simulation tools, in order to properly configure the devices, in these scenarios BGP routing protocols will be applied, administration protocol such as VTP, VLANs will be created, trunks will be configured, the corresponding IP addresses will be configured and to verify each of the procedures, commands such as Show ip route will be used to verify the configurations.

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

INTRODUCCIÓN

Las pruebas de habilidades practicas permiten demostrar y colocar a prueba todos los conocimientos y habilidades desarrolladas durante el diplomado, esto tiene como objetivo ayudar en la buena formación académica y profesional para estar preparados para solucionar cualquier entorno que se presente.

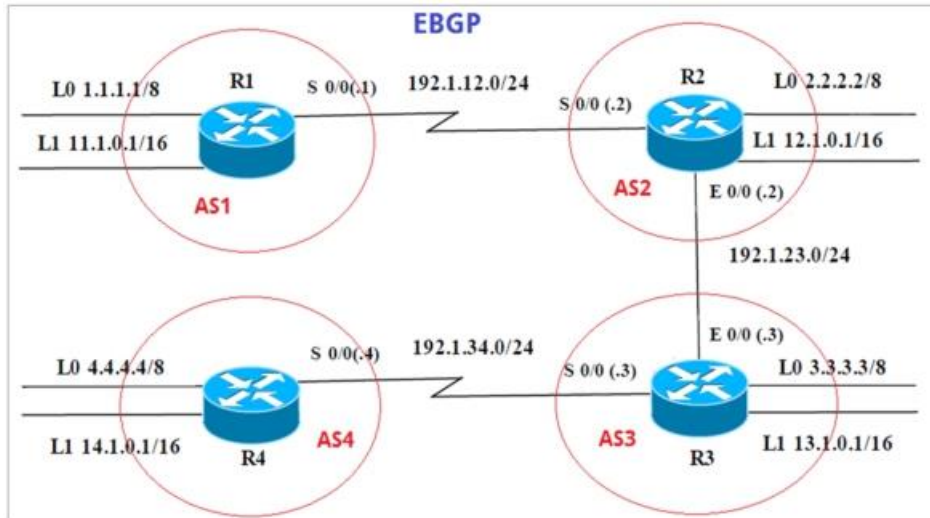
Dentro del primer escenario se configura la relación de BGP entre R1 y R2, R1 debe estar en AS1 y R2 debe estar en AS2. Se anuncia las direcciones de Loopback en BGP, y se codifica los id para los routers BGP.

En el segundo escenario se configuran los switches para hacer uso de las VTP, verificando las configuraciones mediante el comando show vtp status, ademas se utiliza el comando show interface trunk, para la verificación del enlace trunk entre SW-AA y SW-BB.

DESARROLLO

ESCENARIO 1

Figura 1. Topología del escenario 1.



R1

Tabla 1. Configuración de 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

Tabla 2. Configuración de 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

Tabla 3. Configuración de R3.

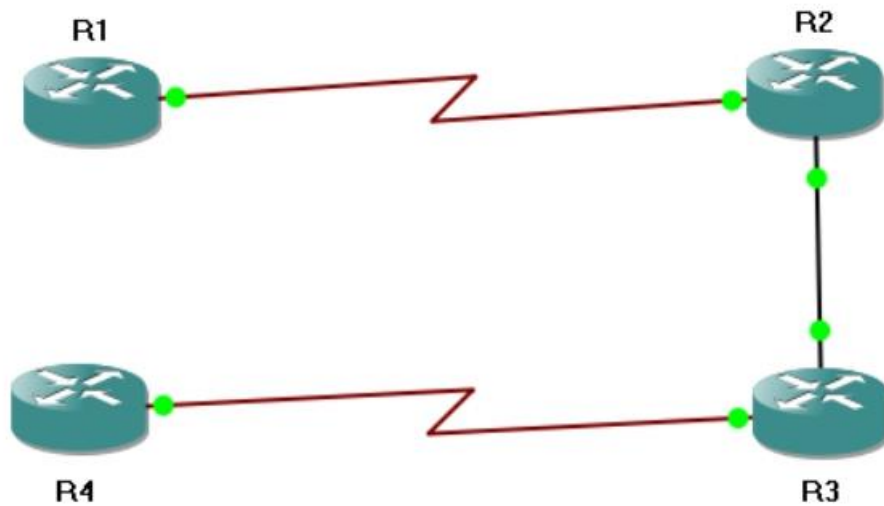
Interfaz	Dirección IP	Máscara
Loopback 0	3.3.3.3	255.0.0.0
Loopback 1	13.1.0.1	255.255.0.0
E 0/0	192.1.23.3	255.255.255.0
S 0/0	192.1.34.3	255.255.255.0

R4

Tabla 4. Configuración de 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	192.1.34.4	255.255.255.0

Figura 2. Topología en GNS3.



```
R1>enable
R1#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface loopback 0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config)#exit
R1(config)#interface loopback 1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config)#exit
R1(config)#int serial 1/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#no shut
```

```
R1(config-if)#exit R2>enable R2#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# interface loopback 0 R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#exit
R2(config)# interface loopback 1 R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#exit
R2(config)#interface s1/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shut R2(config-if)#exit R2(config)#interface f0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shutdown R2(config-if)#exit
```

```
R3>enable
R3#config t
Enter configuration commands, one per line. End with CNTL/Z. R3(config)#
interface loopback 0
R3(config-if)#ip address 3.3.3.3 255.0.0.0 R3(config-if)#exit
R3(config)# interface loopback 1 R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#exit
R3(config)#interface s1/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0 R3(config-if)#no shutdown
R3(config-if)#exit R3(config)#interface f0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0 R3(config-if)#no shutdown
```

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

```
R4>enable
```

```
R4#config terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z. R4(config)#  
interface loopback 0
```

```
R4(config-if)#ip address 4.4.4.4 255.0.0.0 R4(config-if)#exit
```

```
R4(config)# interface loopback 1 R4(config-if)#ip address 14.1.0.1 255.255.0.0
```

```
R4(config-if)#exit
```

```
R4(config)#interface s1/0
```

```
R4(config-if)#ip address 192.1.34.4 255.255.255.0 R4(config-if)#no shutdown
```

```
R4(config-if)#exit
```

1. Configure 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)#router bgp 1 R1(config-router)#bgp router-id 22.22.22.22
```

```
R1(config-router)#network 192.1.12.0 mask 255.255.255.0
```

```
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
```

```
R1(config-router)#network 1.0.0.0 mask 255.0.0.0
```

```
R1(config-router)#neighbor 192.1.12.2 remote-as 2
```

Figura 3. Tabla de enrutamiento.

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

  1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       1.0.0.0/8 is directly connected, Loopback0
L       1.1.1.1/32 is directly connected, Loopback0
B       2.0.0.0/8 [20/0] via 192.1.12.2, 00:02:59
B       11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       11.1.0.0/16 is directly connected, Loopback1
L       11.1.0.1/32 is directly connected, Loopback1
B       12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.12.2, 00:02:59
C       192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.12.0/24 is directly connected, Serial1/0
L       192.1.12.1/32 is directly connected, Serial1/0
B       192.1.23.0/24 [20/0] via 192.1.12.2, 00:02:59
```

```

R2(config)#router bgp 2
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#network 192.1.12.0 mask 255.255.255.0
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)#neighbor 192.1.12.1 remote-as 1

```

Figura 4. Tabla de enrutamiento.

```

R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:04:58
     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, 00:04:58
     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, FastEthernet0/0
L    192.1.23.2/32 is directly connected, FastEthernet0/0

```

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

```

R3(config)#router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#network 192.1.23.0 mask 255.255.255.0
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 192.1.34.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.23.2 remote-as 2

```

Figura 5. Tabla de enrutamiento.

```
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:02:50
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:02:50
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
L    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 192.1.23.2, 00:02:50
B    12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 192.1.23.2, 00:02:50
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    192.1.12.0/24 [20/0] via 192.1.23.2, 00:02:50
C    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, FastEthernet0/0
L    192.1.23.3/32 is directly connected, FastEthernet0/0
C    192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial1/0
L    192.1.34.3/32 is directly connected, Serial1/0
```

```
R2(config-router)#network 192.1.23.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.23.3 remote-as 3
```

Figura 6. Tabla de enrutamiento.

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:14:08
C    2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    2.0.0.0/8 is directly connected, Loopback0
L    2.2.2.2/32 is directly connected, Loopback0
L    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 192.1.12.1, 00:14:08
C    12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    12.1.0.0/16 is directly connected, Loopback1
L    12.1.0.1/32 is directly connected, Loopback1
L    13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0 [20/0] via 192.1.23.3, 00:14:08
L    14.0.0.0/16 is subnetted, 1 subnets
B    14.1.0.0 [20/0] via 192.1.23.3, 00:14:08
B    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
L    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, FastEthernet0/0
L    192.1.23.2/32 is directly connected, FastEthernet0/0
B    192.1.34.0/24 [20/0] via 192.1.23.3, 00:14:08
R2#
```


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

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

Figura 7. Tabla de enrutamiento.

```
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:11:45
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:11:45
     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, 00:11:45
     12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 192.1.23.2, 00:11:45
     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, 00:11:46
B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:11:45
     192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, FastEthernet0/0
L    192.1.23.3/32 is directly connected, FastEthernet0/0
     192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial1/0
L    192.1.34.3/32 is directly connected, Serial1/0
R3#
```

```

R4(config)#router bgp 4
R4(config-router)#bgp router-id 66.66.66.66
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)#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
R4(config-router)#exit
R4(config)#ip route 3.0.0.0 255.0.0.0 192.1.34.3

```

Figura 8. Tabla de enrutamiento.

```

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

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 3.3.3.3, 00:15:52
B    2.0.0.0/8 [20/0] via 3.3.3.3, 00:15:52
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, 00:15:52
     12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 3.3.3.3, 00:15:52
     13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0 [20/0] via 3.3.3.3, 00:16:22
     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, 00:15:52
B    192.1.23.0/24 [20/0] via 3.3.3.3, 00:16:22
     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#

```

ESCENARIO 2

Figura 9. Topología del escenario 2.

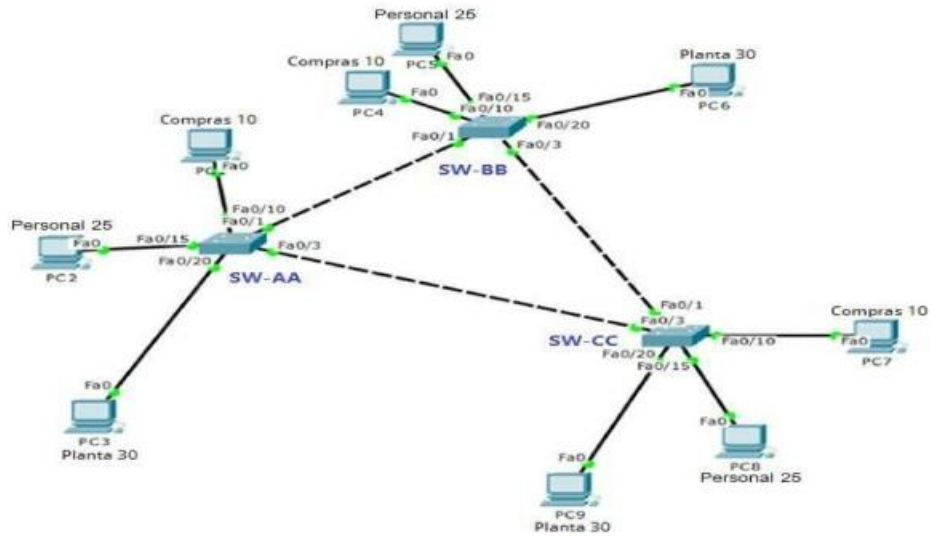
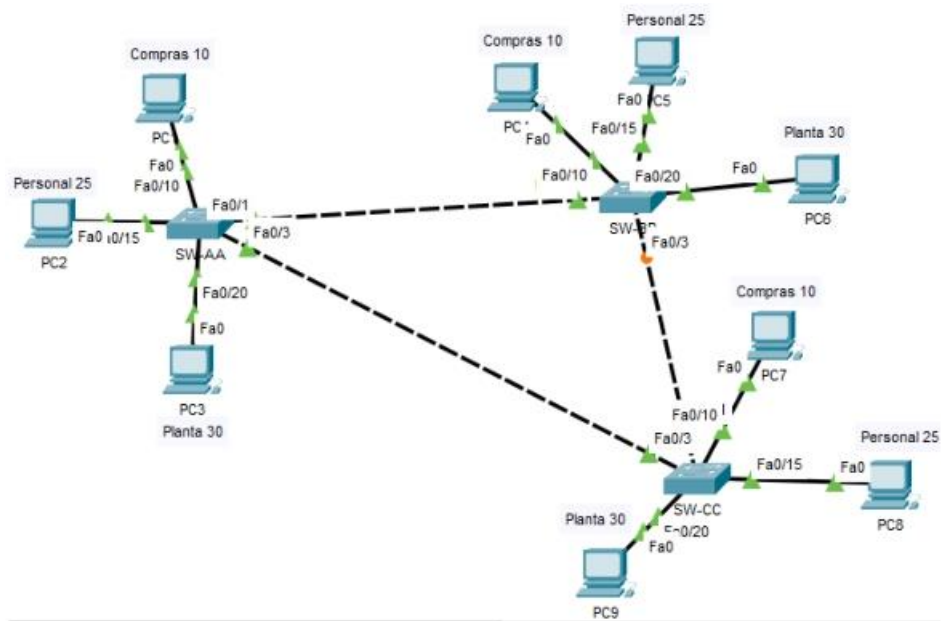


Figura 10. Topología en Packet Tracer.



A. Configuración 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 VTP llamado CCNP y usando la contraseña cisco.

```
SW-AA>enable
```

```
SW-AA #conf terminal
```

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

```
SW-AA(config)#vtp mode client Setting device to VTP CLIENT mode. SW-  
AA(config)#vtp domain CCNP SW-AA(config)#vtp password cisco
```

```
SW-BB>enable
```

```
SW-BB #conf terminal
```

Enter configuration commands, one per line. End with CNTL/Z. SW-BB(config)#vtp mode server

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

```
SW-CC>enable
```

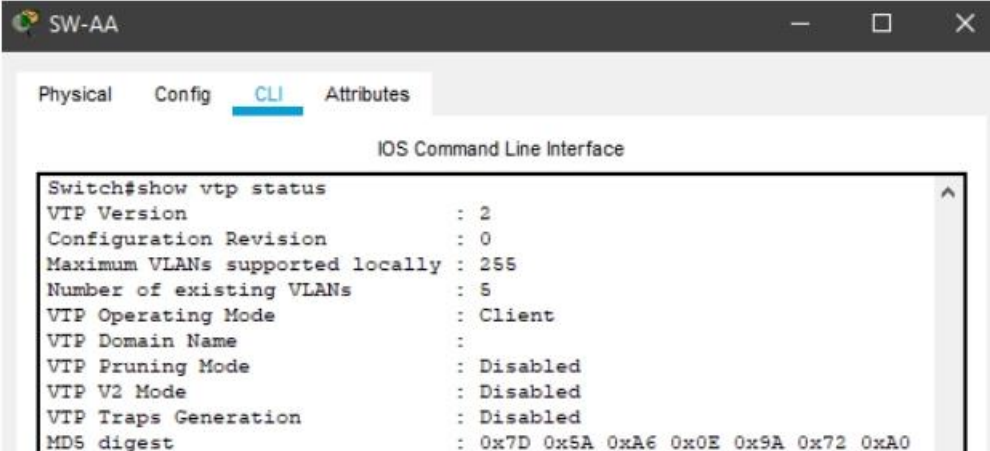
```
SW-CC #conf terminal
```

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

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

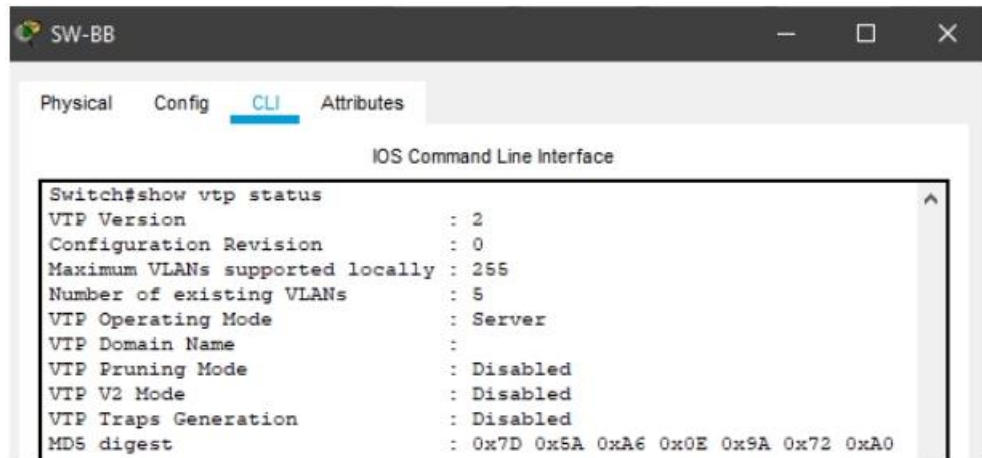
2. Verifique las configuraciones mediante el comando *show vtp status*.

Figura 11. Se verifica VTP.



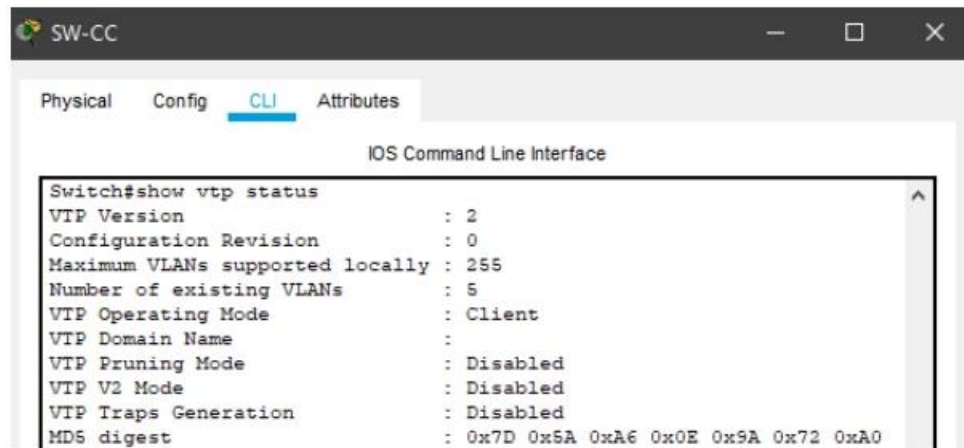
```
SW-AA  
Physical Config CLI Attributes  
IOS Command Line Interface  
Switch#show vtp status  
VTP Version : 2  
Configuration Revision : 0  
Maximum VLANs supported locally : 255  
Number of existing VLANs : 5  
VTP Operating Mode : Client  
VTP Domain Name :  
VTP Pruning Mode : Disabled  
VTP V2 Mode : Disabled  
VTP Traps Generation : Disabled  
MD5 digest : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0
```

Figura 12. Se verifica VTP.



```
SW-BB
Physical Config CLI Attributes
IOS Command Line Interface
Switch#show vtp status
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode : Server
VTP Domain Name :
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0
```

Figura 13. Se verifica VTP.



```
SW-CC
Physical Config CLI Attributes
IOS Command Line Interface
Switch#show vtp status
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode : Client
VTP Domain Name :
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0
```

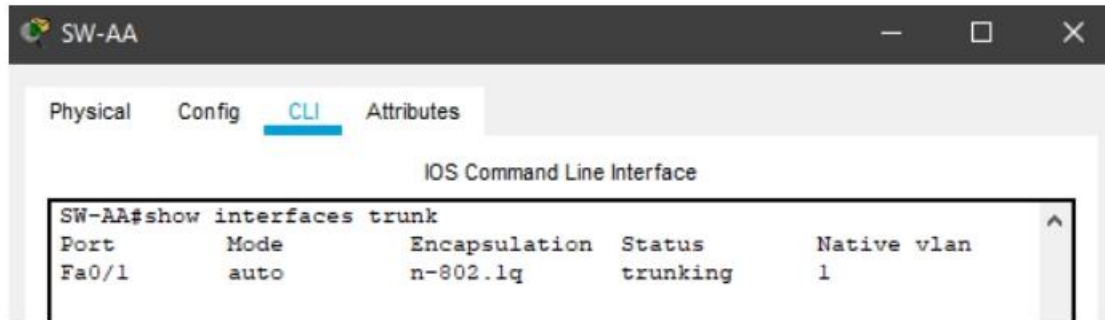
B. Configuración DTP(Dynamic Trunking Protocol)

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-AA>enable
SW-AA#config terminal
SW-AA(config)#interface f0/1
SW-AA(config-if)#switch mode dynamic desirable
SW-AA(config-if)#exit
```

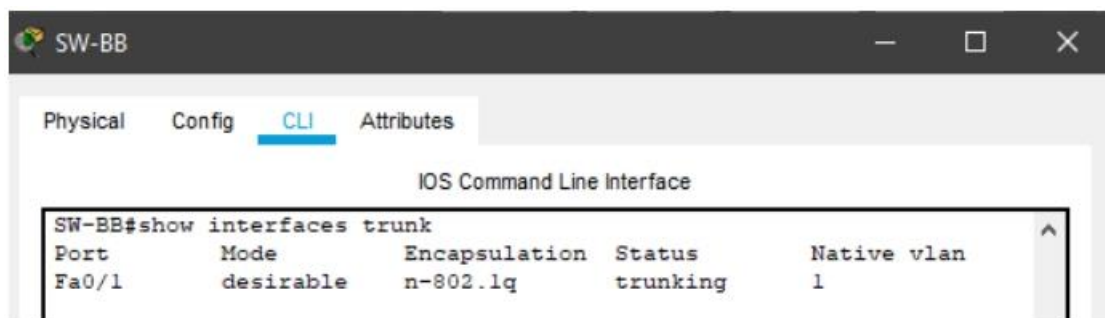
2. Verifique el enlace "trunk" entre SW-AA y SW-BB usando el comando *show interfaces trunk*.

Figura 14. Se verifica el enlace troncal.



```
SW-AA#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     auto      n-802.1q       trunking    1
```

Figura 15. Se verifica el enlace troncal.



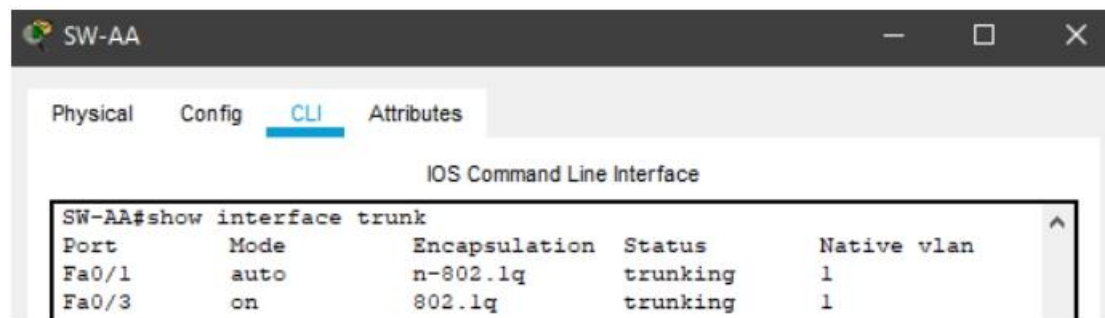
```
SW-BB#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     desirable n-802.1q       trunking    1
```

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

```
SW-AA>enable
SW-AA#conf terminal
SW-AA(config)#interface f0/3
SW-AA(config-if)#switchport mode trunk
```

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

Figura 16. Se verifica el enlace troncal..



```
SW-AA#show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     auto      n-802.1q       trunking    1
Fa0/3     on        802.1q         trunking    1
```


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

```
SW-BB>enable SW-  
BB#conf terminal SW-  
BB(config)#int f0/3  
SW-BB(config-if)#switchport mode trunk
```

```
SW-CC>enable SW-  
CC#conf terminal SW-  
CC(config)#int f0/3  
SW-CC(config-if)#switchport mode trunk
```

Figura 17. Se verifica el enlace troncal.

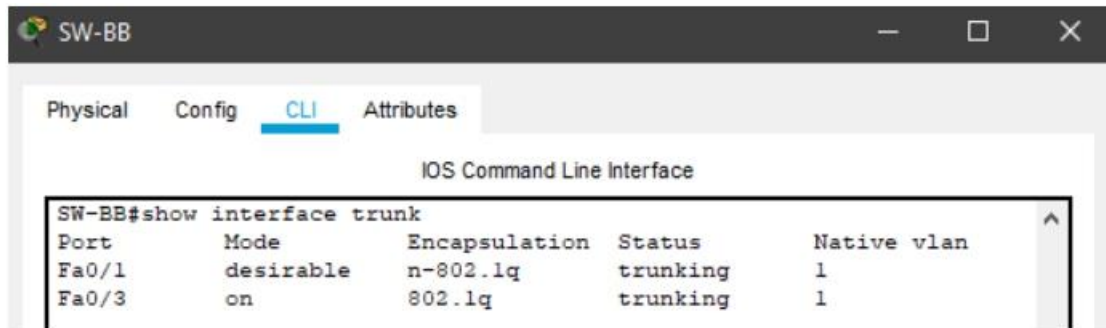
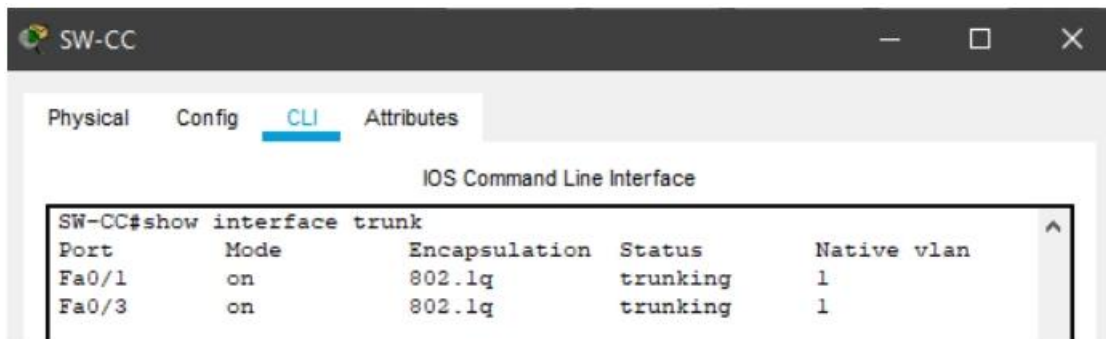


Figura 18. Se verifica el enlace troncal.



C. Agregar VLANs y asignar puertos.

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

En el momento que se intenta agregar la vlan 10 al Switch SW-AA muestra un mensaje el cual hace referencia a que la configuración del vlan vtp no se permite cuando el dispositivo está en el modo cliente.

```
SW-AA>enable SW-  
AA#conf terminal
```

```
SW-AA(config)#vlan 10  
VTP VLAN configuration not allowed when device is in CLIENT mode.
```

```
SW-BB>enable SW-  
BB#conf t 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
```

2. Verifique que las VLANs han sido agregadas correctamente.

Figura 19. Se verifica las Vlan agregadas.

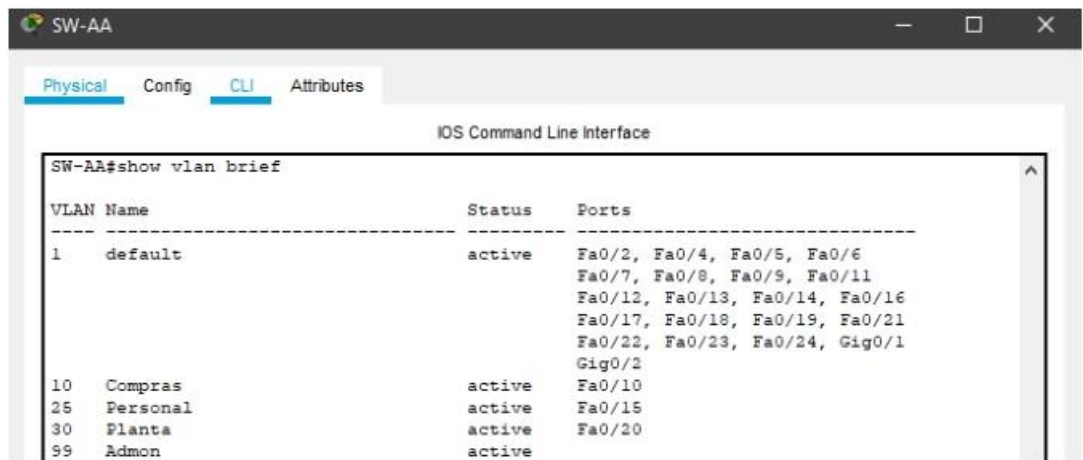


Figura 20. Se verifica las Vlan agregadas.

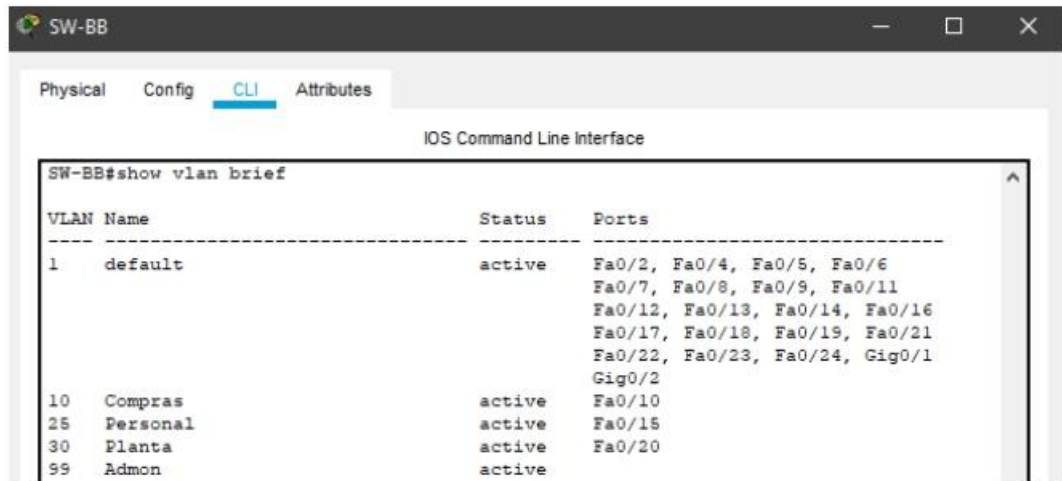
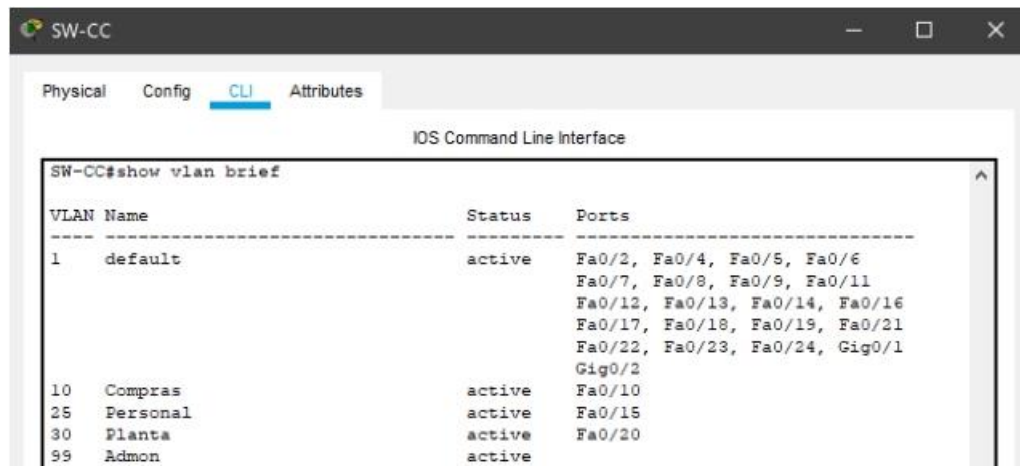


Figura 21. Se verifica las Vlan agregadas.



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

Tabla 5. Configuración de los puertos y direccionamiento de las Vlan.

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

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

5. 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>enable SW-  
AA#config terminal
```

```
SW-AA(config)#int f0/10 SW-AA(config-  
if)#switchport mode access SW-AA(config-  
if)#switchport access vlan 10 SW-  
AA(config-if)#int f0/15 SW-AA(config-  
if)#switchport mode access SW-AA(config-  
if)#switchport access vlan 25 SW-  
AA(config-if)#int f0/20 SW-AA(config-  
if)#switchport mode access SW-AA(config-  
if)#switchport access vlan 30
```

```
SW-BB>enable SW-  
BB#conf t SW-  
BB(config)#int f0/10  
SW-BB(config-if)#switchport mode access  
SW-BB(config-if)#switchport access vlan 10  
SW-BB(config-if)#int f0/15 SW-BB(config-  
if)#switchport mode access SW-BB(config-  
if)#switchport access vlan 25 SW-  
BB(config-if)#int f0/20 SW-BB(config-  
if)#switchport mode access SW-BB(config-  
if)#switchport access vlan 30
```

```
SW-CC>enable SW-  
CC#conf t SW-  
CC(config)#int f0/10  
SW-CC(config-if)#switchport mode access  
SW-CC(config-if)#switchport access vlan 10  
SW-CC(config-if)#int f0/15 SW-CC(config-  
if)#switchport mode access SW-CC(config-  
if)#switchport access vlan 25 SW-  
CC(config-if)#int f0/20 SW-CC(config-  
if)#switchport mode access SW-CC(config-  
if)#switchport access vlan 30
```

Para el direccionamiento de los PC se asignaron las siguientes IP según la tabla anterior.

VLAN 10 = 190.108.10.X
VLAN 25 = 190.108.20.X
VLAN 30 = 190.108.30.X

PC1: 190.108.10.1
PC4: 190.108.10.2
PC7: 190.108.10.3

PC2: 190.108.20.1
PC5: 190.108.20.2
PC8: 190.108.20.3

PC3: 190.108.30.1
PC6: 190.108.30.2
PC9: 190.108.30.3

D. Configurar las direcciones IP en los Switches.

14. En cada uno de los Switches asigne una dirección IP al SVI (*Switch Virtual Interface*) para VLAN 99 de acuerdo con la siguiente tabla de direccionamiento y active la interfaz.

Tabla 6. Asignación de dirección IP al SVI.

Equipo	Interfaz	Dirección IP	Máscara
SW-AA	VLAN 99	190.108.99.1	255.255.255.0
SW-BB	VLAN 99	190.108.99.2	255.255.255.0
SW-CC	VLAN 99	190.108.99.3	255.255.255.0

```
SW-AA>enable SW-  
AA#config t SW-  
AA(config)#int vlan 99  
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
```

```
SW-BB>enable SW-  
BB#config t SW-  
BB(config)#int vlan 99  
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
```

```
SW-CC>enable
```

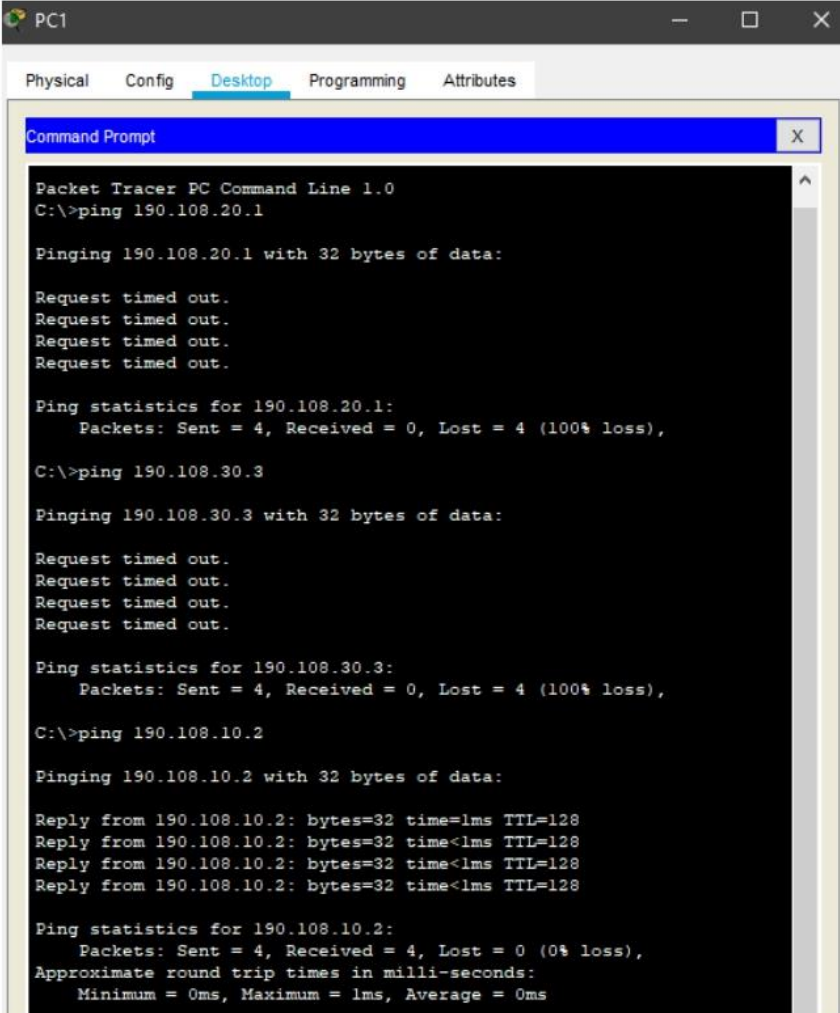
```
SW-CC#config t
SW-CC(config)#int vlan 99
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0
```

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.

Se realizó los Ping respectivos de PC a PC y no todos los Ping tuvieron éxito, esto se debe a que solamente los PC de la misma VLAN pueden hacer Ping entre ellos, en la siguiente imagen se ve el ejemplo que se realiza Ping del PC1 al PC2, PC9 y PC4 y solamente se pudo realizar Ping al PC4 que pertenece a la misma Vlan.

Figura 22. Ping desde PC1 a PC2, PC9 y PC4.



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 190.108.20.1

Pinging 190.108.20.1 with 32 bytes of data:

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

Ping statistics for 190.108.20.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.30.3

Pinging 190.108.30.3 with 32 bytes of data:

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

Ping statistics for 190.108.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.10.2

Pinging 190.108.10.2 with 32 bytes of data:

Reply from 190.108.10.2: bytes=32 time=1ms TTL=128
Reply from 190.108.10.2: bytes=32 time<1ms TTL=128
Reply from 190.108.10.2: bytes=32 time<1ms TTL=128
Reply from 190.108.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

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

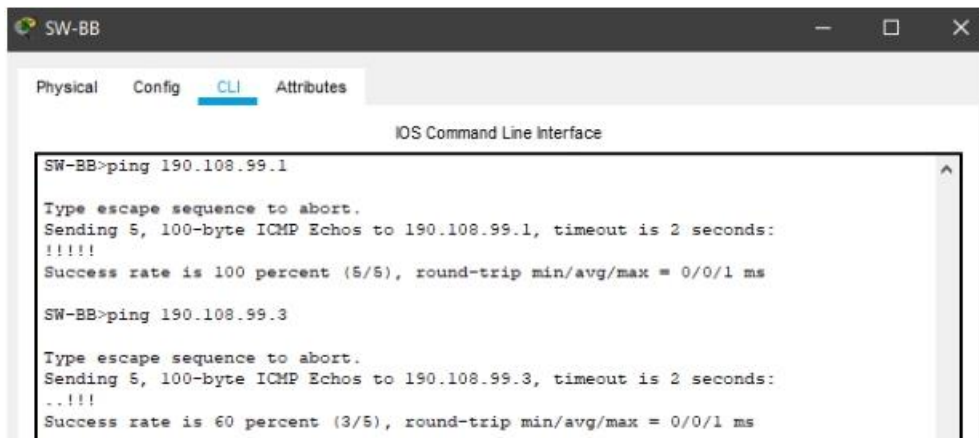
Figura 23. Comando Ping en los Switches.



```
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 60 percent (3/5), round-trip min/avg/max = 0/1/2 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 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms
```

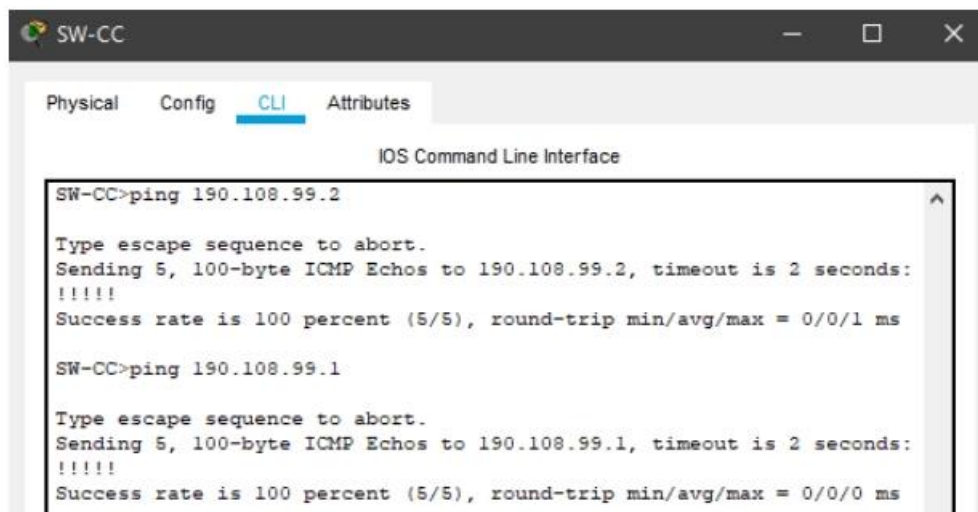
Figura 24. Comando Ping en los Switches.



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

SW-BB>ping 190.108.99.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/1 ms
```

Figura 25. Comando Ping en los Switches.



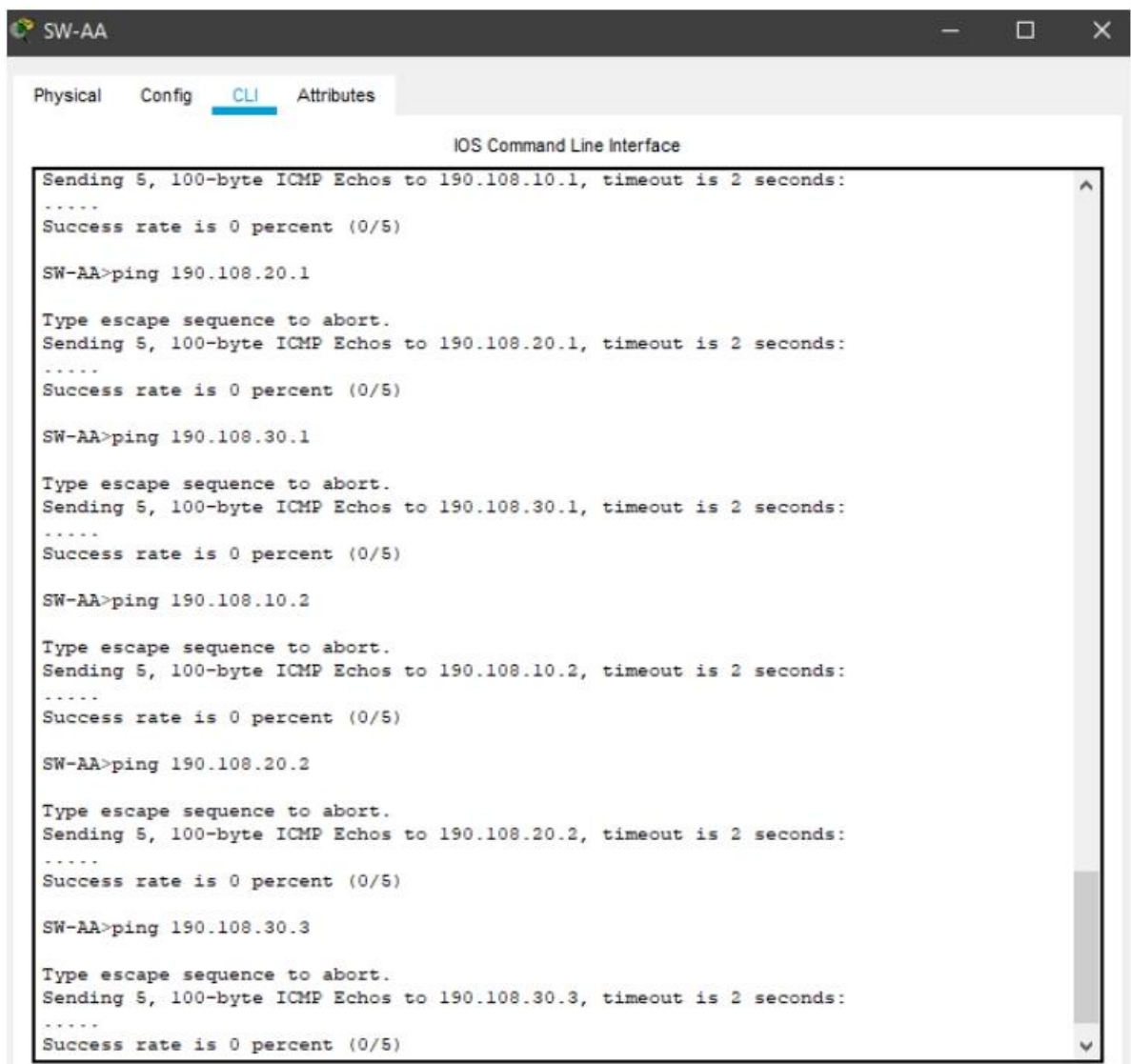
```
SW-CC>ping 190.108.99.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

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

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

Se realizo Ping desde cada Switch a cada PC y en todos los casos el Ping no pudo ser enviado, esto se debe a que no se configuro la direcciones IP en las Vlan, solamente se configuro la Vlan 99 la cual nos permite tener una conexión entre Switches, en conclusión para poder realizar Ping desde los Switches a cualquier PC se le debe asignar un direccionamiento a cada Vlan según la Subred que se este manejando.

Figura 26. Ping desde SW-AA a PC1, PC2, PC3.



```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
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 190.108.20.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA>ping 190.108.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA>ping 190.108.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.2, 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)
```

CONCLUSIONES

Con el desarrollo de esta actividad se pudo afianzar los conocimientos adquiridos durante el diplomado en profundización CCNP, gracias a esta prueba de habilidades se logró colocar a prueba las habilidades para la comprensión y solución de problemas como los dos escenarios propuestos.

Para la elaboración de cada escenario se utilizó herramientas de simulación como GNS3 y Packet Tracer, esto permite entender el funcionamiento de las topologías y sus configuraciones como si fuera un entorno real.

Las indicaciones de la guía para la elaboración de los dos escenarios fue bastante clara, las configuraciones realizadas con las herramientas de simulación fueron satisfactorias para el desarrollo de los ejercicios.

BIBLIOGRÁFIA

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

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!AmIJYei-NT1InMfy2rhPZHwEoWx>