

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

**JHOAN SEBASTIAN ALMARIO TIERRADENTRO**

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

**NEIVA  
2020**

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

**JHOAN SEBASTIAN ALAMARIO**

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

**Director:**

**GERARDO GRANADOS ACUÑA**

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

NOTA DE ACEPTACIÓN:

---

---

---

---

---

---

---

---

Presidente del Jurado

---

Jurado

---

Jurado

Neiva, 15 de mayo de 2020

## **AGRADECIMIENTOS**

Agradezco inmensamente a los directivos y tutores de la Universidad Nacional Abierta y a Distancia, quienes, con su vocación siempre han estado atentos como guías que iluminan los pasos de sus estudiantes para forjar una mejor sociedad.

## TABLA DE CONTENIDO

AGRADECIMIENTOS .....	4
LISTA DE FIGURAS .....	6
LISTA DE TABLAS .....	7
GLOSARIO .....	8
RESUMEN .....	9
ABSTRACT .....	10
INTRODUCCIÓN .....	11
Desarrollo del trabajo .....	12
Escenario 1 .....	12
Escenario 2 .....	20
CONCLUSIONES .....	37
BIBLIOGRAFÍA .....	38

## LISTA DE FIGURAS

Figura 1 Topología en packet tracer (Escenario 1).....	12
Figura 2 Topología Escenario 1 .....	12
Figura 3 Escenario 1 GNS3 - Autoría propia.....	15
Figura 4 Enrutamiento de R1 con respecto a R2 - Escenario 1 .....	16
Figura 5 Enrutamiento de R2 con respecto a R1 - Escenario 1 .....	16
Figura 6 Enrutamiento de R2 con respecto a R3 - Escenario 1 .....	17
Figura 7 Enrutamiento de R3 con respecto a R2 - Escenario 1 .....	18
Figura 8 Enrutamiento de R3 con respecto a R4 - Escenario 1 .....	19
Figura 9 Enrutamiento de R4 con respecto a R3 - Escenario 1 .....	20
Figura 10 Topología en packet tracer (Escenario 2).....	20
Figura 11 Topología Escenario 2 .....	20
Figura 12 Verificación Vtp status en SWAA - Escenario 2.....	21
Figura 13 Verificación Vtp status en SWBB - Escenario 2 .....	22
Figura 14 Verificación Vtp status en SWCC - Escenario 2.....	22
Figura 15 Verificación interface troncal de SWBB a SWAA Escenario 2.....	24
Figura 16 Verificación interface troncal de SWBB a SWAA Escenario 2.....	24
Figura 17 configuración un enlace trunk SWAA.....	25
Figura 18 Verificación interface troncal de SWAA a SWCC.....	26
Figura 19 Verificación interface troncal de SWBB a SWCC .....	26
Figura 20 Configuración de VLAN en SWAA.....	27
Figura 21 Verificación Vlans agregadas .....	28
Figura 22 Direccionamiento IP de PC - SWAA .....	29
Figura 23 Direccionamiento IP de PC - SWBB.....	30
Figura 24 Direccionamiento IP de PC - SWCC.....	31
Figura 25 Ping desde cada PC1 a los demás .....	33
Figura 26 Ping desde cada PC a los demás .....	33
Figura 27 Ping desde SWAA a SWBB y SWCC (Escenario 2) .....	34
Figura 28 Ping desde SWCC a SWBB y SWAA (Escenario 2) .....	35
Figura 29 Ping desde SWBB a SWAA y SWCC (Escenario 2) .....	35
Figura 30 Ping desde SWAA a los Pc (Escenario 2) .....	36

## LISTA DE TABLAS

Tabla 1 configuración Routes – Escenario 1.....	13
Tabla 2 Direccionamiento de los PCs (Escenario 2).....	28
Tabla 3 Direccionamiento SVI (Escenario 2) .....	32

## GLOSARIO

**Topología de red:** mapa físico o lógico de una red para intercambiar datos.

**Router:** producto de hardware que permite interconectar redes de datos, se encarga de establecer la mejor ruta.

**EIGRP:** protocolo de Enrutamiento de Puerta de enlace Interior Mejorado.

**Switch:** dispositivo de interconexión de equipos a nivel local  
**Consola:** método que permite a las personas dar instrucciones a algún programa informático.

**Sistema Autónomo:** grupo de redes IP que poseen una política de rutas propia e Independiente

**Dirección IP:** Dirección de protocolo de Internet, la forma estándar de identificar un equipo que está conectado a Internet, de forma similar a como un número de teléfono identifica un aparato de teléfono en una red telefónica.

**EIGRP:** sesiones externas de BGP

**Interface Loopback:** interfaz de red virtual, son usualmente utilizadas para probar la capacidad de la tarjeta interna si se están enviando datos BGP.

**OSPF:** Camino más cortó abierto; protocolo de enrutamiento que proporciona la ruta más corta.

**VLAN:** Red Virtual de Área Local; arreglo lógico que distingue un conjunto de paquetes de otros independizándolos.



## **RESUMEN**

El desarrollo de esta actividad final del diplomado de profundización CCNP denominada “Prueba de habilidades prácticas”, permite el desarrollo de la capacidad de configurar y verificar operaciones básicas de enrutamiento interno (IGP), enrutamiento externo (EGP), así como la administración eficiente de vlans y enlaces troncales; mediante el uso de comandos específicos con el fin identificar y resolver problemas de conectividad y actualización de tablas de enrutamiento.

En la actividad tenemos escenarios de topologías de redes, con el desarrollo de estos dos ejercicios se podrá identificar el nivel de conocimiento, competencias y habilidades adquiridas durante el desarrollo del curso Diplomado CCNP (Cisco Certified Network Professional). El primer escenario de intercambio de información de enrutamiento entre diferentes sistemas autónomos mediante el protocolo BGP; y un segundo escenario de administración de redes de área local, para la implementación de VLAN, proporcionando segmentación y flexibilidad organizativa, haciendo uso del protocolo VTP, y de la configuración de enlaces troncales mediante el protocolo DTP.

## **ABSTRACT**

The development of this final activity of the CCNP deepening diploma called "Practical skills test", allows the development of the ability to configure and verify basic operations of internal routing (IGP), external routing (EGP), as well as the efficient administration of vlans and trunk links; by using specific commands to identify and resolve connectivity problems and update routing tables.

In the activity we have scenarios of network topologies, with the development of these two exercises the level of knowledge, competences and skills acquired during the development of the CCNP (Cisco Certified Network Professional) Diploma course can be identified. The first scenario of routing information exchange between different autonomous systems using the BGP protocol; and a second local area network administration scenario, for the implementation of VLANs, providing segmentation and organizational flexibility, making use of the VTP protocol, and the configuration of trunks using the DTP protocol.

## **INTRODUCCIÓN**

Dentro de la estructura de este documento podemos hallar el desarrollo de la actividad llamada “Prueba de habilidades” la cual está diseñada para abordar los conocimientos adquiridos en el Diplomado de profundización CCNP.

La actividad se compone de dos ejercicios, llamados escenario uno y escenario dos respectivamente, cuya finalidad es aplicar habilidades para lograr dar con soluciones relacionadas con aspectos de networking.

En el escenario uno, tenemos una topología de la red donde debemos aplicar los diferentes lineamientos de administración y gestión en redes conmutadas y enrutadas. El objetivo es poner en marcha y verificar el funcionamiento de la red a través del protocolo EIGRP. Lograr establecer las relaciones de vecinos entre los diferentes routers.

En segundo lugar, tenemos un escenario donde se logra evidenciar la configuración de una pequeña red estructurada por switches capa dos y PCs, en la cual se configura el enrutamiento IPv4 respectivo, se implementa protocolos como VLAN Trunking Protocol y Dynamic Trunking Protocol.

## Desarrollo del trabajo

### Escenario 1

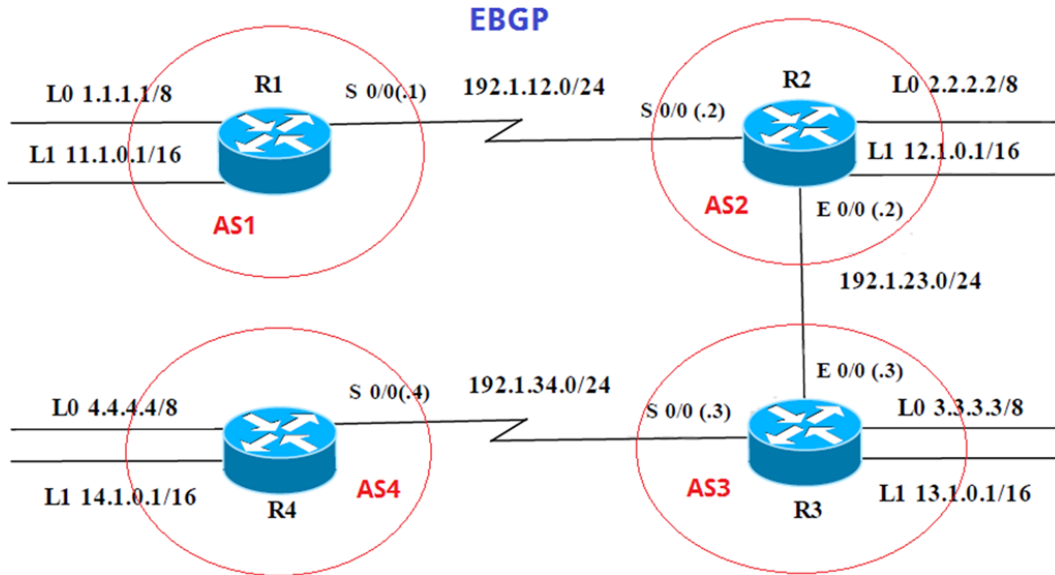


Figura 2 Topología Escenario 1

Interfaz	Dirección IP	Máscara	
<b>R1</b>	<b>Loopback 0</b>	1.1.1.1	255.0.0.0
	<b>Loopback 1</b>	11.1.0.1	255.255.0.0
	<b>S 0/0</b>	192.1.12.1	255.255.255.0

Interfaz	Dirección IP	Máscara	
<b>R2</b>	<b>Loopback 0</b>	2.2.2.2	255.0.0.0
	<b>Loopback 1</b>	12.1.0.1	255.255.0.0
	<b>S 0/0</b>	192.1.12.2	255.255.255.0
	<b>E 0/0</b>	192.1.23.2	255.255.255.0

	Interfaz	Dirección IP	Máscara
<b>R3</b>	<b>Loopback 0</b>	3.3.3.3	255.0.0.0
	<b>Loopback 1</b>	13.1.0.1	255.255.0.0
	<b>E 0/0</b>	192.1.23.3	255.255.255.0
	<b>S 0/0</b>	192.1.34.3	255.255.255.0

	Interfaz	Dirección IP	Máscara
<b>R4</b>	<b>Loopback 0</b>	4.4.4.4	255.0.0.0
	<b>Loopback 1</b>	14.1.0.1	255.255.0.0
	<b>S 0/0</b>	192.1.34.4	255.255.255.0

**Tabla 1 configuración Routes – Escenario 1**

Configuración básica inicial para cada uno de los routers.

```
R1
configure terminal
hostname R1
interface serial 1/0
ip add 192.1.12.1 255.255.255.0
clock rate 64000
no shutdown
exit
interface Loopback0
ip address 1.1.1.1 255.0.0.0
interface Loopback1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
```

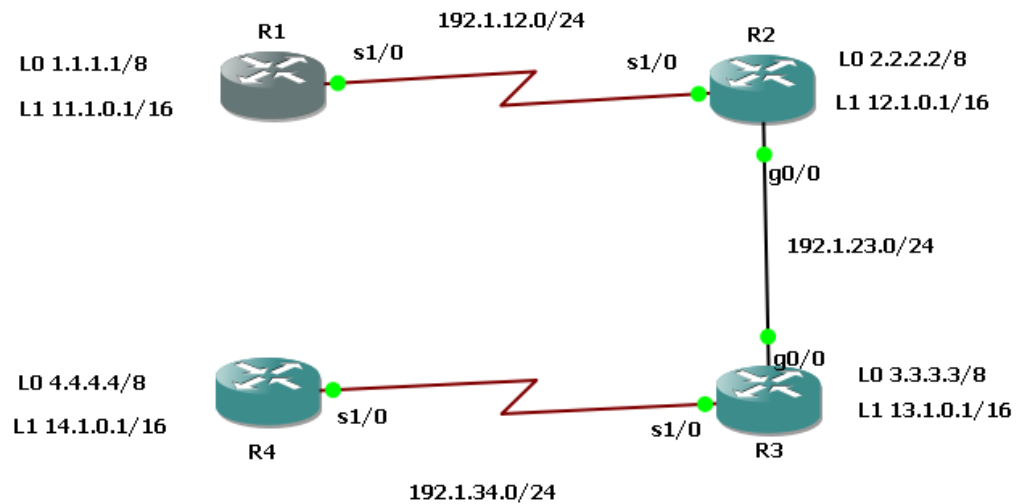
```
R2
configure terminal
hostname R2
interface serial 1/0
ip address 192.1.12.2 255.255.255.0
no shutdown
interface Loopback0
ip address 2.2.2.2 255.0.0.0
interface Loopback1
ip address 12.1.0.1 255.255.0.0
interface gigabitEthernet 0/0
ip address 192.1.23.2 255.255.255.0
no shutdown
```

R3

```
configure terminal
hostname R3
interface serial 1/0
ip address 192.1.34.3 255.255.255.0
no shutdown
interface g0/0
ip address 192.1.23.3 255.255.255.0
no shutdown
interface lo0
ip address 3.3.3.3 255.0.0.0
interface lo1
ip address 13.1.0.1 255.255.0.0
```

R4

```
configure terminal
hostname R4
interface s0/0/0
ip address 192.1.34.4 255.255.255.0
clock rate 64000
no shutdown
description conecta con R3
interface lo0
ip address 4.4.4.4 255.0.0.0
interface lo1
ip address 14.1.0.1 255.255.0.0
```



**Figura 3 Escenario 1 GNS3 - Autoría propia.**

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**.

R1  
 router bgp 1  
 neighbor 192.1.12.2 remote-as 2  
 network 1.1.1.1 mask 255.0.0.0  
 network 11.1.0.1 mask 255.255.0.0  
 bgp router-id 22.22.22.22

R2  
 router bgp 2  
 neighbor 192.1.12.1 remote-as 1  
 network 2.2.2.2 mask 255.0.0.0  
 network 12.1.0.1 mask 255.255.0.0  
 bgp router-id 33.33.33.33

```

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, + - replicated route

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
  11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    11.1.0.0/16 is directly connected, Loopback1
L    11.1.0.1/32 is directly connected, Loopback1
  192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.12.0/24 is directly connected, Serial1/0
L    192.1.12.1/32 is directly connected, Serial1/0

```

**Figura 4 Enrutamiento de R1 con respecto a R2 - Escenario 1**

```

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, + - replicated route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:01:13
  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, 00:01:13
  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

```

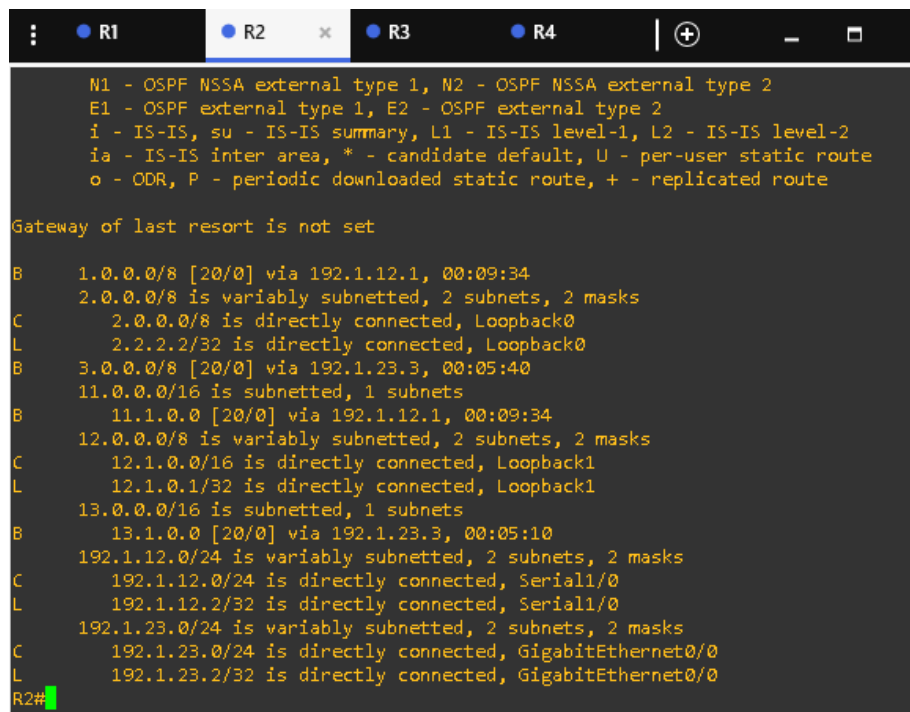
**Figura 5 Enrutamiento de R2 con respecto a R1 - Escenario 1**



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**.

```
R2(config)#router bgp 2
R2(config-router)#neighbor 192.1.23.3 remote-as 3
```

```
R3(config)#router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#no synchronization
R3(config-router)#neighbor 192.1.23.2 remote-as 2
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
```



```

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, + - replicated route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:09:34
C    2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
L    2.0.0.0/8 is directly connected, Loopback0
L    2.2.2.2/32 is directly connected, Loopback0
B    3.0.0.0/8 [20/0] via 192.1.23.3, 00:05:40
L    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 192.1.12.1, 00:09:34
C    12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
L    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, 00:05:10
C    192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
L    192.1.12.0/24 is directly connected, Serial1/0
L    192.1.12.2/32 is directly connected, Serial1/0
C    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
L    192.1.23.0/24 is directly connected, GigabitEthernet0/0
L    192.1.23.2/32 is directly connected, GigabitEthernet0/0
R2#
```

**Figura 6 Enrutamiento de R2 con respecto a R3 - Escenario 1**

```

R1 R2 R3 R4
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, + - replicated route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:07:28
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:07:28
    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, 00:07:28
    12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 192.1.23.2, 00:07:28
    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
    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#

```

**Figura 7 Enrutamiento de R3 con respecto a R2 - Escenario 1**

- 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:

```

R3(config)#router bgp 3
R3(config-router)# neighbor 192.1.34.4 remote-as 4

```

R4:

```
router bgp 4
neighbor 192.1.34.3 remote-as 3
network 14.1.0.1 mask 255.255.0.0
network 4.4.4.4 mask 255.0.0.0
bgp router-id 66.66.66.66
```



```

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, + - replicated route

Gateway of last resort is not set

B   1.0.0.0/8 [20/0] via 192.1.23.2, 00:10:30
B   2.0.0.0/8 [20/0] via 192.1.23.2, 00:10:30
   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, 00:00:22
   11.0.0.0/16 is subnetted, 1 subnets
B   11.1.0.0 [20/0] via 192.1.23.2, 00:10:30
   12.0.0.0/16 is subnetted, 1 subnets
B   12.1.0.0 [20/0] via 192.1.23.2, 00:10:30
   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
   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#
```

**Figura 8 Enrutamiento de R3 con respecto a R4 - Escenario 1**

```

R1 R2 R3 R4 x + - □ >
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, + - replicated route

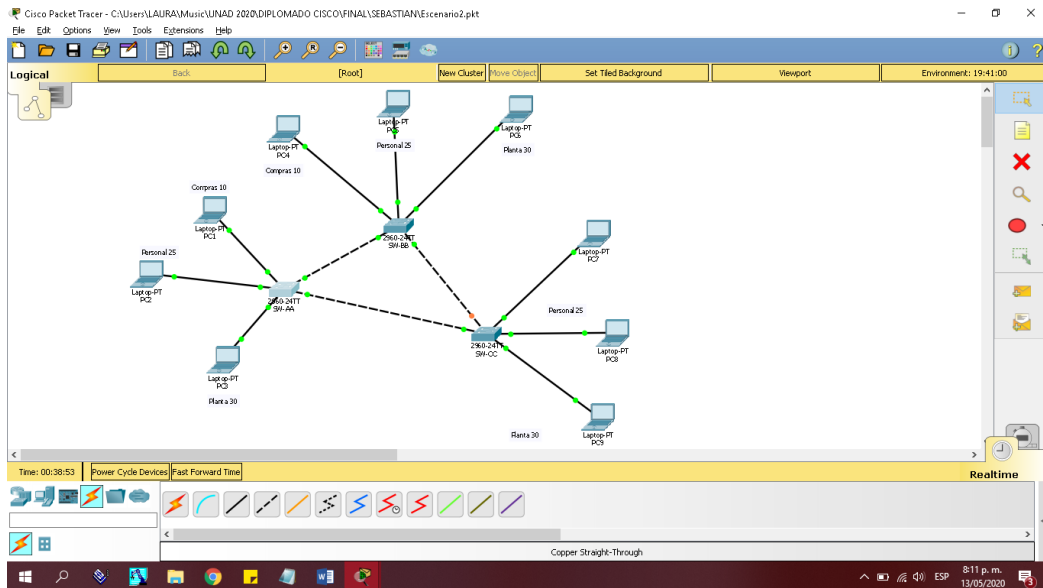
Gateway of last resort is not set

B   1.0.0.0/8 [20/0] via 192.1.34.3, 00:02:27
B   2.0.0.0/8 [20/0] via 192.1.34.3, 00:02:27
B   3.0.0.0/8 [20/0] via 192.1.34.3, 00:02:27
C   4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   4.0.0.0/8 is directly connected, Loopback0
L   4.4.4.4/32 is directly connected, Loopback0
B   11.0.0.0/16 is subnetted, 1 subnets
B   11.1.0.0 [20/0] via 192.1.34.3, 00:02:27
B   12.0.0.0/16 is subnetted, 1 subnets
B   12.1.0.0 [20/0] via 192.1.34.3, 00:02:27
B   13.0.0.0/16 is subnetted, 1 subnets
B   13.1.0.0 [20/0] via 192.1.34.3, 00:02:27
C   14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   14.1.0.0/16 is directly connected, Loopback1
L   14.1.0.1/32 is directly connected, Loopback1
C   192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.1.34.0/24 is directly connected, Serial11/0
L   192.1.34.4/32 is directly connected, Serial11/0
R4#

```

**Figura 9 Enrutamiento de R4 con respecto a R3 - Escenario 1**

## Escenario 2



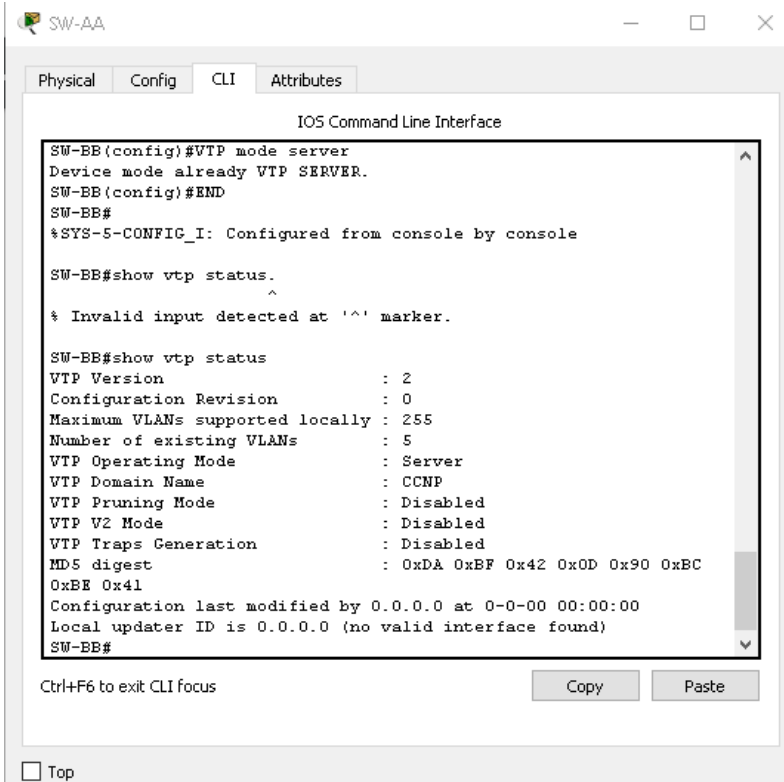
**Figura 11 Topología Escenario 2**

## A. Configurar VTP

1. Todos los switches se configurarán para usar VTP para las actualizaciones de VLAN. El switch SW-BB se configurará como el servidor. Los switches SW-AA y SW-CC se configurarán como clientes. Los switches estarán en el dominio VPT llamado CCNP y usando la contraseña cisco.

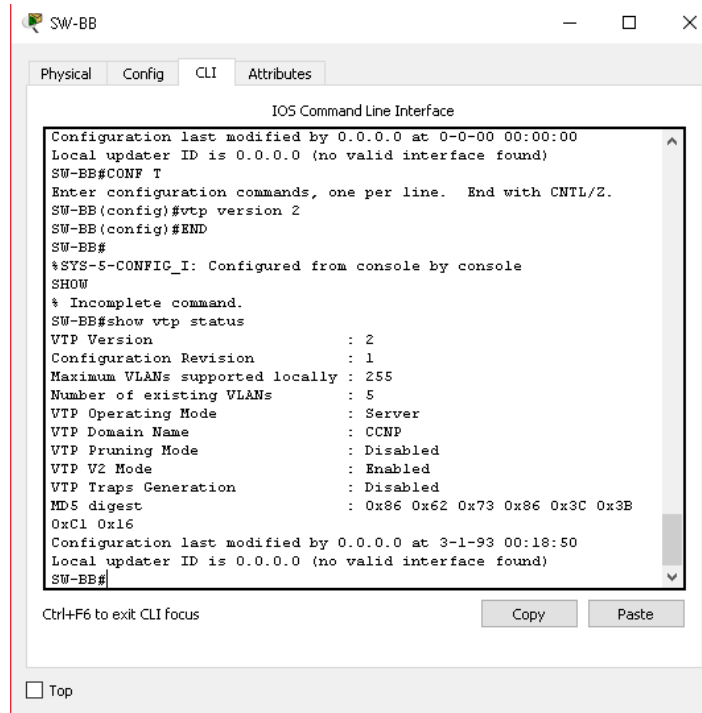
hostname SW-AA vtp mode client vtp domain CCNP vtp versión 2 vtp password cisco	hostname SW-BB vtp domain CCNP vtp version 2 vtp mode server vtp password cisco	hostname SW-CC vtp mode client vtp domain CCNP vtp versión 2 vtp password cisco
---	---	---

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

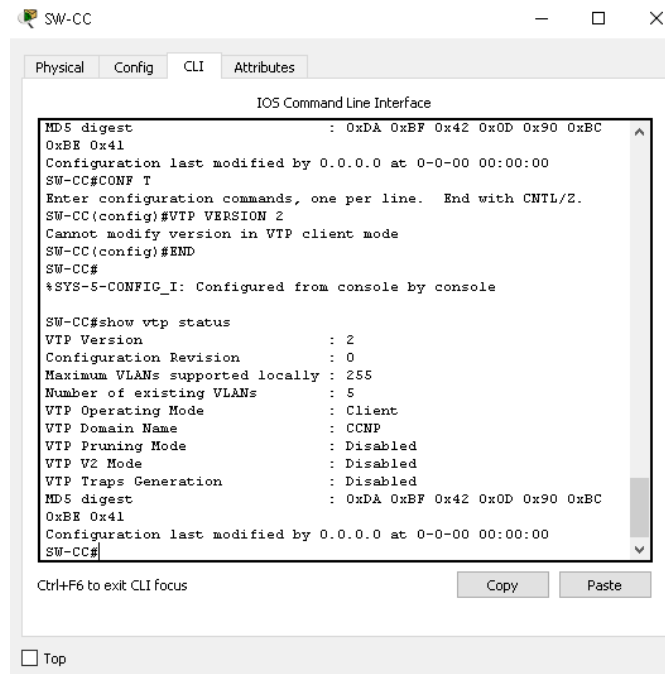


```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
SW-BB(config)#VTP mode server
Device mode already VTP SERVER.
SW-BB(config)#END
SW-BB#
#SYS-5-CONFIG_I: Configured from console by console
SW-BB#show vtp status.
^
# Invalid input detected at '^' marker.
SW-BB#show vtp status
VTP Version          : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode    : Server
VTP Domain Name       : CCNP
VTP Pruning Mode      : Disabled
VTP V2 Mode           : Disabled
VTP Traps Generation  : Disabled
MD5 digest            : 0xD& 0xBF 0x42 0x0D 0x90 0xBC
0xBE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
SW-BB#
```

**Figura 12 Verificación Vtp status en SWAA - Escenario 2**



**Figura 13 Verificación Vtp status en SWBB - Escenario 2**



**Figura 14 Verificación Vtp status en SWCC - Escenario 2**

## **B. Configurar DTP (Dynamic Trunking Protocol)**

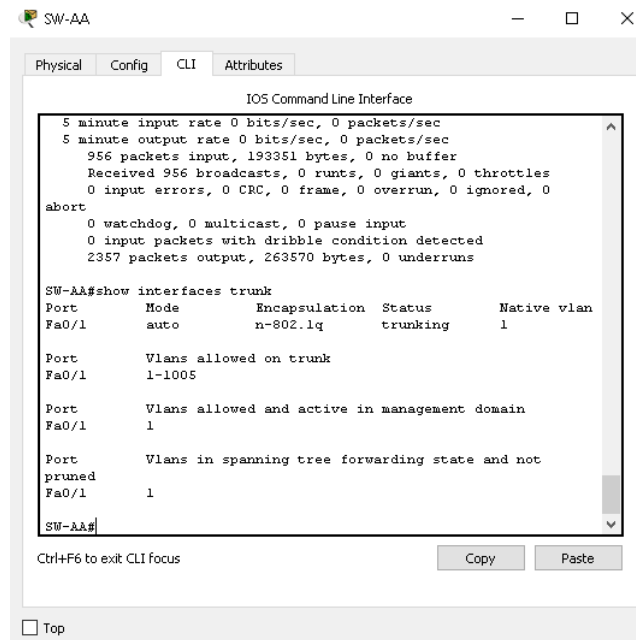
3. Configure un enlace troncal ("trunk") dinámico entre SW-AA y SW-BB. Debido a que el modo por defecto es dynamic auto, solo un lado del enlace debe configurarse como dynamic desirable.

Ya que el modo por defecto es dynamic auto, solo un lado del enlace debe configurarse como dynamic desirable en mi caso, configuraré SWBB.

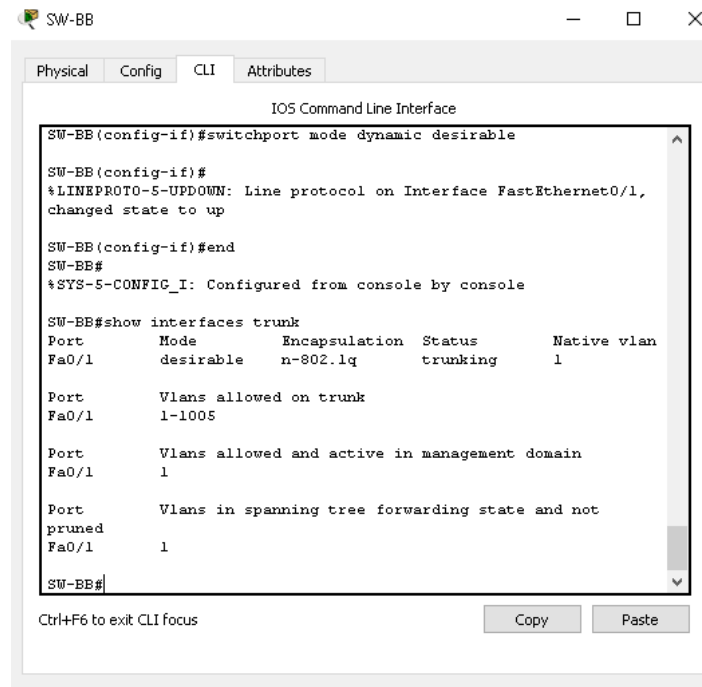
```
SWAA  
int f0/1  
switchport mode dynamic auto
```

```
SWBB  
int f0/1  
switchport mode dynamic desirable
```

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



**Figura 15 Verificación interface troncal de SWBB a SWAA Escenario 2**



**Figura 16 Verificación interface troncal de SWBB a SWAA Escenario 2**

- Entre SW-AA y SW-BB configure un enlace "trunk" estático utilizando el comando



**switchport mode trunk** en la interfaz F0/3 de SW-AA

Int f0/3  
switchport mode trunk

```
SW-AA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-AA(config)#Int f0/3
SW-AA(config-if)#switchport mode trunk

SW-AA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to up
```

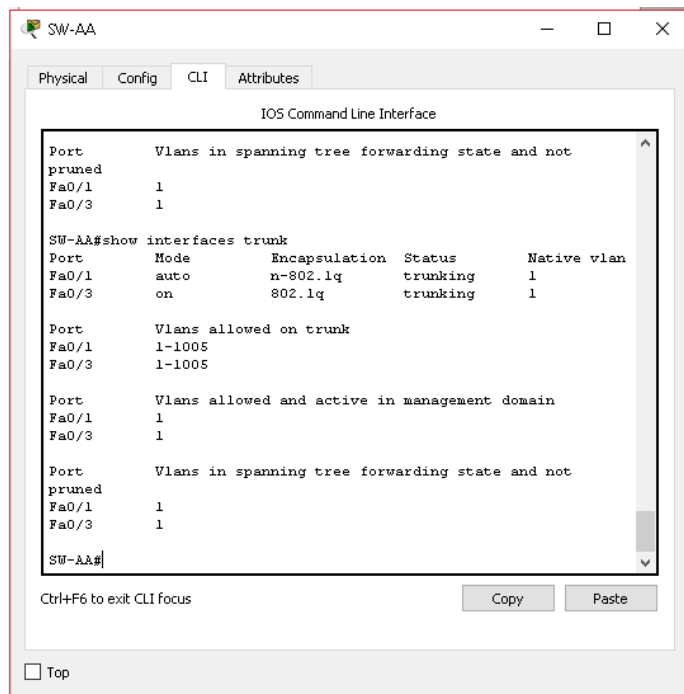
Ctrl+F6 to exit CLI focus

Copy Paste

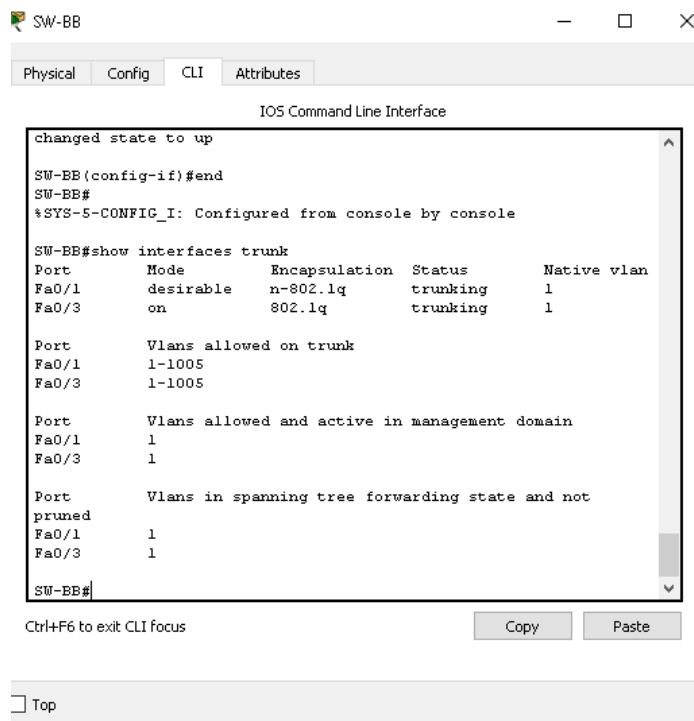
Top

**Figura 17** configuración un enlace trunk SWAA

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



**Figura 18 Verificación interface troncal de SWAA a SWCC**



**Figura 19 Verificación interface troncal de SWBB a SWCC**

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

## SWBB

Int f0/3  
switchport mode trunk

## SWCC

Int f0/3  
switchport mode trunk

### 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)

SWAA(config)#VLAN 10 VTP VLAN configuration not allowed when device is in CLIENT mode.

La Vlan 10

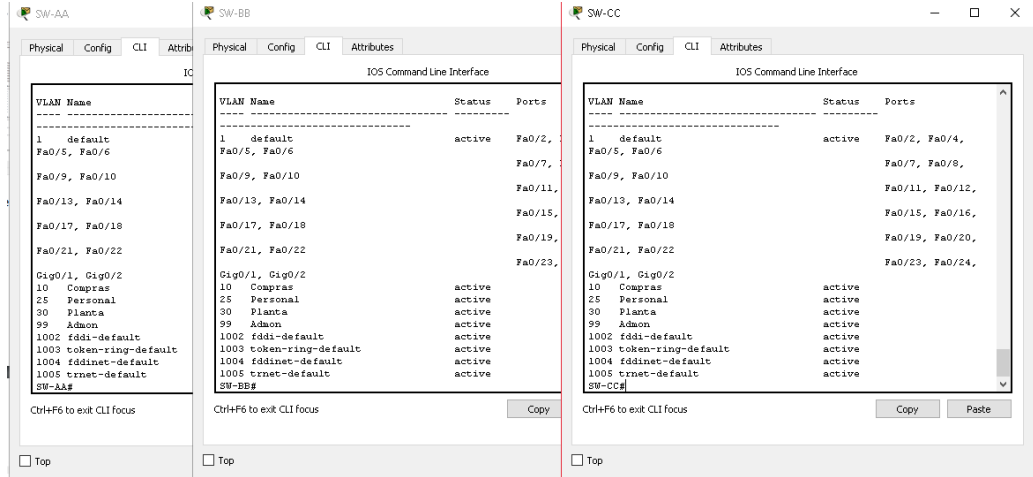
no permite cuando existe una configuración VTP VLAN además el dispositivo está en modo cliente; solo configurando el switch SW-BB aparecen las vlan en el switch SW-AA.

```
SWAA(config)#VLAN 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
SWAA(config)#
SWAA(config)#
```

**Figura 20 Configuración de VLAN en SWAA**

```
vlan 10
name Compras
vlan 25
name Personal
vlan 30
name Planta
vlan 99
name Admon
```

9. Verifique que las VLANs han sido agregadas correctamente.

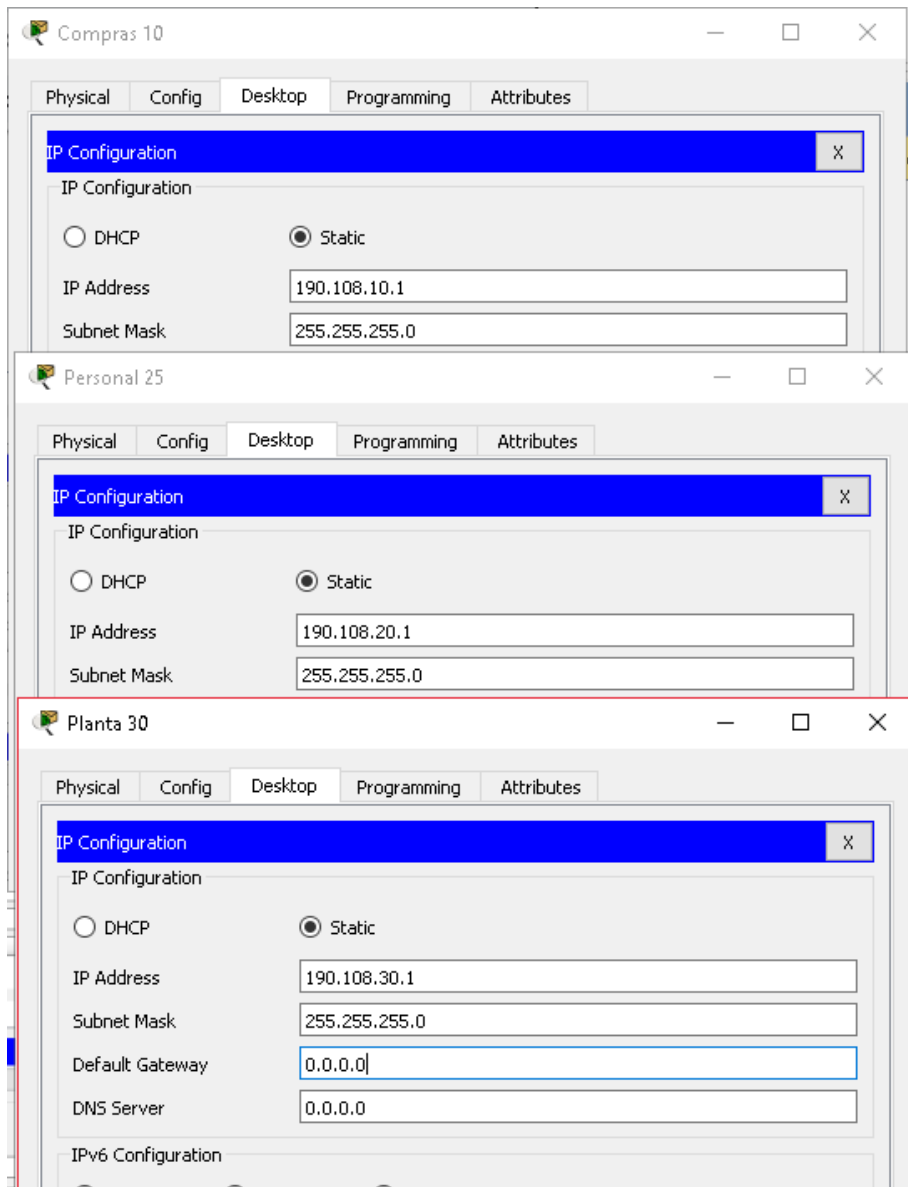


**Figura 21 Verificación Vlans agregadas**

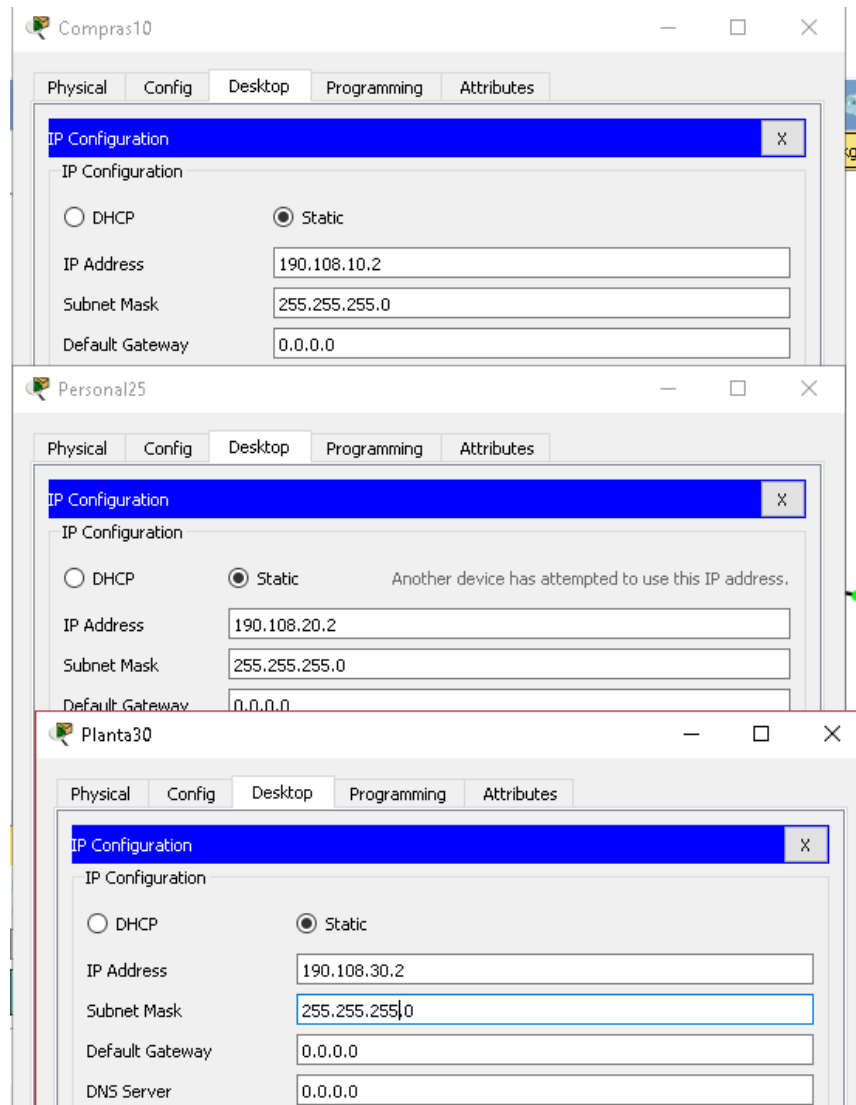
10. Asocie los puertos a las VLAN y configure las direcciones IP de acuerdo con la siguiente tabla.

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

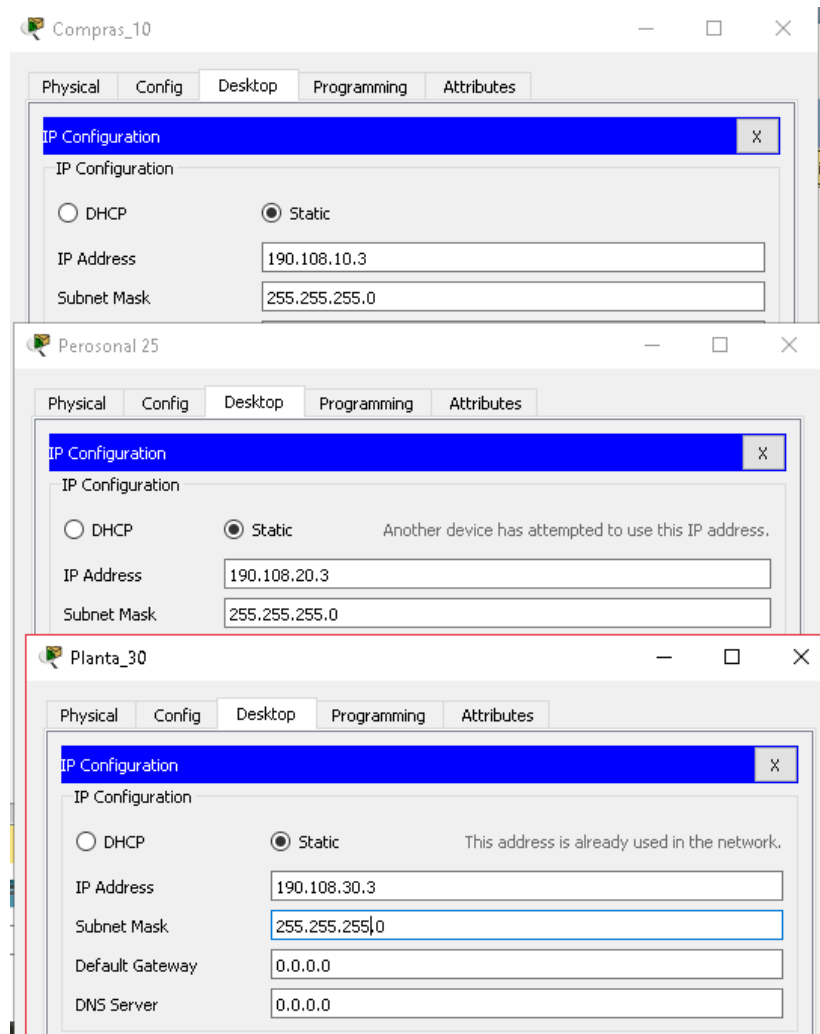
**Tabla 2 Direccionamiento de los PCs (Escenario 2)**



**Figura 22 Direcccionamiento IP de PC - SWAA**



**Figura 23** Direcccionamiento IP de PC - SWBB



**Figura 24 Direcccionamiento IP de PC - SWCC**

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

<pre>interface fastEthernet 0/10 switchport mode access switchport access vlan 10 No shutdown</pre>	<pre>interface fastEthernet 0/10 switchport mode access switchport access vlan 10</pre>	<pre>interface fastEthernet 0/10 switchport mode access switchport access vlan 10</pre>
---	---	---

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.

<b>SWAA:</b>  interface f0/15 switchport mode access switchport access vlan 25 interface fastEthernet 0/20 switchport mode access switchport access vlan 30	<b>SWBB:</b>  interface fastEthernet 0/15 switchport mode access switchport access vlan 25 interface fastEthernet 0/20 switchport mode access switchport access vlan 30	<b>SWCC:</b>  interface fastEthernet 0/15 switchport mode access switchport access vlan 25 interface fastEthernet 0/20 switchport mode access switchport access vlan 30
--	--	--

**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	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

**Tabla 3 Direccionamiento SVI (Escenario 2)**

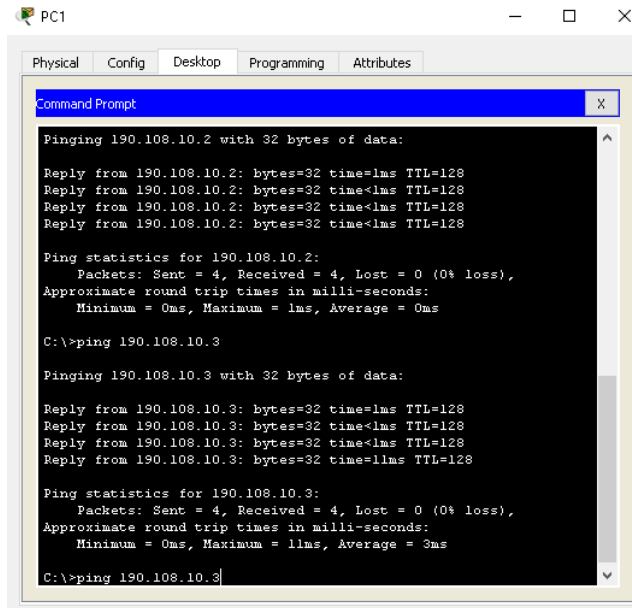
SW- AA Vlan 99 Interface vlan 99 Ip address 190.108.99.1 255.255.255.0	SW - BB Vlan 99 Interface vlan 99 Ip address 190.108.99.2 255.255.255.0	SW – CC Vlan 99 Interface vlan 99 Ip address 190.108.99.3 255.255.255.0
--	---	---

**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

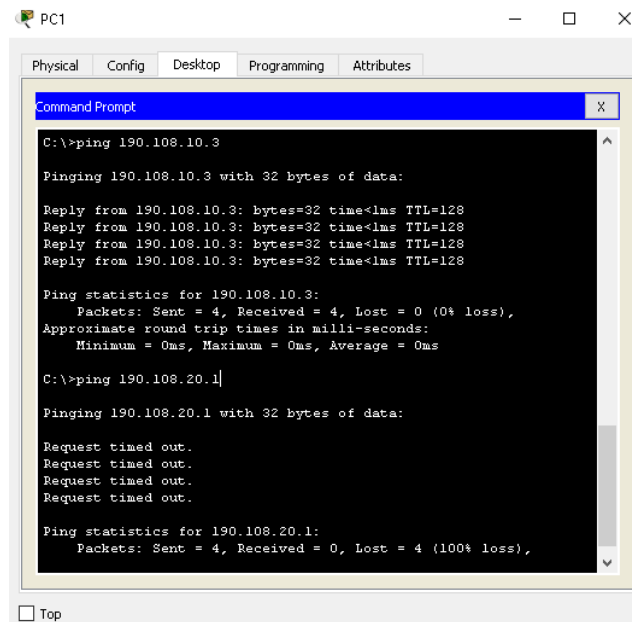


éxito.



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
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
C:\>ping 190.108.10.3
Pinging 190.108.10.3 with 32 bytes of data:
Reply from 190.108.10.3: bytes=32 time<1ms TTL=128
Reply from 190.108.10.3: bytes=32 time<1ms TTL=128
Reply from 190.108.10.3: bytes=32 time<1ms TTL=128
Reply from 190.108.10.3: bytes=32 time=11ms TTL=128
Ping statistics for 190.108.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 3ms
C:\>ping 190.108.10.3
```

**Figura 25** Ping desde cada PC1 a los demás

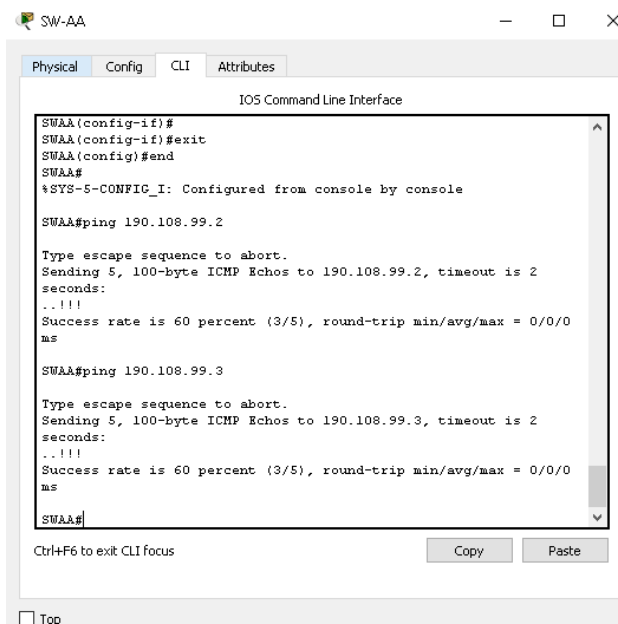


```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 190.108.10.3
Pinging 190.108.10.3 with 32 bytes of data:
Reply from 190.108.10.3: bytes=32 time<1ms TTL=128
Reply from 190.108.10.3: bytes=32 time<1ms TTL=128
Reply from 190.108.10.3: bytes=32 time<1ms TTL=128
Reply from 190.108.10.3: bytes=32 time<1ms TTL=128
Ping statistics for 190.108.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping 190.108.20.1
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),
```

**Figura 26** Ping desde cada PC a los demás

Los PC que tienen la misma vlan y están en la misma red, su ping es exitoso, aquellos que tienen la vlan diferente el ping no es exitoso, esto se debe a que se está estableciendo comunicación entre switch por truncamiento, y entre los pc por medio de las vlan. Por eso se puede comunicar un pc con la misma vlan y red que se encuentra conectado en otro switch.

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



```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
SWAA(config-if)#
SWAA(config-if)#exit
SWAA(config)#end
SWAA#
%SYS-5-CONFIG_I: Configured from console by console
SWAA#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 = 0/0/0
ms
SWAA#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
SWAA#
```

**Figura 27 Ping desde SWT1 a SWBB y SWCC (Escenario 2)**

```
SW-BB
Physical Config CLI Attributes
IOS Command Line Interface
SWBB(config-if)#exit
SWBB(config)#interface fastEthernet 0/15
SWBB(config-if)#switchport mode access
SWBB(config-if)#switchport access vlan 25
SWBB(config-if)#interface fastEthernet 0/20
SWBB(config-if)#switchport mode access
SWBB(config-if)#switchport access vlan 30
SWBB(config-if)#end
SWBB#
%SYS-5-CONFIG_I: Configured from console by console
SWBB#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
SWBB#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
SWBB#
```

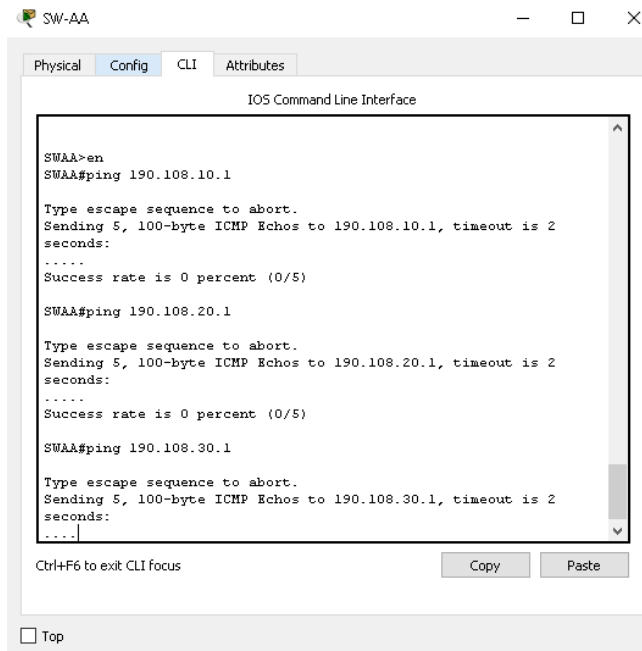
**Figura 28 Ping desde SWT1 a SWBB y SWAA (Escenario 1)**

```
SW-CC
Physical Config CLI Attributes
IOS Command Line Interface
SWCC(config-if)#interface fastEthernet 0/20
SWCC(config-if)#switchport mode access
SWCC(config-if)#switchport access vlan 30
SWCC(config-if)#end
SWCC#
%SYS-5-CONFIG_I: Configured from console by console
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
SWCC#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
SWCC#
```

**Figura 29 Ping desde SWT2 a SWAA y SWCC (Escenario 2)**

El ping tuvo éxito debido a que los switches comparten la vlan 99, además se estableció una comunicación por truncamiento en los switch, además al asignar la interface virtual del switch, todos los switch fueron configurados con la misma vlan, en la misma red.

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



```
SWAA>en
SWAA#ping 190.108.10.1

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

SWAA#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)

SWAA#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:
.....
```

**Figura 30 Ping desde SWAA a los Pc (Escenario 2)**

El ping no fue exitoso, ya que, aunque exista comunicación por truncamiento entre los switches, los pc y sus interfaces de conexión con los switch, están onfigurados en una vlan diferente a la vlan que tienen configurado los switch

## **CONCLUSIONES**

Al finalizar el diplomado de CCNP y la prueba de habilidades el estudiante debe estar en la capacidad de desarrollar los diferentes tipos de escenarios propuestos de forma correcta haciendo uso de los simuladores propuestos, debe comprender los conceptos de switching y routing y los cuales son de utilidad para el desarrollo en general de las redes y las telecomunicaciones

Nos quedó claro que el dominio VTP, está formado con switches configurados mediante troncales ajustados bajo la misma responsabilidad administrativa. Este protocolo nos permite administrar las vlans y una de sus ventajas es que podemos simplificar la administración y configuración, acondicionando los diferentes roles (servidor o cliente).

Se logra contextualizar los conocimientos teóricos y las habilidades practicas construidas a través del curso mediante el uso de herramientas como GNS3, Packet Tracer y SmartLab de cisco.

## BIBLIOGRAFÍA

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

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

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

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-NT1IlnWR0hoMxgBNv1CJ>

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

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

UNAD (2015). Switch CISCO - Procedimientos de instalación y configuración del IOS [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1IlyYRohwtwPUV64dg>