

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JAIME ANDRES ANAYA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
INGENIERIA DE TELECOMUNICACIONES  
DIPLOMADO CISCO CCNP  
BOGOTA  
2020

PRUEBA DE HABILIDADES PRÁCTICAS

JAIME ANDRES ANAYA

Diplomado de profundización CISCO CCNP prueba de  
Habilidades prácticas

GERARDO GRANADOS ACUÑA  
Magíster en Telemática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
INGENIERIA DE TELECOMUNICACIONES  
DIPLOMADO CISCO CCNP  
BOGOTA  
2020

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

\_\_\_\_\_  
Presidente del Jurado

\_\_\_\_\_  
Jurado

\_\_\_\_\_  
Jurado

Bogotá 16 de Mayo 2020

## CONTENIDO

Tabla de contenido

<i>LISTA DE TABLAS</i> .....	5
<i>LISTA DE FIGURAS</i> .....	6
<i>GLOSARIO</i> .....	7
<i>RESUMEN</i> .....	8
<i>ABSTRACT</i> .....	9
<i>INTRODUCCIÓN</i> .....	10
<i>EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNP</i> .....	11
<i>ESCENARIO 1</i> .....	11
<i>ESCENARIO 2</i> .....	20
<i>CONCLUSIONES</i> .....	31
<i>BIBLIOGRAFÍA</i> .....	32

## LISTA DE TABLAS

Tabla 1: Información para configuración de los Routers .....	12
Tabla 2: Configuración de IP de equipos. ....	26
Tabla 3: Configuración de IP de Switch.....	28

## LISTA DE FIGURAS

Figura 1. topología establecida para escenario 1 .....	11
Figura 2. topología creada para escenario 1 .....	11
Figura 3. Configuración relación de vecino BGP entre R1 y R2.....	14
Figura 4. Configuración relación de vecino BGP entre R2 y R1.....	14
Figura 5. Configuración relación de vecino BGP entre R2 y R3.....	15
Figura 6. Configuración relación de vecino BGP entre R3 y R2.....	16
Figura 7. Configuración relación de vecino BGP entre R3 y R4.....	17
Figura 8. Configuración relación de vecino BGP entre R4 y R3.....	18
Figura 9: topología establecida para escenario 2.....	20
Figura 10: topología creada para escenario .....	20
Figura 11. Configuración VTP de SW-BB.....	21
Figura 12. Configuración VTP de SW-AA.....	21
Figura 13. Configuración VTP de SW-CC .....	22
Figura 14. Enlace troncal SW-AA .....	23
Figura 15. Enlace troncal SW-BB .....	23
Figura 16. Enlace troncal SW-AA .....	24
Figura 17. Verificación de VLANs en SW-BB.....	26
Figura 18. Verificación PING SW-AA.....	28
Figura 19. Verificación PING SW-BB.....	29
Figura 20. Verificación PING SW-CC .....	29

## GLOSARIO

**ROUTER:** dispositivo de hardware que permite la interconexión de ordenadores en red. El router o enrutador es un dispositivo que opera en capa tres de nivel de 3. Así, permite que varias redes u ordenadores se conecten entre sí y, por ejemplo, compartan una misma conexión de Internet

**SWITCH:** dispositivo analógico que permite interconectar redes operando en la capa 2 o de nivel de enlace de datos del modelo OSI u Open Systems Interconnection. Un conmutador interconecta dos o más partes de una red, funcionando como un puente que transmite datos de un segmento a otro.

**NETWORKING:** aplica a las redes de cómputo para vincular dos o más dispositivos informáticos con el propósito de compartir datos. Las redes están construidas con una mezcla de hardware y software, incluyendo el cableado necesario para conectar los equipos.

**CONECTIVIDAD:** capacidad de un ordenador, servidor, punto de red o de telecomunicaciones, de estar conectado con otro ubicado en distintos puntos geográficos.

**CCNP:** (Cisco Certified Network Professional) certificación intermedia de los diferentes cursos entregados por CISCO, tanto Enrutamiento (ROUTE) como en Conmutación (SWITCH)

**DTP:** (Dynamic Trunking Protocol) es un protocolo propietario creado por Cisco Systems que opera entre switches Cisco, el cual automatiza la configuración de trunking (etiquetado de tramas de diferentes VLAN's con ISL o 802.1Q) en enlaces Ethernet.

**VLAN:** red de área local virtual (Virtual Local Area Network o VLAN) es un segmento lógico más pequeño dentro de una gran red física cableada. Las diferentes estaciones se combinan en una solución de red independiente de su ubicación

## RESUMEN

En el presente trabajo, se realiza el desarrollo de los dos escenarios establecidos, los cuales fueron planteados para que sean parte del examen final de habilidades prácticas adquiridas por el estudiante en el presente curso de CISCO CCNP, en donde se debe aplicar cada uno de los conocimientos de Conmutación, Enrutamiento, Redes y demás saberes interiorizados en el transcurso del diplomado.

Mediante estos escenarios se el estudiante pone en práctica sus conocimientos, habilidades, aptitudes, niveles de comprensión, resolución de problemas aplicados al desarrollo de eventos reales comúnmente encontrados en entornos laborales y profesionales y a la vez comprende el funcionamiento electrónico que realizan los diferentes componentes usados en la configuración de redes, como lo son los router y switch.

**Palabras claves:** CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

## **ABSTRACT**

In the present work, the development of the two established scenarios is carried out, which were proposed so that they are part of the final exam of practical skills acquired by the student in this CISCSO CCNP course, where each of the Knowledge of Commutation, Routing, Networks and other knowledge internalized in the course of the diploma.

Through these scenarios, the student puts into practice his knowledge, abilities, aptitudes, levels of understanding, problem solving applied to the development of real events commonly found in work and professional environments, and at the same time understands the electronic functioning of the different components used in network configuration, such as routers and switches.

**Keywords:** CISCO, CCNP, Switching, Routing, Networks, Electronics.

## INTRODUCCIÓN

Durante el desarrollo de los escenarios prácticos simulados con la ayuda del software PACKET TRACER y/o GSN3, se observa inicialmente, la aplicación de las habilidades adquiridas por el estudiante dentro del modulo de enrutamiento, en donde se debe realizar la configuración de una red EBGP, con el uso de 4 router 2911, configurando sus loopback y demás interfaces, para finalmente establecer una relación de vecino BGP, en cada uno de ellos.

Seguido a esto se establecerá el desarrollo del segundo escenario en donde se evaluará las capacidades que ha adquirido el estudiante dentro del modulo de switching, a través de la configuración de una red, haciendo uso del switch 2960, realizando sus configuraciones de VLANs tanto troncales como de modo acceso, al igual que la configuración de los equipos finales que se encuentran dentro de la red.

# EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNP

## ESCENARIO 1

Figura 1. topología establecida para escenario 1

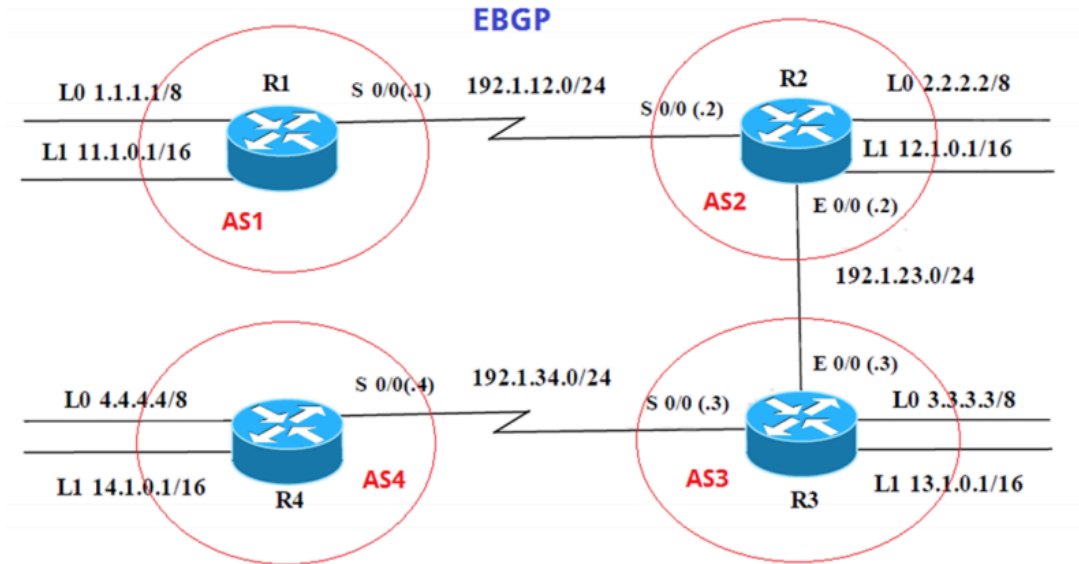


Figura 2. topología creada para escenario 1

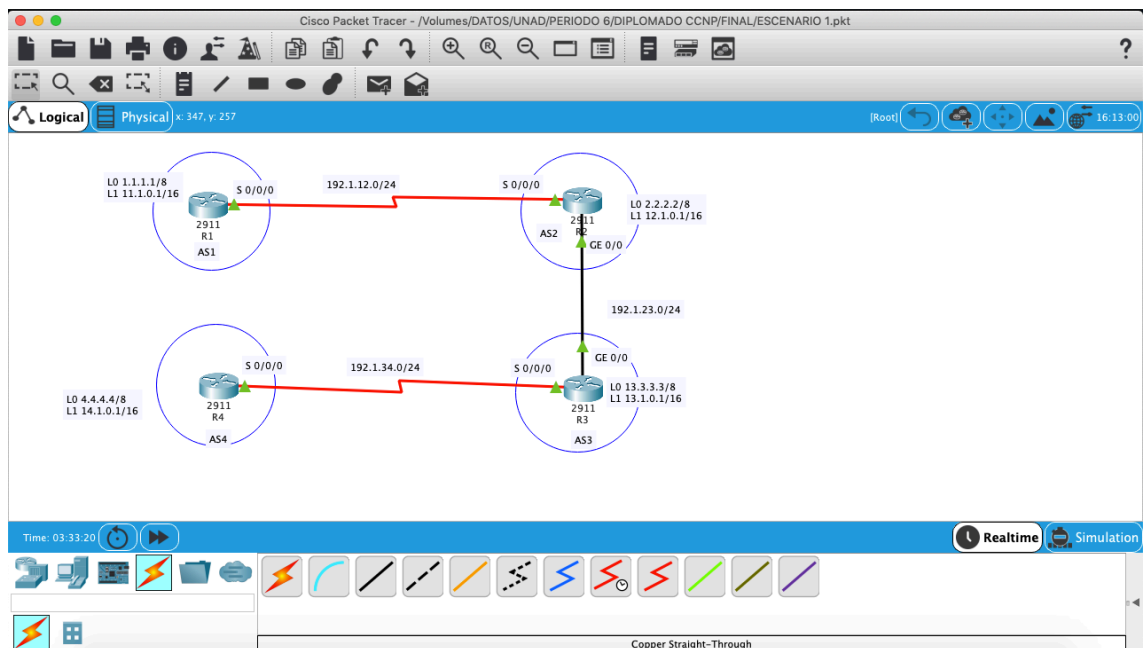


Tabla 1: Información para configuración de los Routers

<b>R1</b>	<b>Interfaz</b>	<b>Dirección IP</b>	<b>Máscara</b>
	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
<b>R2</b>	<b>Interfaz</b>	<b>Dirección IP</b>	<b>Máscara</b>
	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
<b>R3</b>	<b>Interfaz</b>	<b>Dirección IP</b>	<b>Máscara</b>
	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
<b>R4</b>	<b>Interfaz</b>	<b>Dirección IP</b>	<b>Máscara</b>
	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

### Configuración R1

```
R1#configure terminal
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface loopback0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#interface loopback1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#exit
```

### Configuración R2

```
R2#configure terminal
R2(config)#interface serial 0/0/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
```

```
R2(config-if)#exit
R2(config)#interface gigabitEthernet 0/0
R2(config-if)#ip address 192.1.23.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface loopback0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#interface loopback1
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#exit
```

### **Configuración R3**

```
R3#configure terminal
R3(config)#interface serial 0/0/0
R3(config-if)#ip address 192.1.34.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface gigabitEthernet 0/0
R3(config-if)#ip address 192.1.23.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface loopback0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#interface loopback1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#exit
```

### **Configuración R4**

```
R4#configure terminal
R4(config)#interface serial 0/0/0
R4(config-if)#ip address 192.1.34.2 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#interface loopback0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#interface loopback1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#exit
```

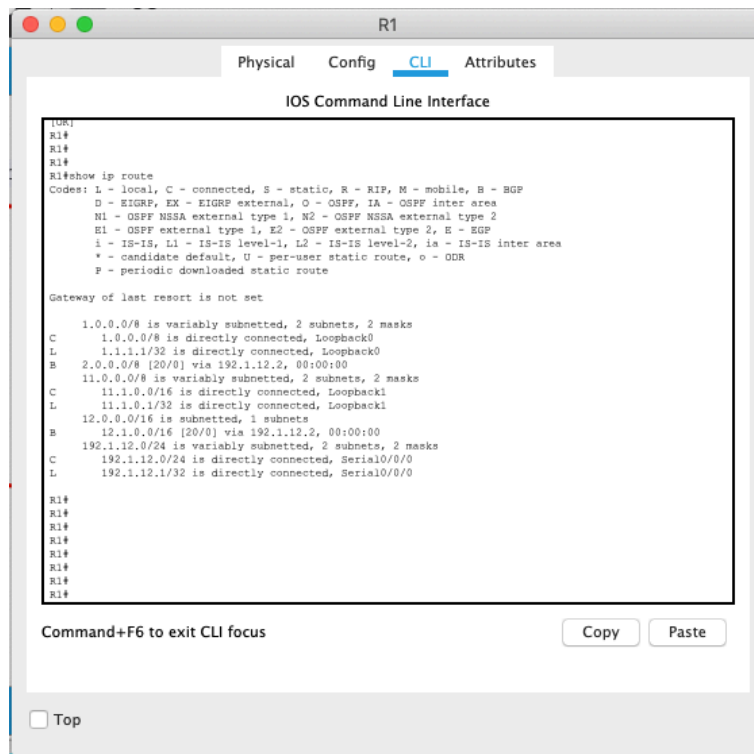
1. Configure una relación de vecino BGP entre R1 y R2. R1 debe estar en AS1 y R2 debe estar en AS2. Anuncie las direcciones de Loopback en BGP. Codifique los ID para los routers BGP como 22.22.22.22 para R1 y como 33.33.33.33 para R2. Presente el paso a con los comandos utilizados y la salida del comando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

```

R1(config)#router bgp 1
R1(config-router)#neighbor 192.1.12.2 remote-as 2
R1(config-router)#network 1.1.1.0 mask 255.0.0.0
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router)#bgp router-id 22.22.22.22

```

Figura 3. Configuración relación de vecino BGP entre R1 y R2

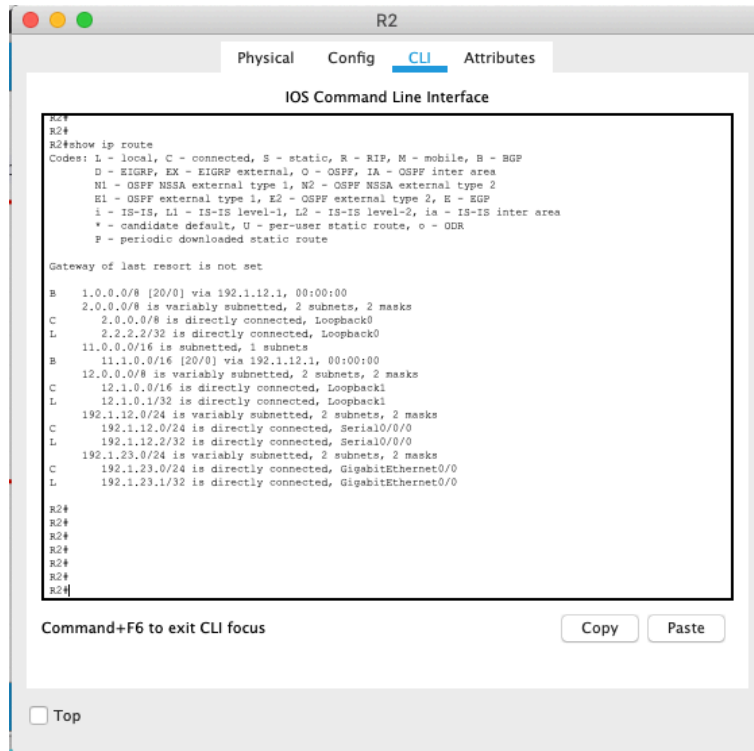


```

R2(config)#router bgp 2
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#network 2.2.2.0 mask 255.0.0.0
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
R2(config-router)#bgp router-id 33.33.33.33

```

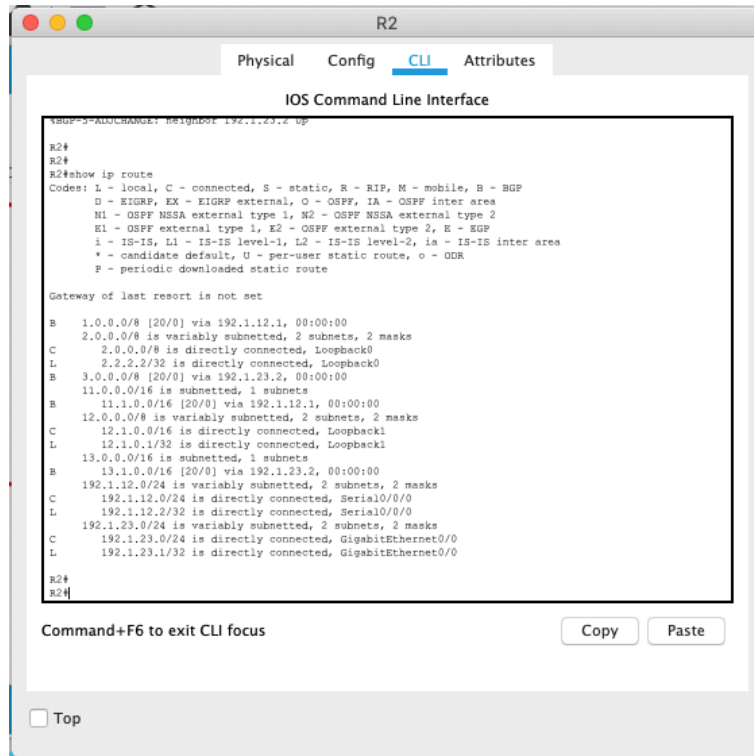
Figura 4. Configuración relación de vecino BGP entre R2 y R1



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 192.1.23.2 remote-as 3
```

*Figura 5. Configuración relación de vecino BGP entre R2 y R3*

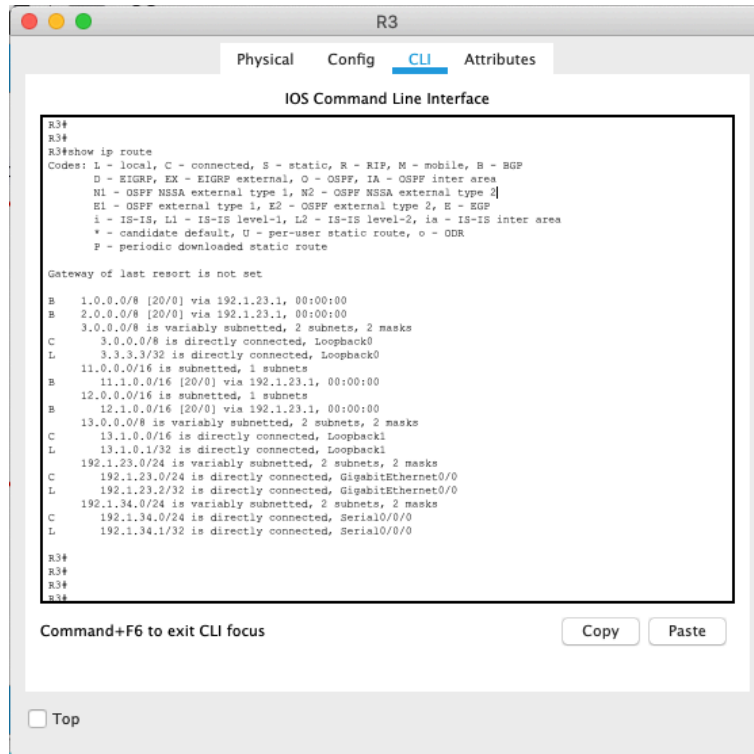


```

R3(config)#router bgp 3
R3(config-router)#neighbor 192.1.23.1 remote-as 2
R3(config-router)#network 3.3.3.0 mask 255.0.0.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3(config-router)#bgp router-id 44.44.44.44

```

Figura 6. Configuración relación de vecino BGP entre R3 y R2



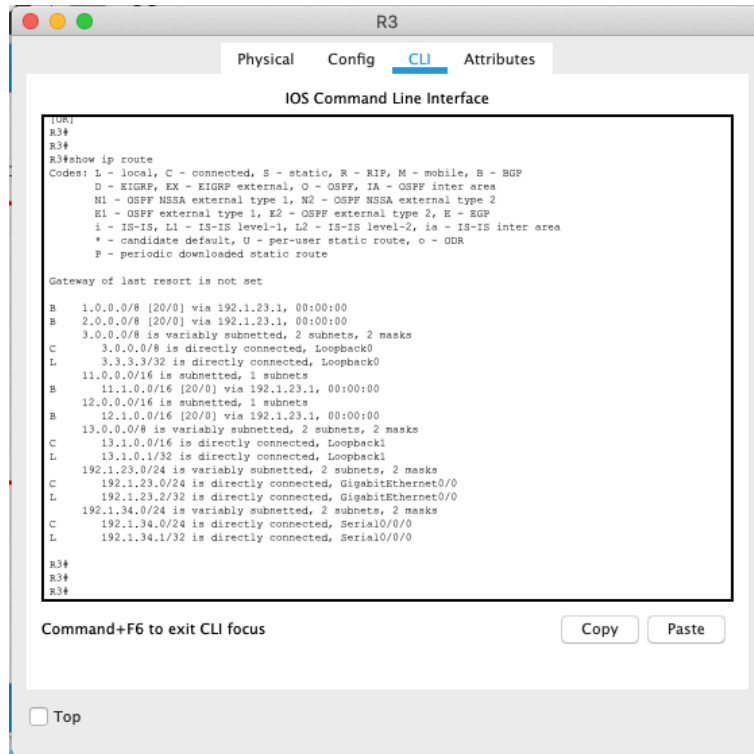
3. Configure una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en AS3 y R4 debería estar en AS4. Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como 66.66.66.66. Establezca las relaciones de vecino con base en las direcciones de Loopback 0. Cree 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 bgp 3
R3(config-router)# neighbor 4.4.4.0 remote-as 4
R3(config)#ip route 4.0.0.0 255.0.0.0 192.1.34.2

```

Figura 7. Configuración relación de vecino BGP entre R3 y R4



```

R4(config)#router bgp 4
R4(config-router)#neighbor 3.3.3.0 remote-as 3
R4(config-router)#network 14.1.0.0 mask 255.255.0.0
R4(config-router)#bgp router-id 66.66.66.66
R4(config)#ip route 3.0.0.0 255.0.0.0 192.1.34.1

```

Figura 8. Configuración relación de vecino BGP entre R4 y R3

R4

Physical Config **CLI** Attributes

IOS Command Line Interface

```
!OK
R4#
R4#
R4#
R4#
R4#
R4#
R4#
R4#
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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    3.0.0.0/8 [1/0] via 192.134.1
C    4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
L    4.0.0.0/8 is directly connected, Loopback0
L    4.4.4.4/32 is directly connected, Loopback0
C    14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
L    14.1.0.0/16 is directly connected, Loopback1
L    14.1.0.1/32 is directly connected, Loopback1
C    192.134.0/24 is variably subnetted, 2 subnets, 2 masks
L    192.134.0/24 is directly connected, Serial10/0/0
L    192.134.2/32 is directly connected, Serial10/0/0

R4#
R4#
R4#
R4#
R4#
```

Command+F6 to exit CLI focus

Copy Paste

Top

## ESCENARIO 2

Figura 9: topología establecida para escenario 2

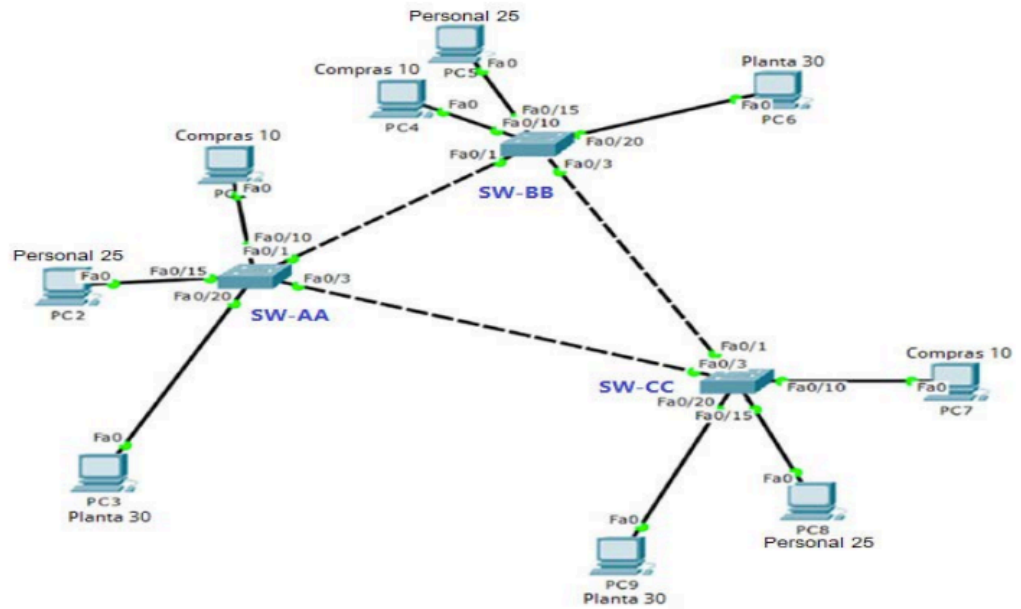
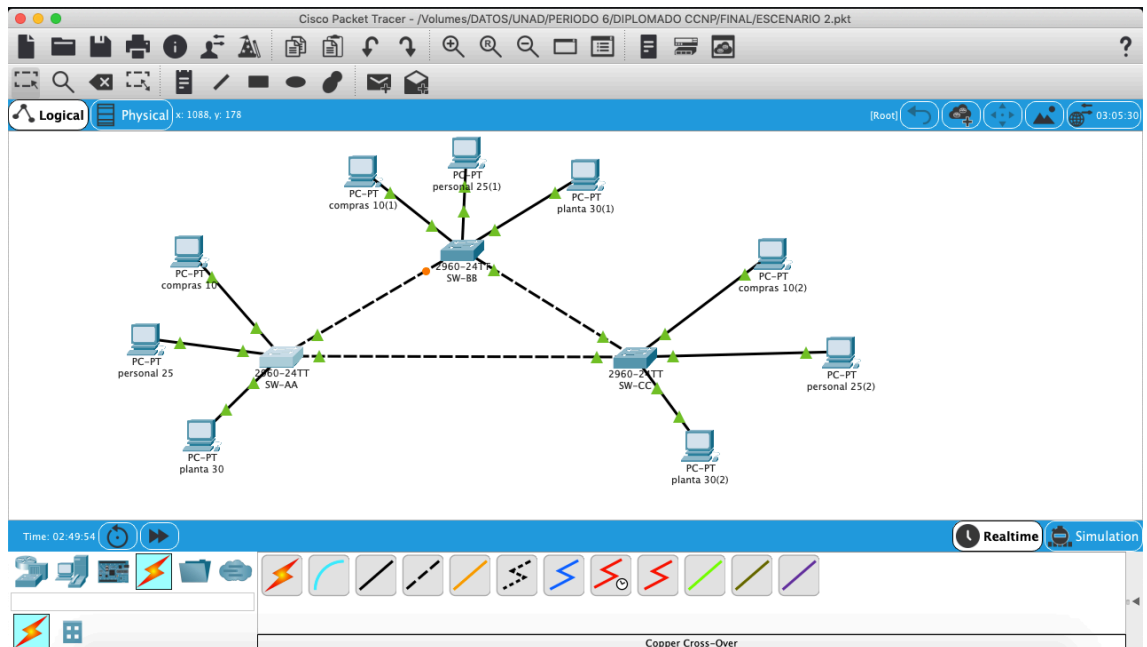


Figura 10: topología creada para escenario



### 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 VTP llamado CCNP y usando la contraseña cisco.

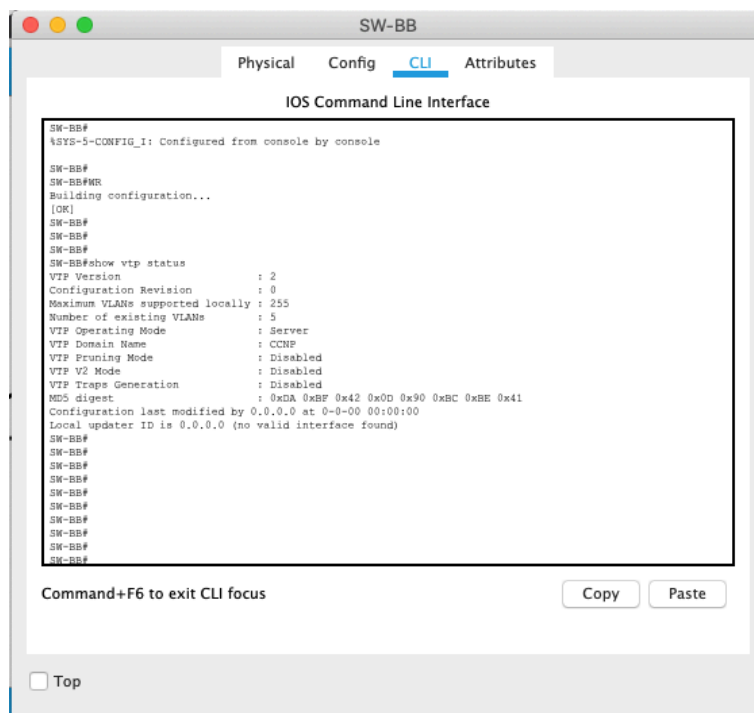
```
SW-BB(config)#vtp domain CCNP
SW-BB (config)#vtp mode server
SW-BB (config)#vtp password cisco
```

```
SW-AA (config)#vtp domain CCNP
SW-AA(config)#vtp mode client
SW-AA (config)#vtp password cisco
```

```
SW-CC(config)#vtp domain CCNP
SW-CC(config)#vtp mode client
SW-CC (config)#vtp password cisco
```

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

Figura 11. Configuración VTP de SW-BB



The screenshot shows the CLI interface of switch SW-BB. The 'CLI' tab is selected. The output of the 'show vtp status' command is displayed, showing the following details:

```
SW-BB#
\SYS-5-CONFIG_I: Configured from console by console
SW-BB#
SW-BB#
SW-BB#
SW-BB#
SW-BB#
SW-BB#
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            : 0xDA 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#
SW-BB#
SW-BB#
SW-BB#
SW-BB#
SW-BB#
SW-BB#
SW-BB#
SW-BB#
```

At the bottom of the window, there is a 'Command+F6 to exit CLI focus' message and 'Copy' and 'Paste' buttons. A 'Top' button is also visible at the bottom left.

Figura 12. Configuración VTP de SW-AA

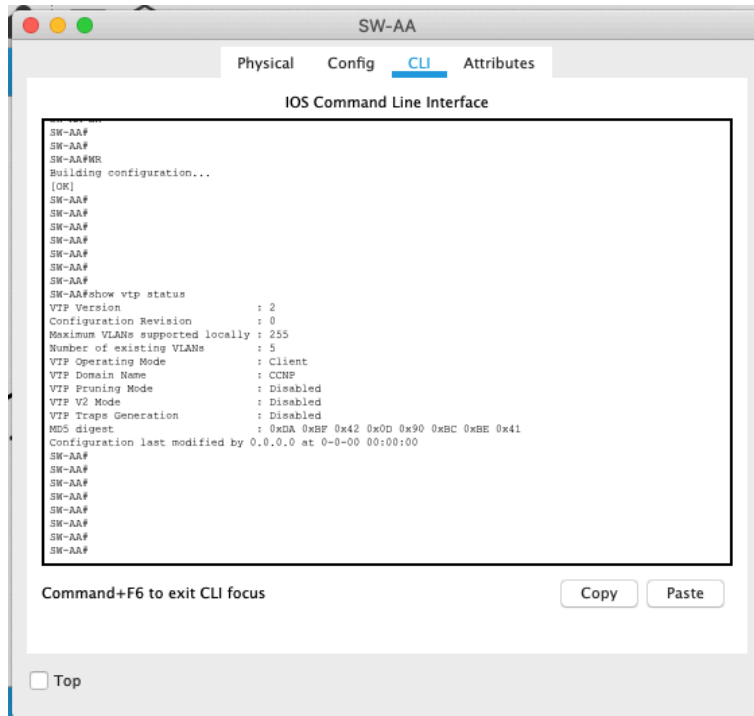
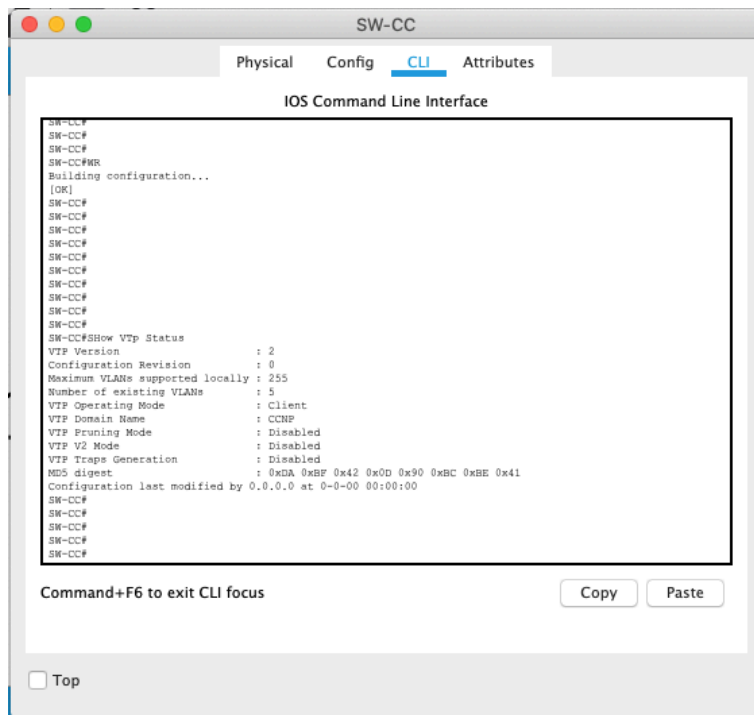


Figura 13. Configuración VTP de SW-CC



## B. Configurar DTP (Dynamic Trunking Protocol)

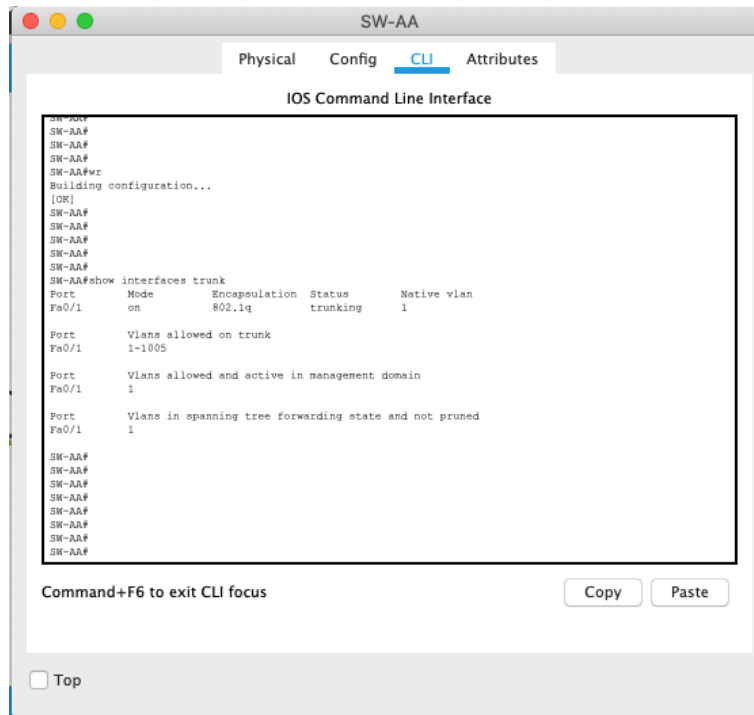
3. Configure un enlace troncal ("trunk") dinámico entre SW-AA y SW-BB. Debido a que el modo por defecto es dynamic auto, solo un lado del enlace debe configurarse como dynamic desirable.

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

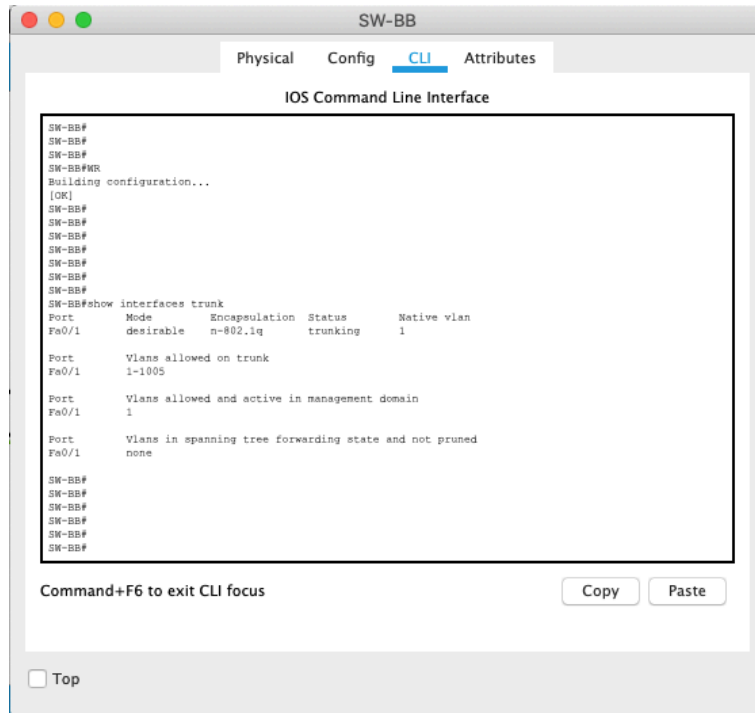
```
SW-BB(config)#interface fastEthernet 0/1  
SW-BB(config-if)#switchport mode dynamic desirable
```

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

*Figura 14. Enlace troncal SW-AA*



*Figura 15. Enlace troncal SW-BB*

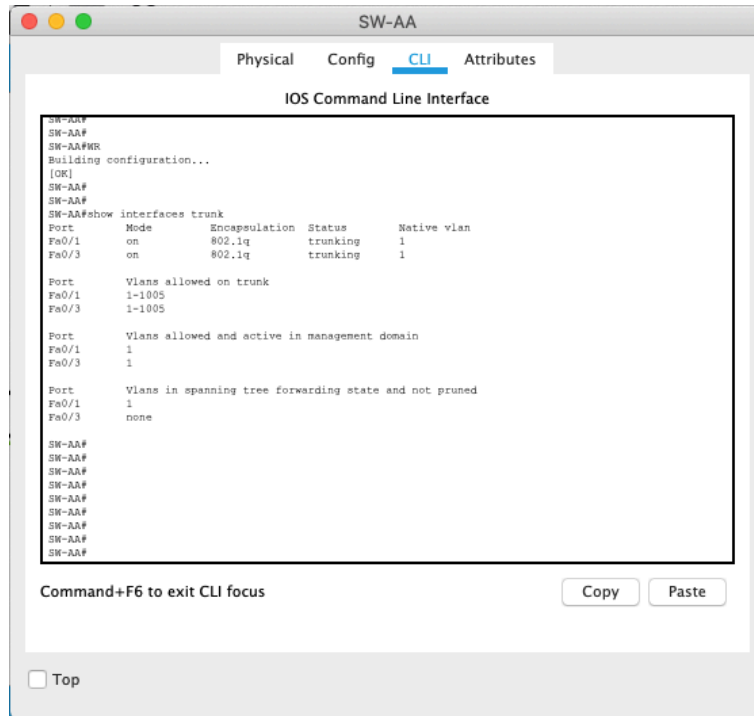


- Entre SW-AA y SW-BB configure un enlace "trunk" estático utilizando el comando switchport mode trunk en la interfaz F0/3 de SW-AA

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

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

*Figura 16. Enlace troncal SW-AA*



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

```

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

```

```

SW-CC(config)#interface fastEthernet 0/1
SW-CC(config-if)#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)

```

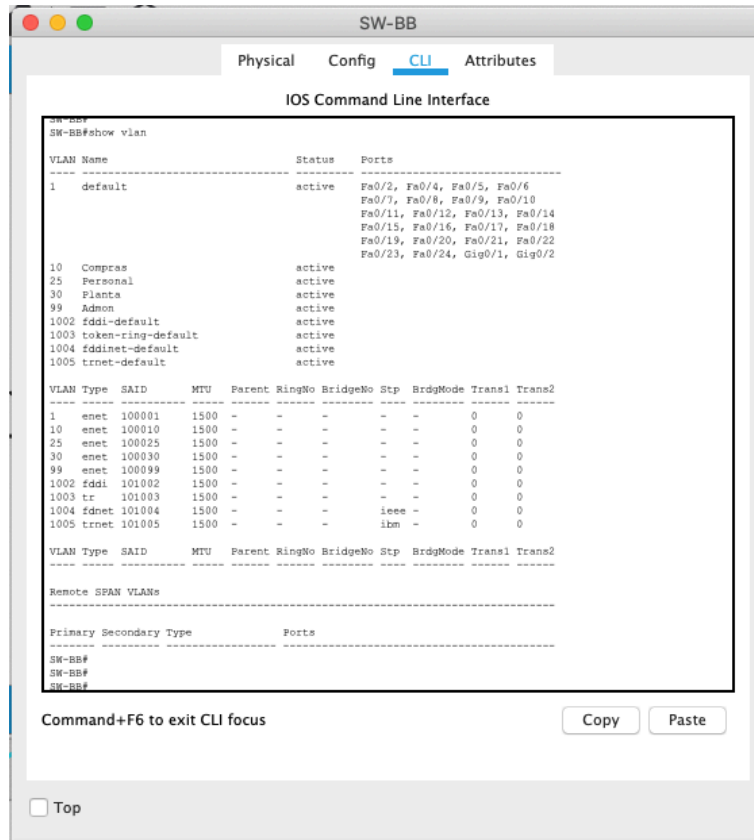
SW-BB(config)#vlan 10
SW-BB(config-vlan)#name Compras
SW-BB(config)#exit
SW-BB(config)#vlan 25
SW-BB(config-vlan)#name Personal
SW-BB(config)#exit
SW-BB(config)#vlan 30
SW-BB(config-vlan)#name Planta
SW-BB(config)#exit
SW-BB(config)#vlan 99

```

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

9. Verifique que las VLANs han sido agregadas correctamente.

Figura 17. Verificación de VLANs en SW-BB



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

Tabla 2: Configuración de IP de equipos.

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.X / 24
F0/15	VLAN 25	190.108.25.X / 24
F0/20	VLAN 30	190.108.30.X / 24
X= numero de cada PC particular		

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

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

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

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

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.

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

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

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

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

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

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

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.

*Tabla 3: Configuración de IP de Switch*

Equipo	Interfaz	Dirección	Masacra
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(config)#interface vlan 99  
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
```

```
SW-BB(config)#interface VLAN 99  
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
```

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

E. Verificar la conectividad Extremo a Extremo

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

Se realiza ping entre los diferentes equipos, observándose lo siguiente:

- Entre equipos que se encuentran dentro de la misma VLAN el ping es exitoso
- Entre equipos que se encuentran en VLAN diferente el ping es fallido.

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

*Figura 18. Verificación PING SW-AA*

```

SW-AA#
SW-AA#
SW-AA#ping 190.108.99.2

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

SW-AA#
SW-AA#
SW-AA#
SW-AA#
SW-AA#ping 190.108.99.3

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

SW-AA#

```

*Figura 19. Verificación PING SW-BB*

```

SW-BB#
SW-BB#
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 = 0/0/0 ms

SW-BB#
SW-BB#
SW-BB#
SW-BB#ping 190.108.99.3

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

SW-BB#
SW-BB#
SW-BB#
SW-BB#

```

*Figura 20. Verificación PING SW-CC*

```

SW-CC#
SW-CC#
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 = 0/0/1 ms

SW-CC#
SW-CC#
SW-CC#
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 = 0/0/0 ms

SW-CC#
SW-CC#

```

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

Se realiza ping desde cada uno de los Switch hacia los equipos, encontrando que todos los ping fueron fallidos, esto se debe a que no existe una discreción IP en cada una de las Vlan de los switch que funcionen como puerta de enlace predeterminada para los equipos.

## CONCLUSIONES

- Las actividades practica desarrolladas en los dos escenarios establecidos, permite que el estudiante evalúe y fortalezca las habilidades adquiridas en el transcurso del Diplomado CCNP, observándose a través de la solución de problemas comúnmente encontrados en entornos laborales y profesionales.
- El uso diferentes Vlan`s (Red de área local virtual) para la creación de redes independientes, permiten dividir y ordenar la red en secciones pequeñas, establecidas dentro de una sola red LAN, al igual que brinda la facilidad de poder volver a establecer y redistribuir la red, debido a que todo se realiza dentro de la configuración de switch y router, evitando la manipulación física y estructural de la red.
- Dentro del desarrollo de los laboratorios prácticos, se puede desarrollar habilidades al igual que orienta al estudiante conforme a los procedimientos necesarios para las diferentes configuraciones tanto de routing como de switching, viéndose la vital importancia del manejo de los simuladores de redes como lo son Packet tracer y Gns3.

## BIBLIOGRAFÍA

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

eare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Path Control Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>

Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de <http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live>

Wallace, K. (2015). CISCO Press (Ed). CCNP Routing and Switching ROUTE 300-101 Official Cert Guide. Recuperado de <https://1drv.ms/b/s!AgIGg5JUgUBthFx8WOxiq6LPJppi>

Hucaby, D. (2015). CISCO Press (Ed). CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. Recuperado de <https://1drv.ms/b/s!AgIGg5JUgUBthF16RWCSsCZnfDo2>