

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

DIEGO ARMANDO RIBERO PATIÑO

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA-ECBTI
INGENIERÍA TELECOMUNICACIONES
BOGOTA D.C.
2020**

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

DIEGO ARMANDO RIBERO PATIÑO

**DIPLOMADO de opción de grado presentado para optar el
título de INGENIERO DE TELECOMUNICACIONES**

**DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA -UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA-ECBTI
INGENIERÍA TELECOMUNICACIONES
BOGOTA D.C.
2020**

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 22 de mayo de 2020.

DEDICATORIA

Un logro alcanzado con esfuerzo y dedicación, es reflejo del apoyo incondicional de mi familia, gracias.

CONTENIDO

DEDICATORIA.....	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.....	15
CONCLUSIONES.....	24
BIBLIOGRAFÍA.....	25

LISTA DE TABLAS

Tabla 1. Información para configuración de los Routers.....	3
Tabla 2. Información para asociar los puertos a las VLAN.....	5
Tabla 3. Información direccionamiento VLAN 99.....	6

LISTA DE FIGURAS

Figura 1. Escenario 1.....	11
Figura 2. Simulación Escenario 1.....	11
Figura 3. Salida del comando show ip route.....	13
Figura 4. Relación de vecinos BGP entre R2 y R3. Comando Show ip route.....	14
Figura 5. Relación de vecinos BGP entre R3 y R4. Comando Show ip route.....	15
Figura 6. Escenario 2.....	15
Figura 7. Simulación Escenario 2.....	16
Figura 8. Configuración VTP en 3 switch, comando show vtp status.....	17
Figura 9. Configuración DTP entre SW-AA y SW-BB.....	18
Figura 10. Enlace trunk entre SW-AA y SW-CC, comando interfaces trunk.....	18
Figura 11. Verificación de VLAN usando comando show VLAN.....	19
Figura 12. Ping entre equipos de otras VLAN.....	22
Figura 13. Ping entre equipos de la misma VLAN.....	22
Figura 14. Ping entre cada switch.....	23
Figura 15. Ping desde cada switch a cada PC.....	23

GLOSARIO

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

Networking: Es la integración de dos o más redes con la finalidad de compartir o 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.

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.

Protocolos de Enrutamiento: Son el conjunto de reglas utilizadas por el Router cuando se comunica con otro Router con el fin de compartir información y tablas de enrutamiento. Un protocolo de enrutamiento es la aplicación de un algoritmo de enrutamiento en el software o hardware.

Vlan: Es un método para crear redes lógicas independientes dentro de una misma red física, su acrónimo de virtual LAN (red de área local virtual). Varias Vlan pueden coexistir en un único conmutador físico o en una única red física.

RESUMEN

El Diplomado de profundización Cisco CCNP entrega a los aprendices los conocimientos necesarios para las configuraciones de Conmutación basadas en switches, mediante el uso de diferentes protocolos y evaluando el desempeño de Enrutamiento mediante el uso de comandos de administración en escenarios de red corporativos para desarrollar competencias en la solución de problemas que se puedan encontrar en el mundo laboral.

Es de esta forma que el desarrollo de los siguientes laboratorios ponen en práctica los conocimientos adquiridos durante el desarrollo del diplomado y prueba el nivel que se tiene en la solución de problemas relacionados en Redes y Electrónica en el mundo del Networking.

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

ABSTRACT

The Cisco CCNP Deepening Diploma provides trainees with the knowledge needed for Switch-Based commutation configurations, using different protocols and evaluating routing performance using management commands in corporate network environments to develop competencies in solving problems you may encounter in the world of work.

It is in this way that the development of the following laboratories will put into practice the knowledge acquired during the development of the diploma and test the level that one has in solving problems related to networks and electronics in the world of Networking.

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

INTRODUCCIÓN

La administración de redes abarca diferentes disciplinas como lo es la gestión adecuada de los recursos disponibles, implementación de la topología necesaria, la seguridad, entre otros.

En el presente informe se evidencia en resumen los conocimientos adquiridos en el diplomado de profundización CCNP, con la elaboración de dos escenarios en los cuales se detalla el paso a paso para la respectiva configuración de BGP, VTP y DTP.

Particularmente se usó dos herramientas GNS3 y Packet Tracer para la simulación de los escenarios, demostrando que los comandos utilizados son iguales y los resultados son tangibles como en la implementación de topologías reales.

DESARROLLO

1. ESCENARIO 1

Figura 1. Escenario 1

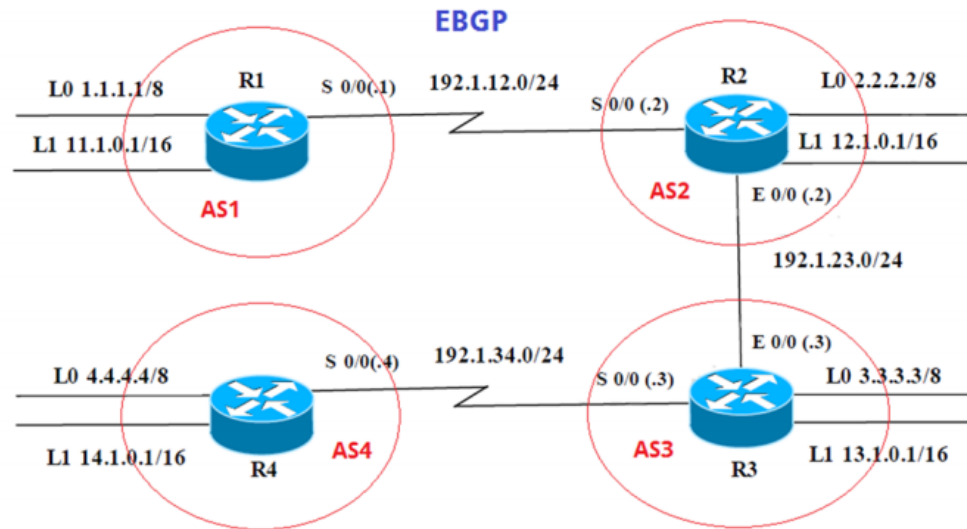


Figura 2. Simulación Escenario 1

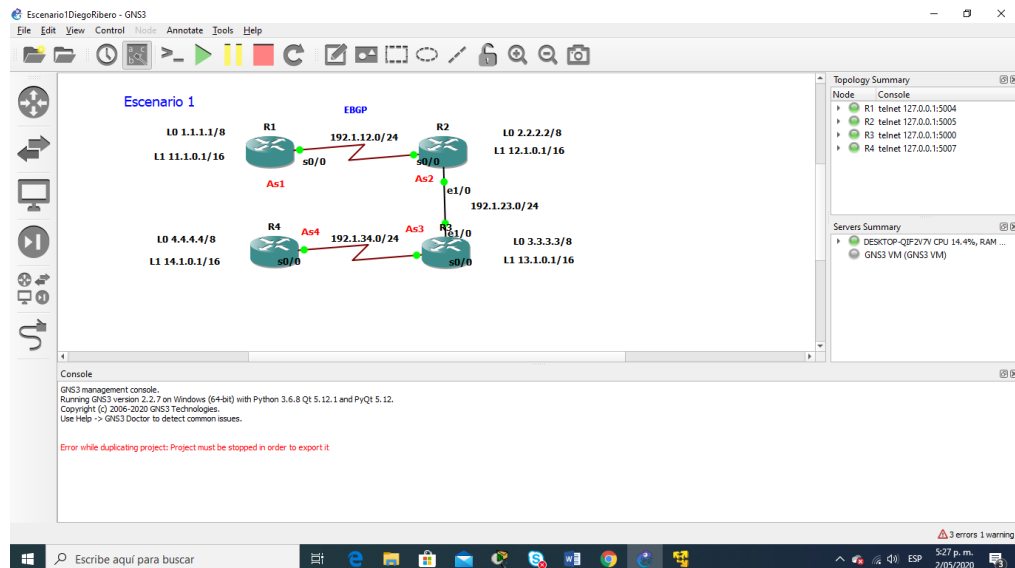


Tabla 1. Información para configuración de los Routers

	Interfaz	Dirección IP	Máscara
R1	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	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	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	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

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 1.1.1.1 mask 255.0.0.0
R1(config-router)#network 11.1.0.1 mask 255.255.0.0
R1(config-router)#bgp router-id 22.22.22.22
R2(config)#router bgp 2
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#network 2.2.2.2 mask 255.0.0.0
R2(config-router)#network 12.1.0.1 mask 255.255.0.0
R2(config-router)#bgp router-id 33.33.33.33

```

Figura 3. Salida del comando show ip route

```

R1
Mar 1 00:00:06.231: %LINK-5-CHANGED: Interface Serial2/1, changed state to administratively down
Mar 1 00:00:06.231: %LINK-5-CHANGED: Interface Serial2/2, changed state to administratively down
Mar 1 00:00:06.235: %LINK-5-CHANGED: Interface Serial2/3, changed state to administratively down
R1#
R1#
R1#
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#router bgp 1
R1(config-router)#neighbor 192.1.12.2 remote-as 2
R1(config-router)#network 1.1.1.1 mask 255.0.0.0
R1: BGP: Incorrect network or mask configured
R1(config-router)#network 11.1.0.1 mask 255.255.0.0
R1: BGP: Incorrect network or mask configured
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#
R1(config-router)#exit
R1(config)#exit
R1#
Mar 1 00:00:49.203: %SYS-5-CONFIG_I: Configured from console by console
R1#show ip ro
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - OOR, P - periodic downloaded static route

Gateway of last resort is not set

R1#
R2
R2#
Mar 1 00:00:06.207: %LINK-5-CHANGED: Interface FastEthernet2/0, changed state to administratively down
R2#
R2#
R2#
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#
R2(config)#router bgp 2
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#network 2.2.2.2 mask 255.0.0.0
R2: BGP: Incorrect network or mask configured
R2(config-router)#network 12.1.0.1 mask 255.255.0.0
R2: BGP: Incorrect network or mask configured
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#exit
R2(config)#
R2#
Mar 1 00:01:33.379: %SYS-5-CONFIG_I: Configured from console by console
R2#show ip ro
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - OOR, P - periodic downloaded static route

Gateway of last resort is not set

R2#
  
```

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)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#network 3.3.3.3 mask 255.0.0.0
R3(config-router)#network 13.1.0.1 mask 255.255.0.0
R3(config-router)#bgp router-id 44.44.44.44
  
```

Figura 4. Relación de vecinos BGP entre R2 y R3. Comando Show ip route

```

R3
*Mar 1 00:00:06.199: %LINK-5-CHANGED: Interface Serial0/0, changed state to adm
inistratively down
*Mar 1 00:00:06.215: %LINK-5-CHANGED: Interface Serial0/1, changed state to adm
inistratively down
*Mar 1 00:00:06.223: %LINK-5-CHANGED: Interface Serial0/2, changed state to adm
inistratively down
*Mar 1 00:00:06.223: %LINK-5-CHANGED: Interface Serial0/3, changed state to adm
inistratively down
*Mar 1 00:00:06.223: %LINK-5-CHANGED: Interface Ethernet1/0, changed state to a
dministratively down
*Mar 1 00:00:06.227: %LINK-5-CHANGED: Interface FastEthernet2/0, changed state
to administratively down
R3#
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#
R3(config)#router bgp 3
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#network 3.3.3.3 mask 255.0.0.0
% BGP: Incorrect network or mask configured
R3(config-router)#network 13.1.0.1 mask 255.255.0.0
% BGP: Incorrect network or mask configured
R3(config-router)#bgp router-id 44.44.44
R3(config-router)#exit
R3(config)#
R3(config)#exit
R3#show
*Mar 1 00:04:28.823: %SYS-5-CONFIG_I: Configured from console by console
R3#show ip ro
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

```

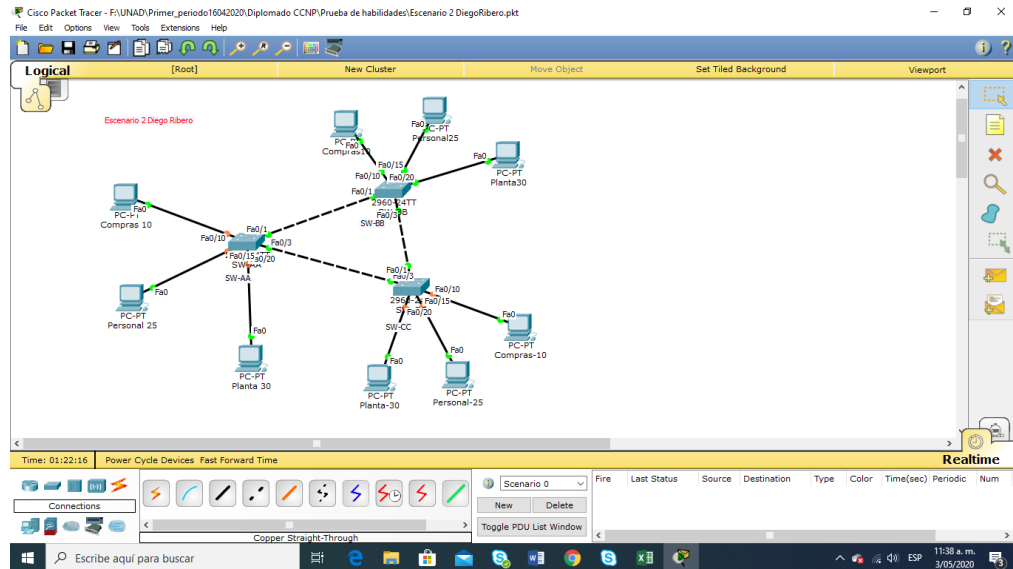
- Configure una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en **AS3** y R4 debería estar en **AS4**. Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como 66.66.66.66. Establezca las relaciones de vecino con base en las direcciones de Loopback 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 4.4.4.4 remote-as 4
R3(config)#ip route 4.0.0.0 255.0.0.0 192.1.34.4
R4(config)#router bgp 4
R4(config-router)#neighbor 3.3.3.3 remote-as 3
R4(config-router)#network 14.1.0.1 mask 255.255.0.0
R4(config-router)#bgp router-id 66.66.66.66
R4(config)#ip route 3.0.0.0 255.0.0.0 192.1.34.3

```


Figura 7. Simulación Escenario 2



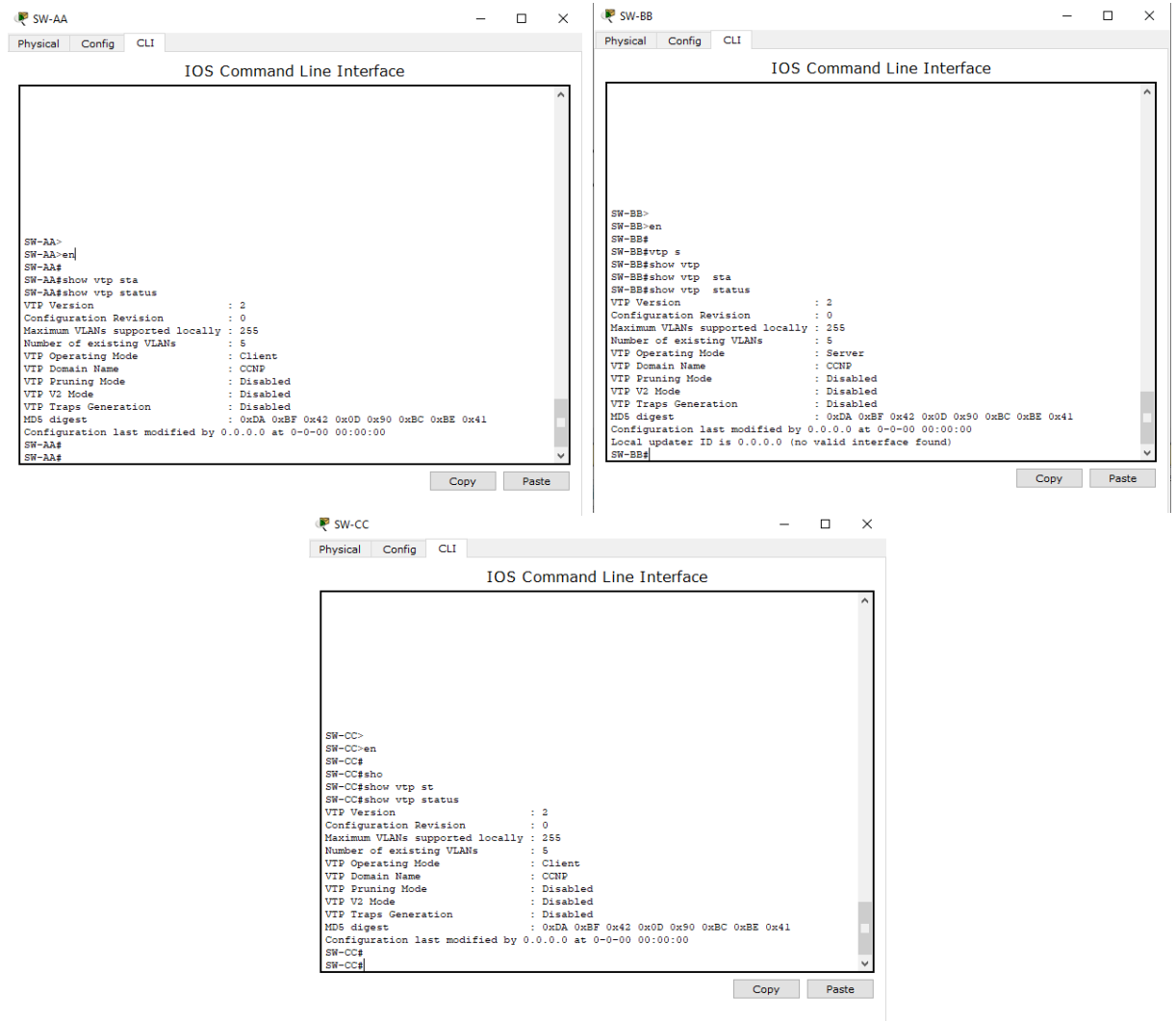
A. Configurar VTP

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 VTP llamado CCNP y usando la contraseña cisco.

```
Switch1(config)#hostname SW-AA
SW-AA (config)#vtp mode client
SW-AA (config)#vtp domain CCNP
SW-AA (config)# vtp password cisco
Switch2(config) hostname SW-BB
SW-BB (config)#vtp domain CCNP
SW-BB (config)#vtp mode server
SW-BB (config)#vtp password cisco
Switch3(config)#hostname SW-CC
SW-CC (config)#vtp mode client
SW-CC (config)#vtp domain CCNP
SW-CC (config)# vtp password cisco
```

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

Figura 8. Configuración VTP en 3 switch, comando show vtp status



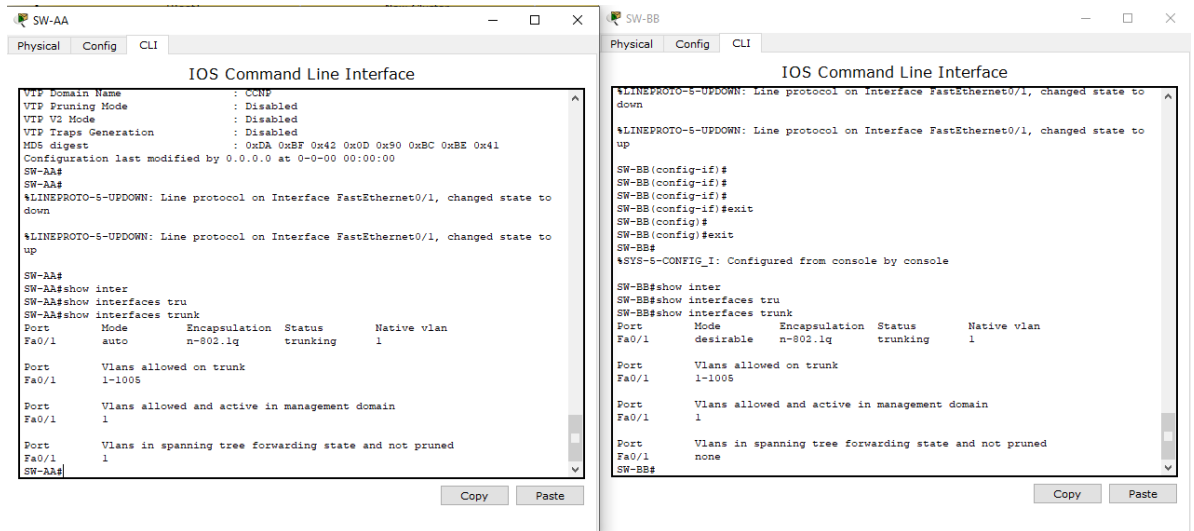
B. Configurar DTP (Dynamic Trunking Protocol)

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

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

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

Figura 9. Configuración DTP entre SW-AA y SW-BB

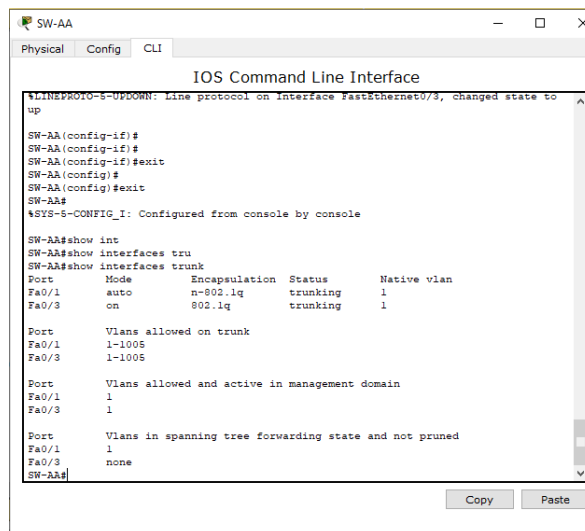


- Entre SW-AA y SW-BB debe ser SW-CC configure un enlace "trunk" estático utilizando el comando **switchport mode trunk** en la interfaz F0/3 de SW-AA

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

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

Figura 10. Enlace trunk entre SW-AA y SW-CC, comando interfaces trunk



- 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.

- En SW-AA agregue la VLAN 10. En SW-BB agregue las VLANs Compras (10), Mercadeo (20), Planta (30) y Admon (99)

```
SW-BB (config)#vlan 10
SW-BB (config-vlan)#name Compras
SW-BB (config-vlan)#vlan 20
SW-BB (config-vlan)#name Mercadeo
SW-BB (config-vlan)#vlan 30
SW-BB (config-vlan)#name Planta
SW-BB (config-vlan)#vlan 99
SW-BB (config-vlan)#name Admon
```

- Verifique que las VLANs han sido agregadas correctamente.

Figura 11. Verificación de VLAN usando comando show VLAN

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

SW-BB#
SW-BB#show vln
SW-BB#show vlan

VLAN Name                Status    Ports
-----
1    default                 active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                           Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                           Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/23, Fa0/24, Gig0/1, Gig0/2

10   Compras                 active
20   Mercadeo                active
30   Planta                  active
99   Admon                   active
1002 fddi-default            act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default        act/unsup
1005 trnet-default         act/unsup

VLAN Type  SAID      MTU   Parent RingNo BridgeNo Stp    BrdgMode Trans1 Trans2
-----
1    enet    100001   1500  -     -     -     -     -     0     0
10   enet    100010   1500  -     -     -     -     -     0     0
--More--
```

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

Tabla 2. Información para asociar los puertos a las VLAN

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.X / 24
F0/15	VLAN 20	190.108.20.X / 24
F0/20	VLAN 30	190.108.30.X / 24

X = número 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-if)#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 20
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 20
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 20
```

```
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. Información direccionamiento VLAN 99

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

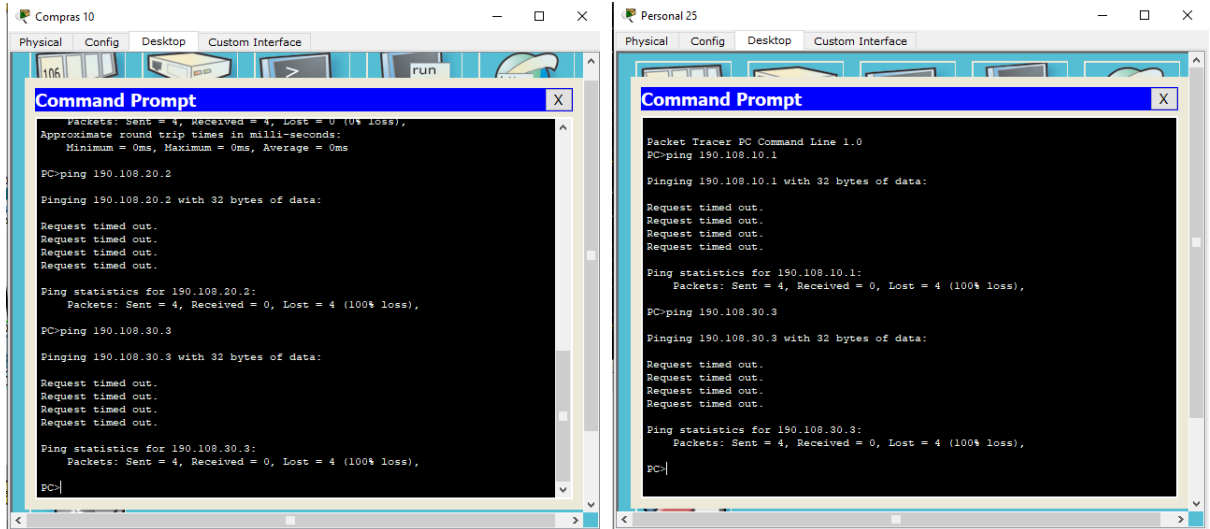
```
SW-AA (config)#interface vlan 99
SW-AA (config-if)#ip address 190.108.99.1 255.255.255.0
SW-AA (config)#no shutdown
SW-BB (config)#interface VLAN 99
SW-BB (config-if)#ip address 190.108.99.2 255.255.255.0
SW-BB (config)# no shutdown
SW-CC (config)#interface vlan 99
SW-CC (config-if)#ip address 190.108.99.3 255.255.255.0
SW-CC (config)# no shutdown
```

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.

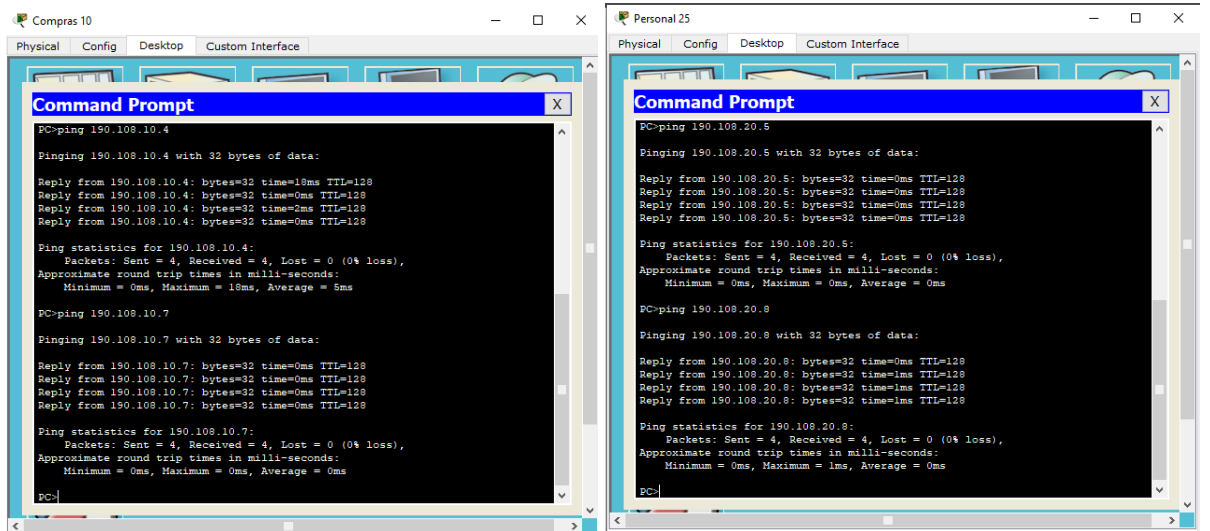
El ping no fue exitoso entre equipos que se encuentran en otras VLAN.

Figura 12. Ping entre equipos de otras VLAN



El ping fue exitoso cuando se hizo ping a los equipos de la misma vlan.

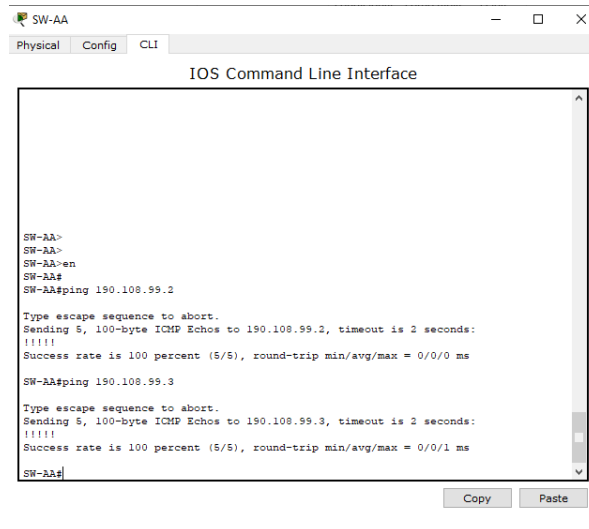
Figura 13. Ping entre equipos de la misma VLAN



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

El ping es exitoso porque se encuentran dentro de la misma VLAN y red.

Figura 14. Ping entre cada switch



```
SW-AA>
SW-AA>
SW-AA>en
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 = 0/0/0 ms

SW-AA#ping 190.108.99.3

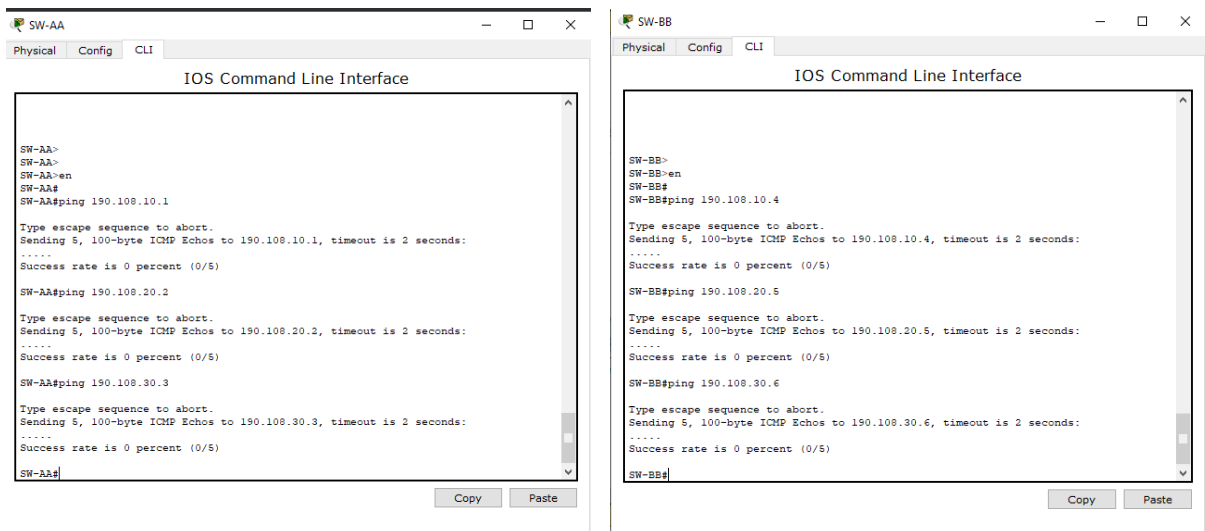
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

SW-AA#
```

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

El ping no es exitoso porque no se encuentran en la misma VLAN ni la misma red.

Figura 15. Ping desde cada switch a cada PC



```
SW-AA>
SW-AA>
SW-AA>en
SW-AA#
SW-AA#ping 190.108.10.1

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

SW-AA#ping 190.108.20.2

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

SW-AA#ping 190.108.30.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#

SW-BB>
SW-BB>en
SW-BB#
SW-BB#ping 190.108.10.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.20.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.5, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.30.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#
```

CONCLUSIONES

- El uso de herramientas como Packet tracer, GNS3 o SMARTLAB fortalecen las habilidades en las configuraciones de switches y routers, permitiendo que se entienda la lógica en la ejecución de cada comando.
- Simular topologías de red afianza y complementan los conocimientos en configuraciones como BGP, VTP, DTP, VLANs entre otros, porque de la misma forma se realiza en topologías reales.
- Los inconvenientes que se presentaron durante la ejecución de los laboratorios ponen a prueba los niveles de comprensión y solución de problemas relacionados con diferentes aspectos de Networking.

REFERENCIAS BIBLIOGRAFICAS

Temática: First Hop Redundancy Protocols

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

Temática: Network Management

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

Temática: Switching Features and Technologies

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

Temática: High Availability

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

Temática: Campus Network Security

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>