

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

GERMAN LOPEZ PEREZ

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

CALI

2020

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

GERMAN LOPEZ PEREZ

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 – ECBT
INGENIERÍA ELECTRONICA
CALI
2020

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

CALI, 22 de mayo de 2020

AGRADECIMIENTOS

Agradezco a nuestros directivos y tutores de nuestra Universidad Nacional Abierta y a Distancia Unad quienes nos han aportado conocimiento para nuestro crecimiento profesional y personal, aquellos que siempre estuvieron guiándonos para que pudiéramos alcanzar nuestras metas

CONTENIDO

AGRADECIMIENTOS.....	4
LISTA DE TABLAS	6
LISTA DE FIGURAS	7
GLOSARIO	8
RESUMEN.....	9
INTRODUCCIÓN	10
1. ESCENARIO 1.....	11
2. ESCENARIO 2.....	20
CONCLUSIONES	41
REFERENCIAS BIBLIOGRÁFICAS.....	42

LISTA DE TABLAS

Tabla 1. Configuración R1, R2, R3, R4.....	12
Tabla 2. Configuración IP.....	28
Tabla 3. Direcciones IP de los PCs.....	29
Tabla 4. Tabla de direccionamiento.....	31

LISTA DE FIGURAS

Figura 1. Escenario 1	11
Figura 2. Simulación del escenario 1	11
Figura 3. Enrutamiento de R1 con respecto a R2	15
Figura 4. Enrutamiento de R2 con respecto a R1	16
Figura 5. Enrutamiento de R2 con respecto a R3	17
Figura 6. Enrutamiento de R3 con respecto a R2	17
Figura 7. Enrutamiento de R3 con respecto a R4	18
Figura 8. Enrutamiento de R4 con respecto a R3	19
Figura 9. Escenario 2	20
Figura 10. Simulación del escenario 2	21
Figura 11. Verificación Vtp en SW-AA	23
Figura 12. Verificación Vtp en SW-CC	23
Figura 13. Verificación Vtp en SW-BB	24
Figura 14. Enlace de trunk en SW-BB	25
Figura 15. Enlace de trunk en SW-AA	25
Figura 16. Enlace de trunk en SW-AA	26
Figura 17. VLANs en SW-BB	28
Figura 18. Ping des la pc1 a las pc2, pc3	32
Figura 19. Ping des la pc1 a las pc4, pc7	33
Figura 20. Ping des la pc5 a las pc1, pc9	34
Figura 21. Ping des la pc5 a las pc2, pc8	35
Figura 22. Ping des la pc9 a las pc3, pc6	36
Figura 23. Ping des la pc9 a las pc2, pc8	37
Figura 24. Ping desde SW-AA a SW-BB y SW-CC	38
Figura 25. Ping desde SW-BB a SW-AA y SW-CC	38
Figura 26. Ping desde SW-CC a SW-AA y SW-BB	38
Figura 27. Ping desde SW-AA a las pc1, pc2, pc5, pc6	39
Figura 28. Ping desde SW-CC a las pc5, pc6, pc3, pc9	39
Figura 29. Ping desde SW-CC a las pc3, pc9, pc6, pc2	40

GLOSARIO

Cisco Packet Tracer. Es un poderoso programa de simulación de red que permite a los estudiantes experimentar con el comportamiento de la red y hacer preguntas de "qué pasaría si". Como parte integral de la experiencia de aprendizaje integral de Networking Academy, Packet Tracer proporciona capacidades de simulación, visualización, autoría, evaluación y colaboración, y facilita la enseñanza y el aprendizaje de conceptos tecnológicos complejos

Red: es un conjunto de equipos nodos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Switch de red: es un dispositivo de interconexión utilizado para conectar equipos en **red** formando lo que se conoce como una **red** de área local (LAN)

ROUTER: es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

VLAN: es un método para crear redes lógicas independientes dentro de una misma red física.

BGP: Se trata del protocolo más utilizado para redes con intención de configurar un protocolo de puerta de enlace exterior. La forma de configurar y delimitar la información que contiene e intercambia el protocolo BGP es creando lo que se conoce como sistema autónomo o AS

OSPF: protocolo de red para enrutamiento jerárquico que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

Interface Loopback: es una interfaz de red virtual. La dirección de loopback crea un método de acceso directo para las aplicaciones y servicios TCP/IP que se ejecutan en el mismo dispositivo para comunicarse entre sí

RESUMEN

El desarrollo de esta actividad final del diplomado de profundización CCNP "Prueba de habilidades prácticas", se desarrollaron los escenarios correspondientes a la configuración de los protocolos de enrutamiento en la topología de las redes en las cuales desarrollaremos Conmutación y configuración como relación de vecino BGP entre los roetes, configurarán para usar VTP para las actualizaciones de VLAN, Configure en enlace troncal entre otros y se subirá evidencia de su correcto funcionamiento.

Es importante resaltar la importancia que tiene la electrónica y las redes en nuestra actualidad y que siempre están en constante crecimiento en todas las aplicaciones que se requieren para una mayor seguridad y rapidez en la obtención de información y las comunicaciones.

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

ABSTRACT

The development of this final activity of the CCNP deepening diploma "Practical skills test", the scenarios corresponding to the configuration of routing protocols in the topology of the networks in which we will develop Switching and configuration as a BGP neighbor relationship between the rocket will configure to use VTP for VLAN updates, configure trunking among others and evidence of its correct operation will be uploaded.

It is important to highlight the importance of electronics and networks today and that they are always constantly growing in all the applications that are required for greater security and speed in obtaining information and communications.

Key Words: CISCO, CCNP, Switching, Routing, Networks, Electronics

INTRODUCCIÓN

El siguiente informe fue desarrollado con el fin de darle solución a los dos escenarios planteados para identificar el grado de habilidades que fueron adquiridas a lo largo del curso diplomado de profundización cisco CCNP, el primer escenario se trata de intercambio de información de enrutamiento entre diferentes sistemas autónomos mediante el protocolo BGP y el segundo escenario se trata de administración de redes de área local, para la implementación de VLAN, haciendo uso del protocolo VTP y de la configuración de enlaces troncales mediante el protocolo DTP.

Podemos observar en nuestro entorno la necesidad por las comunicaciones y la importancia de generar una mayor seguridad para nuestros datos y rapidez en la obtención de información, tanto como en los hogares como en las empresas

Vemos esta gran necesidad de las redes de datos y su respectivo crecimiento en el mundo de las comunicaciones donde nos enfrentamos a un crecimiento diario en lo cual nosotros estamos en la responsabilidad de afrontar estos desafíos que nos ofrece el diario vivir en nuestra ingeniería en lo cual nos fortalecemos en el aprendizaje de un mayor conocimiento para implementar protocolos efectivos de enrutamiento y seguridad de las redes WAN, LAN, PAN, CAN, MAN, SAN, VLAN, etc.

1. ESCENARIO 1

Figura 1. Escenario 1

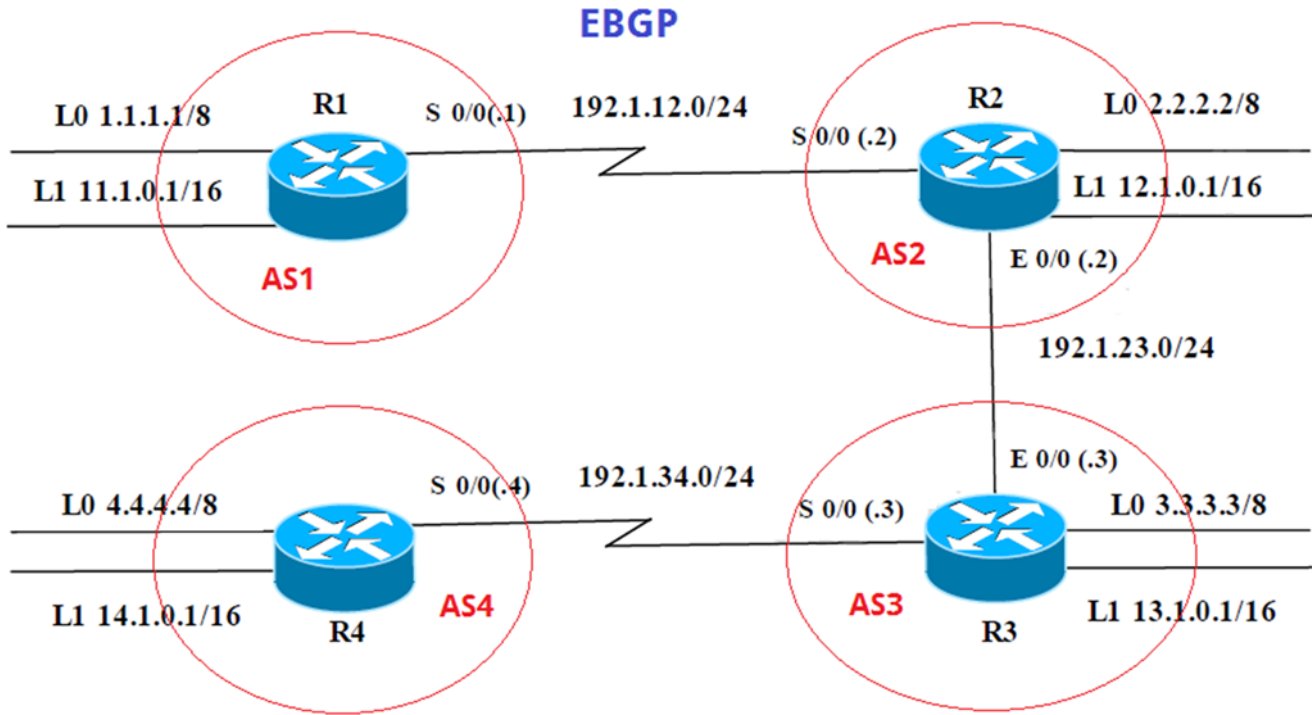
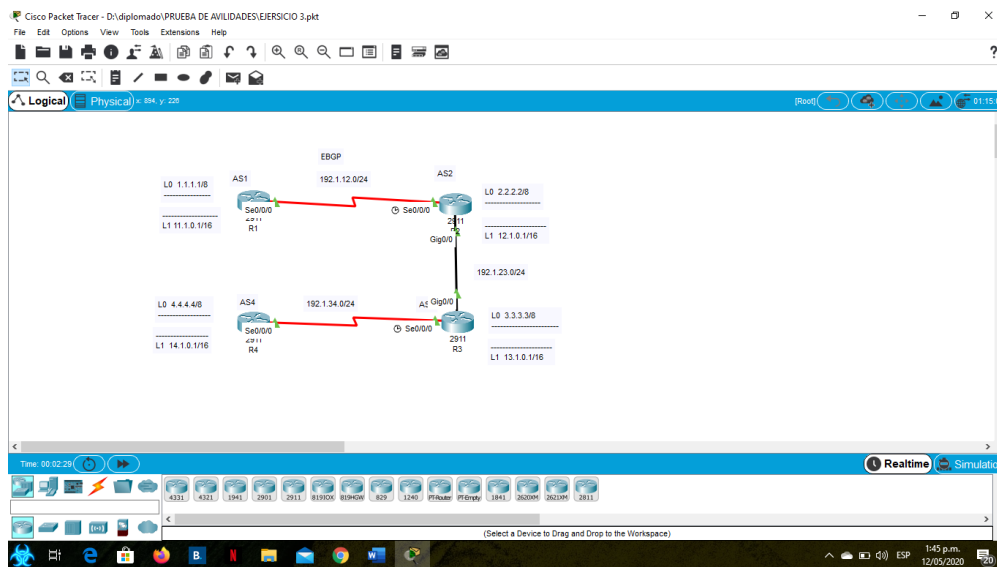


Figura 2. Simulación del escenario 1



Información para configuración de los Routers

Tabla 1. Configuración R1, R2, R3, R4

	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

	Interfaz	Dirección IP	Máscara
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

	Interfaz	Dirección IP	Máscara
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

	Interfaz	Dirección IP	Máscara
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

Vamos a configurar los routers según la tabla que tenemos

```

Router>en / Ingreso a modo privilegiado
Router#conf t / Ingreso a modo de configuración
Router(config)#hostname R1 / Se asigna nombre al router
R1(config)#interface Loopback0 / Configuramos y creamos la interfaz
loopback 0
R1(config-if)#ip address 1.1.1.1 255.0.0.0 / Asignamos la IP
R1(config-if)#interface Loopback1 / Configuramos y creamos la interfaz
loopback 1
R1(config-if)#ip address 11.1.0.1 255.255.0.0 / Asignamos la IP
    
```

```
R1(config-if)#exit
R1(config)#interface s0/0/0          / Configuro interfaz serial 0
R1(config-if)#ip address 192.1.12.1 255.255.255.0 / Asignamos la IP
R1(config-if)#clock rate 64000      / Asignamos configuración de
clock rate
```

```
R1(config-if)#no shutdown          / Activamos interfaz
R1(config-if)#exit
```

```
Router>en
Router#conf t
Router(config)#hostname R2          / Se asignar nombre al router
R2(config)#interface Loopback0      / Configuramos y creamos la interfaz
loopback 0
R2(config-if)#ip address 2.2.2.2 255.0.0.0 / Asignamos la IP
R2(config-if)#interface Loopback1   / Configuramos y creamos la interfaz
loopback 1
R2(config-if)#ip address 12.1.0.1 255.255.0.0 / Asignamos la IP
R2(config-if)#exit
R2(config)#interface s0/0/0         / Configuro interfaz serial 0
R2(config-if)#ip address 192.1.12.2 255.255.255.0 / Asignamos la IP
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface g0/0           / Configuro interfaz FastEthernet 0
R2(config-if)#ip address 192.1.23.2 255.255.255.0 / Asignamos la IP
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
```

```
Router>en
Router#conf t
Router(config)#hostname R3          / Se asignar nombre al router
R3(config)#interface Loopback0      / Configuramos y creamos la interfaz loopback
0
R3(config-if)#ip address 3.3.3.3 255.0.0.0 / Asignamos la IP
R3(config-if)#interface Loopback1   / Configuramos y creamos la interfaz
loopback 1
R3(config-if)#ip address 13.1.0.1 255.255.0.0 / Asignamos la IP
R3(config-if)#exit
R3(config)#interface s0/0/0         / Configuro interfaz serial 0
R3(config-if)#ip address 192.1.34.3 255.255.255.0 / Asignamos la IP
R3(config-if)#no shutdown
R3(config-if)#exit
```

```
R3(config)#interface g0/0      / Configuro interfaz FastEthernet 0
R3(config-if)#ip address 192.1.23.3 255.255.255.0  / Asignamos la IP
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#
```

```
Router>en
Router#conf t
Router(config)#hostname R4
R4(config)#interface Loopback0
R4(config-if)#ip address 4.4.4.4 255.0.0.0  / Asignamos la IP
R4(config-if)#interface Loopback1
R4(config-if)#ip address 14.1.0.1 255.255.0.0  / Asignamos la IP
R4(config-if)#exit
R4(config)#interface s0/0/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0  / Asignamos la IP
R4(config-if)#no shutdown
```

1.2 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)#bgp router-id 22.22.22.22
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)#exit
```

```
R2(config)#router bgp 2
R2(config-router)#bgp router-id 33.33.33.33
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)#exit
```

Figura 3. Enrutamiento de R1 con respecto a R2

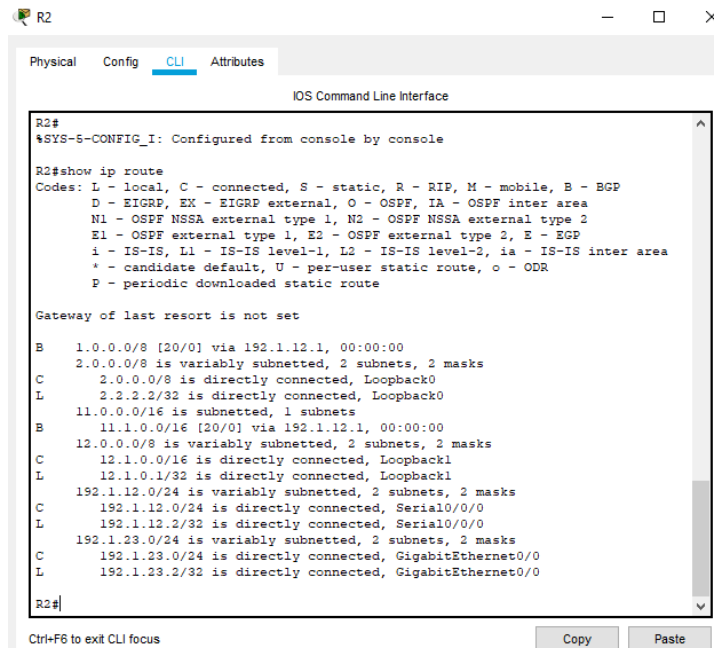
```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, 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

  1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       1.0.0.0/8 is directly connected, Loopback0
L       1.1.1.1/32 is directly connected, Loopback0
B       2.0.0.0/8 [20/0] via 192.1.12.2, 00:00:00
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
L       12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0/16 [20/0] via 192.1.12.2, 00:00:00
B       192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.12.0/24 is directly connected, Serial0/0/0
L       192.1.12.1/32 is directly connected, Serial0/0/0

R1#
```

Figura 4. Enrutamiento de R2 con respecto a R1



```
R2#
%SYS-5-CONFIG_I: Configured from console by console

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, 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

B 1.0.0.0/8 [20/0] via 192.1.12.1, 00:00:00
 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 11.1.0.0/16 [20/0] via 192.1.12.1, 00:00:00
 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, Serial0/0/0
L 192.1.12.2/32 is directly connected, Serial0/0/0
192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.1.23.0/24 is directly connected, GigabitEthernet0/0
L 192.1.23.2/32 is directly connected, GigabitEthernet0/0

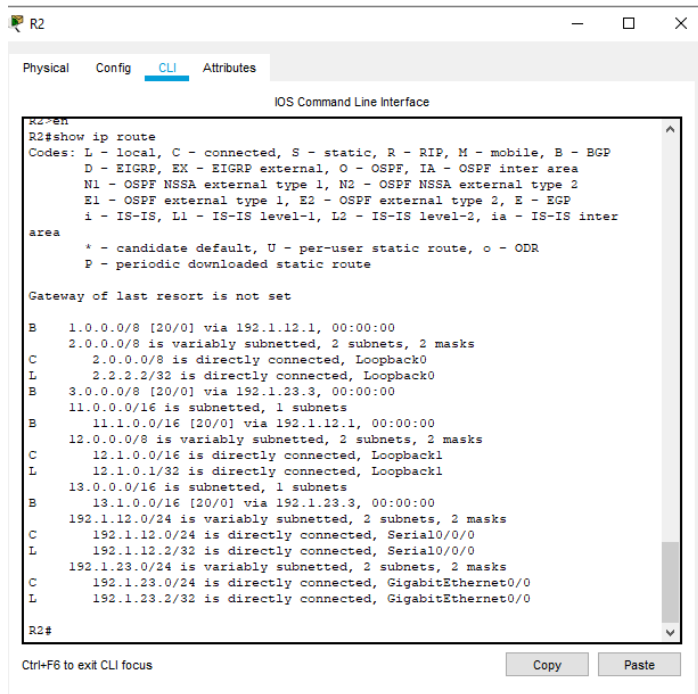
R2#
```

1.3 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)#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
```


Figura 5. Enrutamiento de R2 con respecto a R3



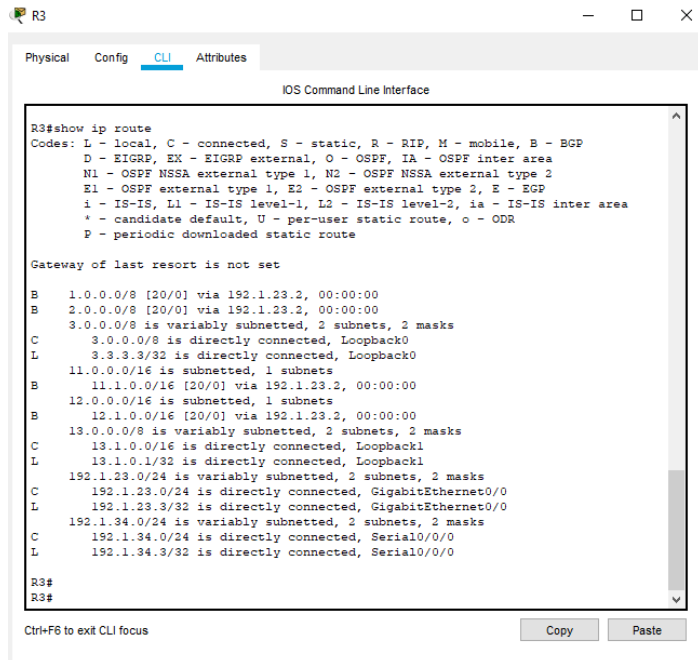
```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       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

B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:00:00
C    2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
L    2.2.2.2/32 is directly connected, Loopback0
B    3.0.0.0/8 [20/0] via 192.1.23.3, 00:00:00
L    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0/16 [20/0] via 192.1.12.1, 00:00:00
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    13.1.0.0/16 [20/0] via 192.1.23.3, 00:00:00
C    192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
L    192.1.12.0/24 is directly connected, Serial0/0/0
L    192.1.12.2/32 is directly connected, Serial0/0/0
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 R3 con respecto a R2



```
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, 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

B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
C    3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
L    3.3.3.3/32 is directly connected, Loopback0
L    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0/16 [20/0] via 192.1.23.2, 00:00:00
L    12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0/16 [20/0] via 192.1.23.2, 00:00:00
C    13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
L    13.1.0.0/16 is directly connected, Loopback1
L    13.1.0.1/32 is directly connected, Loopback1
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    192.1.23.3/32 is directly connected, GigabitEthernet0/0
C    192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
L    192.1.34.0/24 is directly connected, Serial0/0/0
L    192.1.34.3/32 is directly connected, Serial0/0/0

R3#
R3#
```

1.3 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 4.4.4.4 remote-as 4
R3(config)#ip route 4.0.0.0 255.0.0.0 192.1.34.4
R3(config)#exit
```

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

Figura 7. Enrutamiento de R3 con respecto a R4

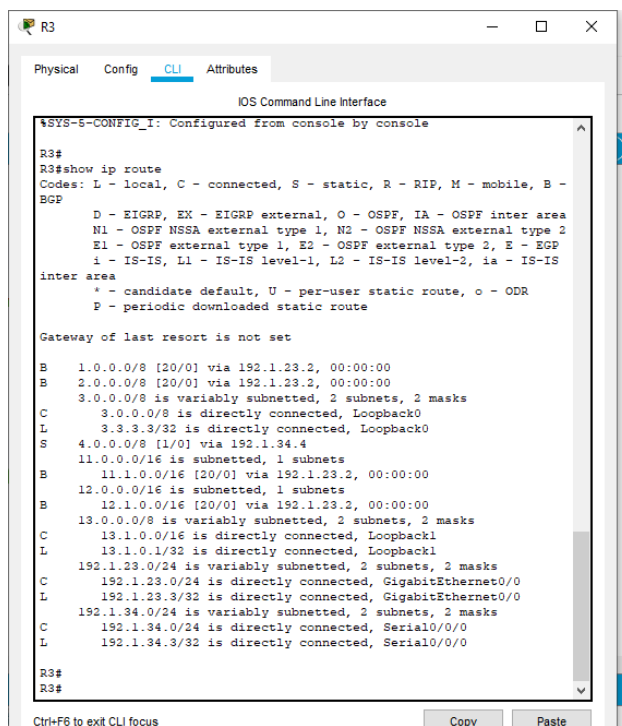


Figura 8. Enrutamiento de R4 con respecto a R3

```
%SYS-5-CONFIG_I: Configured from console by console

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 192.1.34.3
     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
     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
     192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial0/0/0
L    192.1.34.4/32 is directly connected, Serial0/0/0

R4#
```

Ctrl+F6 to exit CLI focus

Copy Paste

2. ESCENARIO 2

Figura 9. Escenario 2

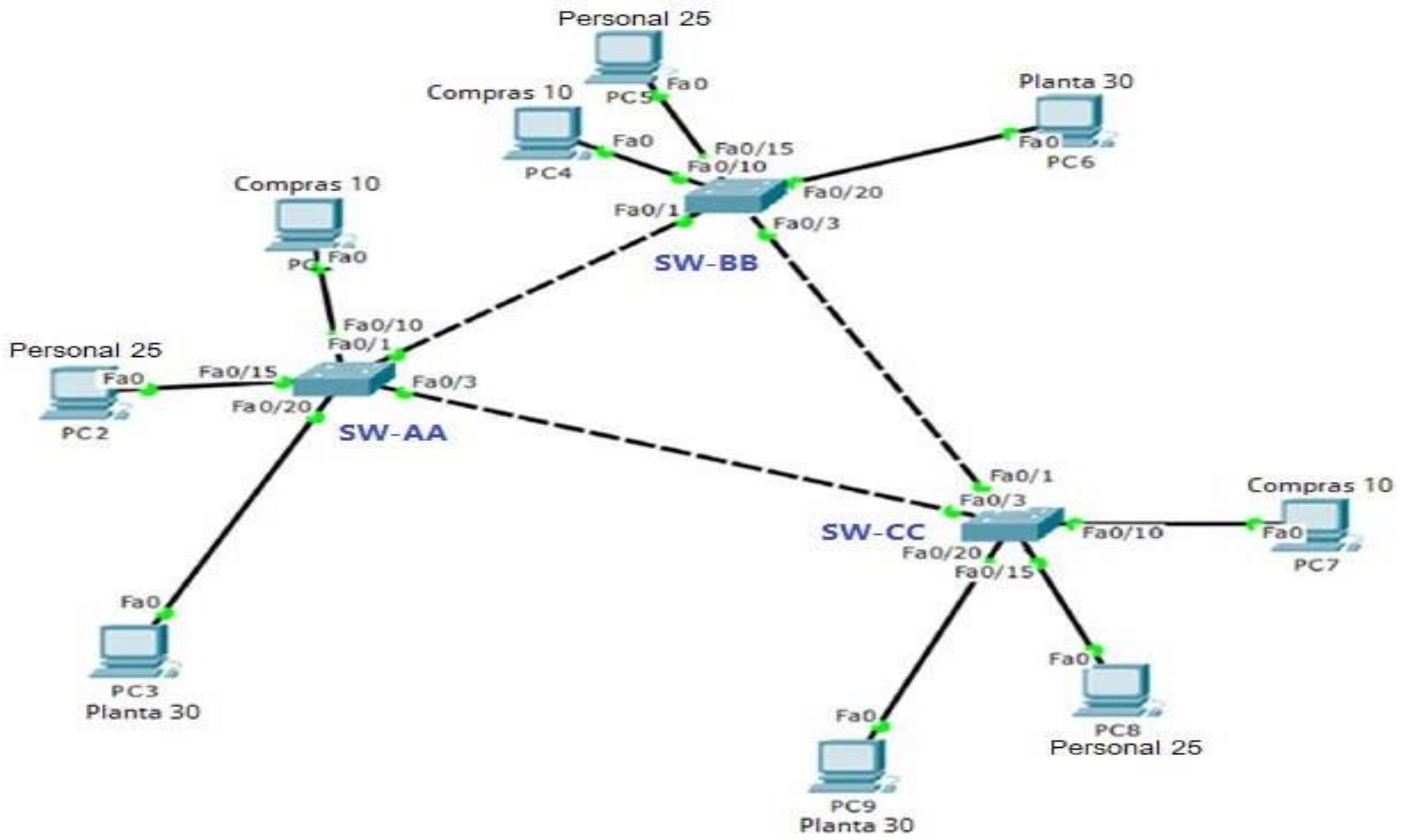
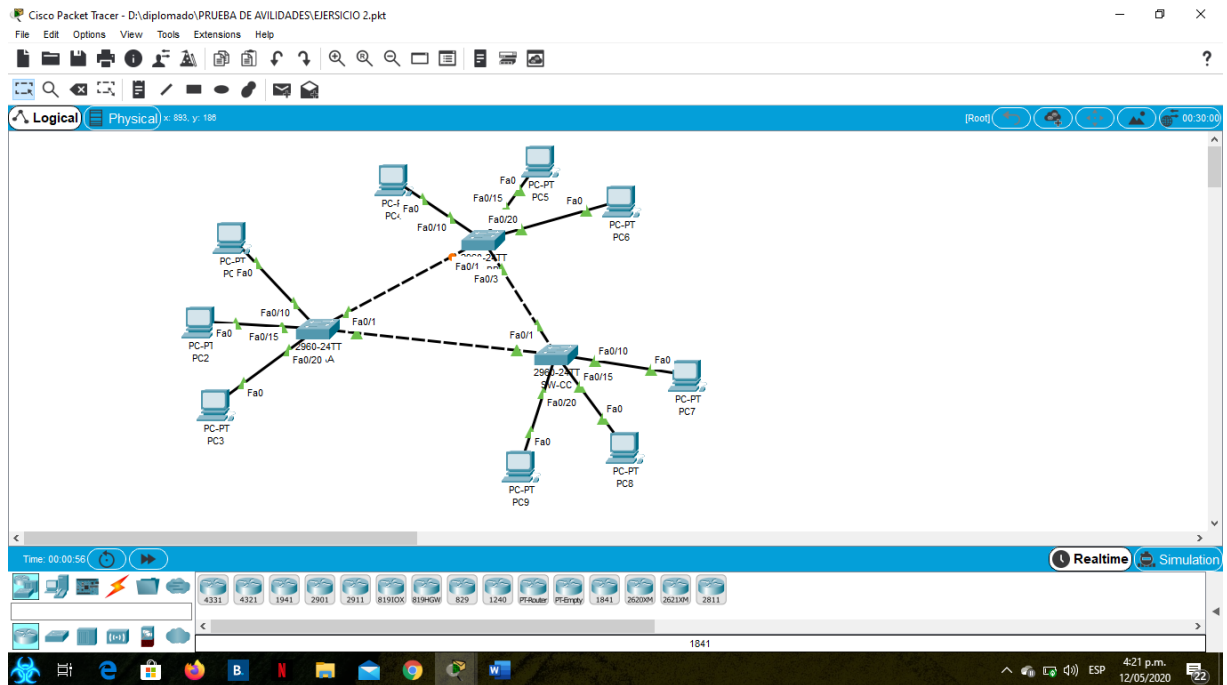


Figura 10. Simulación del escenario 2



2.1 Configurar VTP

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

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-BB
SW-BB(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-BB(config)#vtp version 2
SW-BB(config)#vtp mode server
Device mode already VTP SERVER.
SW-BB(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-BB(config)#
```

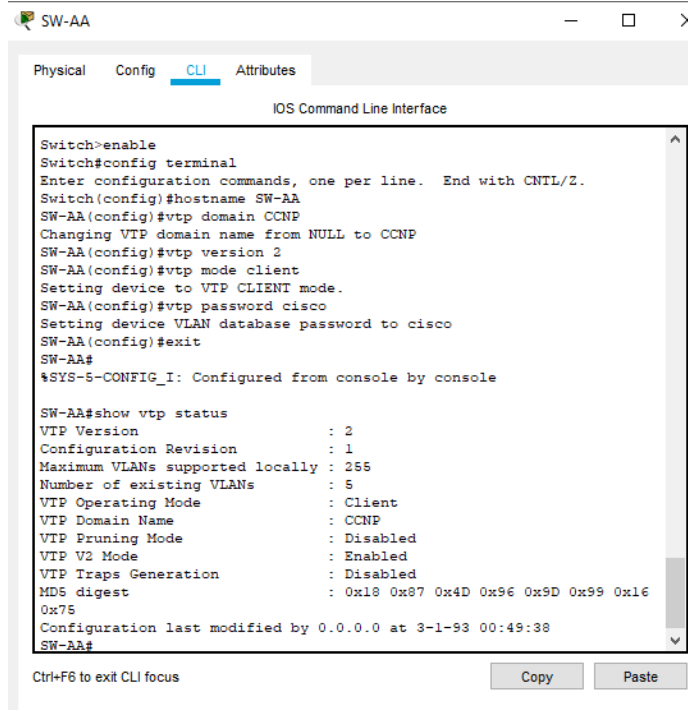
```
Switch>enable
Switch#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Switch(config)#hostname SW-AA
SW-AA(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-AA(config)#vtp version 2
SW-AA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-AA(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-AA(config)#
```

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-CC
SW-CC(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-CC(config)#vtp version 2
SW-CC(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-CC(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-CC(config)#
```

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

Figura 11. Verificación Vtp en SW-AA

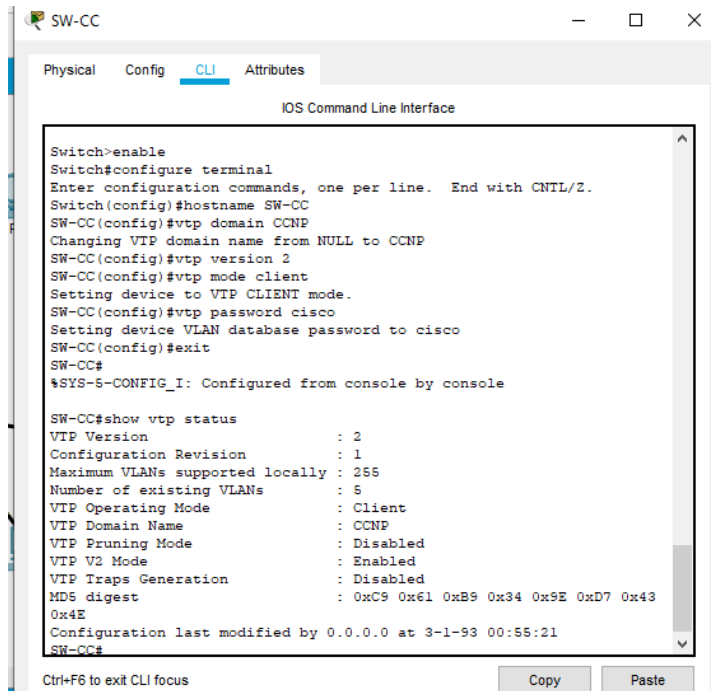


```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface

Switch>enable
Switch#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-AA
SW-AA(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-AA(config)#vtp version 2
SW-AA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-AA(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-AA(config)#exit
SW-AA#
%SYS-5-CONFIG_I: Configured from console by console

SW-AA#show vtp status
VTP Version          : 2
Configuration Revision : 1
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode   : Client
VTP Domain Name     : CCNP
VTP Pruning Mode    : Disabled
VTP V2 Mode         : Enabled
VTP Traps Generation : Disabled
MDS digest          : 0x18 0x87 0x4D 0x96 0x9D 0x99 0x16
0x75
Configuration last modified by 0.0.0.0 at 3-1-93 00:49:38
SW-AA#
```

Figura 12. Verificación Vtp en SW-CC

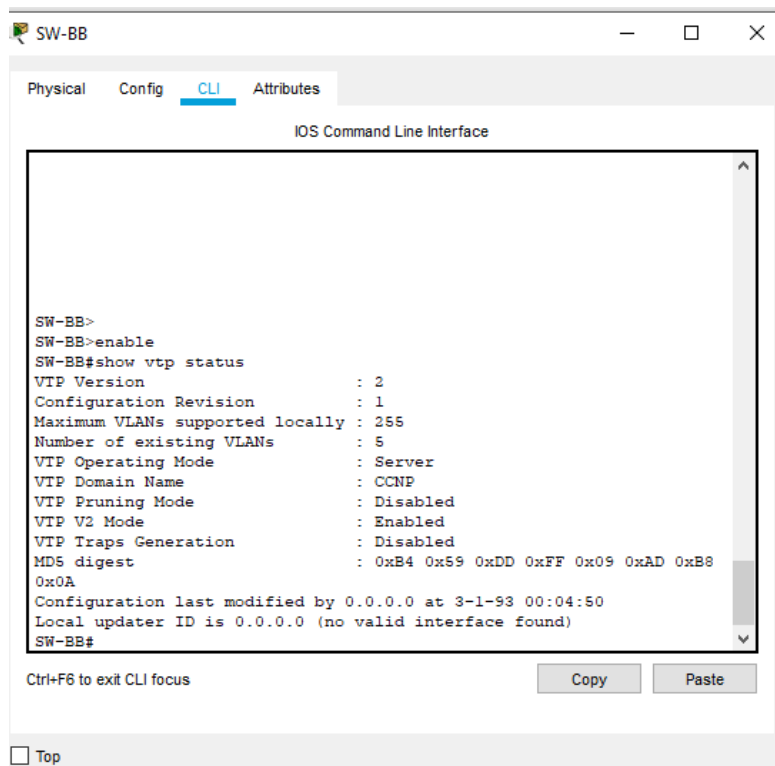


```
SW-CC
Physical Config CLI Attributes
IOS Command Line Interface

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-CC
SW-CC(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-CC(config)#vtp version 2
SW-CC(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-CC(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-CC(config)#exit
SW-CC#
%SYS-5-CONFIG_I: Configured from console by console

SW-CC#show vtp status
VTP Version          : 2
Configuration Revision : 1
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode   : Client
VTP Domain Name     : CCNP
VTP Pruning Mode    : Disabled
VTP V2 Mode         : Enabled
VTP Traps Generation : Disabled
MDS digest          : 0xC9 0x61 0xB9 0x34 0x9E 0xD7 0x43
0x4E
Configuration last modified by 0.0.0.0 at 3-1-93 00:55:21
SW-CC#
```

Figura 13. Verificación Vtp en SW-BB



The screenshot shows a window titled 'SW-BB' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal output shows the following commands and their results:

```
SW-BB>
SW-BB>enable
SW-BB#show vtp status
VTP Version                : 2
Configuration Revision     : 1
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                : Enabled
VTP Traps Generation       : Disabled
MDS digest                  : 0xB4 0x59 0xDD 0xFF 0x09 0xAD 0xB8
0x0A
Configuration last modified by 0.0.0.0 at 3-1-93 00:04:50
Local updater ID is 0.0.0.0 (no valid interface found)
SW-BB#
```

At the bottom of the window, there are buttons for 'Copy' and 'Paste', and a 'Top' button.

2.2 Configurar DTP (Dynamic Trunking Protocol)

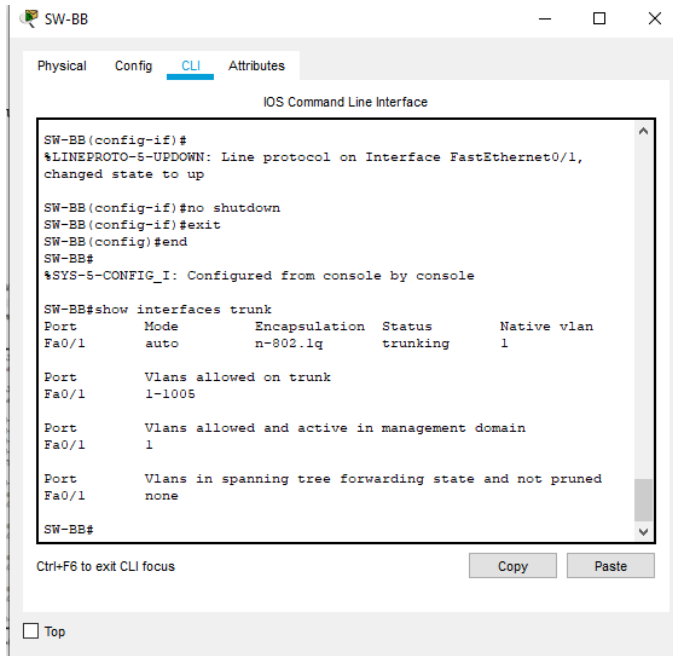
2.2.1 Configure un enlace troncal ("trunk") dinámico entre SW-AA y SW-BB. Debido a que el modo por defecto es **dynamic auto**, solo un lado del enlace debe configurarse como **dynamic desirable**.

```
SW-AA(config)#interface fa0/1
SW-AA(config-if)#switchport mode trunk
```

```
SW-BB(config)#interface fa0/1
SW-BB(config-if)#switchport mode dynamic desirable
```

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

Figura 14. Enlace de trunk en SW-BB



```
SW-BB
Physical Config CLI Attributes
IOS Command Line Interface

SW-BB(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up

SW-BB(config-if)#no shutdown
SW-BB(config-if)#exit
SW-BB(config)#end
SW-BB#
%SYS-5-CONFIG_I: Configured from console by console

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

Port      Vlans allowed on trunk
Fa0/1     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     none

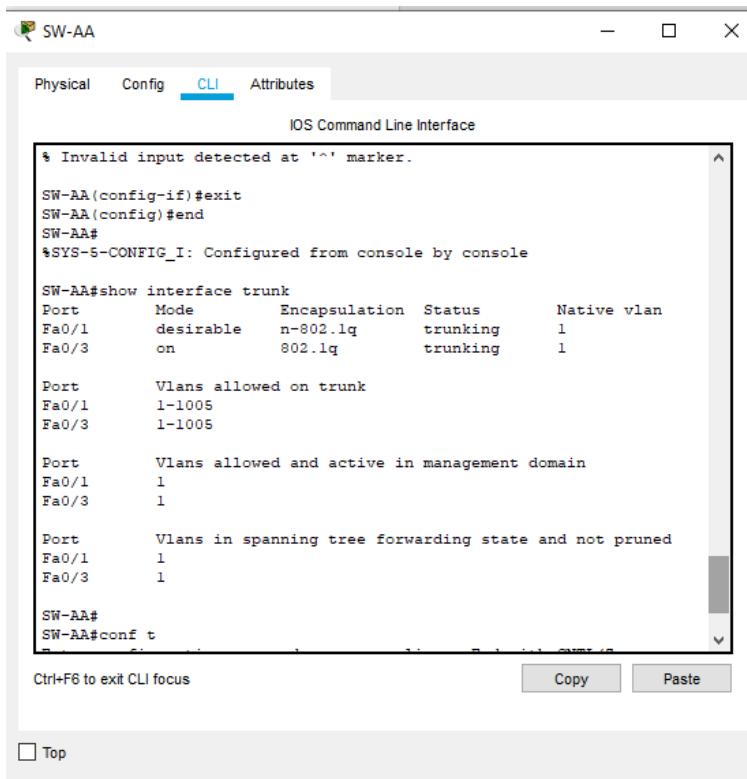
SW-BB#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Figura 15. Enlace de trunk en SW-AA



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

% Invalid input detected at '^' marker.

SW-AA(config-if)#exit
SW-AA(config)#end
SW-AA#
%SYS-5-CONFIG_I: Configured from console by console

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

Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/3     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1
Fa0/3     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1
Fa0/3     1

SW-AA#
SW-AA#conf t
```

Ctrl+F6 to exit CLI focus

Copy Paste

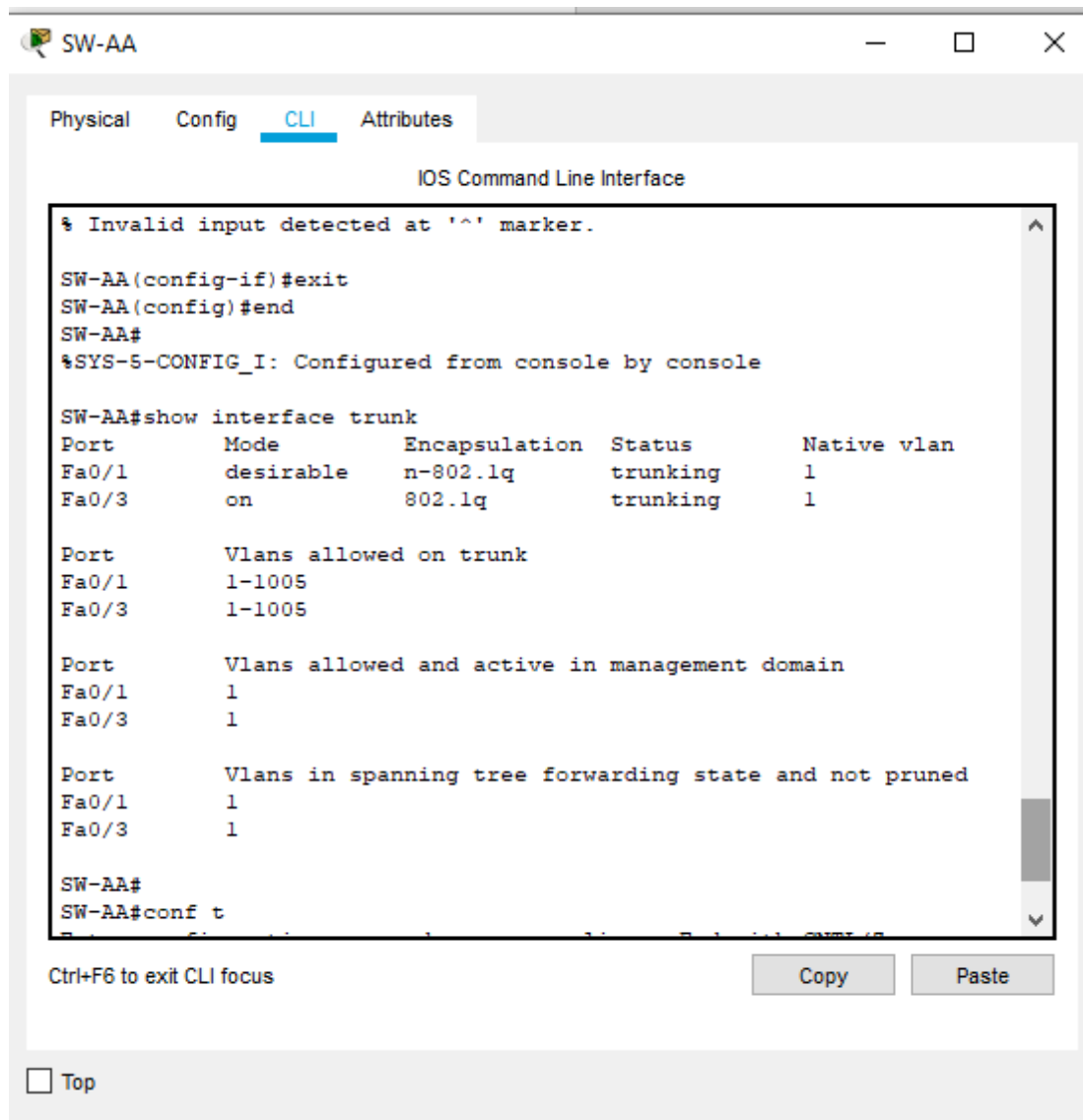
Top

2.2.3 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 f0/3  
SW-AA(config-if)#switchport mode trunk
```

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

Figura 16. Enlace de trunk en SW-AA



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

```
SW-CC(config)#interface f0/1
SW-CC(config-if)#switchport mode trunk
```

```
SW-BB(config)#interface f0/3
SW-BB(config-if)#switchport mode trunk
```

2.3 Agregar VLANs y asignar puertos.

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

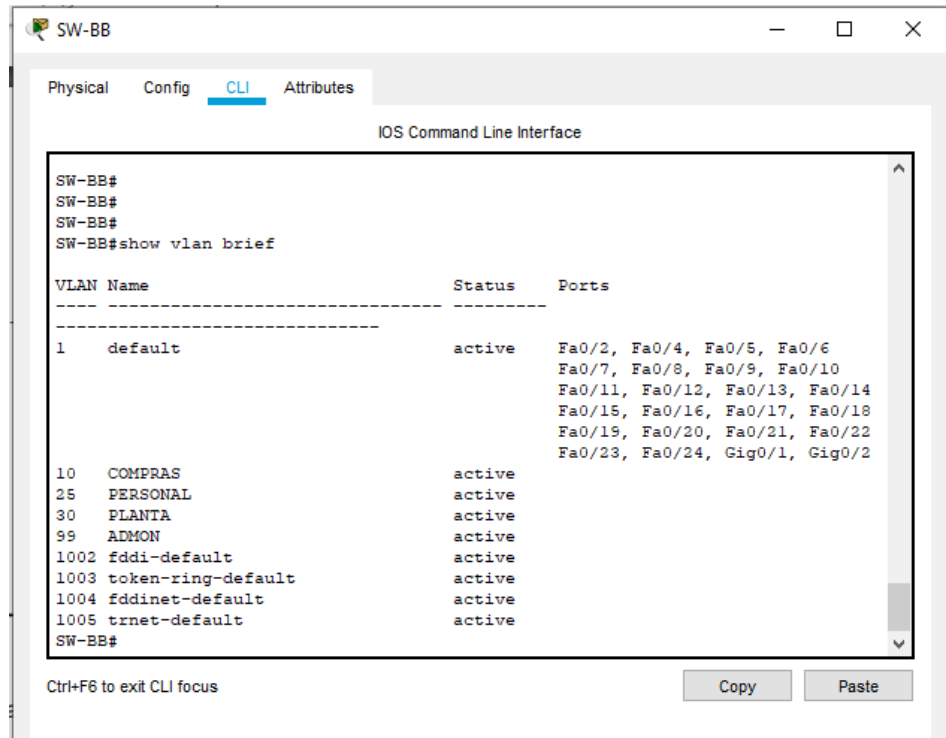
```
SW-AA#conf t
SW-AA(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
SW-AA(config)#
```

La Vlan 10 no puede ser agregada en el SW-AA debido a que se encuentra en modo cliente, se agrega a través de SW-BB que funciona en modo server

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

2.3.2 Verifique que las VLANs han sido agregadas correctamente.

Figura 17. VLANs en SW-BB



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

Tabla 1. Configuración IP

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

X = número de cada PC particular

```

SW-AA#conf t
SW-AA(config)#interface vlan 10
SW-AA(config-if)#ip address 190.180.10.1 255.255.255.0
SW-AA(config-if)#exit
SW-AA(config)#interface vlan 25
SW-AA(config-if)#ip address 190.180.25.1 255.255.255.0
  
```

```

SW-AA(config-if)#exit
SW-AA(config)#interface vlan 30
SW-AA(config-if)#ip address 190.180.30.1 255.255.255.0
SW-AA(config-if)#exit
SW-AA(config)#

```

```

SW-BB#conf t
SW-BB(config)#interface vlan 10
SW-BB(config-if)#ip address 190.180.10.2 255.255.255.0
SW-BB(config-if)#exit
SW-BB(config)#interface vlan 25
SW-BB(config-if)#ip address 190.180.25.2 255.255.255.0
SW-BB(config-if)#exit
SW-BB(config)#interface vlan 30
SW-BB(config-if)#ip address 190.180.30.2 255.255.255.0
SW-BB(config-if)#exit
SW-BB(config)#

```

```

SW-CC#conf t
SW-CC(config)#interface vlan 10
SW-CC(config-if)#ip address 190.180.10.3 255.255.255.0
SW-CC(config-if)#exit
SW-CC(config)#interface vlan 25
SW-CC(config-if)#ip address 190.180.25.3 255.255.255.0
SW-CC(config-if)#exit
SW-CC(config)#interface vlan 30
SW-CC(config-if)#ip address 190.180.30.3 255.255.255.0
SW-CC(config-if)#exit
SW-CC(config)#

```

Tabla 3. Direcciones IP de los PCs

Interfaz	VLAN	Direcciones IP de los PCs
SW-AA F0/10	VLAN 10	190.108.10.1 / 24
SW-AA F0/15	VLAN 25	190.108.25.1 / 24
SW-AA F0/20	VLAN 30	190.108.30.1 / 24
SW-BB F0/10	VLAN 10	190.108.10.2 / 24
SW-BB F0/15	VLAN 25	190.108.25.2 / 24
SW-BB F0/20	VLAN 30	190.108.30.2 / 24

SW-CC F0/10	VLAN 10	190.108.10.3 / 24
SW-CC F0/15	VLAN 25	190.108.25.3 /24
SW-CC F0/20	VLAN 30	190.108.30.3 /24

2.3.4 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 f0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#exit
```

```
SW-BB(config)#interface f0/10
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#exit
```

```
SW-CC(config)#interface f0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#exit
```

2.3.5 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(config)#interface f0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#exit
SW-AA(config)#interface f0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
SW-AA(config-if)#exit
```

```

SW-BB(config)#interface f0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#exit
SW-BB(config)#interface f0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30
SW-BB(config-if)#exit

```

```

SW-CC(config)#interface f0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#exit
SW-CC(config)#interface f0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30
SW-CC(config-if)#exit

```

2.4 Configurar las direcciones IP en los Switches.

2.4.1 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 4. Tabla de direccionamiento

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#conf t
SW-AA(config)#interface vlan 99
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
SW-AA(config-if)#exit

```

```

SW-BB#conf t
SW-BB(config)#interface vlan 99
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0SW-BB(config-if)#exit

```

```

SW-CC#conf t

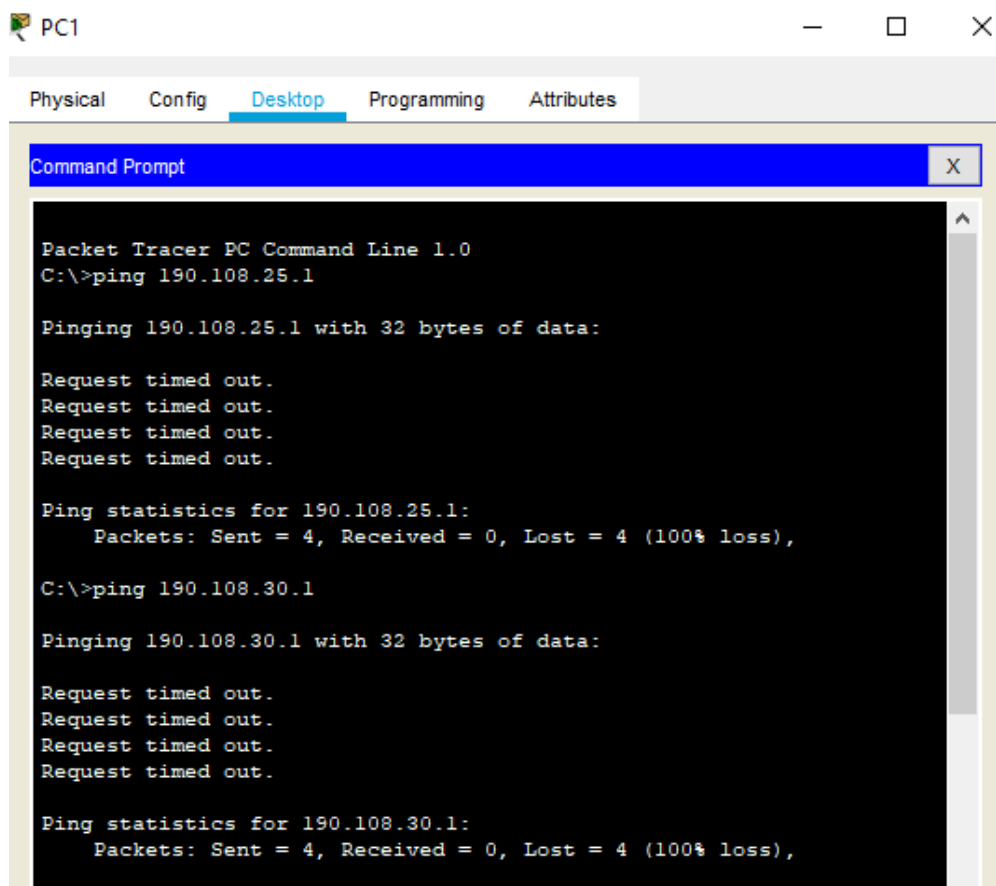
```

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

2.5 Agregar VLANs y asignar puertos.

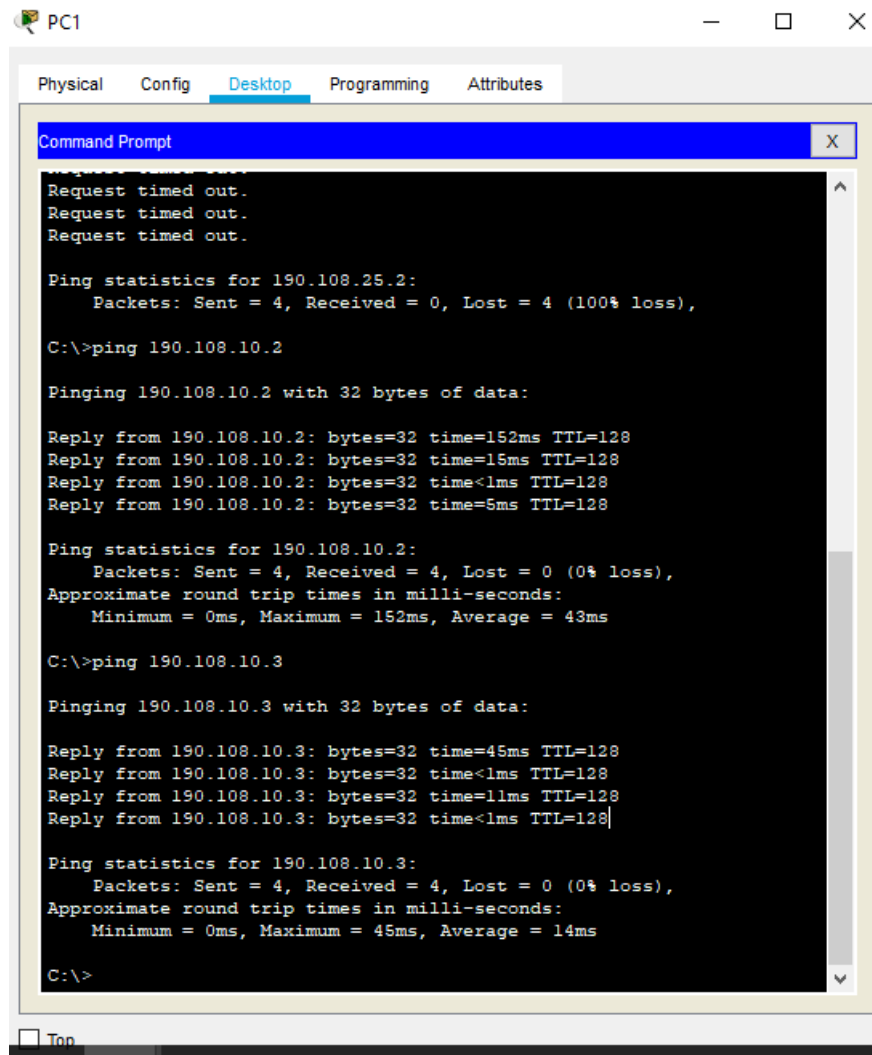
2.5.1 Ejecute un Ping desde cada PC a los demás. Explique por qué el ping tuvo o no tuvo éxito.

Figura 18. Ping des la pc1 a las pc2, pc3



Como podemos ver los ping no fueron exitosos debido a que están en diferente VLAN que en esta pc es la (VLAN 10)

Figura 19. Ping des la pc1 a las pc4, pc7



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.25.2:
    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=152ms TTL=128
Reply from 190.108.10.2: bytes=32 time=15ms TTL=128
Reply from 190.108.10.2: bytes=32 time<1ms TTL=128
Reply from 190.108.10.2: bytes=32 time=5ms 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 = 152ms, Average = 43ms

C:\>ping 190.108.10.3

Pinging 190.108.10.3 with 32 bytes of data:

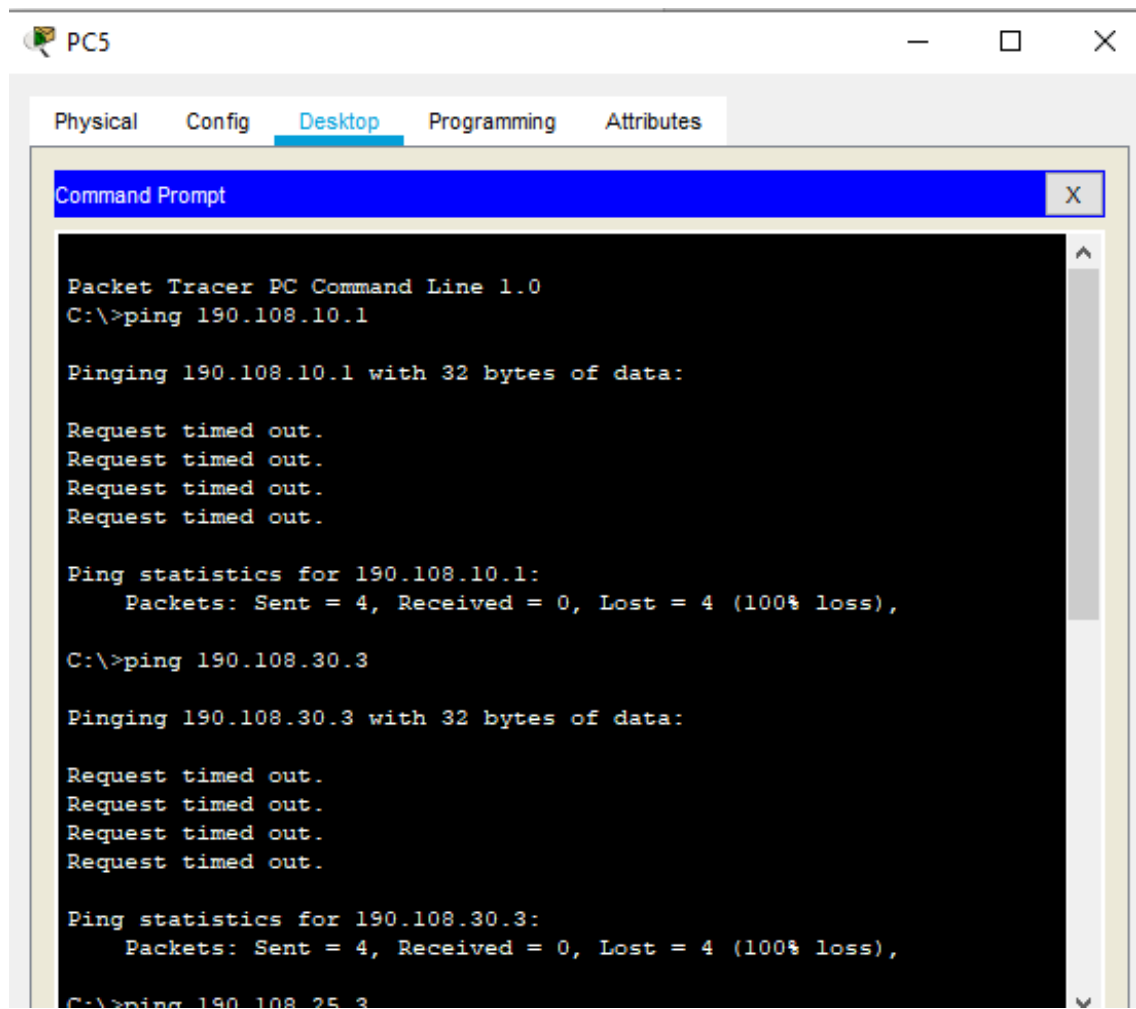
Reply from 190.108.10.3: bytes=32 time=45ms TTL=128
Reply from 190.108.10.3: bytes=32 time<1ms TTL=128
Reply from 190.108.10.3: bytes=32 time=11ms TTL=128
Reply from 190.108.10.3: bytes=32 time<1ms TTL=128

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 = 45ms, Average = 14ms

C:\>
```

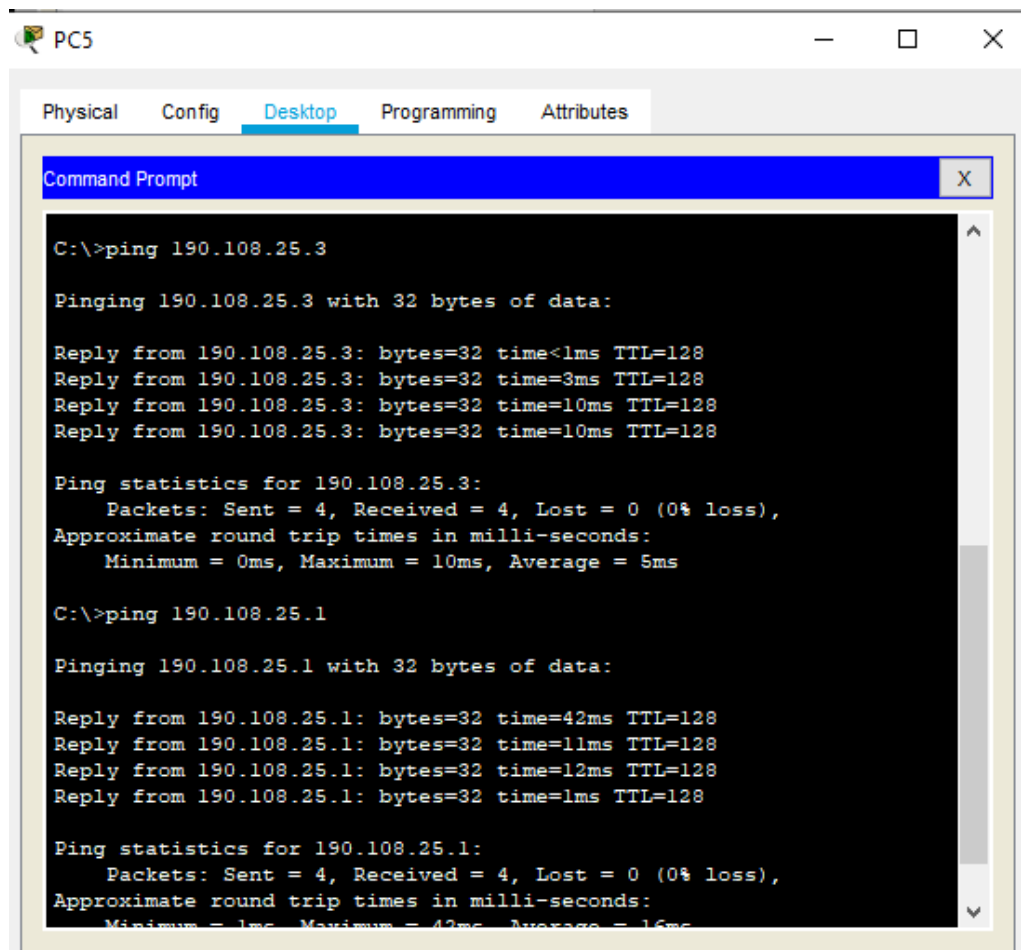
El ping fue exitoso debido a que las pc se encuentran en la misma(vlan 10)
Pc5

Figura 20. Ping des la pc5 a las pc1, pc9



Como podemos ver los ping no fueron exitosos debido a que están en diferente VLAN que en esta pc es la (VLAN 25)

Figura 21. Ping des la pc5 a las pc2, pc8



The screenshot shows a window titled 'PC5' with a 'Desktop' tab selected. Inside the window is a 'Command Prompt' window. The command prompt shows the following output:

```
C:\>ping 190.108.25.3

Pinging 190.108.25.3 with 32 bytes of data:

Reply from 190.108.25.3: bytes=32 time<1ms TTL=128
Reply from 190.108.25.3: bytes=32 time=3ms TTL=128
Reply from 190.108.25.3: bytes=32 time=10ms TTL=128
Reply from 190.108.25.3: bytes=32 time=10ms TTL=128

Ping statistics for 190.108.25.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 5ms

C:\>ping 190.108.25.1

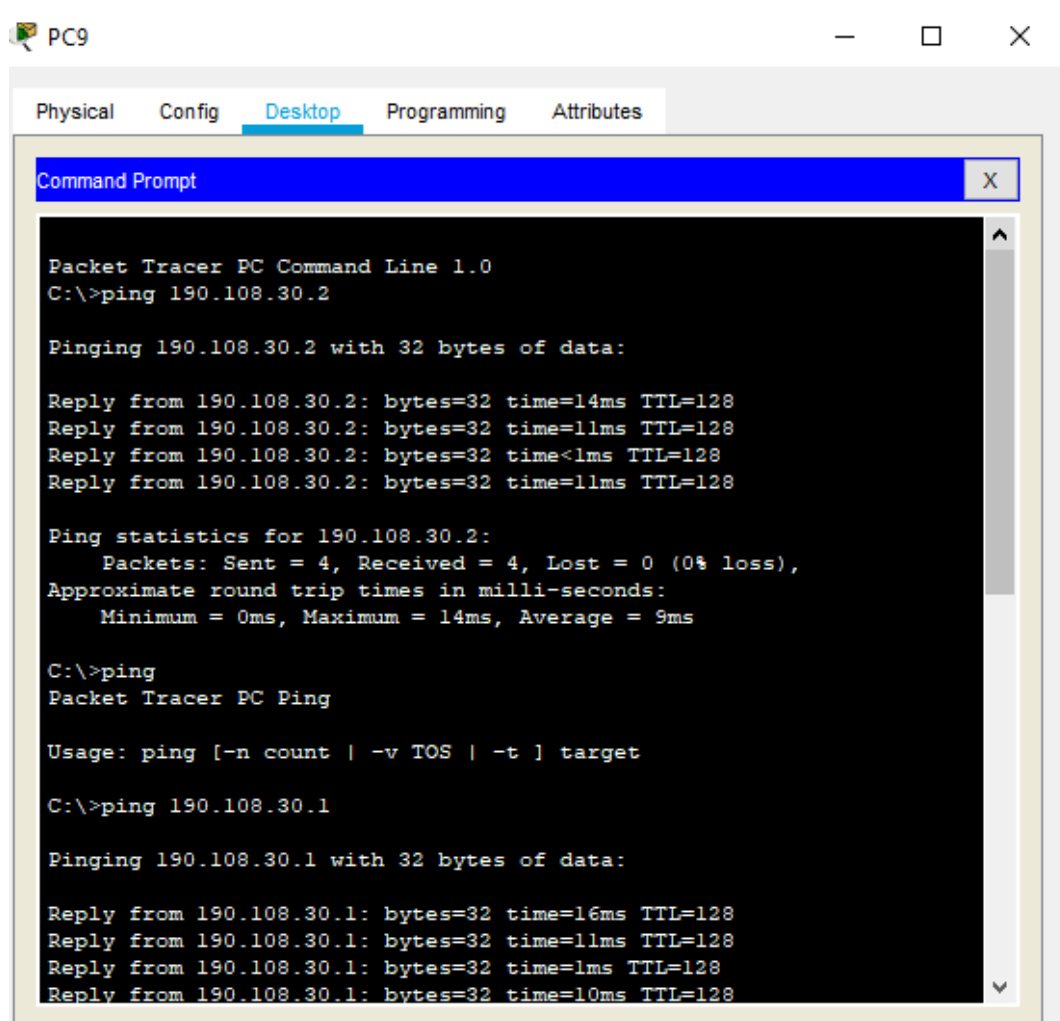
Pinging 190.108.25.1 with 32 bytes of data:

Reply from 190.108.25.1: bytes=32 time=42ms TTL=128
Reply from 190.108.25.1: bytes=32 time=11ms TTL=128
Reply from 190.108.25.1: bytes=32 time=12ms TTL=128
Reply from 190.108.25.1: bytes=32 time=1ms TTL=128

Ping statistics for 190.108.25.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 42ms, Average = 16ms
```

El ping fue exitoso debido a que las pc se encuentran en la misma (vlan 25)

Figura 22. Ping des la pc9 a las pc3, pc6



The screenshot shows a Packet Tracer PC9 desktop environment. The 'Desktop' tab is active, displaying a Command Prompt window. The window title is 'Command Prompt'. The text in the Command Prompt is as follows:

```
Packet Tracer PC Command Line 1.0
C:\>ping 190.108.30.2

Pinging 190.108.30.2 with 32 bytes of data:

Reply from 190.108.30.2: bytes=32 time=14ms TTL=128
Reply from 190.108.30.2: bytes=32 time=11ms TTL=128
Reply from 190.108.30.2: bytes=32 time<1ms TTL=128
Reply from 190.108.30.2: bytes=32 time=11ms TTL=128

Ping statistics for 190.108.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 14ms, Average = 9ms

C:\>ping
Packet Tracer PC Ping

Usage: ping [-n count | -v TOS | -t ] target

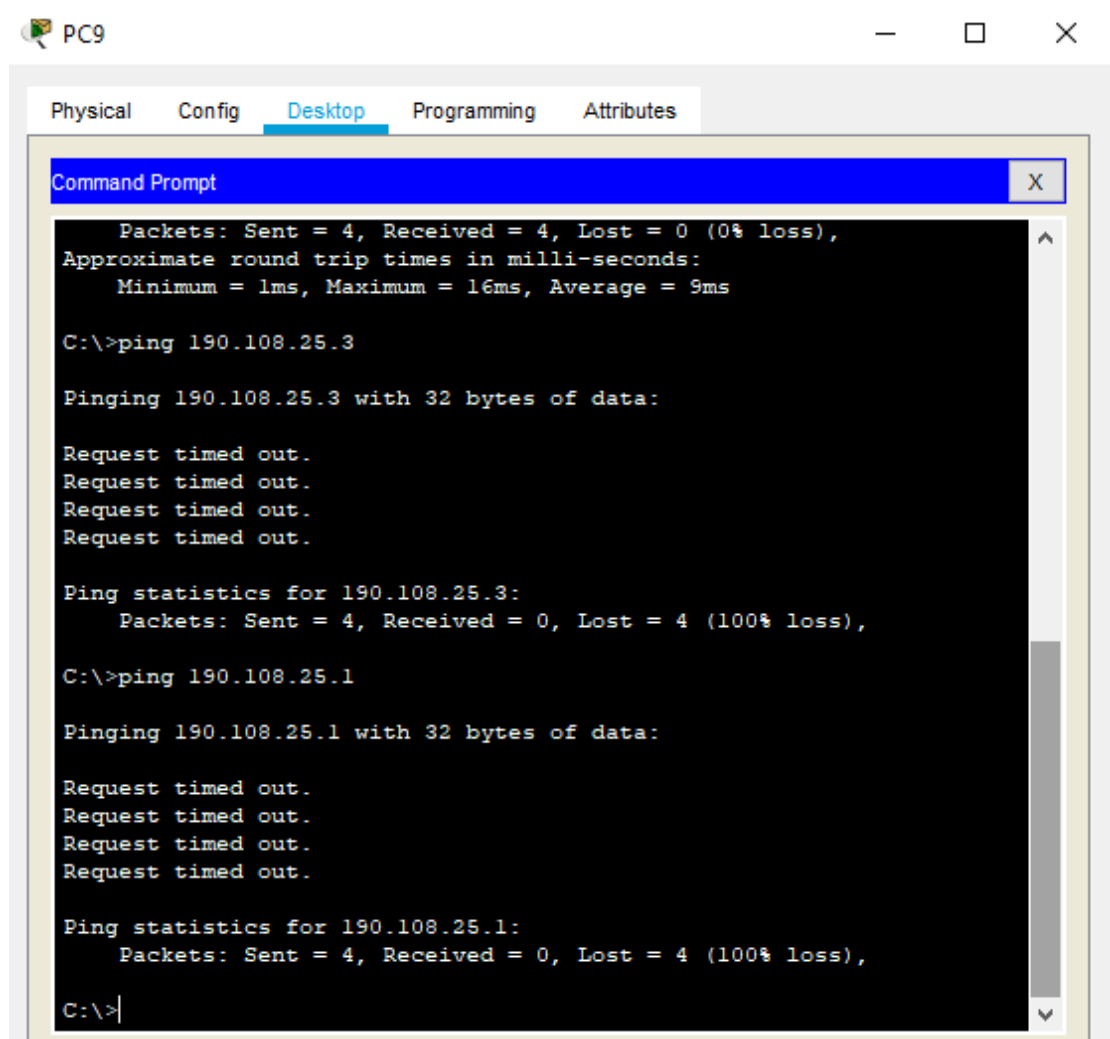
C:\>ping 190.108.30.1

Pinging 190.108.30.1 with 32 bytes of data:

Reply from 190.108.30.1: bytes=32 time=16ms TTL=128
Reply from 190.108.30.1: bytes=32 time=11ms TTL=128
Reply from 190.108.30.1: bytes=32 time=1ms TTL=128
Reply from 190.108.30.1: bytes=32 time=10ms TTL=128
```

El ping fue exitoso debido a que las pc se encuentran en la misma (vlan 30)

Figura 23. Ping des la pc9 a las pc2, pc8



Como podemos ver los ping no fueron exitosos debido a que están en diferente VLAN que en esta pc es la (VLAN 30)

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

Figura 24. Ping desde SW-AA a SW-BB y SW-CC

```
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 = 0/1/4 ms

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 = 0/1/5 ms

SW-AA#
```

Ctrl+F6 to exit CLI focus Copy Paste

Figura 25. Ping desde SW-BB a SW-AA y SW-CC

```
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 = 0/1/4 ms

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

SW-BB#
```

Figura 26. Ping desde SW-CC a SW-AA y SW-BB

```
SW-CC>EN
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

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#
```

Los pings realizados entre los switches son exitosos debido a que tienen en común la (vlan 99)

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

Figura 27. Ping desde SW-AA a las pc1, pc2, pc5, pc6

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#PING 190.108.25.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#PING 190.108.10.1

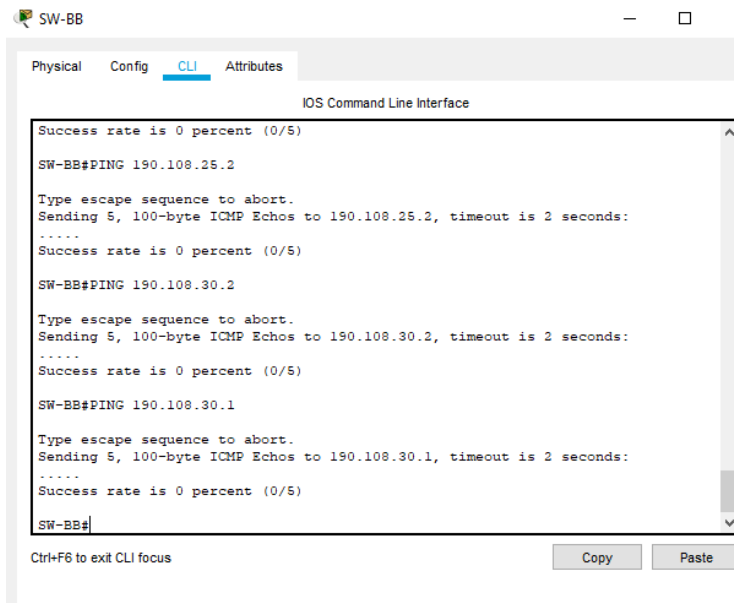
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#PING 190.108.25.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#
```

Figura 28. Ping desde SW-CC a las pc5, pc6, pc3, pc9



The screenshot shows a window titled "SW-BB" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following sequence of commands and results:

```
Success rate is 0 percent (0/5)

SW-BB#PING 190.108.25.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#PING 190.108.30.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

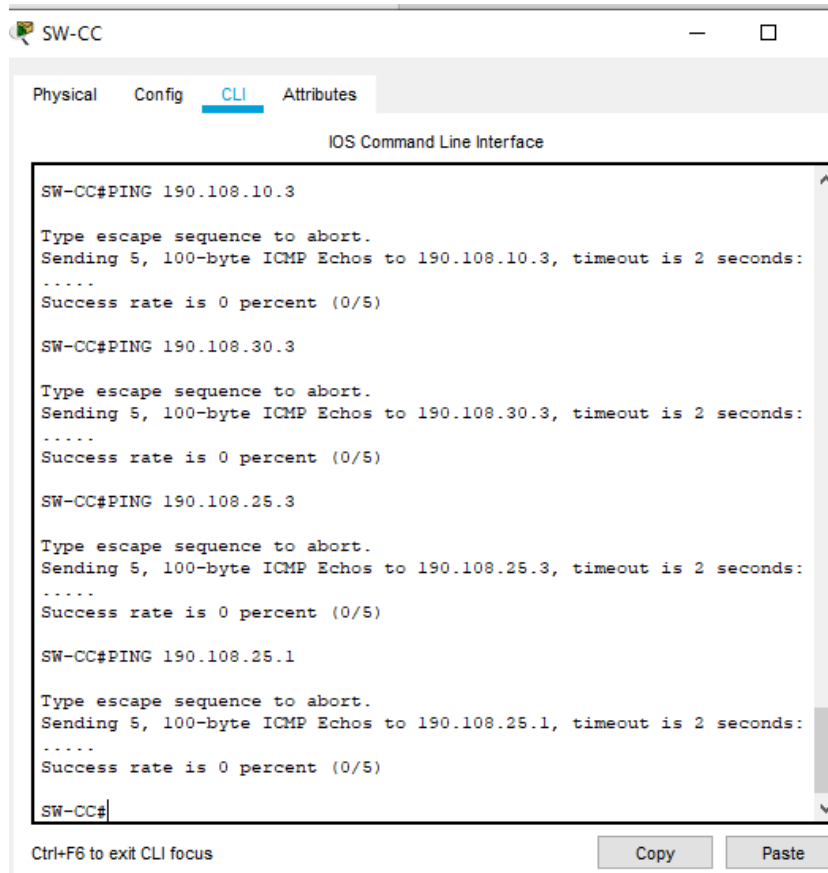
SW-BB#PING 190.108.30.1

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-BB#
```

At the bottom of the window, there is a status bar with "Ctrl+F6 to exit CLI focus" and two buttons: "Copy" and "Paste".

Figura 29. Ping desde SW-CC a las pc3, pc9, pc6, pc2



```
SW-CC
Physical Config CLI Attributes
IOS Command Line Interface
SW-CC#PING 190.108.10.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-CC#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-CC#PING 190.108.25.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-CC#PING 190.108.25.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-CC#
```

Ctrl+F6 to exit CLI focus Copy Paste

Podemos observar que ninguno de ping fue exitoso esto debido a que las interfaces virtuales creadas en los switches están en la vlan 99 y los pc están en las vlan 10, 25 y 30 y en la topología no se implementaron dispositivos de capa 3 que permitan el enrutamiento intervlan.

CONCLUSIONES

En nuestro trabajo pudimos probar nuestros conocimientos adquiridos durante el diplomado de CCNP estableciendo la funcionalidad de los comandos realizados durante el proyecto del paso a paso recordando lo visto en los trabajos colaborativos y los procesos de verificación de conectividad mediante el uso de comandos ping, show ip route, show interfaces trunk, entre otros.

Con nuestro curso diplomado CCNP pudimos adquirir conocimiento necesario para nuestra carrera de ingeniería electrónica ya que desarrollamos habilidades y competencias útiles en la configuración de redes y sus dispositivos como lo son switches y enrutadores que son bases fundamentales para la implementación de redes.

Este curso nos brindó conocimientos debido al método teórico prácticos con el objetivo de que adquirir las capacidades necesarias para proyectar, implementar, asegurar, mantener y solucionar problemas de redes, debemos des tacar los programas de simulación debido a que nos ayudaron a comprender y realizar las redes y sus protocolos de enrutamiento.

REFERENCIAS BIBLIOGRÁFICAS

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

Hucaby, D. (2015). CISCO Press (Ed). CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. Recuperado de <https://1drv.ms/b/s!AqIGg5JUgUBthF16RWCSsCZnfDo2>

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

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