

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

**MALFER MEJIA MENDOZA**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA ELECTRONICA  
BARRANQUILLA  
2020.**

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

**MALFER MEJIA MENDOZA**

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

**DIRECTOR:  
MSc. GERARDO GRANADOS ACUÑA**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA ELECTRONICA  
BARRANQUILLA  
2020.**

**NOTA DE ACEPTACIÓN**

---

---

---

---

---

---

---

\_\_\_\_\_  
**Firma del presidente del Jurado**

\_\_\_\_\_  
**Firma del Jurado**

\_\_\_\_\_  
**Firma del Jurado**

**Barranquilla, Mayo de 2020**

## CONTENIDO

	<b>Pág.</b>
<b>Contenido</b> .....	4
<b>Lista de Figuras</b> .....	6
<b>Lista de Tablas</b> .....	7
<b>Glosario</b> .....	8
<b>Resumen</b> .....	9
<b>Abstract</b> .....	9
<b>Introducción</b> .....	10
<b>Desarrollo de escenarios</b> .....	11
<b>Escenario 1</b> .....	11
Topología.....	12
Configuraciones iniciales.....	13
1. Configuración del vecino BGP para AS1 y AS2.....	15
1.1 Paso a paso de comandos.....	15
1.2 Resultado de configuraciones.....	15
2. Configuración del vecino BGP para AS2 y AS3.....	16
2.1 Paso a paso de comandos.....	16
2.2 Resultado de configuraciones.....	17
3. Configuración del vecino BGP para AS3 y AS4.....	18
3.1 Paso a paso de comandos.....	18
3.2 Resultado de configuraciones.....	18
<b>Escenario 2</b> .....	20
Topología.....	22
A. Configuración VTP.....	22
1. Configuración de switches para uso de VTP.....	23
2. Resultado de configuraciones.....	24
B. Resultado de configuraciones.....	25
1. Configuración de enlaces troncales SW-AA y SW-BB.....	25

2. Resultado de configuraciones.....	26
3. Configuración de enlace troncal estático SW-AA y SW-BB.....	27
4. Resultado de configuraciones.....	27
5. Configuración enlace troncal permanente SW-BB y SW-CC....	27
C. Creación de VLANs y asignación de puertos.....	28
1. Creación de VLANs.....	28
2. Resultado de configuraciones.....	29
3. Asignación de puertos y direcciones IP.....	29
4. Configuración en modo acceso y asignación de VLAN 10.....	30
5. Configuración en modo acceso y asignación de VLANs 25, 30 y fijación de Ip a PC´s.....	30
D. Configuración de direcciones ip en los switches.....	31
E. Verificación de conectividad extremo a extremo.....	32
1. Ping desde cada PC1 a los demás.....	32
2. Ping desde cada PC5 a los demás.....	33
3. Ping desde cada PC9 a los demás.....	34
4. Ping desde cada switch a los demás.....	35
5. Ping desde cada switch a cada PC.....	37
<b>Conclusiones.....</b>	<b>39</b>
<b>Referencias bibliográficas.....</b>	<b>40</b>

## LISTA DE FIGURAS

	<b>Pág.</b>
Figura 1 - Topología sugerida.....	11
Figura 2 - Topología diseñada.....	12
Figura 3 - Resultado en R1.....	15
Figura 4 - Resultados en R2.....	16
Figura 5 - Resultados en R2.....	17
Figura 6 - Resultados en R3.....	17
Figura 7 - Resultados en R3.....	18
Figura 8 - Resultados en R4.....	19
Figura 9 - Topología sugerida.....	20
Figura 10 - Topología diseñada.....	22
Figura 11 - VTP mode client SW-AA.....	24
Figura 12 - VTP mode server SW-BB.....	24
Figura 13 - VTP mode client SW-CC.....	25
Figura 14 - Enlace troncal en SW-AA.....	26
Figura 15 - Enlace troncal en SW-BB.....	26
Figura 16 - Enlace troncal estático en SW-AA.....	27
Figura 17 - VLANs.....	29
Figura 18 - ping de PC1 a PC4, PC5 y PC9.....	32
Figura 19 - ping de PC5 a PC8, PC7 y PC3.....	33
Figura 20 - ping de PC9 a PC6, PC4 y PC2.....	34
Figura 21 - ping en SW-AA.....	35
Figura 22 - ping en SW-BB.....	35
Figura 23 - ping en SW-CC.....	36
Figura 24 - ping desde SW-AA.....	37
Figura 25 - ping desde SW-BB.....	37
Figura 26 - ping desde SW-CC.....	38

## LISTA DE TABLAS

	<b>Pág.</b>
Tabla 1 - Información para la configuración de router.....	11
Tabla 2 - Puertos VLAN y direcciones Ip sugeridas.....	21
Tabla 3 - Direcciones ip para switches sugeridas.....	21
Tabla 4 - Puertos y direcciones ip.....	29
Tabla 5 - Direcciones ip en los switches.....	31

## Glosario

**FASTETHERNET:** Es una Red de Área Local (LAN) de transmisión estándar y que proporciona una cantidad de datos de 100 megabits por segundo.

**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 VLANs con ISL o 802.1Q) en enlaces Ethernet.

**LOOPBACK:** Es una interfaz de red virtual o una dirección especial que los hosts utilizan para dirigir el tráfico hacia ellos mismos. Es un método de acceso directo para las aplicaciones y servicios TCP/IP que se ejecutan en el mismo dispositivo para comunicarse entre sí.

**VLAN (Red de área local virtual o LAN virtual):** Es una red de área local que agrupa un conjunto de equipos de manera lógica y no física.

**PROTOCOL VTP:** Es un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite centralizar y simplificar la administración en un dominio de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos.

**FIREWALL:** Combinación de hardware y software la cual separa una red de área local (LAN) en dos o más partes con propósitos de seguridad. Su objetivo básico es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad, autenticación, etc.

**HOST:** Servidor que nos provee de la información que requerimos para realizar algún procedimiento desde una aplicación cliente a la que tenemos acceso de diversas formas. Al igual que cualquier computadora conectada a Internet, debe tener una dirección o número IP y un nombre.

**INTERFACE:** Interfaz o interface es el punto de conexión ya sea dos componentes de hardware, dos programas o entre un usuario y un programa.



## **RESUMEN**

En este informe se consolida el desarrollo de la prueba final de habilidades prácticas del Diplomado de profundización CCNP, por medio de la cual se plantean dos escenarios o situaciones problemáticas; en los cuales se deben logra contextualizar los conocimientos teóricos sobre conmutación y enrutamiento. Soportándolos en las habilidades prácticas desarrolladas sobre estos, a través del curso. Estos escenarios implican el armado de dos topologías de redes, su configuración electrónica e interconexión de cada uno de los dispositivos CISCO, la redistribución de rutas, creación de subredes, configuración del protocolo DTP (Dynamic Trunking Protocol) y del protocolo VTP. También se hace necesario la configuración de enrutamiento IPv4 en interfaces Seriales, FastEthernet, Loopback y de acceso a la red por parte de usuarios finales. Así mismo se solicita establecer un dispositivo servidor a partir del cual se actualice la configuración de otros dispositivos, clientes, como parte del enrutamiento a través de redes de área local virtuales (Vlans).

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

## **ABSTRACT**

This report consolidates the development of the final practical skills test of the CCNP Deepening Diploma, through which two scenarios or problematic situations are proposed; in which the theoretical knowledge on switching and routing must be contextualized. Supporting them in the practical skills developed on them, through the course. These scenarios involve the assembly of two network topologies, their electronics configuration and interconnection of each of the CISCO devices, the redistribution of routes, the creation of subnets, the configuration of the DTP (Dynamic Trunking Protocol) and the VTP protocol. IPv4 routing configuration is also required on Serial, FastEthernet, Loopback and networking access interfaces by end users. Likewise, it is requested to establish a server device from which the configuration of other devices, clients, is updated as part of the routing through virtual local area networks (Vlans).

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

## INTRODUCCION

En el presente documento se consigna el desarrollo de la Prueba de Habilidades Practicas y evaluativas del curso de Diplomado de Profundización CCNP, mediante la cual se busca identificar el nivel de desarrollo de competencias y habilidades que se ha logramos adquirir a lo largo del mismo. Por medio de dos escenarios propuestos se quiere poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de a las redes. Como principio general se configurará interfaces loopback, la configuración de vecino BGP, configuración VTP, configuración DTP y creación y configuración de VLANs.

Una red de comunicación es un grupo de equipos informáticos interconectados, por medio de los cuales se troca datos, para formar una red se requieren elementos como hardware, software y protocolos. La topología de una red es el vínculo de dispositivos e interconexiones entre ellos. Existen diferentes tipos de topologías, como: topología hibrida o mixta, red en malla, red en árbol, red en estrella, red en anillo, red en bus.

Para lograr el objetivo, se hace necesario abordan temáticas como de enrutamiento a través del protocolo BGP y el proceso de creación de adyacenticas en función del protocolo IPv4, del Router ID e interfaces Loopback. Como también, se evidencia la configuración de una pequeña red basada en Switches capa 2 y PCs, en la cual se configura el enrutamiento IPv4 respectivo, se implementa protocolos como VLAN Trunking Protocol y Dynamic Trunking Protocol, así como una parte inicial del enrutamiento InterVLAN. Ahora la verificación de conectividad, se realiza mediante el uso de comandos como ping, show ip route, show vtp status, show interfaces trunk, entre otros.

## ESCENARIO 1

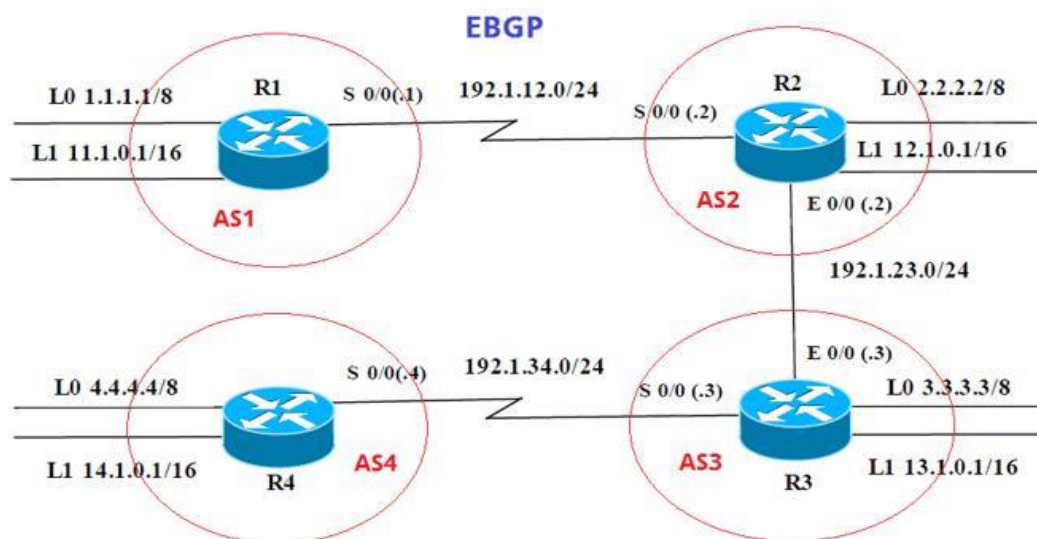


Figura 1 - Topología sugerida

Información para la configuración de los routers

	INTERFAZ	DIRECCION 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	DIRECCION 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
	E1/0	192.1.23.2	255.255.255.0

	INTERFAZ	DIRECCION IP	MÁSCARA
R3	Loopback 0	3.3.3.3	255.0.0.0
	Loopback 1	13.1.0.1	255.255.0.0
	S 0/0	192.1.34.3	255.255.255.0
	E1/0	192.1.23.3	255.255.255.0

	INTERFAZ	DIRECCION 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

Tabla 1 - información para la configuración de routers

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**.
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**.
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 44.44.44.44. 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**.

## SOLUCIÓN

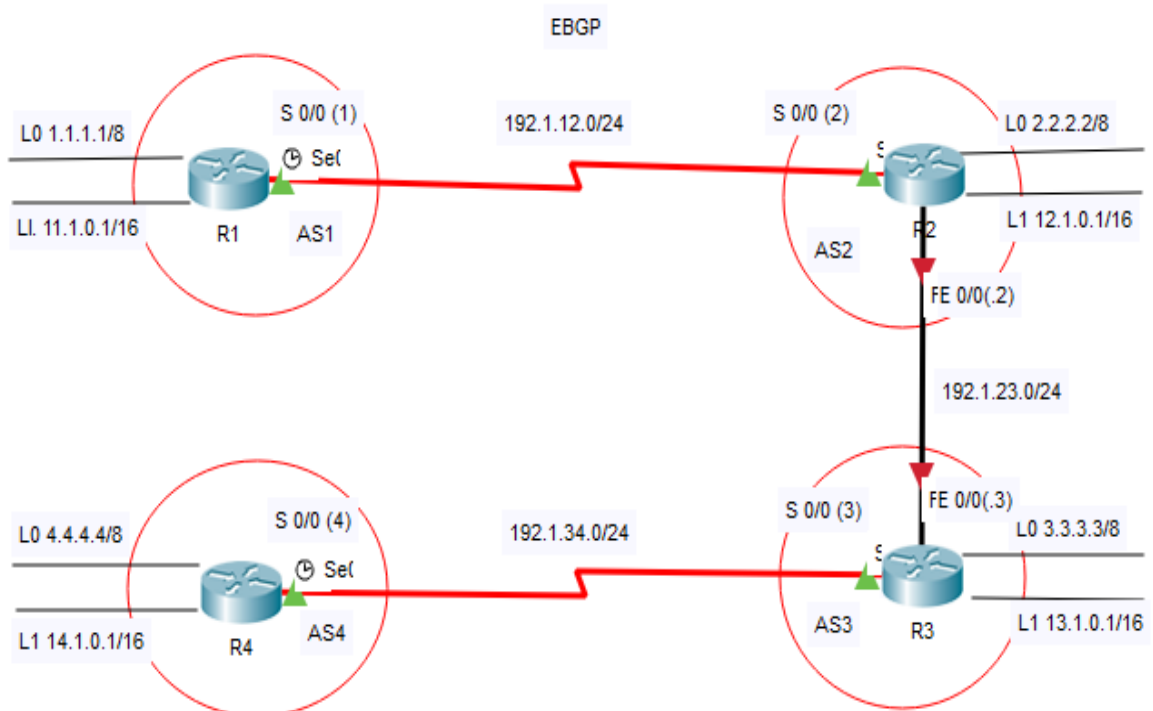


Figura 2 - Topología diseñada

## Configuraciones iniciales

### R1

```
Router> en
Router# conf t
Router(config)# no ip domain-lookup
Router(config)# line con 0
Router(config-line)# logging synchronous
Router(config-line)# exec-timeout 0 0
Router(config-line)# end

Router# conf t
Router(config)# hostname AS1
AS1(config)# int s0/0
AS1(config-if)# ip address 192.1.12.1 255.255.255.0
AS1(config-if)# no shut
AS1(config-if)# exit
AS1(config)# int loopback 0
AS1(config-if)# ip address 1.1.1.1 255.0.0.0
AS1(config-if)# exit

AS1(config)# int loopback 1
AS1(config-if)# ip address 11.1.0.1 255.255.0.0
AS1(config-if)# exit
```

### R2

```
Router> en
Router# conf t
Router(config)# no ip domain-lookup
Router(config)# line con 0
Router(config-line)# logging synchronous
Router(config-line)# exec-timeout 0 0
Router(config-line)# end

Router# conf t
Router(config)# hostname AS2
AS2(config)# int s0/0
AS2(config-if)# ip address 192.1.12.2 255.255.255.0
AS2(config-if)# no shut
AS2(config-if)# exit

AS2(config)# Interface FastEthernet0/0
AS2(config-if)# ip address 192.1.23.2 255.255.255.0
AS2(config-if)# no shut
AS2(config-if)# exit

AS2(config)# int loopback 0
AS2(config-if)# ip address 2.2.2.2 255.0.0.0
AS2(config-if)# exit

AS2(config)# int loopback 1
AS2(config-if)# ip address 12.1.0.1 255.255.0.0
AS2(config-if)# exit
```

## R3

```
Router> en
Router# conf t
Router(config)# no ip domain-lookup
Router(config)# line con 0
Router(config-line)# logging synchronous
Router(config-line)# exec-timeout 0 0
Router(config-line)# end

Router# conf t
Router(config)# hostname AS3
AS3(config)# int s0/0
AS3(config-if)# ip address 192.1.34.3 255.255.255.0
AS3(config-if)# no shut
AS3(config-if)# exit

AS3(config)# Interface FastEthernet0/0
AS3(config-if)# ip address 192.1.23.3 255.255.255.0
AS3(config-if)# no shut
AS3(config-if)# exit

AS3(config)# int loopback 0
AS3(config-if)# ip address 3.3.3.3 255.0.0.0
AS3(config-if)# exit

AS3(config)# int loopback 1
AS3(config-if)# ip address 13.1.0.1 255.255.0.0
AS3(config-if)# exit
```

## R4

```
Router> en
Router# conf t
Router(config)# no ip domain-lookup
Router(config)# line con 0
Router(config-line)# logging synchronous
Router(config-line)# exec-timeout 0 0
Router(config-line)# end

Router# conf t
Router(config)# hostname AS4
AS4(config)# int s0/0
AS4(config-if)# ip address 192.1.34.4 255.255.255.0
AS4(config-if)# no shut
AS4(config-if)# exit

AS4(config)# int loopback 0
AS4(config-if)# ip address 4.4.4.4 255.0.0.0
AS4(config-if)# exit

AS4(config)# int loopback 1
AS4(config-if)# ip address 14.1.0.1 255.255.0.0
AS4(config-if)# exit
```

## 1. Configuración del vecino BGP para AS1 y AS2

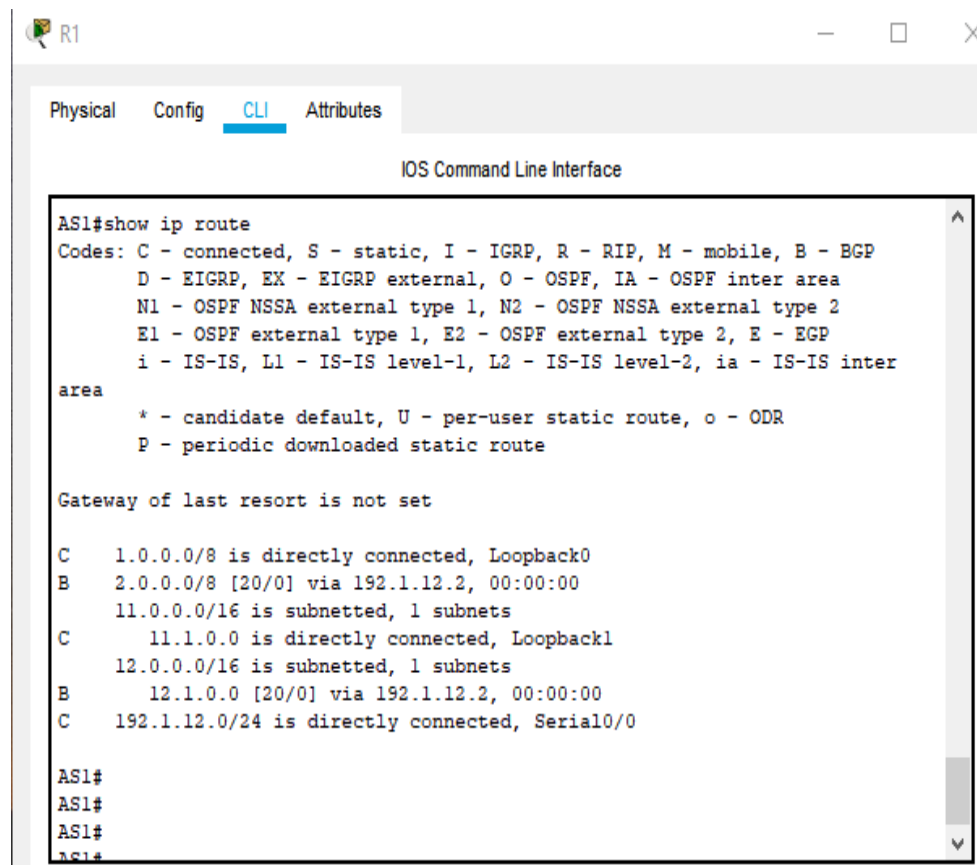
BGP es el protocolo por medio del cual se troca información de direccionamiento entre sistemas autónomos.

### 1.1 Paso a paso de comandos

```
AS1# conf t
AS1(config)# router bgp 10
AS1(config-router)# bgp router-id 22.22.22.22
AS1(config-router)# neighbor 192.1.12.2 remote-as 20
AS1(config-router)# network 1.1.0.0 mask 255.0.0.0
AS1(config-router)# network 11.1.0.0 mask 255.255.0.0
AS1(config-router)# exit

AS2# conf t
AS2(config)# router bgp 20
AS2(config-router)# bgp router-id 33.33.33.33
AS2(config-router)# neighbor 192.1.12.1 remote-as 10
AS2(config-router)# network 2.2.0.0 mask 255.0.0.0
AS2(config-router)# network 12.1.0.0 mask 255.255.0.0
AS2(config-router)# exit
```

### 1.2. Resultados



```
AS1#show ip route
Codes: C - connected, S - static, I - IGRP, 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

C    1.0.0.0/8 is directly connected, Loopback0
B    2.0.0.0/8 [20/0] via 192.1.12.2, 00:00:00
     11.0.0.0/16 is subnetted, 1 subnets
C       11.1.0.0 is directly connected, Loopback1
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.12.2, 00:00:00
C    192.1.12.0/24 is directly connected, Serial0/0

AS1#
AS1#
AS1#
AS1#
```

Figura 3 - resultado en R1

```

AS2#
%SYS-5-CONFIG_I: Configured from console by console

AS2# show ip route
Codes: C - connected, S - static, I - IGRP, 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 directly connected, Loopback0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.12.1, 00:00:00
     12.0.0.0/16 is subnetted, 1 subnets
C       12.1.0.0 is directly connected, Loopback1
C    192.1.12.0/24 is directly connected, Serial0/0

AS2#

```

Figura 4 - Resultados en R2

Las figuras 3 y 4, se puede evidenciar tanto para R1 y para R2, sus tablas de enrutamiento, con las direcciones de Loopback y las redes configuradas en las interfaces Loopback de su respectivo router vecino. Estas últimas fácilmente identificables mediante el código B, esto nos indica que fueron aprendidas a través del protocolo BGP. También, se puede ver en la tabla de enrutamiento que cada router las rutas, la red 192.1.12.0/24 conectada a través de la interfaz serial 0/0.

## 2. Configuración del vecino BGP para AS2 y AS3

### 2.1. Paso a paso de comandos

```

AS2# conf t
AS2(config)# router bgp 20
AS2(config-router)# neighbor 192.1.23.3 remote-as 30
AS2(config-router)# exit

```

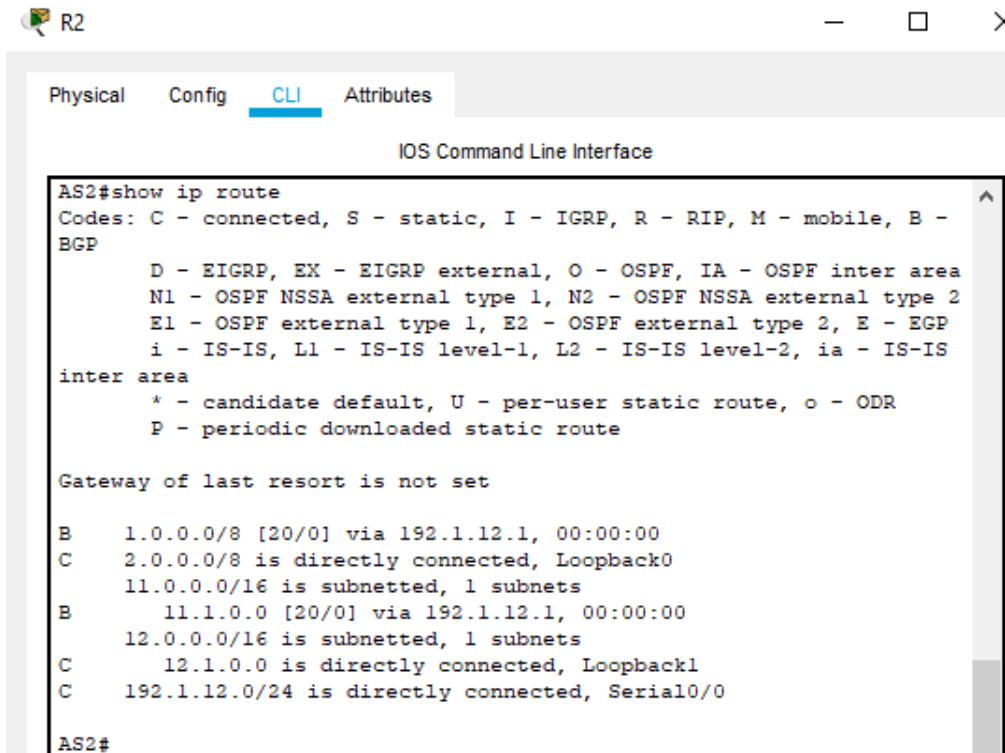
```

AS3# conf t
AS3(config)# router bgp 30
AS3(config-router)# bgp router-id 44.44.44.44
AS3(config-router)# neighbor 192.1.23.2 remote-as 20
AS3(config-router)# network 3.3.0.0 mask 255.0.0.0
AS3(config-router)# network 13.1.0.0 mask 255.255.0.0
AS3(config-router)# exit

```



## 2.2. Resultados



The screenshot shows the CLI of router R2. The command 'show ip route' has been executed, displaying the routing table. The output includes a legend for route codes, a note about the gateway of last resort, and a list of routes with their respective metrics and interfaces.

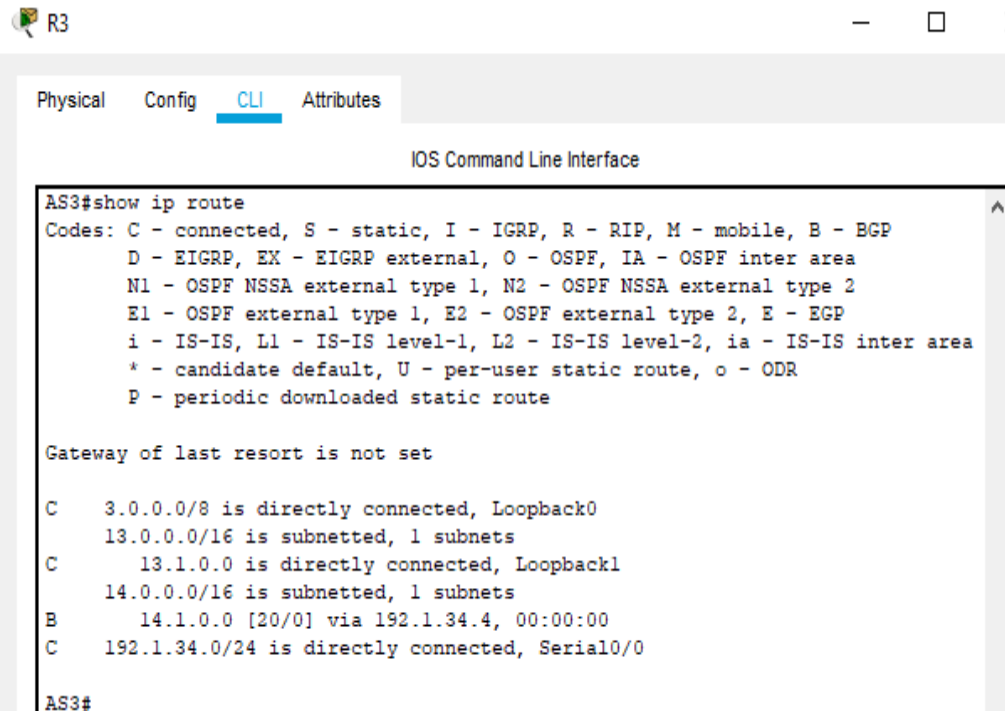
```
AS2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       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 directly connected, Loopback0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.12.1, 00:00:00
     12.0.0.0/16 is subnetted, 1 subnets
C       12.1.0.0 is directly connected, Loopback1
C    192.1.12.0/24 is directly connected, Serial0/0

AS2#
```

Figura 5 - Resultados en R2



The screenshot shows the CLI of router R3. The command 'show ip route' has been executed, displaying the routing table. The output includes a legend for route codes, a note about the gateway of last resort, and a list of routes with their respective metrics and interfaces.

```
AS3#show ip route
Codes: C - connected, S - static, I - IGRP, 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

C    3.0.0.0/8 is directly connected, Loopback0
     13.0.0.0/16 is subnetted, 1 subnets
C       13.1.0.0 is directly connected, Loopback1
     14.0.0.0/16 is subnetted, 1 subnets
B       14.1.0.0 [20/0] via 192.1.34.4, 00:00:00
C    192.1.34.0/24 is directly connected, Serial0/0

AS3#
```

Figura 6 - Resultados en R3

En las figuras 5 y 6. Se observa, la actualización que sufrió la tabla de enrutamiento para R2 y ahora contiene también las direcciones de Loopback configuradas en el router R3. Para este último se dan las direcciones de red correspondientes a las interfaces Loopback que se configuraron en R2 y R1, rutas que aprendió mediante el protocolo BGP gracias a su relación de adyacencia con R2: también se identifica que R3 alcanza todas estas redes a través de la interfaz fastEthernet 0/0 que lo conecta con R2 (192.1.23.0/24). Ahora se configuraron en R2 y R1, rutas que aprendió mediante el protocolo BGP gracias a su relación de adyacencia con R2 y a que dichas redes se anunciaron en cada uno de los routers, así también, R3 contiene la dirección de red que conecta los routers R1 y R2 la cual aprendió mediante el protocolo BGP.

### 3. Configuración del vecino BGP para AS3 y AS4

#### 3.1. Paso a paso de comandos

```
AS3# conf t
AS3(config)# router bgp 30
AS3(config-router)# neighbor 192.1.34.4 remote-as 40
AS3(config-router)# exit

AS4# conf t
AS4(config)# router bgp 40
AS4(config-router)# bgp router-id 66.66.66.66
AS4(config-router)# neighbor 192.1.34.3 remote-as 30
AS4(config-router)# network 14.1.0.0 mask 255.255.0.0
AS4(config-router)# exit
```

#### 3.2. Resultados

```

R3
Physical Config CLI Attributes
IOS Command Line Interface
AS3#show ip route
Codes: C - connected, S - static, I - IGRP, 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

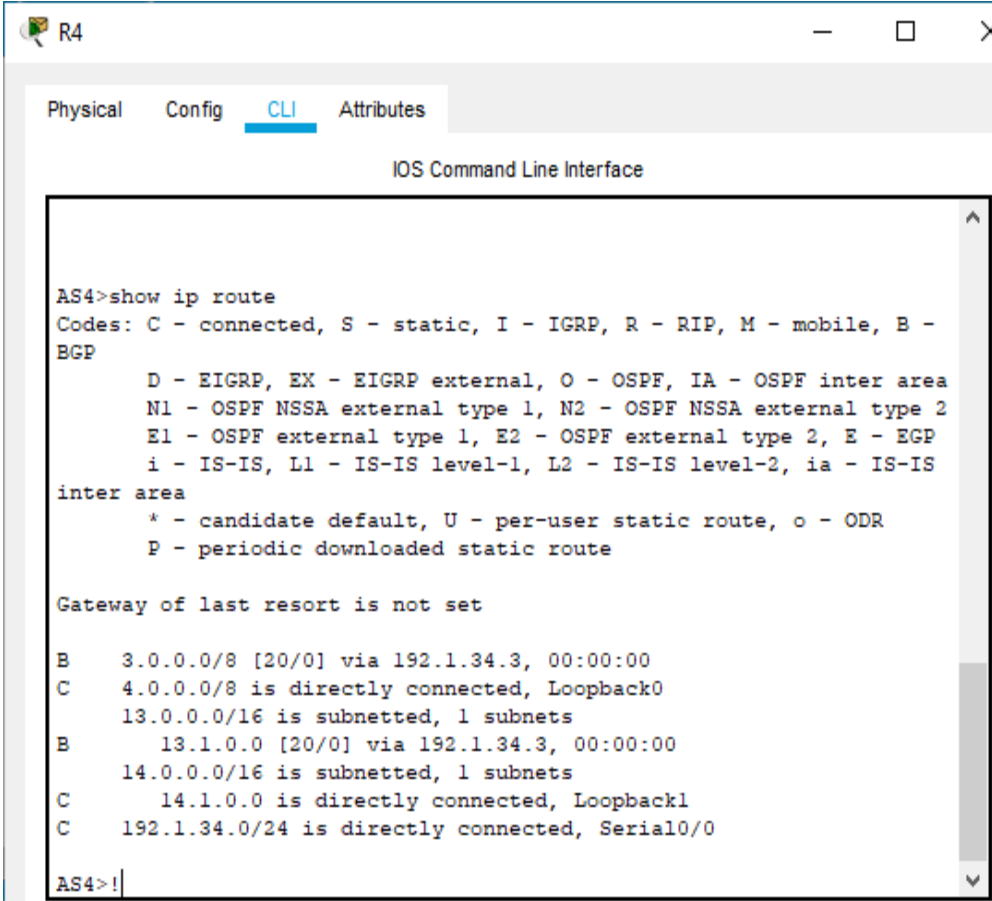
Gateway of last resort is not set

C    3.0.0.0/8 is directly connected, Loopback0
     13.0.0.0/16 is subnetted, 1 subnets
C      13.1.0.0 is directly connected, Loopback1
     14.0.0.0/16 is subnetted, 1 subnets
B      14.1.0.0 [20/0] via 192.1.34.4, 00:00:00
C     192.1.34.0/24 is directly connected, Serial0/0

AS3#

```

Figura 7 - Resultados en R3



```
AS4>show ip route
Codes: C - connected, S - static, I - IGRP, 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    3.0.0.0/8 [20/0] via 192.1.34.3, 00:00:00
C    4.0.0.0/8 is directly connected, Loopback0
     13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0 [20/0] via 192.1.34.3, 00:00:00
     14.0.0.0/16 is subnetted, 1 subnets
C       14.1.0.0 is directly connected, Loopback1
C    192.1.34.0/24 is directly connected, Serial0/0

AS4>!
```

Figura 8 - Resultados en R4

En las figuras 7 y 8, se observa que R3 ha actualizado su tabla de enrutamiento y la dirección de red que conecta este dispositivo con R4 ha cambiado y ahora corresponde a la dirección de Loopback 0, la cual aparece como una dirección estática. Aun así mantiene la dirección lógica Loopback 0 para establecer la adyacencia, la vía de conexión física sigue siendo la red 192.1.4.0/24 correspondiente a la interfaz serial 0/0. Los demás vecinos no se alteraron, por tanto, las demás entradas de la tabla de enrutamiento permanecen iguales. De otro lado, en la tabla de enrutamiento del router R4 se puede evidenciar que la dirección mediante la cual este se comunica con sus vecinos BGP ha cambiado y ahora corresponde a la dirección de la interfaz Loopback 0 de R3. Se muestra, además, en el resultado del comando show ip route, la ruta estática que se creó hacia R3.

## ESCENARIO 2

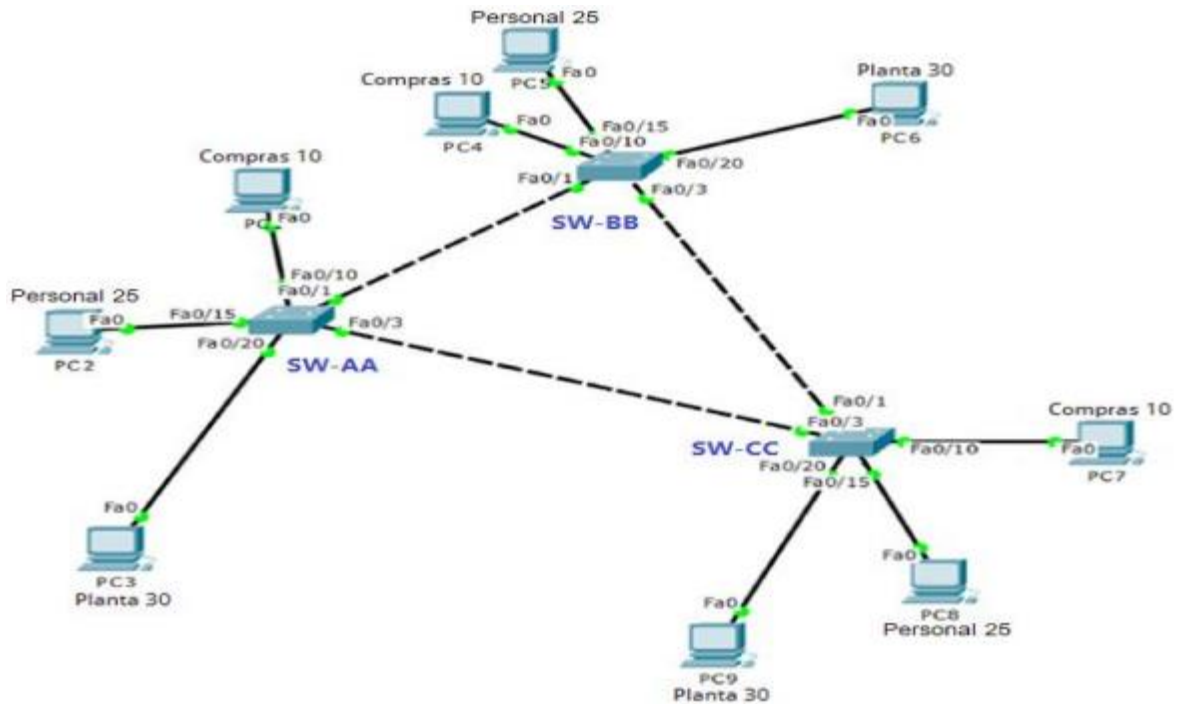


Figura 9 - Topología sugerida

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

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

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

4. Verifique el enlace "trunk" el comando show interfaces trunk en SW-AA.
5. Configure un enlace "trunk" permanente entre SW-BB y SW-CC.

**C. Agregar VLANs y asignar puertos.**

1. En SW-AA agregue la VLAN 10. En SW-BB agregue las VLANs Compras (10), Personal (25), Planta (30) y Admon (99)
2. Verifique que las VLANs han sido agregadas correctamente.
3. Asocie los puertos a las VLAN y configure las direcciones IP de acuerdo con la siguiente tabla.

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.X / 24
F0/15	VLAN 25	190.108.20.X / 24
F0/20	VLAN 30	190.108.30.X / 24

*Tabla 2 - puertos VLAN y direcciones ip sugeridas*

X = número de cada PC particular

4. Configure el puerto F0/10 en modo de acceso para SWT1, SWT2 y SWT3 y asígnelo a la VLAN 10.
5. Repita el procedimiento para los puertos F0/15 y F0/20 en SWT1, SWT2 y SWT3. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

**D. Configurar las direcciones IP en los Switches.**

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.

Equipo	Interfaz	Direcciones IP	Mascara
SW-AA	VLAN 99	190.108.99.1	255.255.255.0
SW-BB	VLAN 99	190.108.99.2	255.255.255.0
SW-CC	VLAN 99	190.108.99.3	255.255.255.0

*Tabla 3 - Switches VLAN y direcciones ip sugeridas*

## E. Verificar la conectividad Extremo a Extremo

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

## SOLUCIÓN

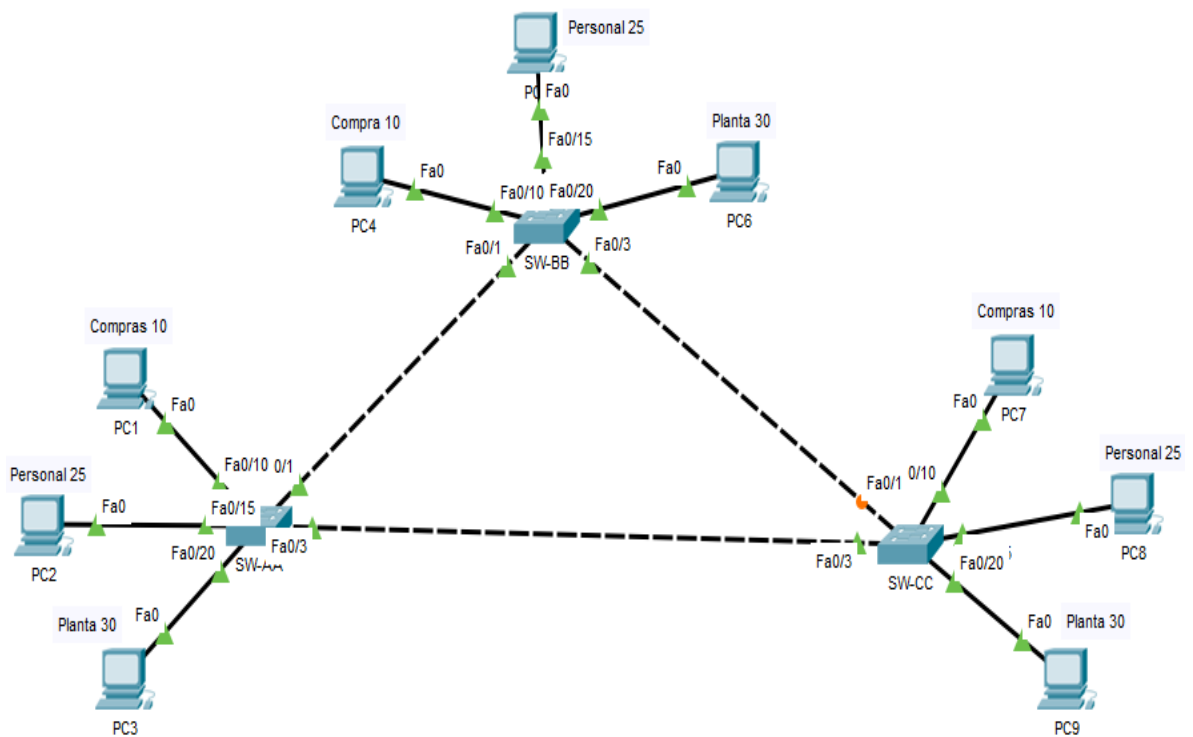


Figura 10- Topología diseñada

## A. Configuración de VTP

Se puede configurar un conmutador para intervenir en modo servidor VTP o modo cliente VTP.

Servidor VTP: en este se puede fundar, transformar, suprimir VLANs y detallar otros criterios de configuración. El servidor VTP anuncia su configuración de VLANs a otros interruptores en el mismo dominio de VTP.

Cliente VTP: estos proceden igual al servidor VTP con la única diferencia que no pueden fundar, transformar ni suprimir VLANs.

## 1. Configuración de switches para uso de VTP

### SW-AA

```
Switch> en
Switch# conf t
Switch(config)# hostname SW-AA
SW-AA(config)# vtp domain CCNP
SW-AA(config)# vtp mode client
SW-AA(config)# vtp password cisco
SW-AA(config)# vtp version 2
SW-AA(config)# exit
```

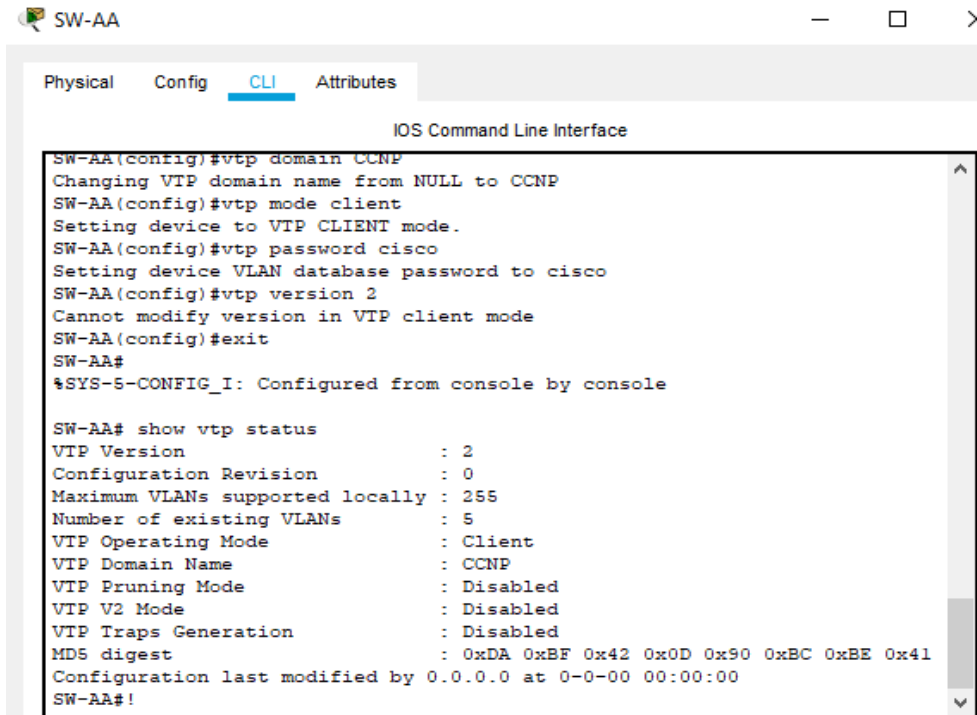
### SW-BB

```
Switch> en
Switch# conf t
Switch(config)# hostname SW-BB
SW-BB(config)# vtp domain CCNP
SW-BB(config)# vtp mode server
SW-BB(config)# vtp password cisco
SW-BB(config)# vtp version 2
SW-BB(config)# exit
```

### SW-CC

```
Switch> en
Switch# conf t
Switch(config)# hostname SW-CC
SW-CC(config)# vtp domain CCNP
SW-CC(config)# vtp mode client
SW-CC(config)# vtp password cisco
SW-CC(config)# vtp version 2
SW-CC(config)# exit
```

## 2. Resultado de configuraciones

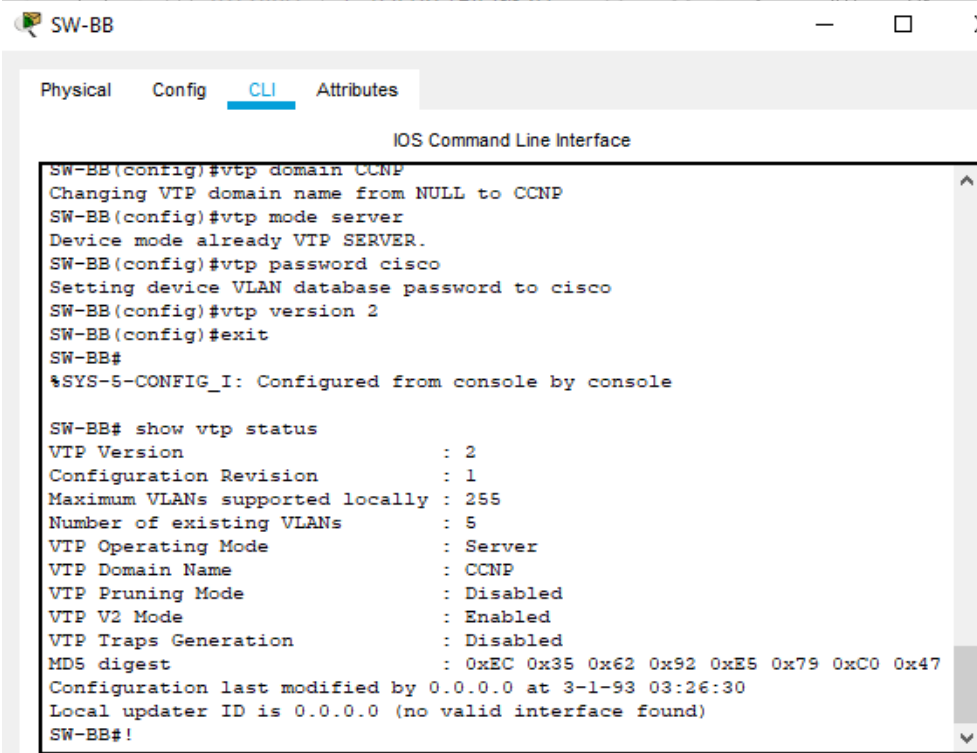


The screenshot shows the CLI of switch SW-AA. The user has configured the switch as a VTP client for the CCNP domain. The configuration steps include setting the domain name, mode, password, and version. The status output shows the switch is now in VTP Client mode with version 2.

```
SW-AA# vtp domain CCNP
Changing VTP domain name from NULL to CCNP
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)#vtp version 2
Cannot modify version in VTP client mode
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     : 0
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                : Disabled
VTP Traps Generation       : Disabled
MDS digest                 : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SW-AA#!
```

Figura 11 - VTP mode client SW-AA



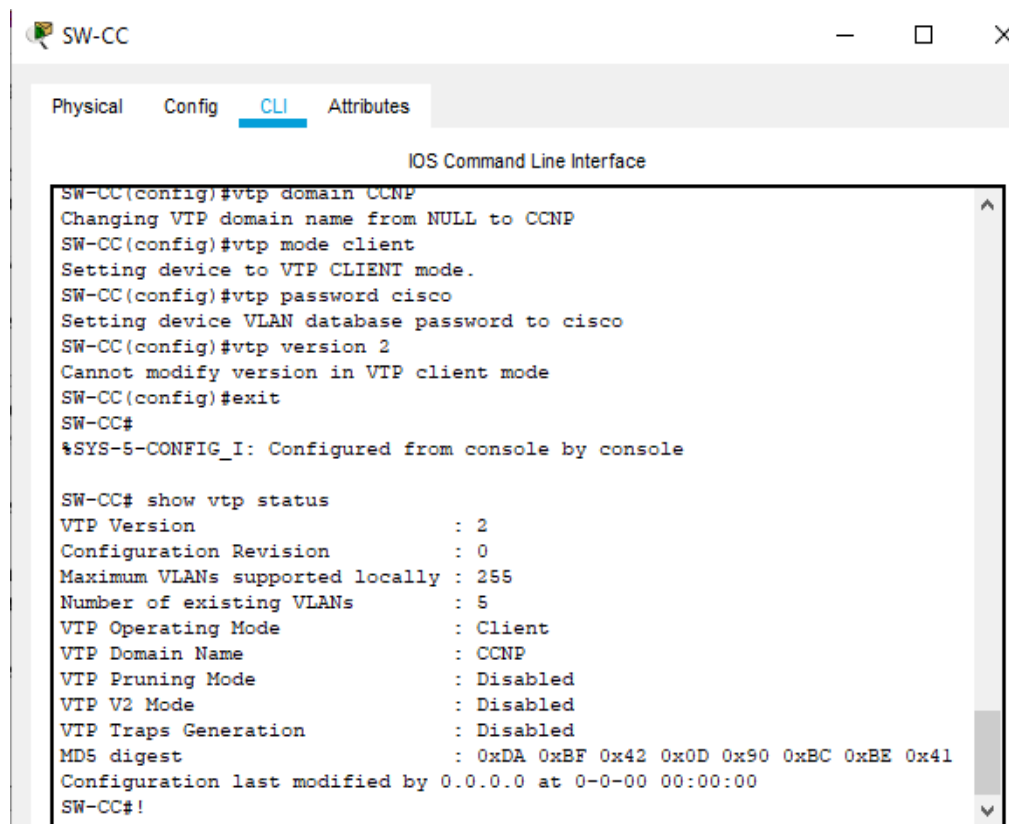
The screenshot shows the CLI of switch SW-BB. The user has configured the switch as a VTP server for the CCNP domain. The configuration steps include setting the domain name, mode, password, and version. The status output shows the switch is now in VTP Server mode with version 2.

```
SW-BB# vtp domain CCNP
Changing VTP domain name from NULL to CCNP
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)#vtp version 2
SW-BB(config)#exit
SW-BB#
%SYS-5-CONFIG_I: Configured from console by console

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                 : 0xEC 0x35 0x62 0x92 0xE5 0x79 0xC0 0x47
Configuration last modified by 0.0.0.0 at 3-1-93 03:26:30
Local updater ID is 0.0.0.0 (no valid interface found)
SW-BB#!
```

Figura 12 - VTP mode server SW-BB





```
SW-CC
Physical Config CLI Attributes
IOS Command Line Interface
SW-CC(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
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)#vtp version 2
Cannot modify version in VTP client mode
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 : 0
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           : 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
SW-CC#!
```

Figura 13 - VTP mode client SW-CC

## B. Configuración de DTP (Dynamic Trunking Protocol)

DTP opera entre interruptores y es el encargado de mecanizar la configuración troncal en enlaces Ethernet.

### 1. Configuración de enlaces troncales

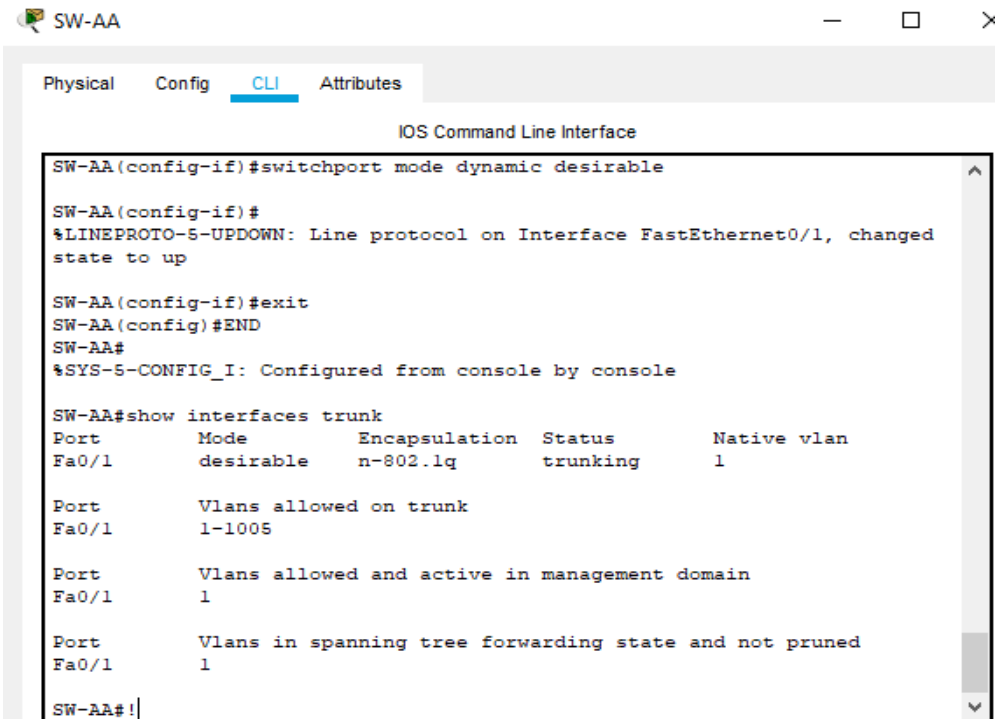
#### SW-AA

```
SW-AA> en
SW-AA# conf t
SW-AA(config)# int f0/1
SW-AA(config-if)# switchport mode trunk
SW-AA(config-if)# switchport mode dynamic desirable
SW-AA(config-if)# exit
```

#### SW-BB

```
SW-BB> en
SW-BB# conf t
SW-BB(config)# int f0/1
SW-BB(config-if)# switchport mode trunk
SW-BB(config-if)# exit
```

## 2. Resultado de configuraciones



SW-AA

Physical Config **CLI** Attributes

IOS Command Line Interface

```
SW-AA(config-if)#switchport mode dynamic desirable
SW-AA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up
SW-AA(config-if)#exit
SW-AA(config)#END
SW-AA#
%SYS-5-CONFIG_I: Configured from console by console

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

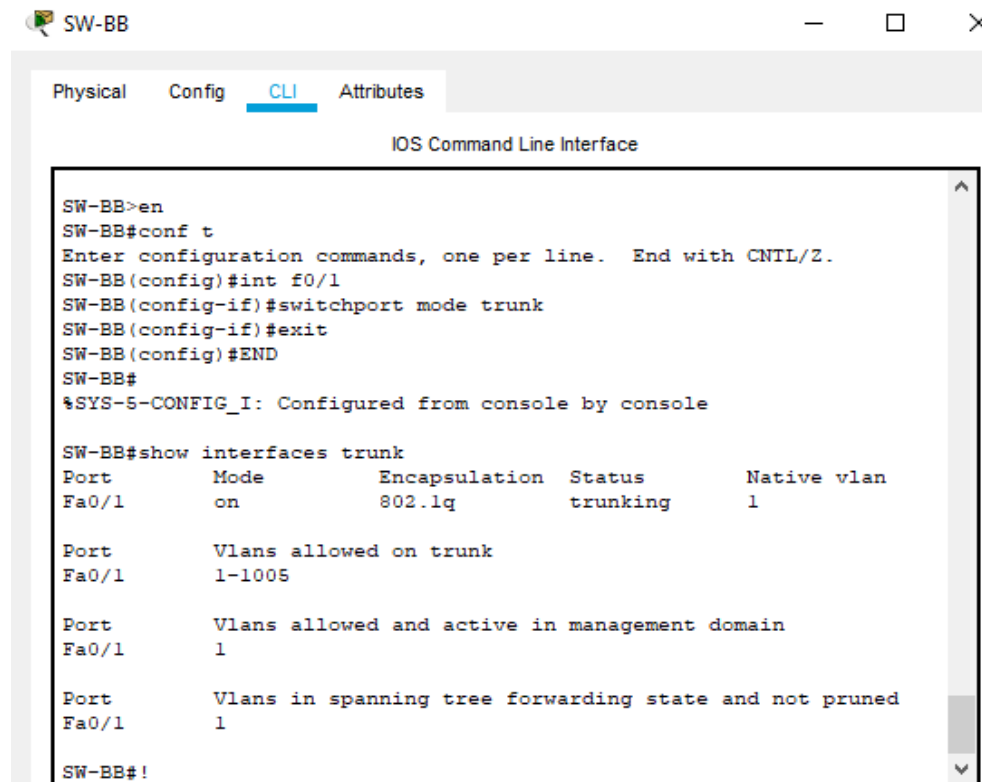
Port      Vlans allowed on trunk
Fa0/1     1-1005

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

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

SW-AA#!
```

Figura 14 – Enlace troncal en SW-AA



SW-BB

Physical Config **CLI** Attributes

IOS Command Line Interface

```
SW-BB>en
SW-BB#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#int f0/1
SW-BB(config-if)#switchport mode trunk
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     on        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     1

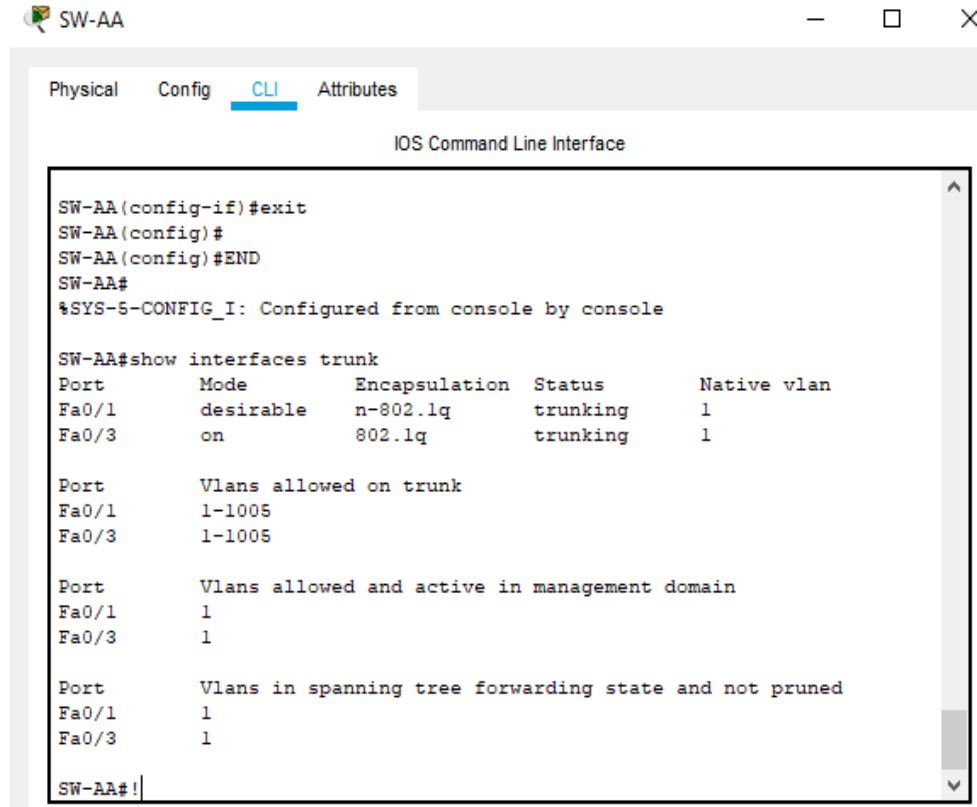
SW-BB#!
```

Figura 15 – Enlace troncal en SW-BB

### 3. Configuración de enlace troncal estático entre SW-AA y SW-CC

```
SW-AA# conf t
SW-AA(config)# int f0/3
SW-AA(config-if)# switchport mode trunk
SW-AA(config-if)# exit
```

### 4. Resultados de configuración



The screenshot shows the CLI interface of SW-AA. The 'CLI' tab is selected. The terminal output shows the configuration of Fa0/3 as a trunk port and the execution of the 'show interfaces trunk' command. The output of the command is as follows:

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

SW-AA#show interfaces 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#!
```

Figura 16- Enlace troncal estático en SW-AA

### 5. Configuración de enlace troncal permanente entre SW-BB y SW-CC

#### SW-BB

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

#### SW-CC

```
SW-CC# conf t
SW-CC(config)# int f0/1
SW-CC(config-if)# switchport mode trunk
```

## C. Creación de VLANs y asignación de puertos

### D. 1. Creación de VLANs

#### SW-AA

```
SW-AA# conf t
SW-AA(config)# vlan 10
```

En SWT1 no la podemos crear porque, en VTP la configuración de VLANs no está permitida ya que el dispositivo lo tenemos configurado en modo cliente.

#### SW-BB

```
SW-BB# conf t
SW-BB(config)# vlan 10
SW-BB(config-vlan)# name compras
SW-BB(config-vlan)# vlan 25
SW-BB(config-vlan)# name personal
SW-BB(config-vlan)# vlan 30
SW-BB(config-vlan)# name planta
SW-BB(config-vlan)# vlan 99
SW-BB(config-vlan)# name admon
SW-BB(config-vlan)#exit
```

## 2. Resultado de configuraciones

```

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
25   personal                active
30   planta                  active
99   admon                   active
1002 fddi-default             active
1003 token-ring-default    active
1004 fddinet-default        active
1005 trnet-default         active

VLAN Type  SAID      MTU   Parent  RingNo BridgeNo  Stp   BrdgMode Trans1 Trans2
-----
1    enet     100001   1500   -       -       -       -       -       0     0
10   enet     100010   1500   -       -       -       -       -       0     0
25   enet     100025   1500   -       -       -       -       -       0     0
30   enet     100030   1500   -       -       -       -       -       0     0
99   enet     100099   1500   -       -       -       -       -       0     0
1002 fddi     101002   1500   -       -       -       -       -       0     0
1003 tr      101003   1500   -       -       -       -       -       0     0
1004 fdnet  101004   1500   -       -       -       -       ieee -     0     0
1005 trnet  101005   1500   -       -       -       -       ibm  -     0     0

VLAN Type  SAID      MTU   Parent  RingNo BridgeNo  Stp   BrdgMode Trans1 Trans2
-----

Remote SPAN VLANs
-----

```

Figura 17 - VLANs

## 3. Tabla de asignación de puertos y direcciones ip

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	PC1:190.108.10.10/24
		PC4:190.108.10.40/24
		PC7:190.108.10.70/24
F0/15	VLAN 25	PC2:190.108.25.20/24
		PC5:190.108.25.50/24
		PC8:190.108.25.80/24
F0/20	VLAN 30	PC3:190.108.30.30/24
		PC6:190.108.30.60/24
		PC9:190.108.30.90/24

Tabla 4 - puertos y direcciones ip

#### 4. Configuración en modo acceso y asignación de VLAN 10

##### SW-AA

```
SW-AA# conf t
SW-AA(config)# int f0/10
SW-AA(config-if)# switchport access vlan 10
SW-AA(config-if)# exit
```

##### SW-BB

```
SW-BB# conf t
SW-BB(config)# int f0/10
SW-BB(config-if)# switchport access vlan 10
SW-BB(config-if)# exit
```

##### SW-CC

```
SW-CC# conf t
SW-CC(config)# int f0/10
SW-CC(config-if)# switchport access vlan 10
SW-CC(config-if)# exit
```

#### 5. Configuración en modo acceso, asignación de VLANs 25 y 30 y fijación de Ip a PC's

##### SW-AA

```
SW-AA# conf t
SW-AA(config)# int f0/15
SW-AA(config-if)# switchport access vlan 25
SW-AA(config-if)# exit
SW-AA(config)# int f0/20
SW-AA(config-if)# switchport access vlan 30
SW-AA(config-if)# exit
```

##### SW-BB

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

##### SW-CC

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

## D. Configuración de direcciones ip en los switches

Equipo	Interfaz	Dirección IP	Máscara
SWT1	VLAN 99	190.108.99.1	255.255.255.0
SWT2	VLAN 99	190.108.99.2	255.255.255.0
SWT3	VLAN 99	190.108.99.3	255.255.255.0

Tabla 5 - direcciones ip en los switches

### SW-AA

```
SW-AA# conf t
SW-AA(config)# int vlan 99
SW-AA(config-if)# ip address 190.108.99.1 255.255.255.0
SW-AA(config-if)# no shut
SW-AA(config-if)# exit
```

### SW-BB

```
SW-BB# conf t
SW-BB(config)# int vlan 99
SW-BB(config-if)# ip address 190.108.99.2 255.255.255.0
SW-BB(config-if)# no shut
SW-BB(config-if)# exit
```

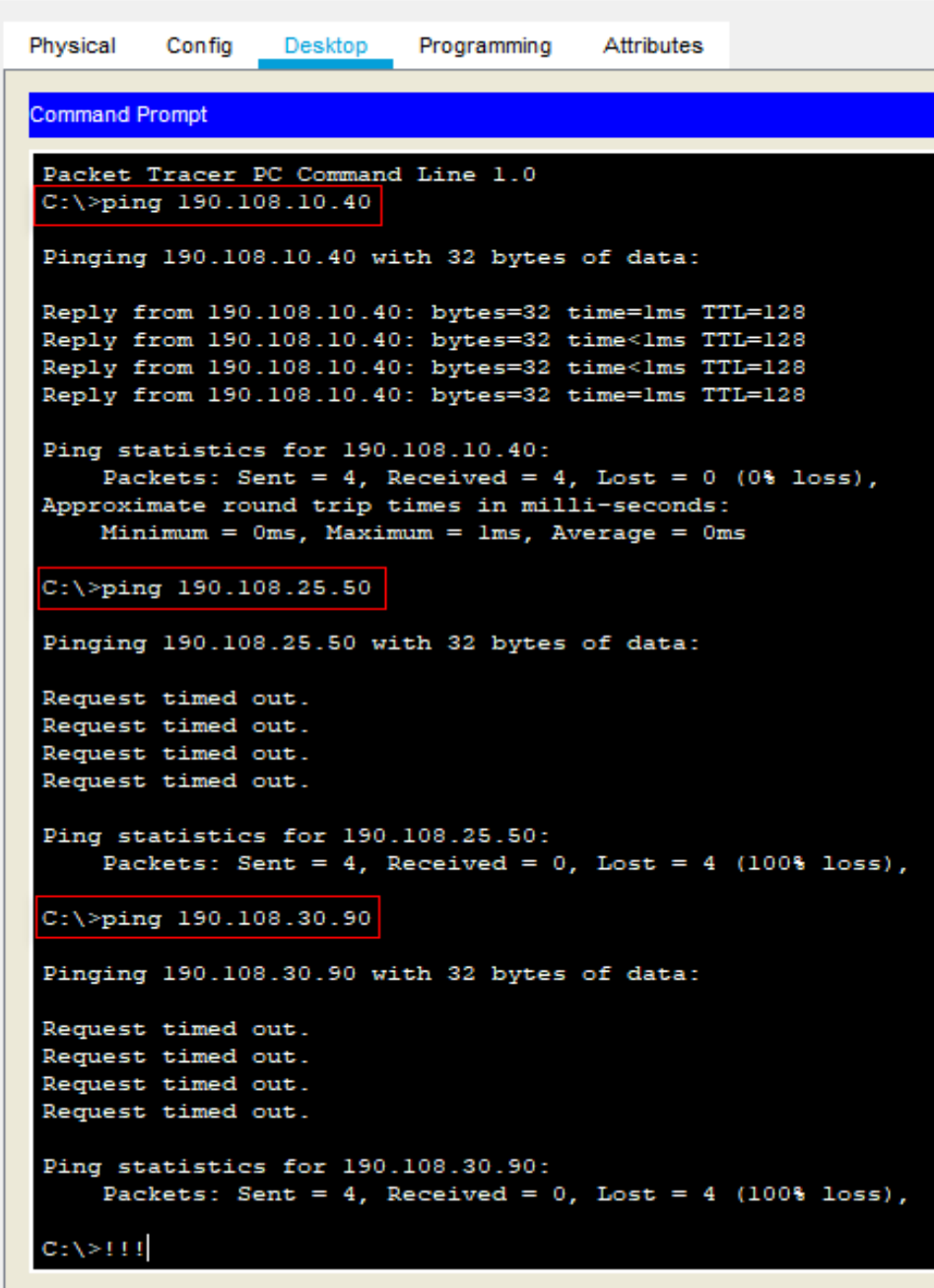
### SW-CC

```
SW-CC# conf t
SW-CC(config)# int vlan 99
SW-CC(config-if)# ip address 190.108.99.3 255.255.255.0
SW-CC(config-if)# no shut
SW-CC(config-if)# exit
```

## E. verificación de conectividad extremo a extremo

### 1. Ping desde cada pc a los demás.

#### Ping de PC1 a PC4, PC5 y PC9



The screenshot shows the Desktop tab of PC1 in Packet Tracer. A Command Prompt window is open, displaying the results of three ping commands. The first command, `C:\>ping 190.108.10.40`, is successful, showing 4 received packets with 0% loss. The second command, `C:\>ping 190.108.25.50`, fails with 100% loss (4 packets sent, 0 received). The third command, `C:\>ping 190.108.30.90`, also fails with 100% loss (4 packets sent, 0 received). The prompt ends with `C:\>!!!|`.

```
Packet Tracer PC Command Line 1.0
C:\>ping 190.108.10.40

Pinging 190.108.10.40 with 32 bytes of data:

Reply from 190.108.10.40: bytes=32 time=1ms TTL=128
Reply from 190.108.10.40: bytes=32 time<1ms TTL=128
Reply from 190.108.10.40: bytes=32 time<1ms TTL=128
Reply from 190.108.10.40: bytes=32 time=1ms TTL=128

Ping statistics for 190.108.10.40:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 190.108.25.50

Pinging 190.108.25.50 with 32 bytes of data:

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

Ping statistics for 190.108.25.50:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.30.90

Pinging 190.108.30.90 with 32 bytes of data:

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

Ping statistics for 190.108.30.90:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

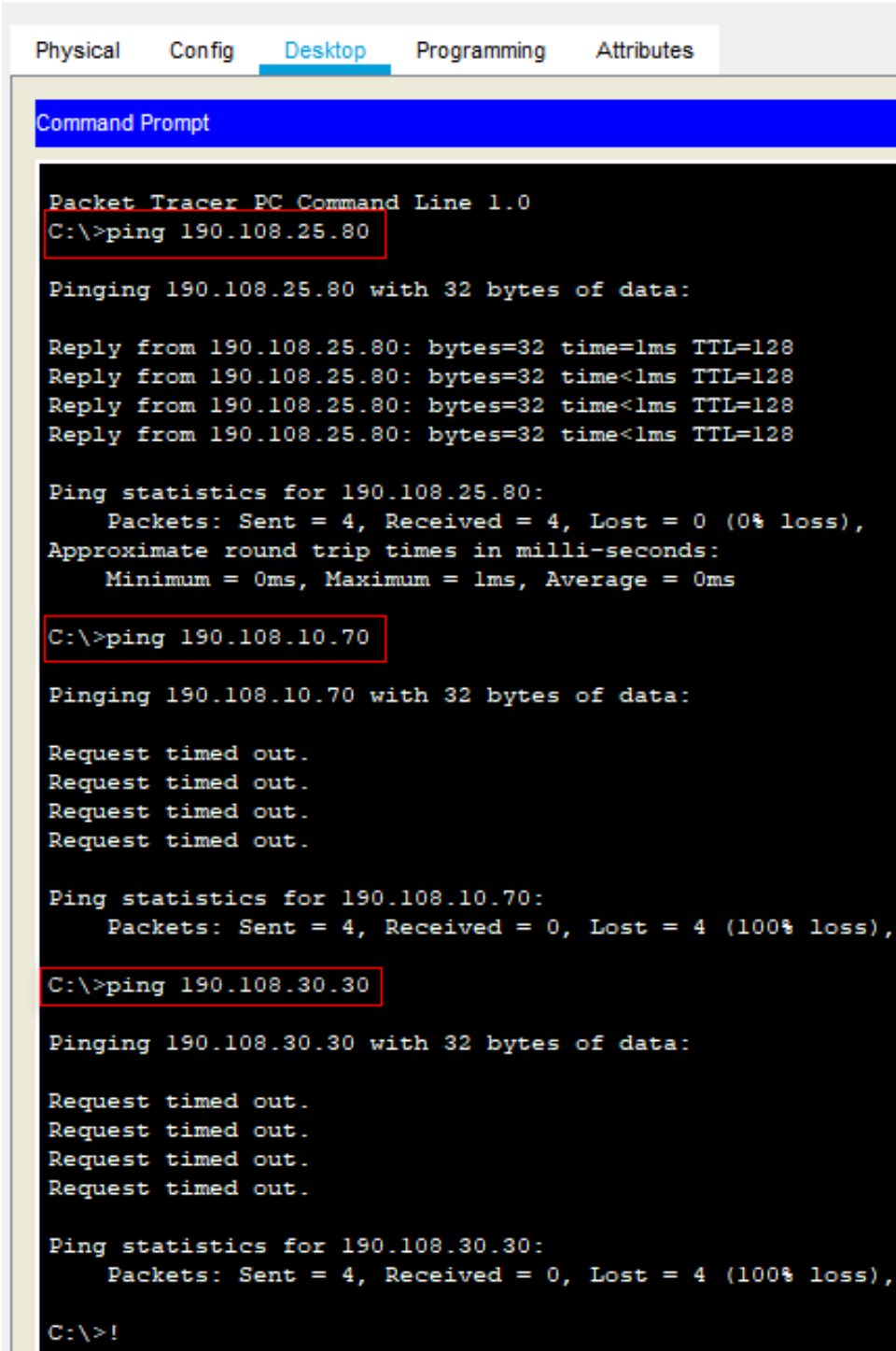
C:\>!!!|
```

Figura 18- Ping de PC1 a PC4, PC5 y PC9



## 2. Ping de PC5 a PC8, PC7 y PC3.

PC5



The screenshot shows the Packet Tracer interface for PC5, with the 'Desktop' tab selected. The Command Prompt window displays the following text:

```
Packet Tracer PC Command Line 1.0
C:\>ping 190.108.25.80

Pinging 190.108.25.80 with 32 bytes of data:

Reply from 190.108.25.80: bytes=32 time=1ms TTL=128
Reply from 190.108.25.80: bytes=32 time<1ms TTL=128
Reply from 190.108.25.80: bytes=32 time<1ms TTL=128
Reply from 190.108.25.80: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.25.80:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 190.108.10.70

Pinging 190.108.10.70 with 32 bytes of data:

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

Ping statistics for 190.108.10.70:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.30.30

Pinging 190.108.30.30 with 32 bytes of data:

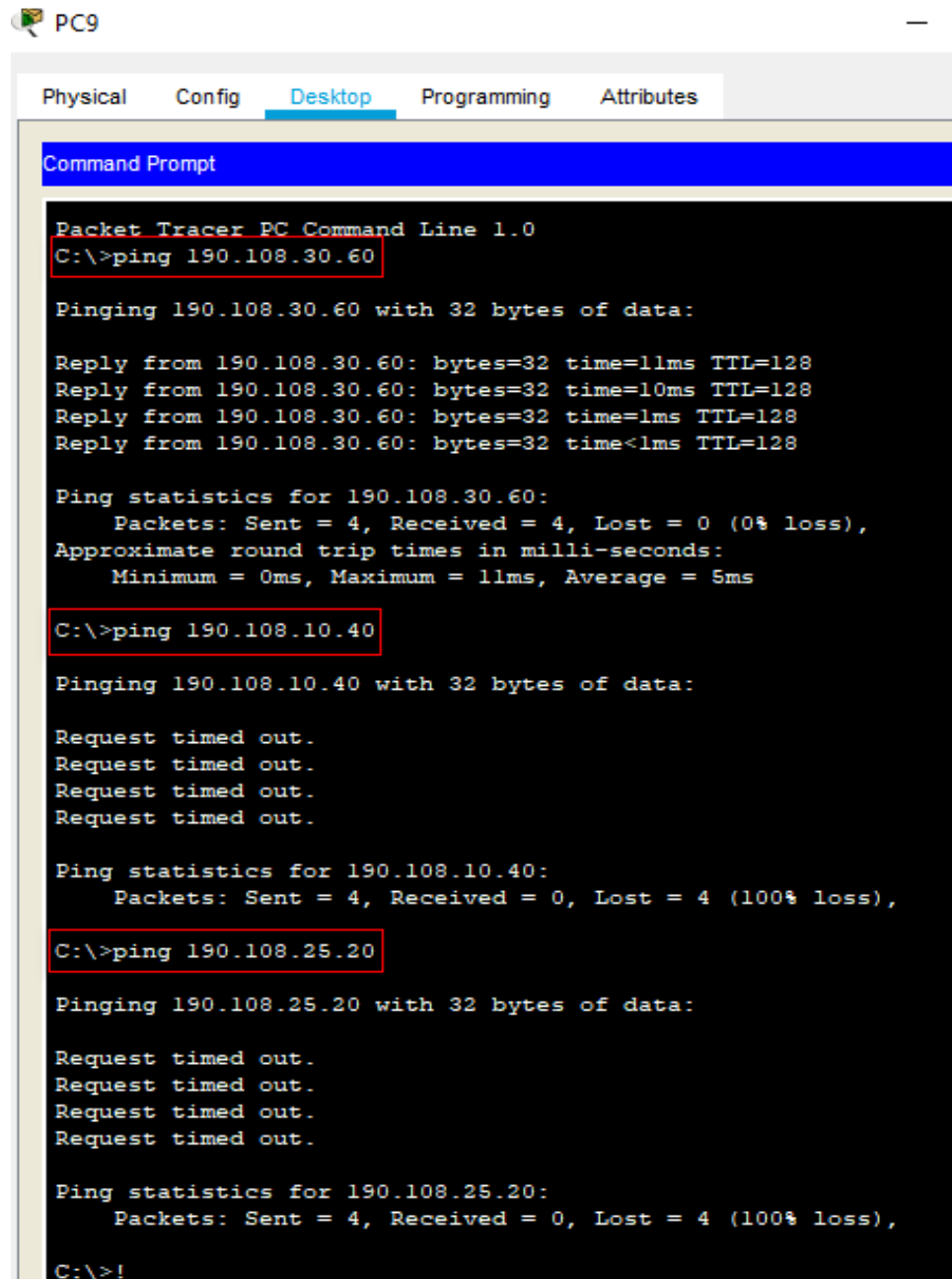
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.30.30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>!
```

Figura 19 - Ping de PC5 a PC8, PC7 y PC3

### 3. Ping de PC9 a PC6, PC4 y PC2.



```
PC9
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 190.108.30.60

Pinging 190.108.30.60 with 32 bytes of data:

Reply from 190.108.30.60: bytes=32 time=11ms TTL=128
Reply from 190.108.30.60: bytes=32 time=10ms TTL=128
Reply from 190.108.30.60: bytes=32 time=1ms TTL=128
Reply from 190.108.30.60: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.30.60:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 5ms

C:\>ping 190.108.10.40

Pinging 190.108.10.40 with 32 bytes of data:

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

Ping statistics for 190.108.10.40:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.25.20

Pinging 190.108.25.20 with 32 bytes of data:

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

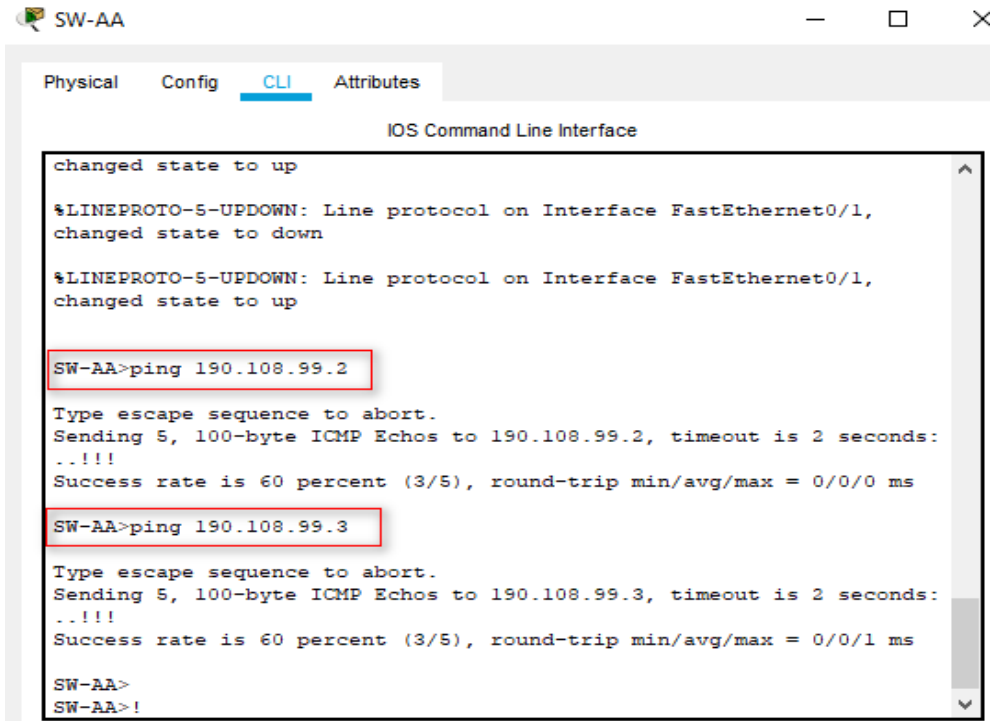
Ping statistics for 190.108.25.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>!
```

Figura 20- Ping de PC9 a PC6, PC4 y PC2

Los Pings realizado entre los PCs pertenecientes a diferentes Vlans no tuvieron éxito, sin embargo, los pings realizados a PCs que pertencen a la misma Vlan, si fueron exitosos. El error en los PCs pertenecientes a diferentes Vlans se presenta ya que cada PC pertenece a un segmento de red diferente. Por tanto, sería necesario incluir en la topología de la red un Switch de capa 3 (Switch Multicapa), los cuales tienen la funcionalidad intrínseca de enrutamiento entre VLANs.

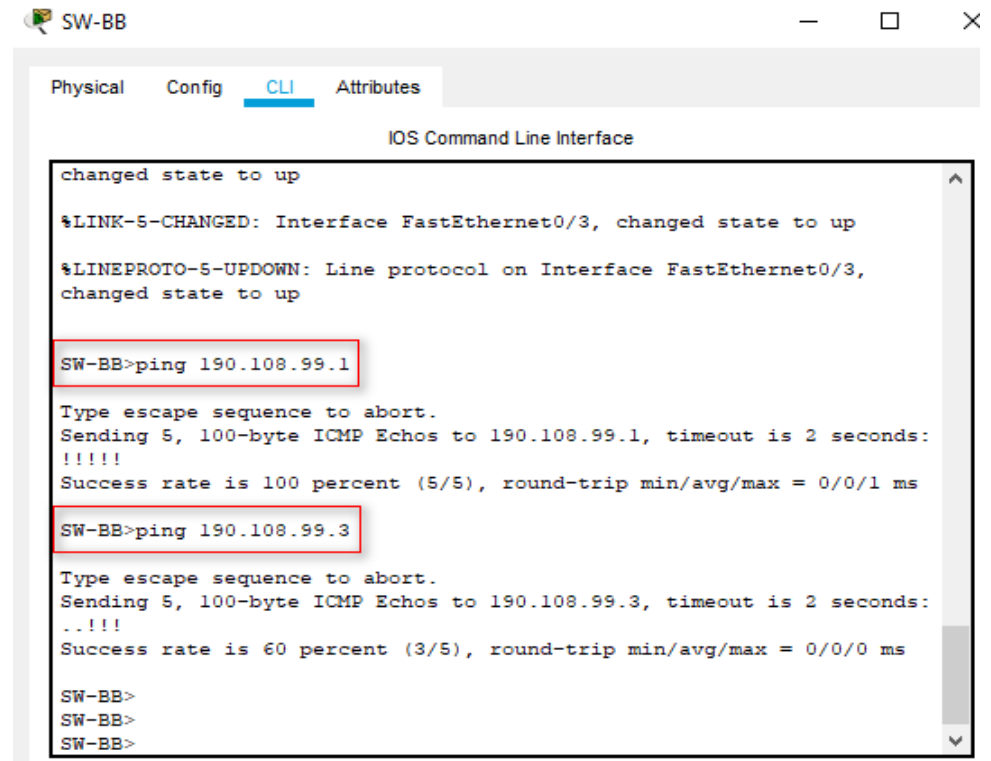
## 2. ping desde cada switch a los demás



The screenshot shows the CLI of switch SW-AA. The interface is 'IOS Command Line Interface'. The output shows the following sequence of events:

```
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
SW-AA>ping 190.108.99.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 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 60 percent (3/5), round-trip min/avg/max = 0/0/1 ms
SW-AA>
SW-AA>!
```

Figura 21- Ping de SW-AA a SW-BB y SW-CC



The screenshot shows the CLI of switch SW-BB. The interface is 'IOS Command Line Interface'. The output shows the following sequence of events:

```
changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to up
SW-BB>ping 190.108.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
SW-BB>ping 190.108.99.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms
SW-BB>
SW-BB>
SW-BB>
```

Figura 22- Ping de SW-BB a SW-AA y SW-CC

The screenshot shows a network switch's CLI interface with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the following text:

```
IOS Command Line Interface

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

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

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

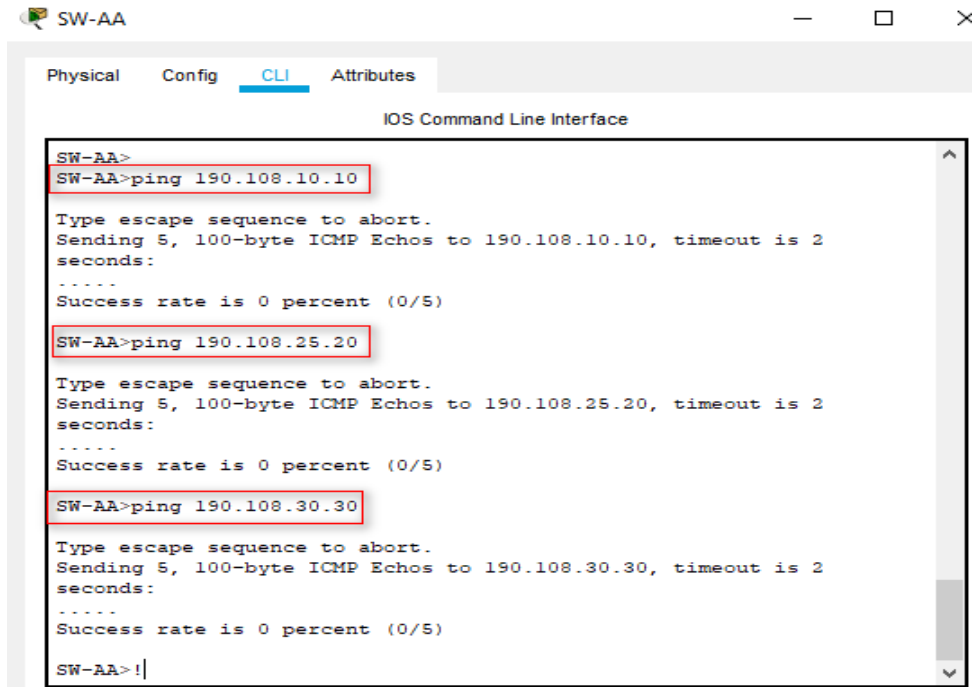
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/5 ms

SW-CC>
SW-CC>
SW-CC>|
```

Figura 23- Ping de SW-CC a SW-AA y SW-BB

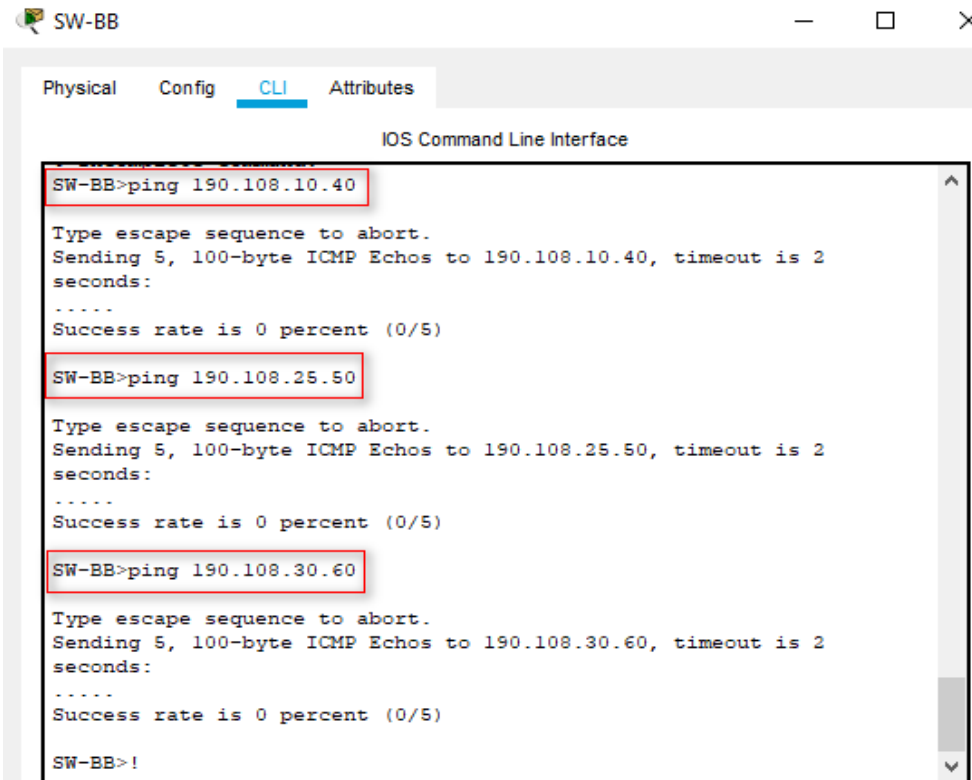
Los pings realizado entre los Switches fueron exitosos, dado que las interfaces físicas que enrutan los datos enviados a través del protocolo ICMP entre los tres Switches están configuradas en modo troncal, y según se verifico mediante el comando show interfaces trunk, comparten el mismo tipo de encapsulamiento, así como se encuentran en un modo compatible. Es decir la Ip que les fue asignada está configurada en la misma VLAN (VLAN 99) para los tres.

### 3. Ping desde casa switch a cada PC



```
SW-AA>
SW-AA>ping 190.108.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.10, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
SW-AA>ping 190.108.25.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.20, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
SW-AA>ping 190.108.30.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.30, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
SW-AA>|
```

Figura 24- Ping de SW-AA a PC1, PC2 y PC3.



```
SW-BB>ping 190.108.10.40
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.40, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
SW-BB>ping 190.108.25.50
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.50, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
SW-BB>ping 190.108.30.60
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.60, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
SW-BB>|
```

Figura 25- Ping de SW-BB a PC4, PC5 y PC6.



The screenshot shows a terminal window titled "SW-CC" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". Three ping commands are entered and executed, each resulting in a 0% success rate. The commands and their outputs are:

```
SW-CC>ping 190.108.10.70
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.70, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW-CC>ping 190.108.25.80
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.25.80, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW-CC>ping 190.108.30.90
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.90, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW-CC>!
```

Figura 26- Ping de SW-CC a PC7, PC8 y PC9.

Los pings realizado entre los Switches y los PCs no fueron exitosos ya que no se configuro en ninguno de los switches una dirección Ip a las VLANs. En cada uno de los Switches a través del protocolo VTP, y se configuro cada una de las interfaces que conectan los switches a los PCs en modo de acceso según la respectiva VLAN a la cual pertenecen, aun no se configura un enrutamiento IP en las VLANs creadas (10-Compras / 25-Personal / 30-Planta).

Ahora para que tengan éxito se haría la siguiente configuración para cada uno de los switches con las respectivas ip de los PCs

```
SWT1# configure terminal
SWT1(config)# int vlan 10
SWT1(config-if)# ip address 190.108.10.10 255.255.255.0
SWT1(config-if)# exit
SWT1(config)#int vlan 20
SWT1(config-if)# ip address 190.108.20.10 255.255.255.0
SWT1(config-if)# exit
SWT1(config)# int vlan 30
SWT1(config-if)# ip address 190.108.30.10 255.255.255.0
SWT1(config-if)# exit
```

## CONCLUSIONES

Tras completar cada uno de los ejercicios y las configuraciones requeridas para cada dispositivo, en los dos escenarios propuestos, se logra poner a prueba los conocimientos teóricos y las habilidades prácticas construidas a través del curso mediante el uso de herramientas como GNS3 y Packet Tracer de Cisco. Mediante estos software, logramos montar dos topologías basadas en la configuración de enrutamiento IPv4 en interfaces Seriales, FastEthernet y Loopback, en dispositivos de enrutamiento, conmutación y acceso a la red por parte de usuarios finales.

Se estudiaron las redes de área local virtuales (VLANs). El concepto de VLAN se emplea en el terreno de la informática para nombrar al desarrollo de redes lógicas vinculadas a una única red de tipo físico. Estas son un método que permite crear redes que lógicamente son independientes. Fue posible configurar varios dispositivos lógicos en un solo sistema, cada dispositivo lógico VLAN constituyó una instancia adicional del adaptador Ethernet.

Finalmente se desarrolla la solución a la prueba de habilidades prácticas para el diplomado de profundización Cisco CCNP y al realizar la verificación final de la conectividad de Extremo a Extremo en el último escenario propuesto, se logra contrastar los conocimientos obtenidos tras el cumplimiento del curso sobre estas temáticas, al tener que analizar las posibles causas de los fallos en la búsqueda de paquetes mediante los pings realizados entre los dispositivos.

## REFERENCIAS BIBLIOGRAFICAS

Diego Hernando Torres Valencia. (2012), universidad de pamplona, enrutamiento con OSPF y EIGRP, recuperado de:

<https://es.slideshare.net/diegotorres/enrutamiento-con-ospf-y-eigrp>

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

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

John Bonilla. (2011), protocolos de enrutamiento, tipos de enrutamiento, recuperado de: <https://es.slideshare.net/jonenkairos/protocolos-de-enrutamiento-7555314>

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

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing a Border Gateway Protocol (BGP) Solution for ISP Connectivity. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101 Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>

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