

DIPLOMADO DE PROFUNDIZACION  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JULIO CESAR CORREA SIERRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA  
INGENIERIA ELECTRÓNICA  
BARRANQUILLA  
2020

DIPLOMADO DE PROFUNDIZACION CISCO  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JULIO CESAR CORREA SIERRA

Diplomado de opción de grado presentado para  
optar el título de INGENIERO ELECTRÓNICO

DIRECTOR:  
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD ESCUELA DE  
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA INGENIERIA  
ELECTRÓNICA  
BARRANQUILLA  
2020

NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

Firma del Presidente del Jurado

---

Firma del Jurado

---

Firma del Jurado

Barranquilla, 20 de mayo de 2020

## **AGRADECIMIENTOS**

A Dios todo poderoso por brindarme guía en los momentos más duro de mi vida, a mi familia en general y sobre todo a mi madre por confiar más en mi que incluso yo mismo, ha sido mi inspiración y guía incluso en épocas de adversidad, en memoria de mi padre el hombre que me enseñó mas con su ejemplo que con sus palabras.

## CONTENIDO

AGRADECIMIENTOS .....	4
CONTENIDO .....	5
LISTA DE TABLAS .....	6
LISTA DE FIGURAS .....	7
GLOSARIO .....	8
RESUMEN .....	9
ABSTRACT .....	9
INTRODUCCIÓN .....	10
DESARROLLO .....	11
Escenario 1 .....	11
Escenario 2 .....	23
CONCLUSIONES .....	47
BIBLIOGRAFÍA .....	48

## LISTA DE TABLAS

Tabla 1: Configuración de los routers .....	13
Tabla 2: Interfaz y VLAN .....	37

## LISTA DE FIGURAS

Figura 1: Ip route and sh ip bgp .....	17
Figura 2: Command Line Interface.....	18
Figura 3: Salida del comando show .....	20
Figura 4: Comando show ip route .....	22
Figura 5: Ejecución comando show .....	26
Figura 6: Ejecución comando show vtp status en SW-BB .....	26
Figura 7: Ejecución comando.....	27
Figura 8: Interfaces trunk en SW-AA .....	28
Figura 9: Interfaces trunk en SW-AA .....	29
Figura 10: Interfaces trunk en SW-CC .....	29
Figura 11 Vlan 10 en SW-AA .....	30
Figura 12 0,25,30 y 99 en SW-BB .....	31
Figura 13 Creación de Vlan .....	32
Figura 14 Vlan en SW-CC .....	32
Figura 15 Configuración de direccionamiento en PCs.....	33
Figura 16 Verificación de interfaz Vlan en SW-AA.....	35
Figura 17 Vlan en SW-BB.....	36
Figura 18 Verificación de interfaz.....	36
Figura 19 Direccionamiento IP en PCs de compras. ....	37
Figura 20 Direccionamiento IP en PCs .....	38
Figura 21 Direccionamiento IP .....	38
Figura 22: Ping exitoso .....	40
Figura 23: 190.108.20.3 desde personal 25 .....	40
Figura 24 190.108.20.3 desde personal 25 .....	40
Figura 25: Ping desde compras .....	41
Figura 26: Compras 30.2 .....	41
Figura 27: Ping desde compras a personal y planta .....	42
Figura 28: SW-AA a SW-BB y SW-CC .....	43
Figura 29: Ping desde SW-BB hacia SW-AA y SW-CC .....	44
Figura 30: Hacia SW-AA y SW-BB .....	44
Figura 31: Hacia los PCs .....	45
Figura 32: Ping desde SW-BB hacia los PCs .....	46
Figura 33: SW-CC hacia los PCs.....	46

## GLOSARIO

**INTERFAZ:** Son las rutas que se establecen de datos y toman vía los destinos particulares.

**VLAN:** Son agrupaciones lógicas de dispositivos en el mismo dominio de difusión. Las VLAN generalmente se configuran en los conmutadores colocando algunas interfaces en un dominio de difusión y algunas interfaces en otro. Cada VLAN actúa como un subgrupo de los puertos del conmutador en una LAN Ethernet.

**LOOPBACK:** El bucle invertido es un canal de comunicación con un solo punto final. Las redes TCP / IP especifican un loopback que permite que el software del cliente se comunique con el software del servidor en la misma computadora. los usuarios pueden especificar una dirección IP, generalmente 127.0.0.1, que apuntará a la configuración de red TCP / IP de la computadora

**BGP:** Border Gateway Protocol (BGP) es un protocolo de puerta de enlace externo estandarizado diseñado para intercambiar información de enrutamiento y accesibilidad entre sistemas autónomos (AS) en Internet

**VTP:** VTP (VLAN Trunking Protocol) es un protocolo de propiedad de Cisco utilizado por los conmutadores de Cisco para intercambiar información de VLAN.



## **RESUMEN**

A continuación se desarrollan dos escenarios planteados como pruebas de habilidades prácticas cada uno exige los métodos aprendidos en el desarrollo para la solución de problemas, en el escenario uno debemos elaborar una relación BGP entre los diferentes R1, R2, así como los comandos utilizados y la salida de estos, a su vez se debe realizar una codificación con los parámetros establecidos, por su parte en el escenario dos se tiene que configurar los Switches mientras se verifica los como clientes, además de repetir los procedimientos en los puertos propuestos.

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

## **ABSTRACT**

Next, two scenarios are developed as tests of practical skills, each one requires the methods learned in development for the solution of problems, in scenario one we must develop a BGP relationship between the different R1, R2, as well as the commands used and the Once these are finished, a coding must be carried out with the established parameters. In turn, in scenario two, the switches must be configured while verifying them as clients, in addition to repeating the procedures on the proposed ports.

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

## INTRODUCCIÓN

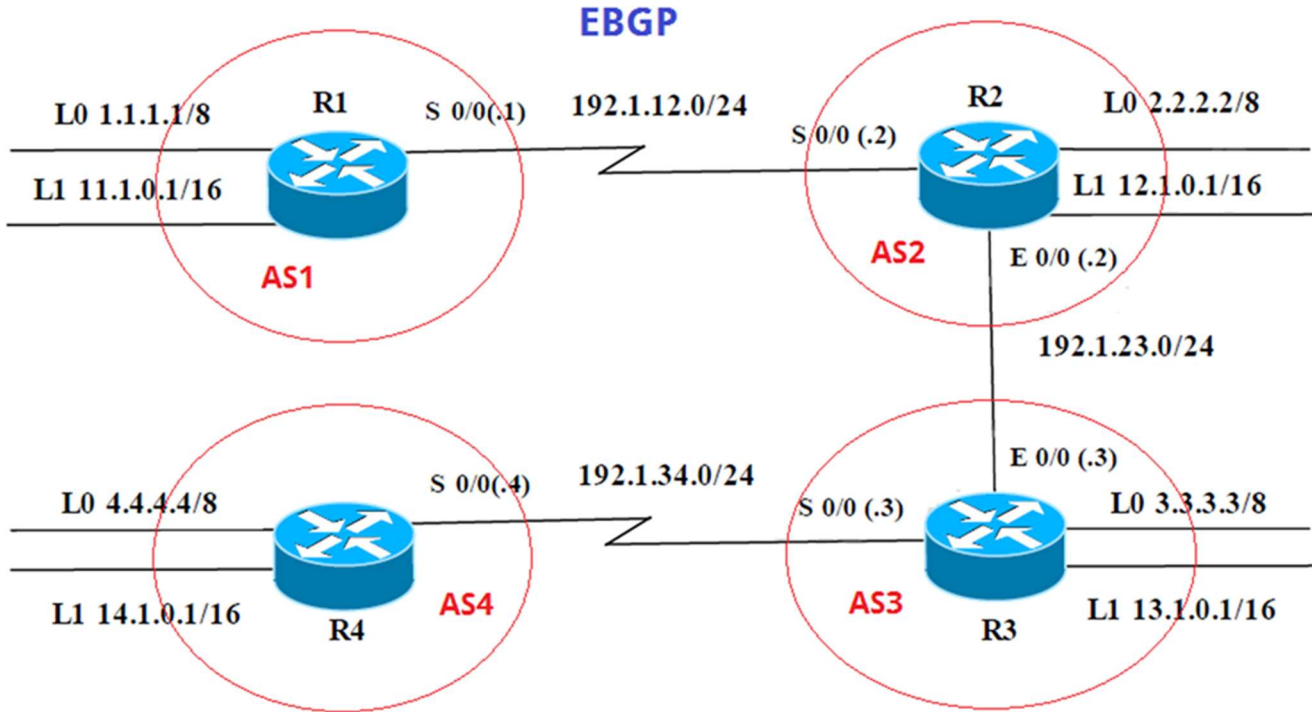
A continuación, usando los diferentes programas de simulación se describen paso a paso la configuración de los dispositivos de cada escenario, se exhibe su correcta operación ayudado de los comandos respectivos que permiten evidenciar su operatividad tanto en la utilización de protocolos BGP, en el intercambio de información de sistemas autónomos, como la distribución de VLAN mediante el protocolo VTP.

Se va evidenciar la configuración de los equipos mediante imágenes de las simulaciones y ejecución de comandos específicos para dar solución a las necesidades y requerimientos de la red, se va a utilizar las herramientas de simulación de redes especializadas para la creación de los escenarios como Packet tracer en su versión 7.2.1.0218 de Cisco y GNS3 en su versión 2.2.6.

Los dos escenarios que se describen a continuación se va a Configurar una relación de vecino BGP entre R1 y R2. R1 dado un escenario, además se va a configurar una relación de vecino BGP entre R2 y R3. R2 aplicando a cada una las diferentes relaciones con sus respectivos direccionamientos.

## DESARROLLO

### Escenario 1



Información para configuración de los Routers

Interfaz	Dirección IP	Máscara
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
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
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
Loopback 0	4.4.4.4	255.0.0.0
Loopback 1	14.1.0.1	255.255.0.0
S 0/0	192.1.34.4	255.255.255.0

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

### Configuración de IPS AS1

```
Router(config)#hostname AS1
```

```
AS1(config)#inter lo
```

```
AS1(config)#inter loopback 0
```

```
AS1(config-if)#
```

%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

AS1(config-if)#ip add

AS1(config-if)#ip address 1.1.1.1 255.0.0.0

AS1(config-if)#exit

AS1(config)#inter lo

AS1(config)#inter loopback 1

AS1(config-if)#

%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

AS1(config-if)#ip add

AS1(config-if)#ip address 11.1.0.1 255.255.0.0

AS1(config-if)#exit

AS1(config)#inter se0/3/1

AS1(config-if)#ip add

AS1(config-if)#ip address 192.1.12.1 255.255.255.0

### **Configuracion de IPS AS2**

Router(config)#hostname AS2

AS2(config)#inter lo

AS2(config)#inter loopback 0

AS2(config-if)#

%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up  
ip add

AS2(config-if)#ip address 2.2.2.2 255.0.0.0

AS2(config-if)#exit

AS2(config)#int loo 1

AS2(config-if)#

%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up  
ip address

AS2(config-if)#ip address 12.1.0.1 255.255.0.0

AS2(config-if)#exit

AS2(config)#inter se0/3/0

AS2(config-if)#ip ad

AS2(config-if)#ip address 192.1.12.2 255.255.255.0

AS2(config-if)#no sh

%LINK-5-CHANGED: Interface Serial0/3/0, changed state to down

AS2(config-if)#

%LINK-5-CHANGED: Interface Serial0/3/0, changed state to up

AS2(config-if)#exit

AS2(config)#inter fa

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up

AS2(config)#inter fastEthernet 0/0

AS2(config-if)#ip add

AS2(config-if)#ip address 192.1.23.2 255.255.255.0

AS2(config-if)#no sh

AS2(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

### **Configuracion de IPS AS3**

Router(config)#hostname AS3

AS3(config)#inter loo 0

AS3(config-if)#

%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

AS3(config-if)#ip add

```
AS3(config-if)#ip address 3.3.3.3 255.0.0.0
AS3(config-if)#exit
AS3(config)#inte lo
AS3(config)#inte loopback 1
```

```
AS3(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
ip add
```

```
AS3(config-if)#ip address 13.1.0.1 255.255.0.0
AS3(config-if)#exit
AS3(config)#inter fa
AS3(config)#inter fastEthernet 0/0
AS3(config-if)#192.1.23.3 255.255.255.0
```

```
^
```

```
% Invalid input detected at '^' marker.
AS3(config-if)#ip add192.1.23.3 255.255.255.0
AS3(config-if)#ip add 192.1.23.3 255.255.255.0
AS3(config-if)#no sh
```

```
AS3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
up
```

```
AS3(config-if)#exit
AS3(config)#inter se0/3/0
AS3(config-if)#ip add
AS3(config-if)#ip address 192.1.34.3 255.255.255.0
AS3(config-if)#no sh
```

```
%LINK-5-CHANGED: Interface Serial0/3/0, changed state to down
```

### **Configuracion de IPS AS4**

```
Router>ena
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#inter lo
Router(config)#inter loopback 0
```

```
Router(config-if)#
```

%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up  
ip add

Router(config-if)#ip address 4.4.4.4 255.0.0.0

Router(config-if)#exit

Router(config)#inter lo

Router(config)#inter loopback 1

Router(config-if)#

%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

Router(config-if)#14.1.0.1 255.255.0.0

^

% Invalid input detected at '^' marker.

Router(config-if)#inter se

Router(config-if)#inter se0/3/0

Router(config-if)#ip add

Router(config-if)#ip address 192.1.34.4 255.255.255.0

Router(config-if)#no sh

Router(config-if)#

%LINK-5-CHANGED: Interface Serial0/3/0, changed state to up

Router(config-if)#exit

Router(config)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to up

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 11.11.11.11 para R1 y como 22.22.22.22 para R2. Presente el paso a con los comandos utilizados y la salida del comando **show ip route**.

AS1>ena

AS1#conf ter

Enter configuration commands, one per line. End with CNTL/Z.

AS1(config)#router

AS1(config)#router bg

AS1(config)#router bgp 1

AS1(config-router)#exit

AS1(config)#router bgp 1



```

AS1(config-router)#bg
AS1(config-router)#bgp ro
AS1(config-router)#bgp router-id 11.11.11.11
AS1(config-router)#ne
AS1(config-router)#neig
AS1(config-router)#neighbor 192.1.12.2 rem
AS1(config-router)#neighbor 192.1.12.2 remote-as 2
AS1(config-router)#net
AS1(config-router)#network 1.1.1.1 mas
AS1(config-router)#network 1.1.1.1 mask 255.0.0.0
AS1(config-router)#net
AS1(config-router)#network 11.1.0.1 mas
AS1(config-router)#network 11.1.0.1 mask 255.255.0.0
AS1(config-router)#exit

```

```

AS1#sh ip bgp
BGP table version is 1, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
AS1#sh 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
C     11.0.0.0/16 is subnetted, 1 subnets
C       11.1.0.0 is directly connected, Loopback1
C     192.1.12.0/24 is directly connected, Serial0/3/1

AS1#

```

Figura 1: Ip route and sh ip bgp

```

AS2(config)#router b
AS2(config)#router bgp 2
AS2(config-router)#bgo
AS2(config-router)#bgp
AS2(config-router)#bgp rout
AS2(config-router)#bgp router-id 22.22.22.22
AS2(config-router)#beu
AS2(config-router)#nei
AS2(config-router)#neighbor 192.1.12.1 rem
AS2(config-router)#neighbor 192.1.12.1 remote-as 1

```

```

AS2(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.12.1 Up
neig
AS2(config-router)#neighbor 192.1.34.3 remo
AS2(config-router)#neighbor 192.1.34.3 remote-as 3
AS2(config-router)#neig
AS2(config-router)#neighbor 192.1.23.3 remo
AS2(config-router)#neighbor 192.1.23.3 remote-as 3
AS2(config-router)#net
AS2(config-router)#network 1.1.1.0
AS2(config-router)#network 11.1.0.0

```

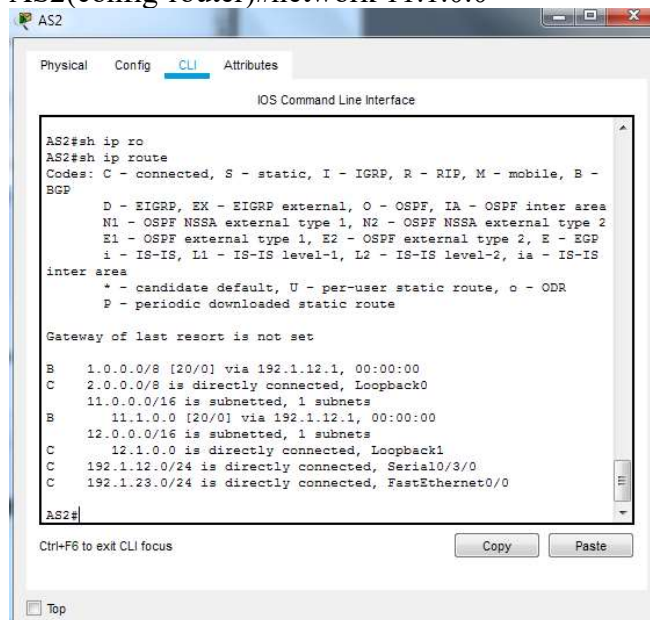


Figura 2: Command Line Interface

- 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 33.33.33.33. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

```

AS3(config)#router bgp 3
AS3(config-router)#router
AS3(config-router)#router-
AS3(config-router)#bgp
AS3(config-router)#bgp rou
AS3(config-router)#bgp router-id 33.33.33.33
AS3(config-router)#nei
AS3(config-router)#neighbor 192.1.12.2 re
AS3(config-router)#neighbor 192.1.12.2 remote-as 2

```

```
AS3(config-router)#nei
AS3(config-router)#neighbor 192.1.23.2 re
AS3(config-router)#neighbor 192.1.23.2 remote-as 2
AS3(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.23.2 Up
nei
AS3(config-router)#neighbor 192.1.34.4 rem
AS3(config-router)#neighbor 192.1.34.4 remote-as 4
AS3(config-router)#net
AS3(config-router)#network 4.4.4.4 mask 255.0.0.0
AS3(config-router)#network 14.1.0.1 mask 255.255.0.0
AS3(config-router)#netw
AS3(config-router)#network 2.2.2.2m
AS3(config-router)#network 2.2.2.2 ,
AS3(config-router)#network 2.2.2.2 ms
AS3(config-router)#network 2.2.2.2 ma
AS3(config-router)#network 2.2.2.2 mask 255.0.0.0
AS3(config-router)#net
AS3(config-router)#network 12.1.0.1 mask 255.255.0.0
AS3(config-router)#net
AS3(config-router)#network 3.3.3.3 mask 255.0.0.0
AS3(config-router)#networkr
AS3(config-router)#netwo
AS3(config-router)#network 13.1.0.1 mask 255.255.0.0
AS3(config-router)#exit
```

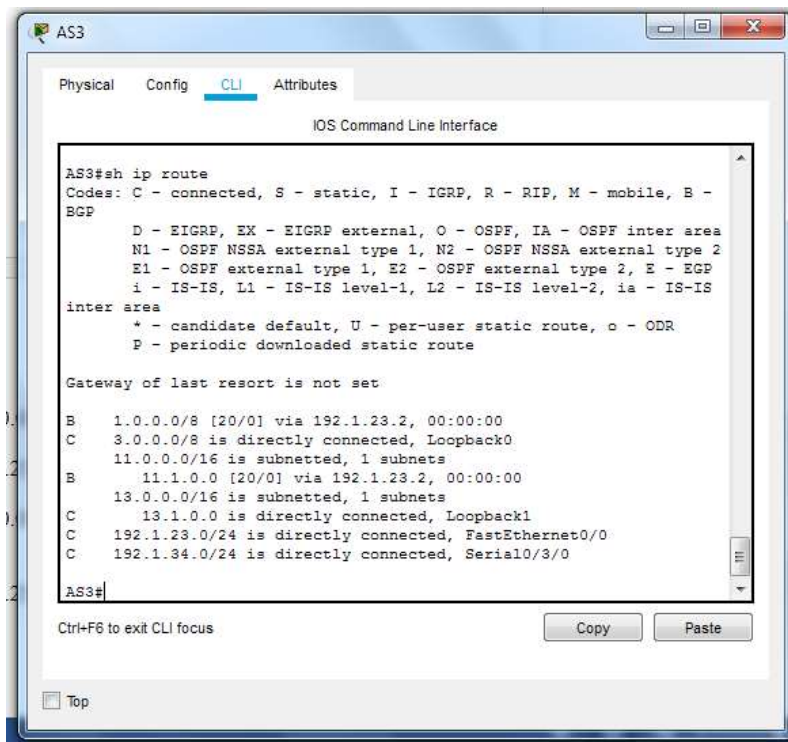


Figura 3: Salida del comando show

- 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.

```
AS4#conf term
```

Enter configuration commands, one per line. End with CNTL/Z.

```
AS4(config)#router b
```

```
AS4(config)#router bgp 4
```

```
AS4(config-router)#bg
```

```
AS4(config-router)#bgp router
```

```
AS4(config-router)#bgp router-id 44.44.44.44
```

```
AS4(config-router)#neio
```

```
AS4(config-router)#ne
```

```
AS4(config-router)#nei
```

```
AS4(config-router)#neighbor 192.1.34.3 re
```

```
AS4(config-router)#neighbor 192.1.34.3 remote-as 3
```

```
AS4(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.34.3 Up
```

```
neig
```

```
AS4(config-router)#neighbor 192.1.23.3 re
AS4(config-router)#neighbor 192.1.23.3 remote-as 3
AS4(config-router)#ne
AS4(config-router)#nei
AS4(config-router)#neighbor 192.1.23.2 re
AS4(config-router)#neighbor 192.1.23.2 remote-as 2
AS4(config-router)#nei
AS4(config-router)#neighbor 192.1.12.2 re
AS4(config-router)#neighbor 192.1.12.2 remote-as 2
AS4(config-router)#neig
AS4(config-router)#neighbor 192.1.12.1 re
AS4(config-router)#neighbor 192.1.12.1 remote-as 1
AS4(config-router)#ne
AS4(config-router)#net
AS4(config-router)#network 3.3.3.3 mask 255.0.0.0
AS4(config-router)#net
AS4(config-router)#network 13.1.0.1 mask 255.255.0.0
AS4(config-router)#neto
AS4(config-router)#net
AS4(config-router)#network 12.1.0.1 mask 255.255.0.0
AS4(config-router)#net
AS4(config-router)#network 2.2.2.2 mask 255.0.0.0
AS4(config-router)#net
AS4(config-router)#network 11.1.0.1 mask
AS4(config-router)#network 11.1.0.1 mask 255.255.0.0
AS4(config-router)#network 14.1.0.1 mask
AS4(config-router)#network 14.1.0.1 mask 255.255.0.0
AS4(config-router)#net
AS4(config-router)#network 4.4.4.4 mask 255.0.0.0
AS4(config-router)#exit
```

```
AS4#sh ip rot
AS4#sh ip ro
AS4#sh 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 192.1.34.3, 00:00:00
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
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.34.3, 00:00:00
     13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0 [20/0] via 192.1.34.3, 00:00:00
C    192.1.34.0/24 is directly connected, Serial10/3/0

AS4#
```

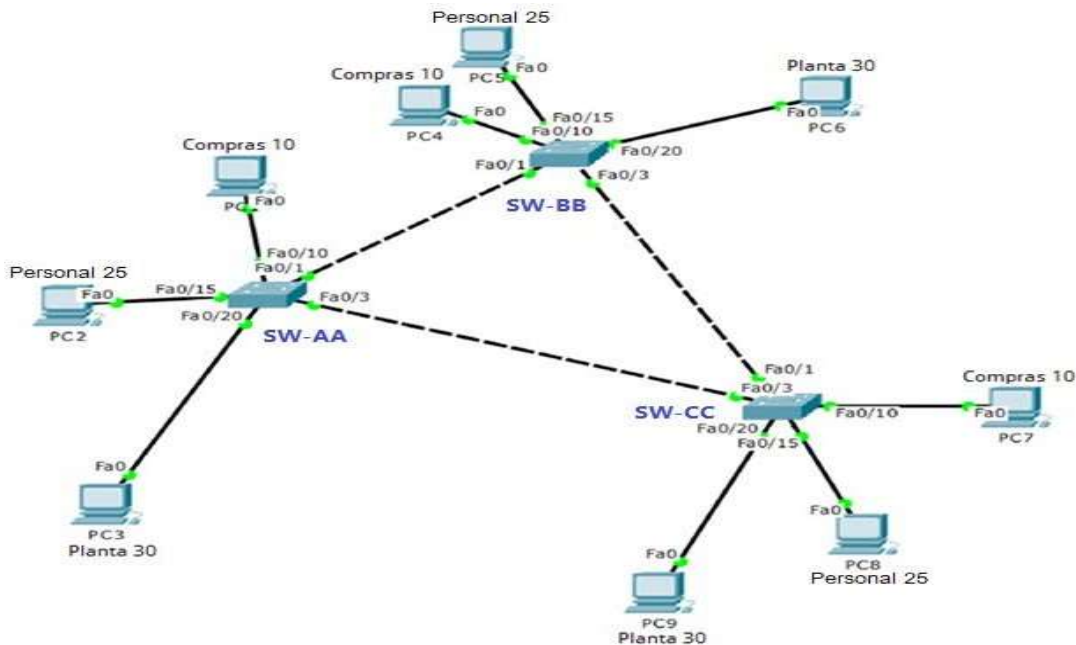
Ctrl+F6 to exit CLI focus

Copy Paste

Top

Figura 4: Comando show ip route

## Escenario 2



### A. Configurar VTP

1. Todos los switches se configurarán para usar VTP para las actualizaciones de VLAN. El switch SW-BB se configurará como el servidor. Los switches SW-AA y SW-CC se configurarán como clientes. Los switches estarán en el dominio VTP llamado CCNP y usando la contraseña cisco.
2. Verifique las configuraciones mediante el comando `show vtp status`.

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

4. 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**.
5. Verifique el enlace "trunk" entre SW-AA y SW-BB usando el comando **show interfaces trunk**.
6. 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
7. Verifique el enlace "trunk" el comando **show interfaces trunk** en SW-AA.

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

12. Configure el puerto F0/10 en modo de acceso para SW-AA, SW-BB y SW-CC y asígnelo a la VLAN 10.
13. 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.

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

14. En cada uno de los Switches asigne una dirección IP al SVI (*Switch Virtual Interface*) para VLAN 99 de acuerdo con la siguiente tabla de direccionamiento y active la interfaz.

Equipo	Interfaz	Dirección IP	Máscara
SW-AA	VLAN 99	190.108.99.1	255.255.255.0
SW-BB	VLAN 99	190.108.99.2	255.255.255.0
SW-CC	VLAN 99	190.108.99.3	255.255.255.0

15. Ejecute un Ping desde cada PC a los demás. Explique por qué el ping tuvo o no tuvo éxito.
  16. Ejecute un Ping desde cada Switch a los demás. Explique por qué el ping tuvo o no tuvo éxito.
  17. Ejecute un Ping desde cada Switch a cada PC. Explique por qué el ping tuvo o no tuvo éxito.
- Configurar VTP

```
Switch>enable Switch#conf t
Enter configuration commands, one per line. End with
CNTL/Z. Switch(config)#hostname SW-AA
SW-AA(config)#vtp mode
client Setting device to VTP
CLIENT mode. SW-
AA(config)#vtp domain CCNP
Changing VTP domain name from NULL to
CCNP SW-AA(config)#vtp password cisco
Setting device VLAN database password
to cisco SW-AA(config)#
SW-AA#
%SYS-5-CONFIG_1: Configured from console by console
```



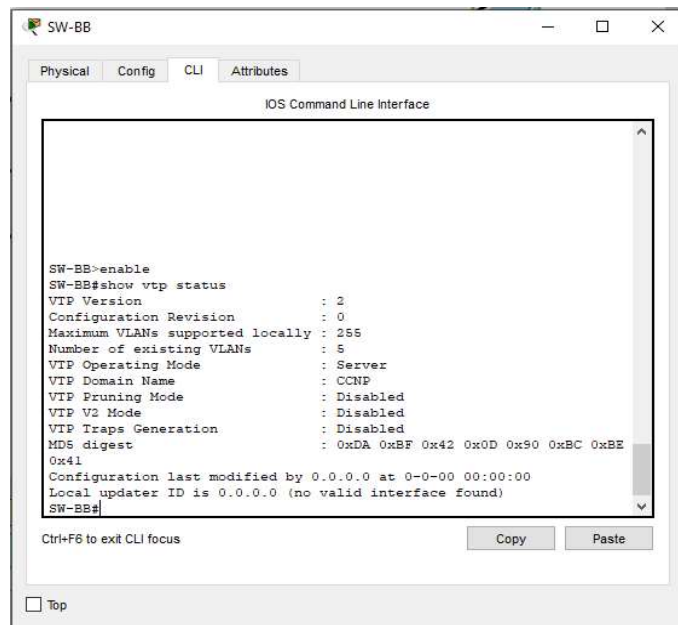
Configuración de switch como cliente en el dominio CCNP con el nombre SW-AA y con contraseña cisco.

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

Configuración de switch como servidor en el dominio CCNP con el nombre SW-BB con contraseña cisco

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

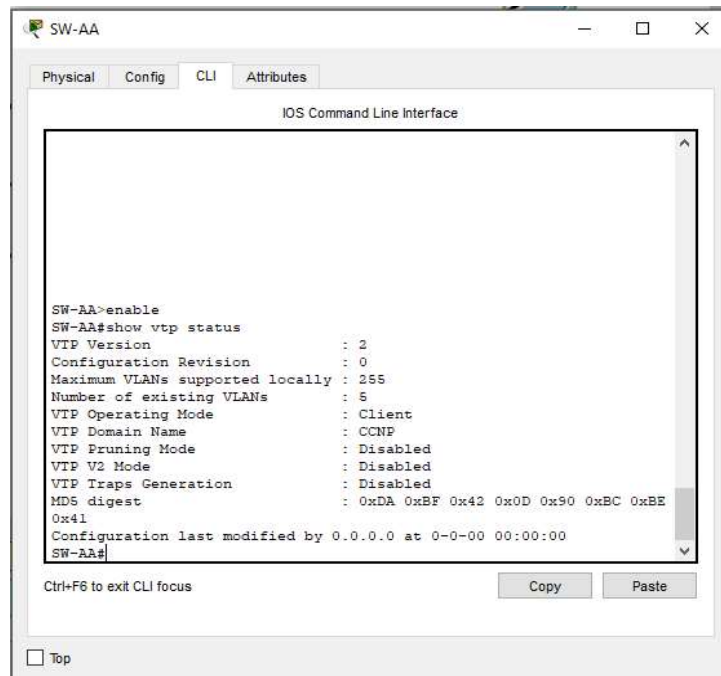
Configuración de switch a modo cliente en el dominio CCNP con contraseña cisco.



The screenshot shows a terminal window for switch SW-BB. The user has entered the command 'show vtp status' and the output is displayed. The output shows that the switch is currently in 'Server' mode. The VTP domain name is 'CCNP'. The VTP pruning mode is 'Disabled'. The VTP traps generation is 'Disabled'. The MD5 digest is '0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE 0x41'. The configuration was last modified by '0.0.0.0' at '0-0-00 00:00:00'. The local updater ID is '0.0.0.0 (no valid interface found)'. The prompt is 'SW-BB#'. There are 'Copy' and 'Paste' buttons at the bottom right of the terminal window.

```
SW-BB>enable
SW-BB#show vtp status
VTP Version          : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode   : Server
VTP Domain Name     : CCNP
VTP Pruning Mode    : Disabled
VTP V2 Mode        : Disabled
VTP Traps Generation : Disabled
MD5 digest          : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE
0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
SW-BB#
```

Figura 6: Ejecución comando show vtp status en SW-BB



The screenshot shows a terminal window for switch SW-AA. The user has entered the command 'show vtp status' and the output is displayed. The output shows that the switch is currently in 'Client' mode. The VTP domain name is 'CCNP'. The VTP pruning mode is 'Disabled'. The VTP traps generation is 'Disabled'. The MD5 digest is '0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE 0x41'. The configuration was last modified by '0.0.0.0' at '0-0-00 00:00:00'. The prompt is 'SW-AA#'. There are 'Copy' and 'Paste' buttons at the bottom right of the terminal window.

```
SW-AA>enable
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
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-AA#
```

Figura 5: Ejecución comando show

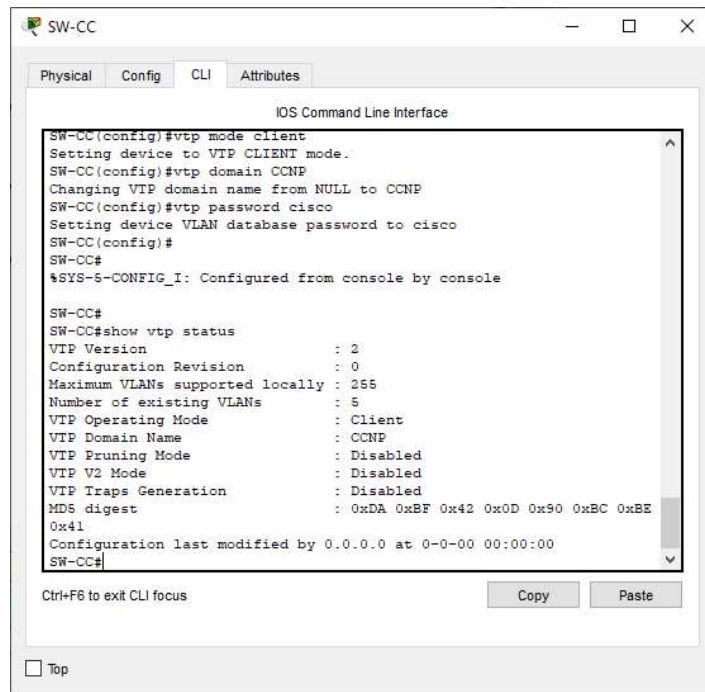


Figura 7: Ejecución comando

Configurar DTP (Dynamic Trunking Protocol)

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-

BB>ena

ble SW-

BB#conf

t

SW-BB(config-if)#interface f0/1

SW-BB(config-if)#switchport mode dynamic desirable

Se configura el switch SW-BB en modo Dynamic desirable en el otro switch no se realizan cambios.

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

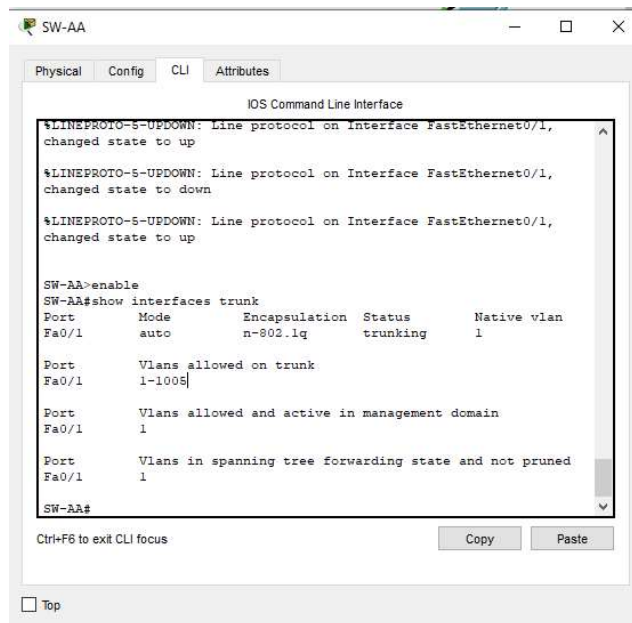


Figura 8: Interfaces trunk en SW-AA

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#conf t

*Enter configuration commands, one per line. End with*

*CNTL/Z. SW-AA(config)#interface f0/3*

*SW-AA(config-if)#switchport mode trunk*

*SW-AA(config-if)#*

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

Se realiza la configuración del switch SW-AA para un enlace estático usando el comando y la interfaz solicitada

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

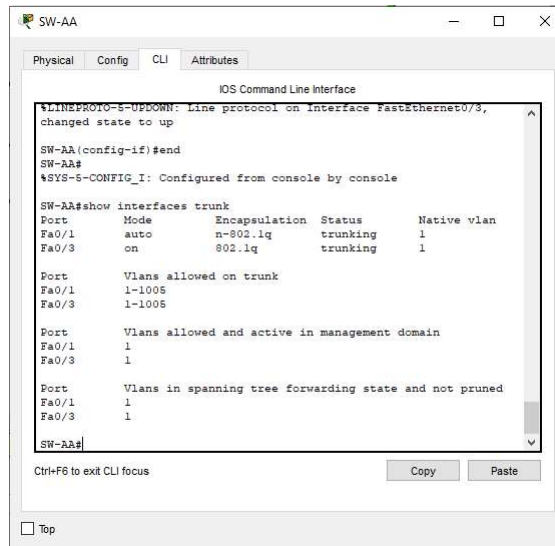


Figura 9: Interfaces trunk en SW-AA

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

SW-  
CC>ena  
ble SW-  
CC#conf  
t

Enter configuration commands, one per line. End with  
CNTL/Z. SW-CC(config)#interface f0/1  
SW-CC(config-if)#switchport mode trunk

Se configura el enlace entre los switches usando la interfaz  
seleccionada entre SW-CC y SW-CC

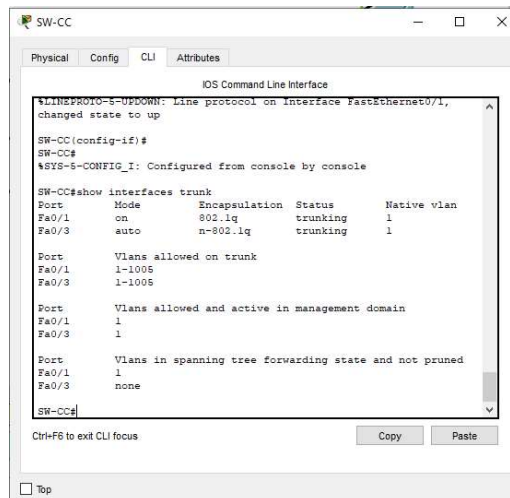


Figura 10: Interfaces trunk en SW-CC

Agregar VLANs y asignar puertos.

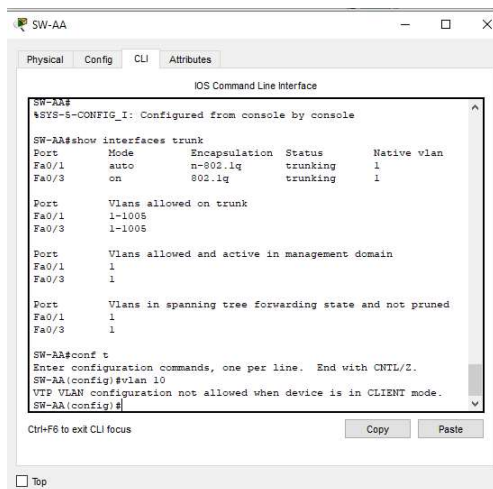
En SW-AA agregue la VLAN 10. En SW-BB agregue las VLANs Compras (10), Personal (25), Planta (30) y Admon (99)

*SW-AA#conf t*

*Enter configuration commands, one per line. End with CNTL/Z. SW-AA(config)#vlan 10*

*VTP VLAN configuration not allowed when device is in CLIENT mode. SW-AA(config-vlan)#name Compras*

Se realiza la configuración de la vlan en el switch SW-AA



```
SW-AA#
%SYS-5-CONFIG_I: Configured from console by console
SW-AA#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     auto      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#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
SW-AA(config-vlan)#
```

Figura 11 Vlan 10 en SW-AA

```

SW-BB#conf t
Enter configuration commands, one per line. End with
CNTL/Z. SW-BB(config)#
SW-BB(config)#vlan 10
SW-BB(config-vlan)#name
Compras SW-BB(config-
vlan)#vlan 30
SW-BB(config-vlan)#name
Planta SW-BB(config-
vlan)#vlan 25
SW-BB(config-vlan)#name
Personal SW-BB(config-
vlan)#vlan 99
SW-BB(config-vlan)#name
Admon SW-BB(config-
vlan)#exit
SW-
BB(config)#
exit SW-BB#

```

Se crean y nombran las Vlan en SW-BB compras, planta, personal y admon.

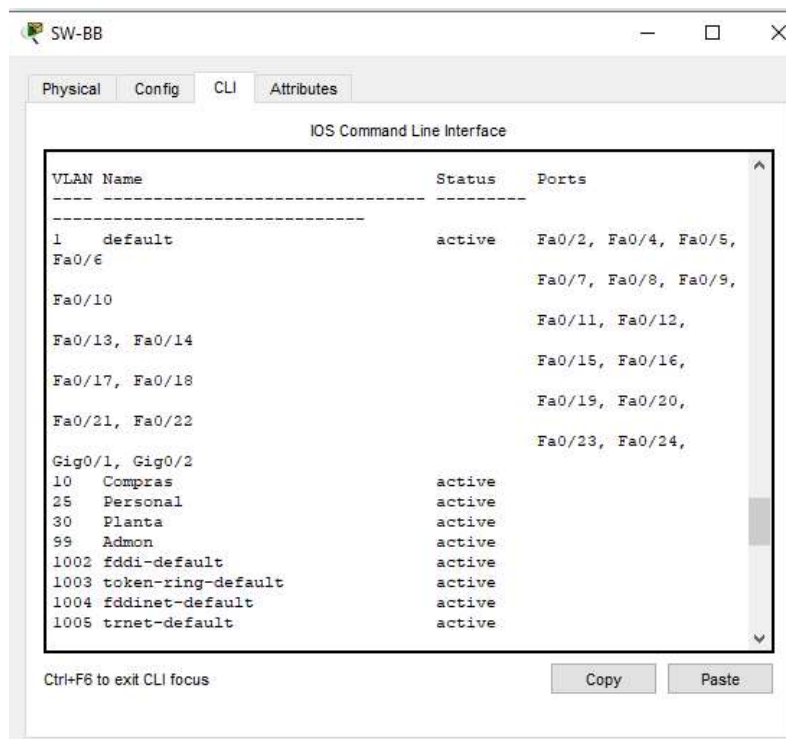


Figura 12 0,25,30 y 99 en SW-BB

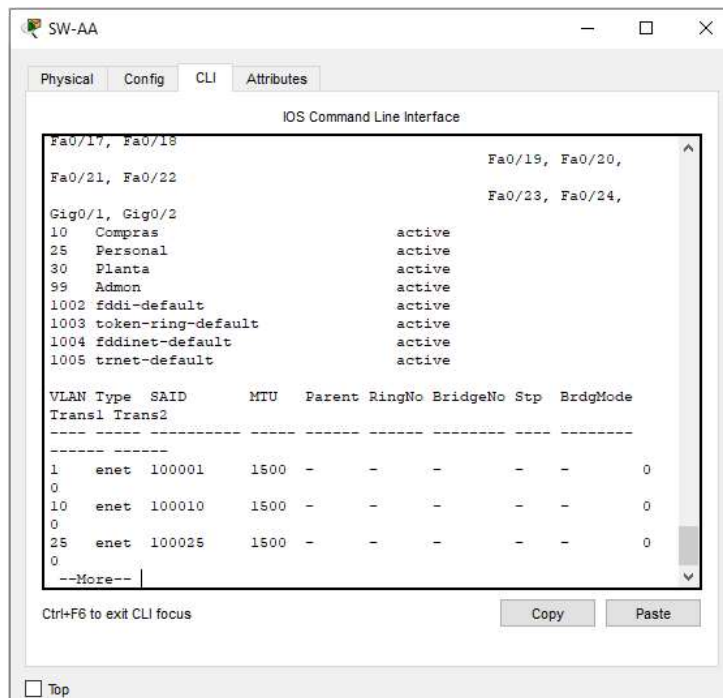


Figura 13 Creación de Vlan

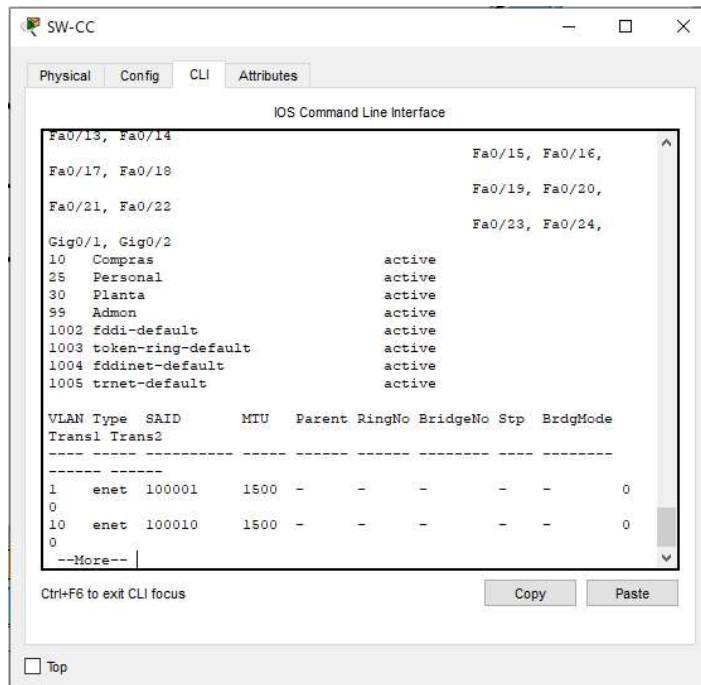


Figura 14 Vlan en SW-CC



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

Tabla 2: Interfaz y VLAN direccionamiento

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

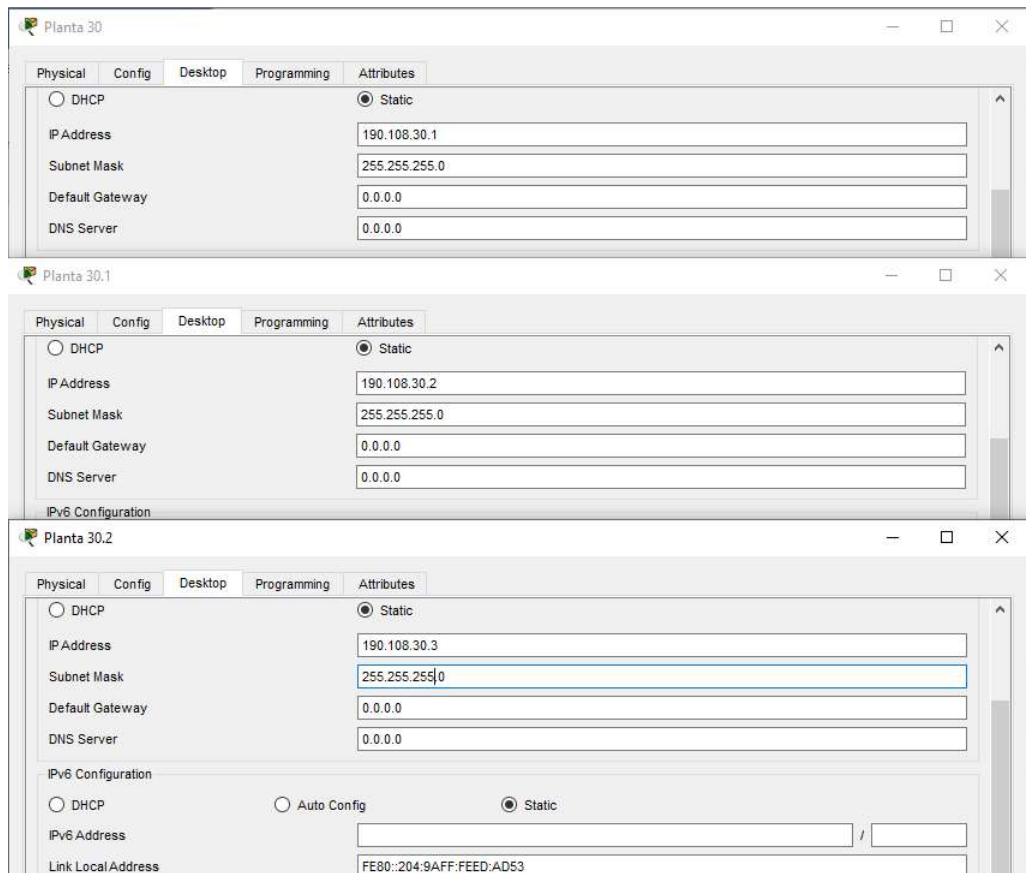


Figura 15 Configuración de direccionamiento en PCs

Se realiza la misma configuración con los demás equipos conectados teniendo en cuenta la tabla suministrada.

2. 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#  
SW-AA#conf t  
Enter configuration commands, one per line. End with  
CNTL/Z. 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)#interface f0/15  
SW-AA(config-if)#switchport mode  
access SW-AA(config-if)#switchport  
access vlan 25 SW-AA(config-  
if)#interface f0/20  
SW-AA(config-if)#switchport mode  
access SW-AA(config-if)#switchport  
access vlan 30 SW-AA(config-if)#
```

Se realiza la configuración de las interfaces para que pueda pasar solo una Vlan usando el comando switchport mode Access. La misma operación es ejecutada en los demás switches teniendo en cuenta la información suministrada del escenario.

```
SW-  
BB>ena  
ble SW-  
BB#conf  
t  
Enter configuration commands, one per line. End with  
CNTL/Z. 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)#interface f0/15  
SW-BB(config-if)#switchport mode  
access SW-BB(config-if)#switchport  
access vlan 25 SW-BB(config-  
if)#interface f0/20  
SW-BB(config-if)#switchport mode  
access SW-BB(config-if)#switchport  
access vlan 30 SW-BB(config-if)#
```

El mismo procedimiento es aplicado para SW-BB y SW-CC, asignando cada interfaz a una vlan especifica.

```
SW-  
CC>ena  
ble SW-  
CC#conf  
t
```

Enter configuration commands, one per line. End with  
CNTL/Z. 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)#interface f0/15  
SW-CC(config-if)#switchport mode  
access SW-CC(config-if)#switchport  
access vlan 25 SW-CC(config-  
if)#interface f0/20
```

```
SW-CC(config-if)#switchport mode  
access SW-CC(config-if)#switchport  
access vlan 30 SW-CC(config-if)#
```

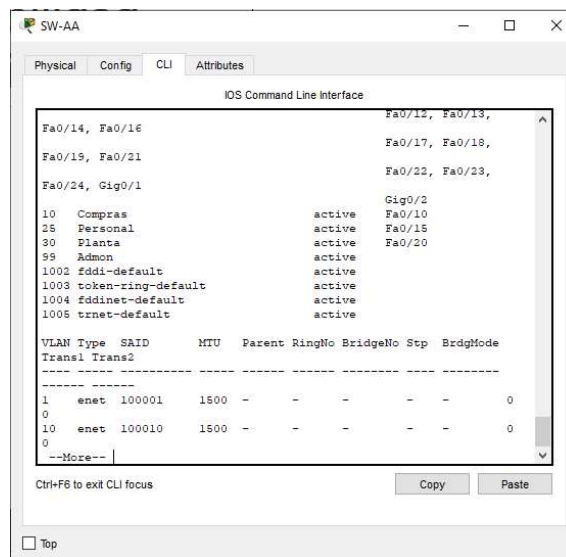


Figura 16 Verificación de interfaz Vlan en SW-AA

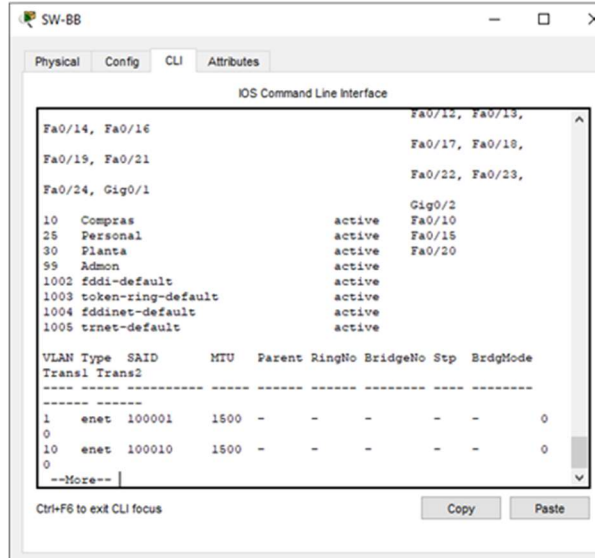


Figura 17 Vlan en SW-BB

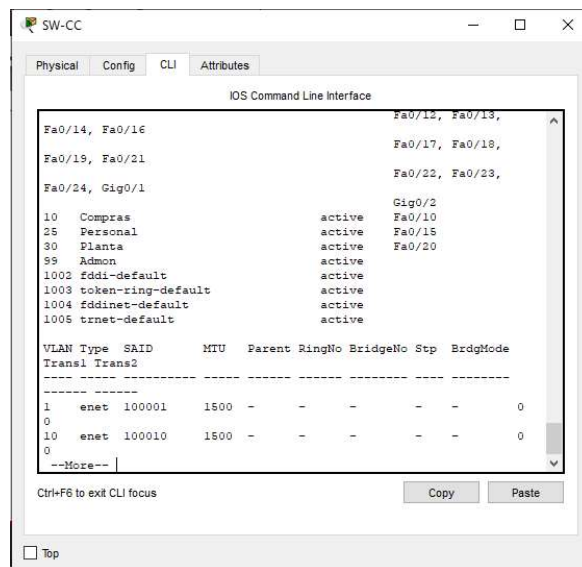
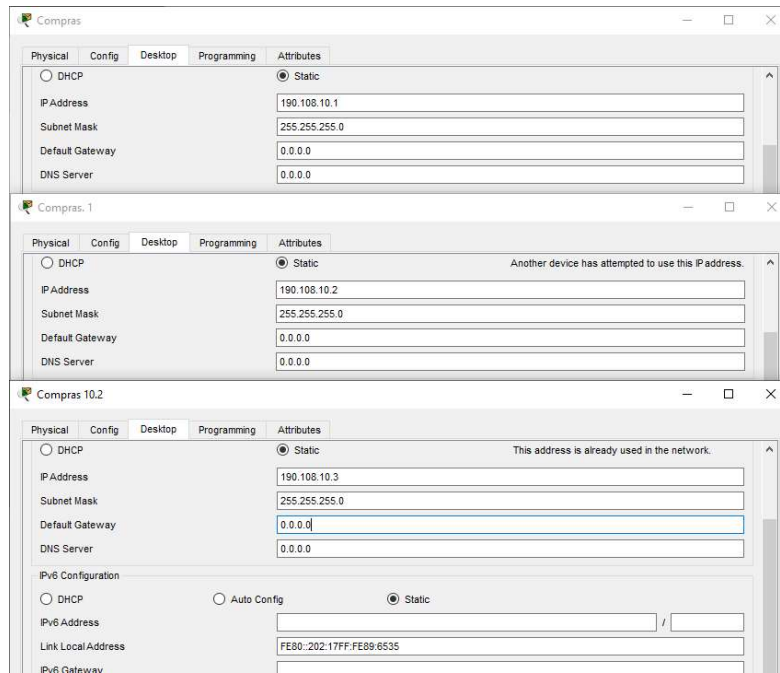


Figura 18 Verificación de interfaz

3. 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.



*Figura 19 Direcccionamiento IP en PCs de compras.*

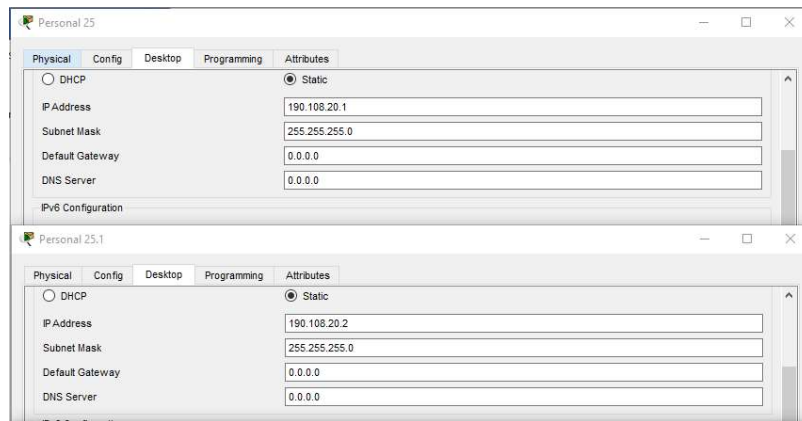


Figura 20 Direccionamiento IP en PCs

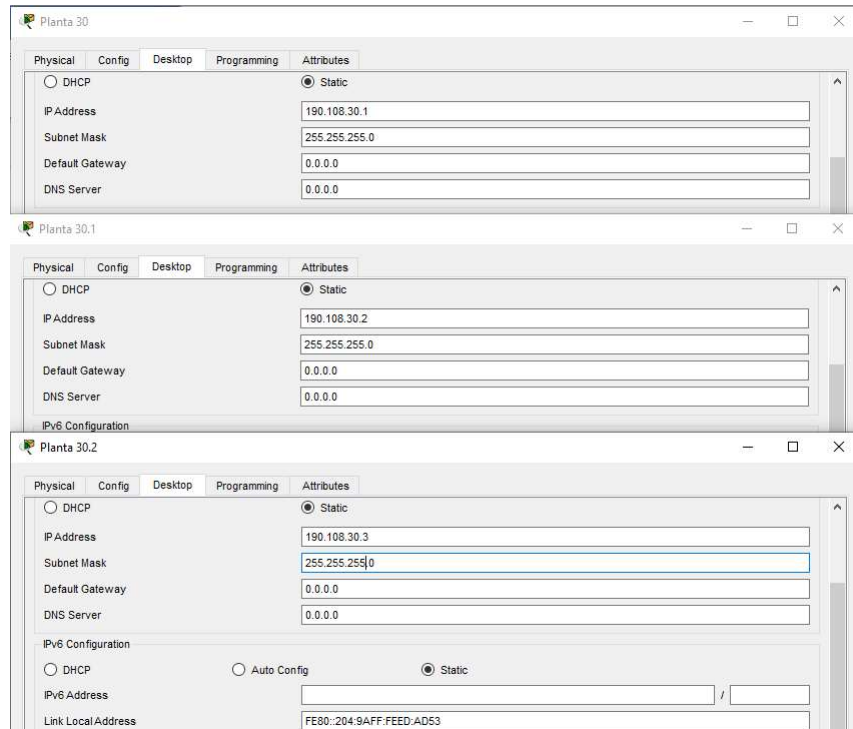


Figura 21 Direccionamiento IP

### Configurar las direcciones IP en los Switches.

4. En cada uno de los Switches asigne una dirección IP al SVI (*Switch Virtual Interface*) para VLAN 99 de acuerdo con la siguiente tabla de direccionamiento y active la interfaz.

Equipo	Interfaz	Dirección IP	Máscara
SW-AA	VLAN 99	190.108.99.1	255.255.255.0
SW-BB	VLAN 99	190.108.99.2	255.255.255.0
SW-CC	VLAN 99	190.108.99.3	255.255.255.0

```
SW-
AA>ena
ble SW-
AA#conf
t
Enter configuration commands, one per line. End with
CNTL/Z. SW-AA(config)#interface vlan 99
SW-AA(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
SW-AA(config-if)#
```

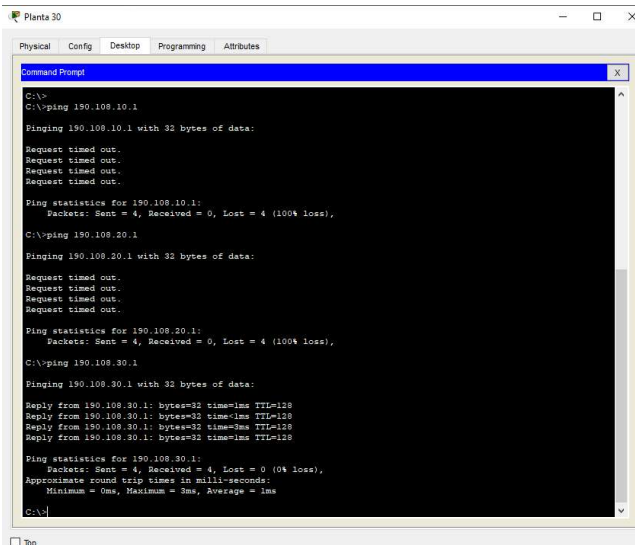
```
SW-
BB>ena
ble SW-
BB#conf
t
Enter configuration commands, one per line. End with
CNTL/Z. SW-BB(config)#interface vlan 99
SW-BB(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
SW-BB(config-if)#end
```

```
SW-
CC>ena
ble SW-
CC#conf
t
Enter configuration commands, one per line. End with
CNTL/Z. SW-CC(config)#interface vlan 99
SW-CC(config-if)#
```

*%LINK-5-CHANGED: Interface Vlan99, changed state to up*  
*%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up*  
*SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0*  
*SW-CC(config-if)#end*  
*SW-CC#*

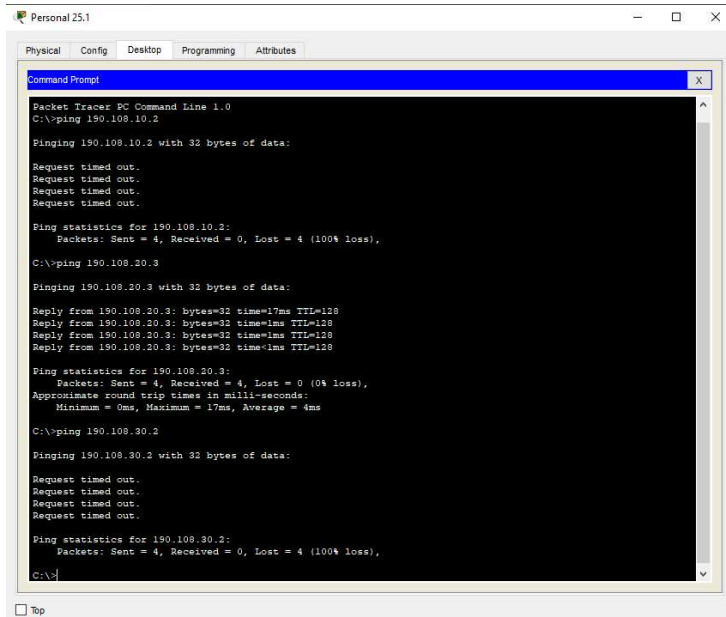
Verificar la conectividad Extremo a Extremo

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



```
Planta 30
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>ping 190.108.10.1
Pinging 190.108.10.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.10.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 190.108.20.1
Pinging 190.108.20.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.20.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
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=1ms TTL=128
Reply from 190.108.30.1: bytes=32 time=1ms TTL=128
Reply from 190.108.30.1: bytes=32 time=3ms TTL=128
Reply from 190.108.30.1: bytes=32 time=1ms TTL=128
Ping statistics for 190.108.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms
C:\>
```

Figura 22: Ping exitoso



```
Personal 25.1
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 190.108.10.2
Pinging 190.108.10.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.10.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 190.108.20.3
Pinging 190.108.20.3 with 32 bytes of data:
Reply from 190.108.20.3: bytes=32 time=17ms TTL=128
Reply from 190.108.20.3: bytes=32 time=1ms TTL=128
Reply from 190.108.20.3: bytes=32 time=1ms TTL=128
Reply from 190.108.20.3: bytes=32 time=1ms TTL=128
Ping statistics for 190.108.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 17ms, Average = 4ms
C:\>ping 190.108.30.2
Pinging 190.108.30.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.30.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

Figura 24 190.108.20.3 desde personal 25



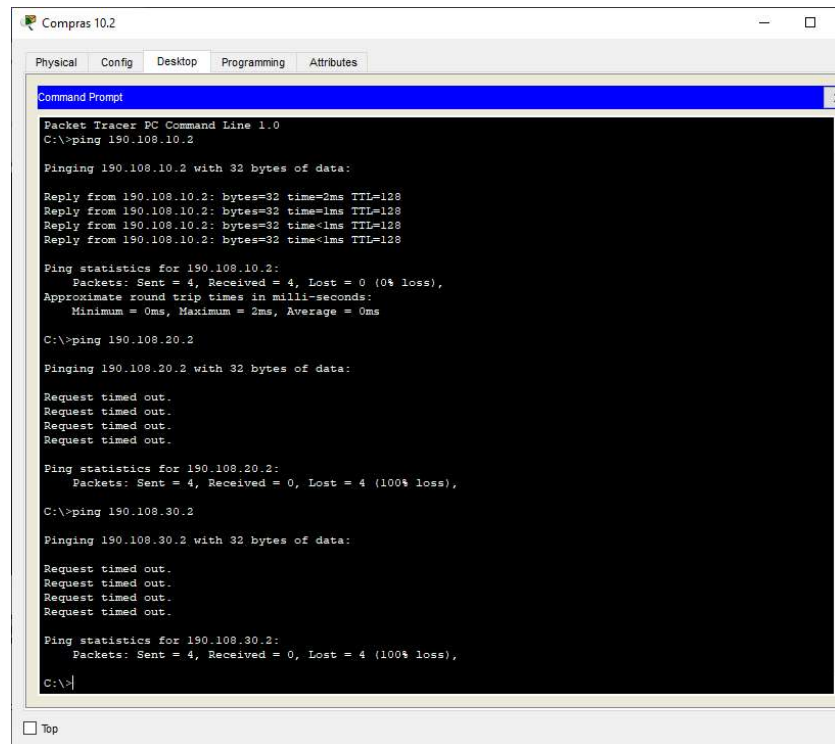


Figura 25: Ping desde compras

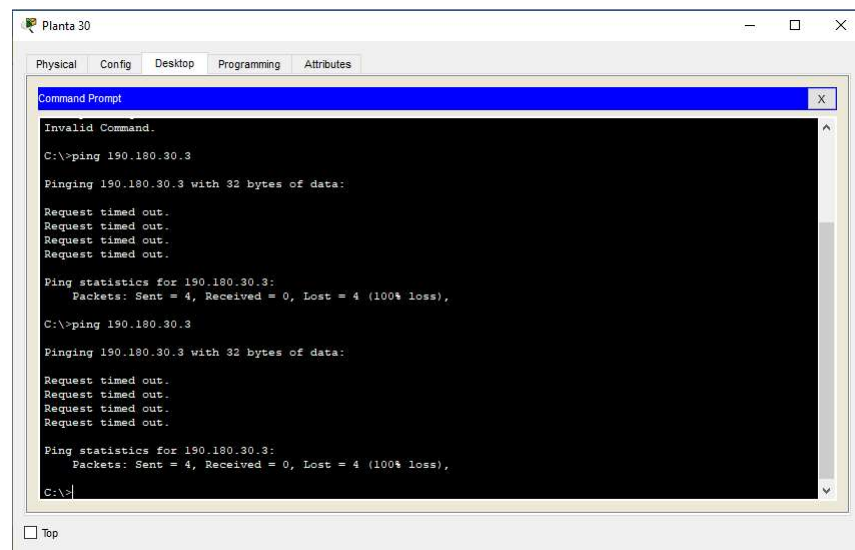
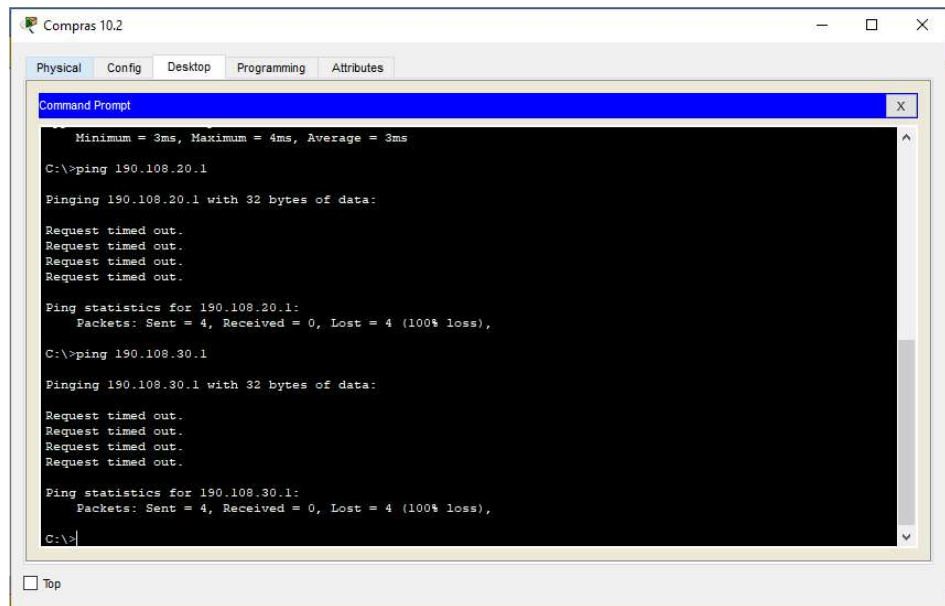


Figura 26: Compras 30.2



*Figura 27: Ping desde compras a personal y planta*

Ping desde los switches:

```
SW-AA>enable
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 =  
0/0/1 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 =  
0/1/3 ms SW-AA#

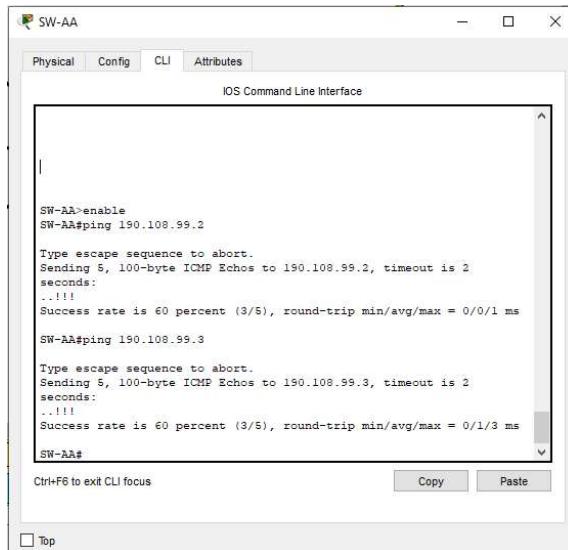


Figura 28: SW-AA a SW-BB y SW-CC

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 =

0/0/1 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

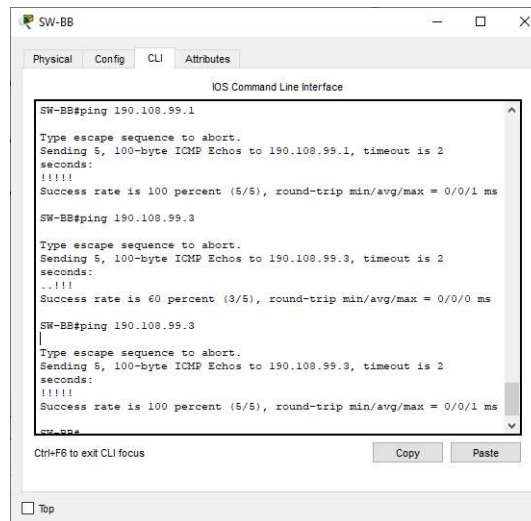


Figura 29: Ping desde SW-BB hacia SW-AA y SW-CC

```

SW-CC#ping 190.108.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/0/0 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:
!!!!

```

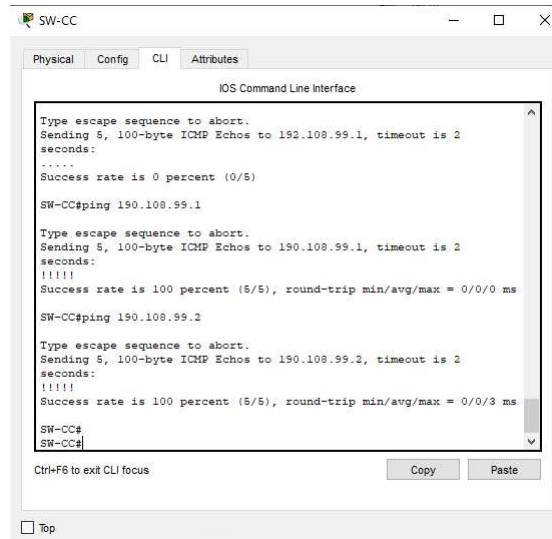
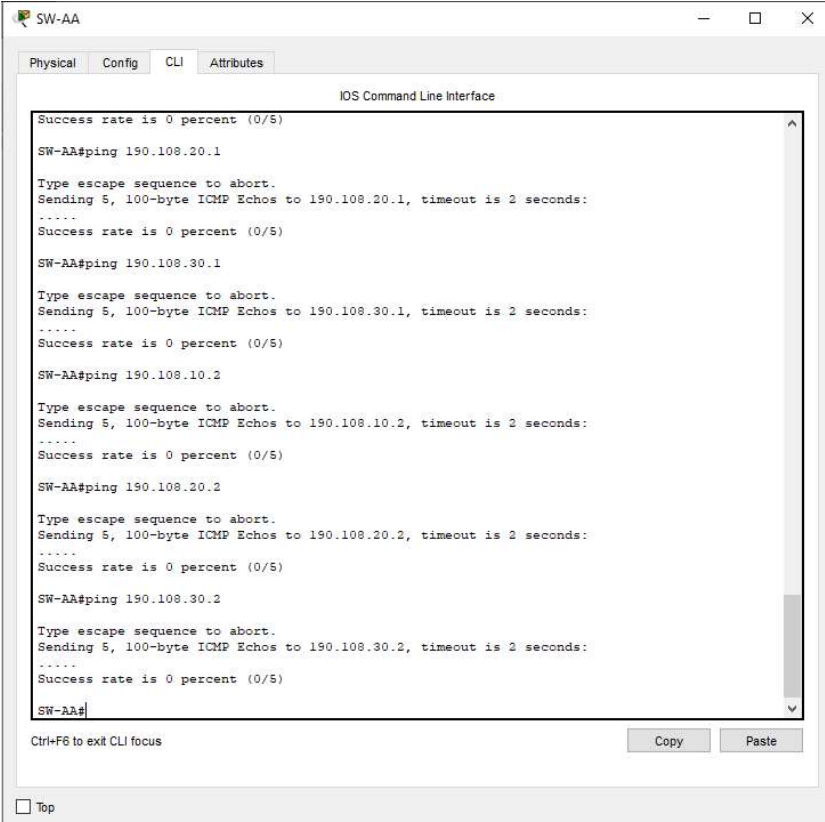


Figura 30: Hacia SW-AA y SW-BB

Los pings entre los switches es exitoso ya que ellos están configurados con el comando switchport mode trunk o enlace troncal lo cual les permite el paso de información de diferentes VLAN por un enlace, además los comandos switchport mode dynamic desirable permiten que los enlaces troncales se conviertan en activos.

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



```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
Success rate is 0 percent (0/5)
SW-AA#ping 190.108.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#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-AA#ping 190.108.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#ping 190.108.20.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#ping 190.108.30.2
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-AA#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Figura 31: Hacia los PCs

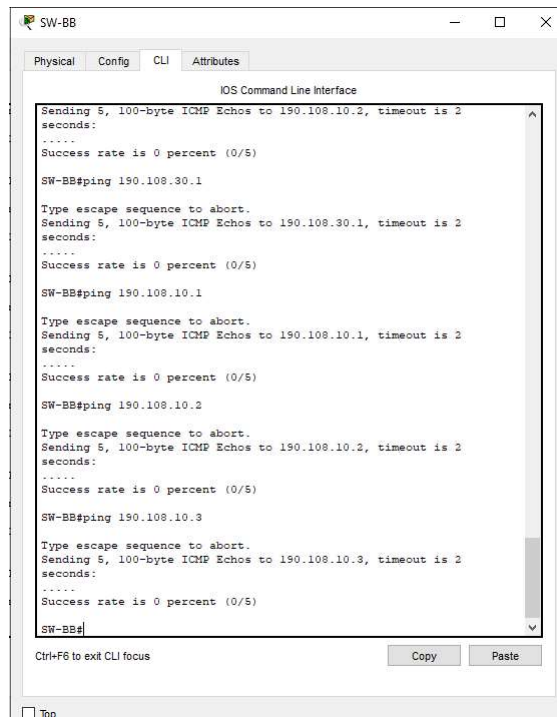


Figura 32: Ping desde SW-BB hacia los PCs

Los pings efectuados de los switches a los PCs no fueron exitosos ya que no se ha realizado la configuración de direccionamiento ip y gateway en cada una de las Vlan creadas en cada switch.

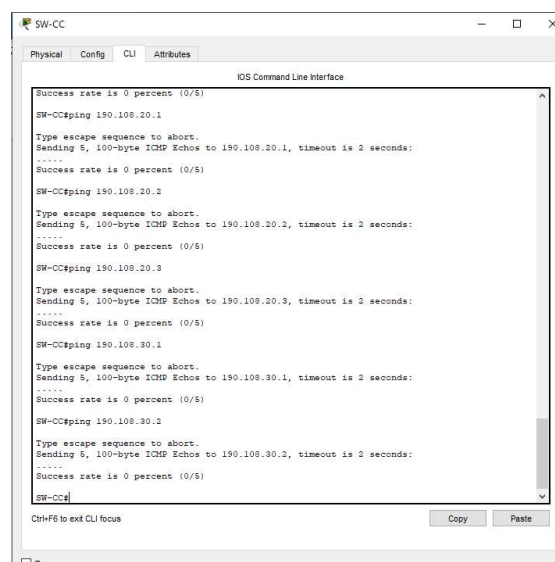


Figura 33: SW-CC hacia los PCs

## CONCLUSIONES

Se utilizó el Border Gateway Protocol (BGP) el cual es un protocolo de puerta de enlace estandarizado que intercambia información de enrutamiento a través de sistemas autónomos (AS) en Internet. Cuando un enrutador de red está conectado a otras redes, no puede determinar a qué red es la mejor red para enviar sus datos por sí mismo. Border Gateway Protocol considera a todos los socios de interconexión que tiene un enrutador y envía el tráfico al enrutador más cercano al destino de los datos. Esta comunicación es posible porque, durante el arranque, BGP permite a los pares comunicar su información de enrutamiento y luego almacena esa información en una Base de información de enrutamiento (RIB).

Por su parte el protocolo de enlace dinámico (DTP) se utiliza para transportar el tráfico de más de una VLAN. El puerto que conecta dos conmutadores diferentes y los conmutadores tienen más de una VLAN configurada, entonces ese puerto debe convertirse en troncal. Si se permiten todas las VLAN, los puertos troncales transportarán el tráfico de todas las VLAN, incluida la VLAN nativa para la cual el tráfico no se etiqueta, de lo contrario, solo el tráfico troncal permitirá el tráfico de las VLAN permitidas.

Acceso al modo de puerto de conmutación (modo DTP ) -

Este modo pone la interfaz del conmutador en modo permanente sin enlace troncal, independientemente de si la interfaz vecina es un puerto troncal o si intenta convertirse en un puerto troncal, por eso se conoce como modo DTP OFF. El puerto es un puerto de acceso de capa 2 dedicado.

## BIBLIOGRAFÍA

- ARIGANELLO. Ernesto, BARRIENTOS SEVILLA. Enrique. Redes Cisco Guía de Estudio para la Certificación CCNP. Segunda Edición. Madrid: Editorial RA-MA. 2014. 369 p.
- Graziani, D. T. (2015). Implementing Cisco IP Routing (ROUTE). Indianapolis: Cisco Press.
- INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. Compendio, tesis y otros trabajos de grado. Bogotá. ICONTEC,2019.
- Switched Networks (SWITCH) Foundation Learning Guide: Foundation learning for SWITCH 642-813. Cisco press.
- TEARE. Diane, VACHON. Bob, GRAZIANI. Rick. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide. Indianapolis. Cisco Press. 2015. 768 p.
- Zhang, R., & Bartell, M. (2003). BGP design and implementation. Cisco Press.