

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

SEREGIO ANDRES HERNANDEZ VELEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA TELECOMUNICACIONES
MEDELLÍN
2020

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

SERGIO ANDRES HERNANDEZ VELEZ

Diplomado de opción de grado presentado para optar el
título de INGENIERO ELECTRONICO/SISTEMAS/TELECO

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA TELECOMUNICACIONES
MEDELLÍN
2020

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

MEDELLÍN, 22 de mayo de 2020

AGRADECIMIENTOS

A mis padres quienes generaron una cultura de estudio y dedicación, a mi hermana quien me ha apoyado en la consecución de este título; a la universidad Nacional Abierta y a Distancia quien permitió con su modalidad virtual permitió mi desarrollo académico mientras realizaba las labores profesionales.

CONTENIDO

AGRADECIMIENTOS.....	4
LISTAS DE TABLA	6
LISTA DE FIGURAS	7
GLOSARIO	8
RESUMEN.....	9
ABSTRACT.....	9
INTRODUCCIÓN	10
DESARROLLO	11
ESCENARIO 1	11
ESCENARIO 2	20
CONCLUSIONES	43
BIBLIOGRAFÍA.....	44

LISTAS DE TABLA

Tabla 1. Interfaces Loopback para configurar R1	11
Tabla 2. Interfaces Loopback para configurar R2	11
Tabla 3. Interfaces Loopback para configurar R3	12
Tabla 4. Interfaces Loopback para configurar R4	12
Tabla 5. Asignación direcciones IP a las VLAN	30
Tabla 6. Asignación direcciones IP de los conmutadores	35

LISTA DE FIGURAS

Figura 1 Simulación escenario 1	11
Figura 2 Tabla enrutamiento R1	15
Figura 3 Tabla enrutamiento R2	16
Figura 4 Tabla enrutamiento R3	17
Figura 5 Tabla enrutamiento R4	19
Figura 6 Escenario 2.....	20
Figura 7 Simulación Escenario 2	21
Figura 8 Show VTP en SW-AA	23
Figura 9 Show VTP status en SW-BB.....	23
Figura 10 Show VTP status en SW-CC	24
Figura 11 Show interface trunk en SW-AA	25
Figura 12 Show interface trunk en SW-BB	26
Figura 13 Show interface trunk en SW-AA	27
Figura 14 Comando Show Vlan en el SW-BB.....	30
Figura 15 Configuración equipo 1 SW-AA	31
Figura 16 Configuración equipo 2 SW-AA	31
Figura 17 Configuración equipo 3 SW-AA	31
Figura 18 Configuración equipo 1 SW-BB	32
Figura 19 Configuración equipo 2 SW-BB	32
Figura 20 Configuración equipo 3 SW-BB	32
Figura 21 Configuración equipo 1 SW-CC.....	33
Figura 22 Configuración equipo 2 SW-CC.....	33
Figura 23 Configuración equipo 3 SW-CC.....	33
Figura 24 Ping entre equipos VLAN 10.....	36
Figura 25 Ping entre equipos VLAN 25.....	37
Figura 26 Ping entre equipos VLAN 30.....	38
Figura 27 Ping entre los conmutadores	39
Figura 28 Ping desde SW-AA hacia los PCs de la VLAN 10	40
Figura 29 Ping desde SW-AA hacia los PCs de la VLAN 10	41
Figura 30 Ping desde SW-AA hacia los PCs de la VLAN 10	42

GLOSARIO

Enrutador: dispositivo de Hardware que opera en la capa 3 del modelo OSI, encargado de hacer el encaminamiento de los paquetes de datos entre redes para permitir su interconexión.

Servidor VTP: protocolo de mensajes de capa 2 que se utiliza para la configuración y administración de VLANs en los equipos Cisco, permite la centralización y la simplificación de la administración de VLANs

VLAN: es un método para crear redes LAN virtuales en una misma red física para diferenciar los dominios de Broadcast

Switch: dispositivo de Hardware que permite realizar la interconexión de dispositivos y redes a nivel de capa de enlace; realiza el reenvío de datos usando direcciones físicas de los elementos (**MAC**).

ACL: listas de control de acceso, es un mecanismo utilizado en seguridad informática que permite determinar los permisos de acceso que se va a tener en un dispositivo; teniendo diferentes niveles de filtrado (MAC, IP, protocolos entre otros)

RESUMEN

Este informe muestra la apropiación de los conceptos y practicas utilizadas en el diplomado de profundización CCNP, para optar por el título de Ingeniero de Telecomunicaciones; se plantean dos escenarios de red en los que actuaremos como administradores, implementadores y configuradores.

En los cuales se pide realizar la configuración de un protocolo de enrutamiento BGP (Border Gateway Protocol) entre diferentes enrutadores, recreando el escenario de interconexión de operadores de comunicaciones; el segundo escenario pide configurar una red corporativa, en la cual se utilizan Switches los cuales a través del protocolo VTP se realiza la administración de las VLAN

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

ABSTRACT

This report shows the appropriation of the concepts and practices used in the CCNP deepening diploma, to choose the title of Telecommunications Engineer; Two network scenarios are proposed in which they act as administrators, implementers and configurators.

In which is requested to configure a BGP (Border Gateway Protocol) routing protocol between 4 routers, simulatting the ISP networks interconection; The second scenario asks to configure a corporate network, in which we'll going to use VTP protocol to VLAN management.

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

INTRODUCCIÓN

A continuación, se presenta la solución del trabajo que denominaremos “Prueba de habilidades prácticas CCNP”; con el cual demostraremos desde la fase de diseño, implementación y configuración los conceptos apropiados en las actividades realizadas en el diplomado de profundización CCNP.

Se solicita diseñar, implementar y configurar 2 escenarios de redes, el primero una red de interconexión de redes usando el protocolo BGP (Border Gateway Protocol), este tipo de configuración muestra cómo funciona la conectividad en los operadores que prestan el servicio de internet.

El segundo escenario nos solicita el desarrollo de una red campus donde se interconectarán tres sedes de una misma entidad, usando la segmentación por VLAN (Virtual Local Area Network) separando los dominios de Broadcast para cada área de la entidad.

DESARROLLO

ESCENARIO 1

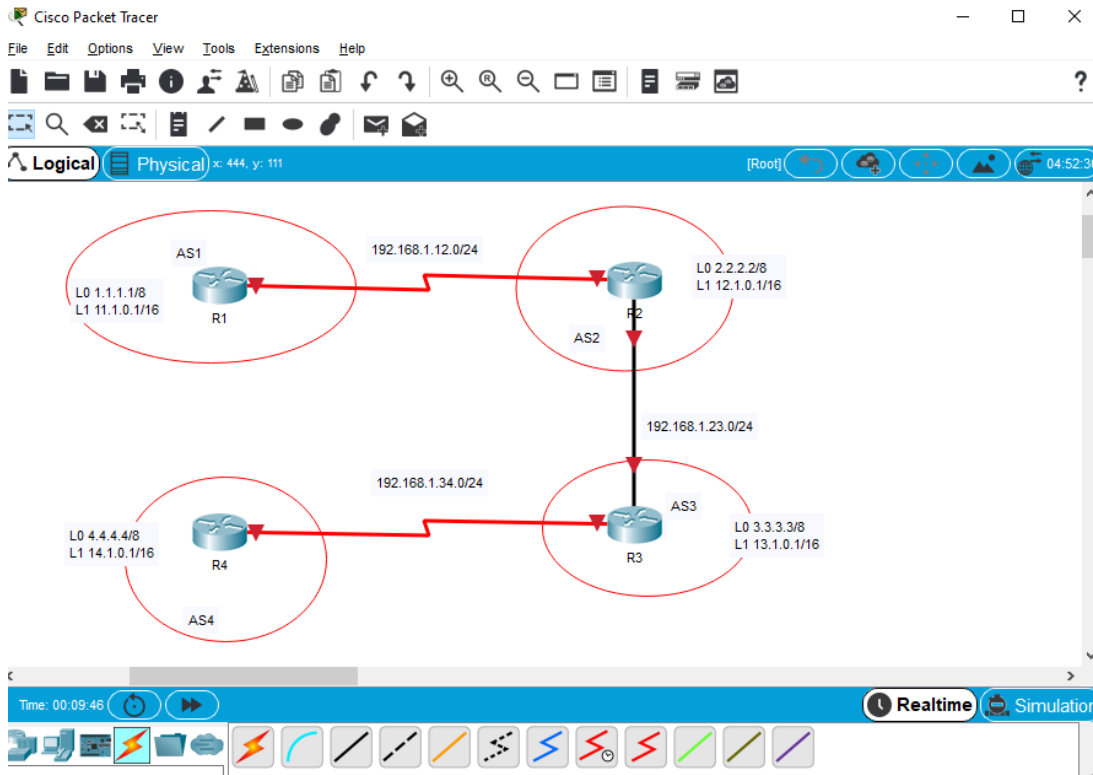


Figura 1 Simulación escenario 1

Data plan para la configuración

Tabla 1. Interfaces Loopback para configurar R1

	Interfaz	Dirección IP	Máscara
R1	Loopback 0	1.1.1.1	255.0.0.0
	Loopback 1	11.1.0.1	255.255.0.0
	S 0/1/0	192.1.12.1	255.255.255.0

Tabla 2. Interfaces Loopback para configurar R2

	Interfaz	Dirección IP	Máscara
R2	Loopback 0	2.2.2.2	255.0.0.0
	Loopback 1	12.1.0.1	255.255.0.0
	S 0/1/0	192.1.12.2	255.255.255.0
	G 0/0/0	192.1.23.2	255.255.255.0

Tabla 3. Interfaces Loopback para configurar R3

	Interfaz	Dirección IP	Máscara
R3	Loopback 0	3.3.3.3	255.0.0.0
	Loopback 1	13.1.0.1	255.255.0.0
	S 0/1/0	192.1.23.3	255.255.255.0
	G 0/0/0	192.1.34.3	255.255.255.0

Tabla 4. Interfaces Loopback para configurar R4

	Interfaz	Dirección IP	Máscara
R4	Loopback 0	4.4.4.4	255.0.0.0
	Loopback 1	14.1.0.1	255.255.0.0
	S 0/1/0	192.1.34.4	255.255.255.0

La actividad se realiza usando el Software propietario de Cisco **Packet tracer**

Se comienza con las configuraciones básicas en cada enrutador

Configuraciones generales de los 2 enrutadores

```
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)#password cisco
```

Configuración R1

```
Router(config)#hostname R1
R1(config)#interface lo0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#exit
R1(config)#intr lo1
R1(config-if)#ip ad 11.1.0.1 255.255.0.0
R1(config-if)#exit
R1(config)#interface s0/1/0
R1(config-if)#ip ad
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#des
R1(config-if)#description CX:T0 R2
R1(config-if)#no shutdown
```

Configuración R2

```
Router(config)#hostname R2
R2(config)#int lo0
R2(config-if)#ip add 2.2.2.2 255.0.0.0
R2(config-if)#int loo1
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#int s 0/1/0
R2(config-if)#ip ad 192.1.12.2 255.255.255.0
R2(config-if)#description CX:T0 R2
R2(config-if)#no shu
R2(config-if)#int g 0/0/0
R2(config-if)#ip ad 192.1.23.2 255.255.255.0
R2(config-if)#description CX:T0 R3
R2(config-if)#no shu
```

Configuración R3

```
Router(config)#host R3
R3(config)#int loo0
R3(config-if)#ip add 3.3.3.3 255.0.0.0
R3(config-if)#int loo1
R3(config-if)#
R3(config-if)#ip add 13.1.0.1 255.255.0.0
R3(config)#int g 0/0/0
R3(config-if)#ip add 192.1.23.3 255.255.255.0
R3(config-if)#des CX:T0 R2
R3(config-if)#no shu
R3(config-if)#int s 0/1/0
R3(config-if)#des CX:T0 R4
R3(config-if)#ip add 192.1.34.3 255.255.255.0
R3(config-if)#no shu
```

Configuración R4

```
Router(config)#host R4
R4(config)#int loo 0
R4(config-if)#ip ad 4.4.4.4 255.0.0.0
R4(config-if)#int loo1
R4(config-if)#ip add 14.1.0.1 255.255.0.0
R4(config-if)#int s 0/1/0
R4(config-if)#ip add 192.1.34.4 255.255.255.0
R4(config-if)#des CX: T0 R3
R4(config-if)#no shu
```

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.

Configuración de BGP

```
R1(config)#router bgp 1
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#neighbor 192.1.12.2 re
R1(config-router)#neighbor 192.1.12.2 remote-as 2
R1(config-router)#network 1.0.0.0 mask 255.0.0.0
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router)#network 192.1.12.0 mask 255.255.255.0
```

```
R2(config)#rout bgp 2
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#neighbor 192.1.12.3 remote-as 3
R2(config-router)#network 2.0.0.0 mask 255.0.0.0
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
R2(config-router)#network 192.1.23.0 mask 255.255.255.0
```

Verificación de la configuración de enrutamiento en R1 y R2

```

R1#sho ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
    D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
    i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
    * - candidate default, U - per-user static route, o - ODR
    P - periodic downloaded static route

Gateway of last resort is not set

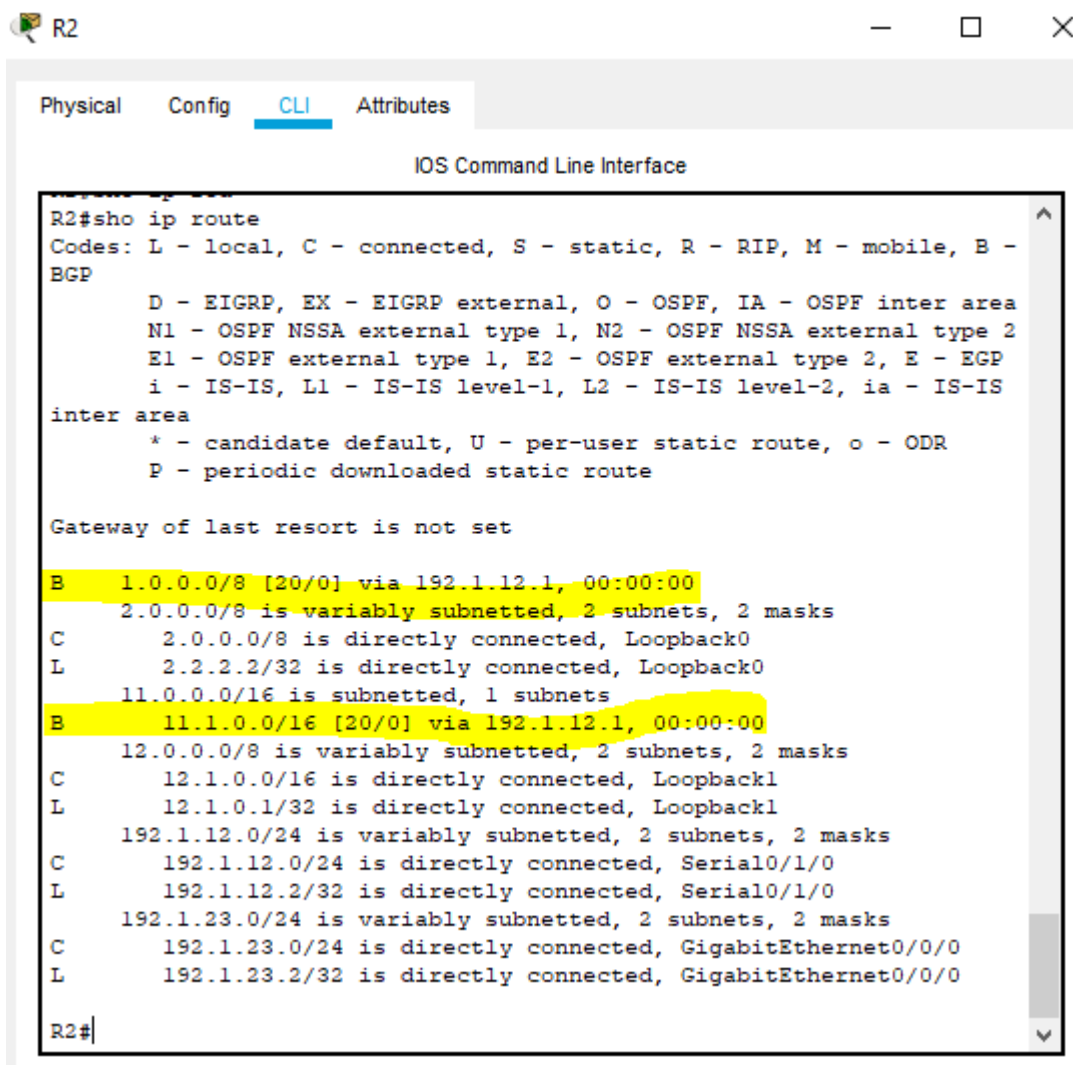
    1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       1.0.0.0/8 is directly connected, Loopback0
L       1.1.1.1/32 is directly connected, Loopback0
B       2.0.0.0/8 [20/0] via 192.1.12.2, 00:00:00
    11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       11.1.0.0/16 is directly connected, Loopback1
L       11.1.0.1/32 is directly connected, Loopback1
    12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0/16 [20/0] via 192.1.12.2, 00:00:00
    192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.12.0/24 is directly connected, Serial0/1/0
L       192.1.12.1/32 is directly connected, Serial0/1/0
B       192.1.23.0/24 [20/0] via 192.1.12.2, 00:00:00

R1#
  
```

Ctrl+F6 to exit CLI focus

Copy Paste

Figura 2 Tabla enrutamiento R1



The screenshot shows a terminal window for R2 with tabs for Physical, Config, CLI (selected), and Attributes. The title bar reads "IOS Command Line Interface". The terminal output is as follows:

```
R2#sho ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

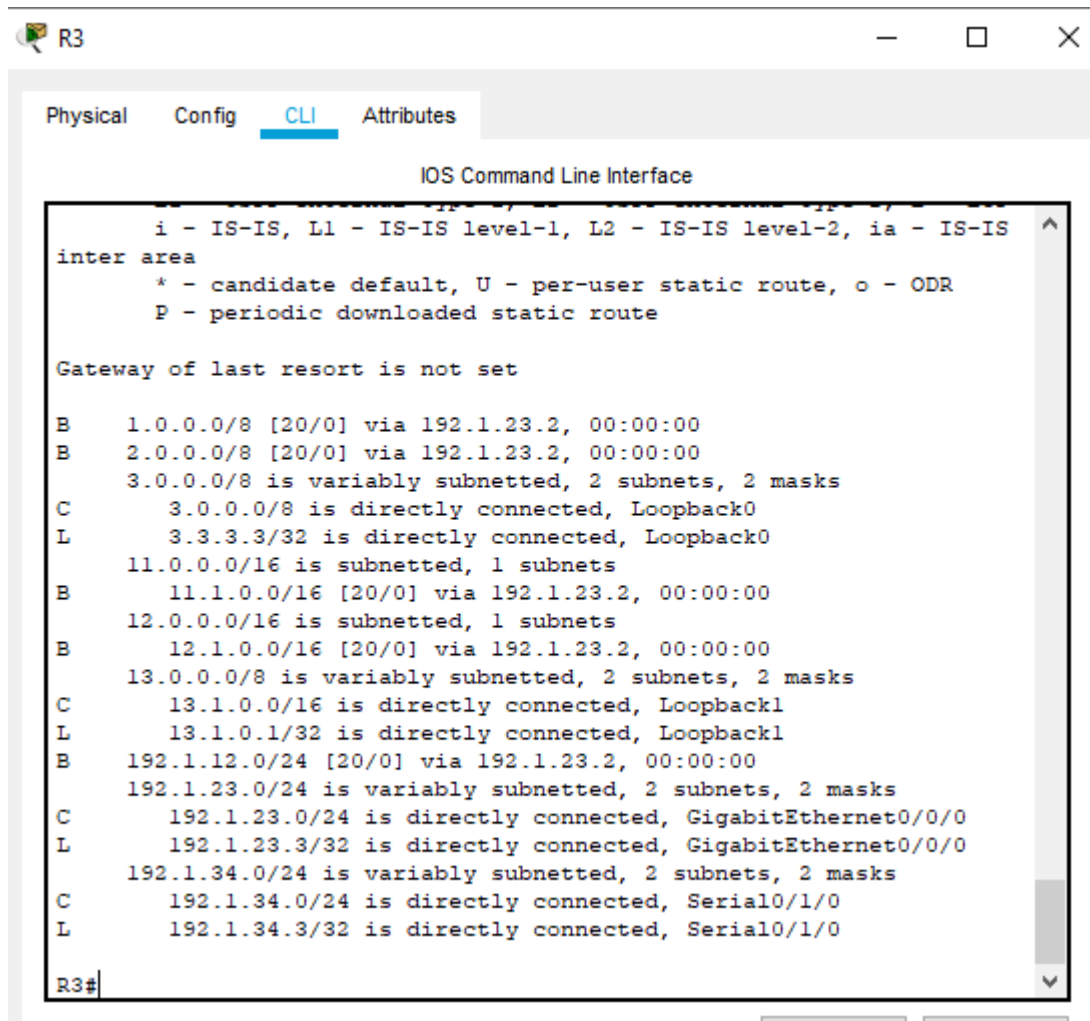
B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:00:00
     2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    2.0.0.0/8 is directly connected, Loopback0
L    2.2.2.2/32 is directly connected, Loopback0
     11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0/16 [20/0] via 192.1.12.1, 00:00:00
     12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    12.1.0.0/16 is directly connected, Loopback1
L    12.1.0.1/32 is directly connected, Loopback1
     192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.12.0/24 is directly connected, Serial10/1/0
L    192.1.12.2/32 is directly connected, Serial10/1/0
     192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, GigabitEthernet0/0/0
L    192.1.23.2/32 is directly connected, GigabitEthernet0/0/0

R2#
```

Figura 3 Tabla enrutamiento R2

2. Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en AS2 y R3 debería estar en AS3. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 44.44.44.44. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

```
R3(config)#router bgp 3
R3(config-router)#bg router-id 44.44.44.44
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#network 192.1.34.0 mask 255.255.255.0
R3(config-router)#network 192.1.23.0 mask 255.255.255.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3(config-router)#network 3.0.0.0 mask 255.0.0.0
```



```
IOS Command Line Interface

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
     3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    3.0.0.0/8 is directly connected, Loopback0
L    3.3.3.3/32 is directly connected, Loopback0
     11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0/16 [20/0] via 192.1.23.2, 00:00:00
     12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0/16 [20/0] via 192.1.23.2, 00:00:00
     13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    13.1.0.0/16 is directly connected, Loopback1
L    13.1.0.1/32 is directly connected, Loopback1
B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:00:00
     192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, GigabitEthernet0/0/0
L    192.1.23.3/32 is directly connected, GigabitEthernet0/0/0
     192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial0/1/0
L    192.1.34.3/32 is directly connected, Serial0/1/0

R3#
```

Figura 4 Tabla enrutamiento R3

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.

```
R4(config)#rout bgp 4
R4(config-router)#bg router-id 66.66.66.66
R4(config-router)#neighbor 192.1.34.3 remote-as 3
R4(config-router)#network 192.1.34.0 mask 255.255.255.0
R4(config-router)#network 14.1.0.0 mask 255.255.0.0
R4(config-router)#network 4.0.0.0 mask 255.0.0.0
```

```
R4#sho ip rou
R4#sho ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.34.3, 00:00:00
B    2.0.0.0/8 [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
     4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    4.0.0.0/8 is directly connected, Loopback0
L    4.4.4.4/32 is directly connected, Loopback0
     11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0/16 [20/0] via 192.1.34.3, 00:00:00
     12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0/16 [20/0] via 192.1.34.3, 00:00:00
     13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0/16 [20/0] via 192.1.34.3, 00:00:00
     14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    14.1.0.0/16 is directly connected, Loopback1
L    14.1.0.1/32 is directly connected, Loopback1
B    192.1.12.0/24 [20/0] via 192.1.34.3, 00:00:00
B    192.1.23.0/24 [20/0] via 192.1.34.3, 00:00:00
     192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial0/1/0
L    192.1.34.4/32 is directly connected, Serial0/1/0
```

Figura 5 Tabla enrutamiento R4

ESCENARIO 2

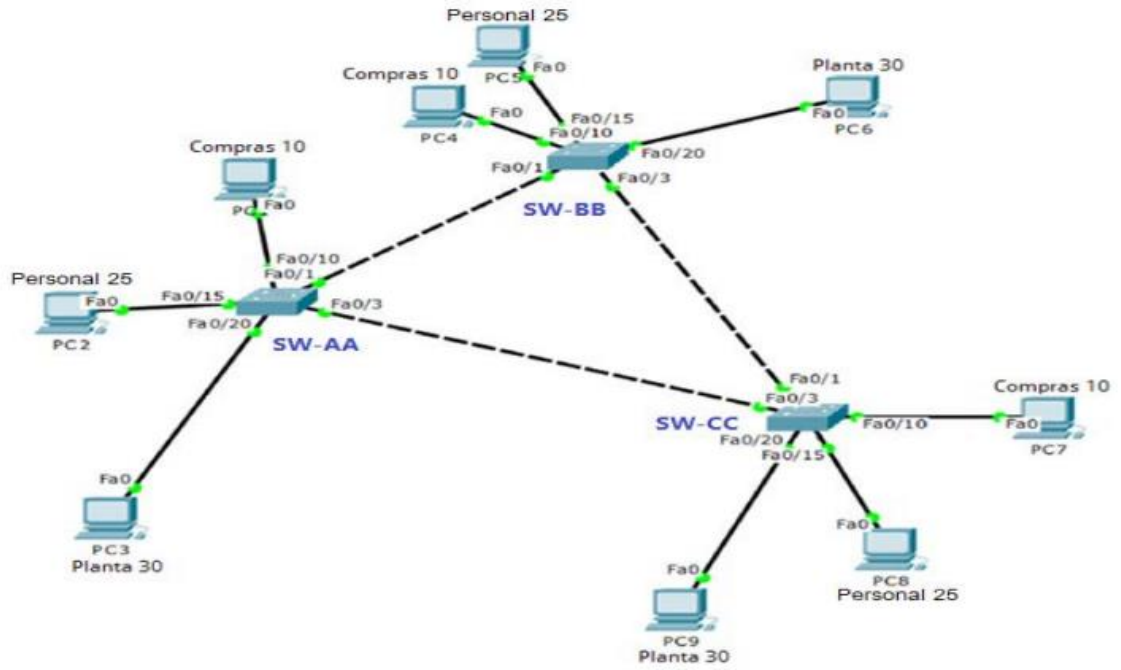


Figura 6 Escenario 2

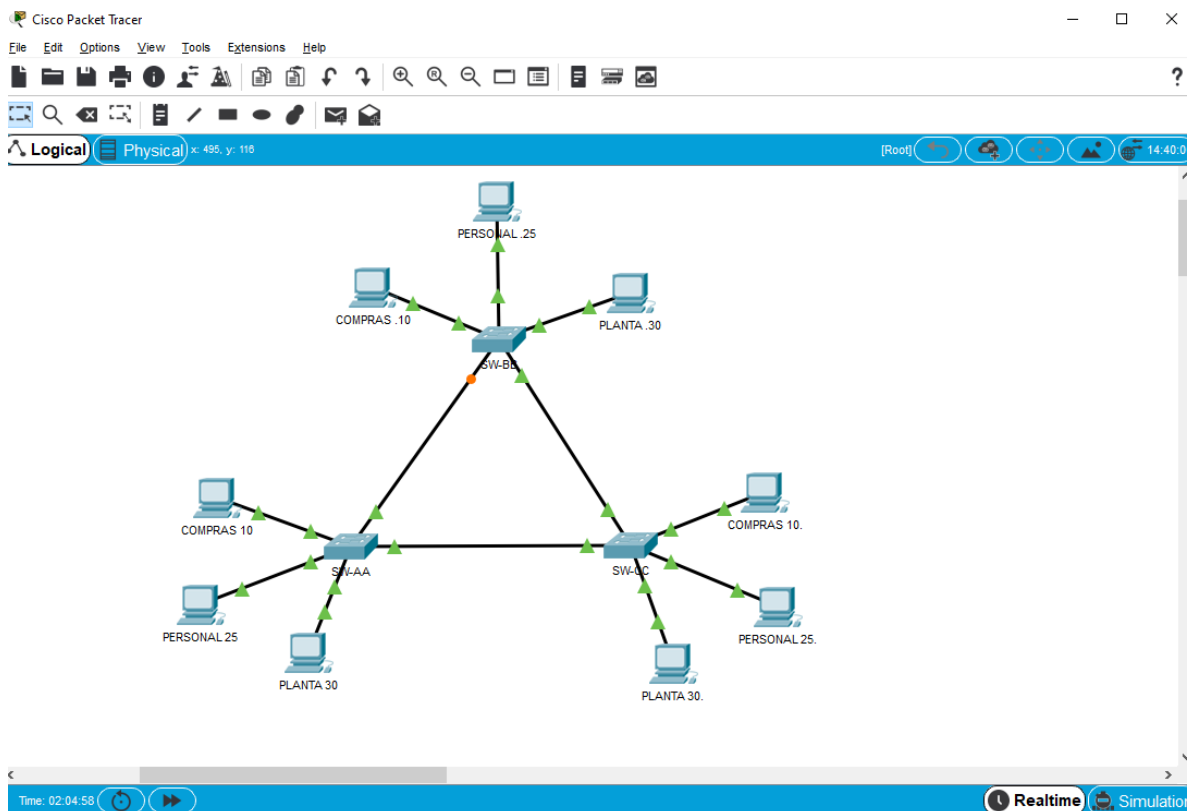


Figura 7 Simulación Escenario 2

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 VPT llamado CCNP y usando la contraseña cisco.

Se utiliza el Software propietario de Cisco **Packet tracert**

Configuración básica en todos los conmutadores

```
Switch(config)#no ip domain-lookup
Switch(config)#line con 0
Switch(config-line)#loggi syn
Switch(config-line)#passw cisco
```

SW-AA

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

SW-BB

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

SW-CC

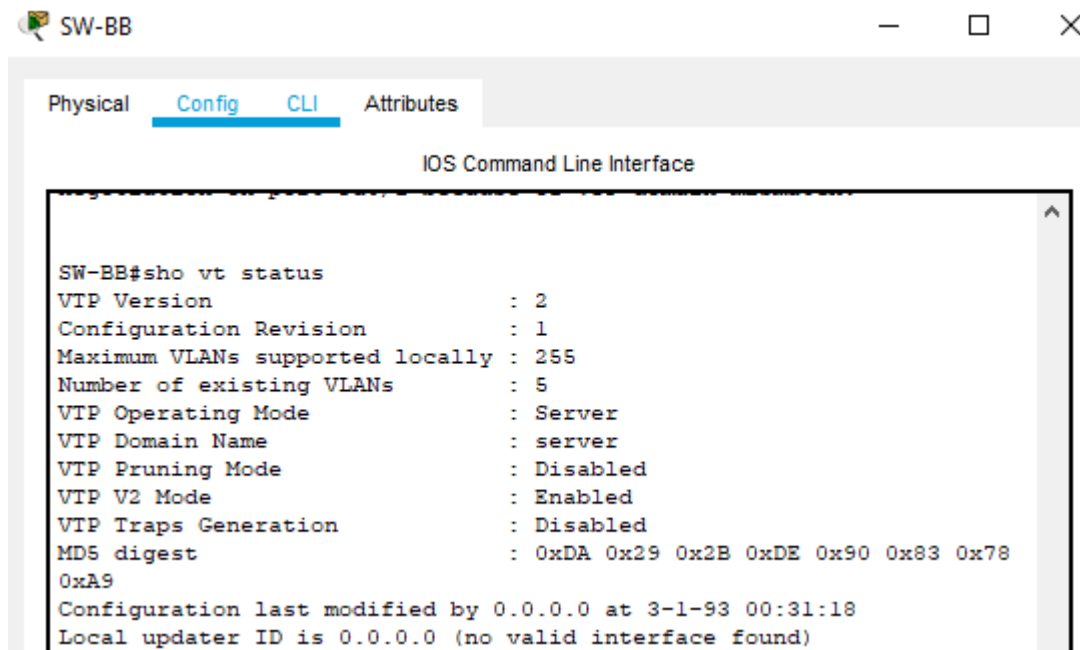
```
Switch(config)#hostname SW-AA
SW-CC(config)#vtp domain CCNP
SW-CC(config)#vtp mode client
SW-CC(config)#vtp version 2
SW-CC(config)#vtp password cisco
SW-CC(config)#exit
```

2. Verifique las configuraciones mediante el comando show vtp status

```
SW-AA#show vtp status
SW-BB#show vtp status
SW-CC#show vtp status
```

```
SW-AA>en
SW-AA#show vtp
SW-AA#show vtp st
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#
```

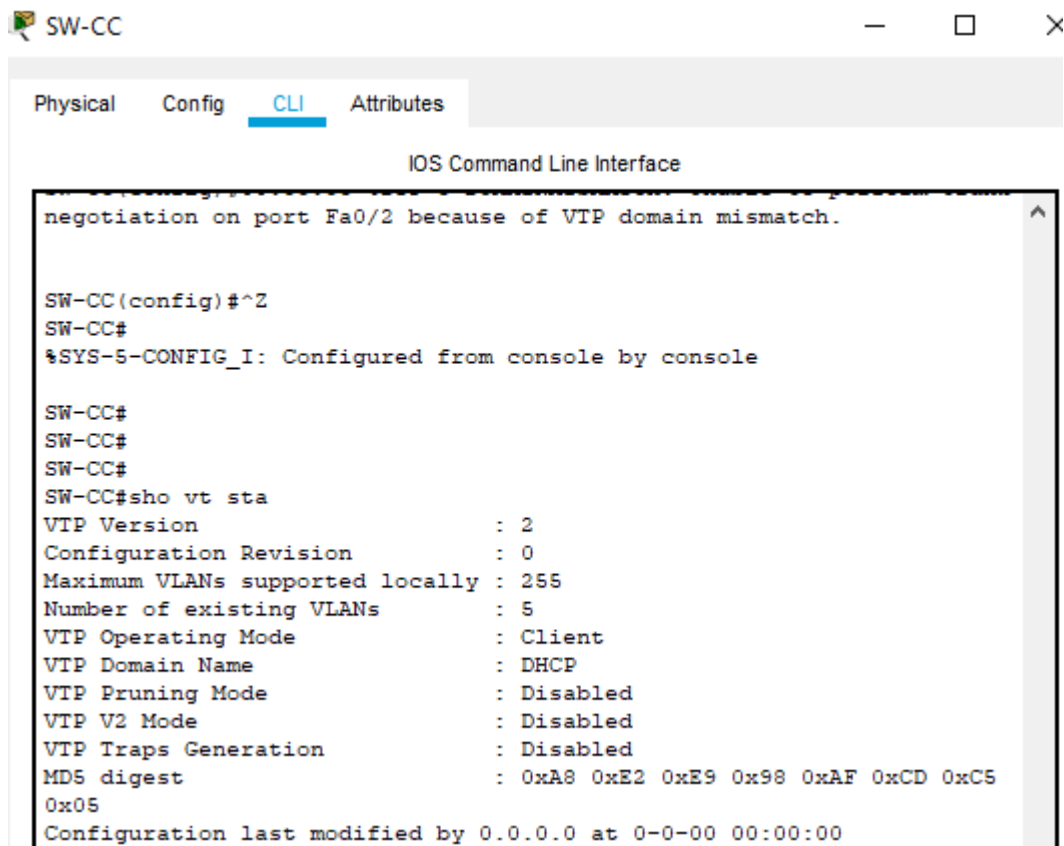
Figura 8 Show VTP en SW-AA



The screenshot shows a window titled "SW-BB" with a tabbed interface. The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following VTP status:

```
SW-BB#sho vt status
VTP Version                : 2
Configuration Revision     : 1
Maximum VLANs supported locally : 255
Number of existing VLANs   : 5
VTP Operating Mode         : Server
VTP Domain Name            : server
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Enabled
VTP Traps Generation       : Disabled
MD5 digest                  : 0xDA 0x29 0x2B 0xDE 0x90 0x83 0x78
0xA9
Configuration last modified by 0.0.0.0 at 3-1-93 00:31:18
Local updater ID is 0.0.0.0 (no valid interface found)
```

Figura 9 Show VTP status en SW-BB



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". The terminal output shows a message about VTP domain mismatch on port Fa0/2, followed by the user pressing Ctrl-Z to exit configuration mode. The user then enters the command "show vtp status", which displays the following VTP configuration details:

```
negotiation on port Fa0/2 because of VTP domain mismatch.

SW-CC(config)^Z
SW-CC#
%SYS-5-CONFIG_I: Configured from console by console

SW-CC#
SW-CC#
SW-CC#
SW-CC#sho vt sta
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 255
Number of existing VLANs   : 5
VTP Operating Mode        : Client
VTP Domain Name           : DHCP
VTP Pruning Mode          : Disabled
VTP V2 Mode               : Disabled
VTP Traps Generation      : Disabled
MDS digest                 : 0xA8 0xE2 0xE9 0x98 0xAF 0xCD 0xC5
0x05
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Figura 10 Show VTP status en SW-CC

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

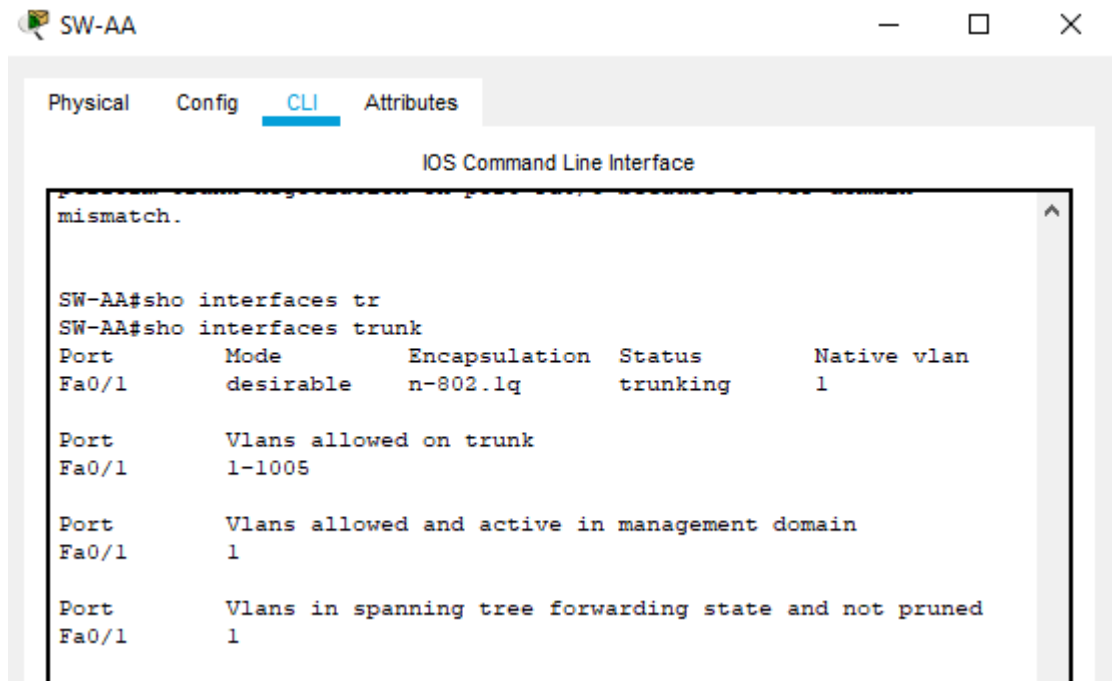
Configuración en SW-AA

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

Configuración en SW-BB

```
SW-BB(config)#int f 0/1
SW-BB(config-if)#switchport mode trunk
SW-BB(config-if)#
```


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



The screenshot shows a terminal window titled "SW-AA" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows a "mismatch." message followed by the command "SW-AA#sho interfaces tr". Below this, the command "SW-AA#sho interfaces trunk" is executed, resulting in a table of trunking information for Fa0/1.

```
mismatch.  
  
SW-AA#sho interfaces tr  
SW-AA#sho 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
```

Figura 11 Show interface trunk en SW-AA

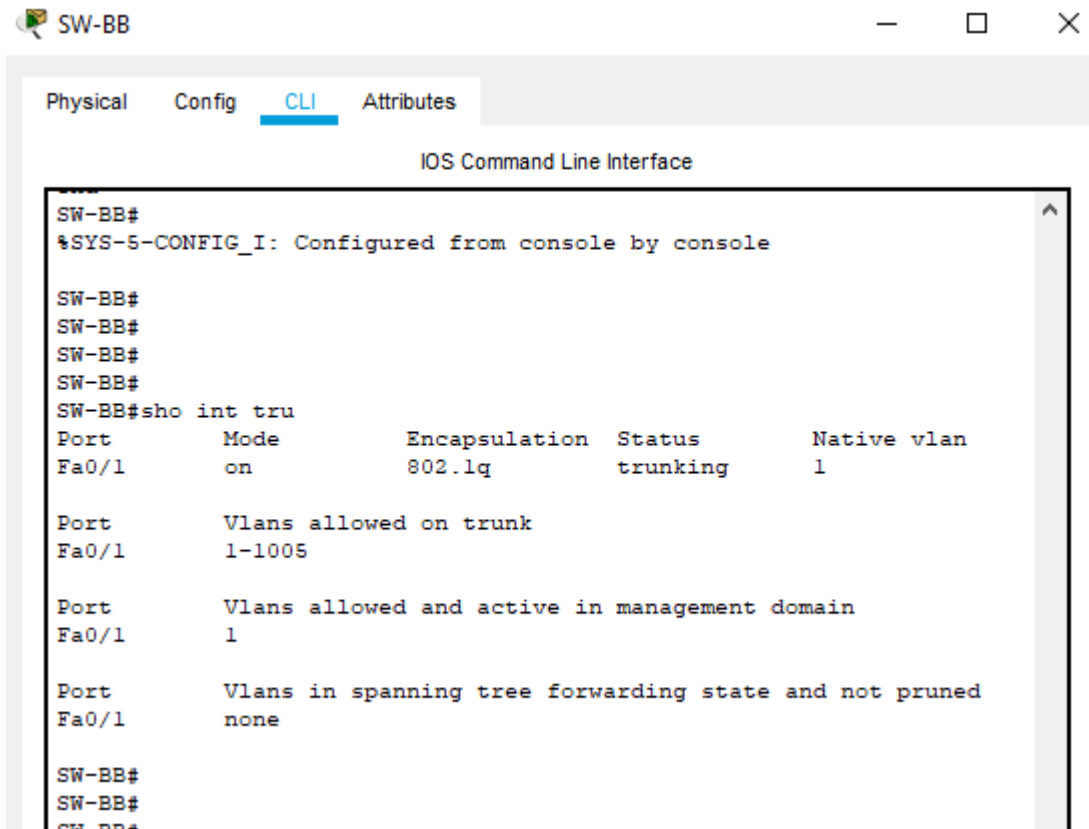


Figura 12 Show interface trunk en SW-BB

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

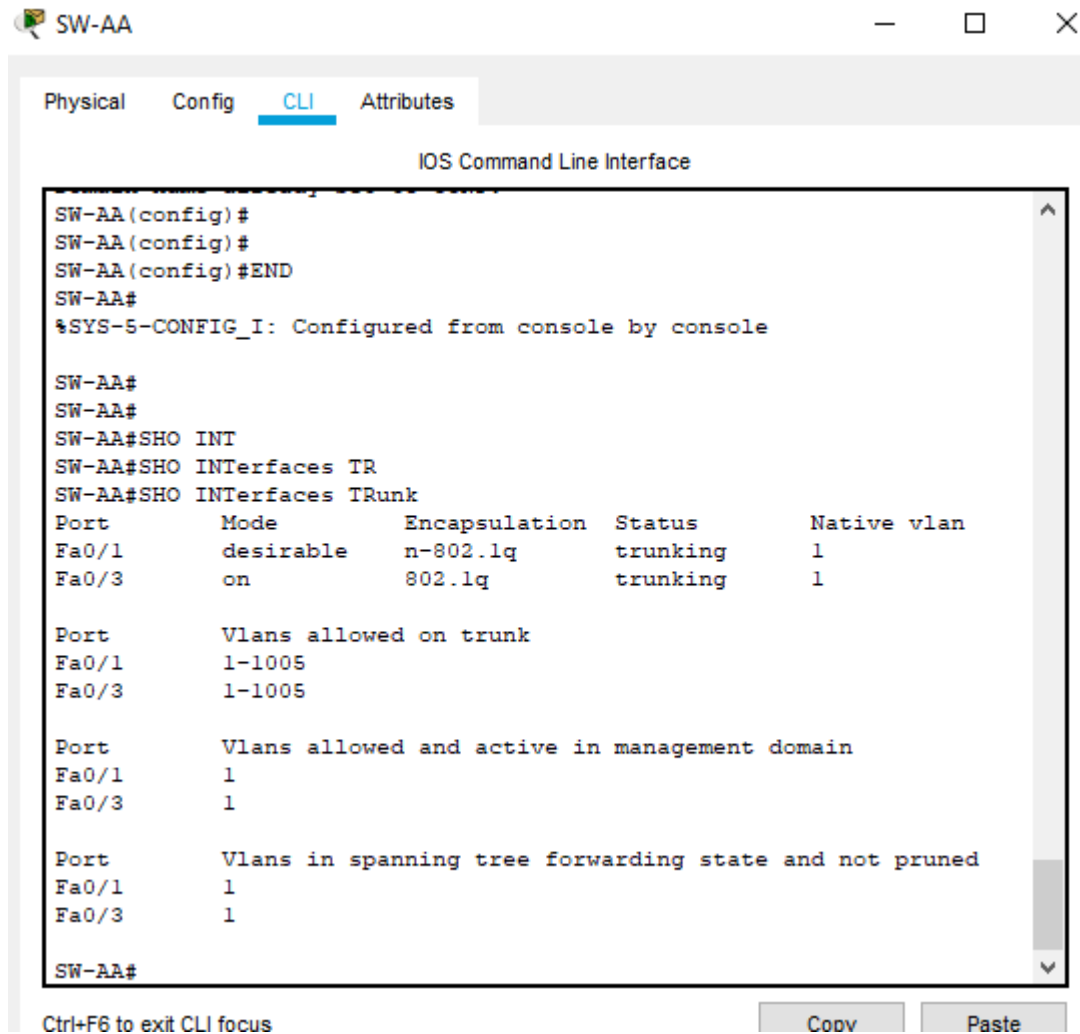
Configuración en SW-AA

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

Configuración en SW-CC

```
SW-CC(config)#int f 0/3
SW-CC(config-if)#switchport mode trunk
SW-CC(config-if)#
```

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



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

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

SW-AA#
SW-AA#
SW-AA#SHO INT
SW-AA#SHO INTERfaces TR
SW-AA#SHO 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#
```

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

Figura 13 Show interface trunk en SW-AA

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

Configuración en SW-BB

```
SW-AA(config)#interface fastEthernet 0/2  
SW-AA(config-if)#switchport mode trunk  
SW-AA(config-if)#switchport mode dynamic desirable
```

Configuración en SW-CC

```
SW-CC(config)#int f 0/2  
SW-CC(config-if)#switchport mode trunk  
SW-CC(config-if)#
```

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

Configuración SW-AA

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

Configuración SW-BB

```
SW-BB(config)#vlan 10
SW-BB(config-vlan)#na
SW-BB(config-vlan)#name compras
SW-BB(config-vlan)#vl
SW-BB(config-vlan)#vl 25
SW-BB(config-vlan)#name personal
SW-BB(config-vlan)#vl 30
SW-BB(config-vlan)#nam planta
SW-BB(config-vlan)#vl 99
SW-BB(config-vlan)#nam admon
```

9. Verifique que las VLANs han sido agregadas correctamente

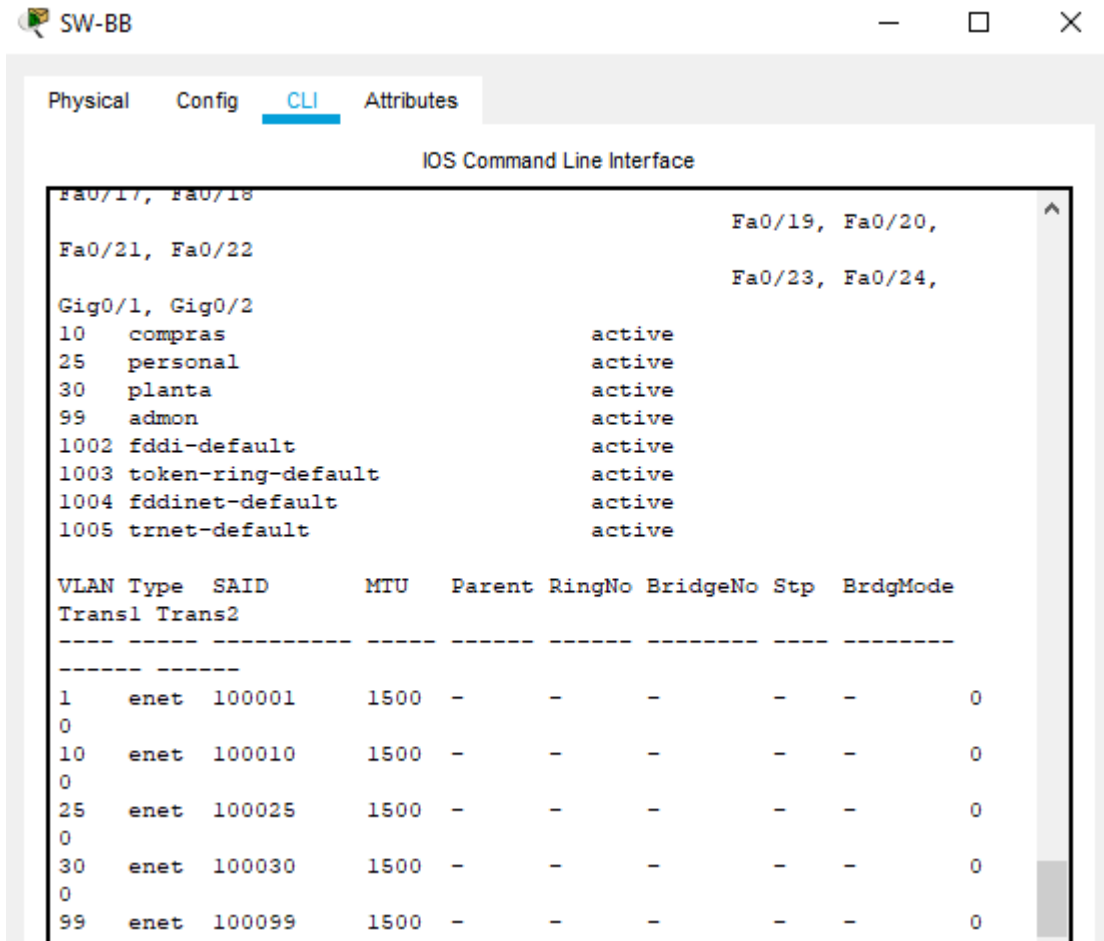


Figura 14 Comando Show Vlan en el SW-BB

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

Tabla 5. Asignación direcciones IP a las VLAN

Interfaz	VLAN	Direcciones de IP en los PCs
Fa 0/10	10	190.108.10.X / 24
Fa 0/15	25	190.108.20.X / 24
Fa 0/20	30	190.108.30.X / 24

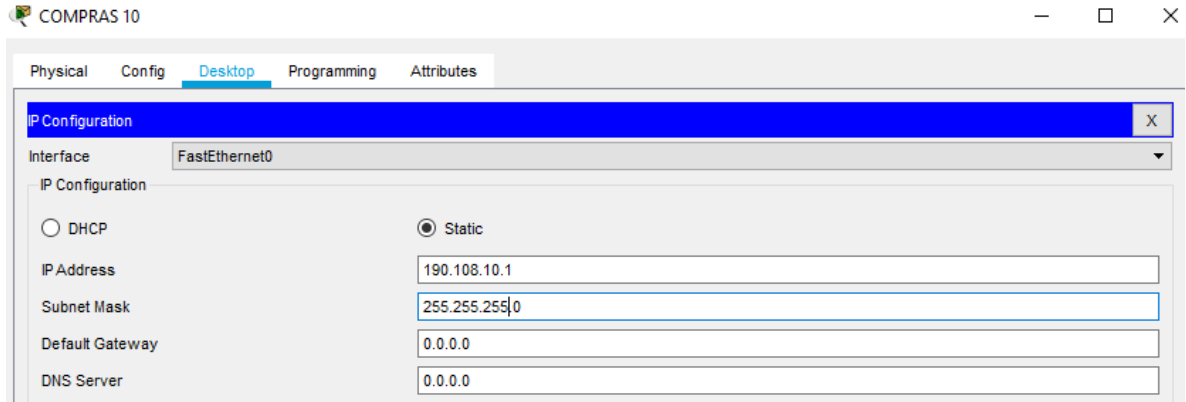


Figura 15 Configuración equipo 1 SW-AA

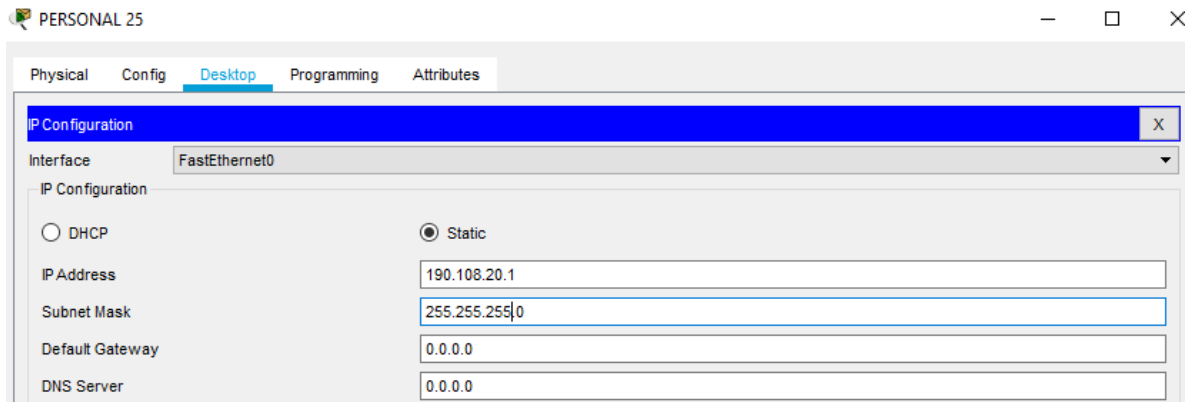


Figura 16 Configuración equipo 2 SW-AA

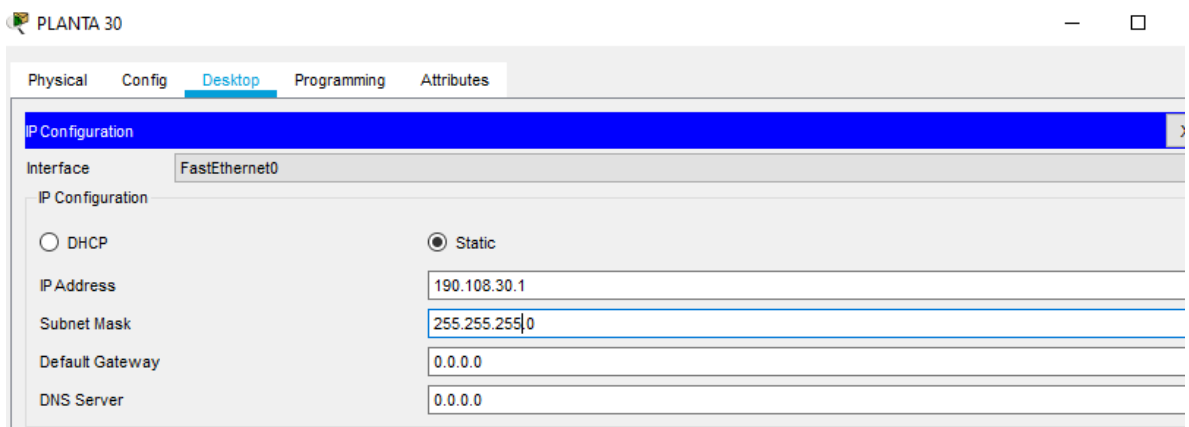


Figura 17 Configuración equipo 3 SW-AA

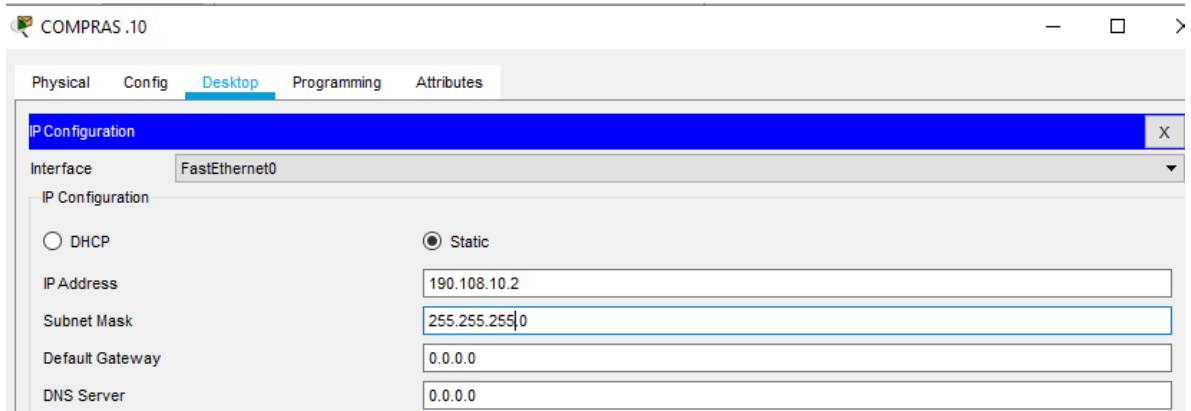


Figura 18 Configuración equipo 1 SW-BB

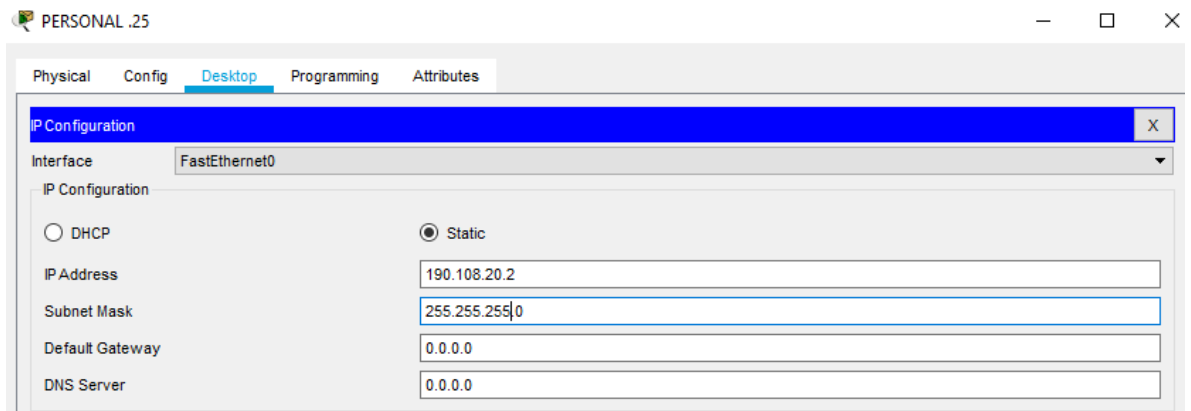


Figura 19 Configuración equipo 2 SW-BB

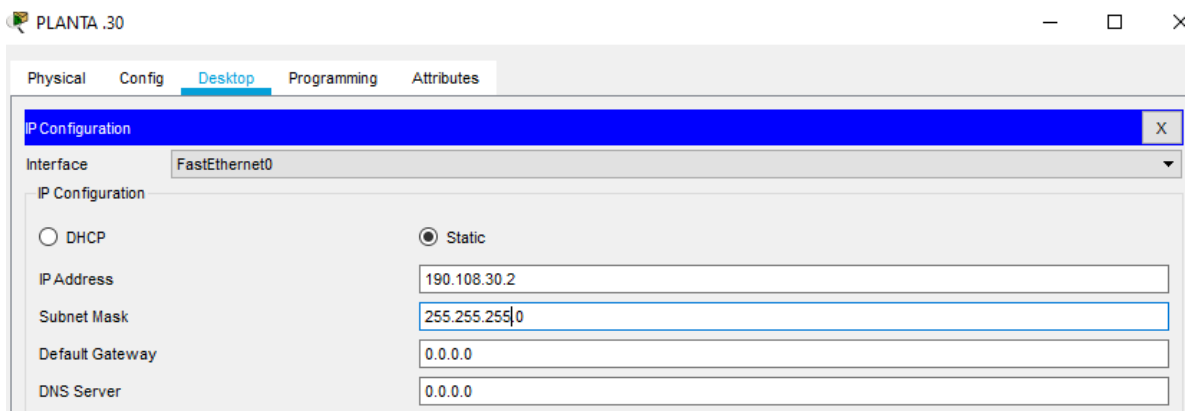


Figura 20 Configuración equipo 3 SW-BB

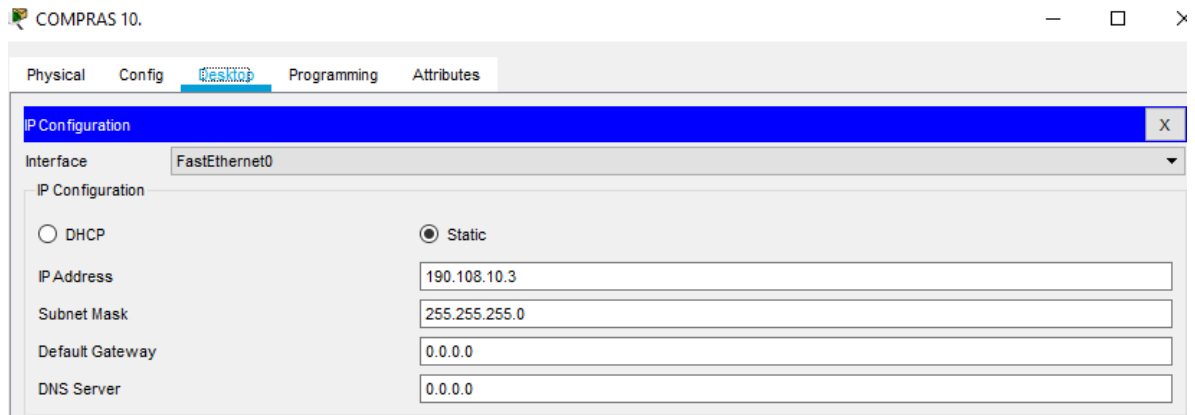


Figura 21 Configuración equipo 1 SW-CC

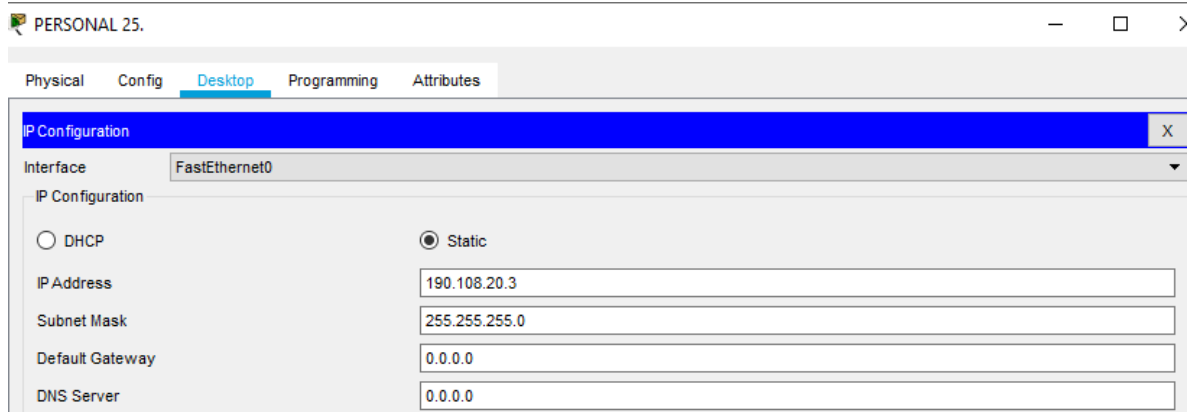


Figura 22 Configuración equipo 2 SW-CC

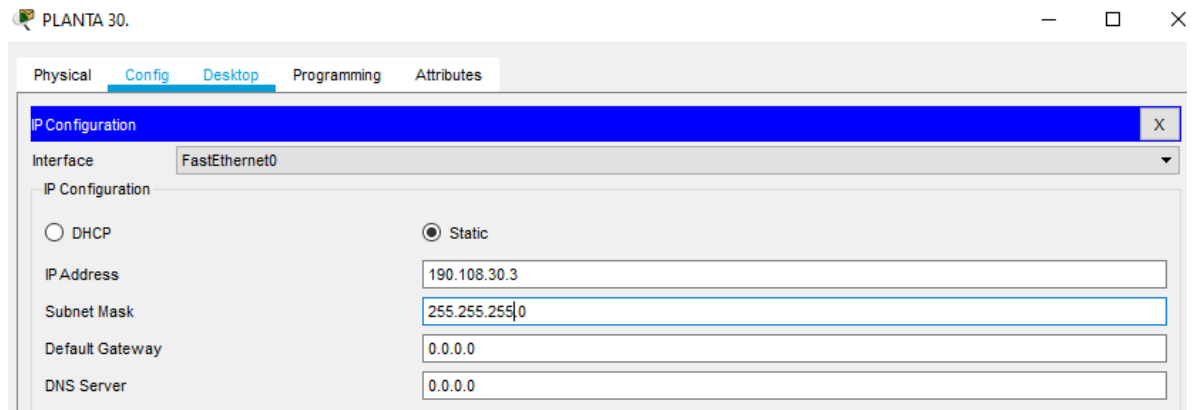


Figura 23 Configuración equipo 3 SW-CC

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

12.. Repita el procedimiento para los puertos F0/15 y F0/20 en SW-AA, SW-BB y SW-CC. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

Configuración VLANs en SW-AA

```
SW-AA(config)#int fa 0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#int fa 0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#int fa 0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
```

Configuración VLANs en SW-BB

```
SW-BB(config)#int fa 0/1
SW-BB(config-if)#int fa 0/10
SW-BB(config-if)#sw
SW-BB(config-if)#switchport mode acc
SW-BB(config-if)#swit ac vl 10
SW-BB(config-if)#int fa 0/15
SW-BB(config-if)#switchport mode acc
SW-BB(config-if)#swit ac vl 25
SW-BB(config-if)#int fa 0/20
SW-BB(config-if)#switchport mode acc
SW-BB(config-if)#swit ac vl 30
```

Configuración VLANs en SW-BB

```
SW-CC(config-if)#int fa0/10
SW-CC(config-if)#sw mod acc
SW-CC(config-if)#sw ac vl 10
SW-CC(config-if)#int fa0/15
SW-CC(config-if)#sw mod acc
SW-CC(config-if)#sw ac vl 25
SW-CC(config-if)#int fa0/20
SW-CC(config-if)#sw mod acc
SW-CC(config-if)#sw ac vl 30
```

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

Tabla 6. Asignación direcciones IP de los conmutadores

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

Configuración en los SW-AA

```
SW-AA(config-if)#int vl 99
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
SW-AA(config-if)#no shutdown
SW-AA(config-if)#
```

Configuración en los SW-BB

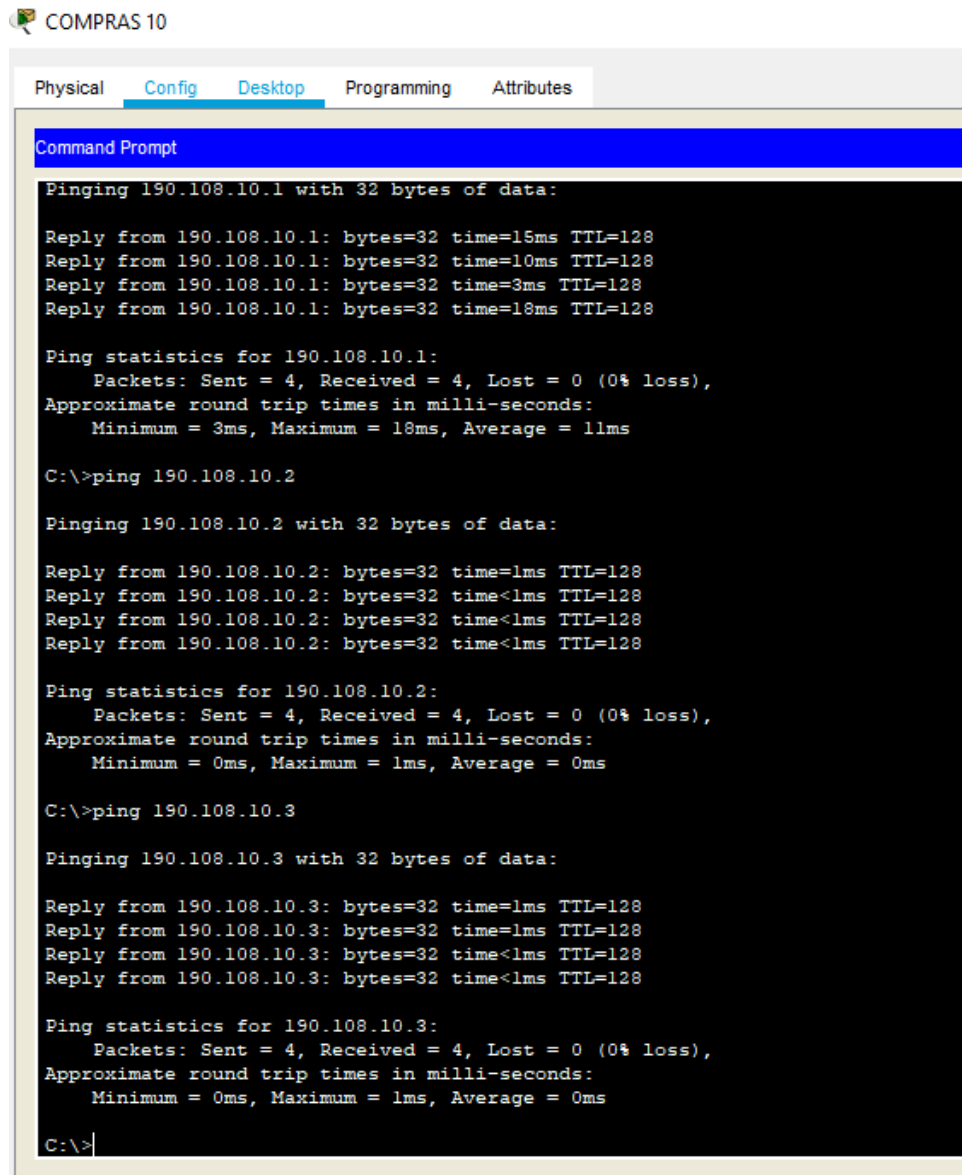
```
SW-BB(config-if)#int vl 99
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
SW-BB(config-if)#no shutdown
SW-BB(config-if)#
```

Configuración en los SW-CC

```
SW-AA(config-if)#int vl 99
SW-AA(config-if)#ip address 190.108.99.3 255.255.255.0
SW-AA(config-if)#no shutdown
SW-AA(config-if)#
```

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

Ping de PC compras SW-AA hacía los otros de compras



```
COMPRAS 10
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 190.108.10.1 with 32 bytes of data:
Reply from 190.108.10.1: bytes=32 time=15ms TTL=128
Reply from 190.108.10.1: bytes=32 time=10ms TTL=128
Reply from 190.108.10.1: bytes=32 time=3ms TTL=128
Reply from 190.108.10.1: bytes=32 time=18ms TTL=128

Ping statistics for 190.108.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 18ms, Average = 11ms

C:\>ping 190.108.10.2

Pinging 190.108.10.2 with 32 bytes of data:

Reply from 190.108.10.2: bytes=32 time=1ms TTL=128
Reply from 190.108.10.2: bytes=32 time<1ms TTL=128
Reply from 190.108.10.2: bytes=32 time<1ms TTL=128
Reply from 190.108.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 190.108.10.3

Pinging 190.108.10.3 with 32 bytes of data:

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

Ping statistics for 190.108.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Figura 24 Ping entre equipos VLAN 10

Ping de PC personal SW-AA hacía los otros de personal

PERSONAL 25

Physical Config **Desktop** Programming Attributes

Command Prompt

```
Pinging 190.108.20.1 with 32 bytes of data:
Reply from 190.108.20.1: bytes=32 time=4ms TTL=128
Reply from 190.108.20.1: bytes=32 time=10ms TTL=128
Reply from 190.108.20.1: bytes=32 time=1ms TTL=128
Reply from 190.108.20.1: bytes=32 time=1ms TTL=128

Ping statistics for 190.108.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 10ms, Average = 4ms

C:\>ping 190.108.20.2

Pinging 190.108.20.2 with 32 bytes of data:
Reply from 190.108.20.2: bytes=32 time<1ms TTL=128
Reply from 190.108.20.2: bytes=32 time=1ms TTL=128
Reply from 190.108.20.2: bytes=32 time<1ms TTL=128
Reply from 190.108.20.2: bytes=32 time=1ms TTL=128

Ping statistics for 190.108.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 190.108.20.3

Pinging 190.108.20.3 with 32 bytes of data:
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
Reply from 190.108.20.3: bytes=32 time=7ms 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 = 7ms, Average = 2ms

C:\>|
```

Figura 25 Ping entre equipos VLAN 25

Ping de PC planta SW-AA hacía los otros de planta

PLANTA 30

Physical Config **Desktop** Programming Attributes

```
Command Prompt

Pinging 190.108.30.1 with 32 bytes of data:

Reply from 190.108.30.1: bytes=32 time=8ms TTL=128
Reply from 190.108.30.1: bytes=32 time=5ms 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

Ping statistics for 190.108.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 8ms, Average = 4ms

C:\>ping 190.108.30.2

Pinging 190.108.30.2 with 32 bytes of data:

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

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

C:\>ping 190.108.30.3

Pinging 190.108.30.3 with 32 bytes of data:

Reply from 190.108.30.3: bytes=32 time=1ms TTL=128
Reply from 190.108.30.3: bytes=32 time<1ms TTL=128
Reply from 190.108.30.3: bytes=32 time<1ms TTL=128
Reply from 190.108.30.3: bytes=32 time=1ms TTL=128

Ping statistics for 190.108.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Figura 26 Ping entre equipos VLAN 30

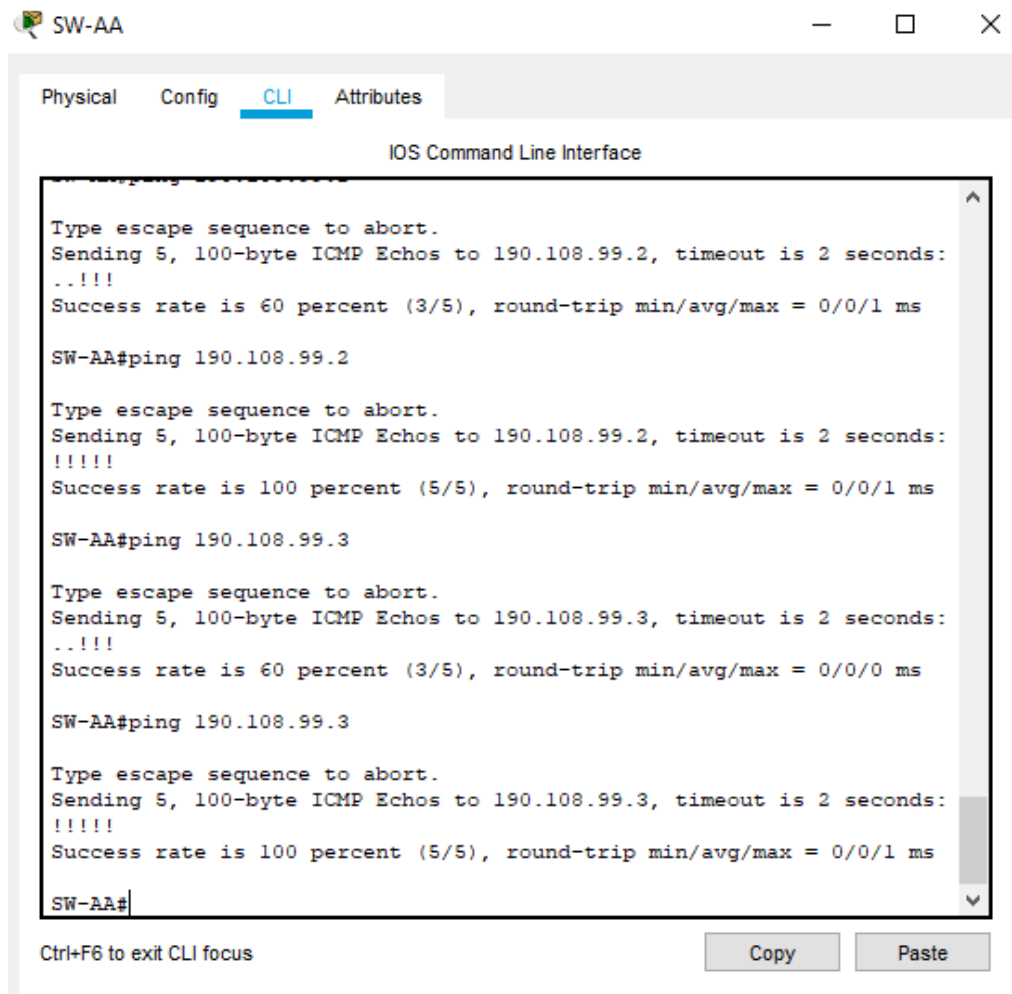
Conclusión

La prueba de conectividad ICMP es satisfactoria debido a que el protocolo VTP nos ayuda a configurar las VLAN en un dispositivo que funciona como servidor propagándolas a los dispositivos que están como clientes.

Se observa el principio de funcionamiento de las VLAN ya que aísla los dominios de Broadcast

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

Prueba ICMP entre los conmutadores SW-AA, SW-BB y SW-CC



```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
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 190.108.99.2

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

SW-AA#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-AA#ping 190.108.99.3

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

SW-AA#
```

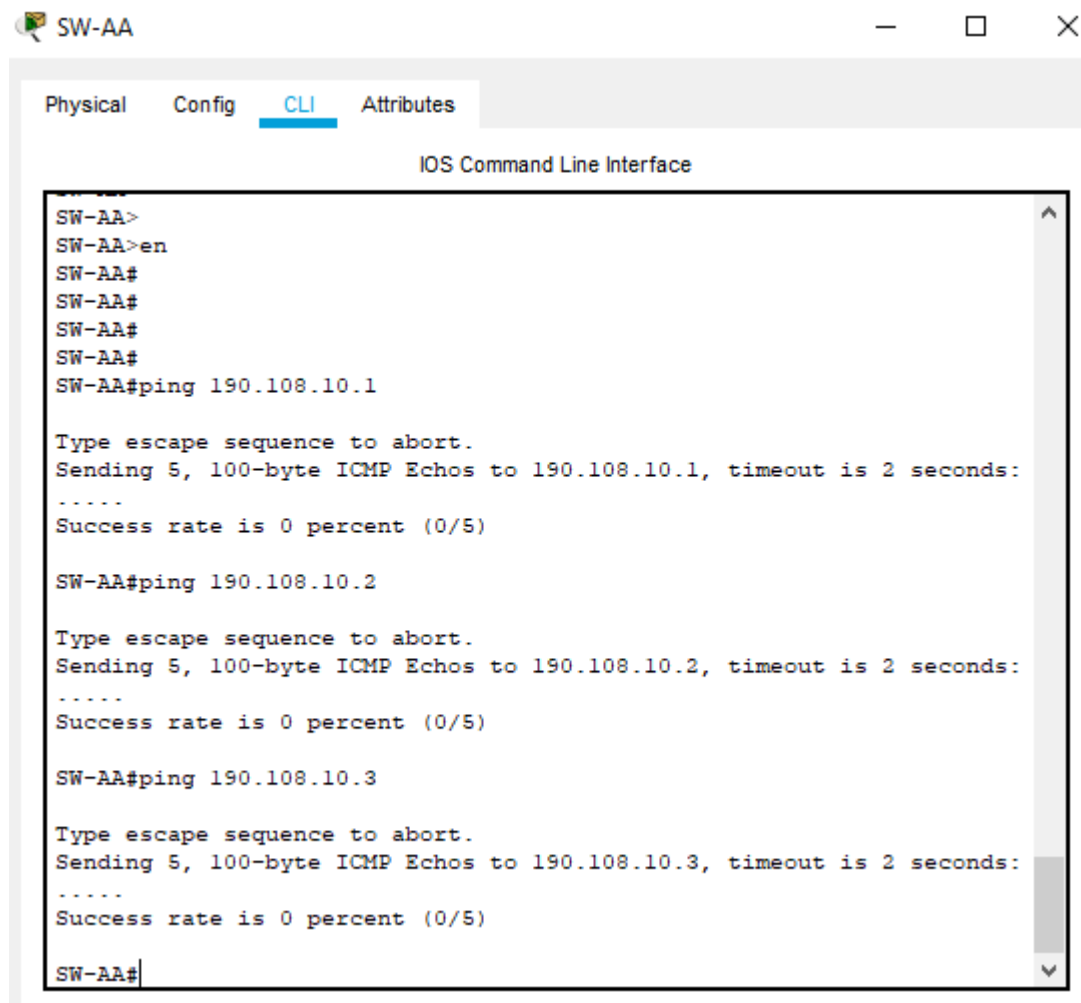
Ctrl+F6 to exit CLI focus Copy Paste

Figura 27 Ping entre los conmutadores

Conclusión: se observa que desde el SW-AA se tienen conectividad ICMP hacía los otros equipos (SW-BB y SW-CC); se aprecia que se pierden unos paquetes, ya que se necesita el calculo del protocolo ARP (Address Resolution Protocol)

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

Ping desde SW-AA hacía los PC de la VLAN 10



```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
SW-AA>
SW-AA>en
SW-AA#
SW-AA#
SW-AA#
SW-AA#ping 190.108.10.1

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

SW-AA#ping 190.108.10.2

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 190.108.10.3

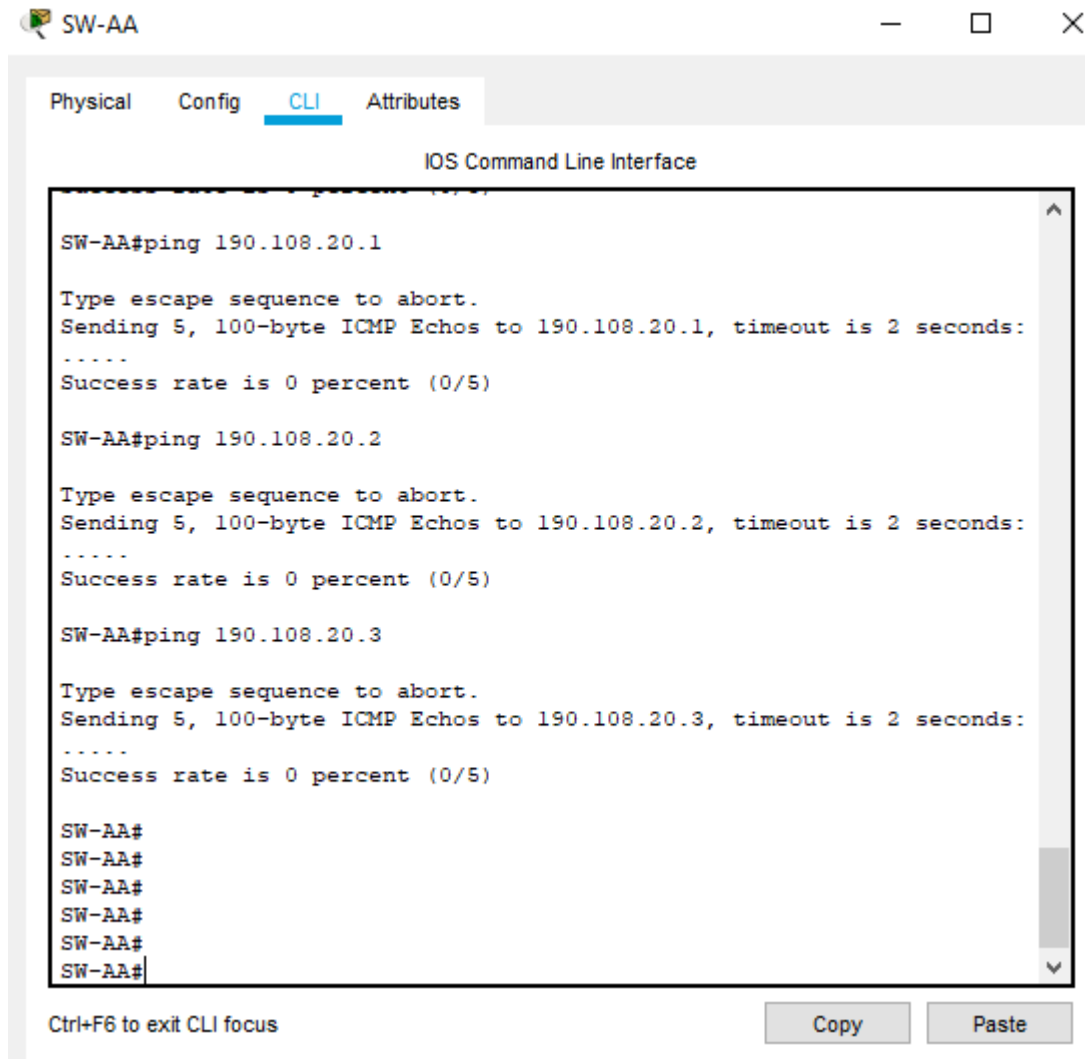
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#
```

Figura 28 Ping desde SW-AA hacía los PCs de la VLAN 10

Conclusión: no se tienen conectividad ICMP entre el SW-AA y los PC de la VLAN 10 por que esta no tiene una interfaz de capa 3 en los equipos; adicional los switches no tienen algún enrutamiento estático que direcciona los paquetes a su destino y los PC no tienen una puerta de enlace predeterminada para devolver la respuesta a la VLAN 99

Ping desde SW-AA hacia los PC de la VLAN 25



```
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 190.108.20.2
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)

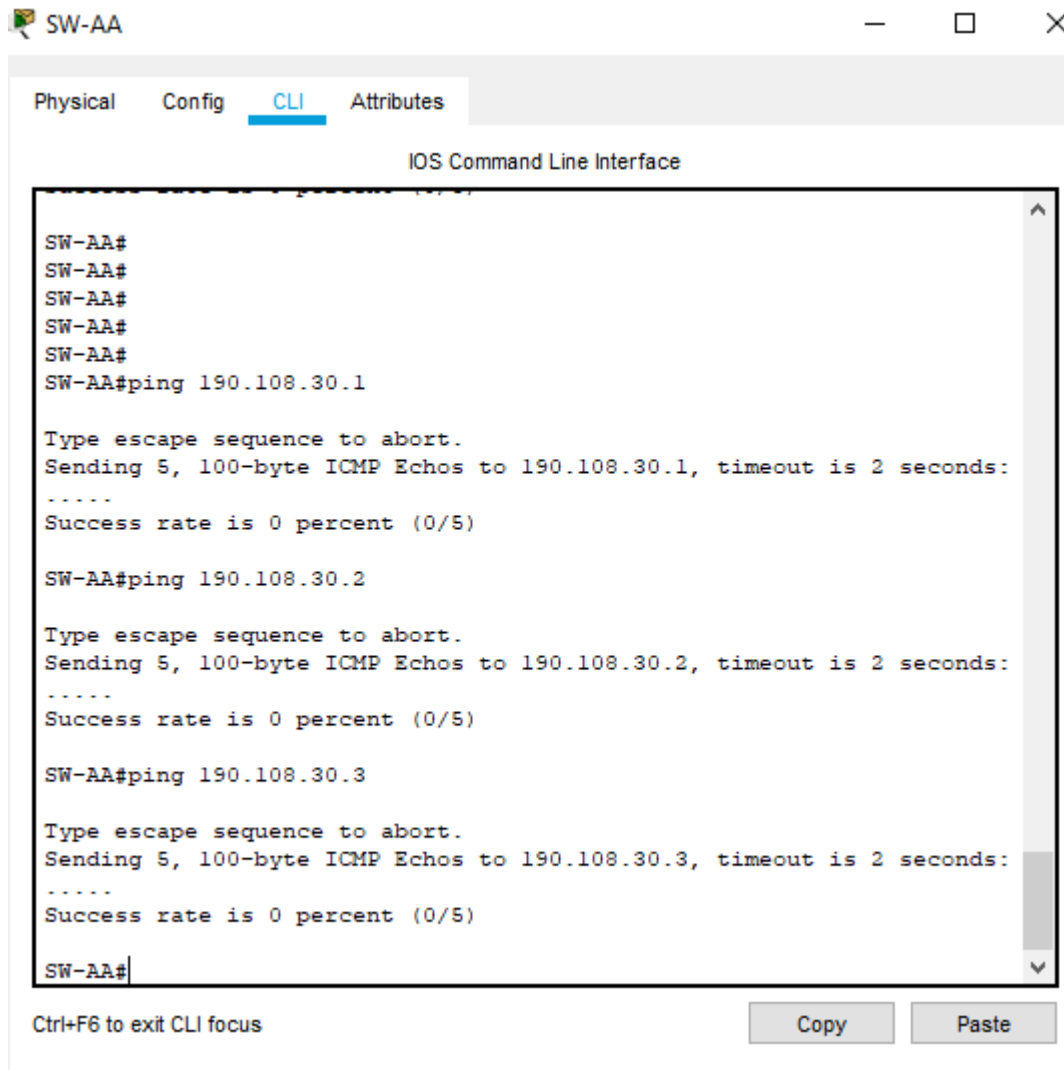
SW-AA#ping 190.108.20.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#
SW-AA#
SW-AA#
SW-AA#
SW-AA#
SW-AA#
```

Figura 29 Ping desde SW-AA hacia los PCs de la VLAN 10

Conclusión: no se tienen conectividad ICMP entre el SW-AA y los PC de la VLAN 25 porque esta no tiene una interfaz de capa 3 en los equipos; adicional los switches no tienen algún enrutamiento estático que direccionen los paquetes a su destino y los PC no tienen una puerta de enlace predeterminada para devolver la respuesta a la VLAN 99

Ping desde SW-AA hacía los PC de la VLAN 30



```
SW-AA
SW-AA#
SW-AA#
SW-AA#
SW-AA#
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 190.108.30.2

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#ping 190.108.30.3

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

SW-AA#
```

Figura 30 Ping desde SW-AA hacía los PCs de la VLAN 10

Conclusión: no se tienen conectividad ICMP entre el SW-AA y los PC de la VLAN 30 porque esta no tiene una interfaz de capa 3 en los equipos; adicional los switches no tienen algún enrutamiento estático que dirija los paquetes a su destino y los PC no tienen una puerta de enlace predeterminada para devolver la respuesta a la VLAN 99

CONCLUSIONES

La refuerzan y apersonan los principios de enrutamiento y conmutación enfocados a simulaciones de escenarios que se presentaron en diferentes empresas prestadoras de servicio de internet (ISPs) como empresas corporativas de usuarios finales.

Se comprende el funcionamiento y la aplicación del modelo OSI, especialmente en las capas de enlace (Capa 2) y de red (capa 3), protocolos que incluyen y su funcionamiento práctico.

Se conocen los protocolos propietarios de Cisco, y su comparación con los protocolos globales que se tienen en la industria.

BIBLIOGRAFÍA

Compatible Systems Setup Guides: BGP Configuration Guide. . {En línea}. {22 Enero de 2007} Disponible en <https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/17612-bgp.html>

Ejemplo de Configuración de VLANs en Controladores de LAN Inalámbrica. . {En línea}. {10 Julio de 2019} Disponible en https://www.cisco.com/c/es_mx/support/docs/wireless-mobility/wireless-vlan/68100-wlan-controllers-vlans.html

How to configure VLAN Trunk Protocol. {En línea}. {22 Enero de 2007} Disponible en <https://www.beaming.co.uk/knowledge-base/configuring-basic-vtp-on-cisco-switches>

MAECHA DIAZ. mauricio. CARREÑO, Angela, GUTIERREZ MEDINA. Diego, MORA, Julián. Diplomado de profundización CISCO CCNP {En línea}. {30 noviembre de 2017} Disponible en <https://repository.unad.edu.co/handle/10596/17864?mode=full>