

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DUVÁN FELIPE SÁNCHEZ FLÓREZ

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

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DUVÁN FELIPE SÁNCHEZ FLÓREZ

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 – ECBTI
INGENIERÍA ELECTRÓNICA
MEDELLÍN
2020

NOTA DE ACEPTACIÓN

Firma del presidente del jurado

Firma del Jurado

Firma del Jurado

MEDELLÍN, 22 de mayo de 2020

AGRADECIMIENTOS

Este trabajo se realizó gracias al trabajo y empeño personal, siempre con la intención de crecer y desarrollar hábitos para crecer profesionalmente. A mis compañeros de grupo colaborativo y al asesoramiento de la Universidad Nacional Abierta y a Distancia mediante bajo la dirección del MSc. Gerardo Granados Acuña.

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	3
CONCLUSIONES	22
BIBLIOGRAFÍA.....	23

LISTA DE TABLAS

Tabla 1. Interfaces Loopback para crear R1 -----	12
Tabla 2. Interfaces Loopback para crear R2 -----	12
Tabla 3. Interfaces Loopback para crear R3 -----	13
Tabla 4. Interfaces Loopback para crear R4 -----	13
Tabla 5. Direcciones IP de los PCs -----	11
Tabla 6. Configuración IP en los PCs-----	11
Tabla 7. Direcciones IP en los Switches -----	13

LISTA DE FIGURAS

Figura 1. Escenario 1 -----	11
Figura 2. Simulación de escenario 1 -----	11
Figura 3. Simulación de escenario 1 -----	12
Figura 4. Tabla de enrutamiento R1 -----	16
Figura 5. Tabla de enrutamiento R2 -----	17
Figura 6. Tabla de enrutamiento R3 -----	18
Figura 7. Tabla de enrutamiento R4 -----	19
Figura 8. Escenario 2-----	3
Figura 9. Simulación de escenario 2-----	4
Figura 10. VTP en SW-AA -----	6
Figura 11. VTP en SW-BB -----	6
Figura 12. VTP en SW--CC -----	7
Figura 13. Comando Show interfaces trunk en SW-AA -----	8
Figura 14. Comando Show interfaces trunk en SW-AA -----	9
Figura 15. Comando show vlan en SW-BB-----	10
Figura 16. Ping PC1 compras 10 -----	14
Figura 17. Ping PC3 Planta 30 -----	15
Figura 18. Ping desde SW-AA-----	16
Figura 19. Ping desde SW-BB-----	17
Figura 20. Ping desde SW-CC -----	18
Figura 21. Ping desde SW-AA a PC -----	19
Figura 22. Ping desde SW-BB a PC -----	20
Figura 23. Ping desde SW-CC a PC-----	21

GLOSARIO

Ciente–Servidor: Es una forma de dividir y especializar programas y equipos de cómputo a fin de que la tarea que cada uno de ellos realizaba se efectuó con la mayor eficiencia y permita simplificarlas. En esta arquitectura la capacidad de proceso esta repartida entre el servidor y los clientes.

Enrutador: Dispositivo hardware o software de interconexión de redes de computadores que opera en la capa tres del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

Interfaz: Punto, área, o la superficie a lo largo de la cual dos cosas de naturaleza distinta convergen. Cualquier medio que permita la interconexión de dos procesos diferenciados con un único propósito común. Son los medios utilizados para la conexión de un computador son el medio de transporte de la red. Puede ser un módem, una tarjeta de red, un puerto serie, enlace infrarrojo, un conexión inalámbrica, etc.

Switch: Dispositivo de interconexión de computadores que opera en la capa 2 del modelo OSI. Interconecta dos o más segmentos de red, pasando datos de un segmento a otro, de acuerdo con la dirección de destino de los datagramas en la red. Los switches se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola.

VLAN: Es la agrupación de puertos denominada red de área local virtual. Los grupos de puertos (VLAN) pueden considerarse un segmento LAN individual. Las VLAN también se describen como dominios de difusión.

VTP Server: Configuración que permite crear, modificar y eliminar una VLAN y especificar otros parámetros de configuración, para todo el dominio VTP. Los servidores VTP anuncian su configuración de VLAN a otros switches en el mismo dominio VTP y sincronizan su configuración de VLAN con otros switches basados en anuncios.

RESUMEN

El informe a presentar consta de la solución a las actividades evaluativas del Diplomado de Profundización CCNP, para optar por el título de Ingeniero Electrónico, donde inicialmente se debe configurar un protocolo de enrutamiento avanzado, llamado EBG (Protocolo de puerta de enlace de frontera) con el fin de permitir identificación, comunicación y redundancia entre redes y routers vecinos.

En cambio para la segunda parte se trabaja con una red bajo el dominio VTP, también llamado dominio de administración VLAN, el cual tiene la intención de configurar Switches que tengan la misma responsabilidad administrativa y que compartan el mismo nombre de dominio VTP. Es propiedad de CISCO y tiene la capacidad de administrar todas las VLANs en un solo dispositivo de conmutación.

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

ABSTRACT

The report to be presented consists of the solution to the evaluation activities of the CCNP Deepening Diploma, to choose the title of Electronic Engineer, where an advanced routing protocol, called EBG (Border Gateway Protocol) must initially be configured with in order to allow identification, communication and redundancy between neighboring networks and routers.

Instead, for the second part, we work with a network under the VTP domain, also called the VLAN administration domain, which has the intention of configuring switches that have the same administrative responsibility and that share the same VTP domain name. It is owned by CISCO and has the ability to manage all VLANs on a single switching device.

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

INTRODUCCIÓN

A continuación se presenta la solución del trabajo denominado “Prueba de habilidades prácticas”, el cual forma parte de las actividades evaluativas del Diplomado de Profundización CCNP, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado y así optar por el título de Ingeniero Electrónico. Lo importante de la actividad es comprender los temas relacionados con Networking.

Para este trabajo se asignan dos escenarios. En los cuales se desarrolla un proceso de documentación de la solución, configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante el desarrollo y por último el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, show, entre otros.

En el escenario 1 se soluciona un protocolo de enrutamiento avanzado, EBGp y la configuración se hace gracias a la herramienta de GNS3.

Para el escenario 2 se trabaja con una red bajo el dominio VTP (VLAN Trunking Protocol) y la configuración se realiza mediante software Packet Tracer 7.2.

DESARROLLO

ESCENARIO 1

Figura 1. Escenario 1

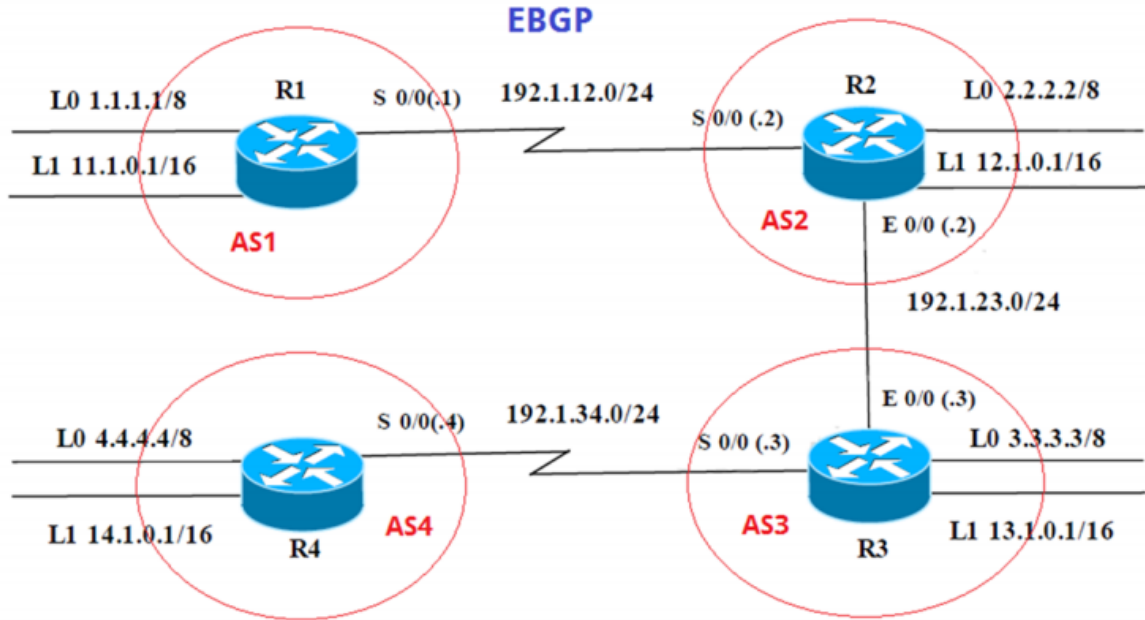


Figura 2. Simulación de escenario 1

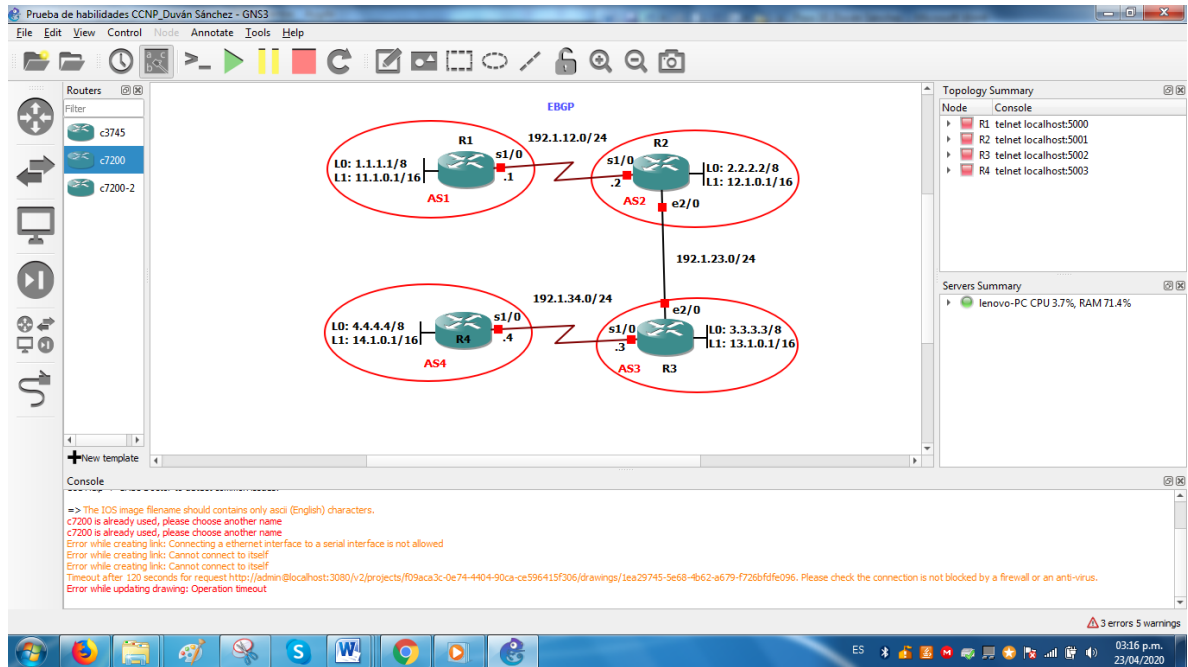
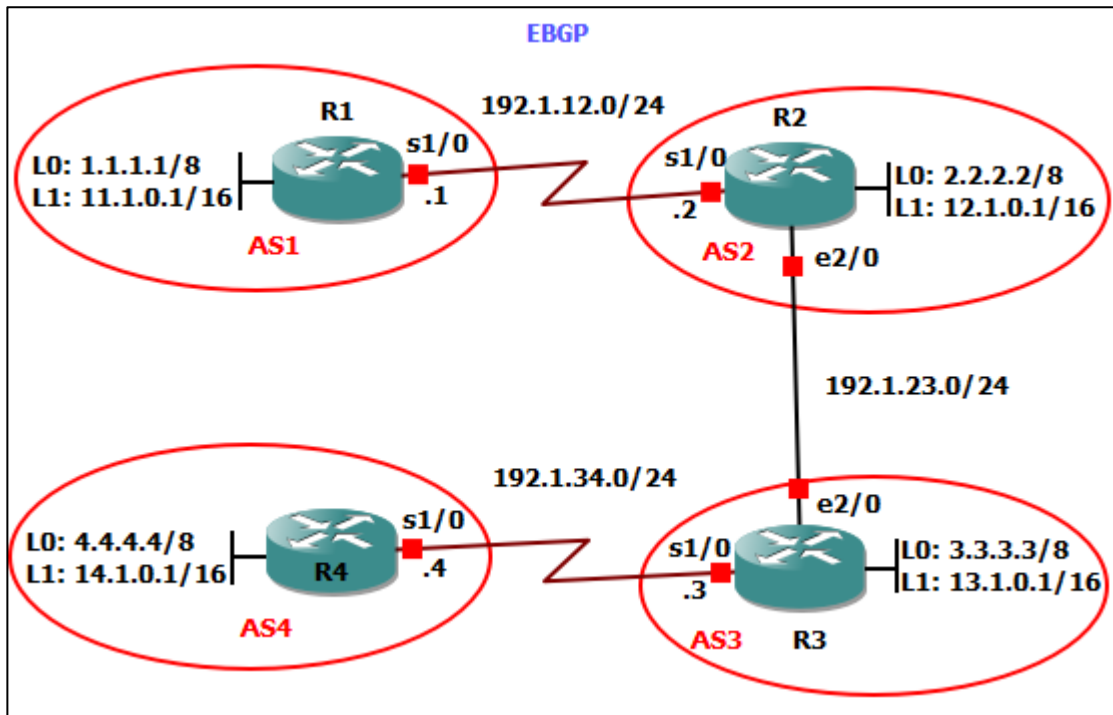


Figura 3. Simulación de escenario 1



Información para configuración de los Routers

Tabla 1. Interfaces Loopback para crear 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 0/0	192.1.12.1	255.255.255.0

Tabla 2. Interfaces Loopback para crear 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 0/0	192.1.12.2	255.255.255.0
	E 0/0	192.1.23.2	255.255.255.0

Tabla 3. Interfaces Loopback para crear 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 0/0	192.1.23.3	255.255.255.0
	E 0/0	192.1.34.3	255.255.255.0

Tabla 4. Interfaces Loopback para crear 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 0/0	192.1.34.4	255.255.255.0

La práctica se desarrolla con la ayuda del simulador **GNS3**. En cada router se realiza las configuraciones iniciales y la configuración de interfaces:

Configuración de todos los routers:

```
Router#configure terminal
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)#exit
```

Router R1

```
R1(config)# interface Lo0
R1(config-if)# ip address 1.1.1.1 255.0.0.0
R1(config-if)# exit
R1(config)# interface Lo1
R1(config-if)# ip address 11.1.0.1 255.255.0.0
R1(config-if)# exit
R1(config)# interface Serial1/0
R1(config-if)# description R1 -> R2
R1(config-if)# ip address 192.1.12.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# end
```

Router R2

```
R2(config)# interface Lo0
R2(config-if)# ip address 2.2.2.2 255.0.0.0
R2(config-if)# exit
R2(config)# interface Lo1
R2(config-if)# ip address 12.1.0.1 255.255.0.0
R2(config-if)# exit
R2(config)# interface Serial1/0
R2(config-if)# description R2 -> R1
R2(config-if)# ip address 192.1.12.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)exit
R2(config)# interface ethernet2/0
R2(config-if)# description R2 -> R3
R2(config-if)# ip address 192.1.23.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# end
```

Router R3

```
R3(config)# interface Lo0
R3(config-if)# ip address 3.3.3.3 255.0.0.0
R3(config-if)# exit
R3(config)# interface Lo1
R3(config-if)# ip address 13.1.0.1 255.255.0.0
R3(config-if)# exit
R3(config)# interface ethernet2/0
R3(config-if)# description R3 -> R2
R3(config-if)# ip address 192.1.23.3 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)exit
R3(config)# interface Serial1/0
R3(config-if)# description R3 -> R4
R3(config-if)# ip address 192.1.34.3 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)# end
```

Router R4

```
R4(config)# interface Lo0
R4(config-if)# ip address 4.4.4.4 255.0.0.0
R4(config-if)# exit
R4(config)# interface Lo1
R4(config-if)# ip address 14.1.0.1 255.255.0.0
R4(config-if)# exit
R4(config)# interface Serial1/0
R4(config-if)# description R4 -> R3
R4(config-if)# ip address 192.1.34.4 255.255.255.0
R4(config-if)# no shutdown
R4(config-if)# end
```

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 paso con los comandos utilizados y la salida del comando **show ip route**.

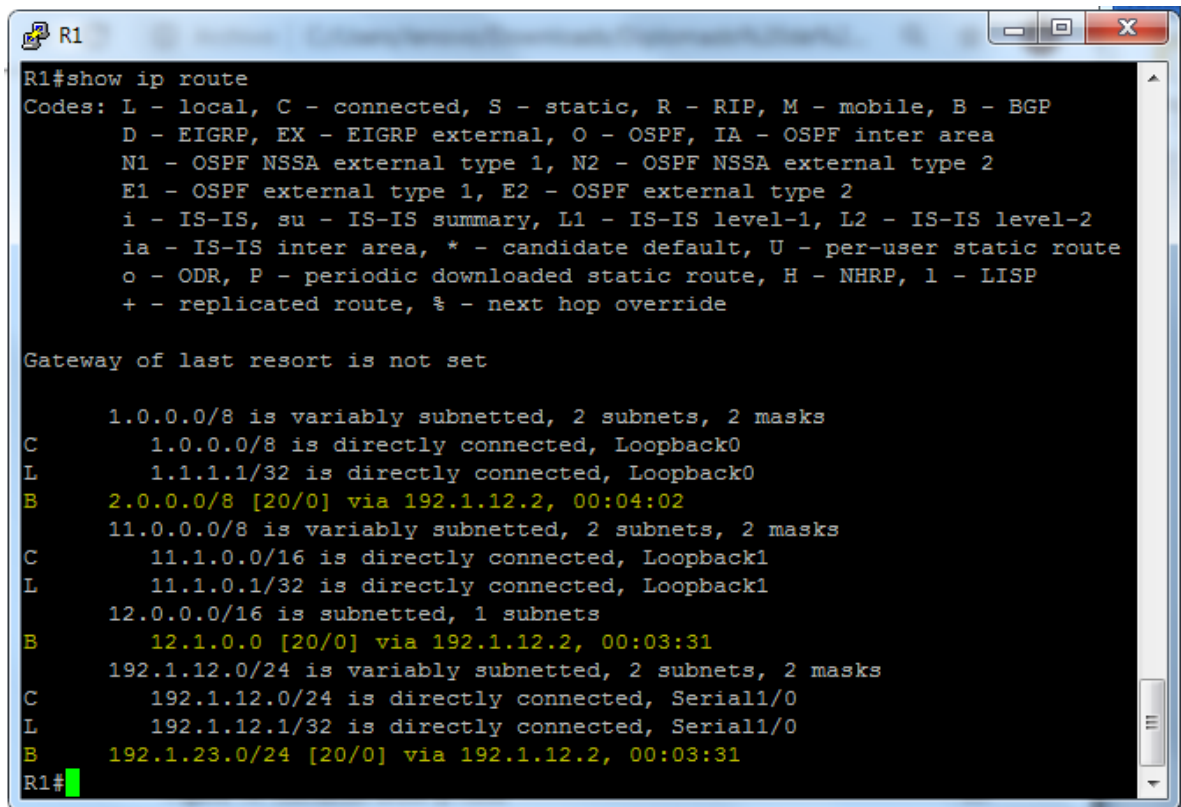
Configuración de BGP en los routers R1 y R2:

```
R1(config)# router bgp 1
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)# neighbor 192.1.12.2 remote-as 2
R1(config-router)# network 1.0.0.0 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)# router bgp 2
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)# neighbor 192.1.12.1 remote-as 1
R2(config-router)# neighbor 192.1.12.3 remote-as 3
R2(config-router)# network 192.1.12.0 mask 255.255.255.0
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
R1(config-router)# network 192.1.23.0 mask 255.255.255.0
```

Se verifica la configuración de la tabla de enrutamiento en R1 y R2.

Figura 4. Tabla de enrutamiento R1



```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

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, 00:04:02
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 [20/0] via 192.1.12.2, 00:03:31
192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.12.0/24 is directly connected, Serial1/0
L    192.1.12.1/32 is directly connected, Serial1/0
B    192.1.23.0/24 [20/0] via 192.1.12.2, 00:03:31
R1#
```


Figura 5. Tabla de enrutamiento R2

```

R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:17:44
     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 [20/0] via 192.1.12.1, 00:17:44
     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, Serial1/0
L       192.1.12.2/32 is directly connected, Serial1/0
     192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.23.0/24 is directly connected, Ethernet2/0
L       192.1.23.2/32 is directly connected, Ethernet2/0
R2#

```

- 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 paso con los comandos utilizados y la salida del comando **show ip route**.

```

R3(config)# router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)# neighbor 192.1.23.2 remote-as 2
R3(config-router)# 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

```

Figura 6. Tabla de enrutamiento R3

```

R3#
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.1.23.2 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 192.1.23.2
     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
B     4.0.0.0/8 [20/0] via 192.1.34.4, 00:18:54
     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
     14.0.0.0/16 is subnetted, 1 subnets
B     14.1.0.0 [20/0] via 192.1.34.4, 00:18:54
     192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.1.23.0/24 is directly connected, Ethernet2/0
L     192.1.23.3/32 is directly connected, Ethernet2/0
     192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.1.34.0/24 is directly connected, Serial1/0
L     192.1.34.3/32 is directly connected, Serial1/0
R3#

```

- 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 paso con los comandos utilizados y la salida del comando **show ip route**.

```

R4(config)# router bgp 4
R4(config-router)#bgp 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

```

Figura 7. Tabla de enrutamiento R4

```
R4#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

B    3.0.0.0/8 [20/0] via 192.1.34.3, 00:18:51
    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
    13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0 [20/0] via 192.1.34.3, 00:18:51
    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    192.1.23.0/24 [20/0] via 192.1.34.3, 00:18:51
    192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial1/0
L    192.1.34.4/32 is directly connected, Serial1/0
R4#
```

ESCENARIO 2

Figura 8. Escenario 2

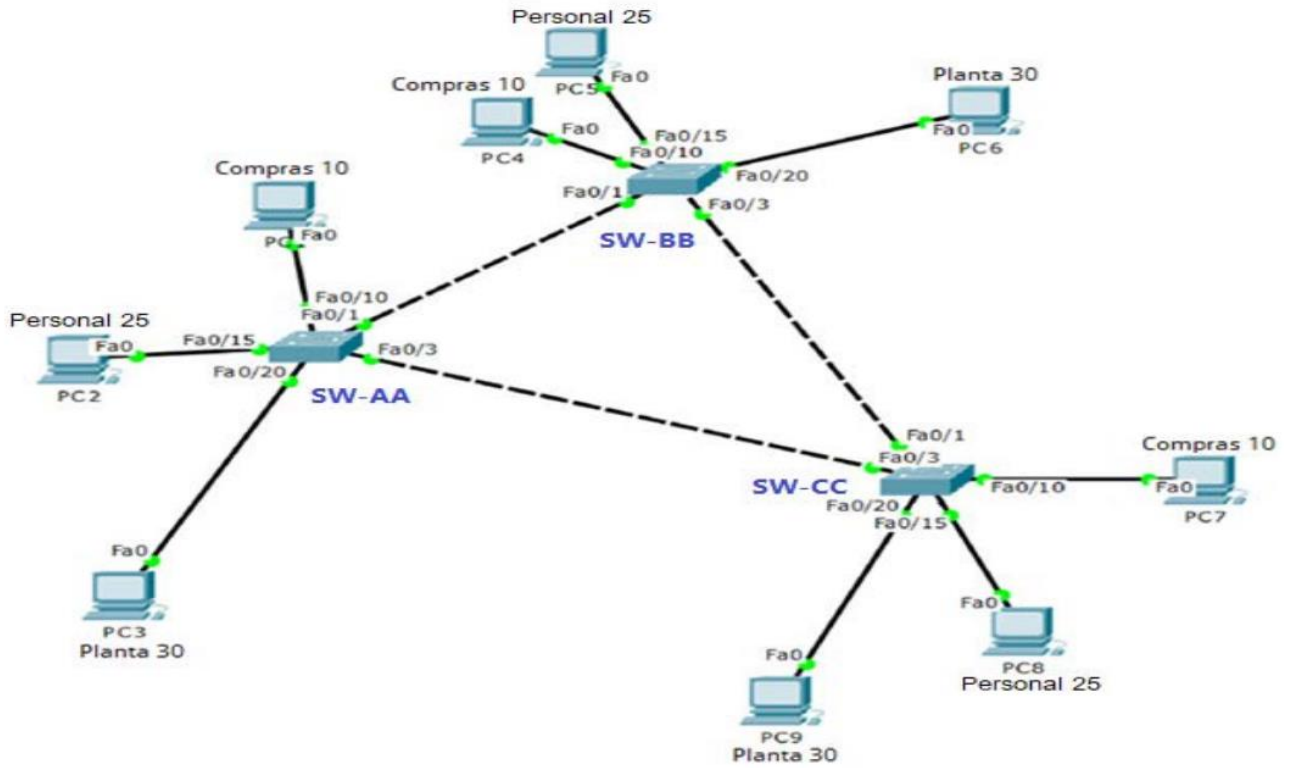
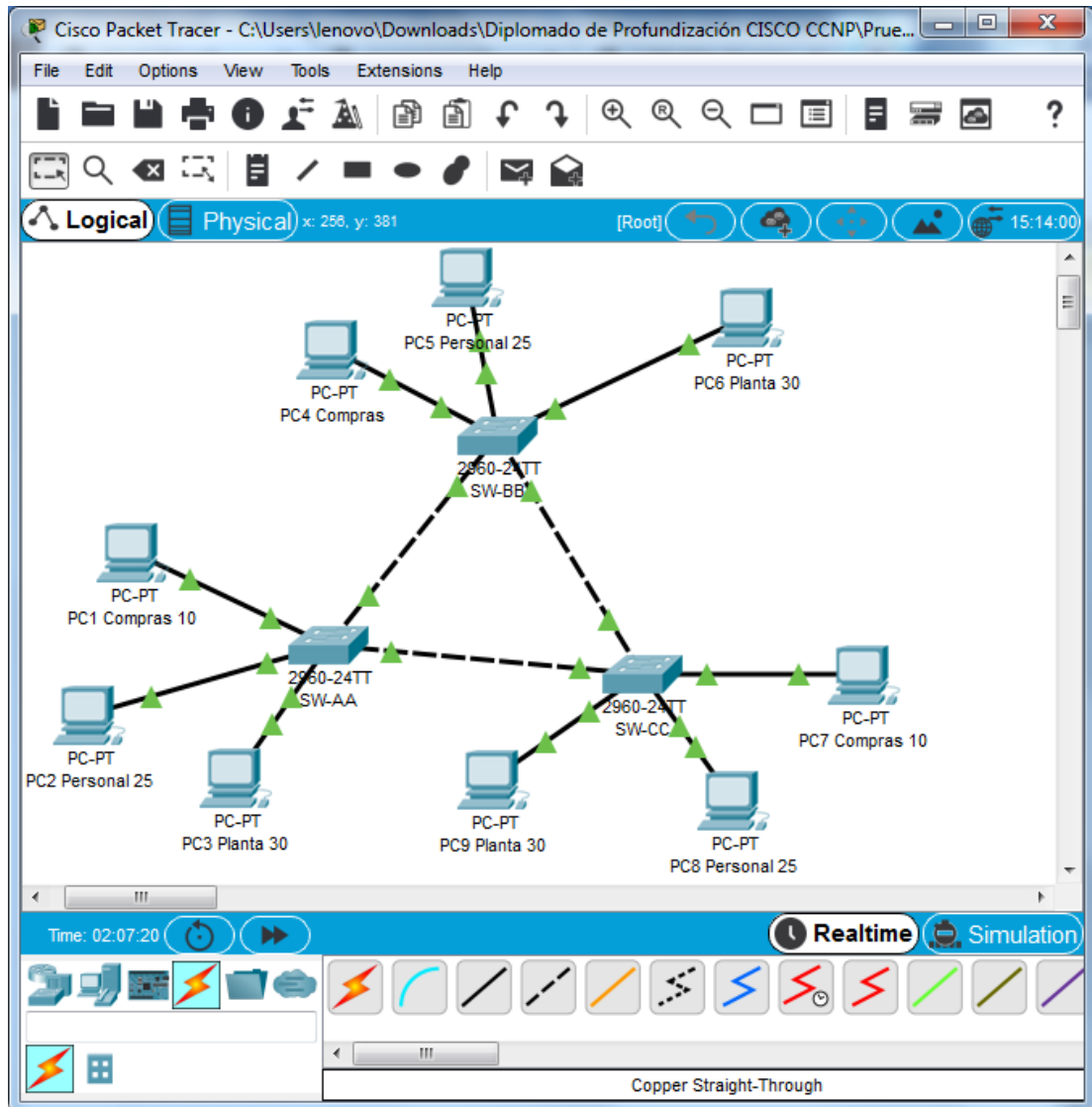


Figura 9. Simulación de escenario 2



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.

La simulación se desarrolla en Cisco Packet Tracer 7.2. A continuación se configura para los tres switches con las configuraciones iniciales y se habilita el Protocolo de truncamiento de VLAN:

SW-AA

```
Switch>enable
Switch#config t
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-BB

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

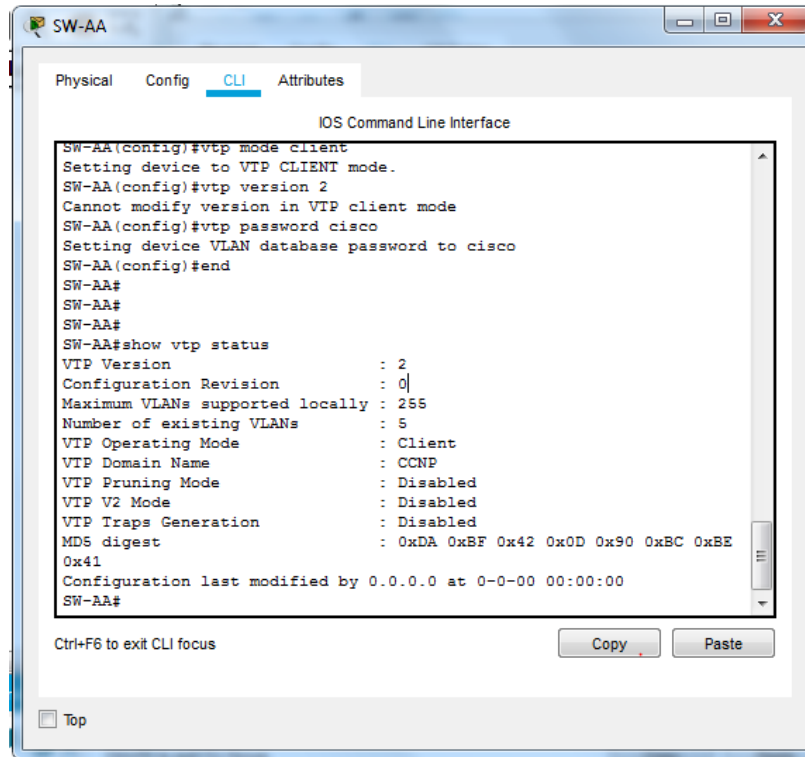
SW-CC

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

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

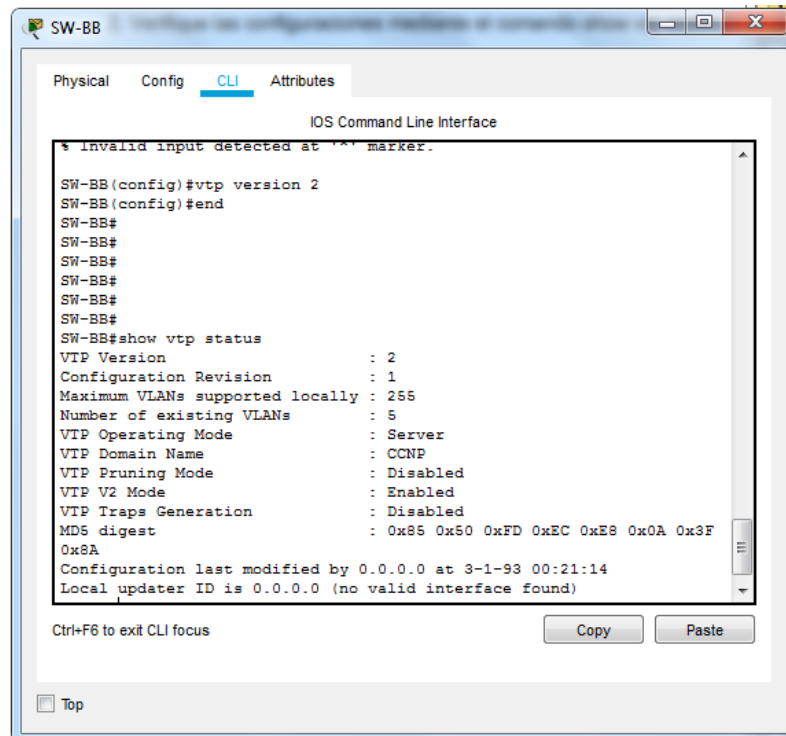
```
SW-AA#show vtp status
SW-BB#show vtp status
SW-BB# show vtp status
```

Figura 10. VTP en SW-AA



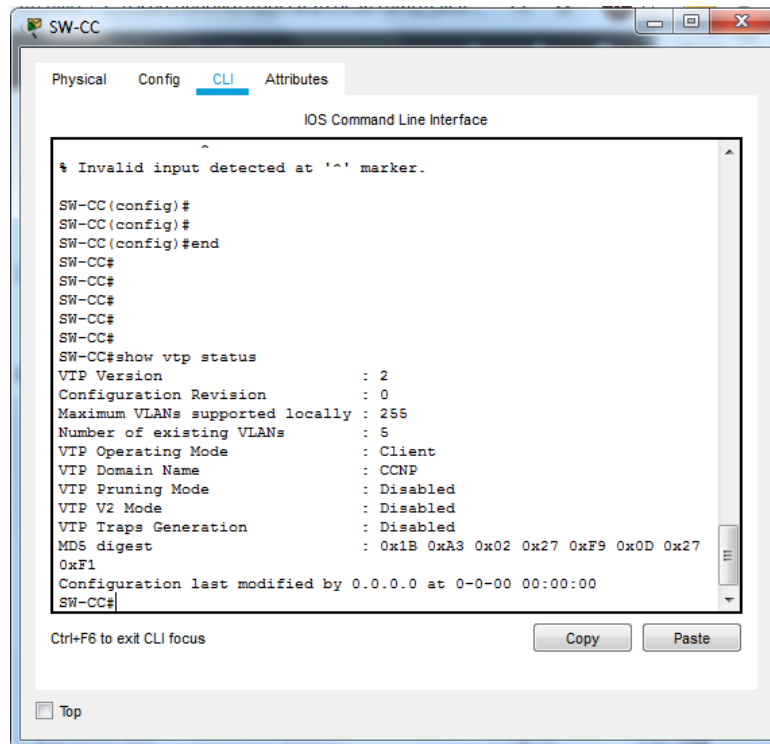
```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
SW-AA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-AA(config)#vtp version 2
Cannot modify version in VTP client mode
SW-AA(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-AA(config)#end
SW-AA#
SW-AA#
SW-AA#
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 11. VTP en SW-BB



```
SW-BB
Physical Config CLI Attributes
IOS Command Line Interface
% Invalid input detected at ... marker.
SW-BB(config)#vtp version 2
SW-BB(config)#end
SW-BB#
SW-BB#
SW-BB#
SW-BB#
SW-BB#
SW-BB#
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
MD5 digest : 0xB5 0x50 0xFD 0xEC 0xEB 0x0A 0x3F
0x8A
Configuration last modified by 0.0.0.0 at 3-1-93 00:21:14
Local updater ID is 0.0.0.0 (no valid interface found)
SW-BB#
```

Figura 12. VTP en SW--CC



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**.

SW-AA

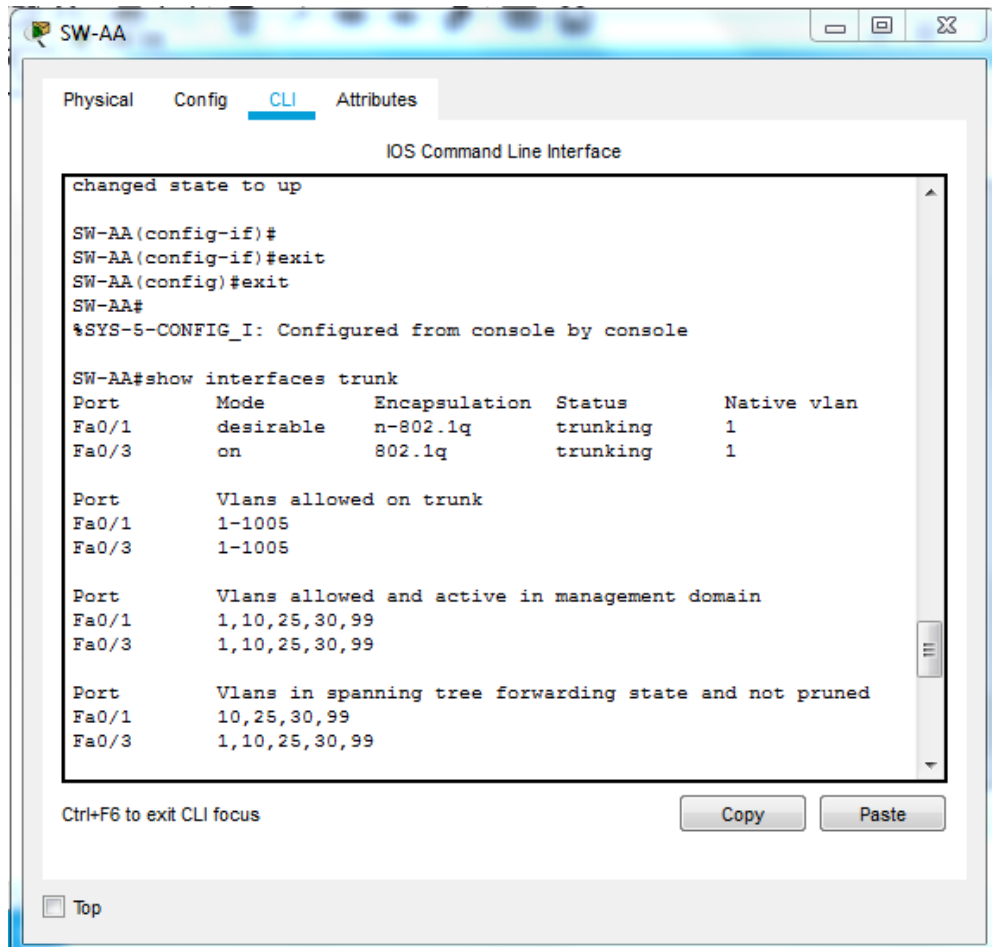
```
SW-AA(config)#int f0/1
SW-AA(config-if)#switchport mode trunk
SW-AA(config-if)#switchport mode dynamic desirable
```

SW-BB

```
SW-BB(config)#int f0/1
SW-BB(config-if)#switchport mode trunk
```

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

Figura 13. Comando Show 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

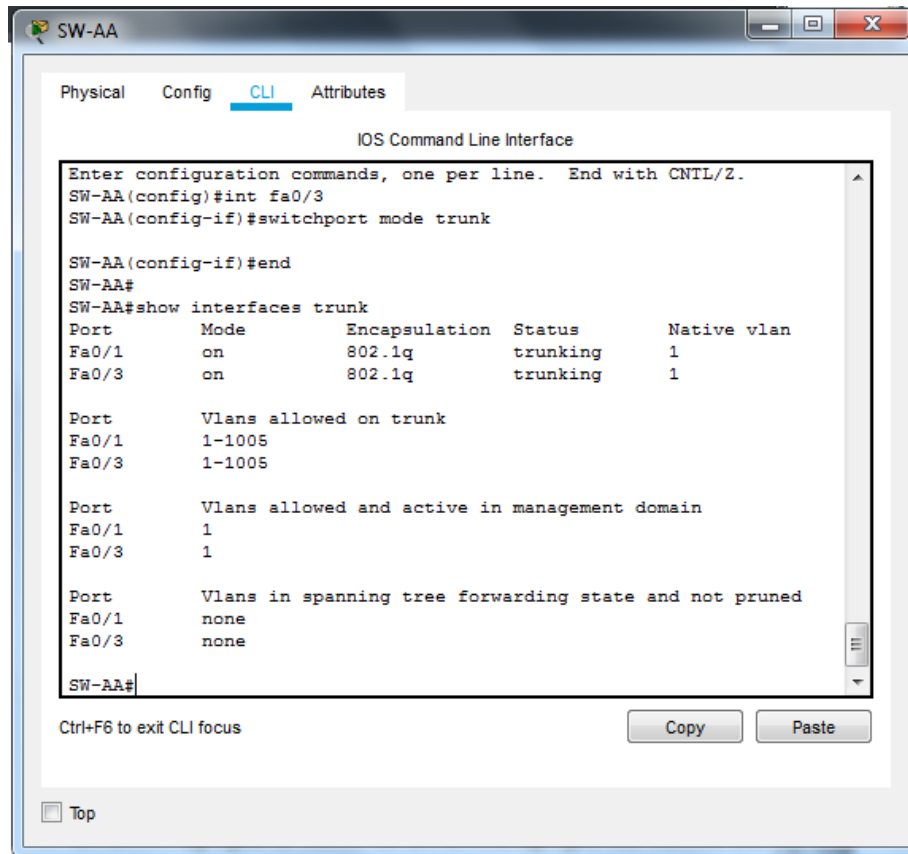
```
SW-AA(config)#int f0/1
SW-AA(config-if)#switchport mode trunk
```

SW-BB

```
SW-BB(config)#int f0/1
SW-BB(config-if)#switchport mode trunk
```

- Verifique el enlace “trunk” con el comando **show interfaces trunk** en SW-AA.

Figura 14. Comando Show interfaces trunk en SW-AA



8. Configure un enlace “trunk” permanente entre SW-BB y SW-CC.

SW-BB

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

SW-CC

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

C. Agregar VLANs y asignar puertos.

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

SW-AA

```
SW-AA#config t
```

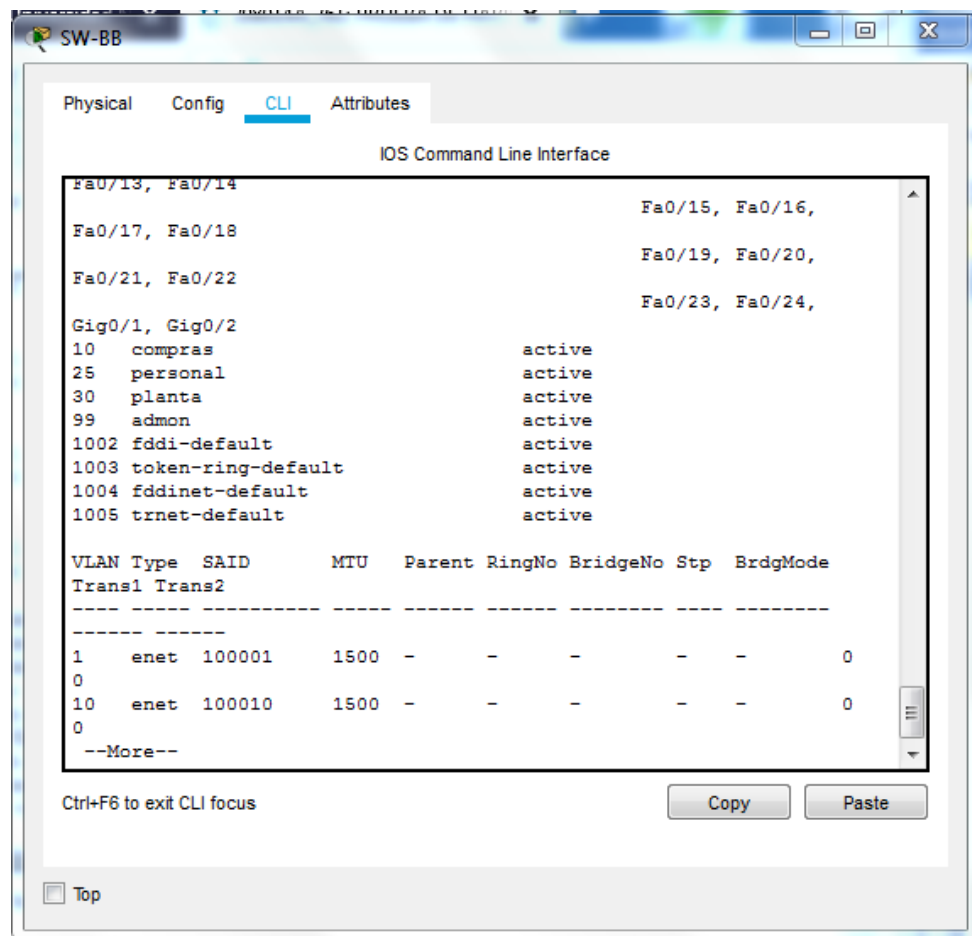
```
SW-AA(config)#int vlan 10
VTP VLAN configuration not allowed when device is in CLIENT
mode.
```

SW-BB

```
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
```

10. Verifique que las VLANs han sido agregadas correctamente

Figura 15. Comando show vlan en SW-BB



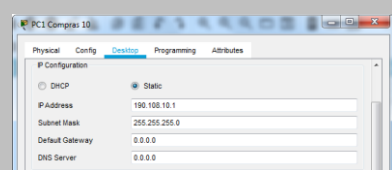
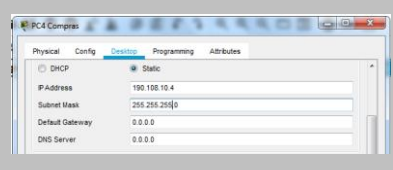
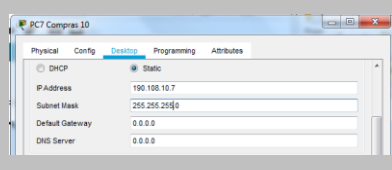

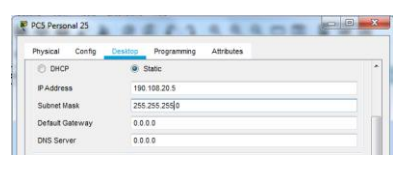
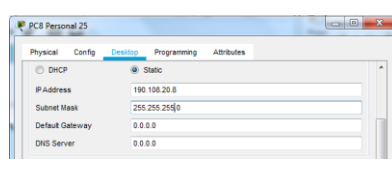
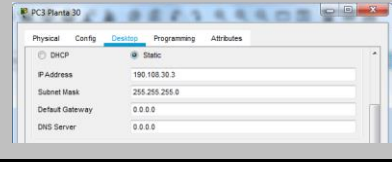
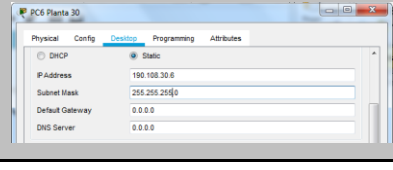
11. Asocie los puertos a las VLAN y configure las direcciones IP de acuerdo con la siguiente tabla.

Tabla 5. Direcciones IP de los PCs

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

Tabla 6. Configuración IP en los PCs

SW-AA	SW-BB	SW-CC
		
		
		

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.

```
SW-AA(config)#int f0/10
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#no shut
SW-AA(config-if)#exit
SW-AA(config)#int f0/15
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#no shut
SW-AA(config-if)#exit
SW-AA(config)#int f0/20
SW-AA(config-if)#switchport access vlan 30
SW-AA(config-if)#no shut
SW-AA(config-if)#exit
```

```
SW-BB(config)#int f0/10
SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#no shut
SW-BB(config-if)#exit
SW-BB(config)#int f0/15
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#no shut
SW-BB(config-if)#exit
SW-BB(config)#int f0/20
SW-BB(config-if)#switchport access vlan 30
SW-BB(config-if)#no shut
SW-BB(config-if)#exit
```

```
SW-CC(config)#int f0/10
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#no shut
SW-CC(config-if)#exit
SW-CC(config)#int f0/15
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#no shut
SW-CC(config-if)#exit
SW-CC(config)#int f0/20
SW-CC(config-if)#switchport access vlan 30
SW-CC(config-if)#no shut
SW-CC(config-if)#exit
```

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.

Tabla 7. Direcciones IP en los Switches

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 SW-AA

```
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
```

Configuración en SW-BB

```
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
```

Configuración en SW-CC

```
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. Verificar la conectividad Extremo a Extremo

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

Figura 16. Ping PC1 compras 10

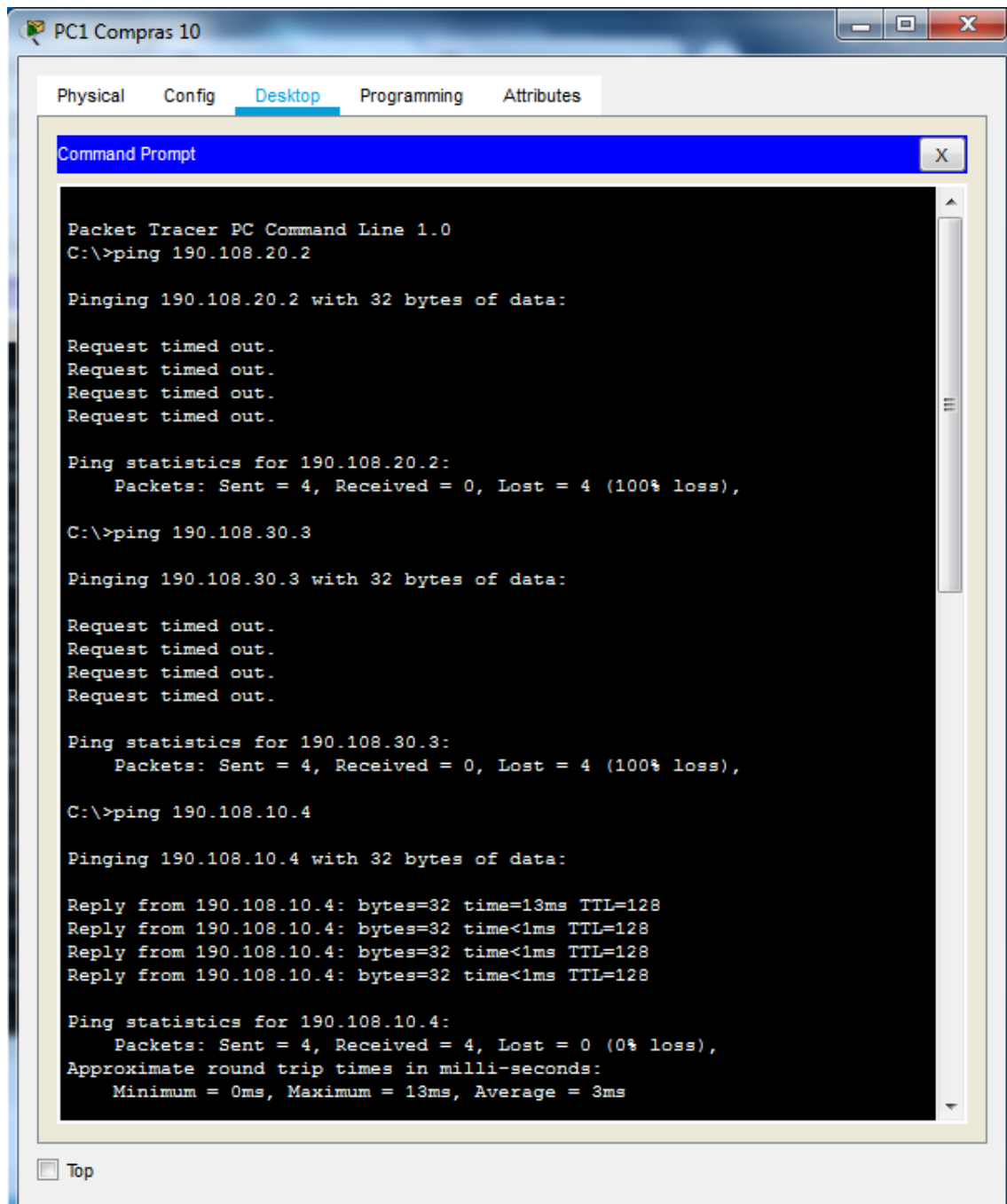
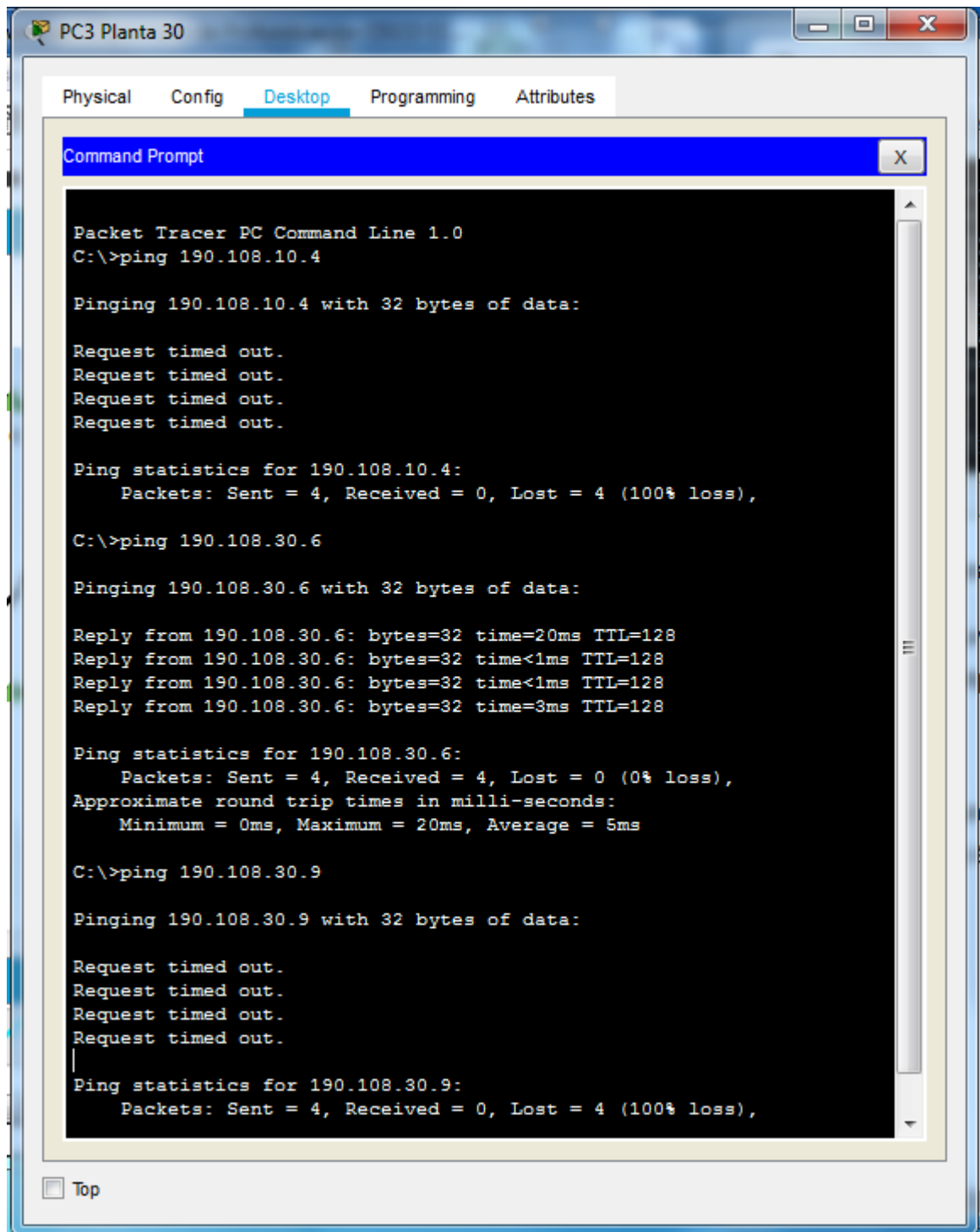


Figura 17. Ping PC3 Planta 30



Conclusión: El ping es exitoso en los PCs que pertenecen a la misma VLAN, pero no es exitoso a las VLANs que son distintas.

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

Figura 18. Ping desde SW-AA

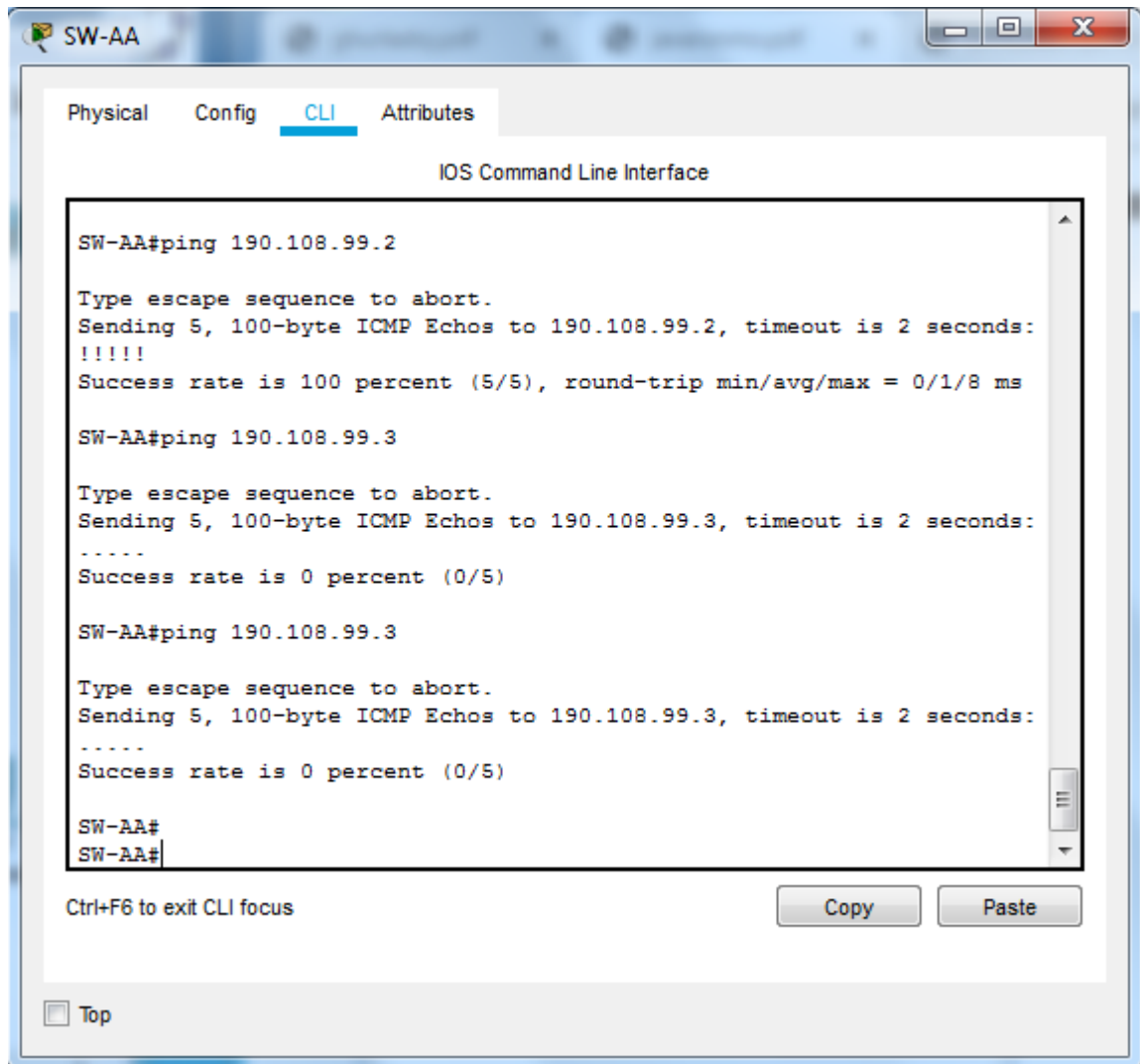


Figura 19. Ping desde SW-BB

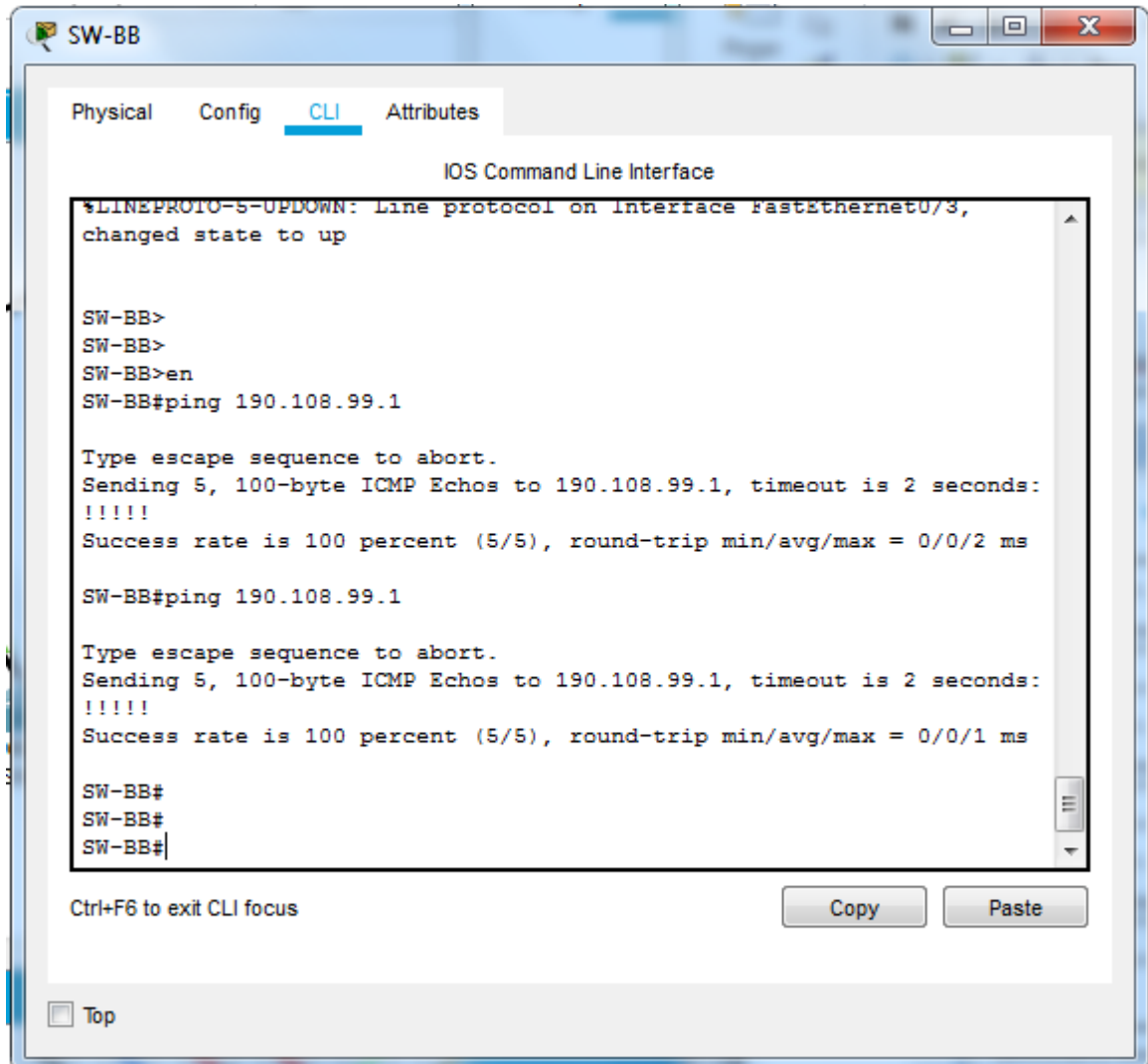
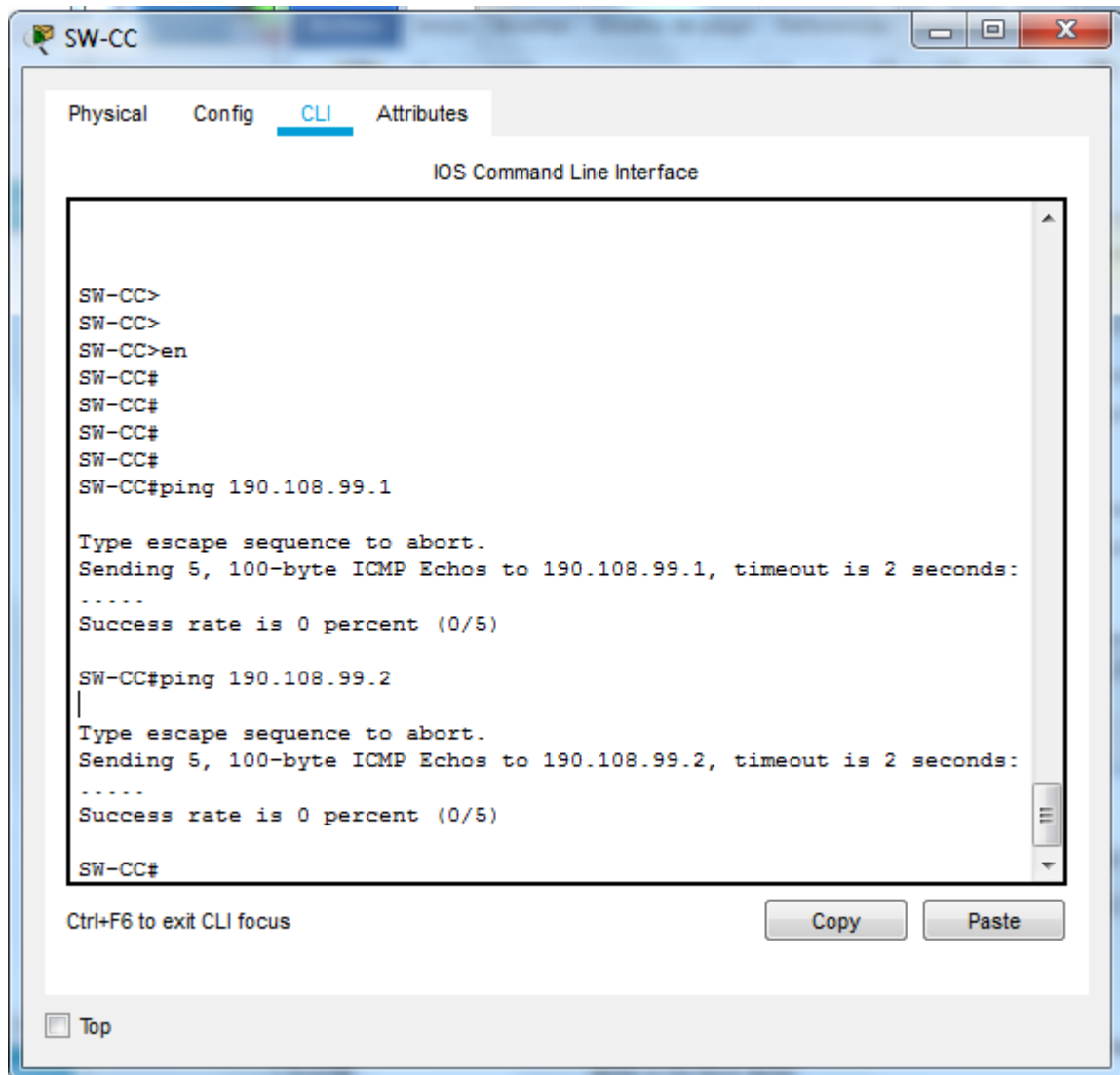


Figura 20. Ping desde SW-CC



```
SW-CC>
SW-CC>
SW-CC>en
SW-CC#
SW-CC#
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 0 percent (0/5)

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 0 percent (0/5)

SW-CC#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

El ping desde el SW-AA tuvo éxito al SW-BB, pero no al SW-CC.

El ping desde el SW-BB tuvo éxito al SW-BB y al SW-CC.

El ping desde el SW-CC no tuvo éxito al SW-AA y al SW-CC

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

Figura 21. Ping desde SW-AA a PC

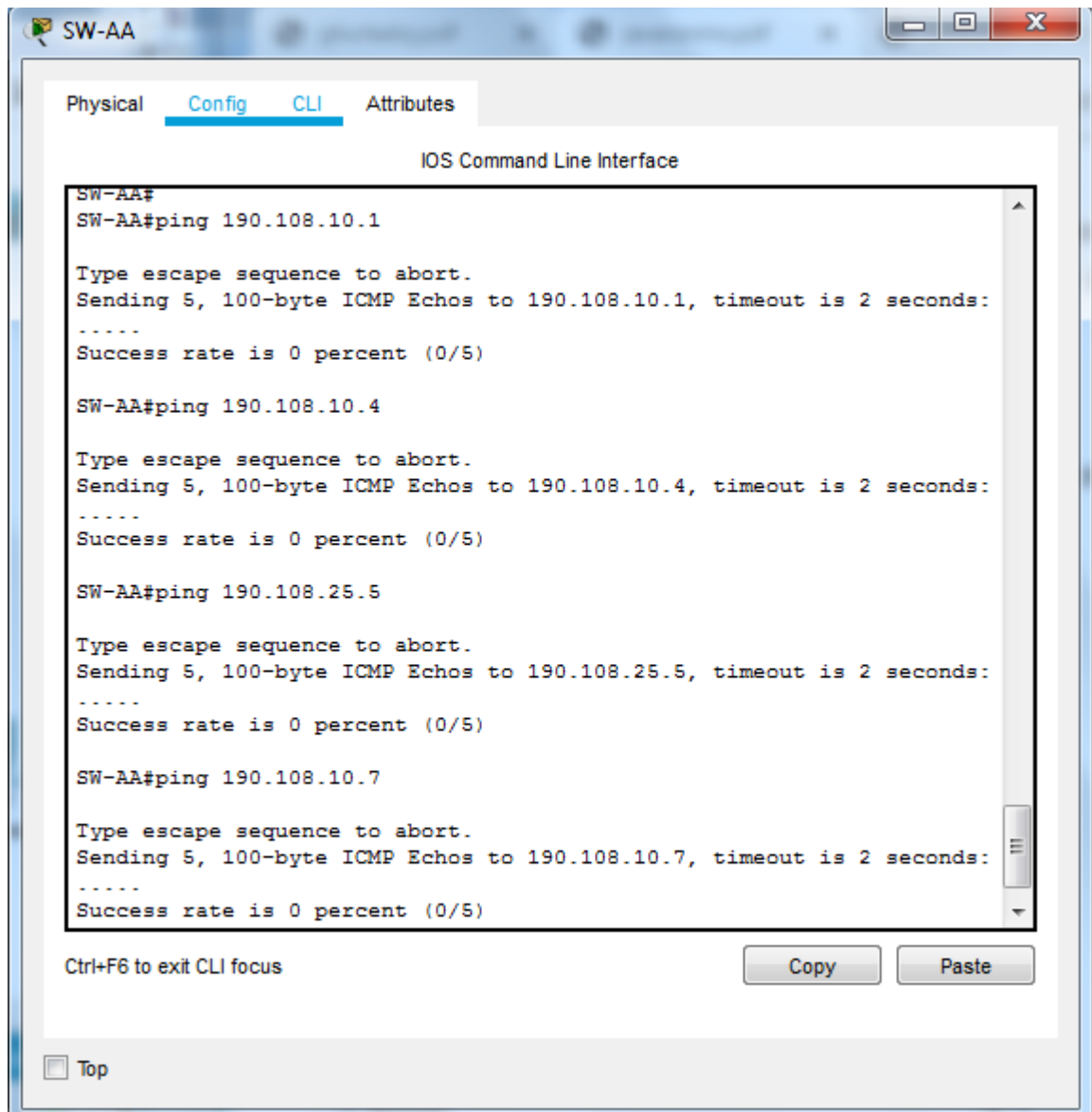


Figura 22. Ping desde SW-BB a PC

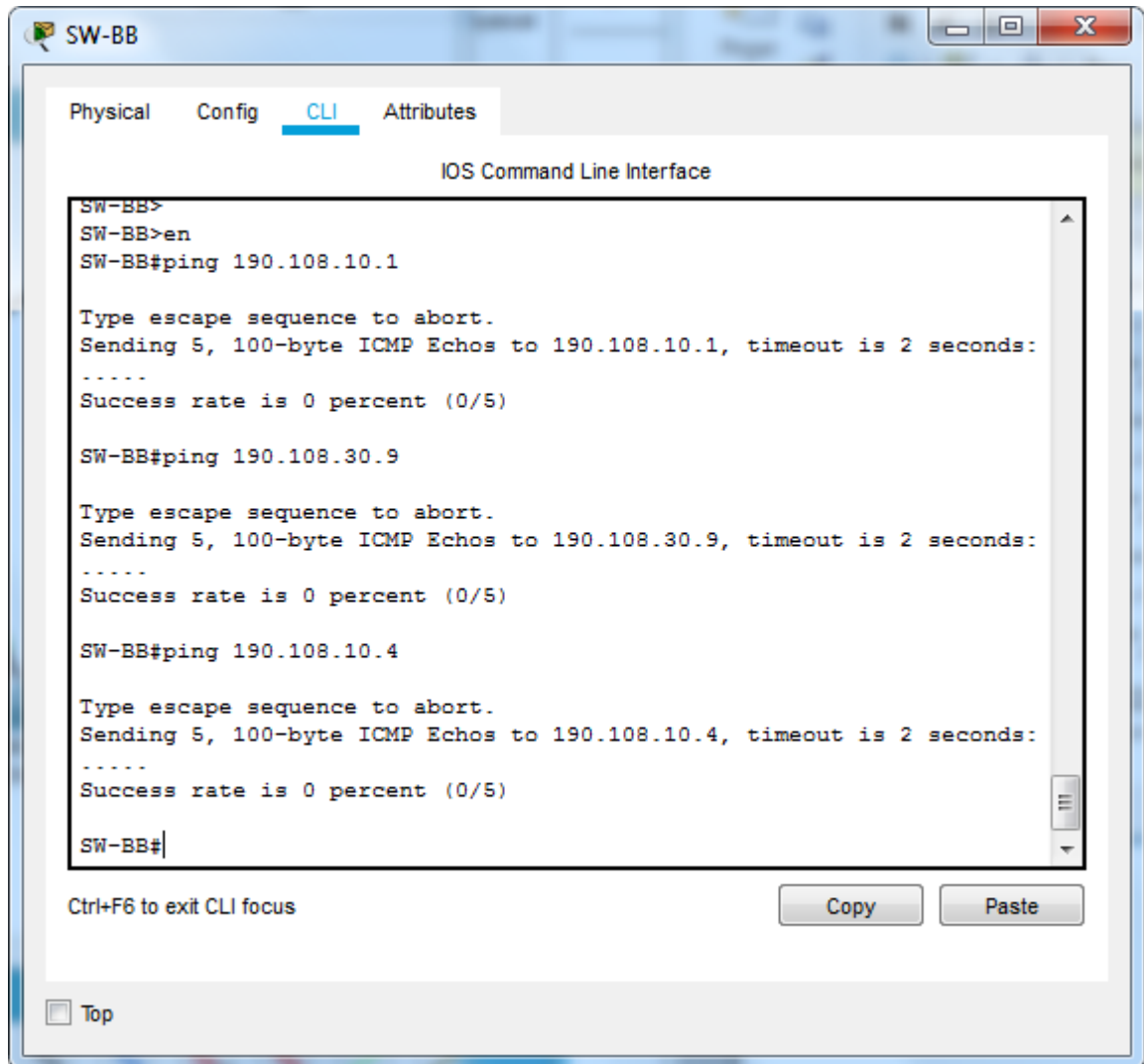
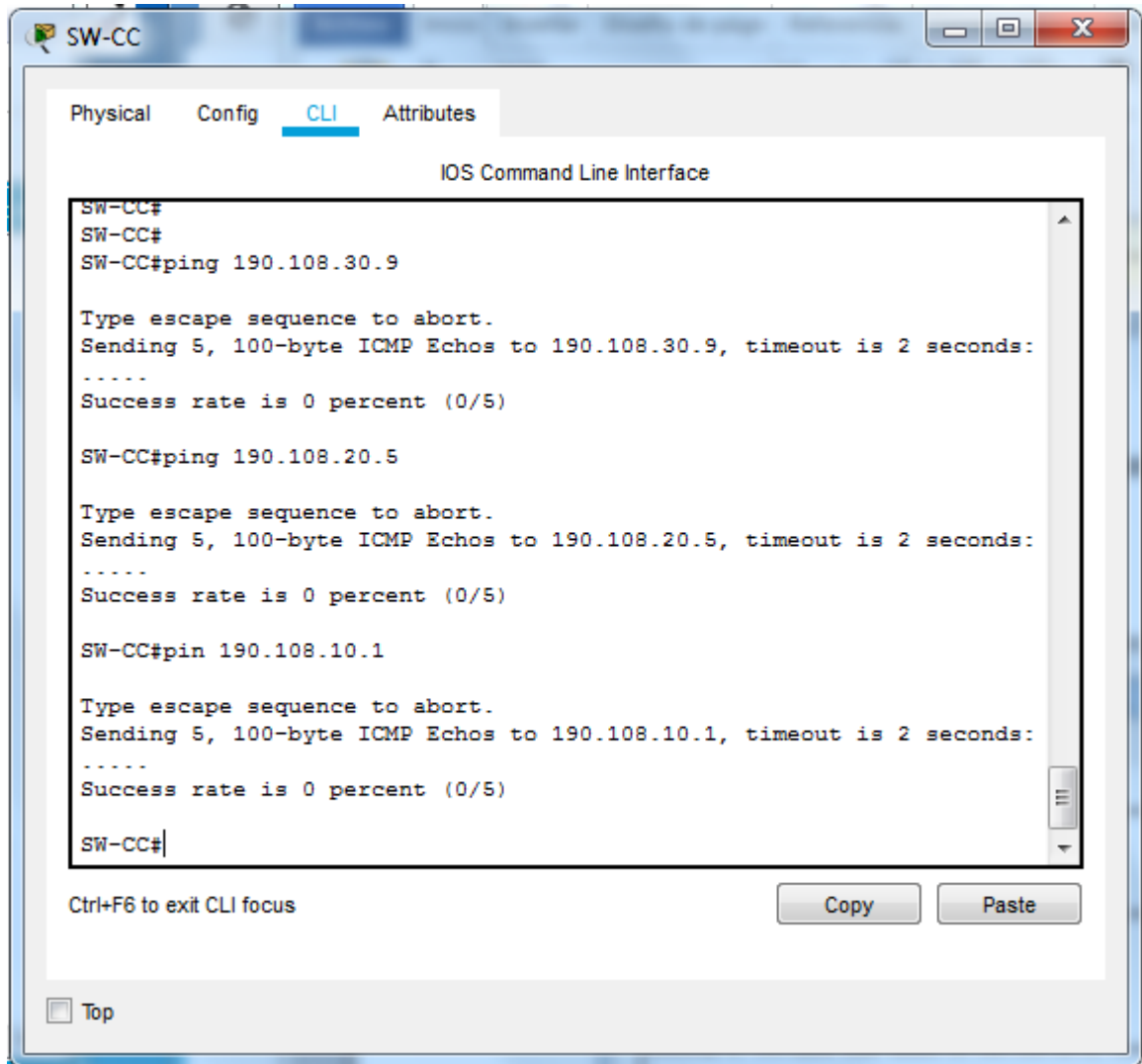


Figura 23. Ping desde SW-CC a PC



Conclusión: El ping no tuvo éxito en los tres Switches debido a que no se asignó una dirección IP a las VLANs.

CONCLUSIONES

Con la práctica del protocolo BGP (Border Gateway Protocol) se pudo conocer la capacidad, en caso de que existan varias rutas, de usar múltiples interfaces IP para comunicarse con un vecino.

Las VLAN se pueden segmentar lógicamente una red por función, equipo o aplicación, sin importar la ubicación física de los usuarios.

Con la implementación de las tecnologías de trunking, conmutadores de conexión y el Protocolo de trunking de VLAN (VTP) gestiona la adición, eliminación y cambio de nombre de VLAN en toda la red desde un solo switch.

Se pudo establecer que un cliente VTP se comporta como un servidor VTP y transmite y recibe actualizaciones VTP en sus troncales, pero con la diferencia que no puede crear, cambiar o eliminar VLAN en un cliente VTP.

BIBLIOGRAFÍA

COLOMBIANA, NORMA TÉCNICA. NTC 1486: 2008, sexta actualización. Documentación de tesis, trabajos de grado y otros trabajos de investigación. Bogotá DC, Colombia: Icontec, 2008.

LANCHEROS LÓPEZ, Jaime. "Diplomado de Profundización CISCO (Diseño e Implementación de Soluciones Integradas LAN / WAN". Repositorio Institucional UMNG. Universidad Militar Nueva Granada. {En línea}. 2018. Web. {14 mayo 2020}. Disponible en <https://repository.unad.edu.co/handle/10596/18961>

PÉREZ SUAREZ, Cristhian Sebastián, et al. Diseño e implementación de un enrutamiento redundante usando el protocolo Border Gateway Protocol (BGP) para la red de un proveedor de servicios de internet en Bogotá. <https://repository.usta.edu.co/bitstream/handle/11634/3947/Perezcristihian2017.pdf?sequence=1&isAllowed=y>

RUBLE, David A., Análisis y diseño práctico para sistemas cliente/servidor con GUI. Prentice-Hall Hispanoamericana, No. 004.7. 1998. Web. 13 mayo 2020

TEARE, Diane, et al. CCNP Routing and Switching Foundation Learning Guide Library: (ROUTE 300-101, SWITCH 300-115, TSHOOT 300-135). Cisco Press 2015.