DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JORGE ORLANDO RODRÍGUEZ ANDRADE

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JORGE ORLANDO RODRÍGUEZ ANDRADE

Diplomado de opción de grado presentado para optar el título
de INGENIERO DE TELECOMUNICACIONES

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTÁ, 22 de mayo de 2020

AGRADECIMIENTOS

En primer lugar, quiero agradecer a todas las personas que me han apoyado a lo largo de estos años de formación como ingeniero de Telecomunicaciones. En especial a mi familia que ha sido mi mayor motivo para continuar; a La universidad Nacional abierta y a Distancia por ofrecerme la opción de estudiar de manera virtual para poder completar mi ciclo académico profesional.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

BGP - Border Gateway Protocol: Es el protocolo de encaminamiento EGP más utilizado en Internet. Funciona sobre TCP por el puerto 179. BGP permite el encaminamiento de los paquetes IP que se intercambian entre los distintos AS.

Dirección IP: Dirección de protocolo de Internet, la forma estándar de identificar un equipo que está conectado a Internet, de forma similar a como un número de teléfono identifica un aparato de teléfono en una red telefónica. La dirección IP consta de cuatro números separados por puntos, en que cada número es menor de 256; por ejemplo 64.58.76.178. Dicho Número IP es asignado de manera permanente o temporal a cada equipo conectado a la red.

Gateway – Pasarela o puerta de acceso: Computador que realiza la conversión de protocolos entre diferentes tipos de redes o aplicaciones. Por ejemplo, una puerta de acceso podría conectar una red de área local a un mainframe. Una puerta de acceso de correo electrónico, o de mensajes, convierte mensajes entre dos diferentes protocolos de mensajes.

VLAN - Red de Área Local Virtual: Tipo de red que aparentemente parece ser una pequeña red de área local (LAN) cuando en realidad es una construcción lógica que permite la conectividad con diferentes paquetes de software. Sus usuarios pueden ser locales o estar distribuidos en diversos lugares.

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

DHCP: Siglas del inglés "Dynamic Host Configuration Protocol." Protocolo Dinámico de configuración del Host. Un servidor de red usa este protocolo para asignar de forma dinámica las direcciones IP a las diferentes computadoras de la red.

CCNP: (Cisco Certified Network Professional) es el nivel intermedio de certificación de la compañía .3 Para obtener esta certificación, se han de superar varios exámenes, clasificados según la empresa en 3 módulos. Esta certificación, es la intermedia de las certificaciones generales de Cisco, no está tan valorada como el CCIE, pero sí, mucho más que el CCNA.

RESUMEN

El diplomado de Cisco CCNP fue diseñado para aquellos que desean adquirir habilidades de gestión de redes orientadas hacia el mundo profesional y de nivel empresarial. El diplomado de CCNP ayuda a adquirir las habilidades necesarias para complementar con éxito títulos universitarios relacionados con las TIC y para prepararse para la certificación Cisco CCNP. Ofrece una experiencia de aprendizaje con una gran carga tanto teórica como práctica que abarca habilidades avanzadas de Routing, Switching y resolución de problemas.

Dentro del presente documento se realizará el paso a paso de dos configuraciones de redes los cuales demuestran que se han adquirido las competencias prácticas requeridas para aprobar el diplomado cisco CCNP.

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

ABSTRACT

The Cisco CCNP Diploma was designed for those who wish to acquire professional and business-oriented network management skills. The CCNP Diploma helps you acquire the skills necessary to successfully complete ICT-related university degrees and prepare for Cisco CCNP certification. It offers a highly charged learning experience in both theory and practice that encompasses advanced routing, switching, and problem-solving skills.

Within this document we will take a step-by-step look at two network configurations which demonstrate that we have acquired the practical skills required to pass the cisco CCNP diploma.

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

INTRODUCCIÓN

El contenido de la presente actividad expone la Prueba de habilidades prácticas que ofrece el Diplomado de Profundización CCNP en el cual se hace demuestran las competencias y habilidades que fueron adquiridas a lo largo del curso y a través de la cual se pondrá a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

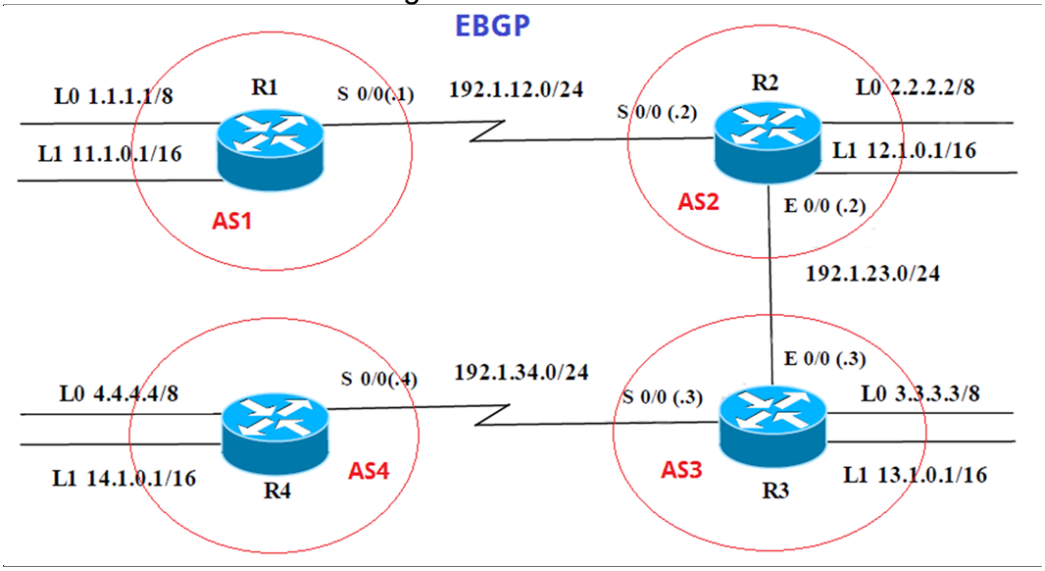
A través de los conocimientos adquiridos desde en el curso, se realizó la planificación, implementación, verificación y solución de problemas de redes empresariales locales y de área amplia, partiendo de conocimientos previos y fundamentos de la configuración de áreas y sistemas autónomos respectivamente y se plasma dentro de este documento el paso a paso detallado del proceso.

Para ello se exponen dos escenarios propuestos para el desarrollo de esta actividad, en el cual se implementan protocolos como VLAN Trunking Protocol, así como el enrutamiento InterVLAN para lo cual se hace mediante la configuración de áreas, sistemas autónomos respectivamente y el enrutamiento a través del protocolo BGP del todo empleando el protocolo IPv4 del Router ID e interfaces Loopback. Por último, se realiza la configuración de una pequeña red basada en Switches capa 2 y PCs, en la cual se configura el enrutamiento IPv4 respectivo.

DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

ESCENARIO 1

Figura 1: Escenario 1



Información para configuración de los Routers

Tabla 1: R1

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 2/0	192.1.12.1	255.255.255.0

Tabla 2: R2

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 2/0	192.1.12.2	255.255.255.0
E 0/0	192.1.23.2	255.255.255.0

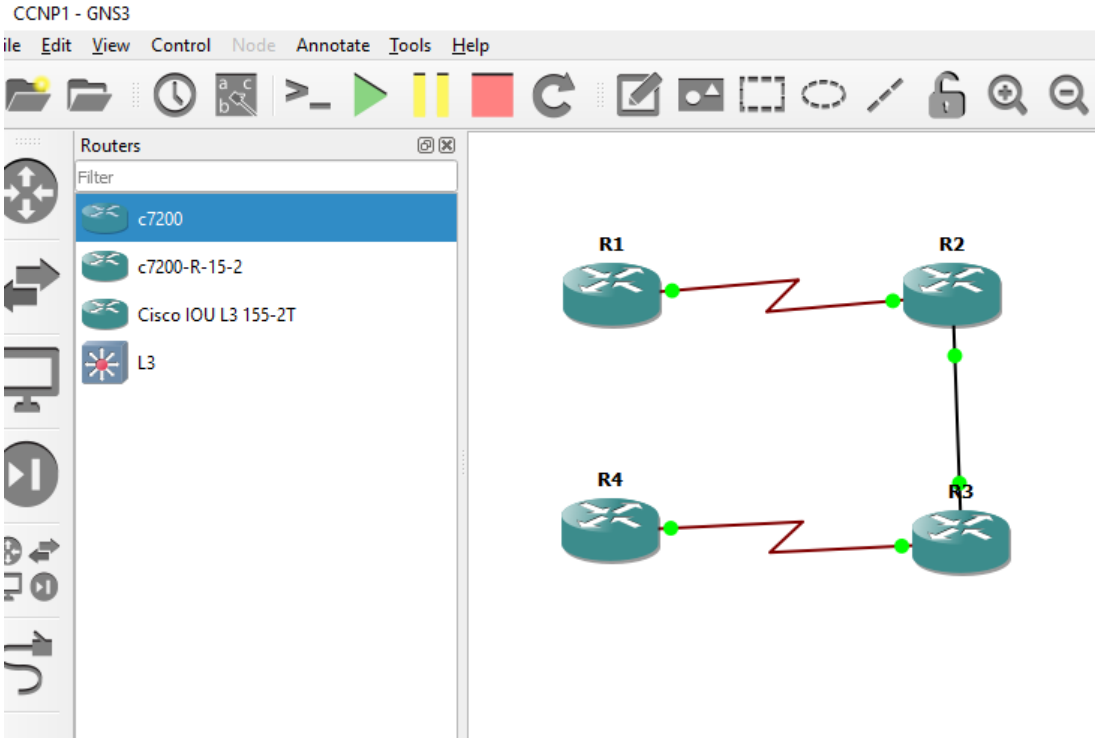
Tabla 3: R3

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 2/0	192.1.34.3	255.255.255.0

Tabla 4: R4

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 2/0	192.1.34.4	255.255.255.0

Figura 2: Montaje en GNS3



1.1. 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.***

R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface Loopback 0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#interface Loopback 1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#interface serial 2/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router bgp 1

R1(config-router)#bgp router-id 22.22.22.22
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
R1(config-router)#neighbor 192.1.12.2 remote-as 2

R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface Loopback 0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#interface Loopback 1
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#interface serial 2/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#interface Ethernet 0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router bgp 2
R2(config-router)#bgp router-id 33.33.33.33
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 192.1.12.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.12.1 remote-as 1

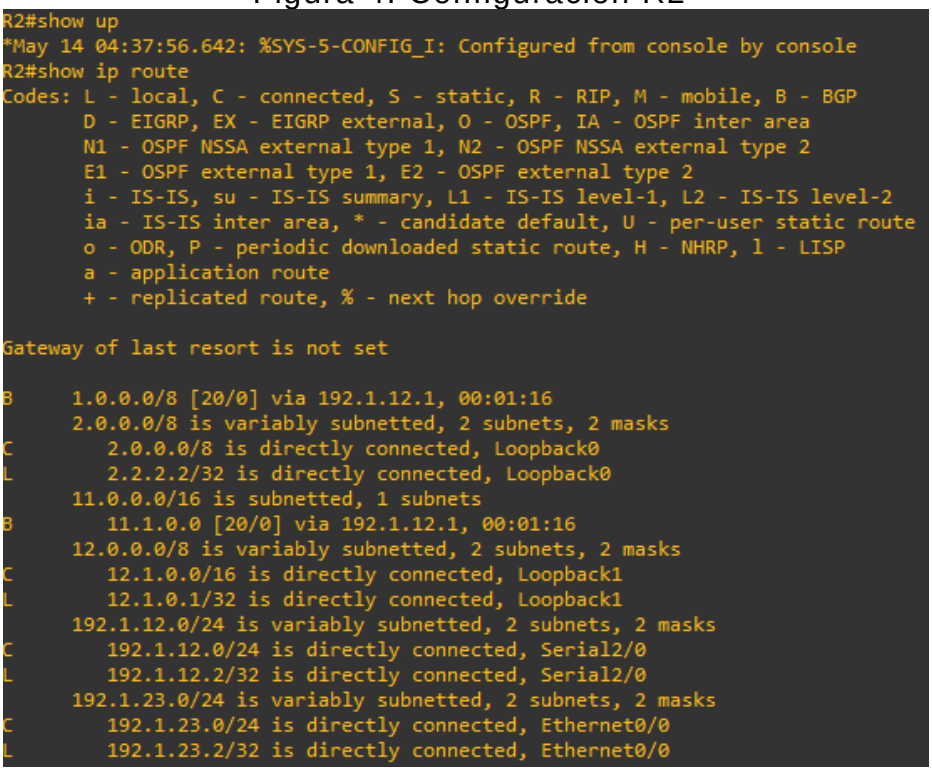
Figura 3: Configuración R1

```
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
       a - application route
       + - 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, 00:00:47
      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, 00:00:47
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial2/0
L        192.1.12.1/32 is directly connected, Serial2/0
```

Figura 4: Configuración R2



En la imagen anterior, se puede ver el resultado obtenido del comando ***show ip route***. El router R1 como el router R2 tiene en su tabla de enrutamiento las direcciones de loopback y las direcciones de las redes a las cuales se encuentran Conectadas en sus interfaces. En este comando también se puede observar un codigo B, correspondiente a BGP que permite ver las redes configuradas con este protocolo.
La tabla de enrutamiento del router R1 y R2 reconoce como siguiente punto para alcanzar las demas rutas, la red 192.1.12.0/24 conectada a través de la interfaz serial 2/0, ya que este es el enlace que comunica físicamente ambos dispositivos.

1.2. 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.***

R2(config)#router bgp 2
R2(config-router)#network 192.1.23.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.23.3 remote-as 3
R2(config-router)#
R2(config-router)#end

R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface Loopback 0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#interface Loopback 1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#interface Ethernet 0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#interface serial 2/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#network 3.0.0.0 mask 255.0.0.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3(config-router)#network 192.1.23.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#

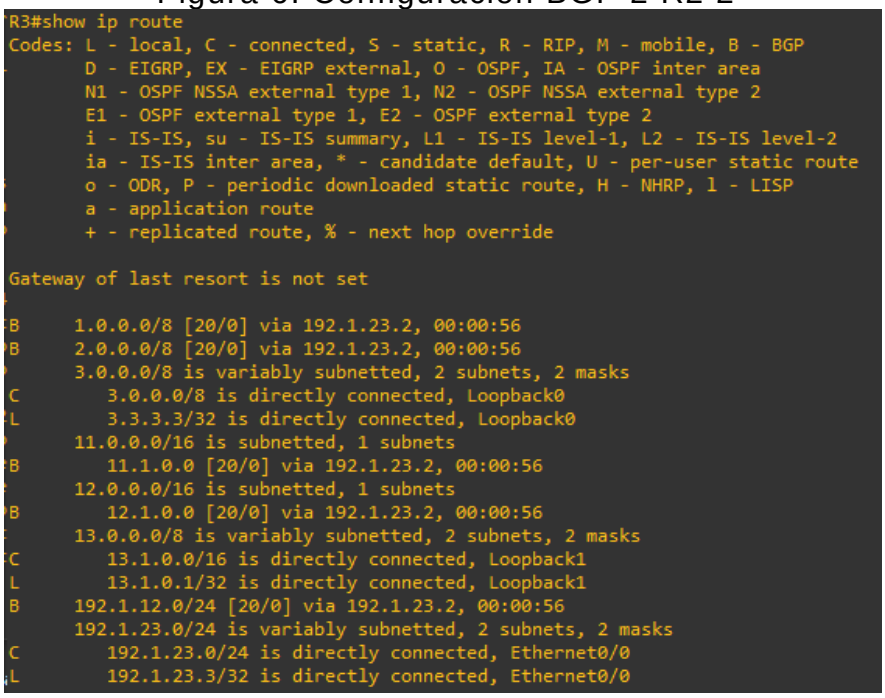
Figura 5: Configuración BGP 2 R2

```
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
       a - application route
       + - 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, 00:02:48
      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
B     3.0.0.0/8 [20/0] via 192.1.23.3, 00:00:22
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.12.1, 00:02:48
      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
      13.0.0.0/16 is subnetted, 1 subnets
B        13.1.0.0 [20/0] via 192.1.23.3, 00:00:22
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial2/0
L        192.1.12.2/32 is directly connected, Serial2/0
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, Ethernet0/0
L        192.1.23.2/32 is directly connected, Ethernet0/0
```

Figura 6: Configuración BGP 2 R2 2



1.3. Configure una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en **AS3** y R4 debería estar en **AS4**. Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como 66.66.66.66. Establezca las relaciones de vecino con base en las direcciones de Loopback 0. Cree rutas estáticas para alcanzar la Loopback 0 del otro router. No anuncie la Loopback 0 en BGP. Anuncie la red Loopback de R4

R3(config)#router bgp 3
R3(config-router)#network 192.1.34.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.34.4 remote-as 4

R4#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#interface Loopback 0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#interface Loopback 1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#interface serial 2/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#router bgp 4
R4(config-router)#bgp router-id 66.66.66.66
R4(config-router)#network 4.0.0.0 mask 255.0.0.0
R4(config-router)#network 14.1.0.0 mask 255.255.0.0

R4(config-router)#network 192.1.34.0 mask 255.255.255.0
R4(config-router)#neighbor 192.1.34.3 remote-as 3

Figura 7: Configuración BGP R4

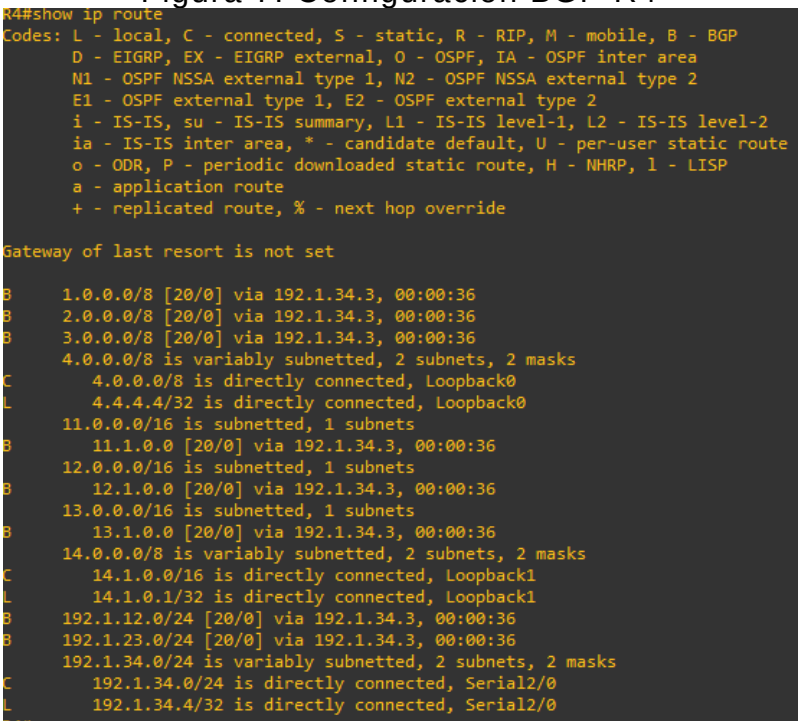
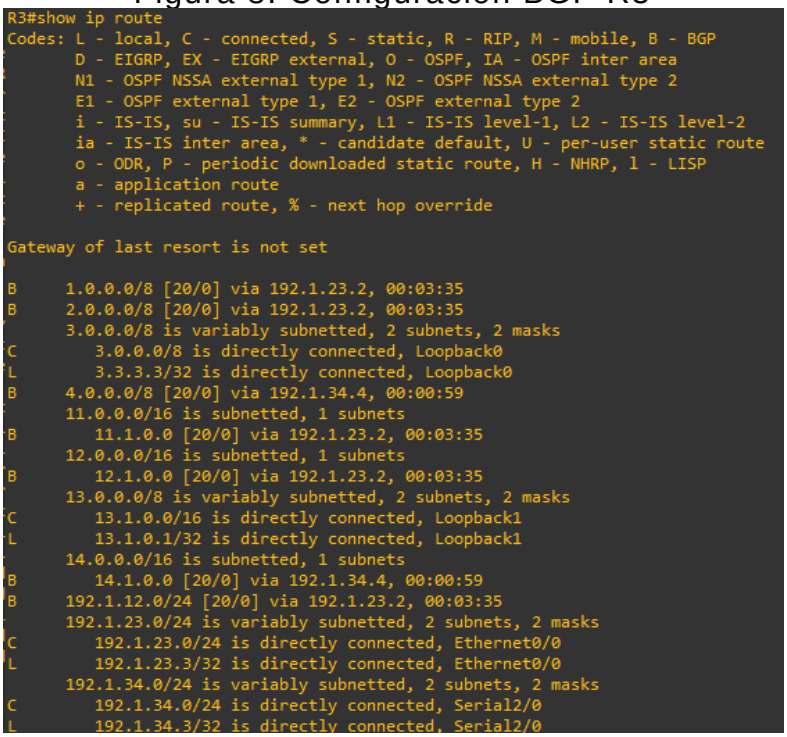


Figura 8: Configuración BGP R3



Mediante las direcciones de Loopback, se puede establecer las relaciones de adyacencia. Para esto el router vecino debe informar sobre el uso de esta interfaz en lugar de una interfaz física. En ese orden de ideas, se realizó una configuración extra para establecer los vecinos:

R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ip route 4.0.0.0 255.0.0.0 192.1.34.4
R3(config)#router bgp 3
R3(config-router)#no neighbor 192.1.34.4
R3(config-router)#no network 3.0.0.0 mask 255.0.0.0
R3(config-router)#neighbor 4.4.4.4 remote-as 4
R3(config-router)#neighbor 4.4.4.4 update-source loopback 0
R3(config-router)#neighbor 4.4.4.4 ebgp-multihop
*May 14 04:43:31.290: %BGP-3-NOTIFICATION: sent to neighbor 192.1.34.4 6/3 (Peer De-configured) 0 bytes
R3(config-router)#neighbor 4.4.4.4 ebgp-multihop

R4#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#ip route 3.0.0.0 255.0.0.0 192.1.34.3
R4(config)#router bgp 4
R4(config-router)#no neighbor 192.1.34.3
R4(config-router)#neighbor 3.3.3.3 remote-as 4
R4(config-router)#neighbor 3.3.3.3 update-source loopback 0
R4(config-router)#neighbor 3.3.3.3 ebgp-multihop

Figura 9: Relación de Adyacencia R3

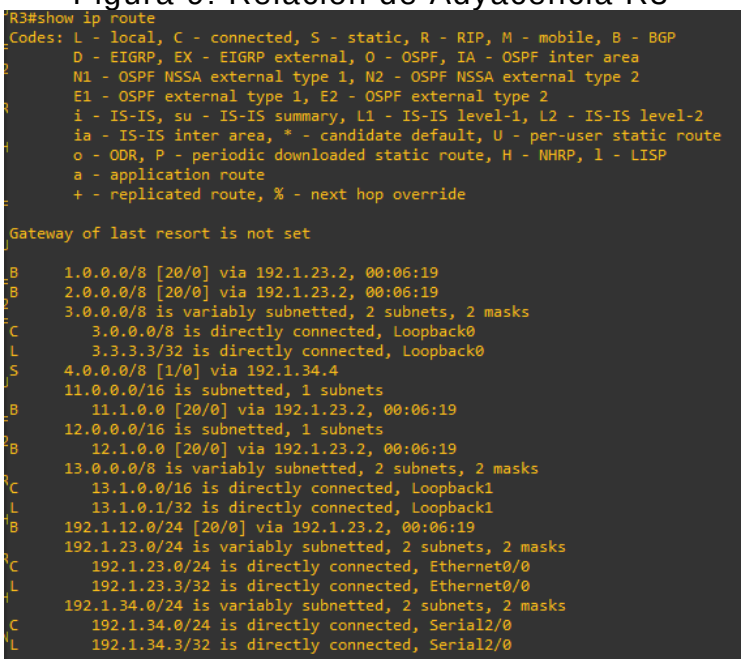


Figura 10: Relación de Adyacencia R4

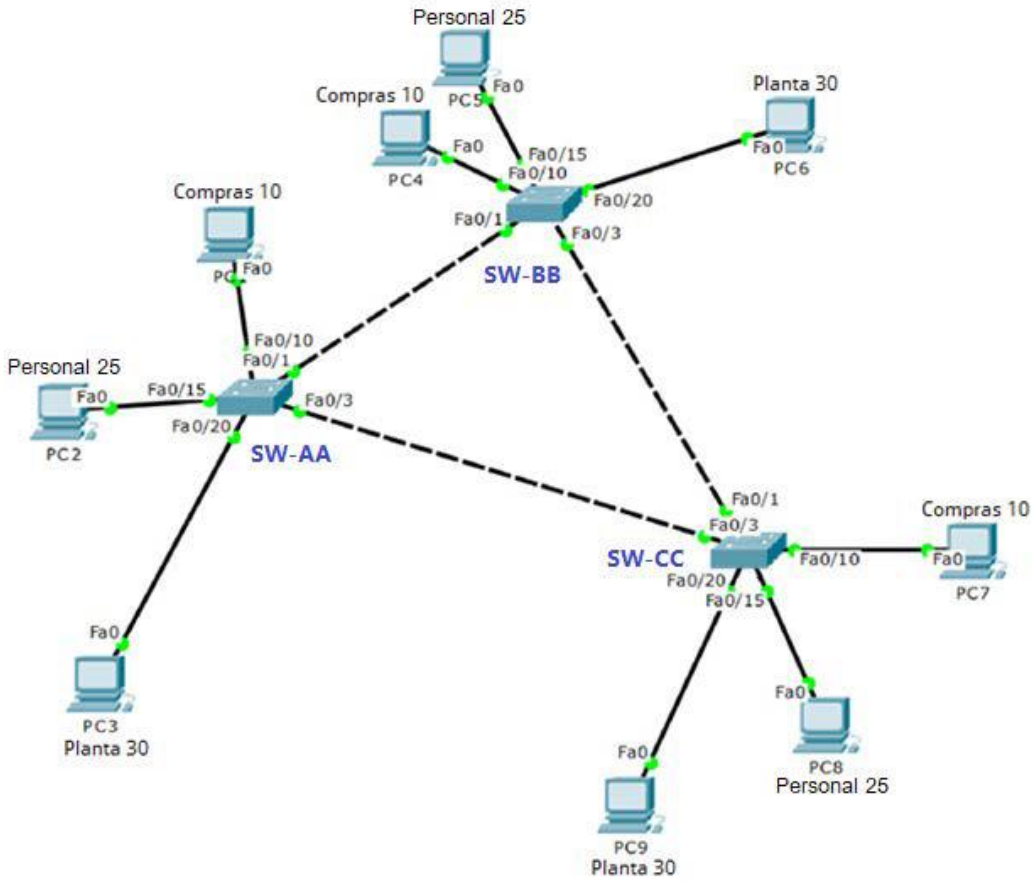
```
R4#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       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
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

S     3.0.0.0/8 [1/0] via 192.1.34.3
      4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        4.0.0.0/8 is directly connected, Loopback0
L        4.4.4.4/32 is directly connected, Loopback0
      14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        14.1.0.0/16 is directly connected, Loopback1
L        14.1.0.1/32 is directly connected, Loopback1
      192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.34.0/24 is directly connected, Serial2/0
L        192.1.34.4/32 is directly connected, Serial2/0
```

ESCENARIO 2

Figura 11: Escenario 2



A. Configurar VTP

1.4. 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.

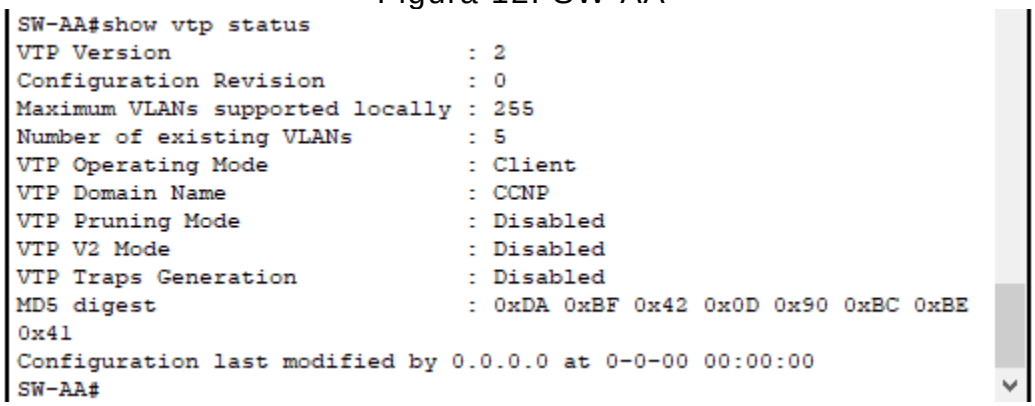
```
SW-AA>enable
SW-AA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-AA(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-AA(config)#vtp password cisco
Setting device VLAN database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

SW-BB>enable
SW-BB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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)#end
SW-BB#

SW-CC>enable
SW-CC#configure terminal
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)#exit
```

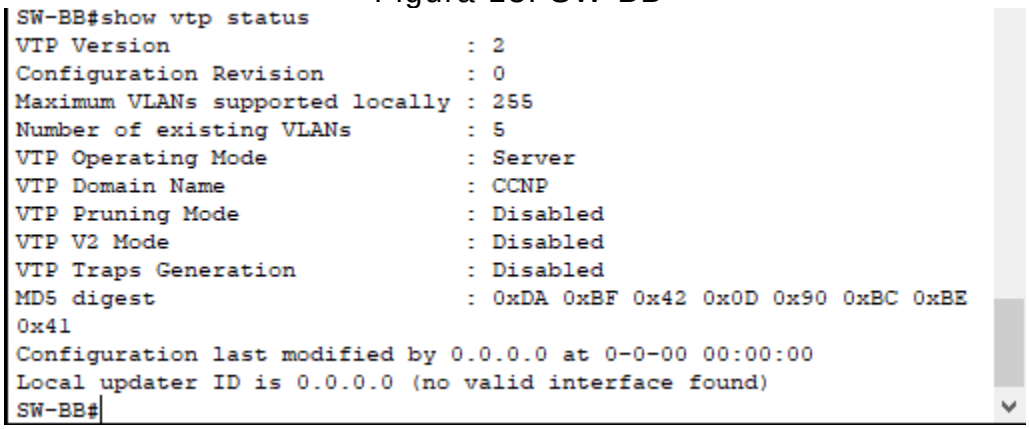
1.5. Verifique las configuraciones mediante el comando ***show vtp status***.

Figura 12: SW-AA



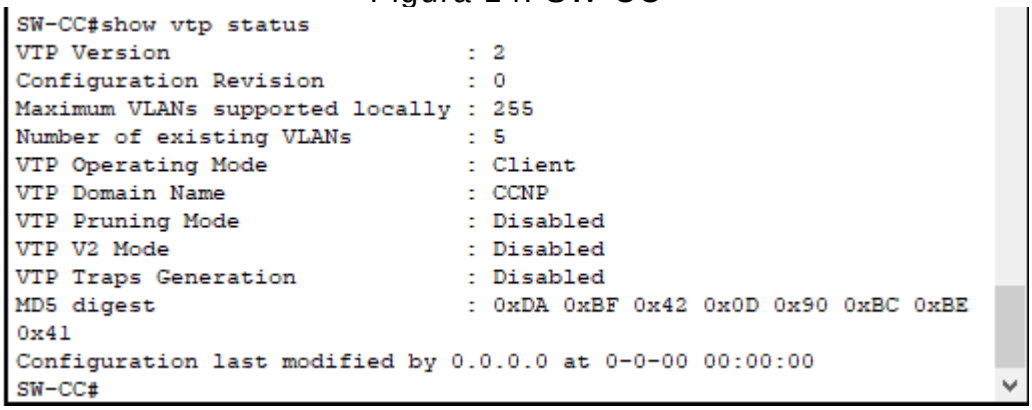
```
SW-AA#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP V2 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 13: SW-BB



```
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 14: SW-CC



```
SW-CC#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE
0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SW-CC#
```

B. Configurar DTP (Dynamic Trunking Protocol)

1.6. 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(config)#inter f0/1
SW-BB(config-if)#switchport mode dynamic desirable
```

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

Figura 15: SW-AA/Trunk

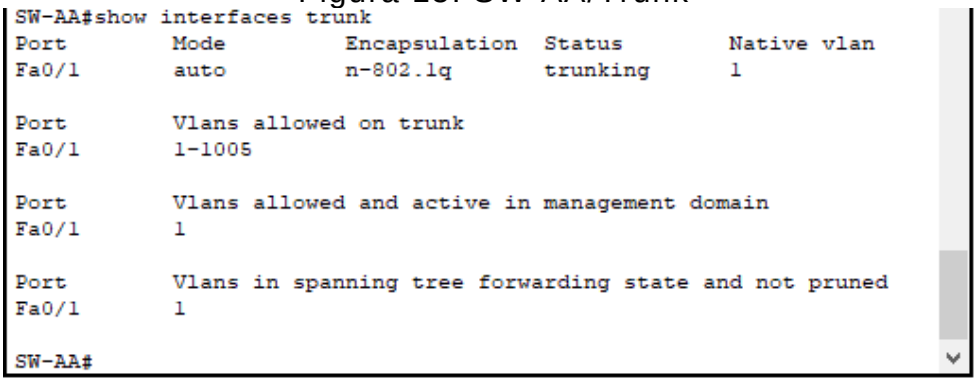
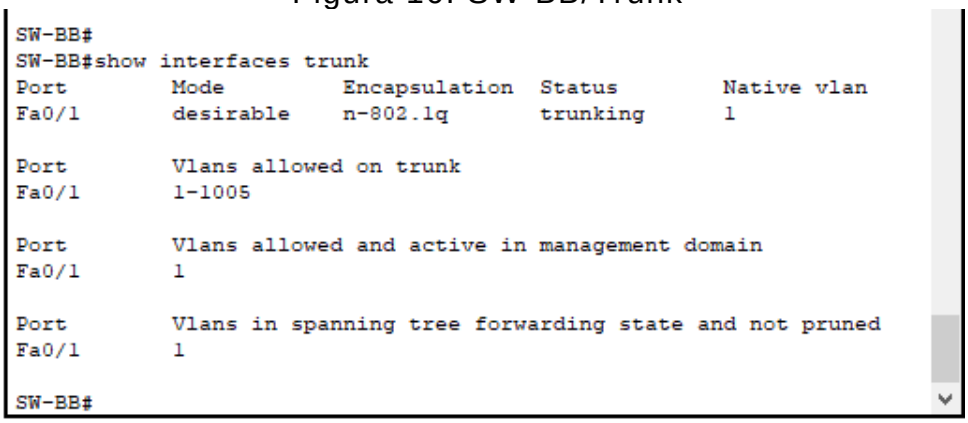


Figura 16: SW-BB/Trunk



1.8. 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#configure terminal
SW-AA(config)#interface fastEthernet 0/3
SW-AA(config-if)#switchport mode trunk
SW-AA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
SW-AA#
%SYS-5-CONFIG_I: Configured from console by console

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

Figura 17: SW-AA/Trunck

```
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#
```

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

SW-CC#configure terminal
SW-CC(config)#interface fastethernet 0/2
SW-CC(config-if)#switchport mode trunk

Figura 18: SW-BB/Trunk

```
SW-BB#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       desirable    n-802.1q       trunking      1
Fa0/2       auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1
Fa0/2       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
Fa0/2       1

SW-BB#
```

Figura 19: SW-CC/Trunk

```
SW-CC#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/2       on           802.1q         trunking      1
Fa0/3       auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/2       1-1005
Fa0/3       1-1005

Port        Vlans allowed and active in management domain
Fa0/2       1
Fa0/3       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/2       none
Fa0/3       none

SW-CC#
```

C. Agregar VLANs y asignar puertos.

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

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

1.12. Verifique que las VLANs han sido agregadas correctamente.

Figura 20: SW-BB/VLAN

```
SW-BB#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   Compras                          active
25   Personal                         active
30   Planta                           active
99   Admon                            active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SW-BB#
```

Figura 21: SW-AA/VLAN

```
SW-AA#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   Compras                          active
25   Personal                         active
30   Planta                           active
99   Admon                            active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SW-AA#
```

Figura 22: SW-CC/VLAN

```
SW-CC#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   Compras                          active
25   Personal                         active
30   Planta                           active
99   Admon                            active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SW-CC#
```

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

Tabla 5: Puertos VLANs

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

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

1.15. 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#conf ter
SW-AA(config)#interface fastethernet 0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#exit
SW-AA(config)#interface fastethernet 0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#exit
SW-AA(config)#interface fastethernet 0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
SW-AA(config-if)#
SW-AA#

SW-BB#conf ter
SW-BB(config)#interface fastethernet 0/10
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#exit
SW-BB(config)#interface fastethernet 0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#exit
SW-BB(config)#interface fastethernet 0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30
SW-BB(config-if)#exit
SW-BB(config)#

SW-CC#conf ter
SW-CC(config)#interface fastethernet 0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#exit
SW-CC(config)#interface fastethernet 0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#exit
SW-CC(config)#interface fastethernet 0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30
SW-CC(config-if)#exit
SW-CC(config)#

PC1: ip address 190.108.10.1 255.255.255.0
PC2: ip address 190.108.20.2 255.255.255.0
PC3: ip address 190.108.30.3 255.255.255.0
PC4: ip address 190.108.10.4 255.255.255.0
PC5: ip address 190.108.20.5 255.255.255.0
PC6: ip address 190.108.30.6 255.255.255.0
PC7: ip address 190.108.10.7 255.255.255.0
PC8: ip address 190.108.20.8 255.255.255.0
PC9: ip address 190.108.30.9 255.255.255.0

D. Configurar las direcciones IP en los Switches.

1.16. 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: Direcciones IP

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

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

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

E. Verificar la conectividad Extremo a Extremo

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

Cuando se hizo Ping entre los PCs de diferentes VLANs el comando no fue exitoso; mientras que al hacerlo entre PCs de la misma VLAN, si lo fue.
Para que el ping pueda funcionar entre todos los PCs es necesario añadir un switch de capa 3 el cual permite el enrutamiento entre VLANs y asi establecer el tráfico ICMP entre las diferentes redes.

Figura 23: PC2

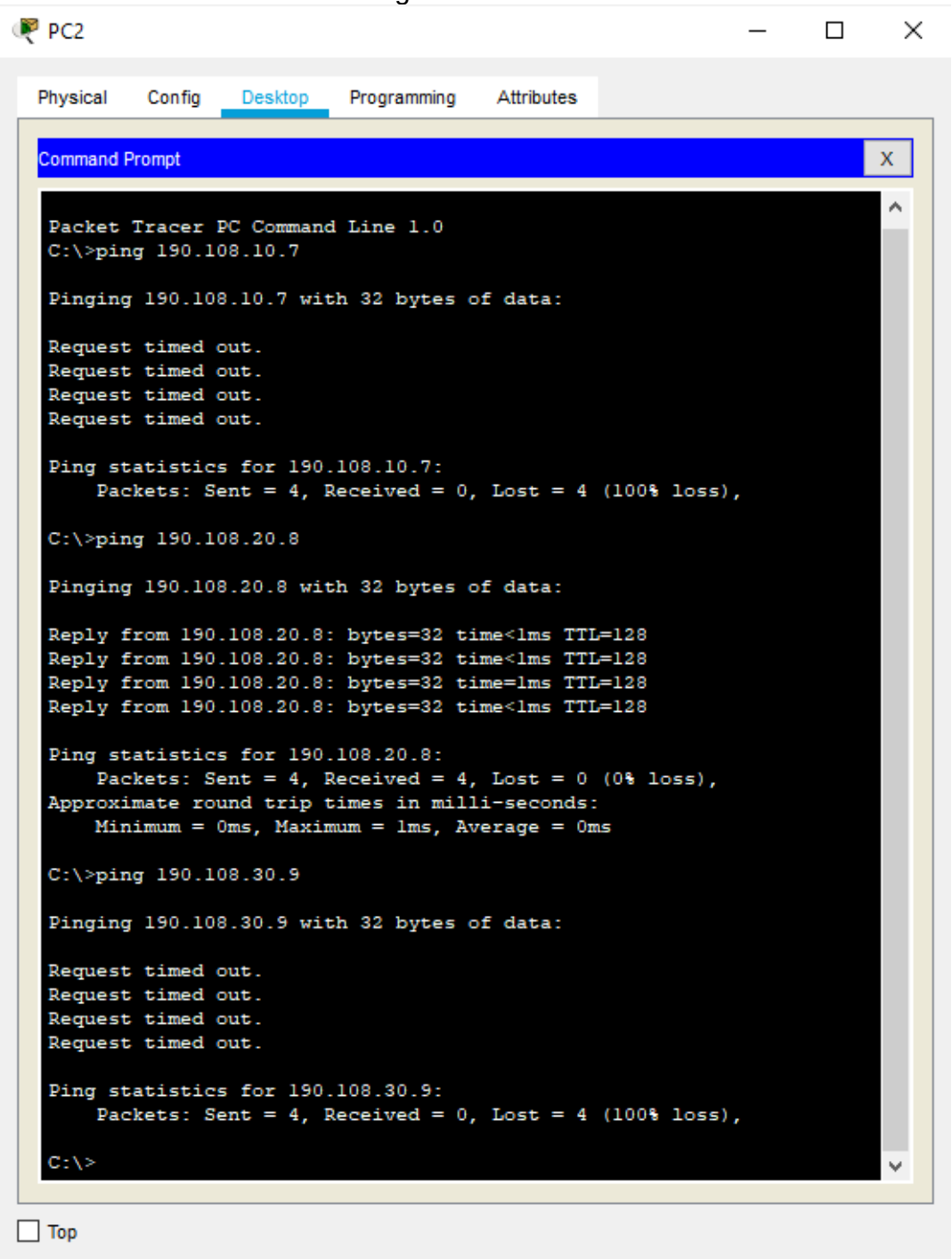


Figura 24: PC4

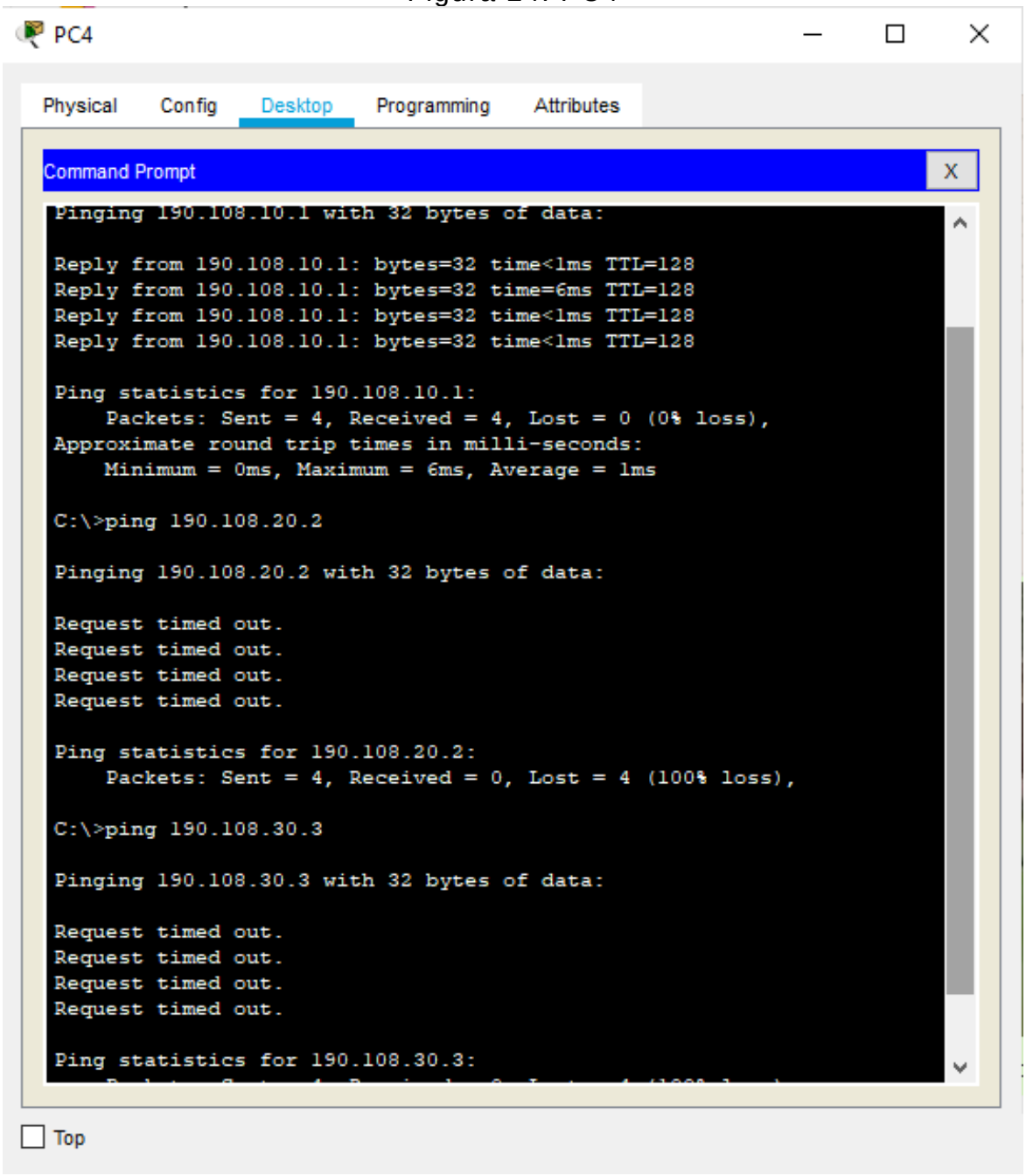
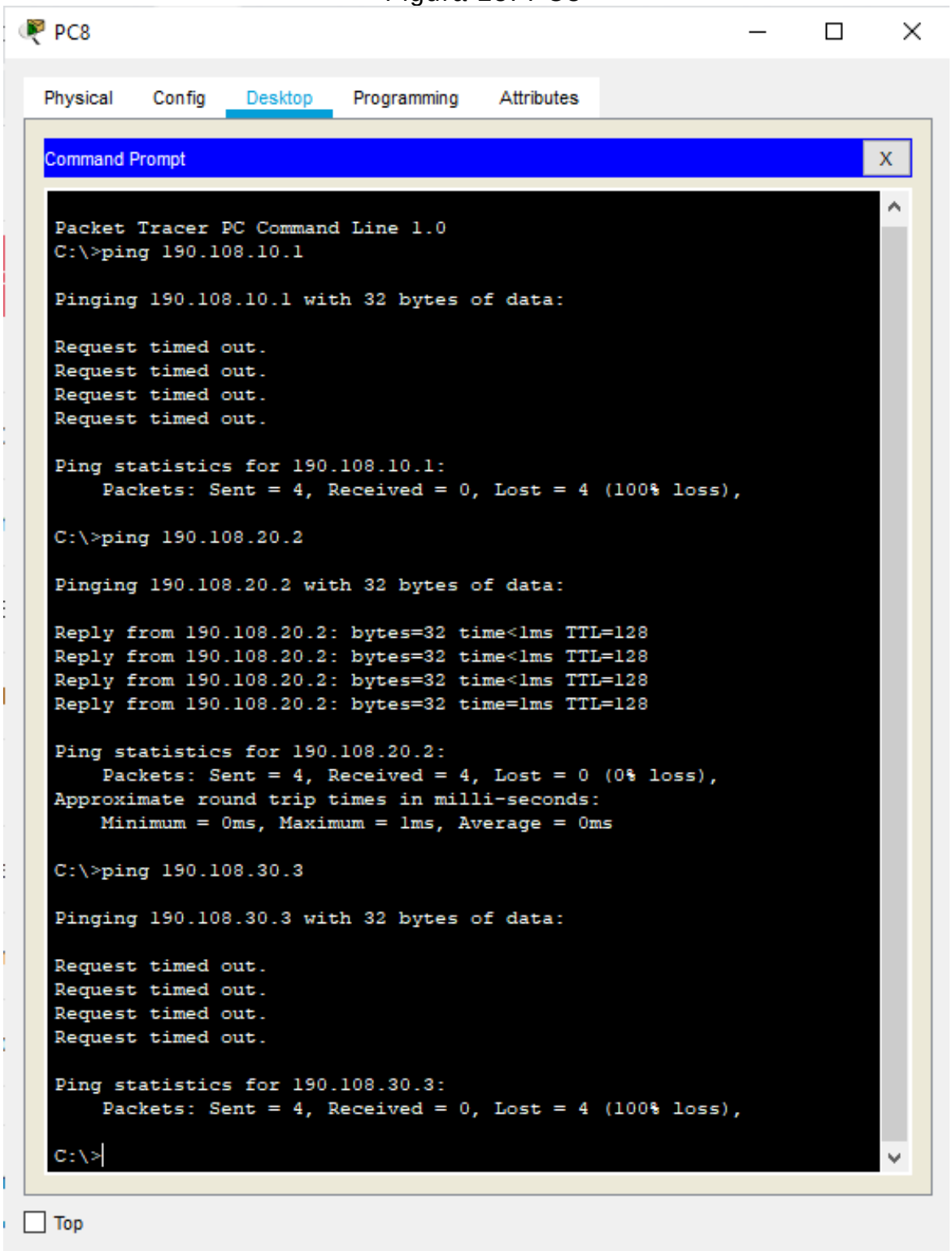


Figura 25: PC8



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

En este caso las interfaces físicas llevan los datos enviados a través del protocolo ICMP entre los tres Switches que están configurados en modo troncal. Al hacer Ping entre los Switches el proceso tuvo éxito. También al verificar con el comando ***show interfaces trunk***, se confirmó que comparten el mismo tipo de encapsulamiento y se estan en modo compatible. A pesar de lo anterior, es necesario implementar el comando ***switchport trunk allowed vlan except "vlan id"***, en las interfaces que conectan los Switches, para establecer el permiso a las VLANs creadas.

Figura 26: SW-AA/Ping 2

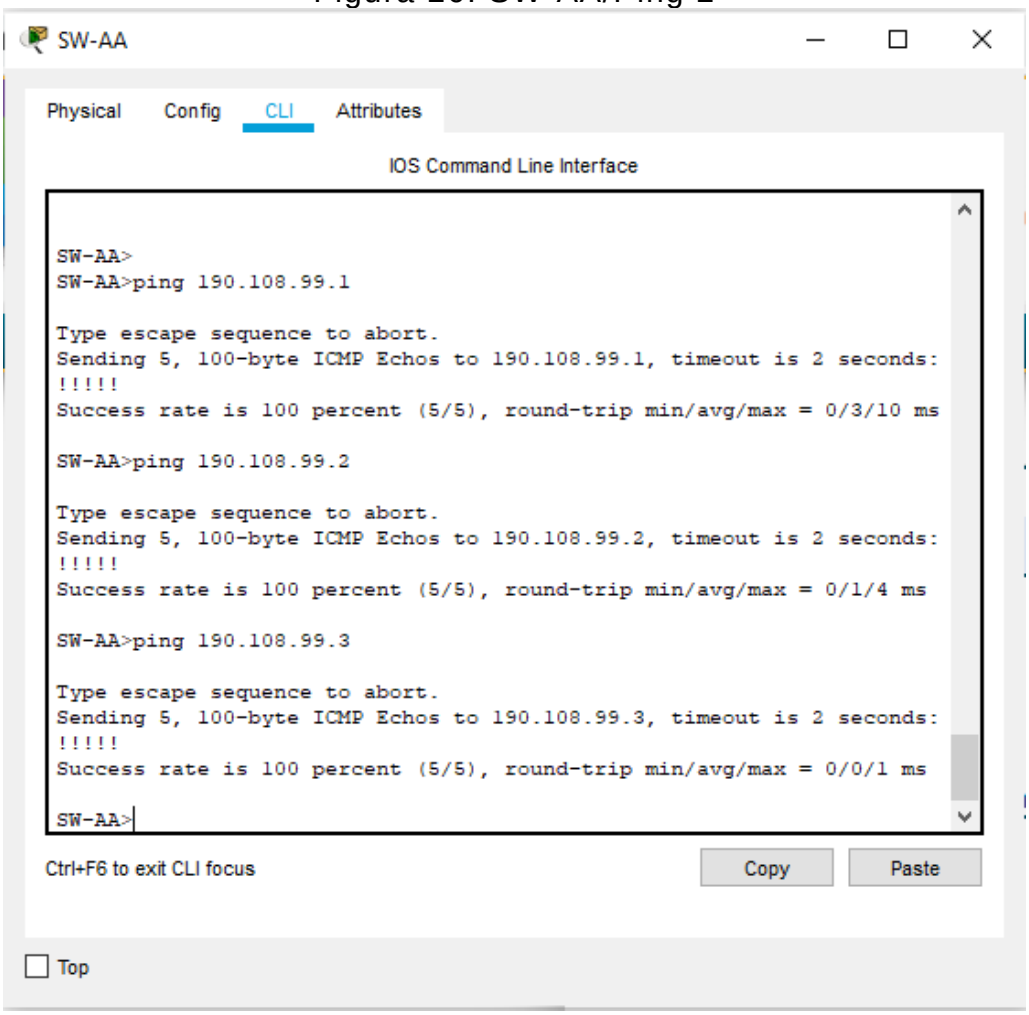


Figura 27: SW-BB/Ping 1

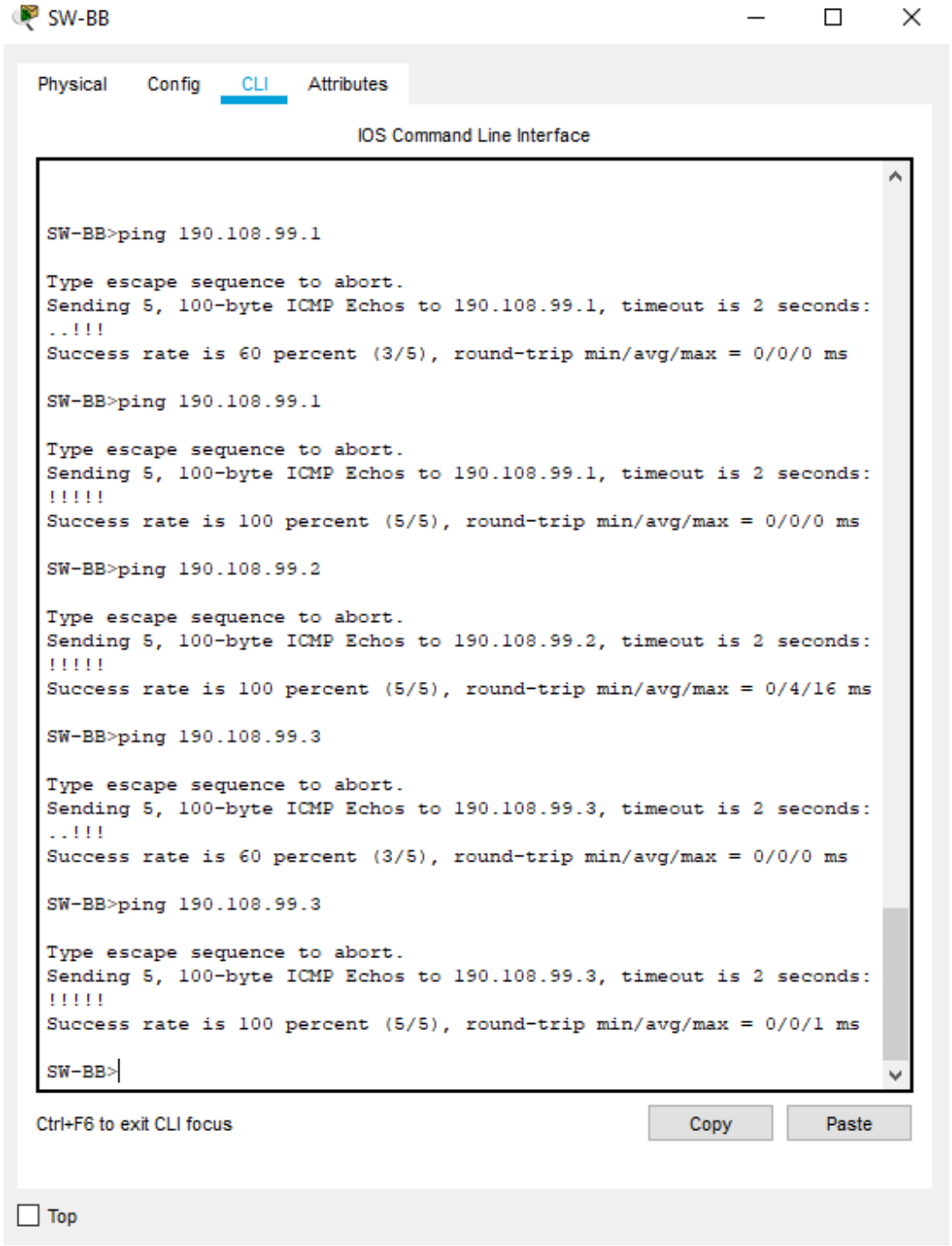
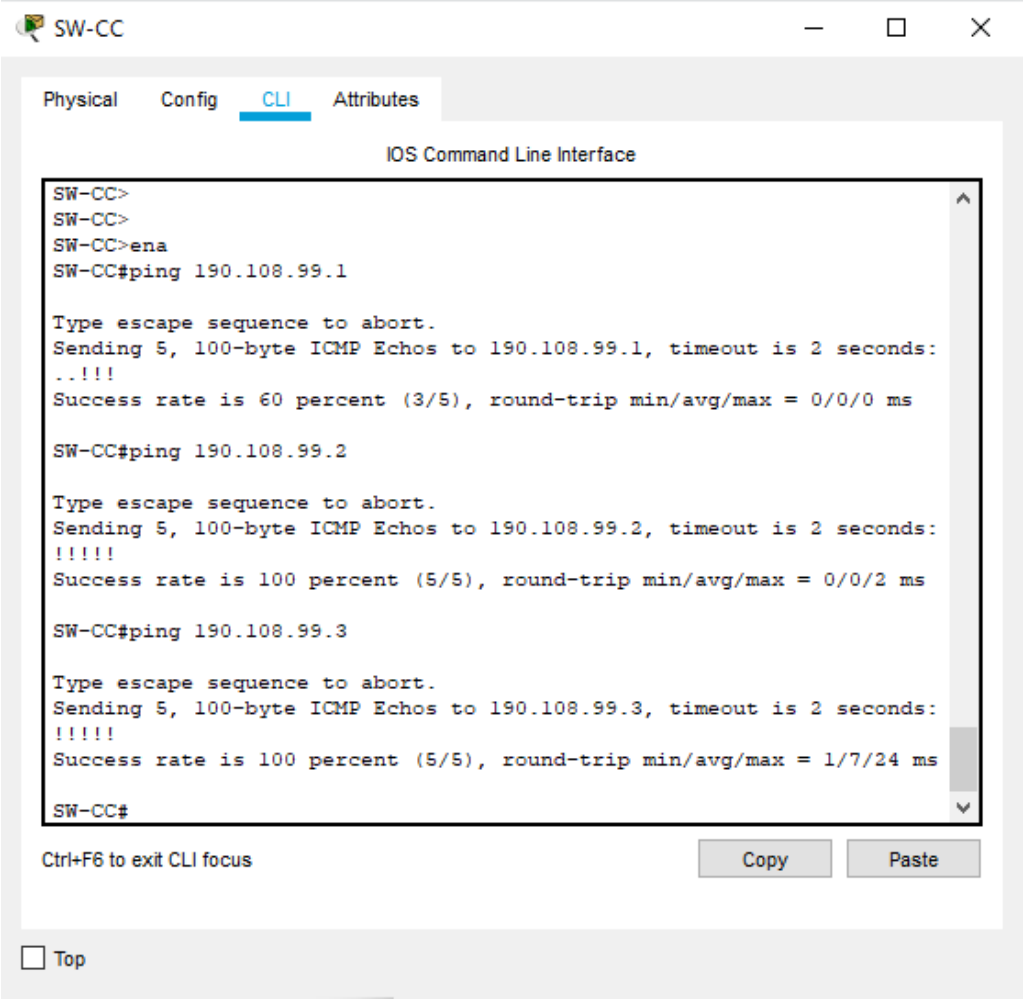


Figura 28: SW-CC/Ping 1



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

Para este paso no hubo éxito al ejecutar el comando ping entre los PCs y Switches. Aunque las VLANs estan habilitadas en todos los Switches a través del protocolo VTP, y que se configuraron todas las interfaces para conectar los switches a los PCs en modo de acceso de acuerdo con la VLAN que pertenecen, no existe el enrutamiento IP en las VLANs creadas para el caso: 10 Compras, 25 Personal y 30 Planta. Esto se solucionaría al configurar una dirección IP y una máscara de subred en cada una de las interfaces VLAN de los Switches, pero esta debe pertenecer al mismo segmento de red al que pertenece el PC que se conecta a cada VLAN incluyendo una VLAN nativa para dichas interfaces.

Figura 29: SW-AA/Ping PC1

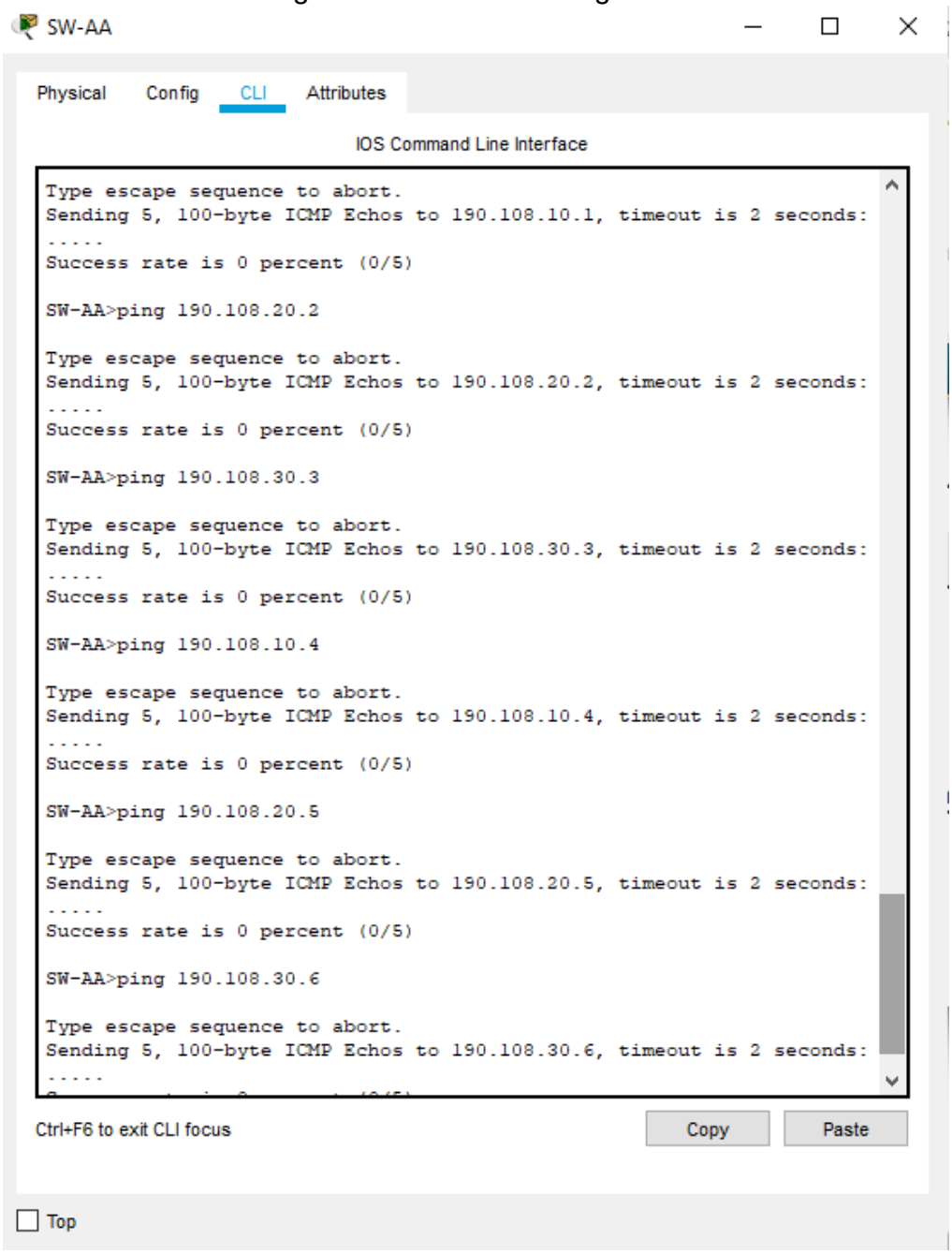


Figura 30: SW-BB/Ping PC2

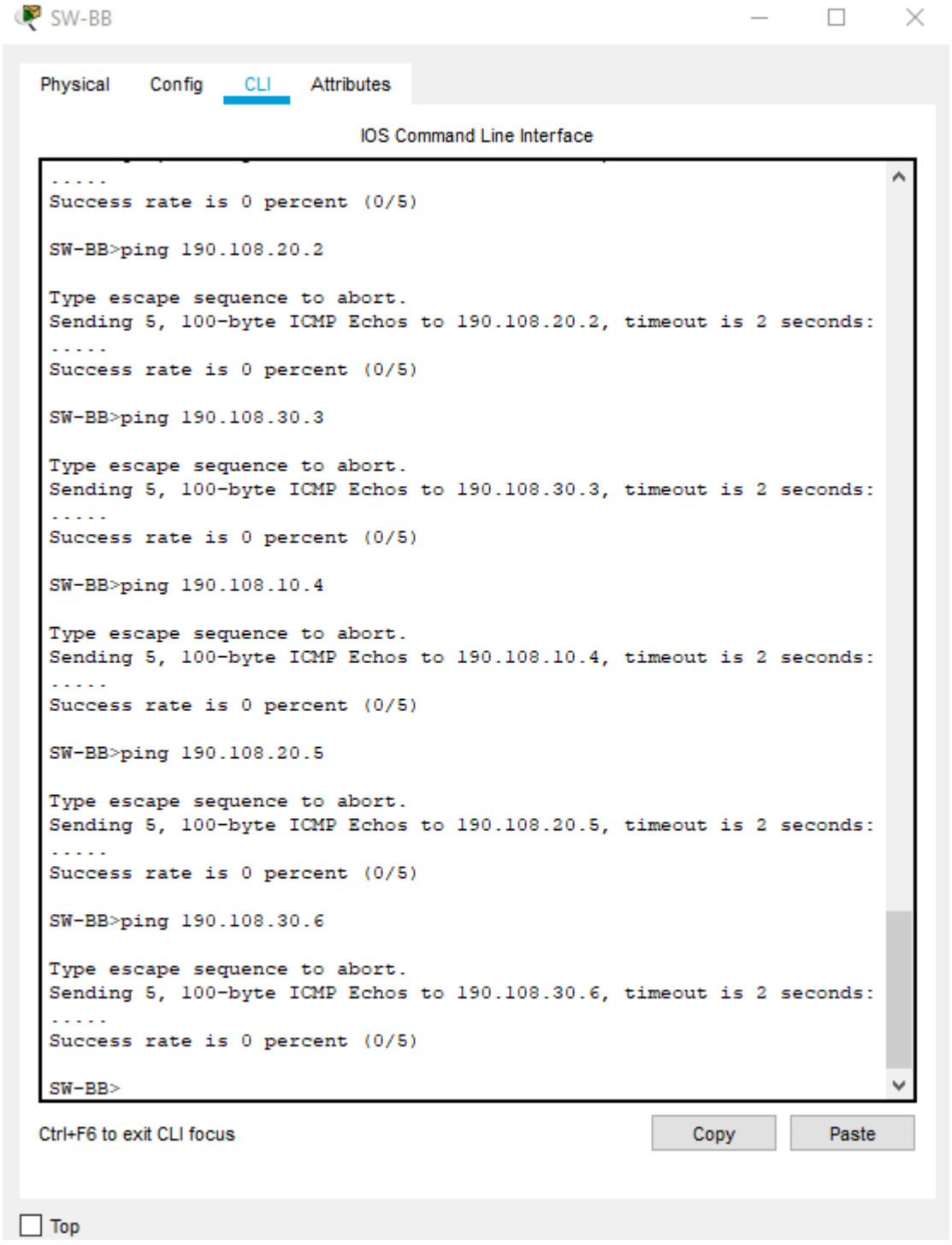
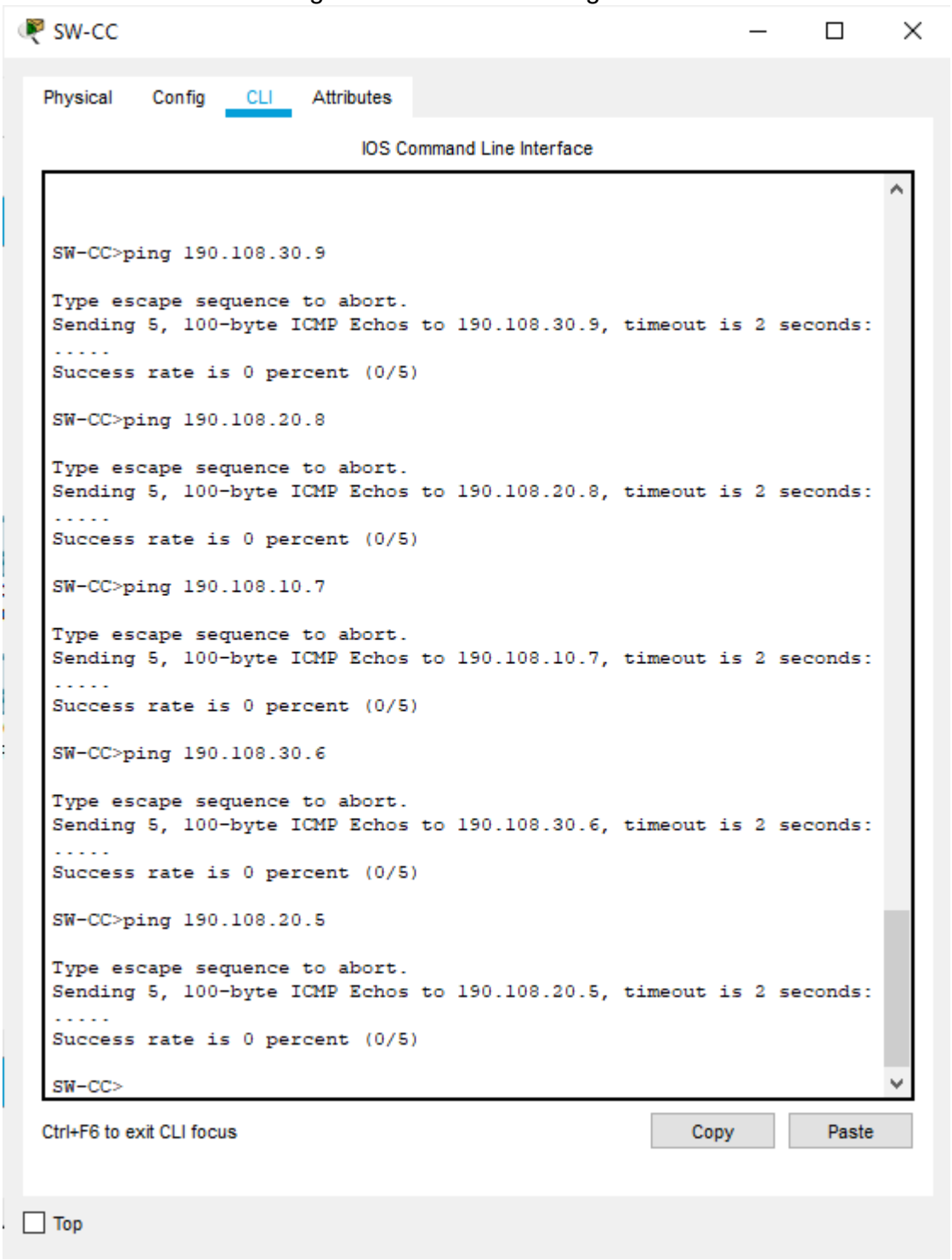


Figura 31: SW-CC/Ping PC2



CONCLUSIONES

Dentro de la prueba de habilidades se ha demostrado de manera práctica que se han adquirido las competencias expuestas a lo largo del curso. Mediante los 2 escenarios propuestos se busca poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking tanto en routing como en switching.

El comando *show ip route* además de mostrar la información de las redes, enrutamiento e interfaces, es muy útil para la resolución de problemas de enrutamiento.

Las interfaces físicas que enrutan los datos enviados a través del protocolo ICMP entre los tres Switches están configuradas en modo troncal. Mediante el uso del comando show interfaces trunk, se evidenció que comparten el mismo tipo de encapsulamiento, por lo cual se encuentran en un modo compatible.

Se presento error de Ping en los PCs de diferentes VLANs; esto sucede porque cada PC pertenece a un segmento de red diferente. Por esto, para lograr establecer comunicación entre estos PCs, es necesario incluir en la topología de la red un enrutador o un Switch de capa 3 (Switch Multicapa), los cuales tienen la funcionalidad de enrutamiento entre VLANs, para así lograr comunicar el tráfico ICMP entre las diferentes redes propuestas en la tabla de enrutamiento para estos dispositivos.

Cuando se hizo ping entre los Switches y los PCs no fueron exitosos. Porque, aunque tienen habilitadas las VLANs en cada uno de los Switches con el protocolo VTP y también se configuraron todas las interfaces que conectan los switches a los PCs en modo de acceso con la VLAN correspondiente, todavía no se configura un enrutamiento IP ente las VLANs creadas.

Se pudo evidenciar la ventaja del protocolo BGP porque permite intercambiar la información de encaminamiento entre sistemas autónomos. Esto es muy utilizado por los ISPs, por que están compuestos de varios de estos.

BIBLIOGRÁFIA

Donohue, D. (2017). CISCO Press (Ed). CCNP Quick Reference. Recuperado de https://1drv.ms/b/s!AgIGg5JUgUBthFt77ehzL5qp0OKD

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

Hucaby, D. (2015). CISCO Press (Ed). CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. Recuperado de https://1drv.ms/b/s!AgIGg5JUgUBthF16RWCSsCZnfDo2

Macfarlane, J. (2014). Network Routing Basics: Understanding IP Routing in Cisco Systems. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live

UNAD (2015). Switch CISCO Security Management [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IlyVeVJCCezJ2QE5c