DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

CLAUDIA LORENA MARCIALES GONZALEZ

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

CLAUDIA LORENA MARCIALES GONZALEZ

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 *TELECOMUNICACIONES*
BOGOTA
2020

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

BOGOTA, 08 de mayo de 2020

AGRADECIMIENTOS

A Dios por darme la oportunidad de vivir y por estar conmigo en cada paso y proyecto de vida, por ser mi fortaleza en los momentos de debilidad.

A mis hijas Nataly y Juliana por toda su colaboración, apoyo incondicional e impulso en todo momento para lograr mi objetivo, por apoyarme siempre y por ser la parte más importante de mi vida y representar la unidad familiar.

A la Universidad Nacional Abierta y a Distancia UNAD por darme la oportunidad de culminar mi carrera.

A mi profesor Raúl Camacho Briñez, líder nacional del programa Ingeniería de Telecomunicaciones. ECBTI, por su asesoría en mi proceso formativo.

Igualmente me gustaría agradecer a mis todos los tutores durante mi carrera porque todos aportaron con sus asesorías a lograr mi objetivo.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

LOOPBACK: Es una interfaz de red virtual las cuales señalan que las direcciones del rango 127.0.0.0 son direcciones de loopback. Generalmente se utiliza la 127.0.0.1 al ser la primera del rango. Son redefinidas en los dispositivos incluso en las direcciones IP públicas.

VTP: Son las siglas de VLAN Trunking Protocol, 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

ROUTER: Dispositivo que permite la interconexión de redes al nivel de la capa de red del modelo de referencia OSI.

ENRUTAMIENTO: Proceso en el que los enrutadores aprenden sobre redes remotas, encuentran todas las rutas posibles para llegar a ellas y luego escogen las mejores rutas para intercambiar datos entre las mismas.

SWITCHES: Se utilizan para conectar múltiples dispositivos de la misma red dentro de un edificio o campus. un switch puede conectar varios ordenadores, impresoras y servidores, creando una red de recursos compartidos. El switch actuará como un controlador, permitiendo a los diferentes dispositivos compartir información y comunicarse entre sí. Mediante el uso compartido de información y la asignación de recursos, los switches permiten ahorrar dinero y aumentar la productividad.

VLAN: (Virtual LAN) agrupa lógicamente dispositivos en un mismo dominio de broadcast, creando lógicamente distintas redes como si fueran distintas redes físicas, sirve para reducir la sobrecarga de CPU en cada dispositivo reduciendo el número de dispositivos que recibirá la trama de broadcast.

IGRP: Es un protocolo patentado desarrollado por Cisco que permite que varias puertas de enlace coordinen su enrutamiento el cual es estable incluso en redes muy grandes o complejas. No deben ocurrir bucles de enrutamiento, incluso como transitorios.

EIGRP: (Enhanced Interior Gateway Routing Protocol) es una versión mejorada de IGRP. La tecnología de vector distancia que se usa en IGRP también se emplea en EIGRP. Además, la información de la distancia subyacente no presenta cambios. Las propiedades de convergencia y la eficacia de operación de este protocolo han mejorado significativamente. Esto permite una arquitectura mejorada y, a la vez, retiene la inversión existente en IGRP.

GATEWAY: Traducido al español como “puerta de enlace” es un nodo de red que conecta dos redes que utilizan diferentes protocolos. Mientras que un puente se utiliza para unir dos tipos similares de redes, un gateway se utiliza para unir dos redes diferentes.

FIREWALL: Dispositivo de contención entre dos redes. Un Firewall o Cortafuegos puede residir en un solo ruteador que filtra los paquetes no deseados o puede usar varias tecnologías en diversas combinaciones de ruteadores y servidores. Varios Firewalls incluyen funciones de filtrado de paquetes y Traducción de Direcciones de Red (NAT).

RESUMEN

Esta prueba de habilidades hace parte de la culminación del Diplomado de Profundización CCNP, donde podemos dejar plasmados no solo el conocimiento adquirido si no las experiencia adquirida en la comprensión de redes e internet, puntualmente conceptos básicos y diseño de redes, arquitectura de redes de campus, conmutación, implementaciones de Spanning Tree (STP), configuración de enrutamiento Inter-VLANs, Implementación de redes de alta disponibilidad y redundancia de primer salto así como la seguridad de redes de campus. En estos 2 ejercicios teórico prácticos podemos aplicar estos conceptos previamente analizados y así darle una correcta solución, Igualmente, estos conocimientos llevan al desarrollo de habilidades para planificar, implementar, verificar y resolver problemas de redes locales lo cual nos hace ser profesionales altamente calificados abriendo campo laborar como profesionales distinguidos en el mundo del networking permitiendo que seamos pieza clave en esta transformación digital y así culminar con la presentación de la certificación para ser profesionales expertos en Configuración de Redes Cisco CCNP reconocidos internacionalmente .

Palabras claves: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica

ABSTRACT

This skills test is part of the culmination of the CCNP Deepening Diploma, where we can reflect not only the knowledge acquired but also the experience gained in understanding networks and the internet, specifically basic concepts and network design, campus network architecture, switching, Spanning Tree (STP) deployments, Inter-VLAN routing configuration, Deployment of high availability networks and first-hop redundancy as well as campus network security. In these 2 practical theoretical exercises we can apply these previously analyzed concepts and thus give you a correct solution. Likewise, this knowledge leads to the development of skills to implement, implement, verify and solve local network problems, which makes us highly qualified professionals opening the field. To work as distinguished professionals in the world of networking that we are a key player in this digital transformation and thus culminate with the presentation of certification for internationally recognized experts in Network Configuration Cisco CCNP.

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

INTRODUCCIÓN

Durante el desarrollo del este diplomado de profundización cisco adquirimos habilidades para planificar, implementar, verificar y resolver problemas de redes locales divididos en 4 fases en donde se profundizo la configuración de los diferentes parámetros de EIGRP, los comandos Stub, RIPng. Al igual que la configuración de direccionamiento IPV6. se emplea herramientas de simulación como GNS3 y laboratorios de acceso remoto con el fin de establecer escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de múltiples protocolos, evaluando el desempeño de los routers, mediante el uso de comandos de administración avanzados y bajo el uso de protocolos de vector distancia y estado de enlace.

Así mismo, configuración de VLANS estático, Trunking, VTP y EtherChannel se analiza como implementar VLAN en las redes del campus, así como configurar y optimizar la alta disponibilidad y redundancia en los conmutadores para proporcionar redundancia de Capa 3, describir e implementar características de seguridad de LAN.

Para colocar en práctica y adquirir nuevas habilidades se realizara el desarrollo de los dos ejercicios propuestos representados en escenarios, donde se aplica el direccionamiento, protocolos de enrutamiento, interfaces, vlans, se configuran relaciones de vecinos BGP,VTP y DTP; actividades desarrolladas en packet tracer. Se realizara verificación deconectividad mediante pruebas con el uso de los comandos ping, traceroute, show ip route,show run para vericicar la configuración completa y detallada de los switch y router cisco implementado en los escenarios

DESARROLLO

1. Escenario 1

Figura 1. Escenario 1

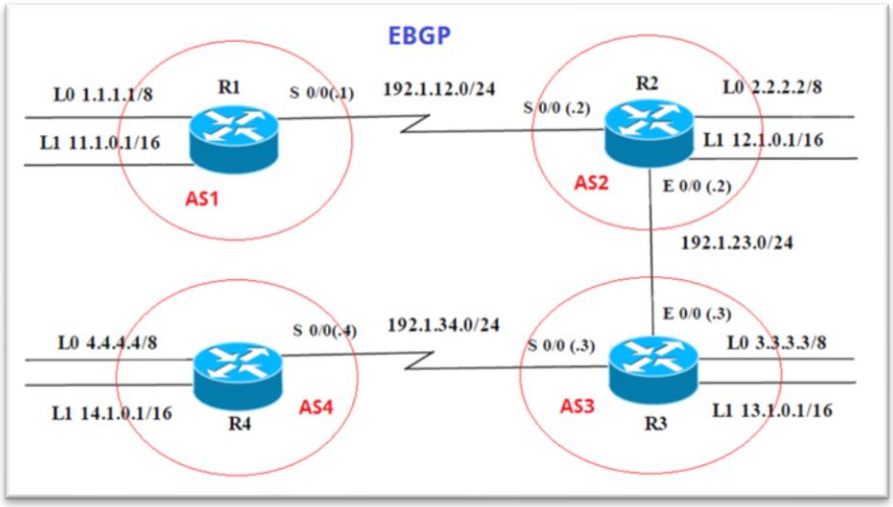
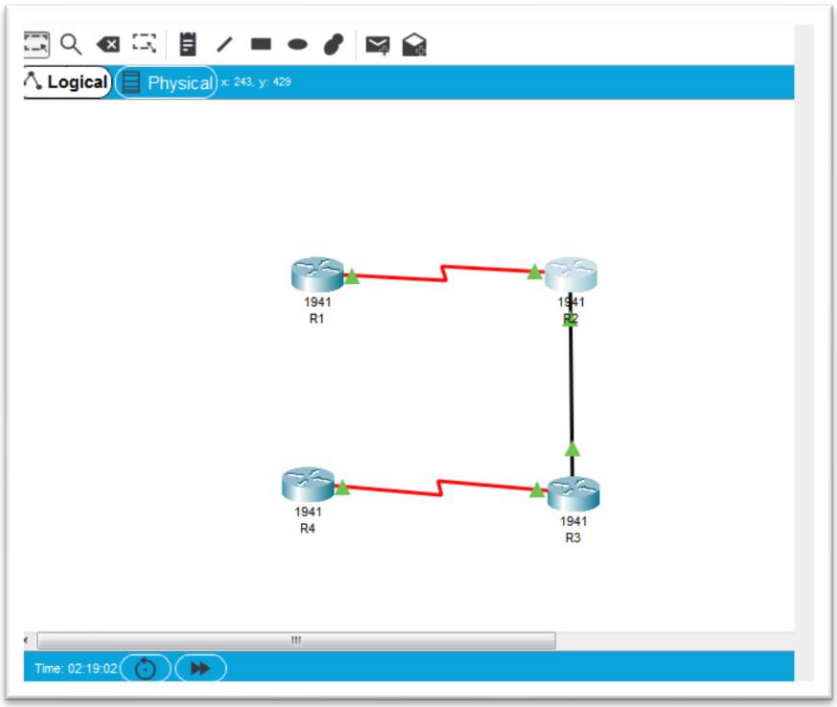


Figura 2. Simulación de escenario 1



Información para configuración de los Routers

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 0/0	192.1.12.1	255.255.255.0

Tabla 1. configuración de los Routers R1

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 0/0	192.1.12.2	255.255.255.0
E 0/0	192.1.23.2	255.255.255.0

Tabla 2. configuración de los Routers R2

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 0/0	192.1.34.3	255.255.255.0

Tabla 3. configuración de los Routers R3

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 0/0	192.1.34.4	255.255.255.0

Tabla 4. configuración de los Routers R4

Configuración IP´s R1

Router>en
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#in s0/0/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#clock rate 64000
R1(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#
R1(config-if)#int lo 0
R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R1(config-if)#ip add 1.1.1.1 255.0.0.0
R1(config-if)#
R1(config-if)#int loo 1
R1(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
R1(config-if)#ip add 11.1.0.1 255.255.0.0
R1(config-if)#

Configuración IP´s R2

```
Router>en
Router#
Router#
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#hostname R2
R2(config)#
R2(config)#in s0/0/0
R2(config-if)#ip add 192.1.12.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
R2(config-if)#
R2(config-if)#in f0/0
R2(config-if)#ip add 192.1.23.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
R2(config-if)#
R2(config-if)#int lo 0
R2(config-if)#ip add 2.2.2.2 255.0.0.0
R2(config-if)#int lo 1
R2(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state
to up
R2(config-if)#ip add 12.1.0.1 255.255.0.0
R2(config-if)#
R2(config-if)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

Configuración IP´s R3

```
Router>
Router>en
Router#
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
        Router(config)#hostname R3
```

```
R3(config)#
R3(config)#in s0/0/0
R3(config-if)#ip add 192.1.34.3 255.255.255.0
R3(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R3(config-if)#
R3(config-if)#in f0/0
R3(config-if)#ip add 192.1.23.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
R3(config-if)#int lo 0
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state
to up
R3(config-if)#ip add 3.3.3.3 255.0.0.0
R3(config-if)#int lo 1
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state
to up
R3(config-if)#ip add 13.1.0.1 255.255.0.0
R3(config-if)#
R3(config-if)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

Configuarción IP´s R4

```
Router>en
Router#
Router#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R4
R4(config)#in s0/0/0
R4(config-if)#ip add 192.1.34.4 255.255.255.0
R4(config-if)#clock rate 64000
R4(config-if)#no shut
R4(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
```

```
R4(config-if)#
R4(config-if)#int lo 0
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
R4(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state
to up
R4(config-if)#ip add 4.4.4.4 255.0.0.0
R4(config-if)#
R4(config-if)#int lo 1
R4(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state
to up
R4(config-if)#ip add 14.1.0.1 255.255.0.0
R4(config-if)#^Z
R4#
%SYS-5-CONFIG_I: Configured from console by console
```

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.***

   Solución

```
R1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#
R1(config)#router bgp 1
R1(config-router)#no synchronization
R1(config-router)#bgp router-id 11.11.11.11
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)#
R1(config-router)#^Z
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
R2>en
R2#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#
R2(config)#router bgp 2
R2(config-router)#no synchronization
R2(config-router)#bgp router-id 22.22.22.22
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.12.1 Up
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)#
R2(config-router)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

Figura 3. Relación de vecino BGP entre R1 y R2. R1

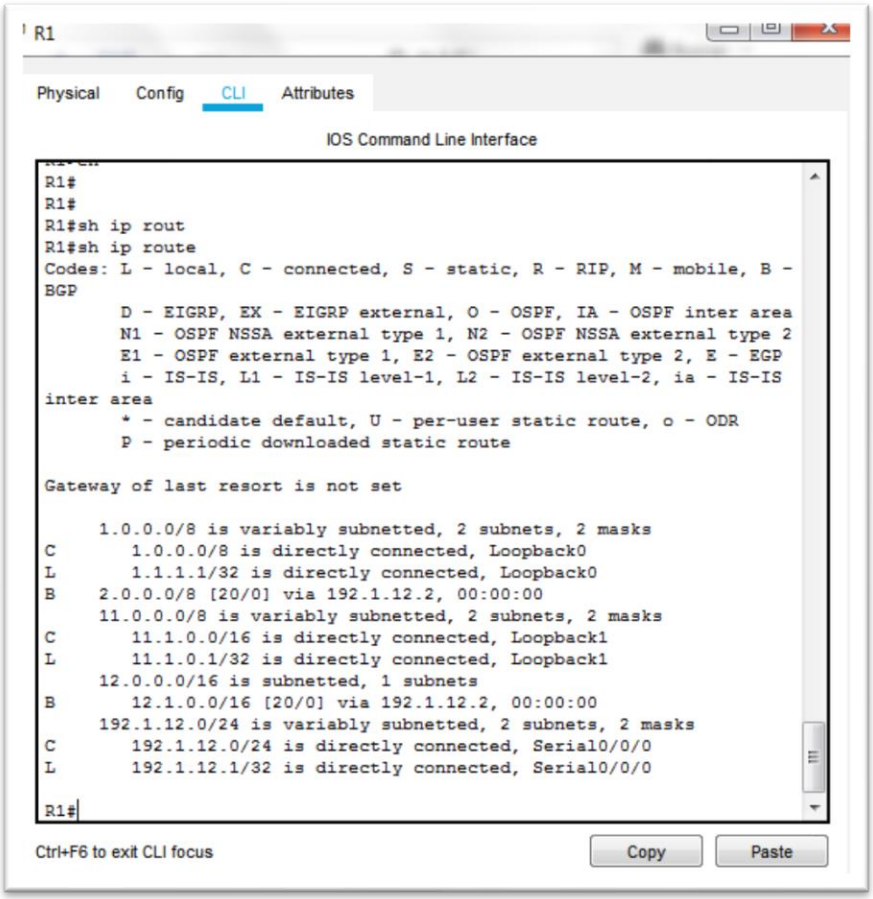
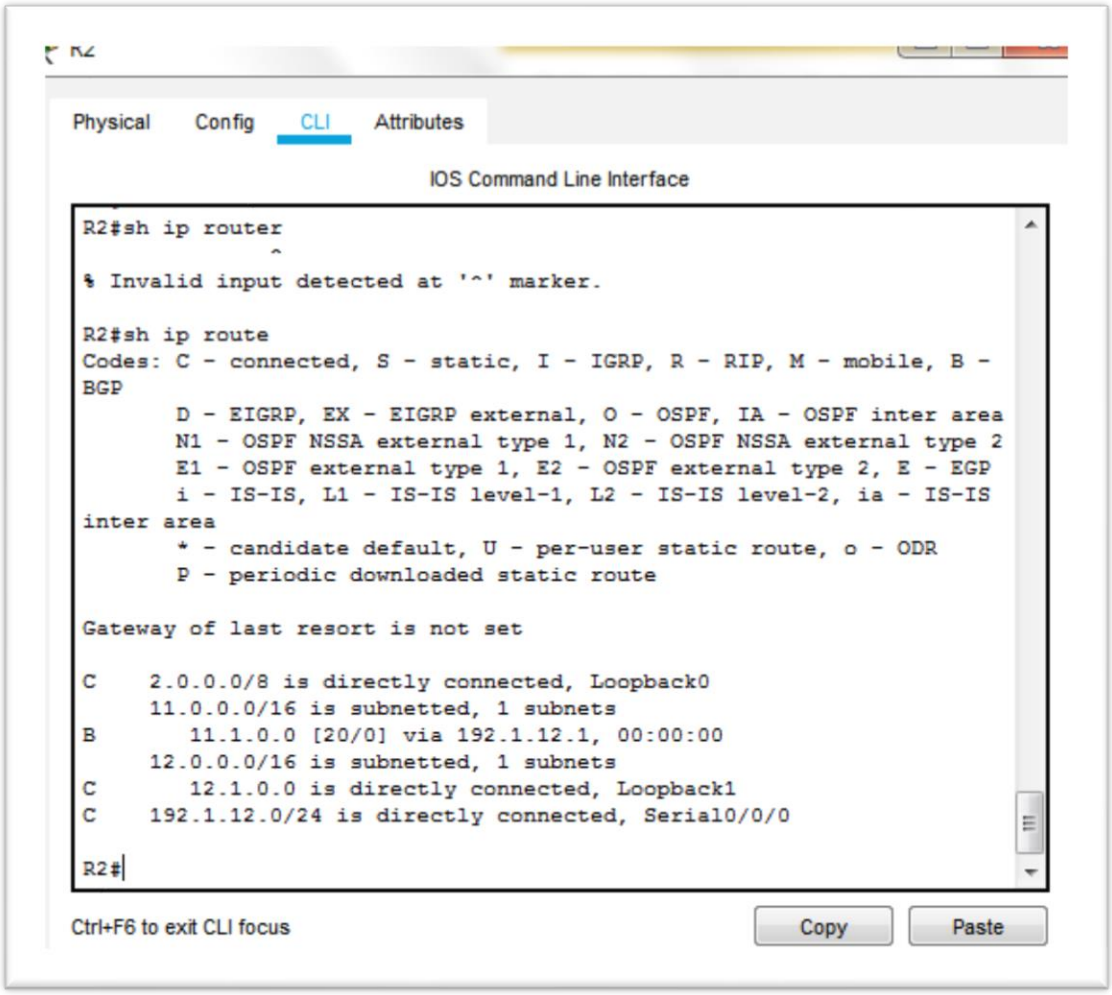


Figura 4. Relación de vecino BGP entre R1 y R2. R1

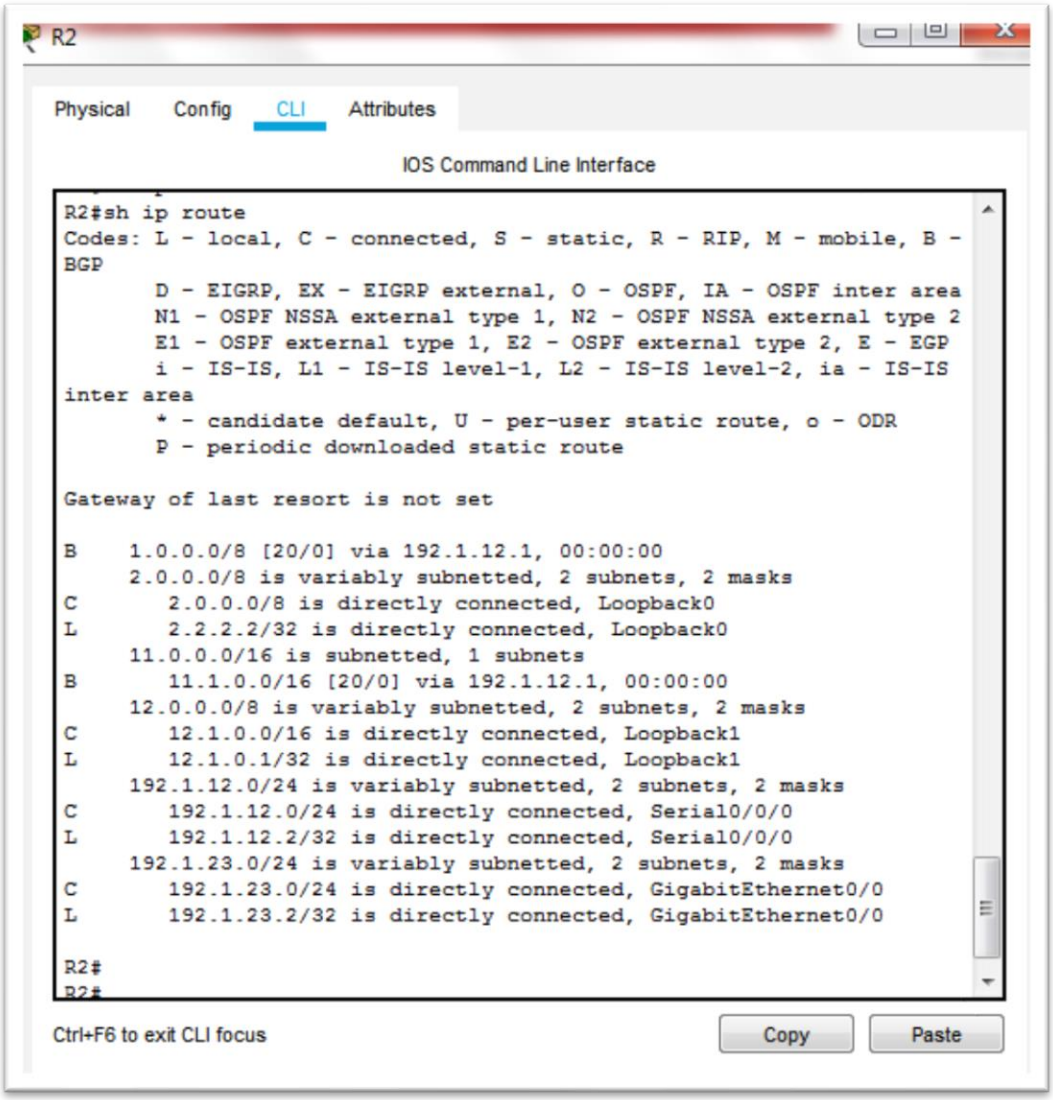


2. Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en AS2 y R3 debería estar en AS3. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 44.44.44.44. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

   Solución en la relación de vecino BGP entre R2 y R3, mediante del comando show iproute

R2#
R2#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router bgp 2
R2(config-router)#neighbor 192.1.23.3 remote-as 3
R2(config-router)#^Z
R2#
%SYS-5-CONFIG_I: Configured from console by console

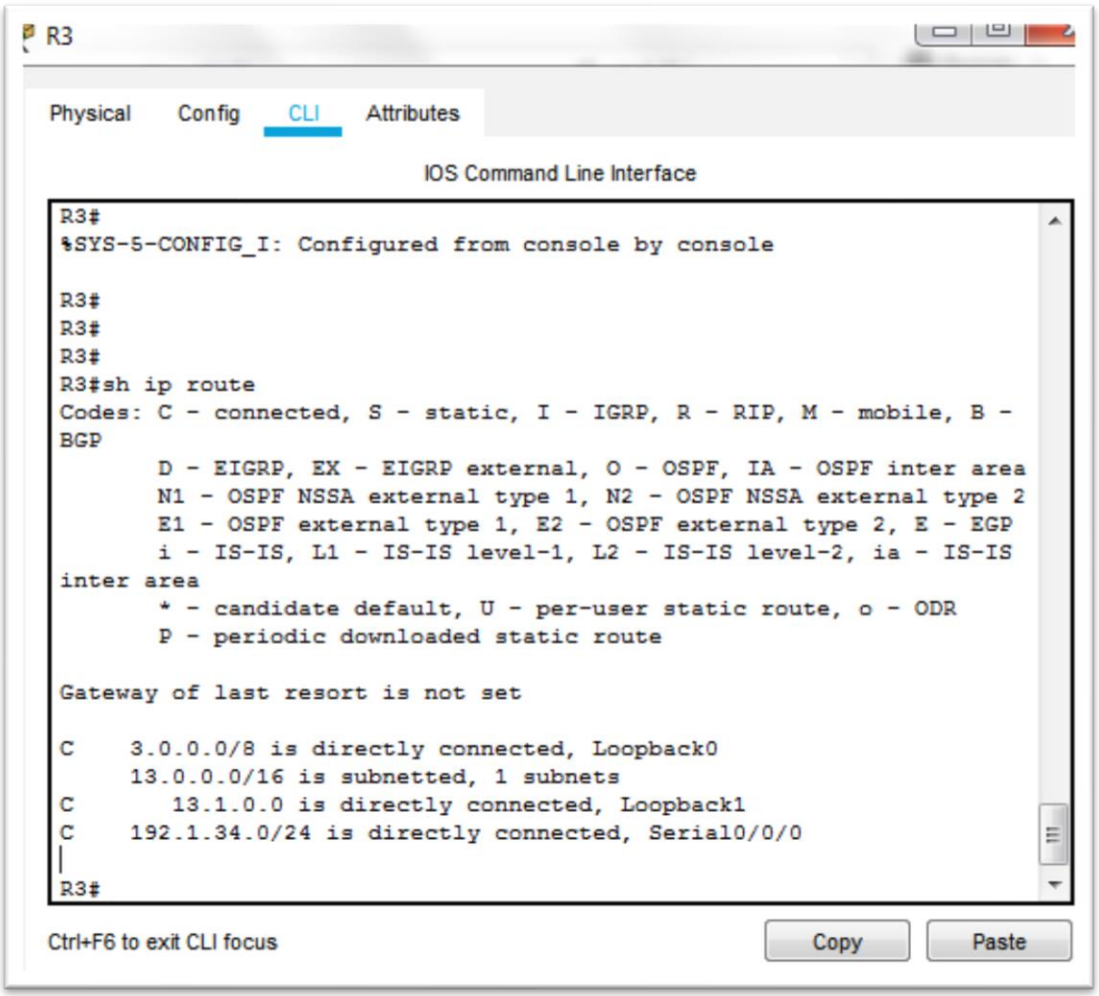
Figura 5. Relación de vecino BGP entre R1 y R2. R1



R3>en
R3#conf ter
Enter configuration commands, one per line. End with CNTL/Z.

```
R3(config)#router bgp 3
R3(config-router)#bgp router-id 33.33.33.33
R3(config-router)#no synchronization
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 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)#
R3(config-router)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#
```

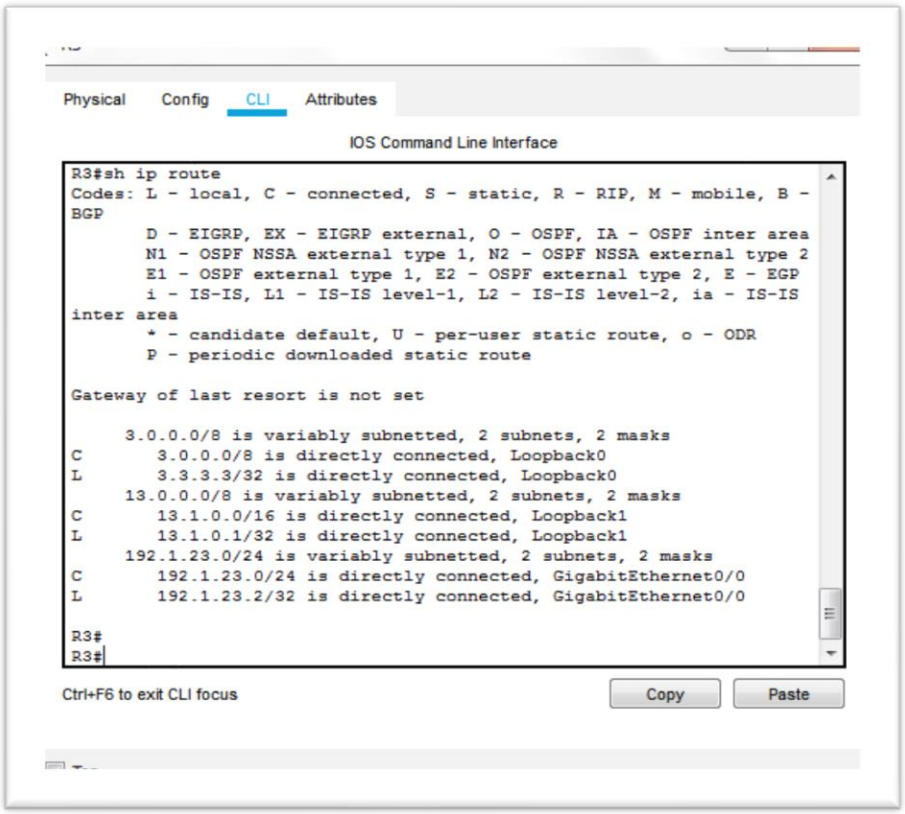
Figura 6. Relación de vecino BGP entre R1 y R2. R1



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.

```
R3#
R3#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router bgp 3
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#
R3(config-router)#^Z
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

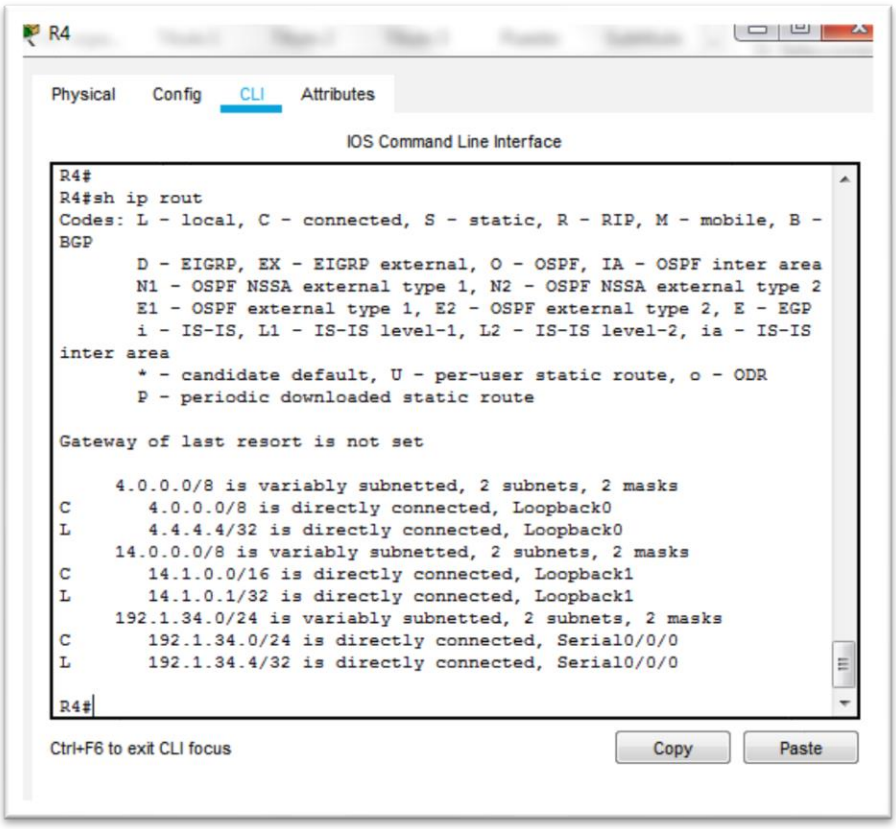
Figura 7. Relación de vecino BGP entre R3 y R4. R3



.

R4(config)#
R4(config)#router bgp 4
R4(config-router)#no synchronization
R4(config-router)#neighbor 192.1.34.3 remote-as 3
R4(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.34.3 Up
R4(config-router)#net
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)#bgp router-id 44.44.44.44
R4(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.34.3 Up
R4(config-router)#
R4(config-router)#
R4(config-router)#^Z
R4#
%SYS-5-CONFIG_I: Configured from console by console
R4#

Figura 8. Relación de vecino BGP entre R3 y R4. R3



2. Escenario 2

Figura 9. Escenario 2

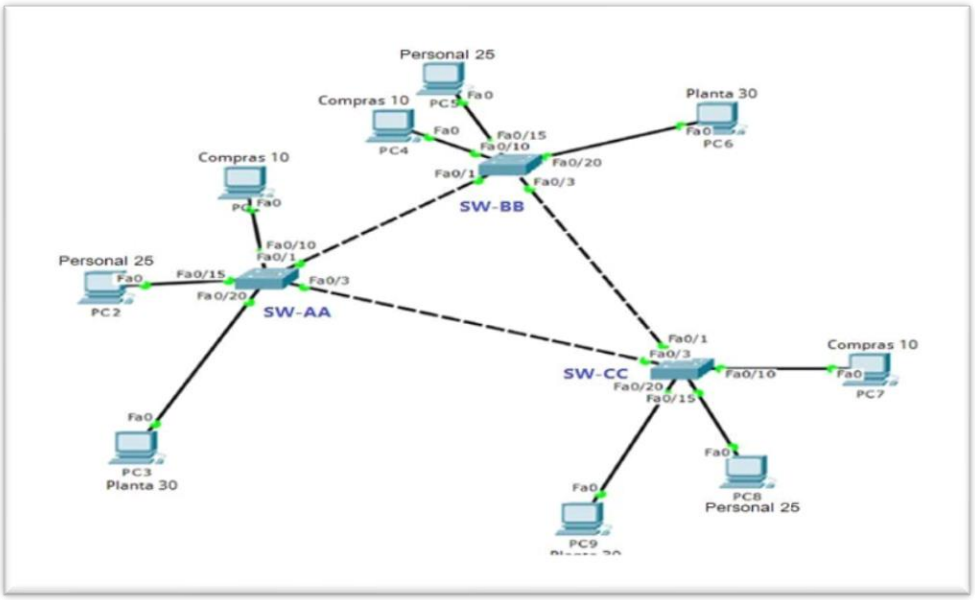
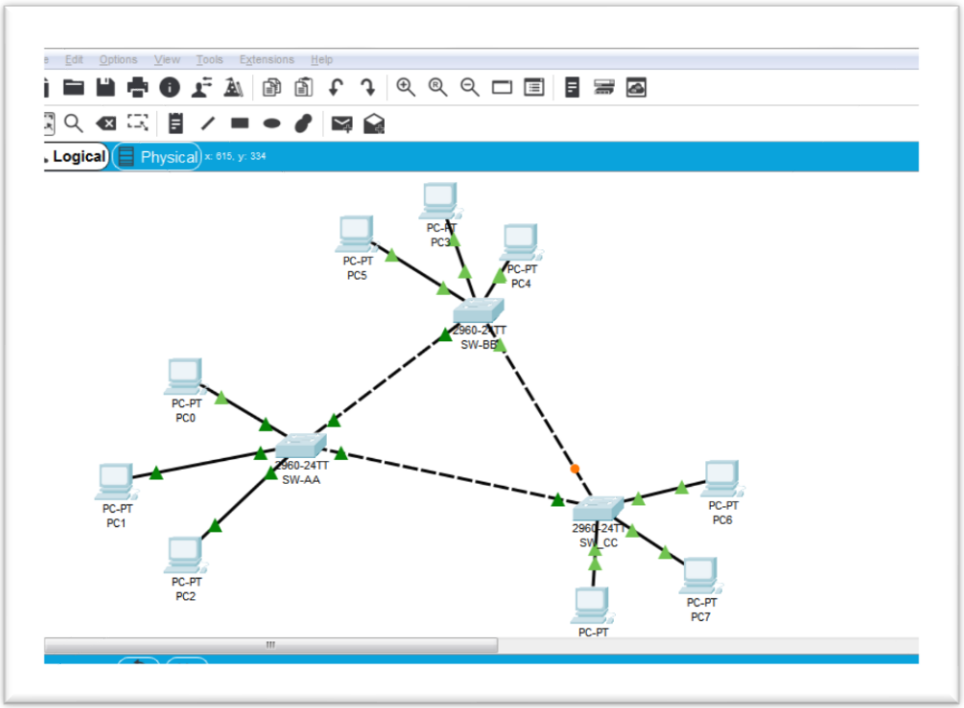


Figura 10. Simulación del escenario 2



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 VPT llamado CCNP y usando la contraseña cisco.

```
SW-AA>en
SW-AA#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#vtp mode client
Device mode already VTP CLIENT.
SW-AA(config)#vtp domain CCNP
Domain name already set to CCNP.
SW-AA(config)#vtp password cisco
Password already set to cisco
SW-AA(config)#
```

```
SW-BB#conf ter
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
Domain name already set to CCNP.
SW-BB(config)#vtp password cisco
Password already set to cisco
SW-BB(config)#
SW-BB(config)#
SW-BB#
```

```
SW-CC>en
SW-CC#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#vtp mode client
Device mode already VTP CLIENT.
SW-CC(config)#vtp domain CCNP
Domain name already set to CCNP.
SW-CC(config)#vtp password cisco
Password already set to cisco
SW-CC(config)#
```

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

Figura 11. Verificación configuración ***show vtp status.***

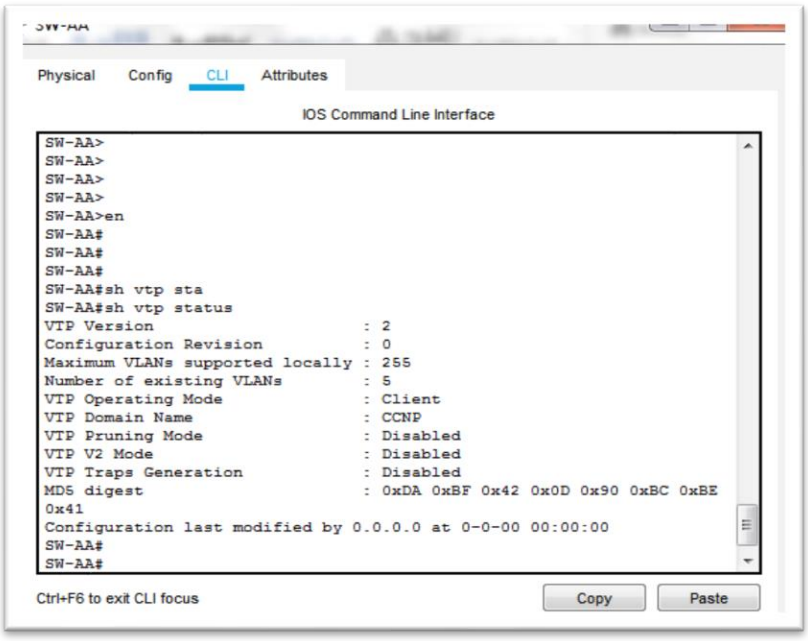


Figura 12. Verificación configuración ***show vtp status***

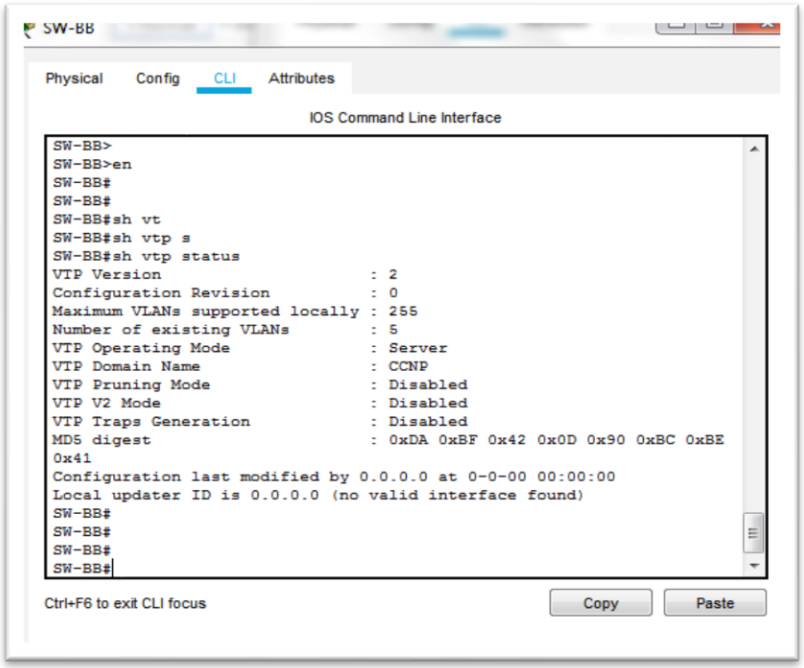
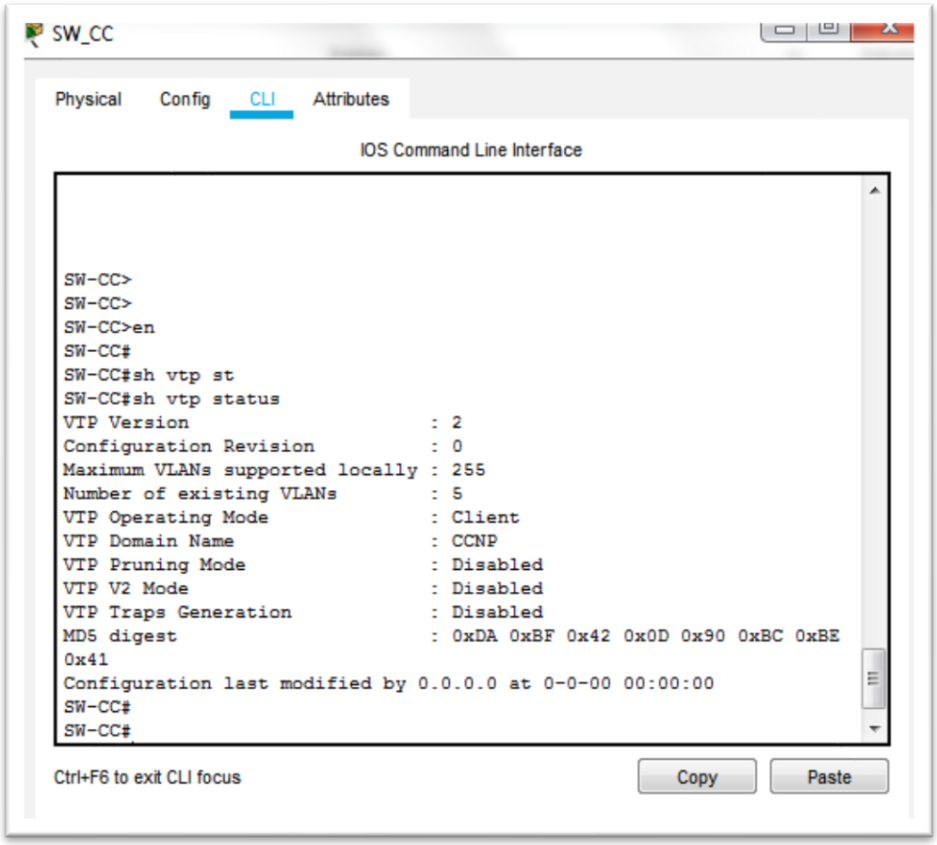


Figura 13. Verificación configuración ***show vtp status***



B. Configurar DTP (Dynamic Trunking Protocol)

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

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

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

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

Figura 14. Verificación enlace "trunk" entre SW-AA y SW-BB

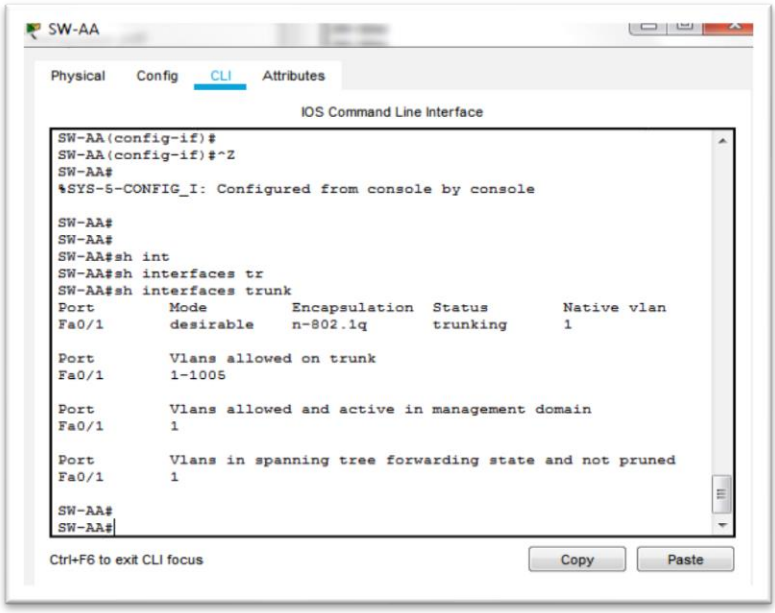
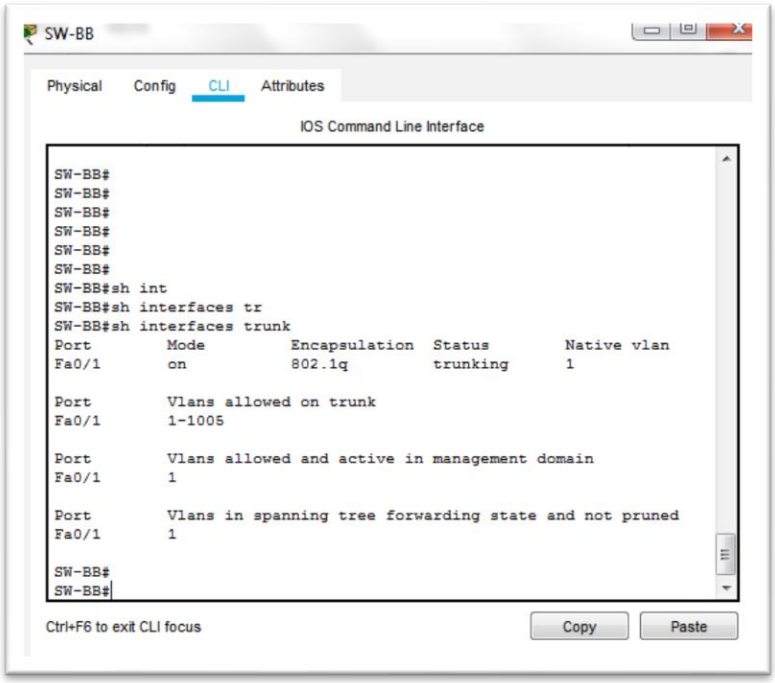


Figura 15. Verificación enlace "trunk" entre SW-AA y SW-BB

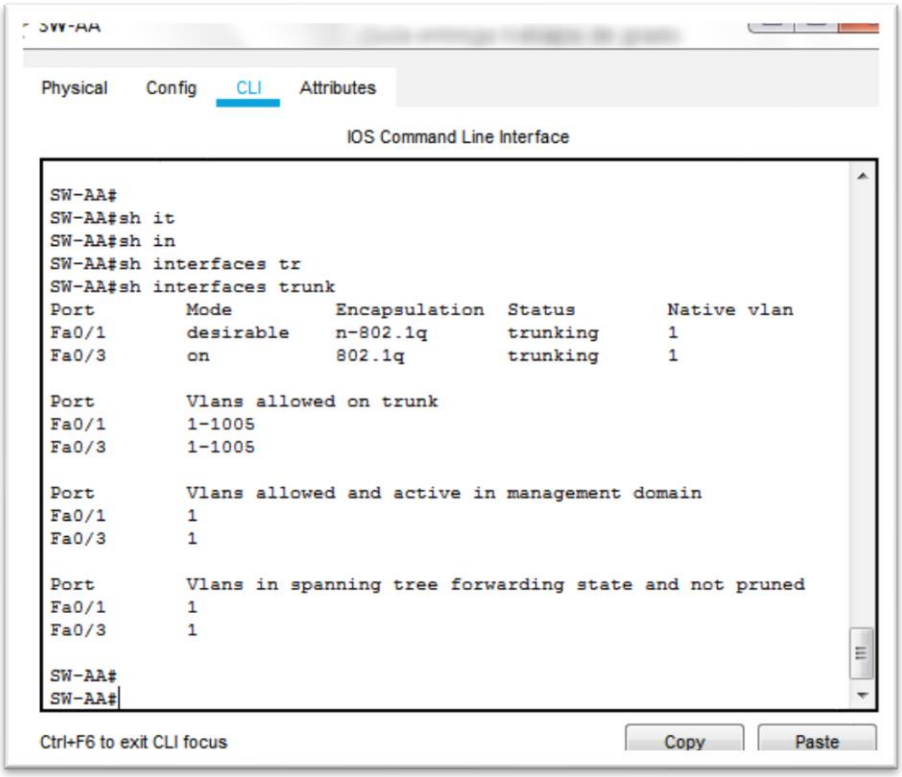


6. Entre SW-AA y SW-BB configure un enlace "trunk" estático utilizando el comando ***switchport mode trunk*** en la interfaz F0/3 de SW-AA

```
SW-AA(config)#
SW-AA(config)#in f0/3
SW-AA(config-if)#switchport mode trunk
```

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

Figura 16. Verificación enlace "trunk" comando ***show interfaces trunk***



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

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

SW-CC(config)#
SW-CC(config)#in f0/3
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#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
SW-AA(config)#
SW-AA(config)#
```

```
SW-BB#
SW-BB#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#
SW-BB(config)#vlan 10
SW-BB(config-vlan)#name COMPRAS
SW-BB(config-vlan)#vlan 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 ADMINISTRACION
SW-BB(config-vlan)#
SW-BB(config-vlan)#exit
SW-BB(config)#exit
SW-BB#
```

10. Verifique que las VLANs han sido agregadas correctamente

Figura 17. Verificación VLANs

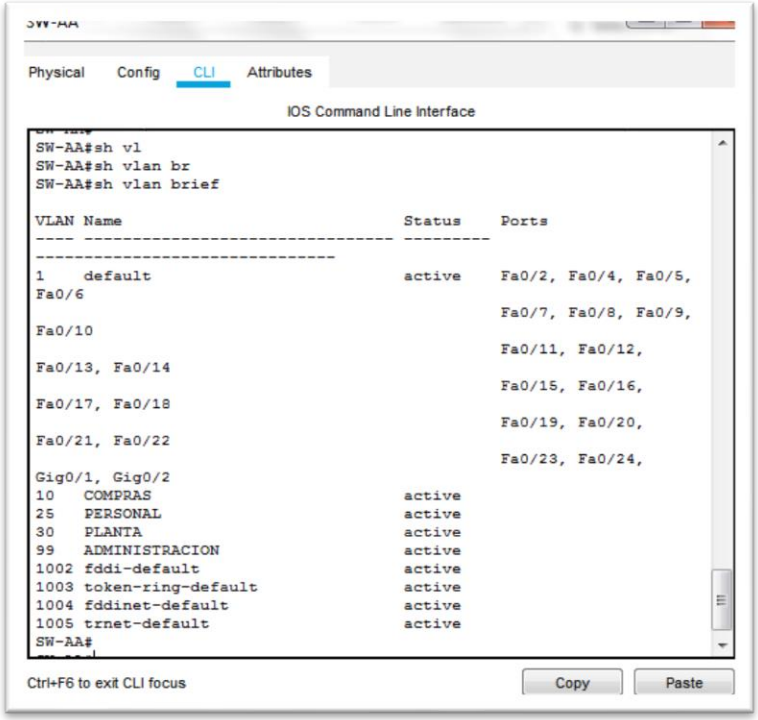
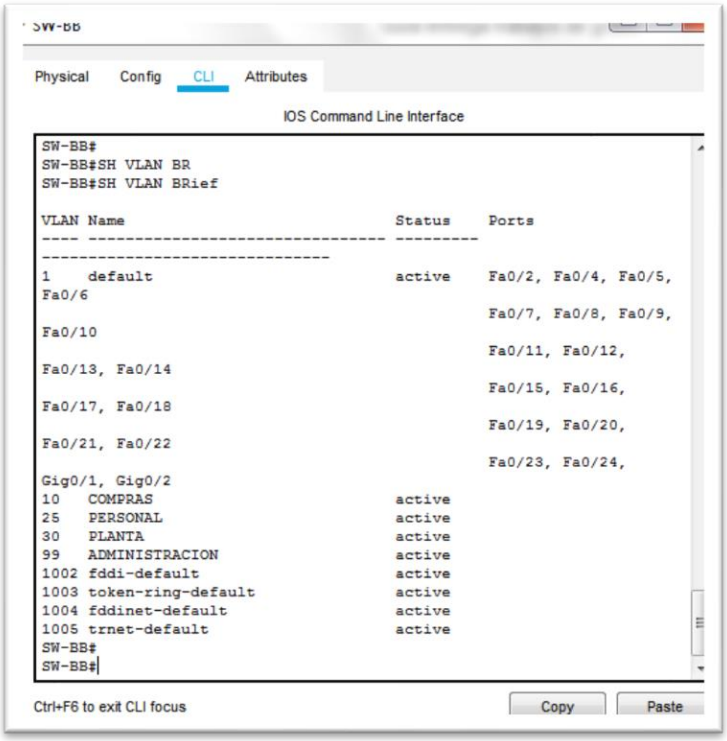


Figura 18. Verificación VLANs



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

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

Tabla 5. X = número de cada PC particular

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.2/ 24
F0/15	VLAN 25	190.108.20.2/24
F0/20	VLAN 30	190.108.30.2 /24

Tabla 6. Asociación puertos a las VLAN

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

```
SW-AA>
SW-AA>en
SW-AA#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#in f0/10
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#
SW-AA(config-if)#
SW-AA(config-if)#
```

```
SW-BB#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#in f0/10
SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#
```

```
SW-CC#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#in f0/10
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#
SW-BB(config-if)#
SW-BB(config-if)#
```

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#
SW-AA#
SW-AA#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#in f0/15
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#in f0/20
SW-AA(config-if)#switchport access vlan 30
SW-AA(config-if)#exit
SW-AA(config)#^Z
SW-AA#
SW-AA#
```

```
SW-BB#
SW-BB#
SW-BB#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#in f0/15
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#in f0/20
SW-BB(config-if)#switchport access vlan 30
SW-BB(config-if)#exit
SW-BB(config)#^Z
SW-BB#
SW-BB#
```

```
SW-CC#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#in f0/15
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#in f0/20
SW-CC(config-if)#switchport access vlan 30
SW-CC(config-if)#exit
SW-CC(config)#^Z
SW-CC#
```

D. Configurar las direcciones IP en los Switches.

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

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

Tabla 7. Asignación una dirección IP al SVI

```
SW-AA#
SW-AA#CONF TER
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#int
SW-AA(config)#interface vl
SW-AA(config)#interface vlan 99
SW-AA(config-if)#ip add
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
SW-AA(config-if)#no shut
SW-AA(config-if)#
SW-AA(config-if)#exit
SW-AA(config)#exit
SW-AA#
```

```
%SYS-5-CONFIG_I: Configured from console by console
SW-AA#


SW-BB#
SW-BB#CONF TER
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#interface 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)#
SW-BB(config-if)#exit
SW-BB(config)#exit
SW-BB#
%SYS-5-CONFIG_I: Configured from console by console
SW-BB#


SW-CC#
SW-CC#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#interface vlan 99
SW-CC(config-if)#ip address 190.108.99.E 255.255.255.0
SW-CC(config-if)#no shut
SW-CC(config-if)#
SW-CC(config-if)#exit
SW-CC(config)#exit
SW-CC#
%SYS-5-CONFIG_I: Configured from console by console
SW-CC#
```

E. Verificar la conectividad Extremo a Extremo

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

Figura 19. Verificación conectividad Extremo a Extremo

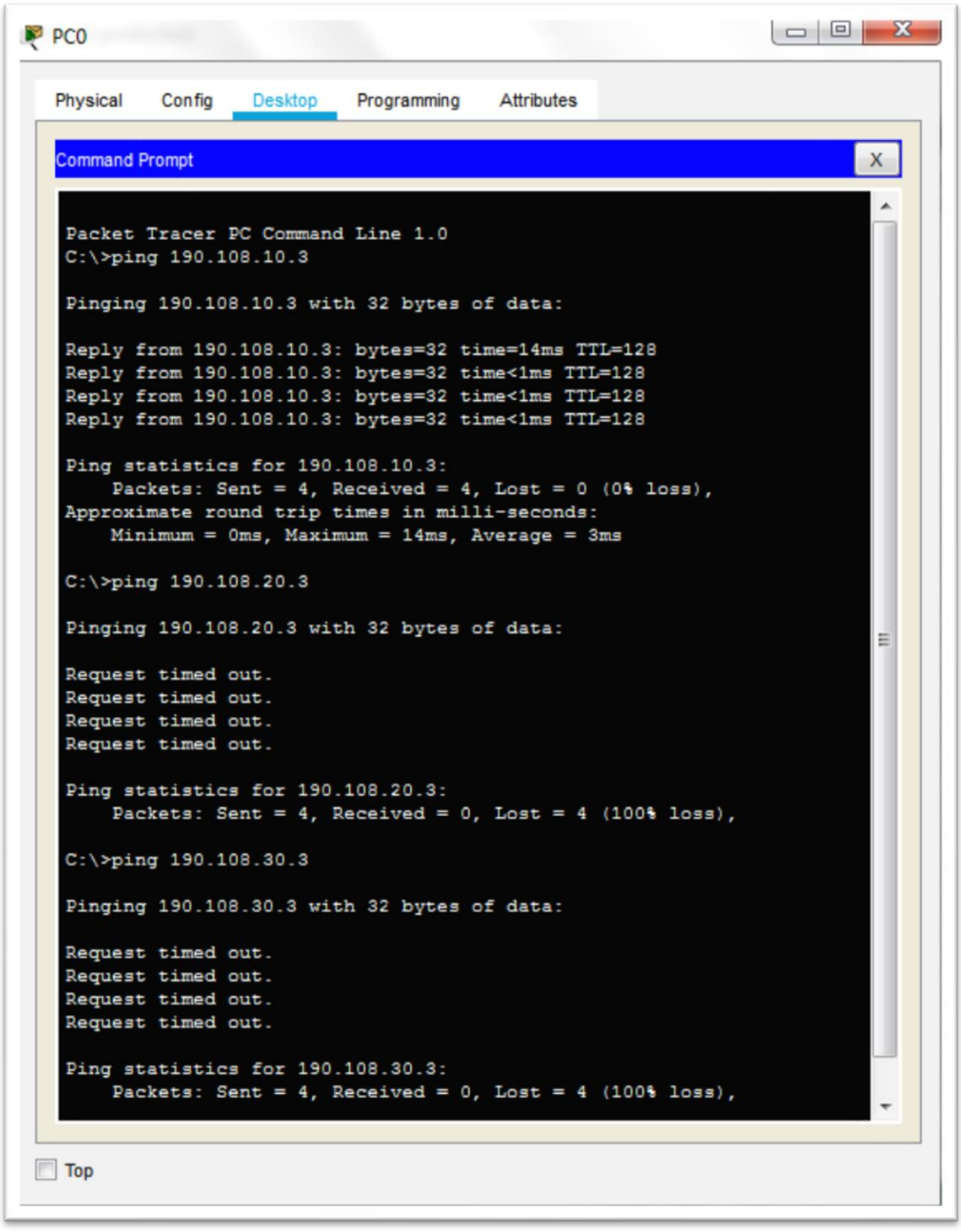


Figura 20. Verificación conectividad Extremo a Extremo

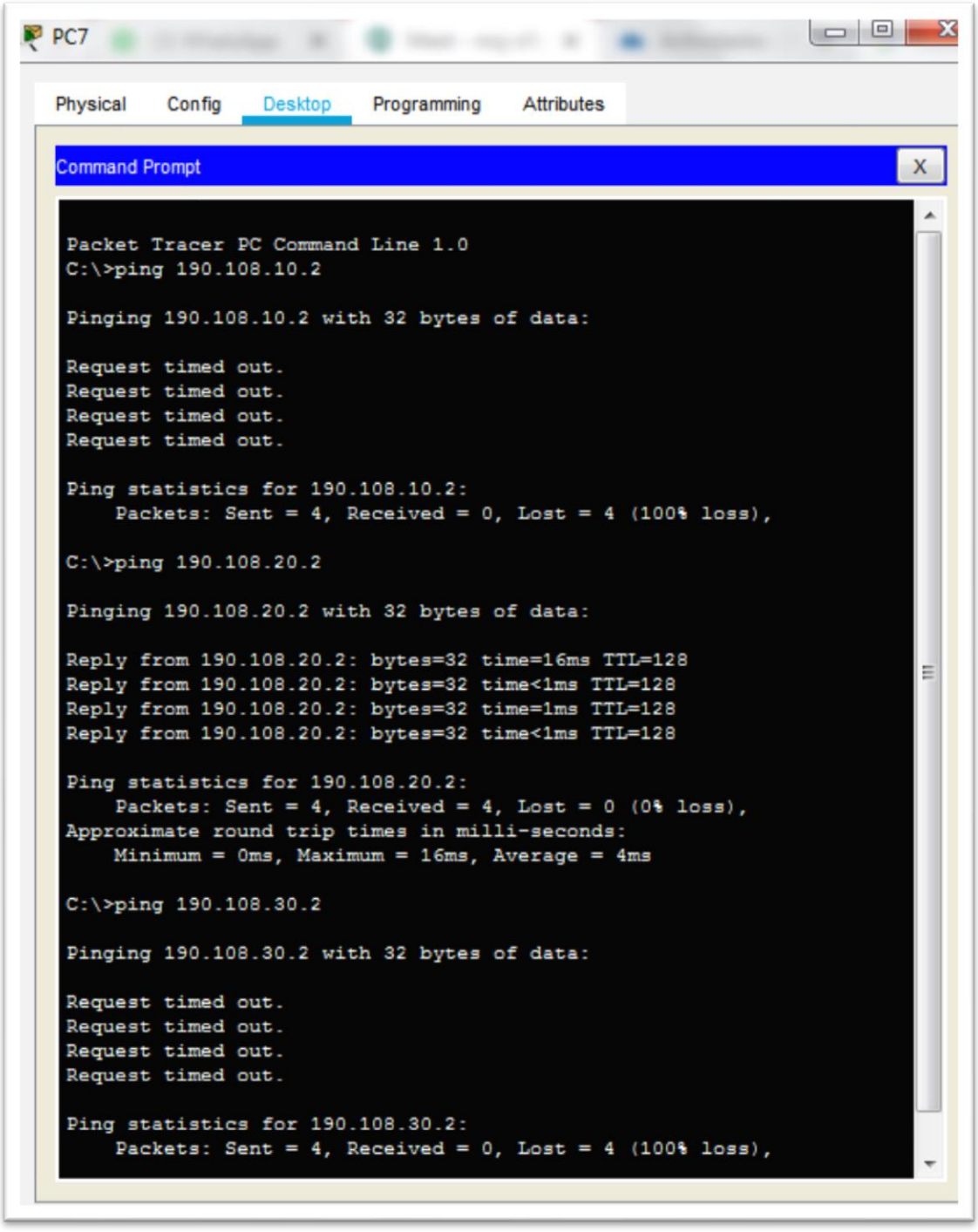
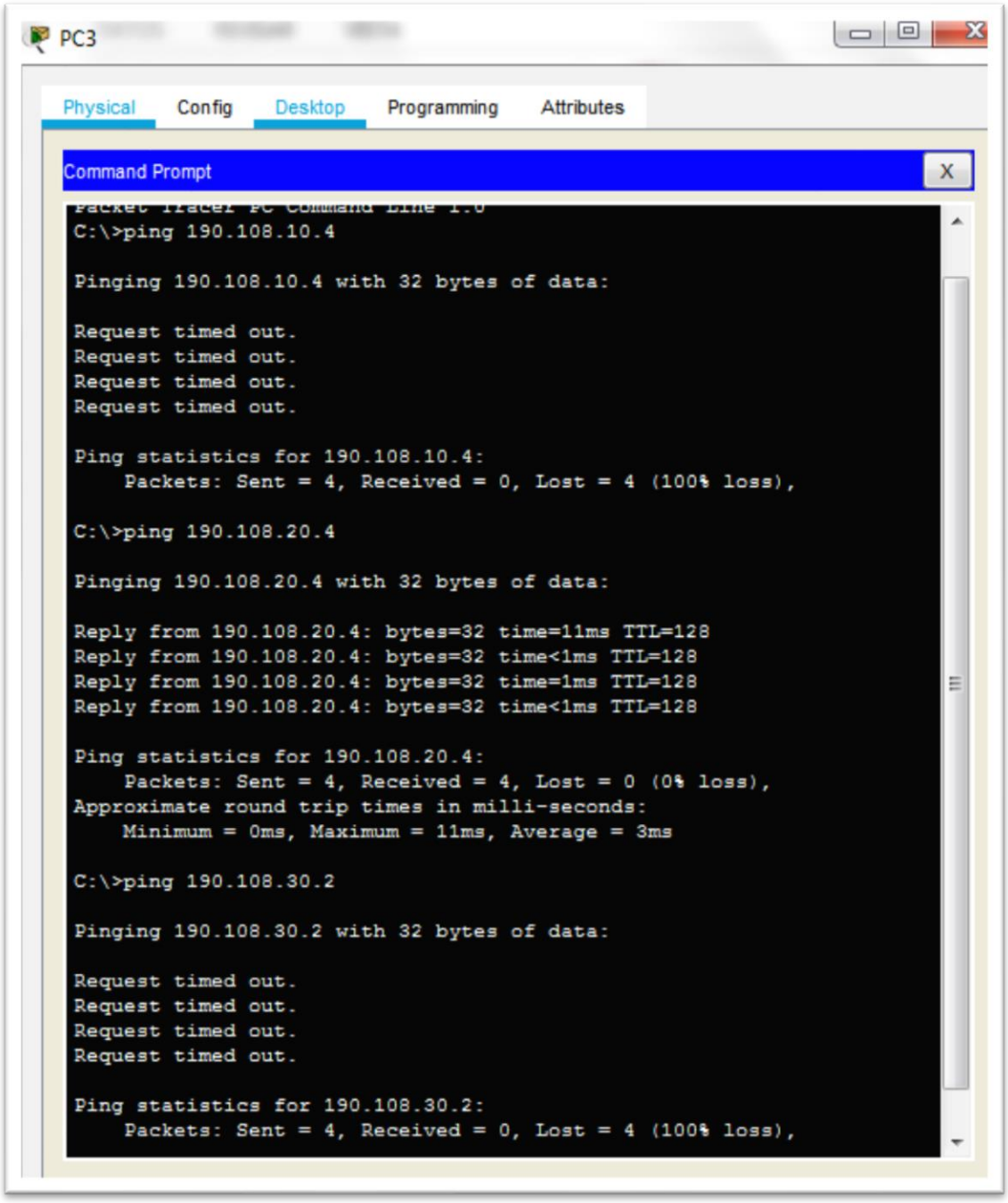


Figura 21. Verificación conectividad Extremo a Extremo



El ping es exitoso cuando son equipos que están en la misma vlan. El ping no es éxito cuando los equipos no se encuentran asociadas a las diferentes vlan.

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

Figura 22. Verificación Ping desde cada Switch

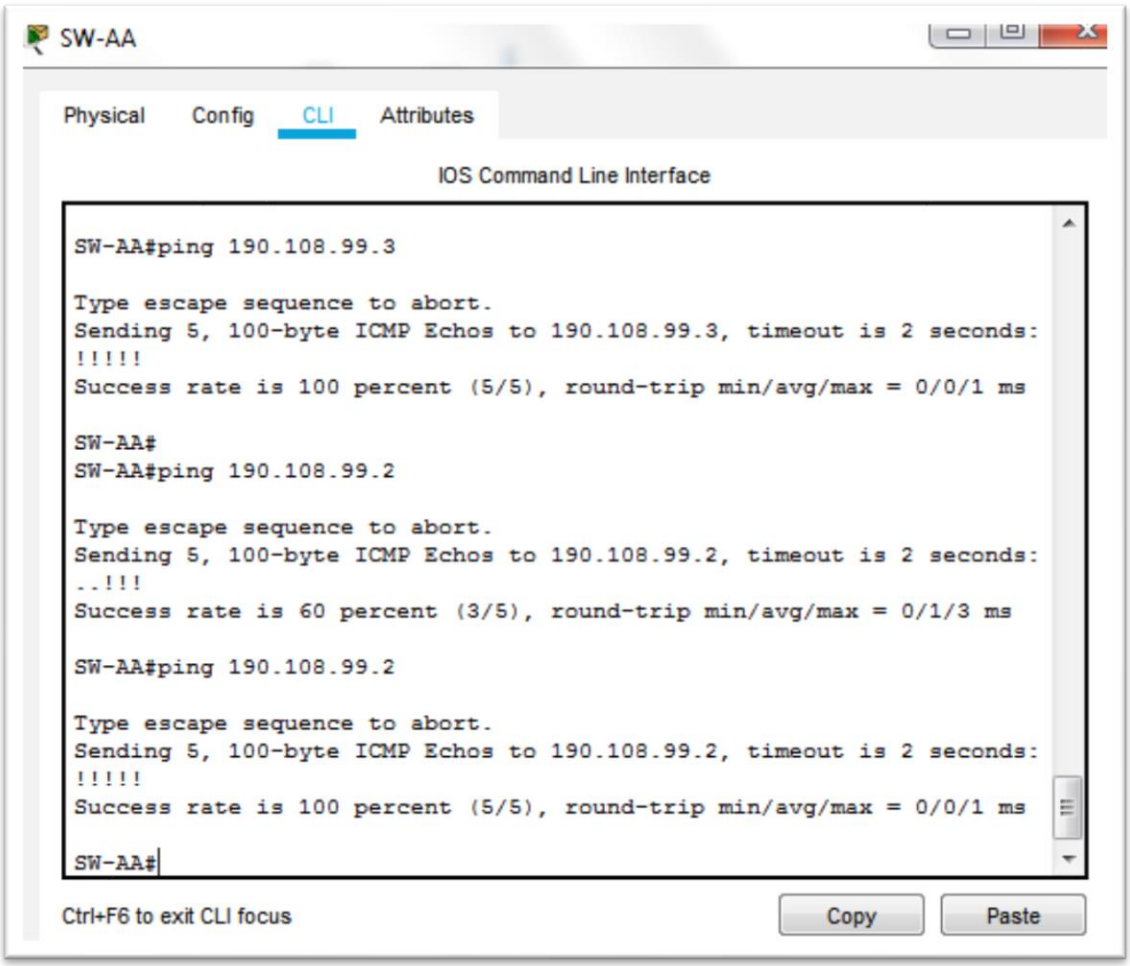


Figura 23. Verificación Ping desde cada Switch

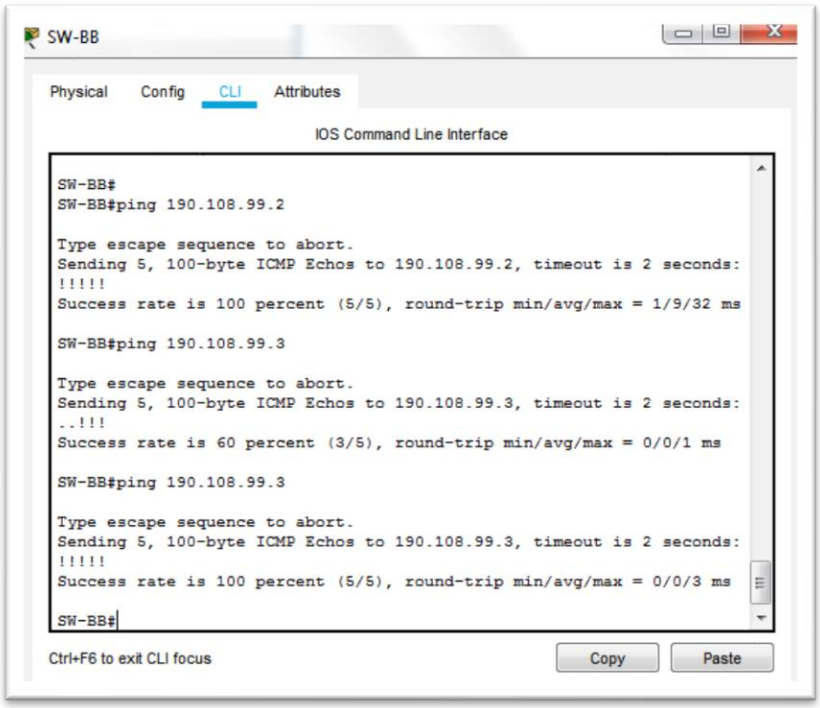
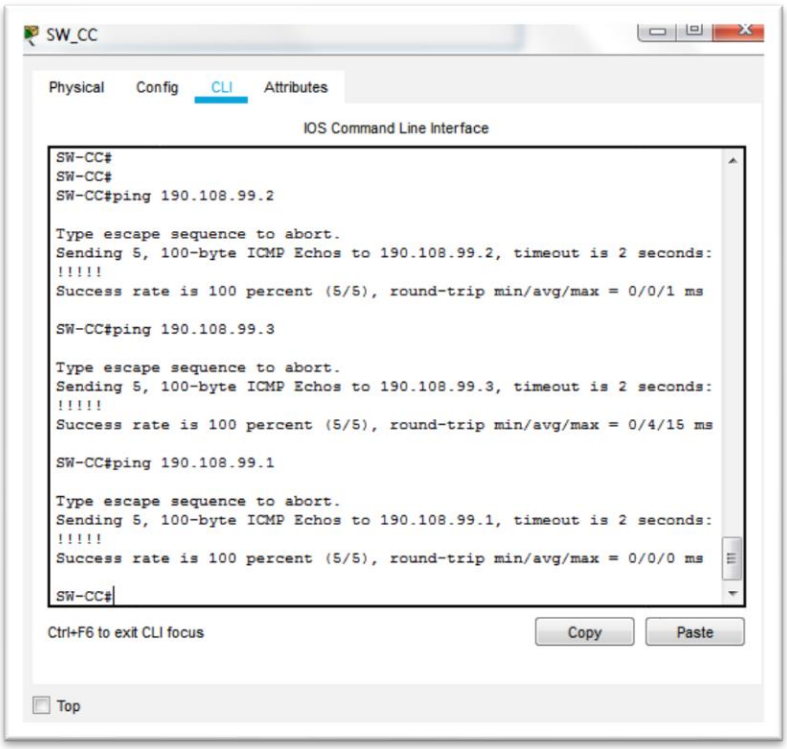


Figura 24. Verificación Ping desde cada Switch



Los ping entre los tres equipos son satisfactorios ya que los tres equipos s encuentran dentro de uan misma vlan, vlan 99 y todos cuentan con puertos trunk lo que permite el paso de paquetes

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

Figura 25. Verificación Ping desde cada Switch a cada PC

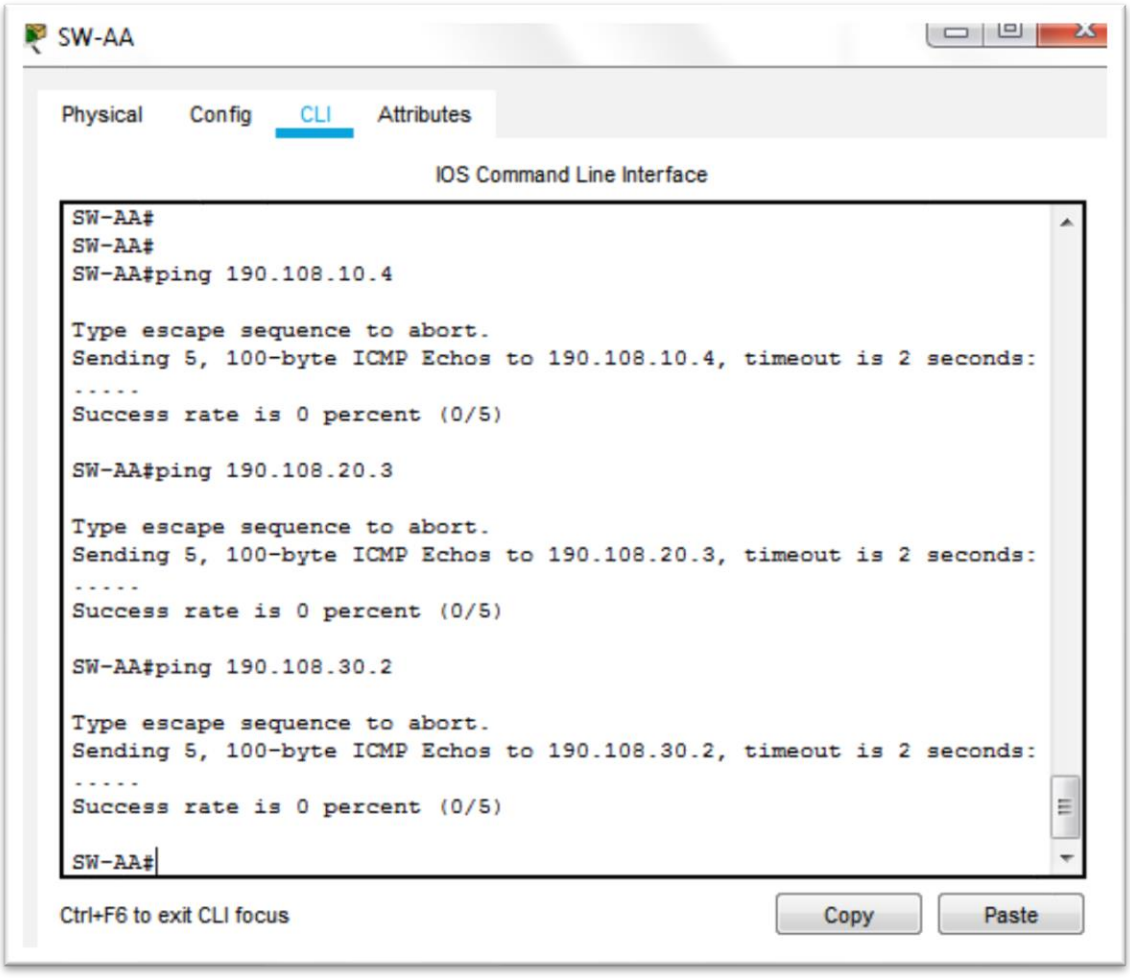


Figura 26. Verificación Ping desde cada Switch a cada PC

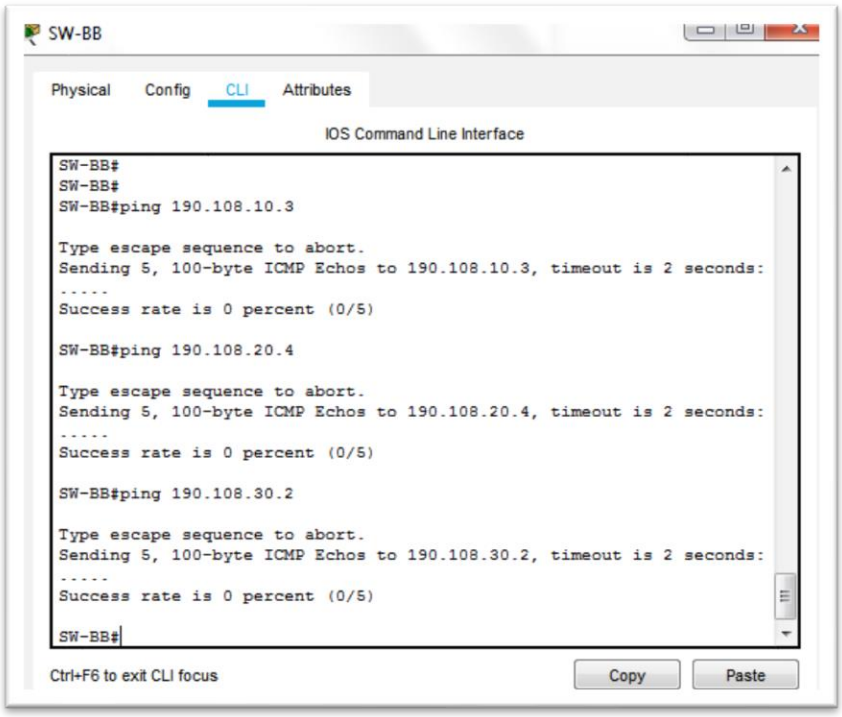
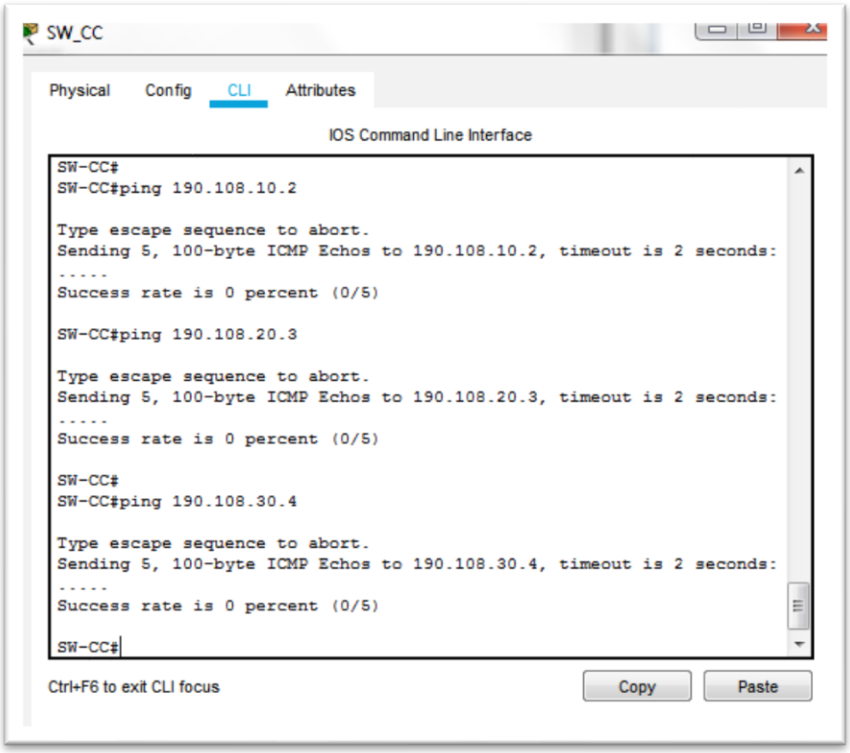


Figura 27. Verificación Ping desde cada Switch a cada PC



En los equipos switc no se configuraron direccionamiento ip asociado alas vlan que pertencen cada unos de los PC, por esta razon no se tiene conectividad de los SW alos PC

CONCLUSIONES

En el desarrollo del trabajo demuestra el aprendizaje obtenido durante el curso de la materia de cisco CCNP, y el manejo de la herramienta de simulación Packet Tracer, En cada escenario desarrollado, se ha simulado y verificado el registro de los procesos de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros, para así poder observar su correcto funcionamiento en base a su programación.

Los escenarios propuestos afianzaron las capacidades en configuración de dispositivos como router y switches, configuración de Vlan, puertos troncales, configuración de redes primarias y secundarias

Con este trabajo se puede comprender como se implementa y configura una red que esté soportada por VLANs con el uso de los protocolos VTP, donde se pueda diseñar las plantillas de configuración para su uso en múltiples dispositivos, configurar sus respectivas troncales y vlan usando el protocolo VTP.

REFERENCIAS

CCNA Desde Cero. “VLAN (Virtual LAN) “{En línea}. {7 May 2020} disponible en:

(https://ccnadesdecero.com/curso/vlan/)

Comunicación de Redes. “LOOPBACK”. {En línea}. {7 May 2020} disponible en:

(http://comunredeslitardo.blogspot.com/2013/08/que-es-un-loopback.html)

Donohue, D. CISCO Press. “CCNP Quick Reference”. {En línea}. {7 May 2020} disponible en: https://1drv.ms/b/s!AgIGg5JUgUBthFt77ehzL5qp0OKD

Enterprise, E., & Gerometta, O. “El CCNP R&S actual y el nuevo CCNP Enterprise”. {En línea}. {7 May 2020} disponible en:

(http://librosnetworking.blogspot.com/2019/10/el-ccnp-r-actual-y-el-nuevo-ccnp.html)

Froom, R., Frahim, E. CISCO Press (Ed). First Hop Redundancy Protocols. “Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115” . {En línea}. {7 May 2020} disponible en:

(https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ)

GlobalVoip. “Routing y Switching “{En línea}. {7 May 2020} disponible en:

(http://www.globalvoip.com.mx/ps_switching-y-routing.html)

Hucaby, D. CISCO Press (Ed). CCNP “Routing and Switching” SWITCH 300-115 Official Cert Guide. {En línea}. {7 May 2020} disponible en:

(https://1drv.ms/b/s!AgIGg5JUgUBthF16RWCSsCZnfDo2)

Macfarlane, J. Network Routing Basics. “Understanding IP Routing in Cisco Systems”. {En línea}. {7 May 2020} disponible en:

(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)

Netec Global knowledge.” CCNP Routing & Switching”. {En línea}. {7 May 2020} disponible en:

(https://www.netec.com/ccnp-routing-and-switching)

Protocolo de Enrutamiento IGRP.”Entre Redes y Servidores”. {En línea}. {7 May 2020} disponible en:

(https://alexalvarez0310.wordpress.com/category/protocolo-de-enrutamiento-igrp/)

Proydesa, R. “Qué es y cómo funciona el protocolo EIGRP”. {En línea}. {7 May 2020} disponible en:

(https://www.proydesa.org/portal/index.php/noticias/1764-que-es-y-como-funciona-el-protocolo-eigrp-2)

UNAD. Switch CISCO. “Security Management” [OVA]. {En línea}. {7 May 2020} disponible en:

(https://1drv.ms/u/s!AmIJYei-NT1IlyVeVJCCezJ2QE5c)

Universidad Ort Urugyay. Facultad de Ingenieria. “Introducción a la configuración de routers cisco “{En linea}. {7 May 2020} disponible en:

(https://www.ort.edu.uy/fi/pdf/configuracionroutersciscomatturro.pdf)