DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JULIÁN DAVID ESTRADA CHALIAL

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JULIÁN DAVID ESTRADA CHALIAL

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

San Juan de Pasto, 22 de mayo de 2020

AGRADECIMIENTOS

Mis agradecimientos a la Universidad Nacional Abierta y a Distancia, por brindarme la oportunidad de formarme como profesional, a mis profesores que, con los saberes impartidos, han hecho de mí una persona idónea capaz de desempeñarme adecuadamente en los Ámbitos laborales.

A mi madre, por su entrega y amor, sin ella este sueño que hoy culmina no sería una realidad. Y muy especialmente quiero agradecer a mi esposa y a mi hijo, por toda la paciencia, por sacrificar momentos de familia con el fin de lograr darme los espacios para desarrollar mis compromisos académicos.

CONTENIDO

LISTA DE FIGURAS

GLOSARIO

DTP: Todos los switches Cisco, usan un protocolo patentado de punto a punto llamado Protocolo de enlace dinámico (DTP) en puertos troncales para negociar el estado de enlace. DTP negocia el modo operativo de los puertos del conmutador directamente conectados a un puerto troncal y selecciona un protocolo de enlace apropiado. Se recomienda negociar el enlace troncal.

VTP: Es un protocolo que se utiliza para distribuir y sincronizar información sobre bases de datos VLAN configurado a través de una red conmutada. VTP minimiza las configuraciones y configuraciones erróneas inconsistencias que pueden dar lugar a varios problemas, como nombres de VLAN duplicados, incorrectos. Especificaciones de tipo VLAN y violaciones de seguridad. Esta sección discute en detalle cómo planificar, implementar y verificar VTP en las redes del campus.

VLAN: Debido a que el router decide cuadro por cuadro qué puertos intercambian datos, es natural extensión para poner lógica dentro del conmutador y permitirle elegir puertos para agrupaciones especiales. Esta agrupación de puertos se denomina red de área local virtual (VLAN). El Switch se asegura de que el tráfico desde un grupo de puertos nunca se envía a otros grupos de puertos (lo que sería enrutamiento). Los grupos de puertos (VLAN) pueden considerarse un segmento LAN individual.

STP: Proporciona redundancia de enlace de red al tiempo que elimina posibles problemas de bucles. Una limitación del STP tradicional es el retraso de convergencia después de un cambio de topología, por lo que el uso de RSTP se recomienda en su lugar.

RSTP: El protocolo de árbol de expansión rápido (IEEE 802.1w, también conocido como RSTP) acelera significativamente recálculo del árbol de expansión cuando cambia la topología de la red. RSTP define funciones adicionales de puerto de alternativa y copia de seguridad y define los estados de puerto como descarte, aprendizaje o reenvío. Esta La sección describe las diferencias entre STP (802.1D) y RSTP (802.1w).

RESUMEN

Este documento presenta la evaluación denominada prueba de habilidades, actividad evaluativa que hace parte del del Diplomado de Profundización CCNP, consta de dos escenarios de configuración de redes a través de software de simulación GNS3 y Packet Tracer, en el primer escenario se presenta la implementación del protocolo BGP entre cuatro Router, entre lo que resalta que en los dos router de los extremos de la red, se conectan cuatro interfaces LoopBack, dos en cada uno de ellos, la intención de este ejercicio comprende en establecer comunicación utilizando el protocolo mencionado entre Routers vecinos y su correspondientes redes internas por medio del protocolo, al finalizar la ejecución de los códigos requeridos para este proceso, se presentan los resultados de salida por medio del comando show ip route.

El segundo de los escenarios presenta la configuración de una Red a través de tres Swicht, cada uno de ellos con tres equipos Host, con una descripción similar al de su Switch vecino, así, un equipo en cada switch denominado Personal, Planta y Compras que serán las VLAN propuestas para este ejercicio. La idea es buscar a través de comandos, implementar en primera instancia el protocolo VTP, definiendo al switch SW-BB como servidor y a los switch SW-AA y SW-CC, como clientes, estos tres incluidos en el dominio CCNP, posterior a ello, se crean los enlaces troncales entre los mismos para asegurar su comunicación, seguido de esto, se definen las VLAN para los respectivos PCs por medio de interfaces semejantes para cada Switch, Finalmente una VLAN para los tres Switch con su respectivo interfaz. Para iniciar con el proceso de verificación, se fijó la dirección IP de los Pcs y se ejecutaron ping entre los diferentes dispositivos, con el fin de analizar su conectividad entre ellos.

Palabras clave: GNS3, Packet Tracer, Redes, BGP, VTP, VLAN, Loopback.

ABSTRACT

This document presents the evaluation called the skills test, an evaluative activity that is part of the CCNP Deepening Diploma, consisting of two network configuration scenarios through simulation software GNS3 and Packet Tracer, in the first scenario the implementation of the BGP protocol between four routers, among which it stands out that in the two routers at the ends of the network, four LoopBack interfaces are connected, two in each one, the intention of this exercise is to establish communication using the aforementioned protocol between routers neighbors and their corresponding internal networks through the protocol, at the end of the execution of the codes required for this process, the output results are presented using the show ip route command.

The second of the scenarios presents the configuration of a Network through

three Swicht, each one with three Host computers, with a description similar to that of its neighboring Switch, thus, a team in each switch called Personal, Plant and Purchases that will be the proposed VLANs for this exercise. The idea is to search through commands, implement the VTP protocol in the first instance, defining the SW-BB switch as a server and the SW-AA and SW-CC switches as clients, these three included in the CCNP domain, after that , the trunk links between them are created to ensure their communication, followed by this, the VLANs for the respective PCs are defined by means of similar interfaces for each Switch, Finally a VLAN for the three Switches with their respective interface. To start with the verification process, the IP address of the PCs was set and ping was performed between the different devices, in order to analyze their connectivity between them.

Key words: GNS3, Packet Tracer, Networks, BGP, VTP, VLAN, Loopback.

INTRODUCCIÓN

En el presente trabajo se encontrará las pruebas de habilidades del diplomado en redes como opción de grado para la carrera de ingeniería en telecomunicaciones, en el mismo indicaremos pruebas e imágenes de los resultados en el software de simulación cisco Packet Tracer y GNS3 con su respectiva configuración desde consola.

Se presenta el primer escenario con la configuración de cuatro Routers por medio del protocolo BGP con la finalidad de establecer comunicación entre Routers vecinos por medio de comandos, una vez se termina esta implementación se realiza ejecuta el código show ip route para obtener los resultados planteados.

En el segundo escenario iniciamos con tres switch y procedemos a establecer el protocolo VTP en busca de establecer un servidor entre los switch, dos clientes, un dominio en general y su respectiva contraseña, una vez conseguido, se define los enlaces troncales entre switch, para poder implementar las VLAN que en esta ocasión serán tres dedicada a los dispositivos Host y una exclusiva para los switch. Al finalizar este proceso se muestran los resultados por medio de ping entre dispositivos.

DESARROLLO

Descripción de escenarios propuestos para la prueba de habilidades

Escenario 1

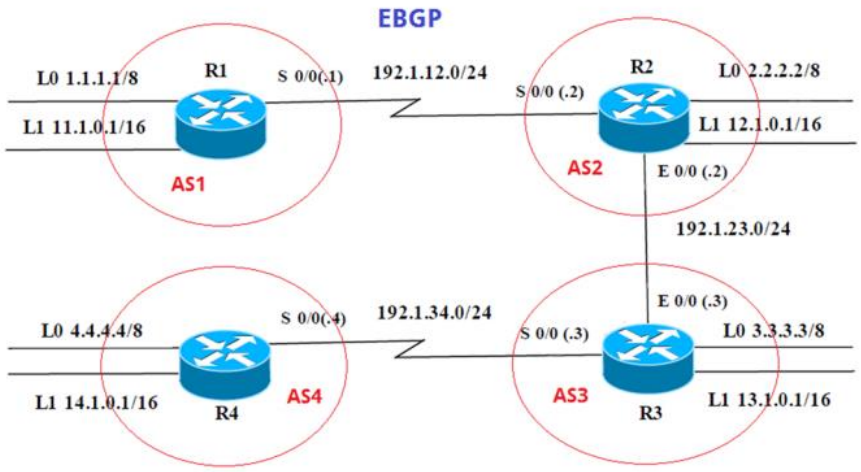

Figura 1. Escenario 1

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

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

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

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

Figura 2. Direccionamiento

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.

Descripción paso 1:

En primera instancia se configurará tanto las interfaces físicas como las virtuales, se establece el protocolo BGP entre los router R1 y R2, se los identifica, se determina el vecino y se crean las redes internas.

```
R1#configure terminal
R1(config)#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)#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)#exit
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#configure terminal
R2(config)#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 FastEthernet 0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#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)#exit
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)#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
```

RESULTADOS

Router 1

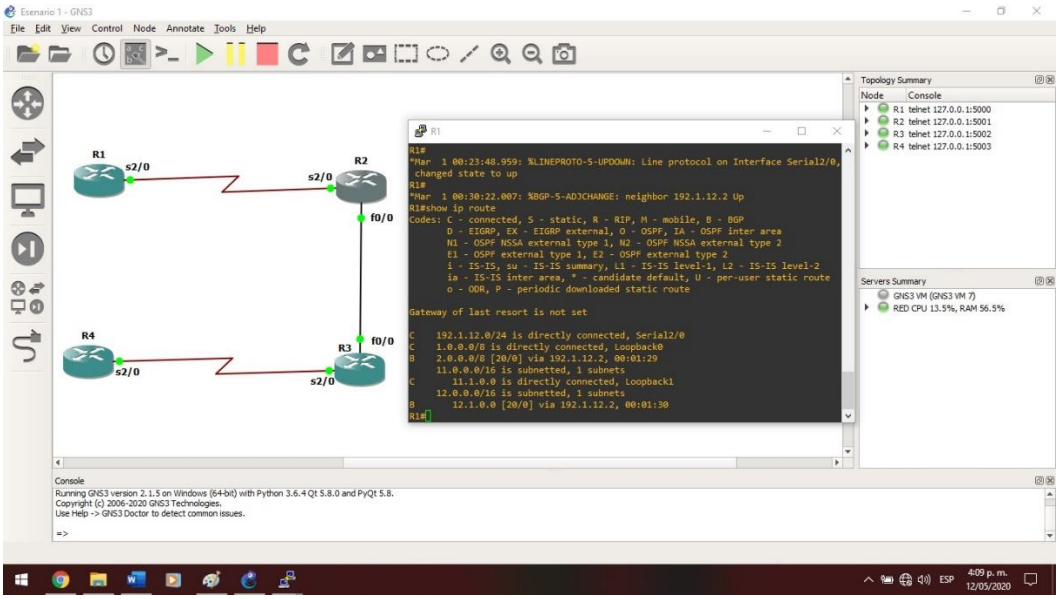

Figura 3. Resultados R1

Router 2

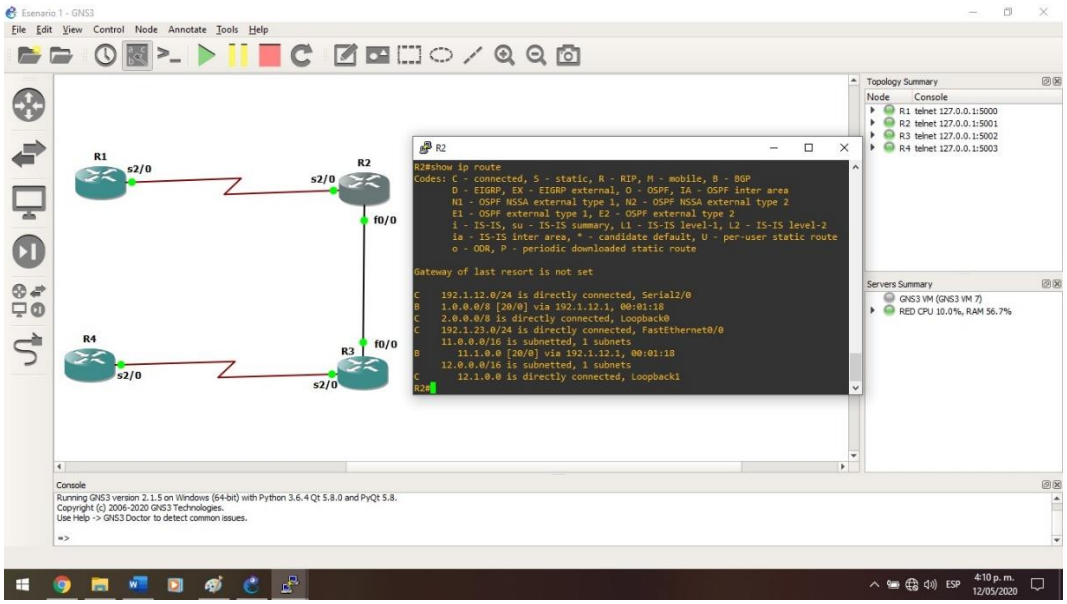

Figura 4. Resultados R2

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

Descripción paso 2:

En primera instancia se continua con la configuración en R2, se aplican comandos en R3 tanto las interfaces físicas como las virtuales, se establece el protocolo BGP entre los router R2 y R3, se los identifica, se determina el vecino y se crean las redes internas.

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

```
R3#configure terminal
R3(config)#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)#interface FastEthernet 0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#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)#exit
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)#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
```

RESULTADOS

Router 2

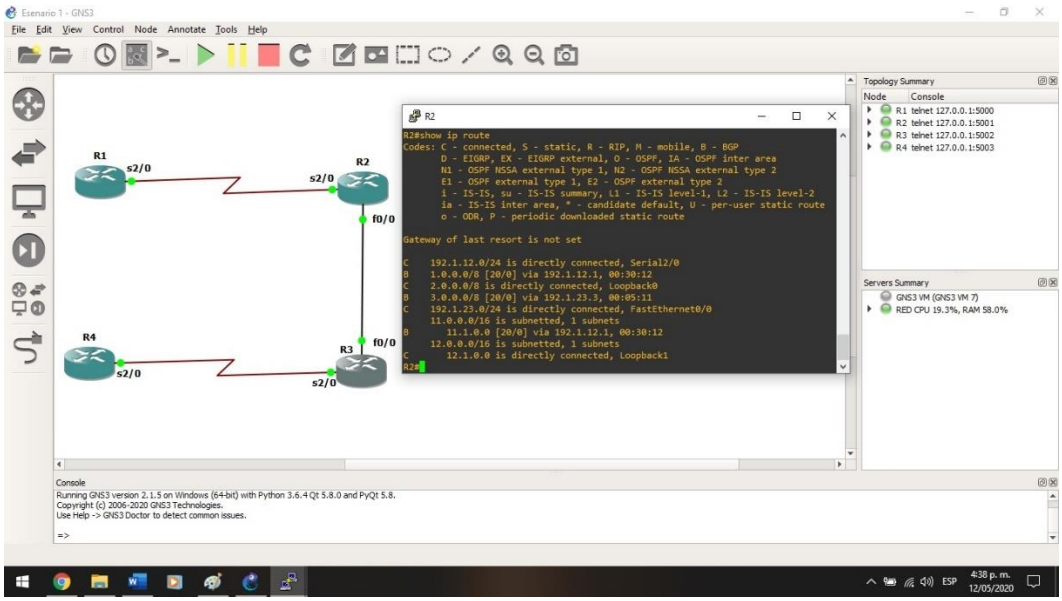

Figura 5. Resultados R2

Router 3

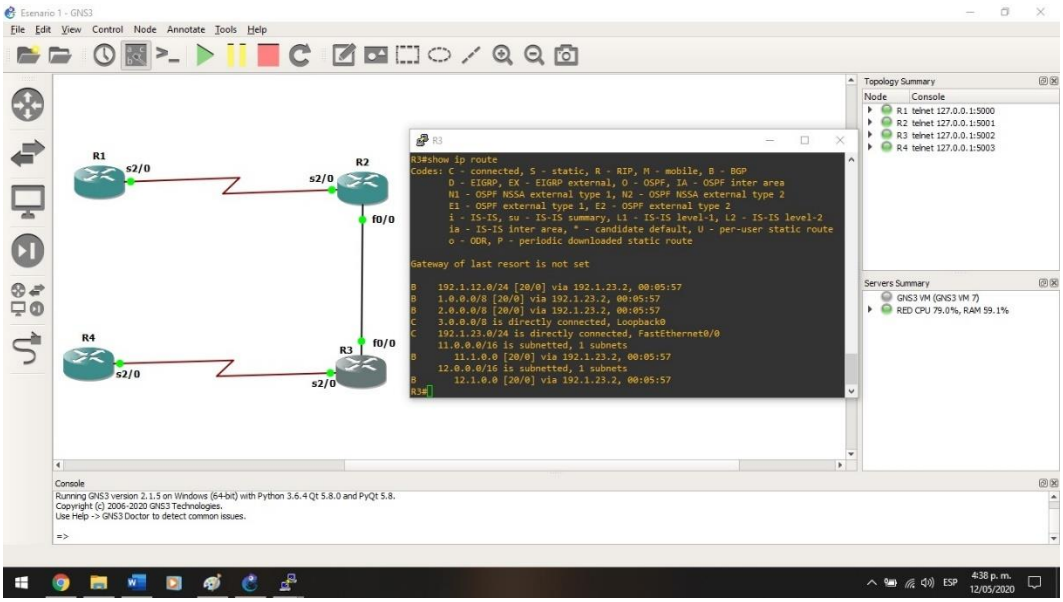

Figura 6. Resultados R3

3. Configure una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en AS3 y R4 debería estar en AS4. Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como 66.66.66.66. Establezca las relaciones de vecino con base en las direcciones de Loopback 0. Cree rutas estáticas para alcanzar la Loopback 0 del otro router. No anuncie la Loopback 0 en BGP. Anuncie la red Loopback de R4 en BGP. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

Descripción paso 3:

En primera instancia se continua con la configuración en R3, se aplican comandos en R4 tanto las interfaces físicas como las virtuales, se establece el protocolo BGP entre los router R3 y R4, se los identifica, se determina el vecino y se crean las redes internas.

R3#configure terminal
R3(config)#router bgp 3
R3(config-router)#neighbor 192.1.34.4 remote-as 4

```
R3(config-router)#network 192.1.34.0 mask 255.255.255.0
R4#configure terminal
R4(config)#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)#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)#exit
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 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
```

RESULTADOS

Router 3

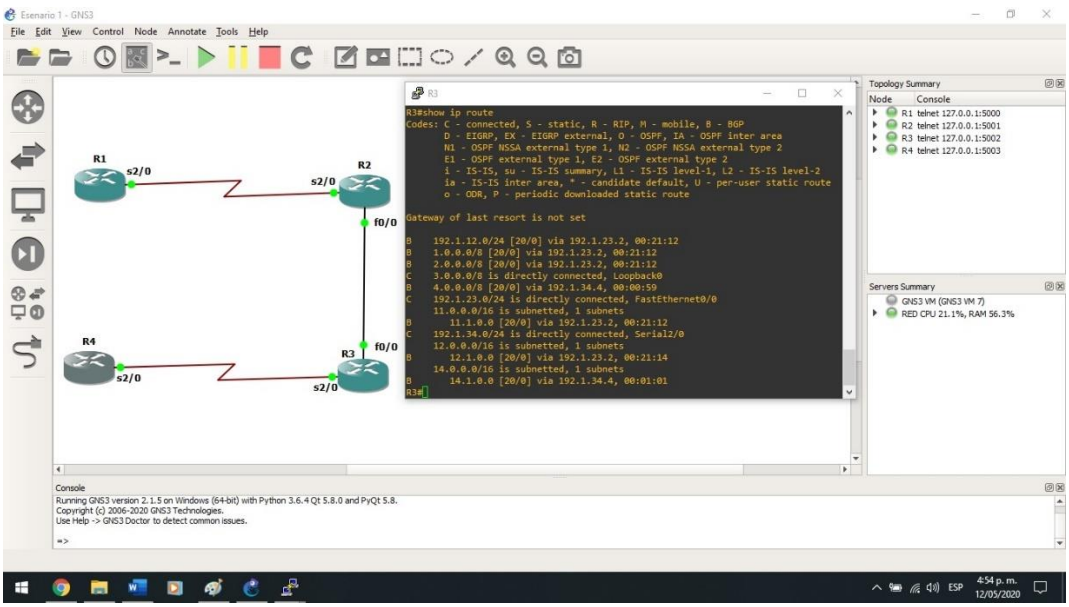

Figura 7. Resultados R3

Router 4

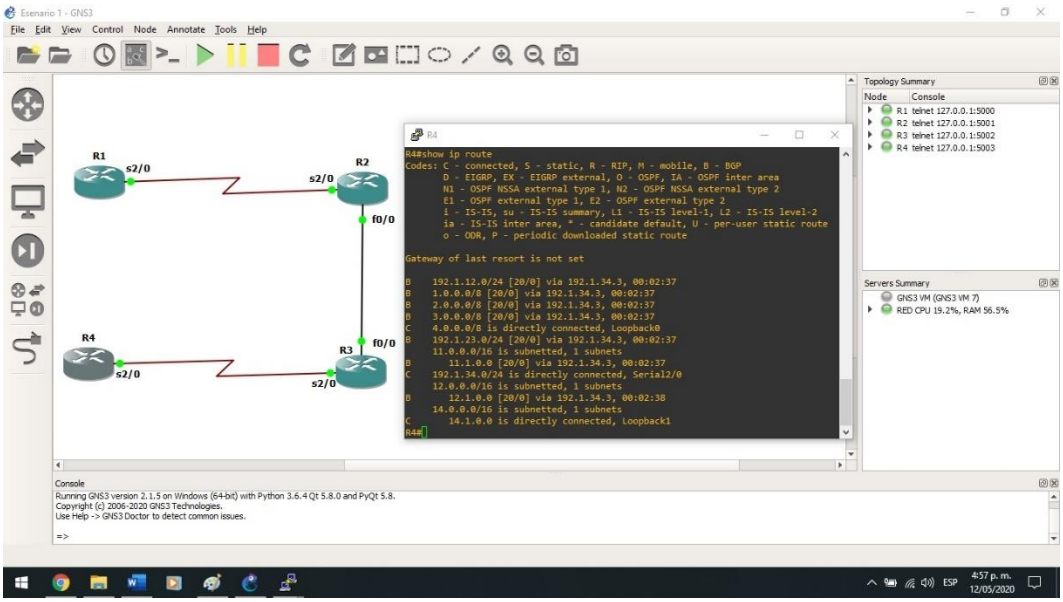

Figura 8. Resultados R4

Escenario 2

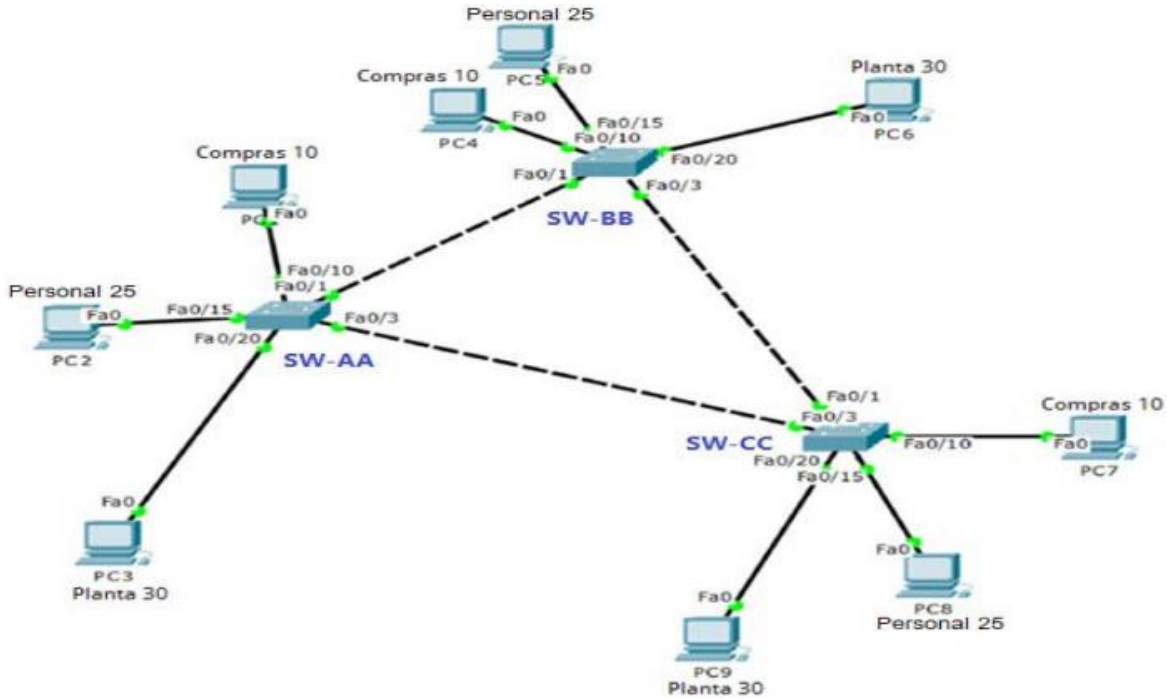

Figura 9. Escenario 2

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.

Se establece SW-AA como cliente, se fija en el dominio CCNP y se le agrega una contraseña

SW-AA#configure terminal
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

2. Verifique las configuraciones mediante el comando show vtp status

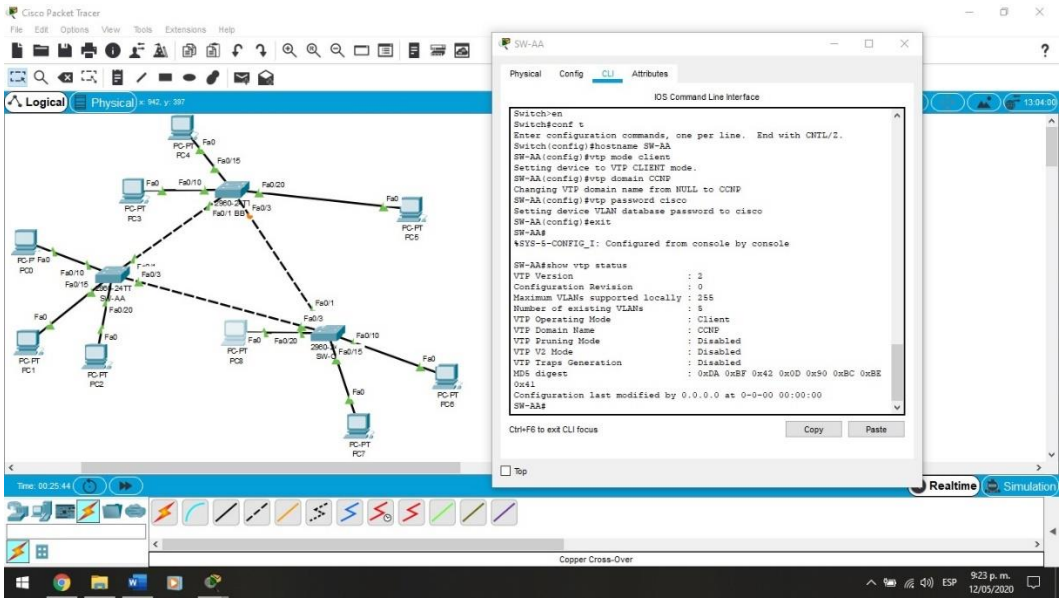

Figura 10. Resultado VTP SW-AA

Se establece SW-BB como servidor, se fija en el dominio CCNP y se le agrega una contraseña

SW-BB#configure terminal
SW-BB (config)#vtp mode server
Setting device to VTP SERVER mode.
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

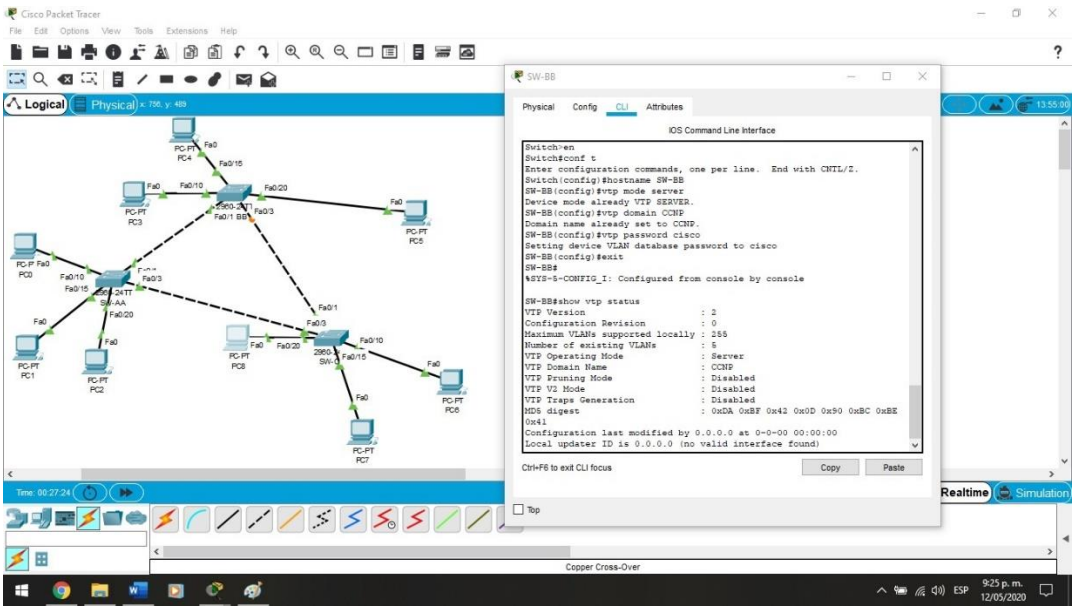

Figura 11. Resultado VTP SW-BB

Se establece SW-CC como cliente, se fija en el dominio CCNP y se le agrega una contraseña.

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

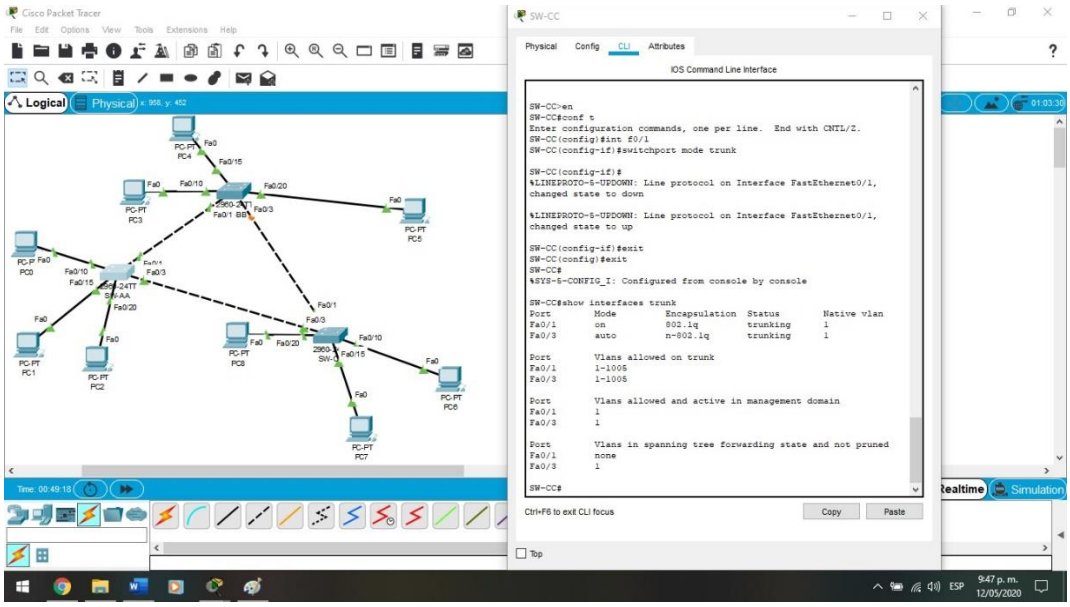

Figura 12. Resultado VTP SW-CC

B. Configurar DTP (Dynamic Trunking Protocol)

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

Se determina interfaz que se comunica con el SW-AA como enlace troncal

SW-BB#configure terminal
SW-BB (config)#interface fastEthernet 0/1
SW-BB (config-if)#switchport mode dynamic desirable

4. Verifique el enlace "trunk" entre SWT1 y SWT2 usando el comando show interfaces trunk.

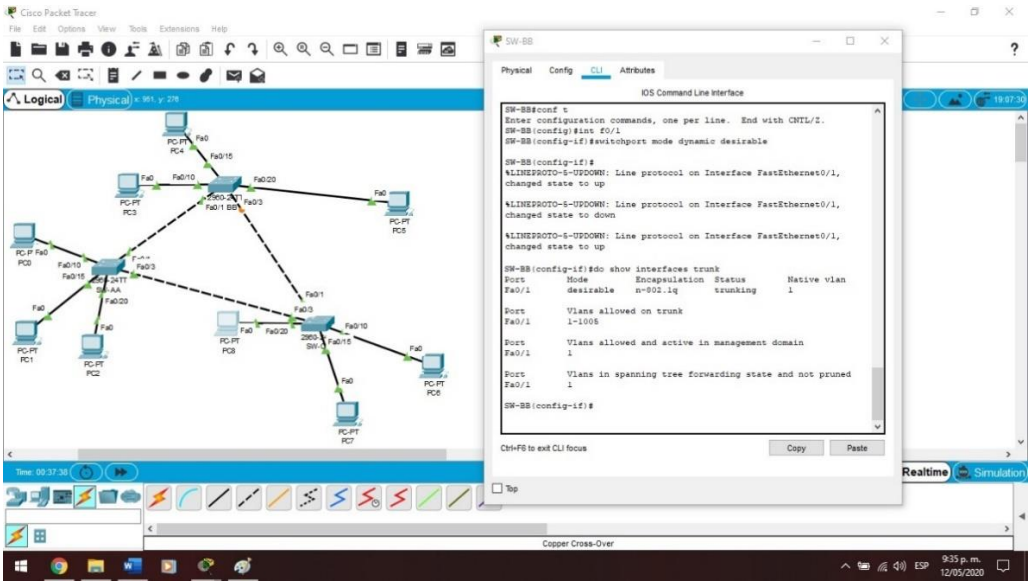

Figura 13. Resultado DTP SW-BB

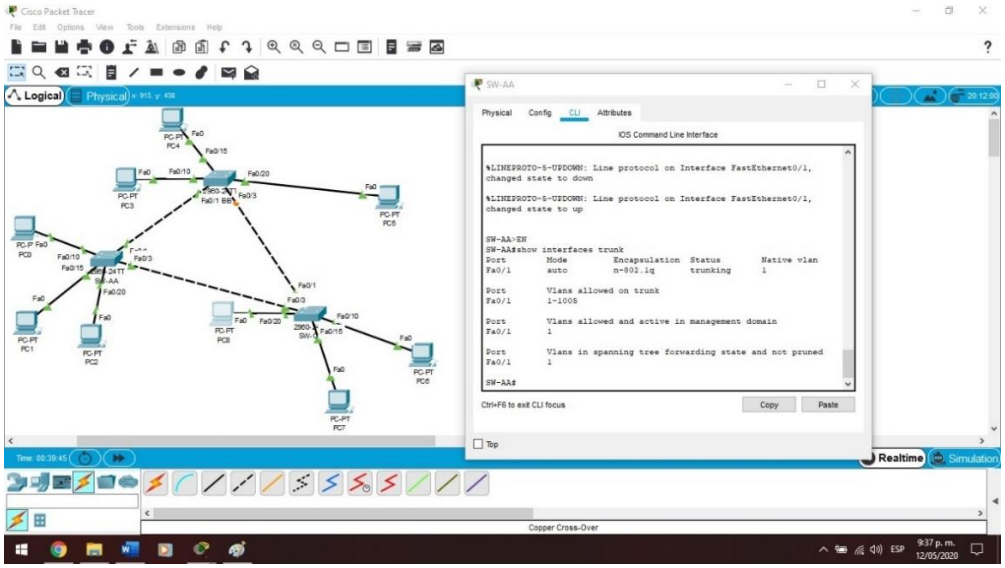

Figura 14. Resultado DTP SW-AA

5. 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

Se determina interfaz que se comunica con el SW-BB como enlace troncal

SW-AA#configure terminal
SW-AA(config)#interface fastEthernet 0/3
SW-AA(config-if)#switchport mode trunk

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

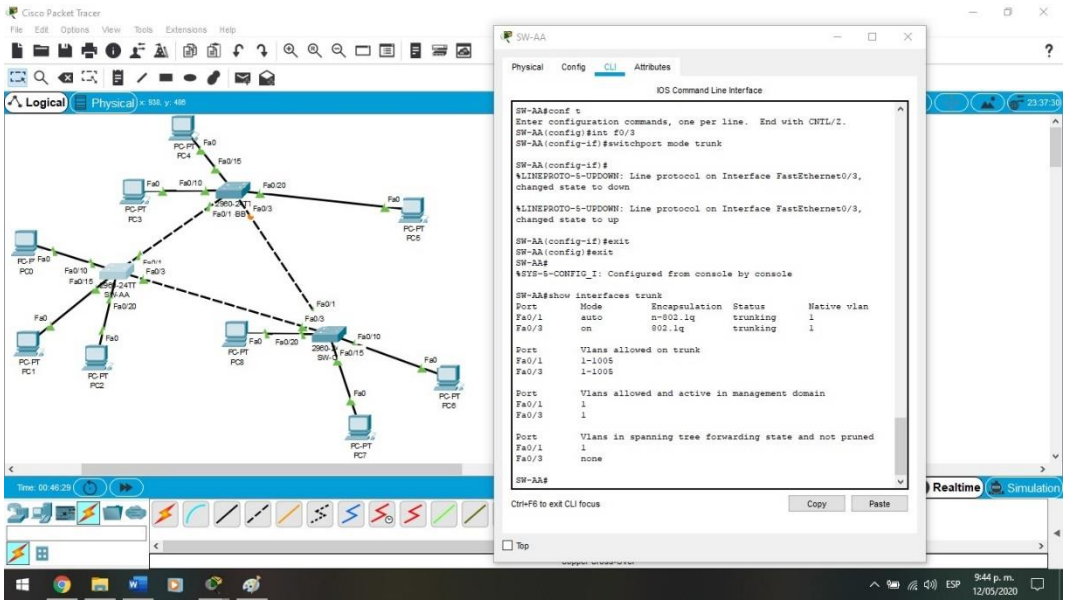

Figura 15. Resultado DTP SW-AA

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

Se determina interfaz que se comunica con el SW-BB como enlace troncal

SW-CC#configure terminal
SW-CC (config)#interface fastEthernet 0/1
SW-CC (config-if)#switchport mode trunk

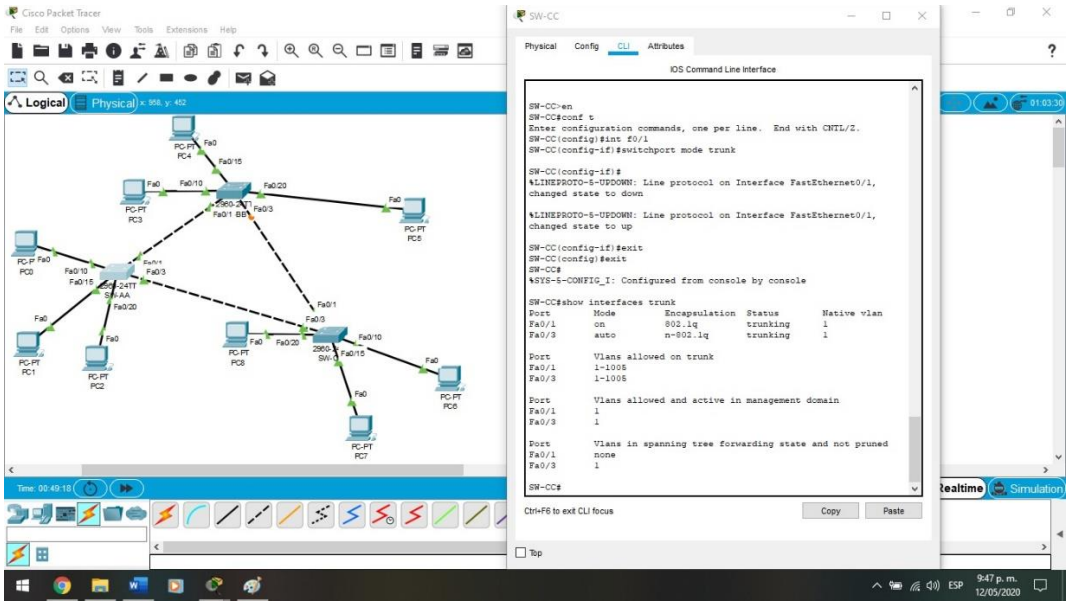

Figura 16. Resultado DTP SW-CC

C. Agregar VLANs y asignar puertos.

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

Primero se ingresa a la VLAN 10 desde SSW-AA, a continuación se agregan las VLAN desde el servidor SW-BB.

SW-AA#configure terminal
SW-AA(config)#vlan 10

SW-BB#configure terminal
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)#exit

9. Verifique que las VLANs han sido agregadas correctamente.

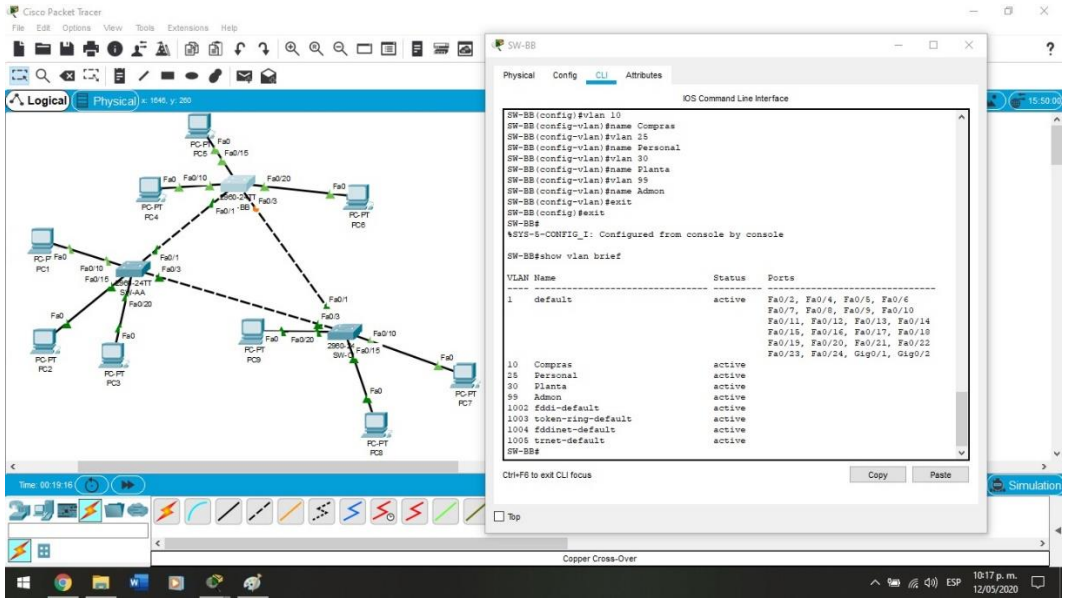

Figura 17. Resultado VLAN SW-BB

Resultados SW-AA y SW-CC

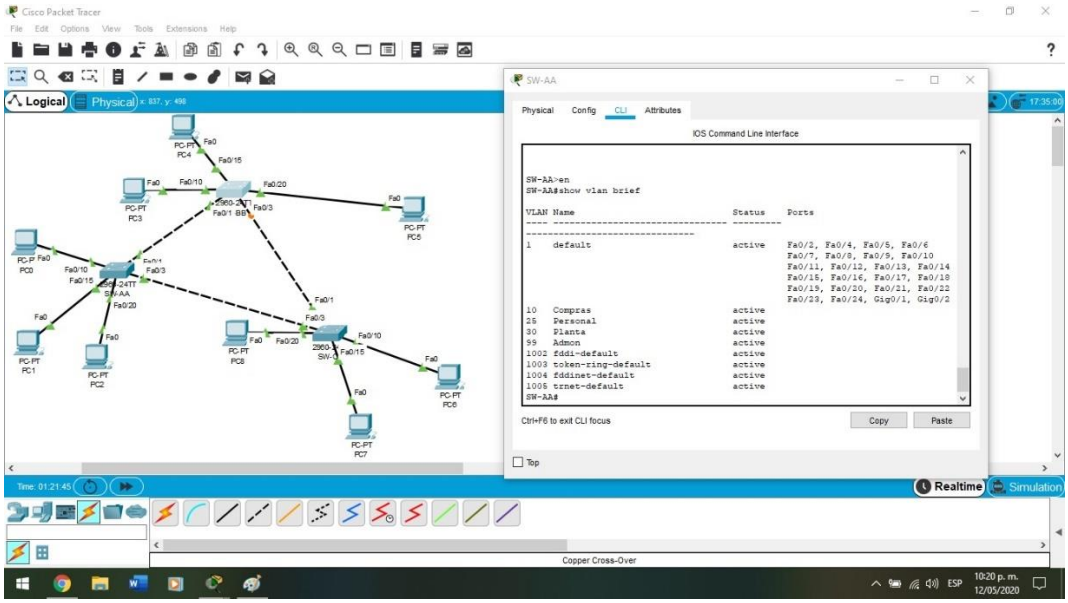

Figura 18. Resultado VLAN SW-AA

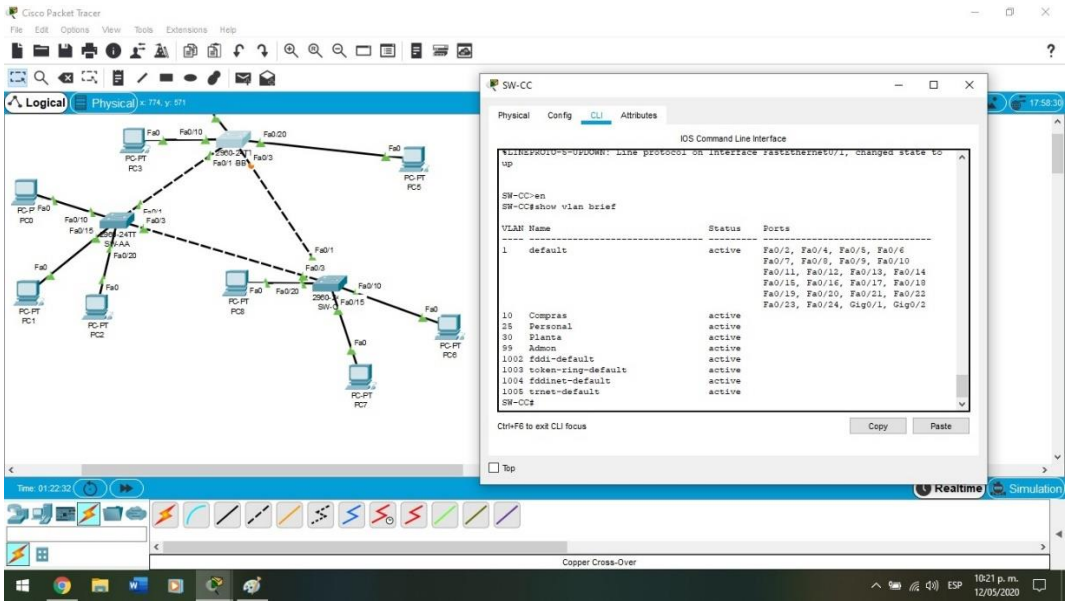

Figura 19. Resultado VLAN SW-CC

10. 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

X = número de cada PC particular

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

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

Se configuran cada interfaz en su correspondiente VLAN según la tabla, este paso se realiza en los tres Switch

SW-AA #configure terminal
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)#interface FastEthernet 0/15
SW-AA (config-if)#switchport mode access
SW-AA (config-if)#switchport access vlan 25
SW-AA (config)#interface FastEthernet 0/20
SW-AA (config-if)#switchport mode access
SW-AA (config-if)#switchport access vlan 30

SW-BB#configure terminal
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)#interface FastEthernet 0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config)#interface FastEthernet 0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30

SW-CC#configure terminal
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)#interface FastEthernet 0/15
SW-CC (config-if)#switchport mode access
SW-CC (config-if)#switchport access vlan 25
SW-CC (config)#interface FastEthernet 0/20
SW-CC (config-if)#switchport mode access
SW-CC (config-if)#switchport access vlan 30

Direccionamiento de PCs

En este punto se fija una dirección IP en cada uno de los Host, siguiendo la indicación del cuadro

PC1: 190.108.10.1 /24
PC2: 190.108.20.2 /24
PC3: 190.108.30.3 /24
PC4: 190.108.10.4 /24
PC5: 190.108.20.5 /24
PC6: 190.108.30.6 /24
PC7: 190.108.10.7 /24
PC8: 190.108.20.8 /24
PC9: 190.108.30.9 /24

D. Configurar las direcciones IP en los Switches.

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

Fijamos a cada Switch una misma VLAN con su correspondiente direccionamiento

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

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

E. Verificar la conectividad Extremo a Extremo

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

Los ping que se realizaron entre PCs de la misma Vlan tienen éxito, sin embargo entre Pcs de distintas Vlan el ping falla debido a que no existe enrutamiento entre las Vlan

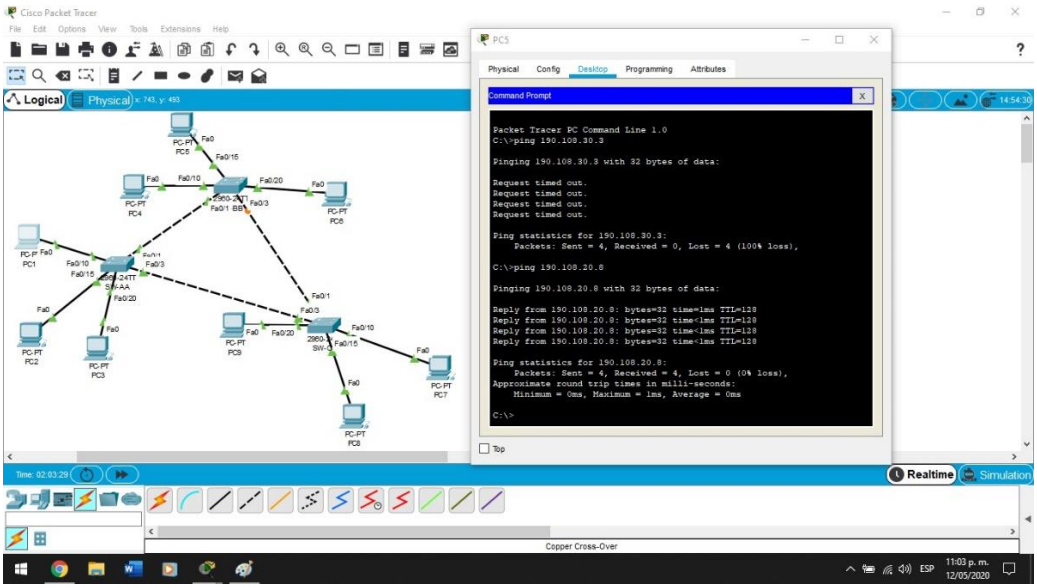

Figura 20. Ping desde PC5

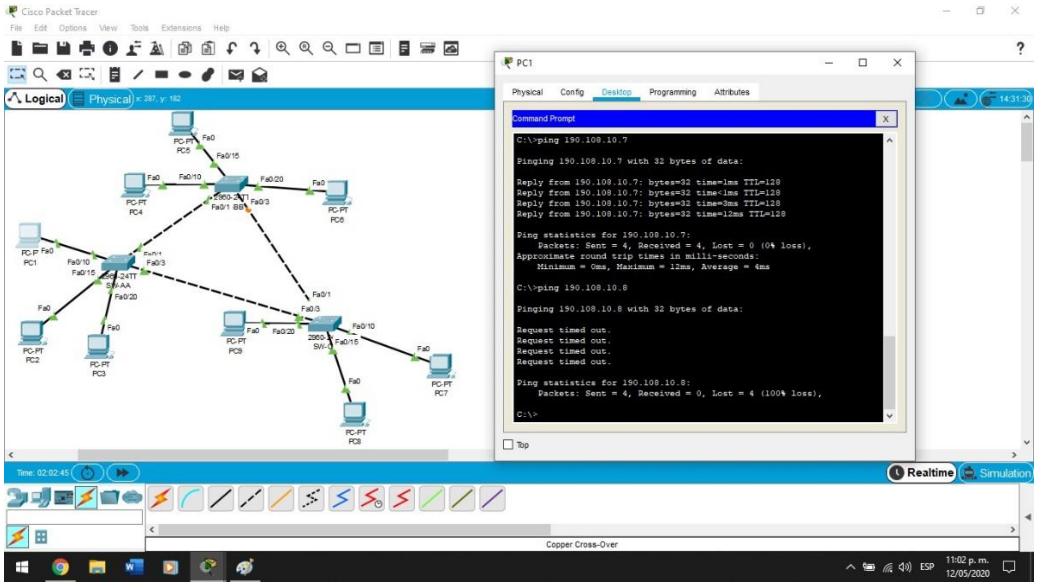

Figura 21. Ping desde PC1

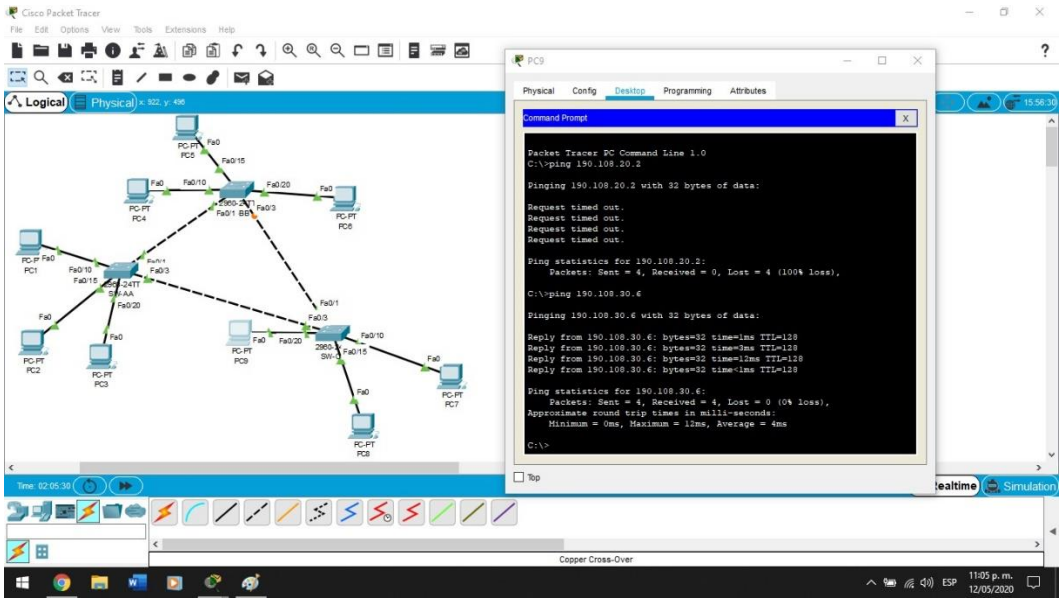

Figura 22. Ping desde PC9

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

Todos los ping entre los Switch fueron exitosos debido a que los tres se encuentran en la misma Vlan

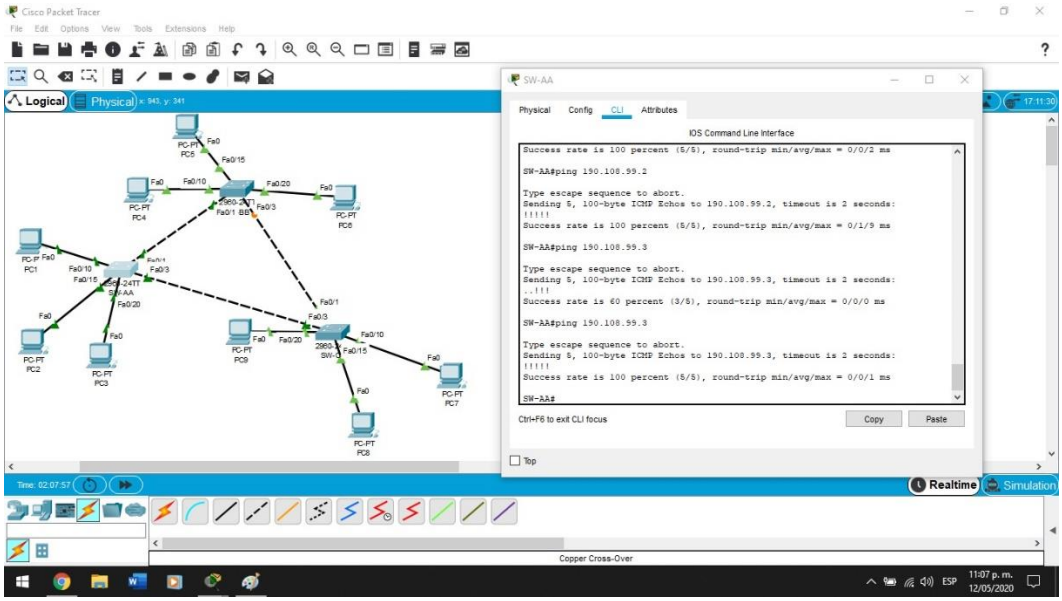

Figura 23. Ping desde SW-AA

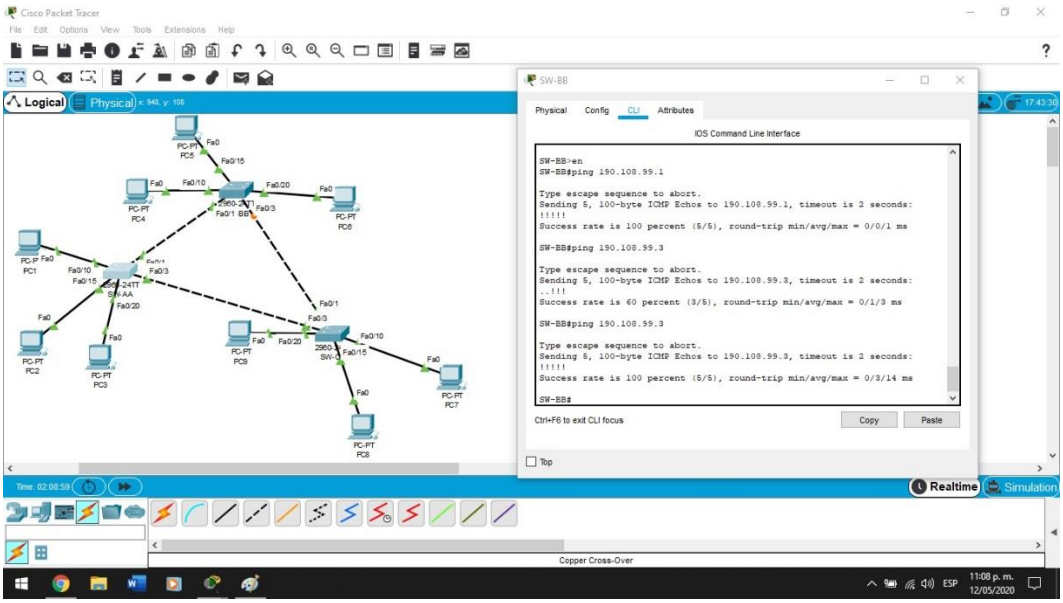

Figura 24. Ping desde SW-BB

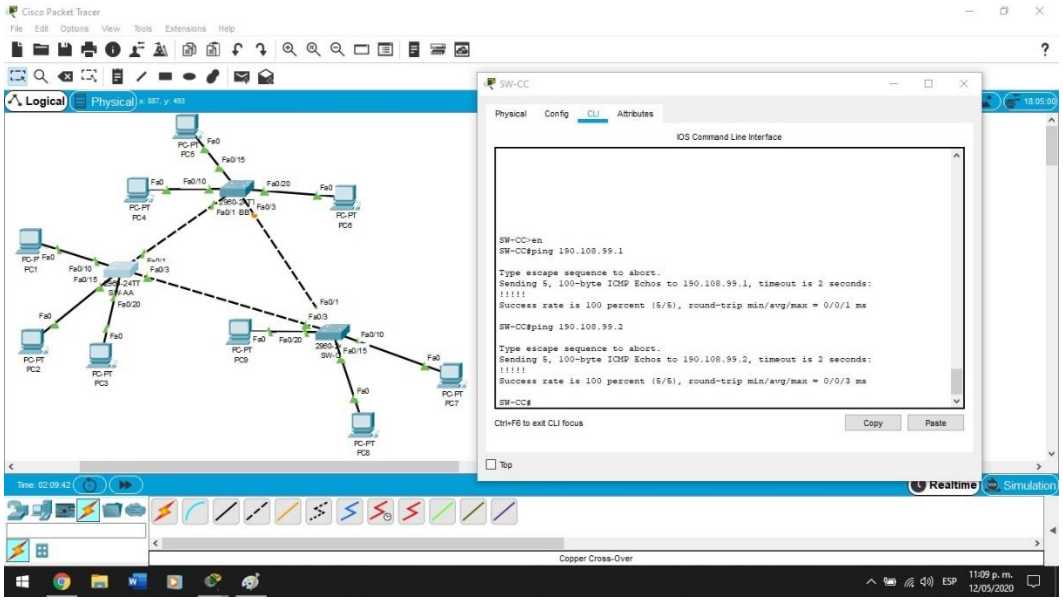

Figura 25. Ping desde SW-CC

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

Los ping no tienen éxito debido a que no se ha fijado una dirección IP a cada una de las VLAN creadas para la comunicación entre Host

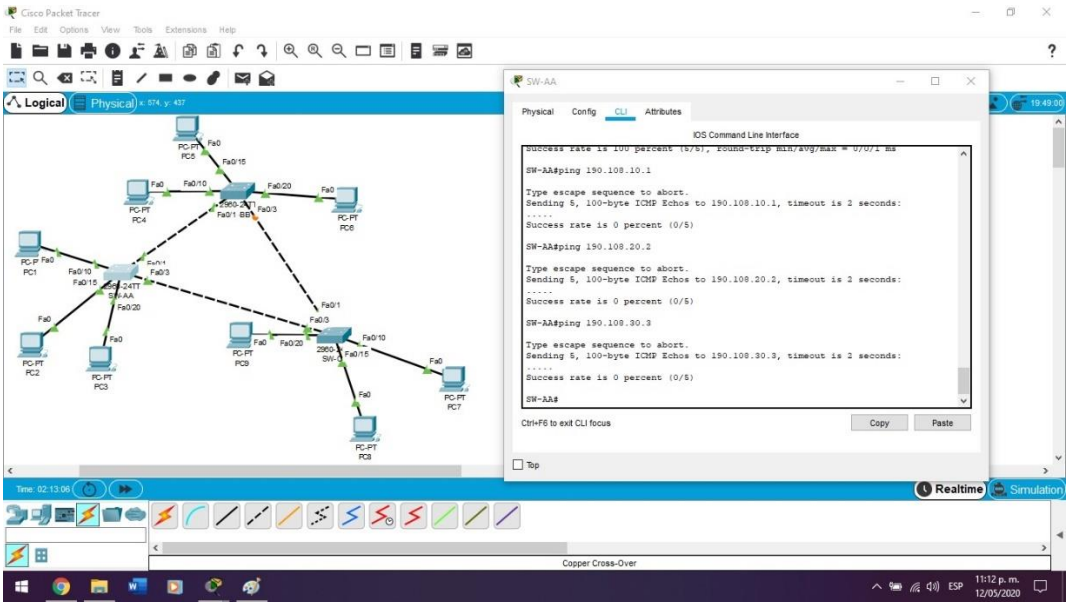

Figura 26. Ping desde SW-AA

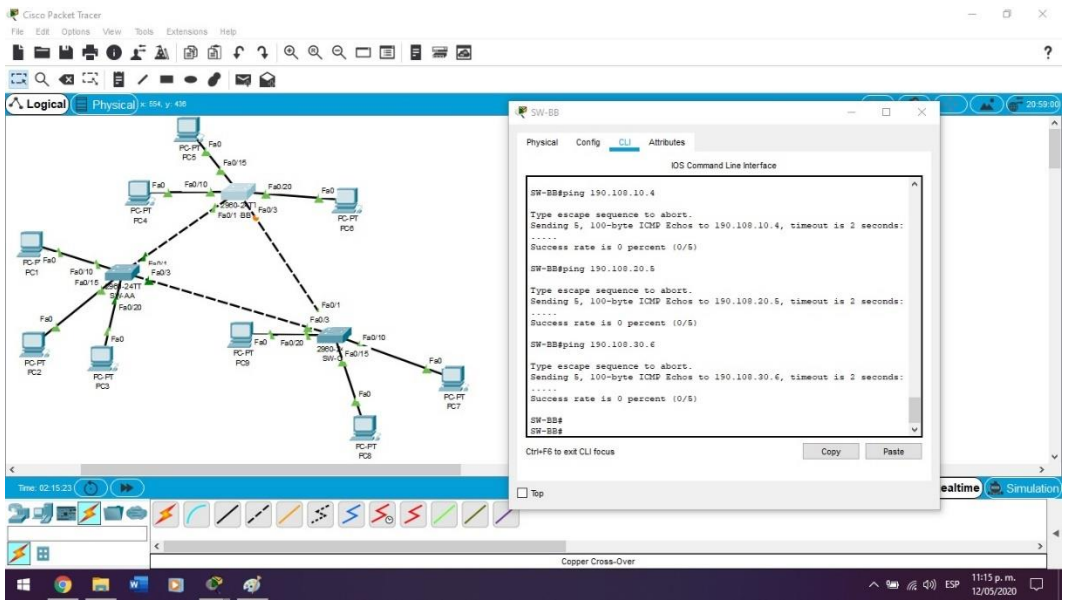

Figura 27. Ping desde SW-BB

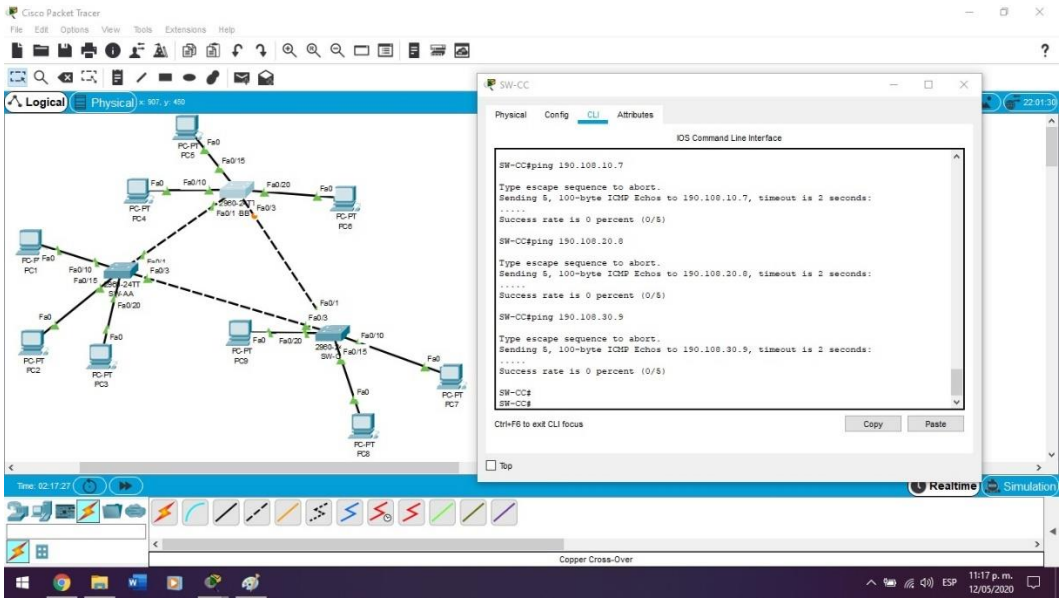

Figura 28. Ping desde SW-CC

CONCLUSIONES

Se obtuvo éxito al hacer los pings entre los switch que comparten la misma VLAN por ende la simulación fue satisfactoria.

Se logro implementar los diferentes códigos en el área de TTP, VLAN, DTP con equipos cisco mediante el software cisco Packet Tracer.

Se aprendió a desarrollar los diferentes conocimientos de enrutamiento BGP por medio del software GNS3.

Observar detalladamente los resultados de la ejecución de los comandos en busca de establecer el protocolo BGP, gracias al comando show ip route que nos permite detallar los cambios en cada router según la implementación del siguiente Router vecino.

Con la verificación en el escenario dos, se logró establecer que la red está parcialmente configurada, lo que nos permite tener en principio, la necesidad de encontrar el posible error y una vez determinado, generar una solución, para lograr el correcto desempeño de la red.

BIBLIOGRÁFIA

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

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Path Control Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx