DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JACKSON ARNULDO CARDENAS ESCOBAR

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

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JACKSON ARNULDO CARDENAS ESCOBAR

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
BOGOTÁ
2020

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

BOGOTÁ, 22 de mayo de 2020

AGRADECIMIENTOS

En primera instancia agradezco a Dios por permitirme culminar los estudios para los cuales dedique mucho tiempo con el fin de ser profesional, una meta que desde niño me trace y que en estos momentos puedo decir que lo estoy logrando, a mis familiares por estar siempre ahí al lado apoyándome e impulsándome para no desfallecer y poder alcanzar los objetivos propuestos, a mis tutores, personas con gran conocimiento que siempre estuvieron ahí para orientarme en el proceso del aprendizaje autónomo y aportaron ese granito de arena fundamental para lograr terminar mi formación universitaria.

CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

BGP: Es el protocolo de enrutamiento interdominio que reemplaza EGP. BGP intercambia información de accesibilidad con otros sistemas BGP.

ROUTER: Es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes.

SWITCH: Es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más host de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada ésta.

VLAN: Grupo de dispositivos en una LAN que están configurados para que puedan comunicarse como si estuvieran conectados al mismo cable, cuando en realidad están ubicado en varios segmentos LAN diferentes.

VTP: Es un protocolo que usa tramas troncales de capa 2 para comunicar información de VLAN entre un grupo de conmutadores y para administrar la adición, eliminación y cambio de nombre de VLAN a través de la red desde un punto central de controlar.

RESUMEN

La evaluación prueba de habilidades prácticas, forma parte de las actividades evaluativas del Diplomado de Profundización CCNP, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

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

ABSTRACT

The evaluation test of practical skills is part of the evaluative activities of the CCNP Deepening Diploma, and seeks to identify the degree of development of competencies and skills that were acquired throughout the diplomat. The essential thing is to test the levels of understanding and solving problems related to various aspects of Networking.

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

INTRODUCCIÓN

El desarrollo del presente trabajo correspondiente al diplomado de profundización permite adquirir las capacidades necesarias para el futuro profesional del estudiante, el objetivo de esta prueba de habilidades es llevar al máximo la capacidad de comprensión y análisis para desarrollar satisfactoriamente los dos escenarios propuestos los cuales se enfocaran en llevar a la parte práctica todo el conocimiento teórico que se fue adquiriendo durante el desarrollo del curso, para el desarrollo de estos dos escenarios se utilizó herramientas como Packet Tracer y GNS3 para la simulación y configuración de los escenarios y poder ver su funcionamiento según las indicaciones de la prueba de habilidades propuesta.

En el escenario 1 se muestra la implementación del protocolo de enrutamiento interdominio BGP, donde se configura la relación entre vecinos en cada router y se codifico cada router por medio de un ID.

En el escenario 2 se configura el VTP de cada Switche para la comunicación y administración de los datos, y se conectan por medio de enlaces troncales, por último, se crean unas Vlan donde se configuran sus puertos, sus modos de acceso y el direccionamiento IP de cada uno de los Switches.

DESARROLLO

1. Escenario 1

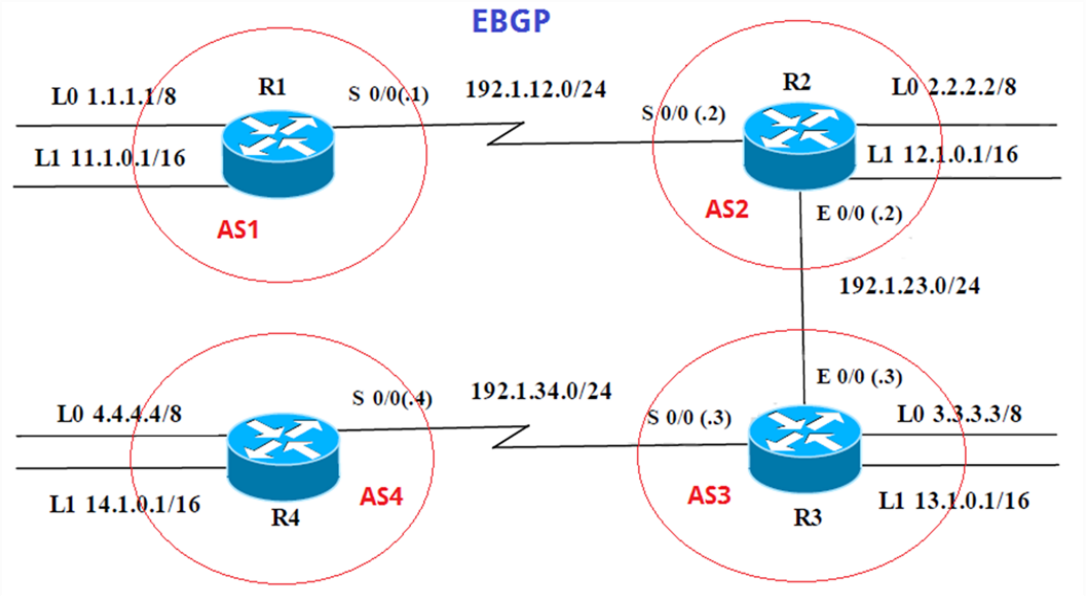

Figura 1. Topología del escenario 1

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 0/0	192.1.12.1	255.255.255.0

Tabla 1. Configuración de las interfaces de 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 las interfaces de 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 las interfaces de 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 las interfaces de R4

Diseño de la topología en GNS3

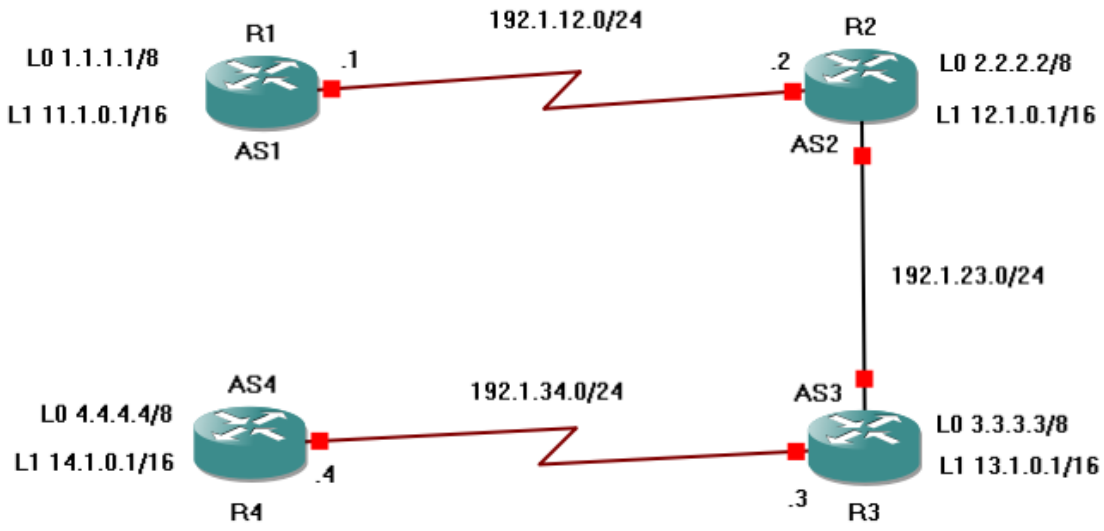

Figura 2. Topología del escenario 1 en GNS3

1. Configure 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
R1(config)#interface loopback 0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config)#interface loopback 1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config)#interface s1/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#router bgp 1
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router)#network 1.0.0.0 mask 255.0.0.0
R1(config-router)#network 192.1.12.0 mask 255.255.255.0
R1(config-router)#neighbor 192.1.12.2 remote-as 2
```

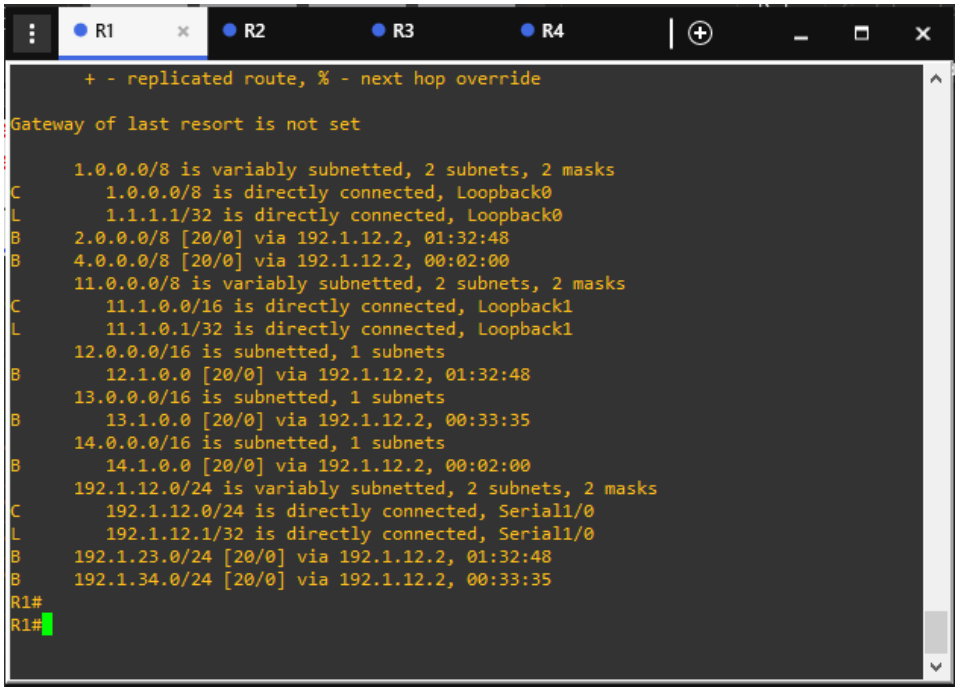

Figura 3. Comando show ip route en R1

```
R2#configure terminal
R2(config)# interface loopback 0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config)# interface loopback 1
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config)#interface s1/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shut
R2(config)#interface f0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shut
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
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)#exit
```

Figura 4. Comando show ip route en 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.*

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)#exit

R3#configure terminal
R3(config)# interface loopback 0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config)# interface loopback 1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config)#interface s1/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config)#interface f0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
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 192.1.23.0 mask 255.255.255.0
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)#neighbor 192.1.23.2 remote-as 2

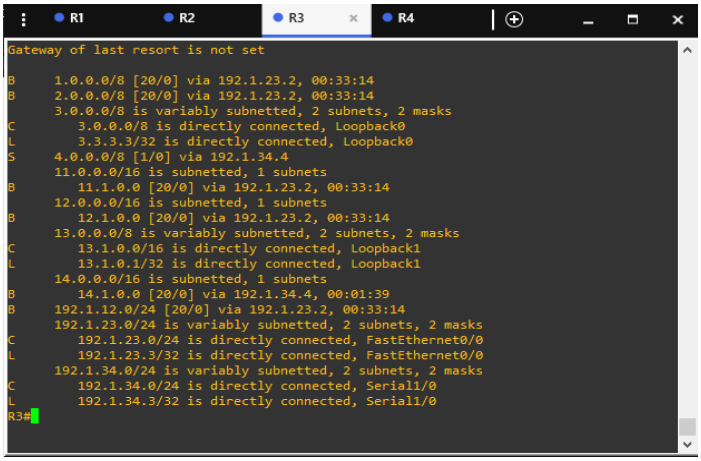

Figura 5. Comando show ip route en R3

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.*

```
R3(config-router)#network 192.1.34.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#exit
R3(config)#ip route 4.0.0.0 255.0.0.0 192.1.34.4
R3(config)#router bgp 3
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
R3(config-router)#exit
```

```
R4#configure terminal
R4(config)# interface loopback 0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config)# interface loopback 1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config)#interface s1/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shut
R4(config-if)#exit
R4(config)#ip route 3.0.0.0 255.0.0.0 192.1.34.3
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
R4(config-router)#neighbor 3.3.3.3 remote-as 3
R4(config-router)#neighbor 3.3.3.3 update-source loopback 0
R4(config-router)#neighbor 3.3.3.3 ebgp-multihop
R4(config-router)#exit
```

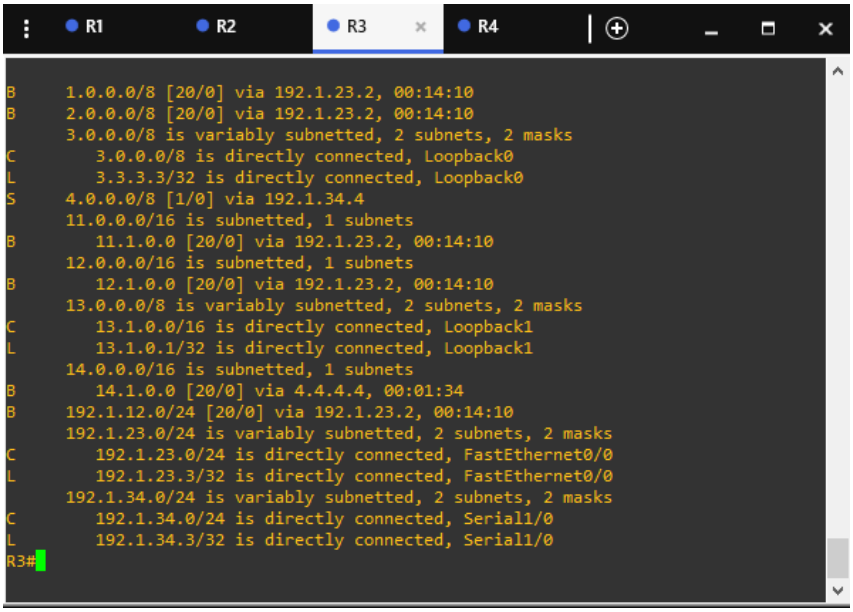

Figura 6. Comando show ip route en R3

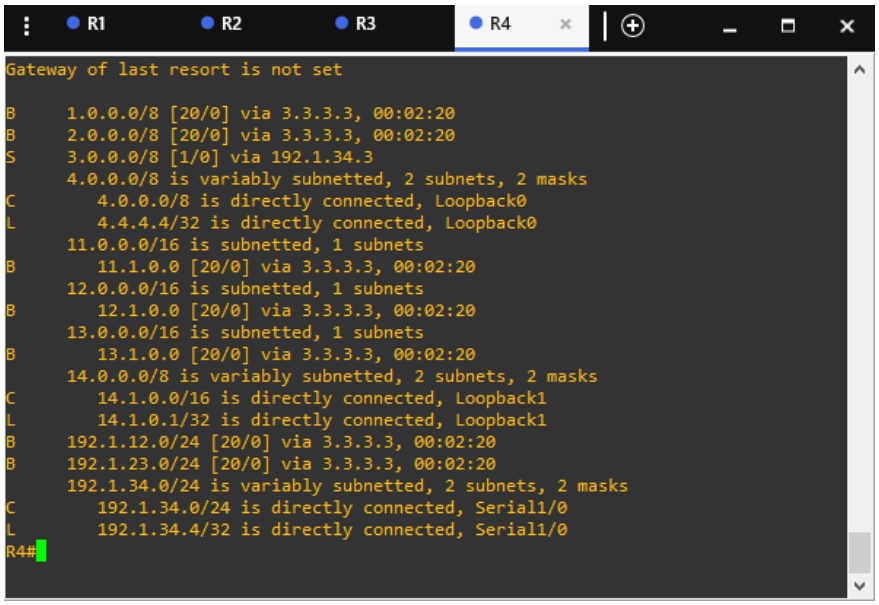

Figura 7. Comando show ip route en R4

Las tablas de enrutamiento que se anexan como evidencia ya se encuentran actualizadas ya que primero se configuro los routers y después se empezó a montar el documento con las evidencias.

En el punto 3 se evidencia el cambio de la tabla de enrutamiento en el Router 3 por la modificación de las relaciones en los vecinos con base en las direcciones de Loopback 0, por último, se realizará un ping de extremo a extremo para verificar la conectividad.

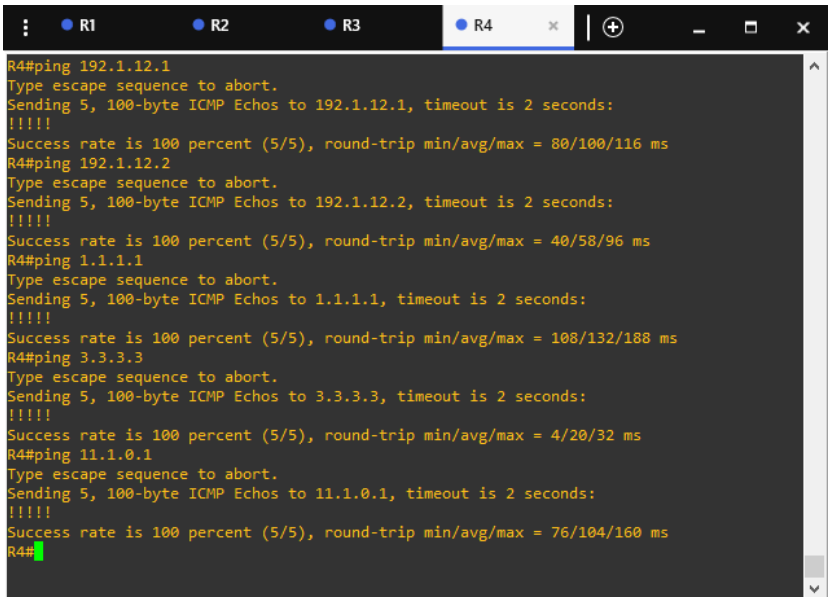

Figura 8. Ping desde R4 a R1 y R2

2. Escenario 2

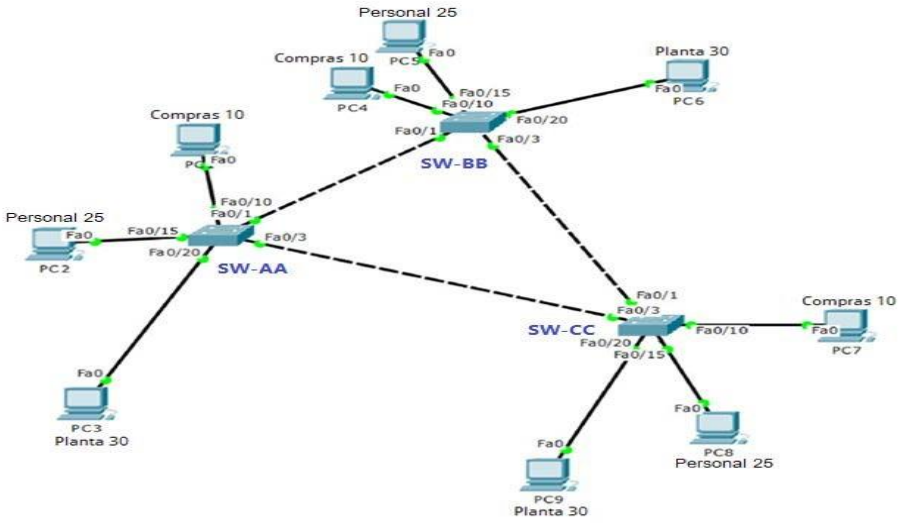

Figura 9. Topología del escenario 2

Diseño de la topología en Packet Tracer.

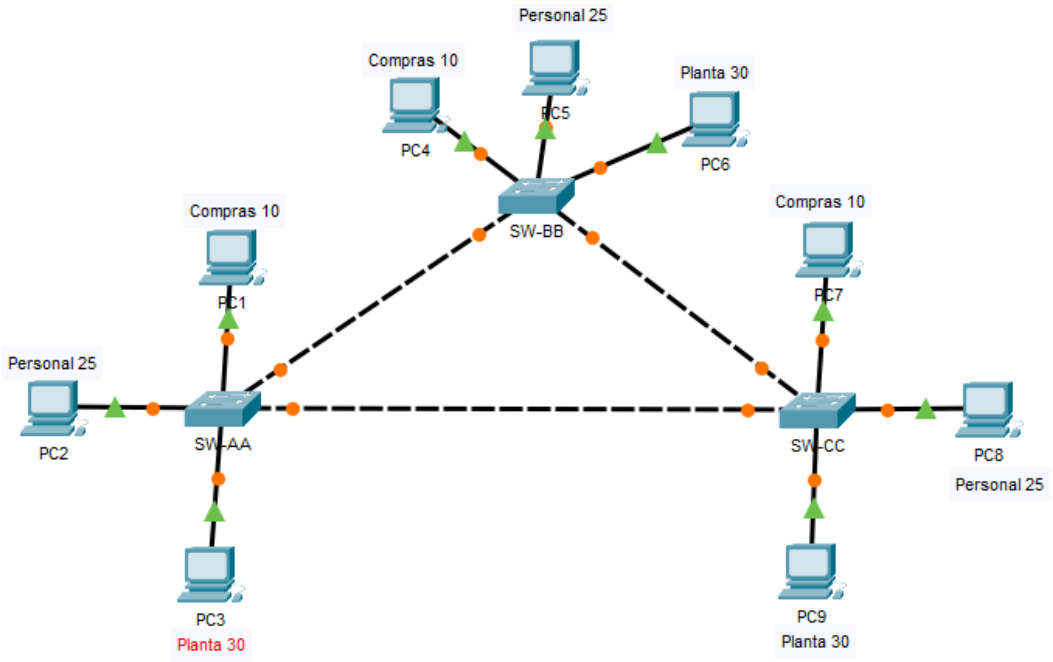

Figura 10. Diseño de la topología en Packet Tracer

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(config)#vtp mode client
SW-AA(config)#vtp domain CCNP
SW-AA(config)#vtp password cisco

SW-BB(config)#vtp mode server
SW-BB(config)#vtp domain CCNP
SW-BB(config)#vtp password cisco

SW-CC(config)#vtp mode client
SW-CC(config)#vtp domain CCNP
SW-CC(config)#vtp password cisco
```

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

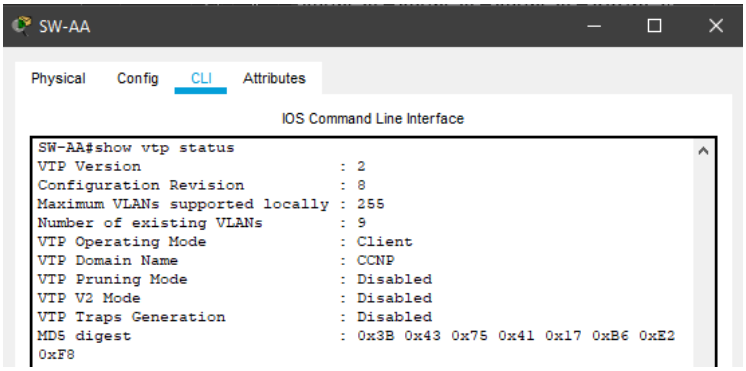

Figura 11. Comando show vtp status

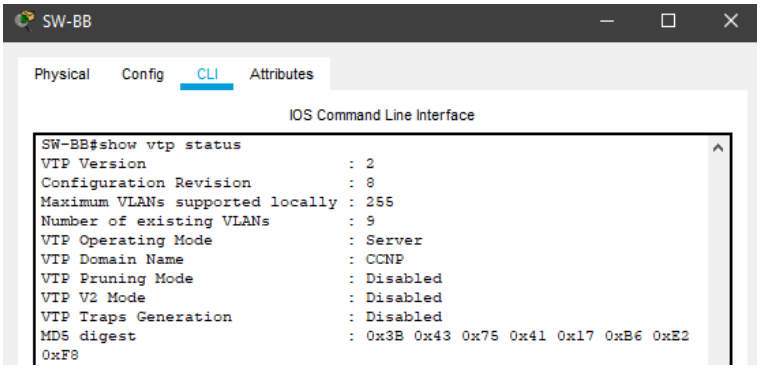

Figura 12. Comando show vtp status

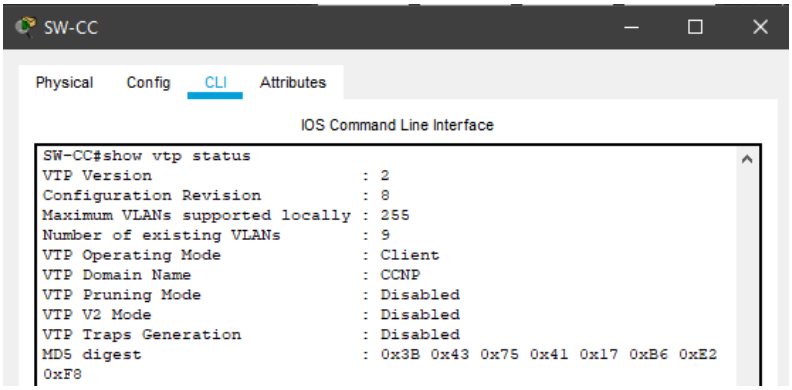

Figura 13. Comando show vtp status

B. Configurar DTP (Dynamic Trunking Protocol)

1. 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#configure terminal
SW-BB(config)#interface f0/1
SW-BB(config-if)#switch mode dynamic desirable
SW-BB(config-if)#exit

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

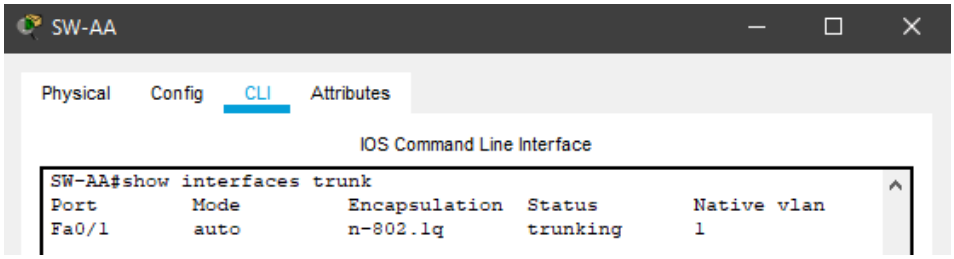

Figura 14. Comando show interface trunk

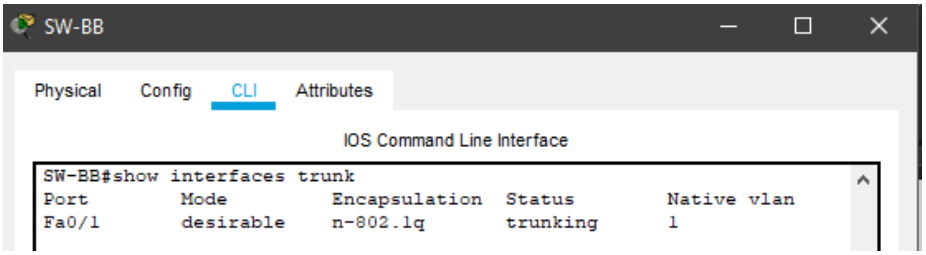

Figura 15. Comando show interface trunk

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

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

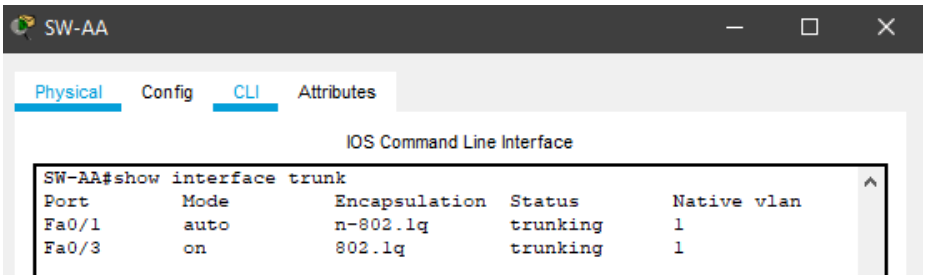

Figura 16. Comando show interface trunk

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

```
SW-BB#configure terminal
SW-BB(config)#interface f0/3
SW-BB(config-if)#switchport mode trunk
```

C. Agregar VLANs y asignar puertos.

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

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

```
SW-BB#configure terminal
SW-BB(config)#vlan 10
SW-BB(config-vlan)#name Compras
SW-BB(config-vlan)#exit
SW-BB(config)#vlan 25
SW-BB(config-vlan)#name Personal
SW-BB(config-vlan)#exit
SW-BB(config)#vlan 30
SW-BB(config-vlan)#name Planta
SW-BB(config-vlan)#exit
SW-BB(config)#vlan 99
SW-BB(config-vlan)#name Admon
SW-BB(config-vlan)#exit
```

2. Verifique que las VLANs han sido agregadas correctamente.

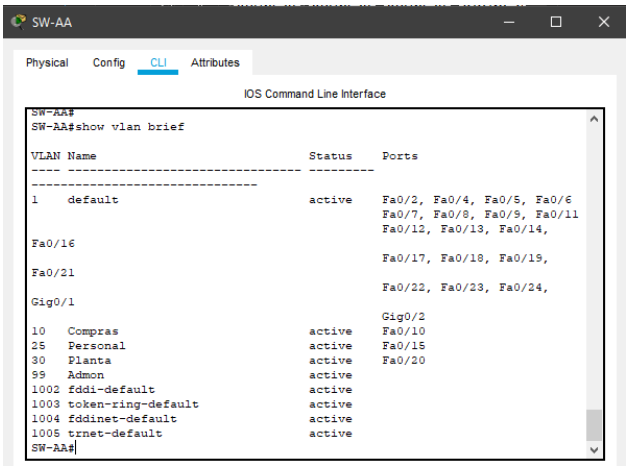

Figura 17. Comando show vlan brief en SW-AA

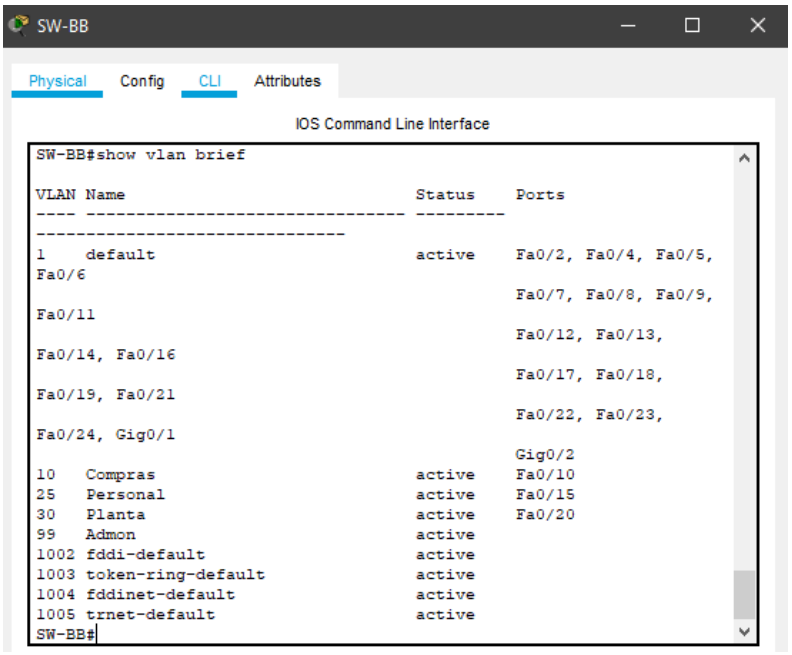

Figura 18. Comando show vlan brief en SW-BB

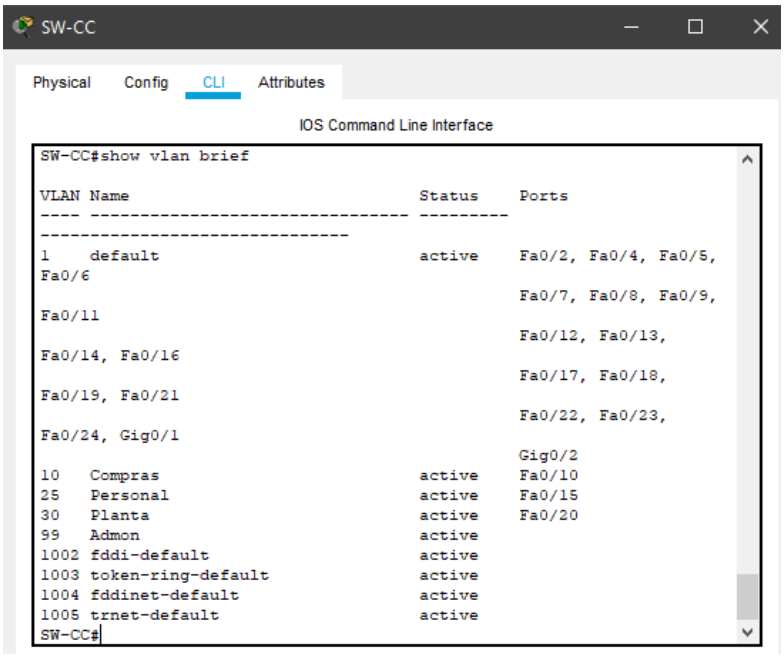

Figura 19. Comando show vlan brief en SW-CC

3. 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. Tabla de asociación de los puertos a las Vlan y las direcciones Ip

Se asigna una ip a cada uno de los computadores por medio de la tabla.

Antes de asignar las ip a los Pc se configura las direcciones Ip para asociar cada una de las interfaces.

```
SW-AA(config)#interface vlan 10
SW-AA(config-if)#ip address 190.108.10.1 255.255.255.0
SW-AA(config-if)#interface vlan 25
SW-AA(config-if)#ip address 190.108.20.1 255.255.255.0
SW-AA(config-if)#interface vlan 30
SW-AA(config-if)#ip address 190.108.30.1 255.255.255.0
```

```
SW-BB(config)#interface vlan 10
SW-BB(config-if)#ip address 190.108.10.2 255.255.255.0
SW-BB(config-if)#interface vlan 25
SW-BB(config-if)#ip address 190.108.20.2 255.255.255.0
SW-BB(config-if)#interface vlan 30
SW-BB(config-if)#ip address 190.108.30.2 255.255.255.0
```

```
SW-CC(config)#interface vlan 10
SW-CC(config-if)#ip address 190.108.10.3 255.255.255.0
SW-CC(config-if)#interface vlan 25
SW-CC(config-if)#ip address 190.108.20.3 255.255.255.0
SW-CC(config-if)#interface vlan 30
SW-CC(config-if)#ip address 190.108.30.3 255.255.255.0
```

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

10. 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#configure terminal
SW-AA(config)#interface f0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#exit
SW-AA(config)#interface f0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#exit
SW-AA(config)#interface f0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30

SW-BB#configure terminal
SW-BB(config)#interface f0/10
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#exit
SW-BB(config)#interface f0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#exit
SW-BB(config)#interface f0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30

SW-CC#configure terminal
SW-CC(config)#interface f0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#exit
```

```
SW-CC(config)#interface f0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#exit
SW-CC(config)#interface f0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30
```

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 6. Configuracion de las direcciones Ip de los Switches

```
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

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

   Se ejecuta el ping desde los PC, se aclara que solo hará ping correctamente con los PC que estén en la misma Vlan, por ejemplo, en el PC1 hará ping con los PC4 y PC7 ya que estos pertenecen a la misma Vlan de lo contrario el resto fallara, como ejemplo se anexa los pings que pueden desarrollar cada uno de ellos.

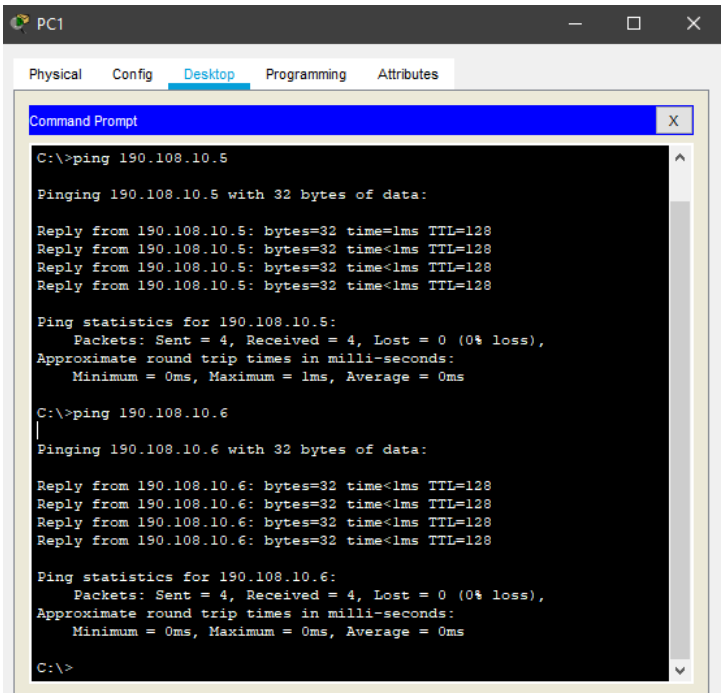

Figura 20. Ping desde PC1

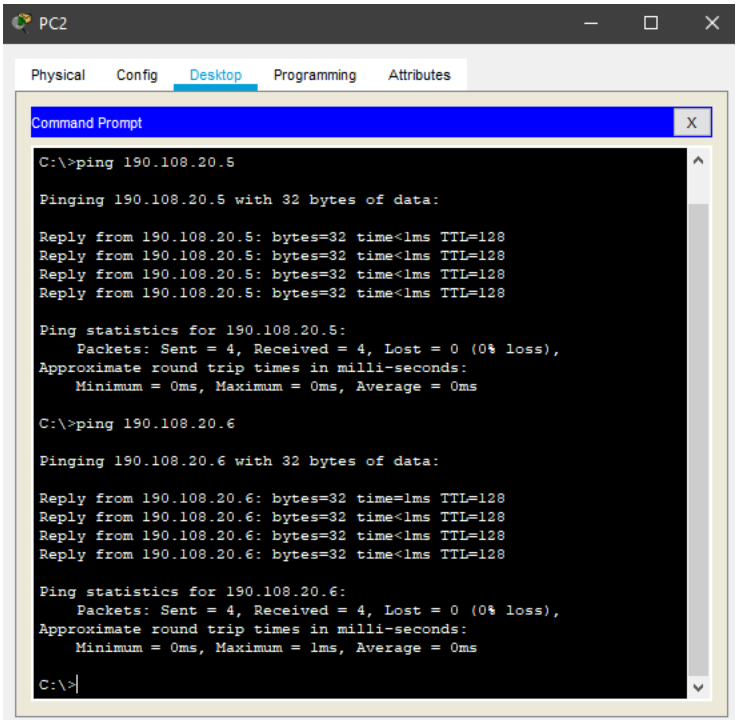

Figura 21. Ping desde PC2

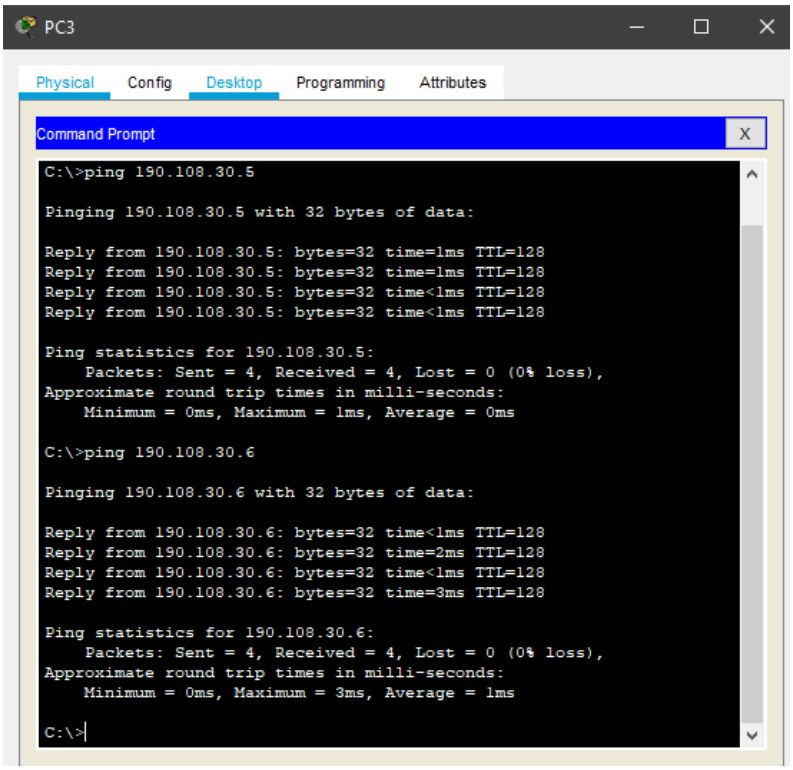

Figura 22. Ping desde PC3

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

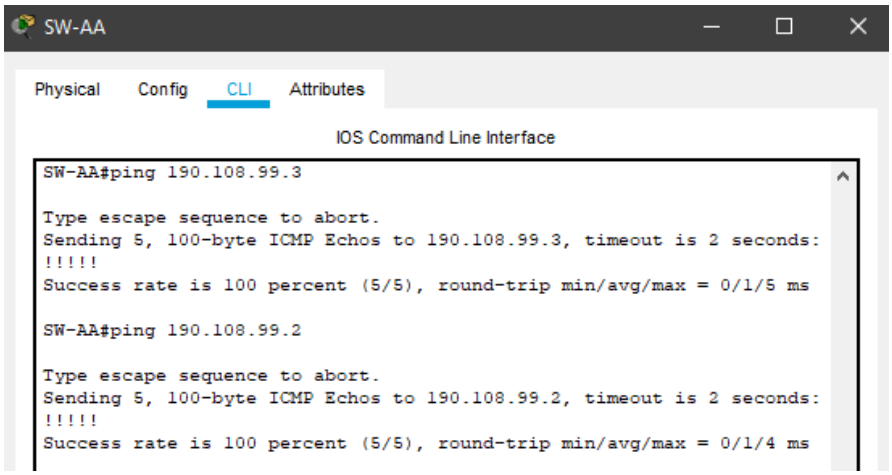

Figura 23. Ping desde SW-AA a SW-BB y SW-CC

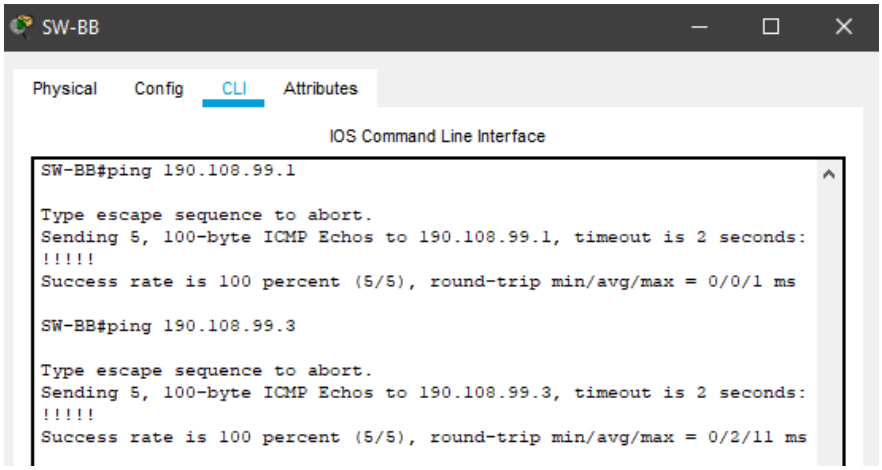

Figura 24. Ping desde SW-BB a SW-AA y SW-CC

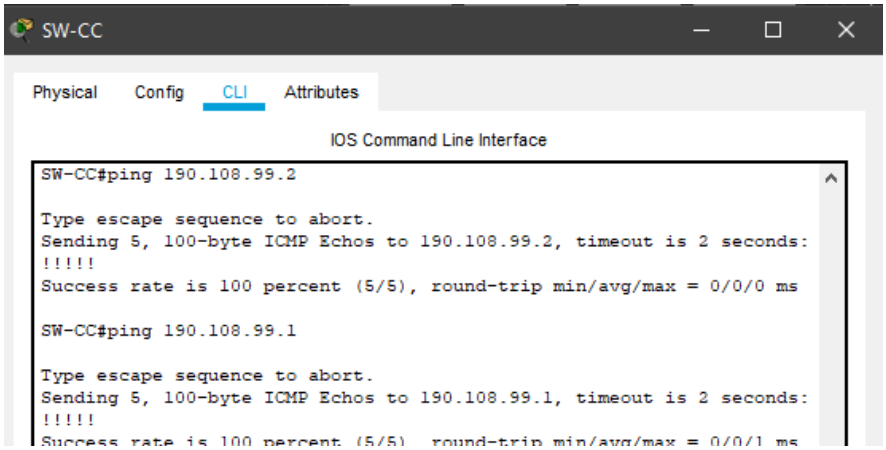

Figura 25. Ping desde SW-CC a SW-AA y SW-BB

Los pings entre los Switches fueron satisfactorio gracias a la configuración que se realizó previamente del modo troncal entre las interfaces físicas conectadas.

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

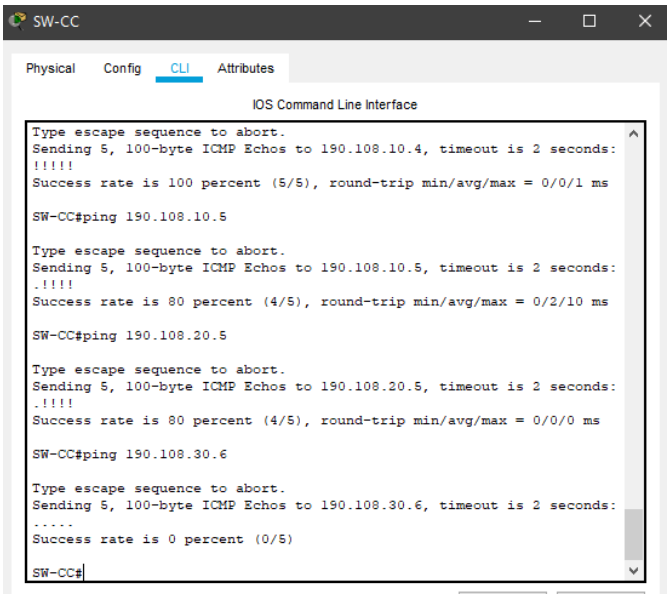

Figura 26. Ping desde SW-CC a distintos PC

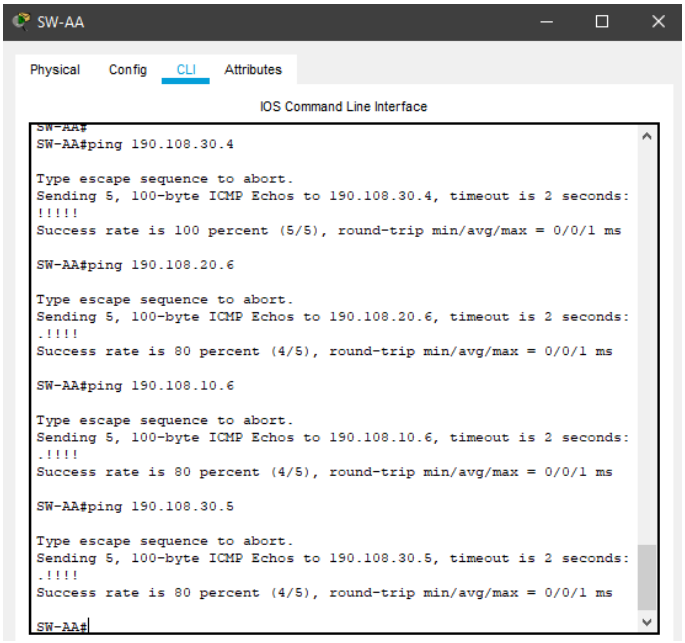

Figura 27. Ping desde SW-AA a distintos PC

Gracias a la configuración de enrutamiento IP en las Vlan creadas es posible realizar estos pings satisfactoriamente, dado el caso que no se configurara el enrutamiento ip en las Vlan al momento de realizar ping entre los PC esta acción no se hubiera logrado realizar ya que es necesario configurar una dirección IP y una máscara de subred en cada una de las interfaces de las Vlan la cual debe pertenecer al mismo segmento de red para que se puedan comunicar.

CONCLUSIONES

Se comprendió y desarrolló de la mejor manera los dos escenarios propuestos en la evaluación prueba de habilidades practicas CCNP, por medio del diseño en herramientas de simulación como Packet Tracer y GNS3.

Se analizó e implementó los conocimientos desarrollados durante el diplomado en cada uno de los escenarios, gracias a esta práctica se puede evidenciar el crecimiento intelectual y lógico para solucionar todo tipo de problemas de diversos aspectos de Networking.

En esta práctica se implementaron diferentes procesos, por ejemplo, en el escenario 1 se implementó el protocolo de enrutamiento interdominio BGP, donde se configuro la relación entre vecinos en cada router y se codifico cada router por medio de un ID.

En el escenario 2 se configuro el VTP de cada Switches para la comunicación y administración de los datos, y se conectaron por medio de enlaces troncales, por último, se crearon unas Vlan donde se configuraron sus puertos, sus modos de acceso y el direccionamiento IP de cada uno de los Switches.

REFERENCIAS BIBLIOGRÁFICAS

ANON., 2013. In: *Cisco.com* [en ligne]. 2013. [Consulté le 15 mai 2020]. Disponible à l'adresse : https://www.cisco.com/c/dam/en_us/training-events/netacad/demos/CCNP1v30/index/glossary/CCNP_v30_glossary.pdf.

Casos Prácticos de BGP. (30 de Octubre de 2008). Obtenido de Cisco: https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocolbgp/26634-bgp-toc.html.

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Fundamentals Review. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de: https://1drv.ms/b/s!AmIJYeiNT1IlnWR0hoMxgBNv1CJ.

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