DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JAISSIR EDUARDO ORTEGA VERGARA

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

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JAISSIR EDUARDO ORTEGA VERGARA

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

BOGOTA D. C., 22 de mayo de 2020

AGRADECIMIENTOS

Quiero agradecer primero a Dios por bendecirnos la vida, por guiarnos a lo largo de nuestra existencia, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad este esfuerzo está dedicado a las personas más especial en mi vida, a mi amada esposa Jessia Sujey Rodríguez, a mi padre Anuar de Jesús Ortega Pérez y mis hermanos y a los demás integrantes de mi familia, por su apoyo incondicional para alcanzar mis metas personales e Institucionales mil Gracias.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

OSPF: Open Shortest Path First (OSPF), Primer Camino Más Corto, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

EIGRP: (Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado en español) es un protocolo de encaminamiento vector distancia avanzado, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancias y del estado de enlace.

BGP: El protocolo de puerta de enlace de frontera (BGP) es un ejemplo de protocolo de puerta de enlace exterior (EGP). BGP intercambia información de encaminamiento entre sistemas autónomos a la vez que garantiza una elección de rutas libres de bucles. Enrutamiento intrautónomo.

VTP: El VLAN Trunk Protocol (VTP) reduce la administración en una red de switch. Al configurar una VLAN nueva en un servidor VTP, se distribuye la VLAN a través de todos los switches del dominio.

DTP: (Dynamic Trunking Protocol) es un protocolo propietario creado por Cisco Systems que opera entre switches Cisco, el cual automatiza la configuración de trunking (etiquetado de tramas de diferentes VLAN's con ISL o 802.1Q) en enlaces Ethernet.

Ancho de Banda - Bandwidth: Cantidad de datos que puede ser enviada o recibida durante un cierto tiempo a través de un determinado circuito de comunicación. Técnicamente, es la diferencia en hertzios (Hz) entre la frecuencia más alta y más baja de un canal de transmisión.

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

RESUMEN

En el siguiente trabajo, se desarrollarán dos escenarios propuesto en diplomado de profundización CISCO CCNP, estos son SWITCH y ROUTE. Tiene como objetivo de evaluar las competencias y habilidades adquiridas durante todo el curso. Comprender el funcionamiento de los dispositivos que conforman las nuevas tecnologías es esencial en el funcionamiento de las REDES de comunicaciones y de NETWORKING, la forma de mejorarlas y hacer que se adapten a cada necesidad en particular. Para constancia del trabajo se evidencias las configuraciones de cada dispositivo en los simuladores GNS3 y Packet Tracer

Palabras Clave: CISCO, CCNP, SWITCH, ROUTE, REDES, NETWORKING, GNS3, Packet Tracer.

ABSTRACT

In the following work, two proposed scenarios will be developed in CISCO CCNP diploma of deepening, these are SWITCH and ROUTE. Its objective is to evaluate the competences and skills acquired during the whole course. Understanding the operation of the devices that make up new technologies is essential in the operation of communications networks and networking, how to improve them and make them adapt to each particular need. For proof of the work, the configurations of each device in the GNS3 and Packet Tracer simulators are shown

Keywords: CISCO, CCNP, SWITCH, ROUTE, NETWORKING, GNS3, Packet Tracer.

INTRODUCCIÓN

Por medio del presente trabajo escrito se pretende dejar evidencia de las actividades requeridas para el trabajo final pruebas de habilidades prácticas CCNP, indicadas en la guía de actividades cuyo objetivo es que apliquemos los conocimientos y destrezas aprendidos durante el desarrollo presente diplomado como son:

En el módulo CCNP ROUTE protocolos de enrutamiento EIGRP, OSPF, BGP, redistribución de rutas, entre otros, así como nuevos e interesantes temas, como Dynamic Multi VPN, VRF Lite y protocolos en IPv6.
En el módulo CCNP SWITCH como operaciones y puertos de swtiches, VLANs y troncales, Spanning Tree, entre otros, así como nuevos e interesantes temas, como manejo de ataques de spoofing y configuración de usuarios.

Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking, como estrategia de aprendizaje que garantizará la asimilación de los conceptos se desarrollaron las siguientes actividades para el logro de los objetivos.

CONTENIDO

Escenario 1

Figura 1. Escenario 1

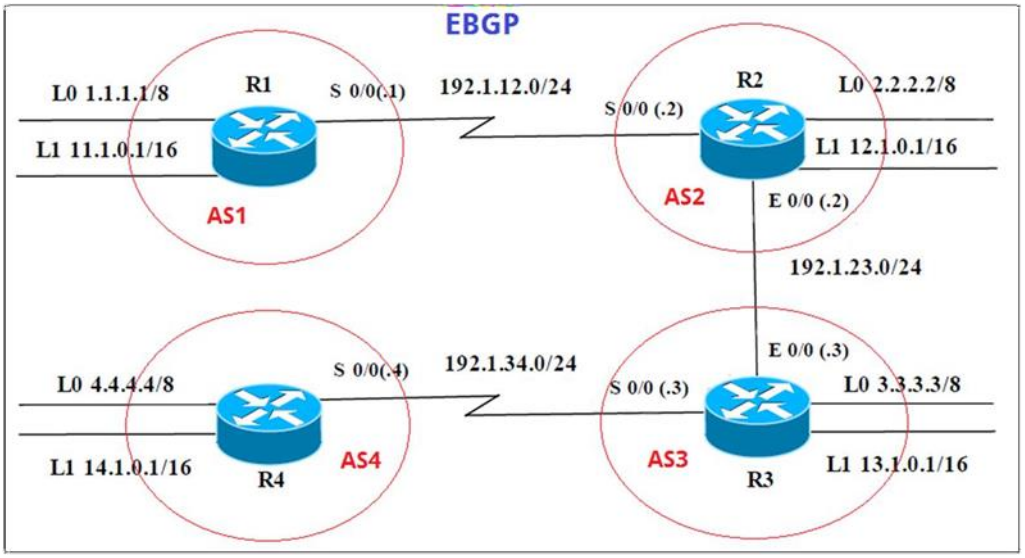


Tabla 1. Información para configuración de los Routers

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

1.

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

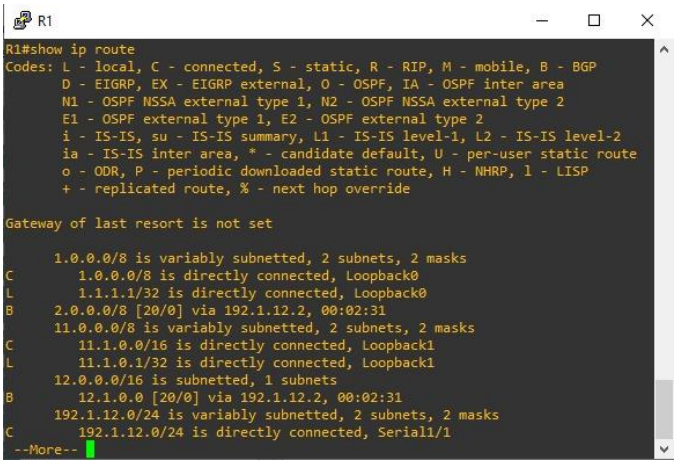
```
Router#configure terminal
R1(config)# interface Loopback 0
R1(config-if)# ip address 1.1.1.1 255.0.0.0
R1(config-if)# exit
R1(config)# interface Loopback 1
R1(config-if) # ip address 11.1.0.1 255.255.0.0
R1(config-if) # exit
R1(config)# interface Serial 1/1
R1(config-if)# description AS1 -> AS2
R1(config-if)# ip address 192.1.12.1 255.255.255.0
R1(config-if) # clock rate 128000
R1(config-if) # no shutdown
R1(config-if) # exit
R1(config)# router bgp 1
R1(config-router) #bgp router-id 22.22.22.22
R1(config-router) # network 1.0.0.0 mask 255.0.0.0
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router) # network 192.1.12.0 mask 255.255.255.0
R1(config-router) # neighbor 192.1.12.2 remote-as 2
```

R2

```
R2#configure terminal
R2(config)# interface Loopback 0
R2(config-if) # ip address 2.2.2.2 255.0.0.0
R2(config-if) # exit
R2(config)# interface Loopback 1
R2(config-if) # ip address 12.1.0.1 255.255.0.0
R2(config-if) # exit
R2(config)# interface Serial 1/1
R2(config-if)# description AS2 -> AS1
R2(config-if) # ip address 192.1.12.2 255.255.255.0
R2(config-if) # clock rate 128000
R2(config-if) # no shutdown
R2(config-if) # exit
R2(config)# interface fastethernet 0/0
R2(config-if)# description AS2 -> AS3
R2(config-if) # ip address 192.1.23.2 255.255.255.0
R2(config-if) # no 10hutdown
R2(config-if) # exit
R2(config)# router bgp 2
R2(config-router)#bgp router-id 33.33.33.33
```

R2(config-router) # network 2.0.0.0 mask 255.0.0.0
R2(config-router) # network 12.1.0.0 mask 255.255.0.0
R2(config-router) # network 192.1.12.0 mask 255.255.255.0
R2(config-router) # neighbor 192.1.12.1 remote-as 1

Figura 2. Resultado aplicar comando show ip route 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.***

R2

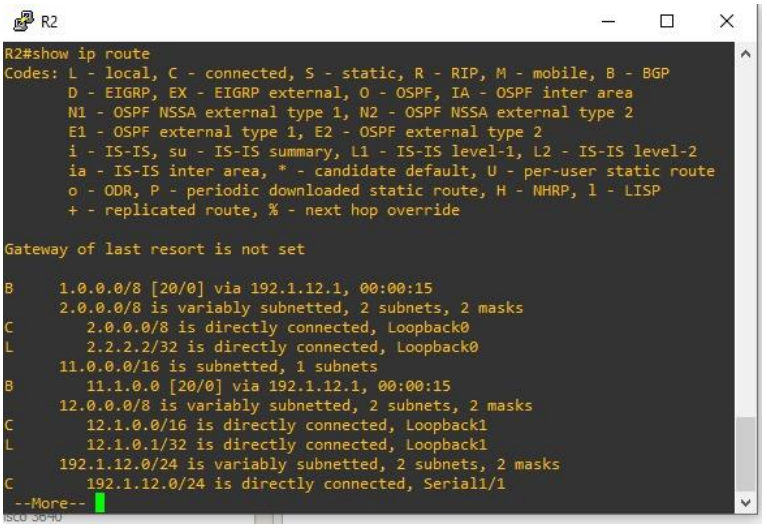
R2# configure terminal
R2(config)# router bgp 2
R2(config-router)# network 192.1.23.0 mask 255.255.255.0
R2(config-router)# neighbor 192.1.23.3 remote-as 3
R2(config-router)#exit
R2(config)#exit

R3

R3# configure terminal
R3(config)# interface Loopback 0
R3(config-if) # ip address 3.3.3.3 255.0.0.0
R3(config-if) # exit
R3(config)# interface Loopback 1
R3(config-if) # ip address 13.1.0.1 255.255.0.0
R3(config-if) # exit
R3(config)# interface fastethernet 0/0
R3(config-if)# description AS3 -> AS2
R3(config-if) # ip address 192.1.23.3 255.255.255.0

R3(config-if) # no shutdown
R3(config-if) # exit
R3(config)# interface Serial 1/1
R3(config-if)# description AS3 -> AS4
R3(config-if) # ip address 192.1.34.3 255.255.255.0
R3(config-if) # no shutdown
R3(config-if) # exit
R3(config)# router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router) # network 3.0.0.0 mask 255.0.0.0
R3(config-router) # network 13.1.0.0 mask 255.255.0.0
R3(config-router) # network 192.1.23.0 mask 255.255.255.0
R3(config-router) # neighbor 192.1.23.2 remote-as 2

Figura 3. Resultado aplicar comando show ip route R2



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

R3(config)#exit

R4

R4#configure terminal
R4(config)# interface Loopback 0
R4(config-if) # ip address 4.4.4.4 255.0.0.0
R4(config-if) # exit
R4(config)# interface Loopback 1
R4(config-if) # ip address 14.1.0.1 255.255.0.0
R4(config-if) # exit
R4(config)# interface Serial 1/1
R4(config-if)# description AS4 -> AS3
R4(config-if) # ip address 192.1.34.4 255.255.255.0
R4(config-if) # no shutdown
R4(config-if) # exit
R4(config)# router bgp 4
R4(config-router)#bgp router-id 66.66.66.66
R4(config-router) # network 4.0.0.0 mask 255.0.0.0
R4(config-router) # network 14.1.0.0 mask 255.255.0.0
R4(config-router) # network 192.1.34.0 mask 255.255.255.0
R4(config-router) # neighbor 192.1.34.3 remote-as 3
R4(config-router) #exit
R4(config)#exit
R3
R3#configure terminal
R3(config)# ip route 4.0.0.0 255.0.0.0 192.1.34.4
R3(config)#router bgp 3
R3(config-router) # no neighbor 192.1.34.4
R3(config-router) # no network 3.0.0.0 mask 255.0.0.0
R3(config-router) # neighbor 4.4.4.4 remote-as 4
R3(config-router) # neighbor 4.4.4.4 update-source Loopback 0
R3(config-router) # neighbor 4.4.4.4 ebgp-multihop
R3(config-router) #exit
R3(config)#exit

R4

R4#configure terminal
R4(config)# ip route 3.0.0.0 255.0.0.0 192.1.34.3
R4(config)#router bgp 4
R4(config-router) # no neighbor 192.1.34.3
R4(config-router) # neighbor 3.3.3.3 remote-as 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

R4(config)#exit

Figura 4. Resultado aplicar comando show ip route router R3

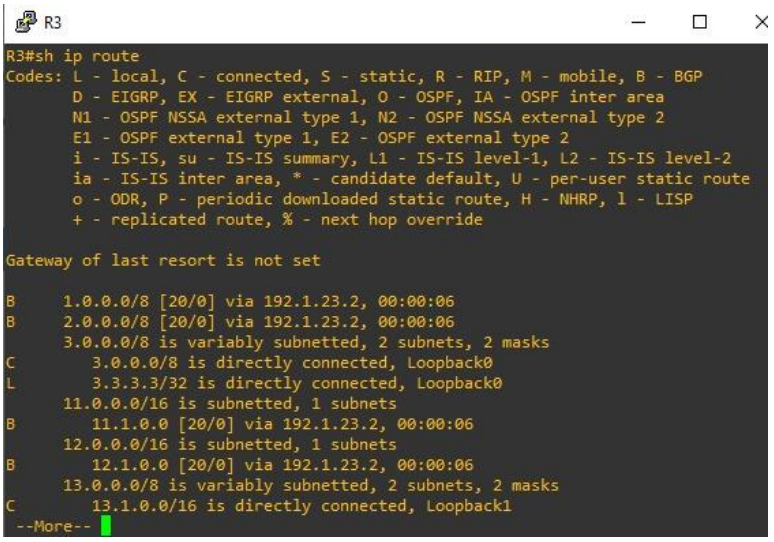
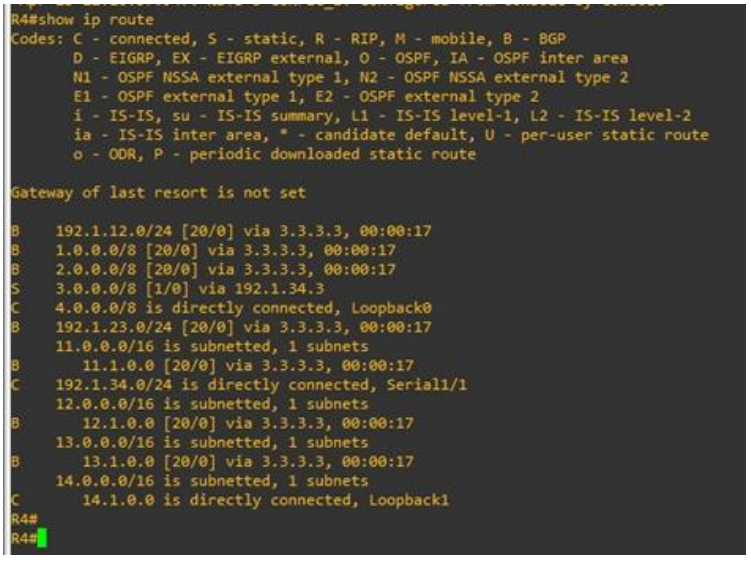
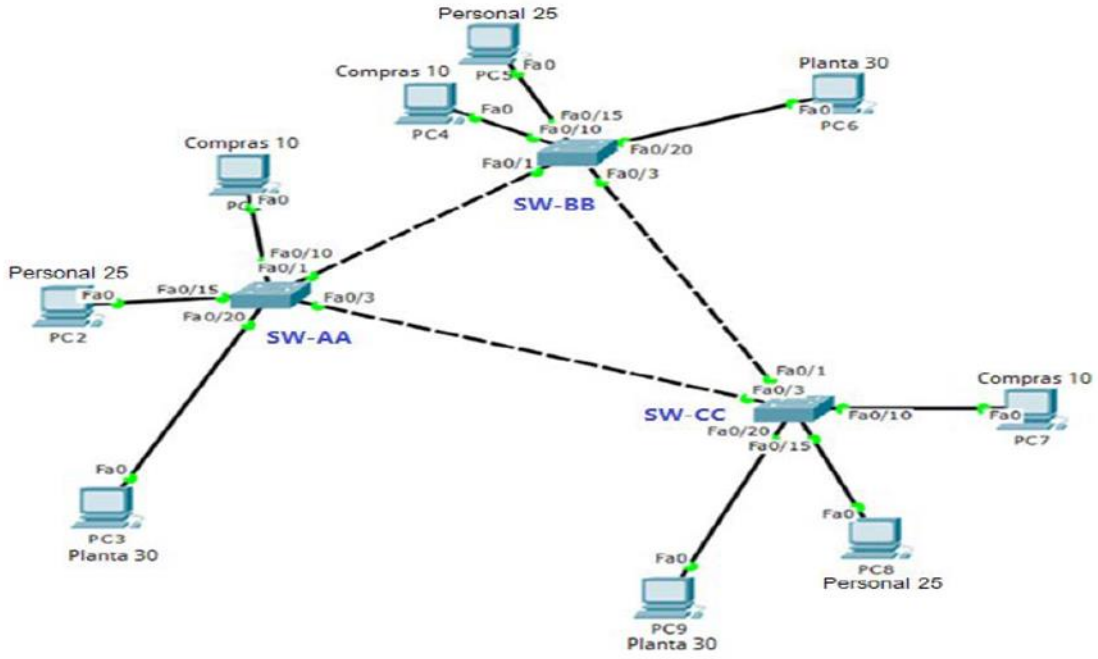


Figura 5. Resultado aplicar comando show ip route router R4



Escenario 2

Figura 6. Escenario 2



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> Enable
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

SW-BB> Enable
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

SW-CC> Enable
SW-CC#configure terminal
SW-CC(config)# vtp mode client
Setting device to VTP CLIENT mode.
SW-CC(config)# vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-CC(config)# vtp Password cisco
Setting device VLAN database password to cisco

2. Verificar las configuraciones mediante el comando ***Show vtp status***

Figura 7. Show vpt status switch SW-AA

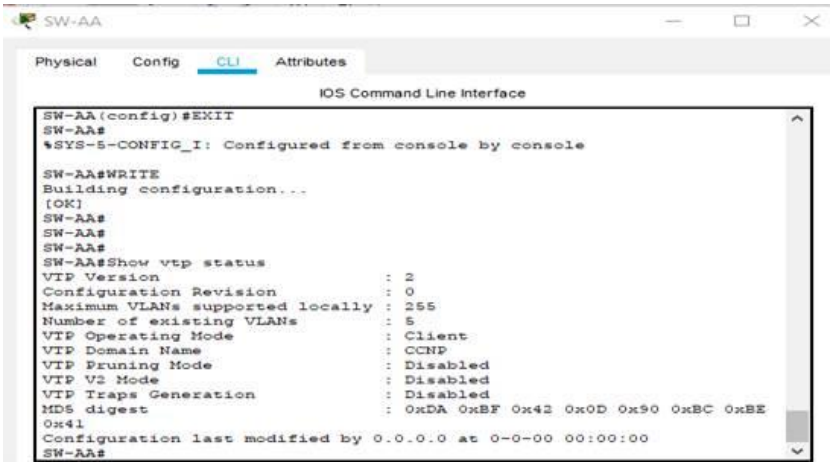


Figura 8. Show vpt status switch SW-BB

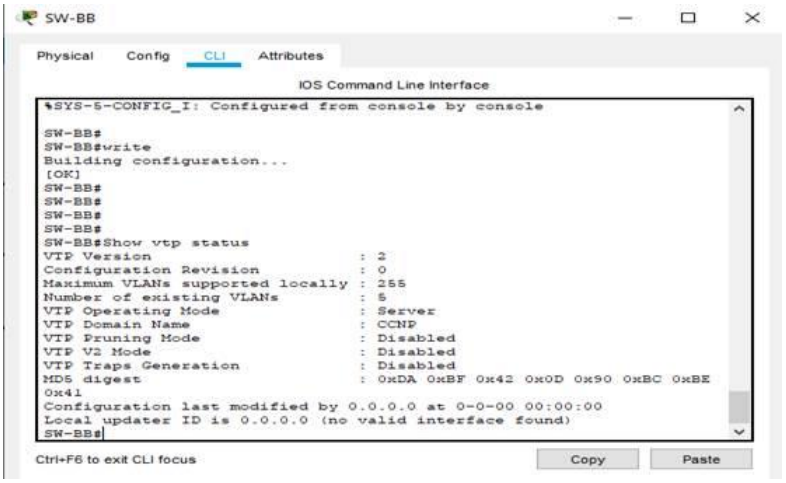


Figura 9. Show vpt status switch SW-CC

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

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

Figura 10. show interface trunk F0/1 SW-AA

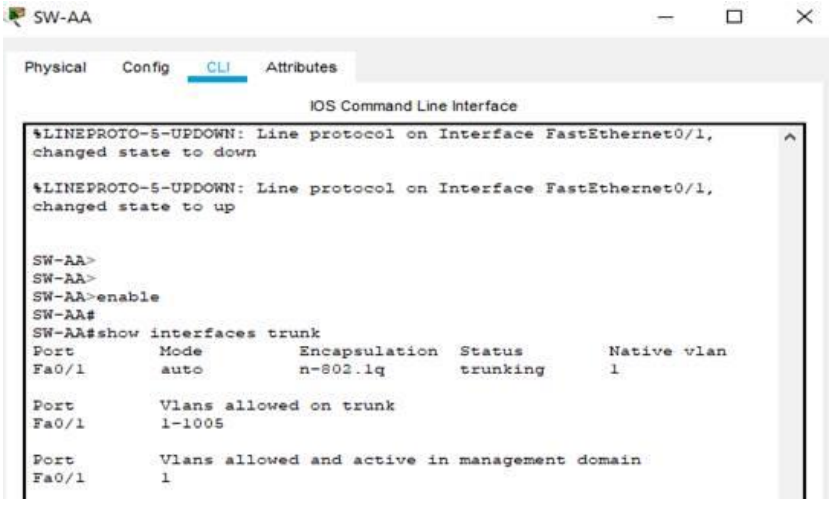
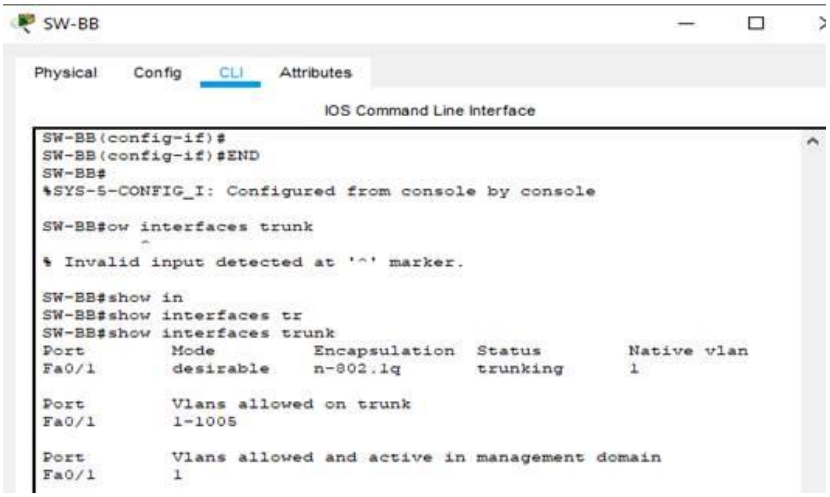


Figura 11. show interface trunk F 0/1 SW-BB

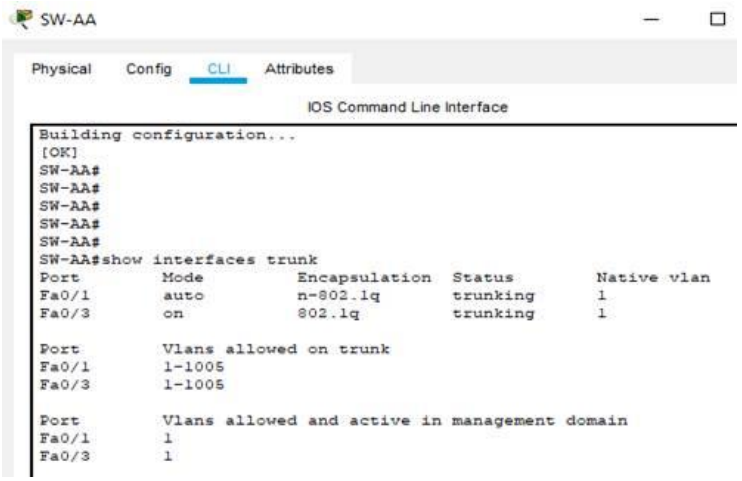


6. Entre **SW-AA** y **SW-CC** configure un enlace "trunk" estático utilizando el comando switchport **mode trunk** en la interfaz F0/3 de **SW-AA**.

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

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

Figura 12. show interface trunk F 0/3 SW-AA



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

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

Validación enlace “trunk” entre **SW-BB** y **SW-CC**

Figura 13. Validación modo trunk SW-BB

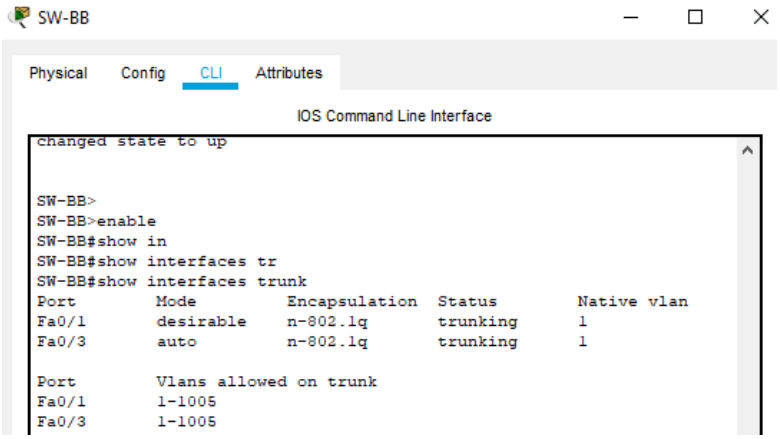
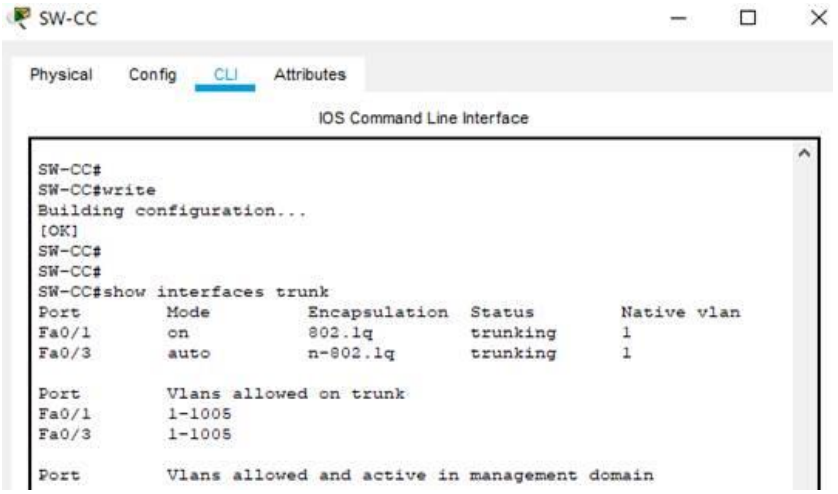


Figura 13:

Figura 14. Validación modo trunk SW-CC



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

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

10. Verifique que las VLANs han sido agregadas correctamente.

Figura 15. Validación Creación de Vlans en SW-BB

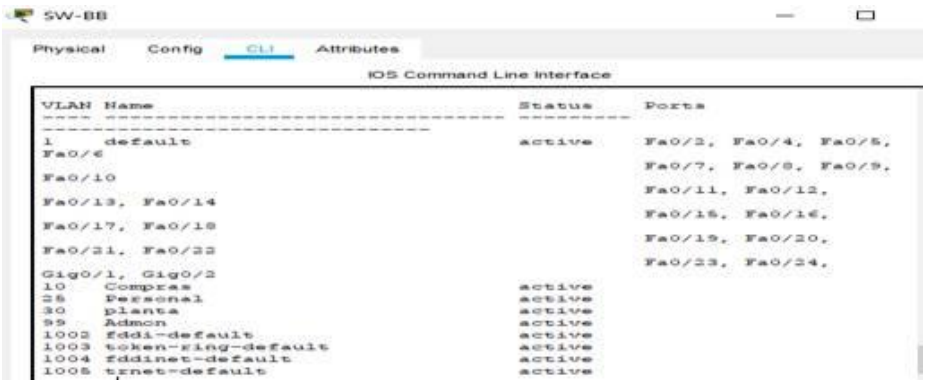
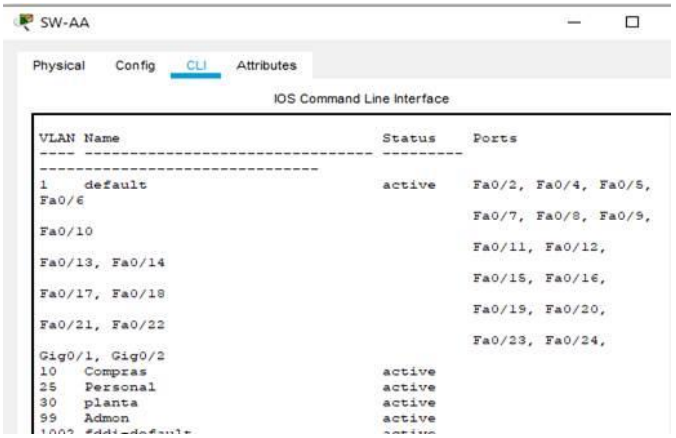


Figura 16. Validación Creación de Vlans en SW-AA



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

Tabla 2. Escenario 2

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

X = número de cada PC particular

Tabla 5 enrutamiento PC

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

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

SW-AA# configure terminal
SW-AA(config)#interface fastEthernet 0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10 / Compras
SW-AA(config-if)#exit
SW-AA(config)# interface fastEthernet 0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25 / Personal

```
SW-AA(config-if)#exit
SW-AA(config)# interface fastEthernet 0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30 / Planta
SW-AA(config)#end


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 / Compras
SW-BB(config-if)#exit
SW-BB(config)# interface fastEthernet 0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25 / Personal
SW-BB(config-if)#exit
SW-BB(config)# interface fastEthernet 0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30 / Planta
SW-BB(config)#end

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 / Compras
SW-CC(config-if)#exit
SW-CC(config)# interface fastEthernet 0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25 / Personal
SW-CC(config-if)#exit
SW-CC(config)# interface fastEthernet 0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30 / Planta
SW-CC(config)#end
```

Tabla 3. Escenario 2

Interfaz	VLAN	N pc	Direcciones IP de los PCs
F0/10	VLAN 10	3	190.108.10.1 / 24
		4	190.108.10.2 / 24
		7	190.108.10.3 / 24
F0/15	VLAN 25	2	190.108.20.1 /24
		5	190.108.20.2 /24
		8	190.108.20.3 /24
F0/20	VLAN 30	1	190.108.30.1 /24
		6	190.108.30.2 /24
		9	190.108.30.3 /24

Tabla 6 enrutamiento PC según Vlan

Figura 17. Validación direccionamiento PC1

Figura 18. Validación direccionamiento PC2

Figura 19. Validación direccionamiento PC3

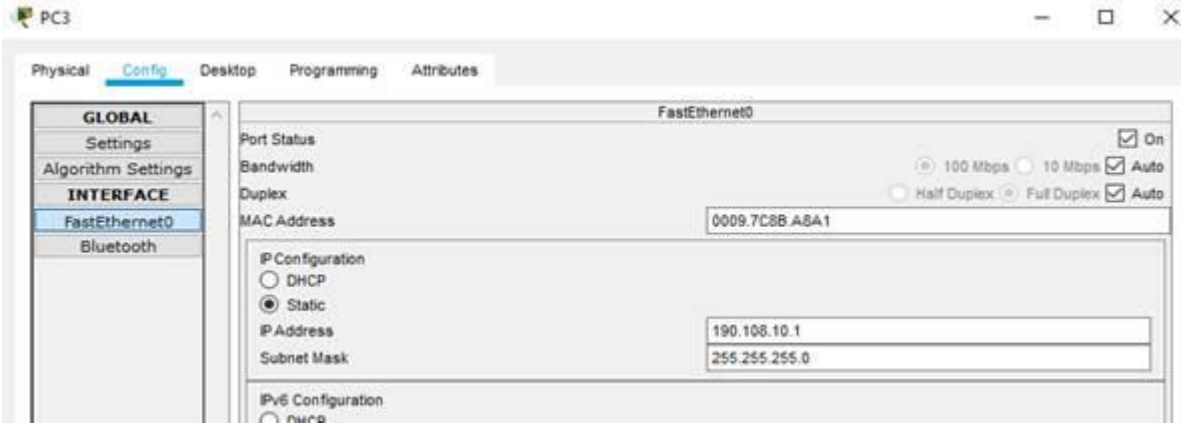


Figura 20. Validación direccionamiento PC4

Figura 21. Validación direccionamiento PC5

Figura 22. Validación direccionamiento PC6

Figura 23. Validación direccionamiento PC7

Figura 24:

Figura 24. Validación direccionamiento PC8

Figura 25. Validación direccionamiento PC

C. Configurar las direcciones ip en los switches.

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

Tabla 4. Enrutamiento Switches

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

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

SW-BB>
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-BB(config-if)# exit

SW-CC>
SW-CC# configure terminal
SWT3(config)# interface vlan 99
SW-CC(config-if)# ip address 190.108.99.3 255.255.255.0
```

SW-CC(config-if)# exit.

D. Verificación de conectividad Extremo a Extremo

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

El ping entre cada una de las PC es éxitos, siempre y cuando estén dentro de la misma vlan. En caso de tratar de hacer ping entre una vlan 10 con otra, el resultado es no exitoso.

Figura 26. Validación ping PC1 a Pc 6

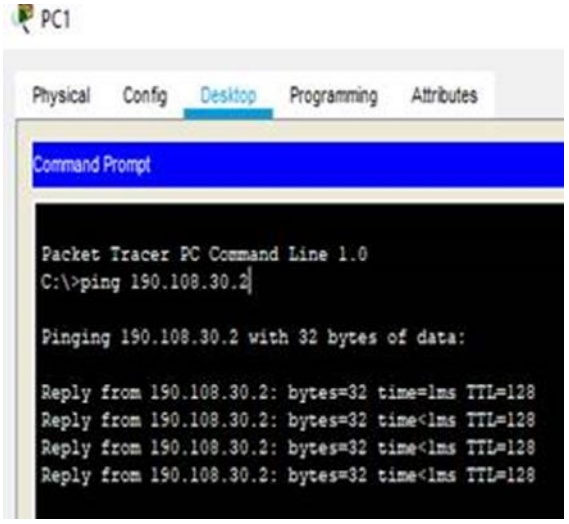


Figura 27. Validación ping Pc2 a Pc5

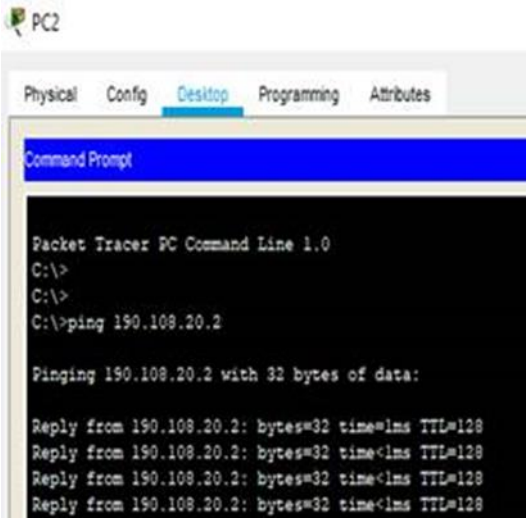


Figura 28. Validación ping Pc3 a Pc4

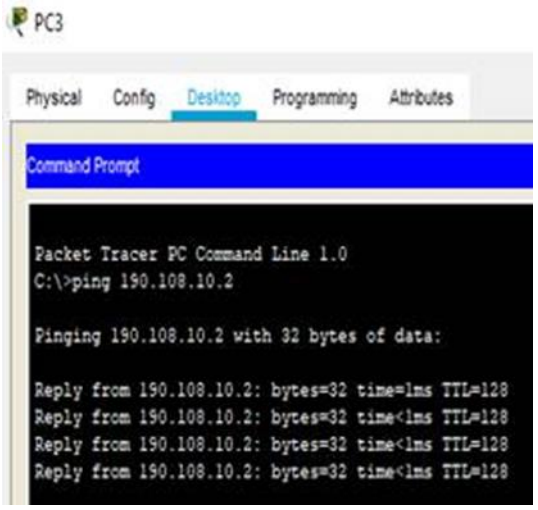


Figura 29. Validación ping Pc4 a Pc7

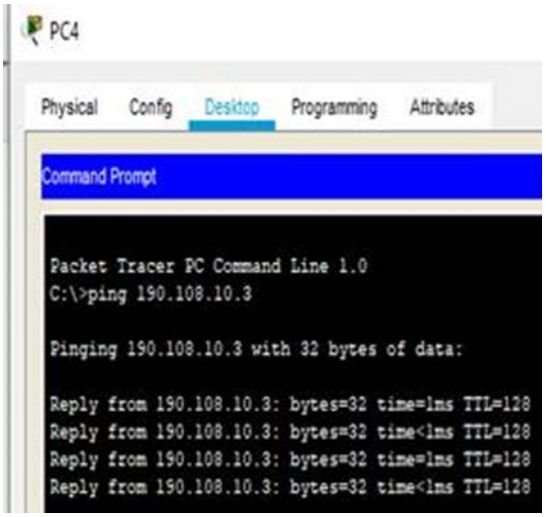


Figura 30. Validación ping Pc8 a Pc2

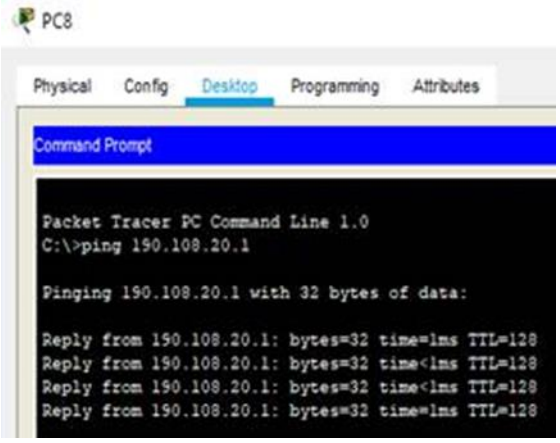


Figura 31. Validación ping Pc9 a Pc1

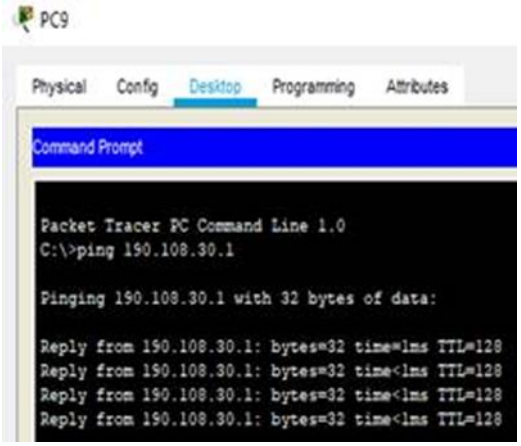


Figura 32. Validación ping Pc1 a Pc8

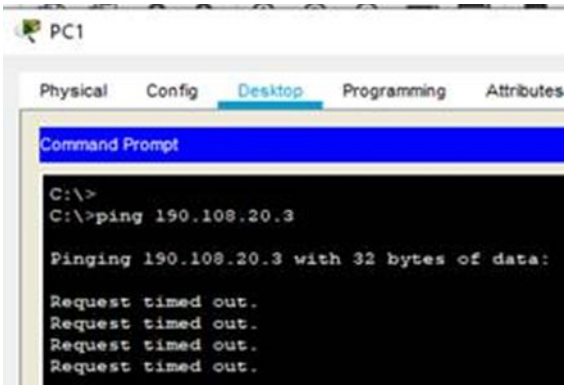
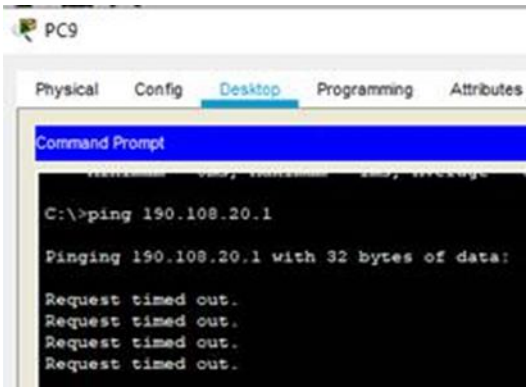


Figura 33. Validación ping Pc9 a Pc2



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

Cuando se envía el ping entre los Switches es exitoso, los Switches están configuradas en modo troncal, estas comparten el mismo tipo de encapsulamiento donde se validó con el comando ***show interfaces trunk*** y estas se encuentran en modo compatible.

Figura 34. Validación ping SW-AA a SW-BB y SW-CC

Figura 35:

Figura 35. Validación ping SW-BB a SW-AA y SW-CC

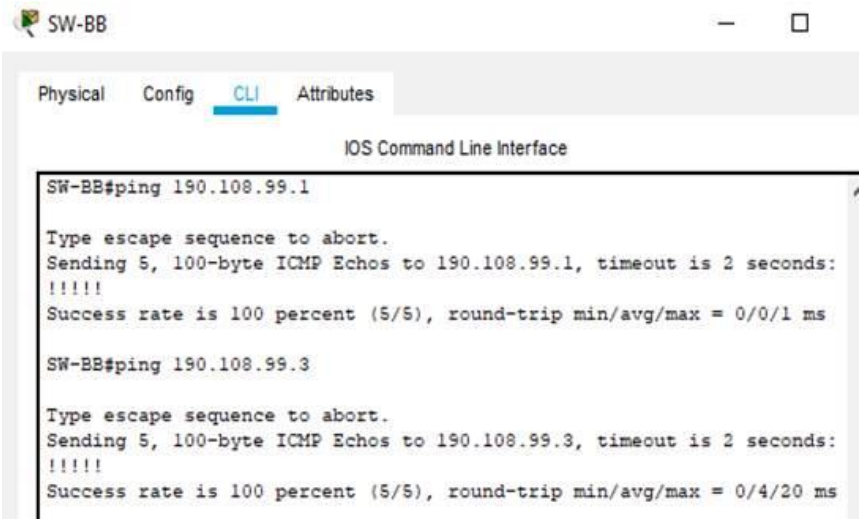
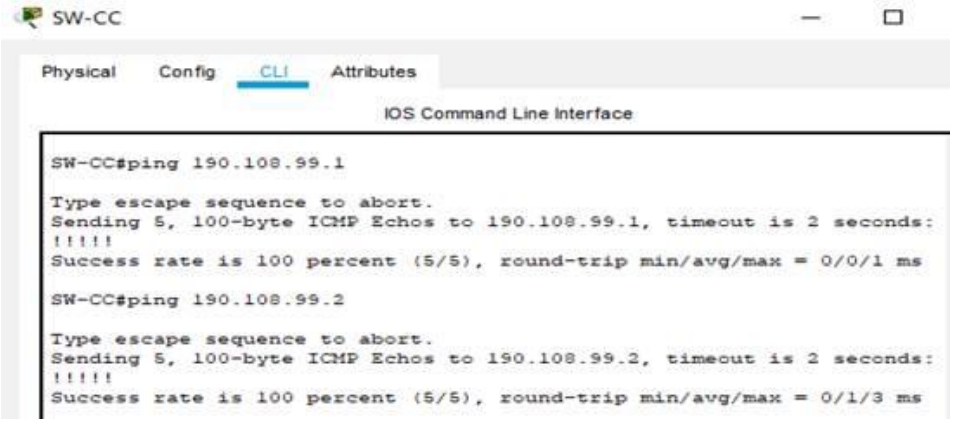


Figura 36:

Figura 36. Validación ping SW-CC a SW-AA y SW-BB



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

Al realizar ping desde los switches a los PC este no es exitoso, debido a que no se tiene configurada una dirección ip y una máscara de sured en cada una de las interfaces Vlan de los switches, para que el ping tenga éxito se debe realizar esta asignación a cada una de las Vlans con una dirección ip del mismo.

Figura 37. Validación ping SW-AA a Pc 1-Pc2 y Pc3

Figura 38. Validación ping SW-BB a Pc 1-Pc2 y Pc3

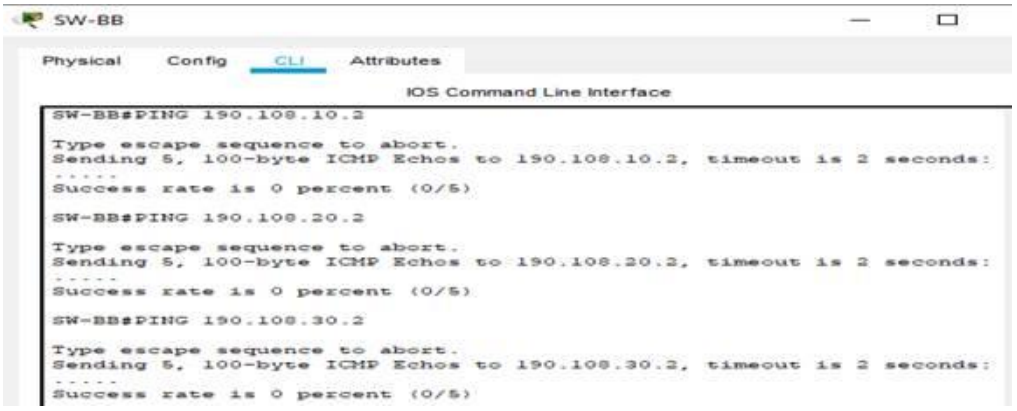


Figura 39. Validación ping SW-CC a Pc7-Pc8 y Pc9

CONCLUSIONES

Con el desarrollo del presente trabajo colaborativo se repasaron muchos comandos de configuración de switches y routers vistos anteriormente y fue necesario aprender muchos más. Fue necesario estudiar gran parte de la temática vista durante el curso.

La temática del presente curso es muy amplia y difícil de sintetizar.

Los routers y switches CISCO tienen una gran variedad de opciones de configuración dependiendo de la topología de la red y requerimiento del usuario, son muy versátiles.

Con el presente trabajo se aprendieron muchos temas súper importantes para aplicar en nuestra labor como futuros administradores de red y configuradores de equipos de comunicación.

Por medio de este trabajo se permite comprender como se puede implementar y configurar una red que este soportada por VLANs con el uso de los protocolos VTP y STP, donde se pueda diseñar las plantillas de configuración para su uso en múltiples dispositivos, configurar troncales y vlan usando el protocolo VTP, los EtherChannel Link en red de switch’s interconectados, entro otros usos.

Con el desarrollo del trabajo de habilidades prácticas se pudo poner a prueba la capacidad de diseñar y configurar una red en los escenarios propuestos, en tal sentido se establecieron los direccionamientos IP, protocolos de enrutamiento y seguridad.

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.

BIBLIOGRAFIAS

Amberg, E. (2014). CCNA 1 Powertraining : ICND1/CCENT (100-101). Heidleberg: MITP. Recuperado de http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=979032&lang=es&site=ehost-live

Lucas, M. (2009). Cisco Routers for the Desperate: Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=440032&lang=es&site=ehost-live•Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYeiNT1IlnMfy2rhPZHwEoWx

UNAD (2015). Introducción a la configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYeiNT1IhgL9QChD1m9EuGqC