DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CARLOS CLIVE ANCHANTE GIRALDO

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

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CARLOS CLIVE ANCHANTE GIRALDO

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, 22 de mayo de 2020

AGRADECIMIENTOS

Agradezco primero que todo a Dios Todopoderoso por haberme permitido llegar a hacer este diplomado para poder concluir mi carrera de Ingeniería de Telecomunicaciones, en segundo lugar, agradezco a mi esposa Luz Elena Jiménez quien ha estado a mi lado en todos estos años de estudio animándome en los momentos difíciles, a mi madre Consuelo Giraldo Coral y a mi familia quien a pesar de no estar a mi lado físicamente ha sido un gran apoyo moral desde mi país de origen Perú.

También agradezco a la UNAD como institución y a todos sus directivos por haberme ayudado con el programa de educación a distancia, el cual abrió el camino para poder comenzar y llegar hasta este punto en el cual se me abren las puertas para mejorar mi situación de vida y lograr seguir realizando mis sueños y metas, a todos y cada uno de los profesores y tutores quienes fueron el mejor soporte durante todo este proceso.

Igualmente debo agradecer al grupo de E-monitores por brindarme su apoyo y amistad permitiendo que me pudiera sentir integrado como en una gran familia.

Extiendo este agradecimiento a todos mis compañeros de carrera por su ayuda incondicional y su esfuerzo en el cumplimiento de los trabajos colaborativos para lograr llegar a la meta y culminar con éxito la carrera universitaria.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

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.

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.

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.

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.

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.

RESUMEN

Este trabajo tiene como objetivo evaluar las competencias y habilidades adquiridas durante todo el curso, desarrollar la prueba de habilidades prácticas que es una herramienta de evaluación del Diplomado de profundización de **CISCO**, **CCNP**, con la cual se busca medir las habilidades y competencias que el estudiante logró alcanzar mediante el desarrollo del periodo académico y cada una de sus actividades.
Esta actividad final contara con dos escenarios, el primero donde se configuran 4 routers y el segundo 3 switches, el estudiante realizará cada una de las configuraciones necesarias, apoyándose en los conocimientos adquiridos en **conmutación**, **enrutamiento, redes** y **electrónica** para dar solución a los dos problemas planteados, también contara durante todo este proceso con el apoyo del software especializado y pondrá en ejecución lo aprendido en el transcurso del curso, para constancia del trabajo se evidencian las configuraciones de cada dispositivo en los simuladores GNS3 y rastreador de paquetes

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

ABSTRACT

This work has the objective of evaluating the competences and skills acquired throughout the course, developing the practical skills test which is an evaluation tool of the **CISCO** in-depth Diploma, **CCNP,** which seeks to measure the skills and competences that the student managed to achieve through the development of the academic period and each of its activities.
This final activity will have two scenarios, the first where 4 routers are configured and the second 3 switches, the student will carry out each of the necessary configurations, relying on the knowledge acquired in **switching**, **routing**, **networks** and **electronics** to provide solutions to both. Problems posed, will also count throughout this process with the support of specialized software and will implement what has been learned during the course, for the record of the work the configurations of each device are evident in the GNS3 simulators and packet tracker

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

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 del presente diplomado.

El primer escenario abarca lo estudiado y aprendido en el módulo CCNP, acerca de los ROUTERS, que consiste en la aplicación del protocolo de puerta de enlace externo (EBGP), a la red conformada por cuatro routers, teniendo como objetivo el intercambio de información de encaminamiento entre sistemas autónomos.

El segundo escenario abarca lo estudiado y aprendido en el módulo CCNP correspondiente a los SWITCHES, teniendo como objetivo la aplicación del protocolo de enlace VLAN en un servidor (VTP) a una red de 3 switches, cada switch se identifica por un nombre y una función diferente, en este caso el switch SW-BB se configura como servidor y los switches SW-AA y SW- CC se configuran como clientes, cada switch se conectara con 3 terminales por medio de la creación de VLAN e interfaces utilizadas, teniendo en cuenta las direcciones IP asignadas.

DESARROLLO

1. ESCENARIO 1

Figura 1. Escenario 1

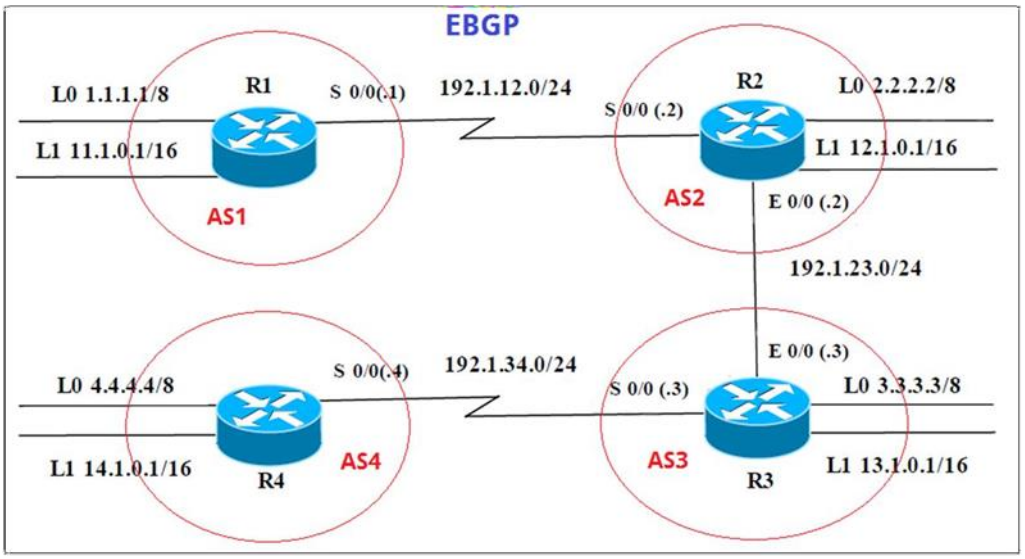


Tabla 1. Información para configuración de los Routers

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

Interfaz	Dirección IP	Máscara

R4	**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.Configure una relación de vecino BGP entre R1 y R2. R1 debe estar en AS1 y R2 debe estar en AS2. Anuncie las direcciones de Loopback en BGP. Codifique los ID para los routers BGP como 22.22.22.22 para R1 y como 33.33.33.33 para R2. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

R1

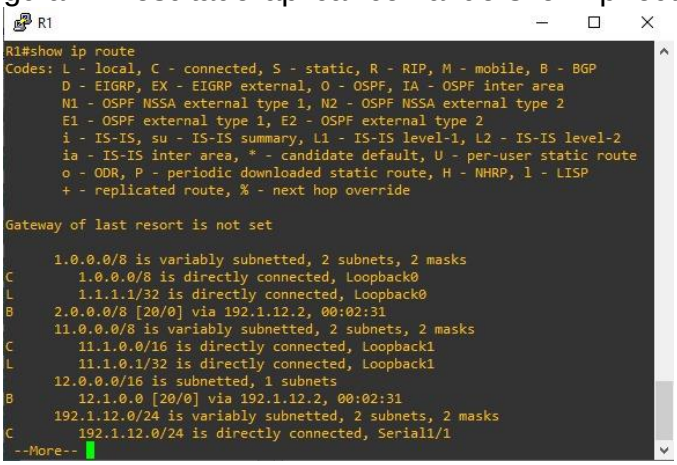
```
Router#configure terminal
R1(config)# interface Loopback 0
R1(config-if)# ip address 1.1.1.1 255.0.0.0
R1(config-if)# exit
R1(config)# interface Loopback 1
R1(config-if) # ip address 11.1.0.1 255.255.0.0
R1(config-if) # exit
R1(config)# interface Serial 1/1
R1(config-if)# description AS1 -> AS2
R1(config-if)# 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 13hutdown
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 router 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.***

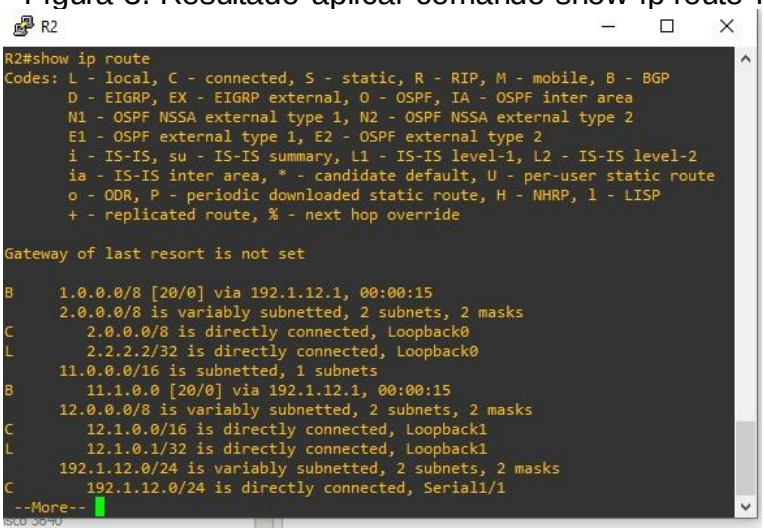
R2

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 route R3

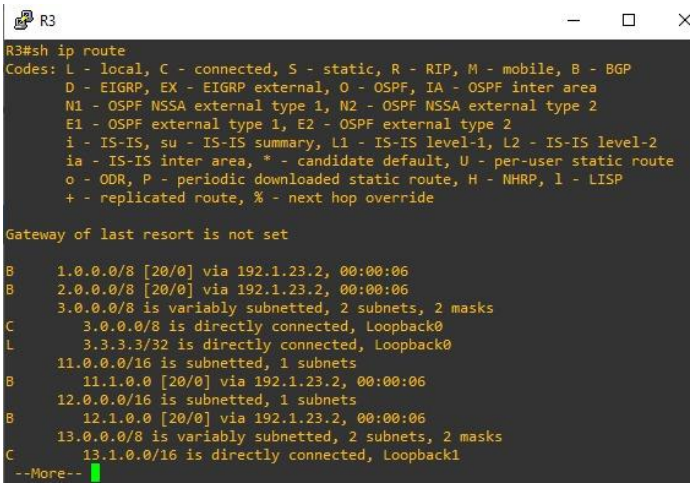
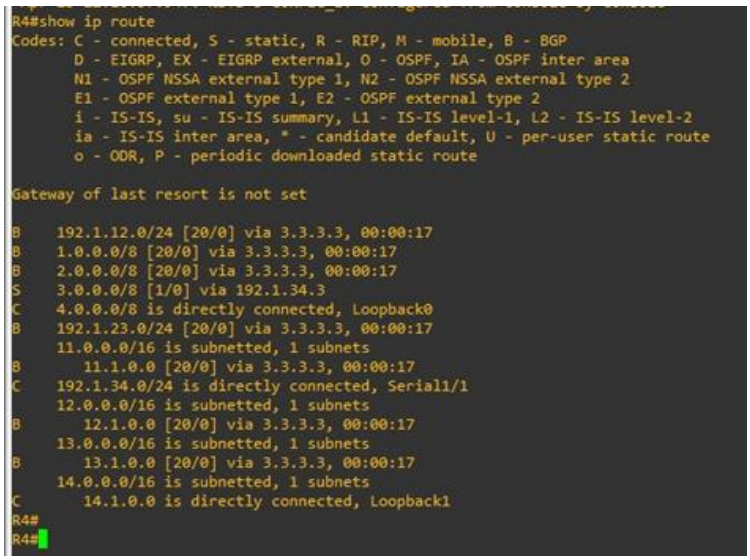
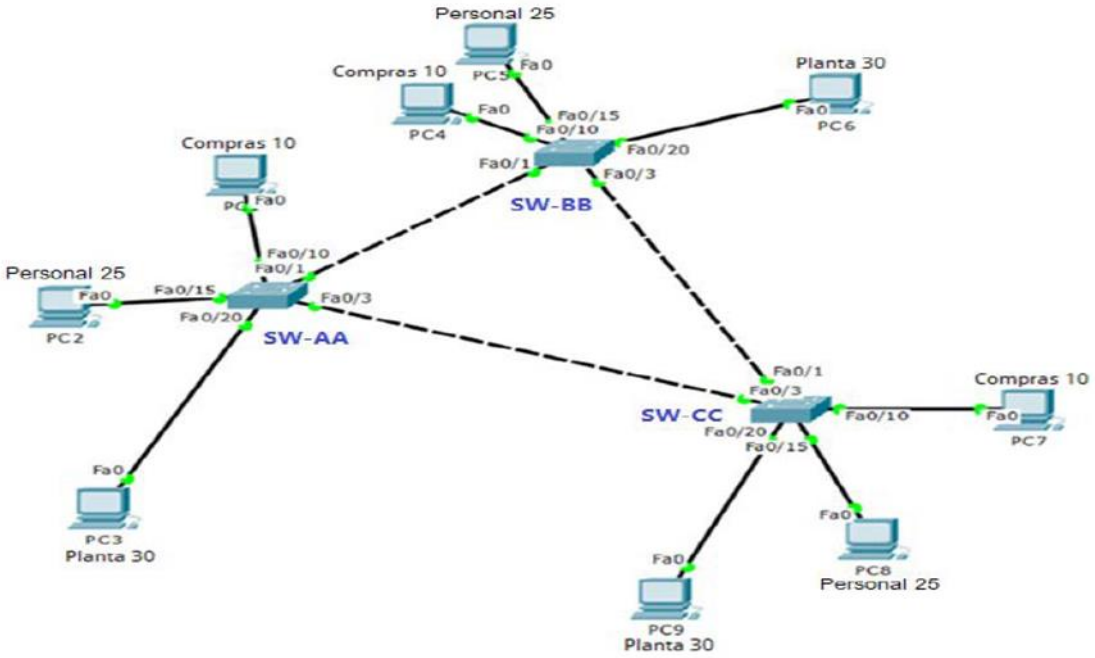


Figura 5. Resultado aplicar comando show ip route route R4



2. 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

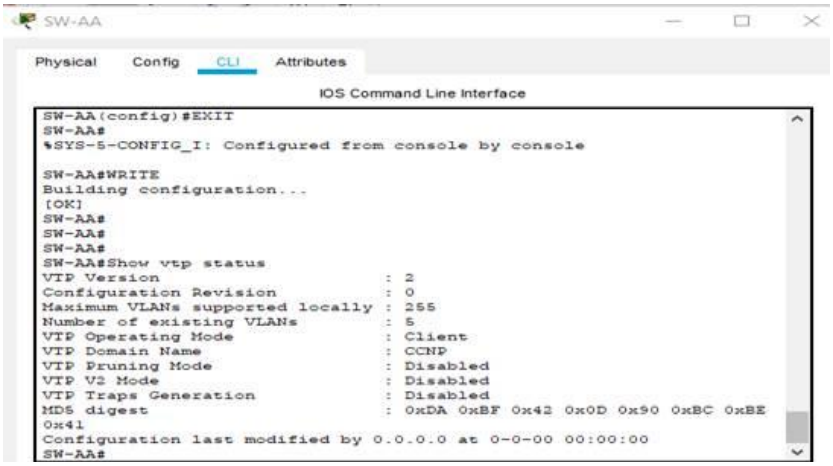


Figura 8. Show vpt status switch SW-BB

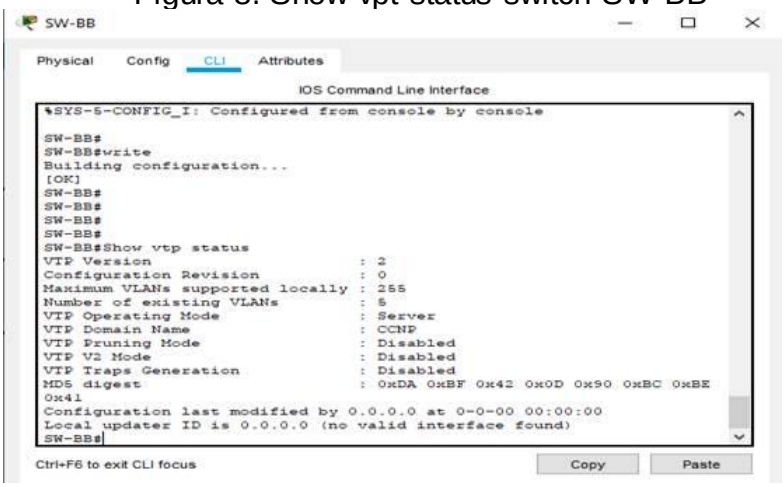
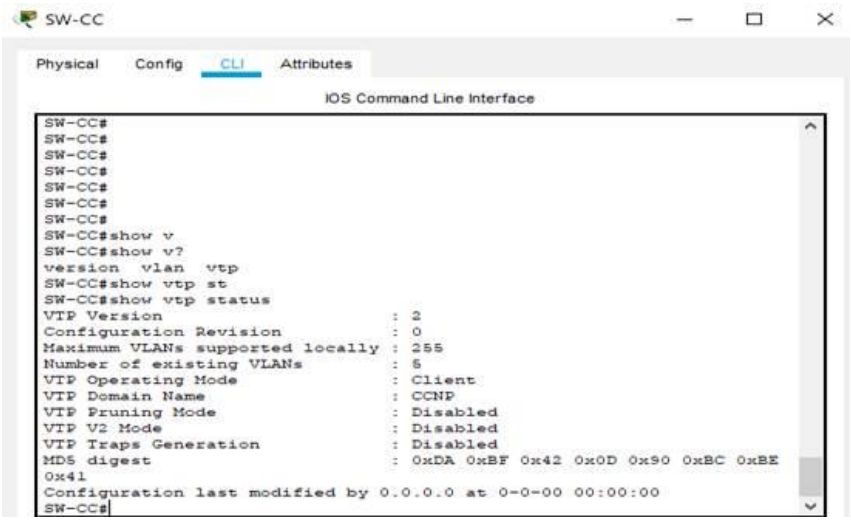


Figura 9. Show vpt status switch SW-CC



A. Configurar DTP (dynamic Trunking protocol)

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

2. 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

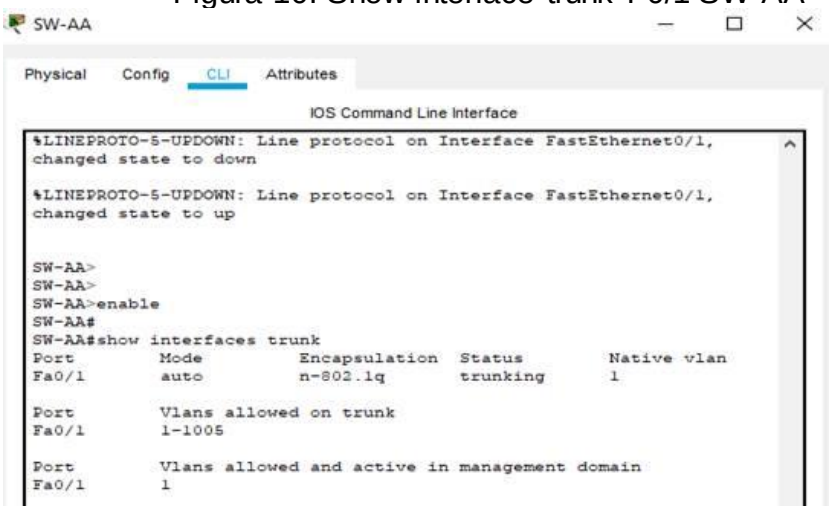
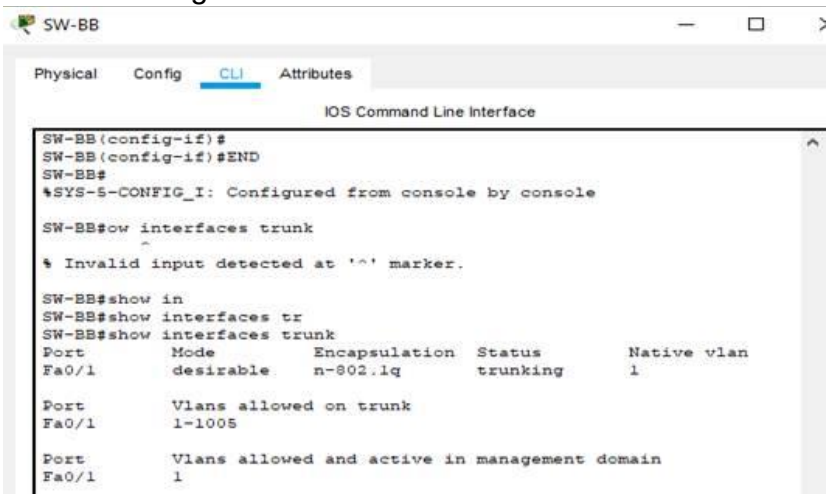


Figura 11. Show interface trunk F 0/1 SW-BB

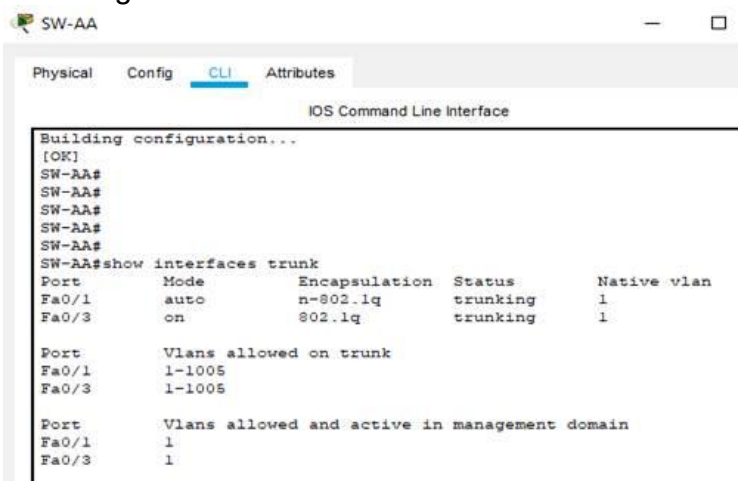


3. Entre **SW-AA** y **SW-CC** configure un enlace "trunk" estático utilizando el comando switchport **mode trunk** en la interfaz F0/3 de **SW-AA**.

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

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

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



5. 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

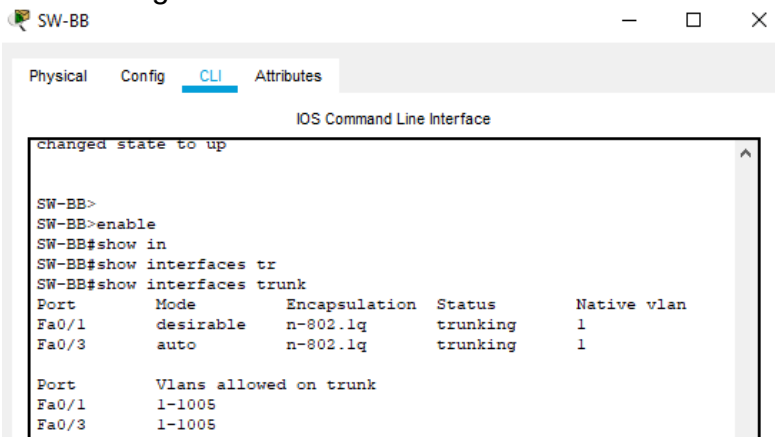
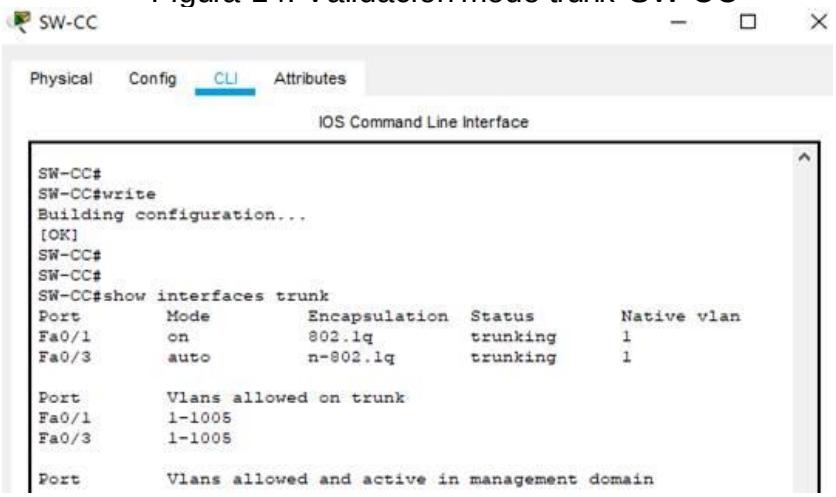


Figura 14. Validación modo trunk SW-CC



B. Agregar VLANs y asignar puertos

6. 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
```

7. Verifique que las VLANs han sido agregadas correctamente.

Figura 15. Validación Creación de VLANs en SW-BB

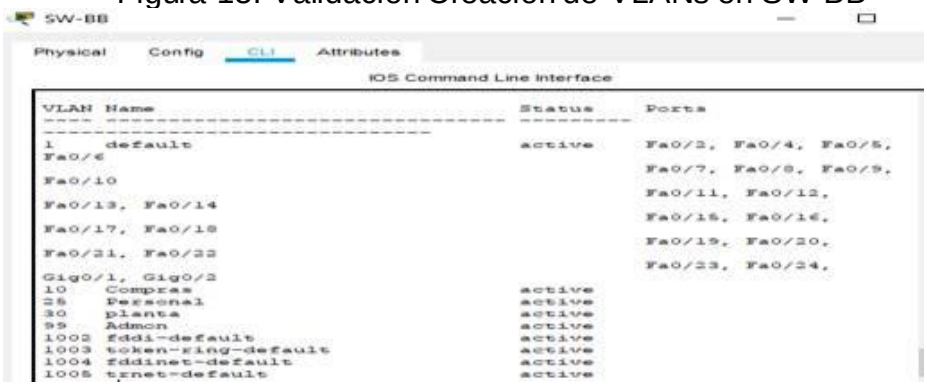
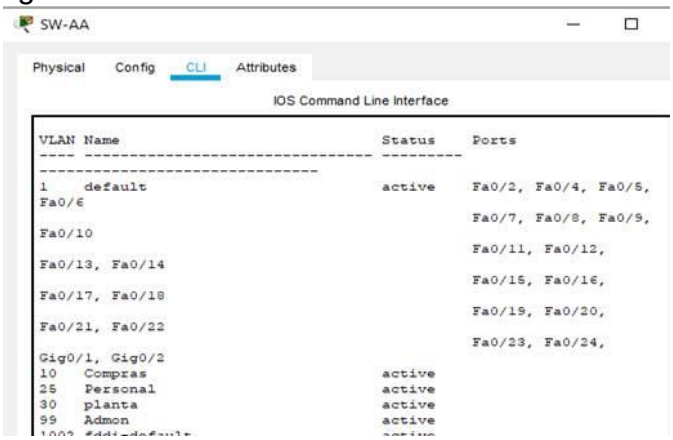


Figura 16. Validación Creación de VLANs en SW-AA



8. 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

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 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

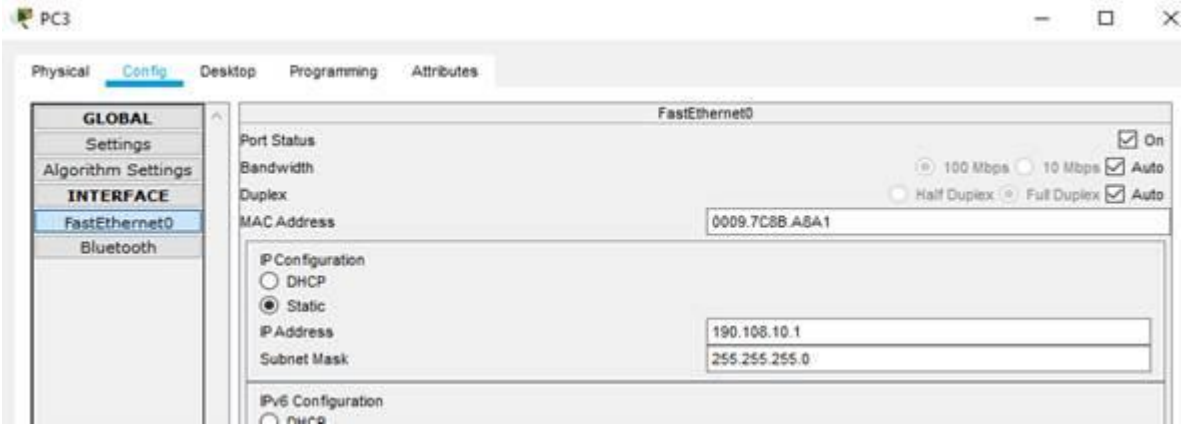


Figura 20. Validación direccionamiento PC4

Figura 21. Validación direccionamiento PC5

Figura 22. Validación direccionamiento PC6

Figura 23. Validación direccionamiento PC7

Figura 24. Validación direccionamiento PC8

Figura 25. Validación direccionamiento PC

C. Configurar las direcciones IP en los switches.

11. 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

12. 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

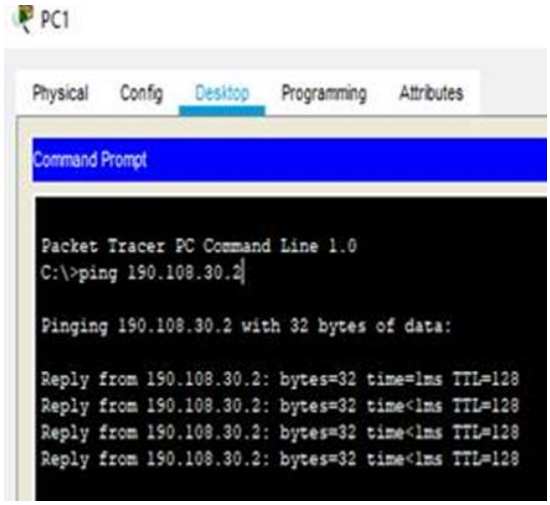


Figura 27. Validación ping Pc2 a Pc5

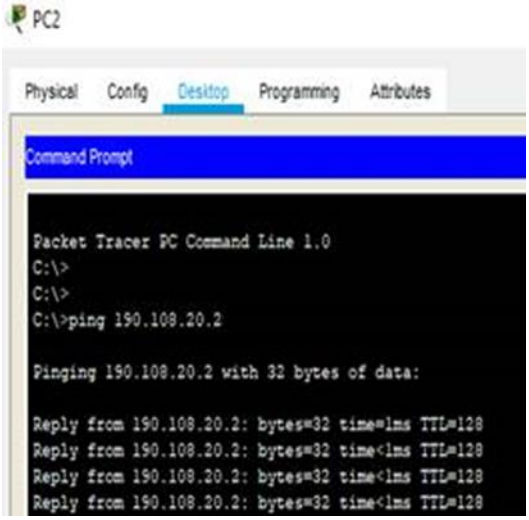


Figura 28. Validación ping Pc3 a Pc4

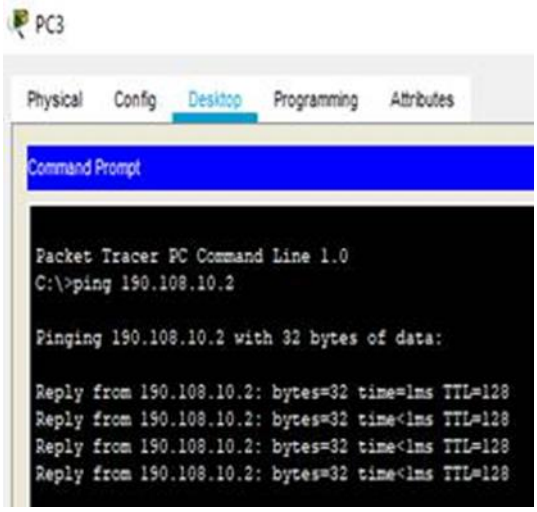


Figura 29. Validación ping Pc4 a Pc7

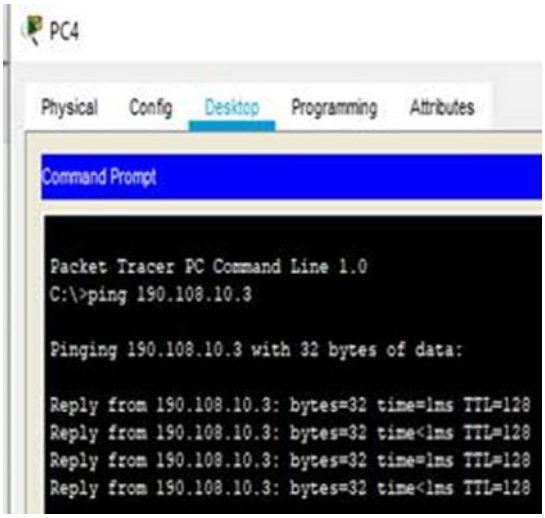


Figura 30. Validación ping Pc8 a Pc2

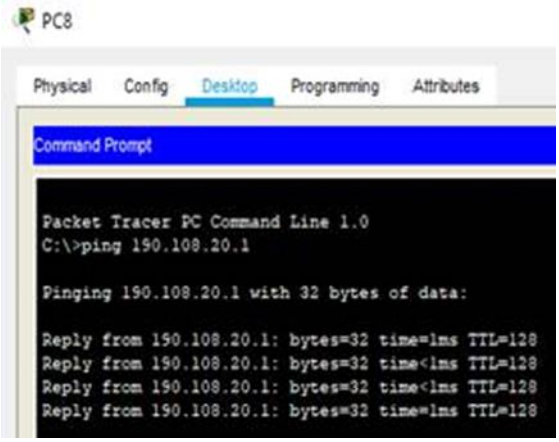


Figura 31. Validación ping Pc9 a Pc1

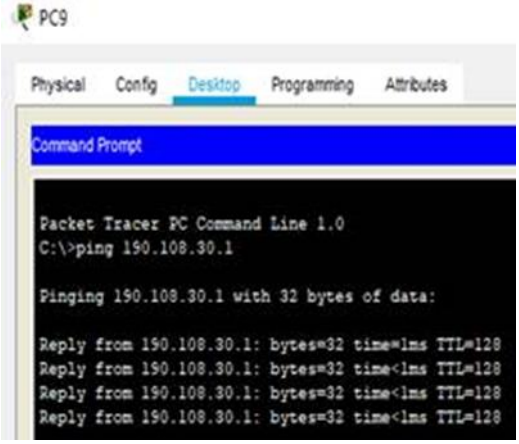


Figura 32. Validación ping Pc1 a Pc8

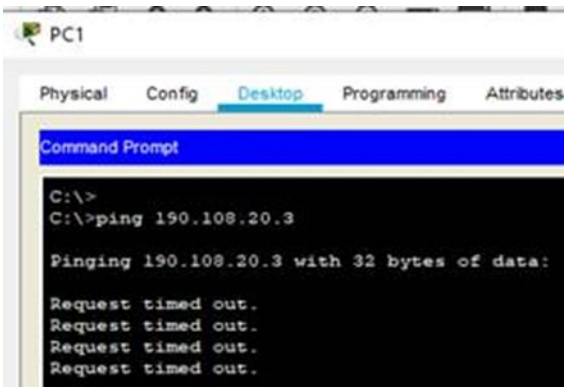
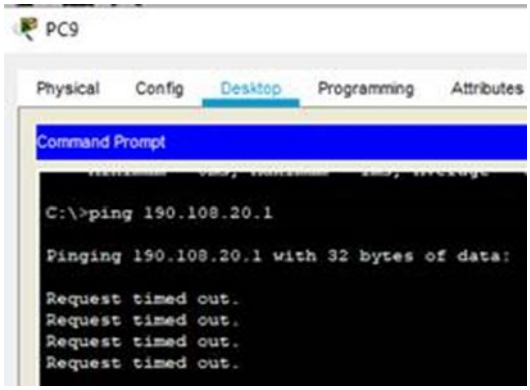


Figura 33. Validación ping Pc9 a Pc2



13. 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

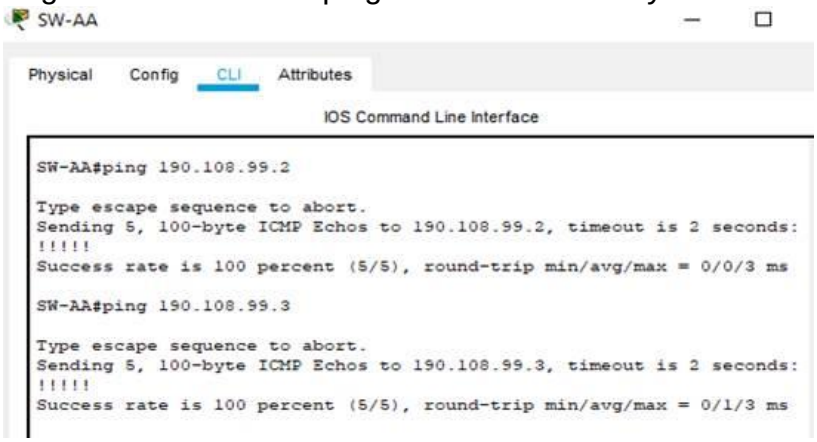


Figura 35. Validación ping SW-BB a SW-AA y SW-CC

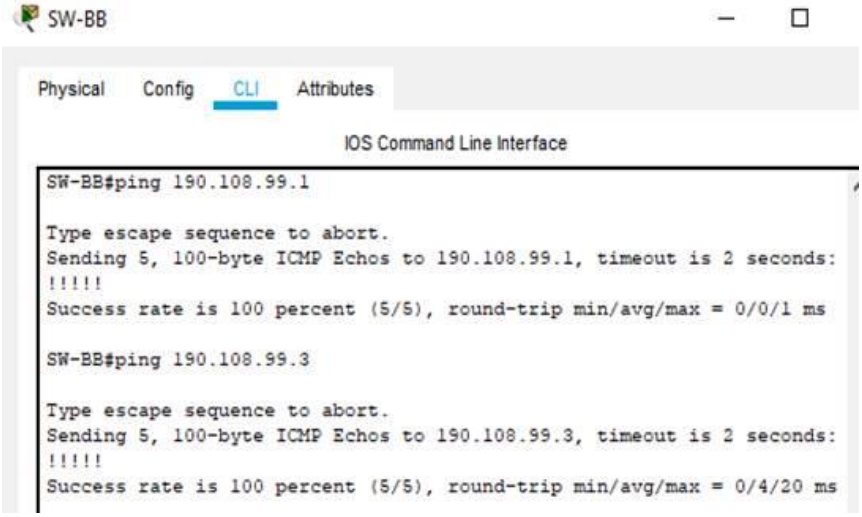
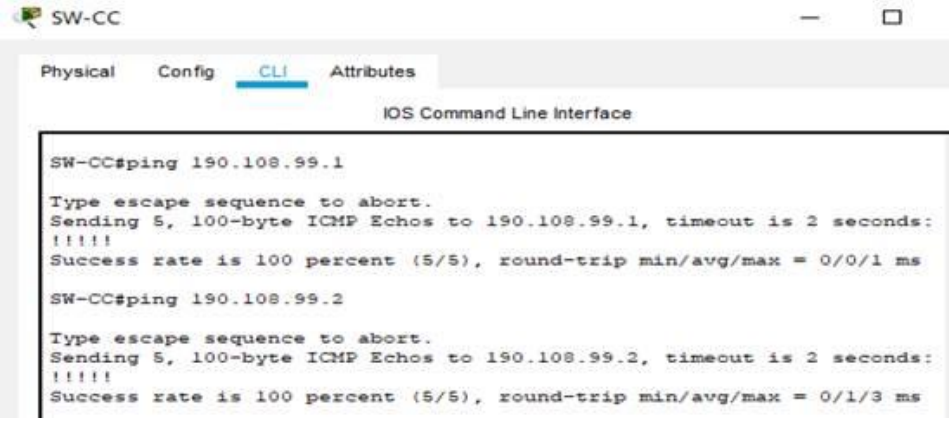


Figura 36. Validación ping SW-CC a SW-AA y SW-BB



14. 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 subred 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

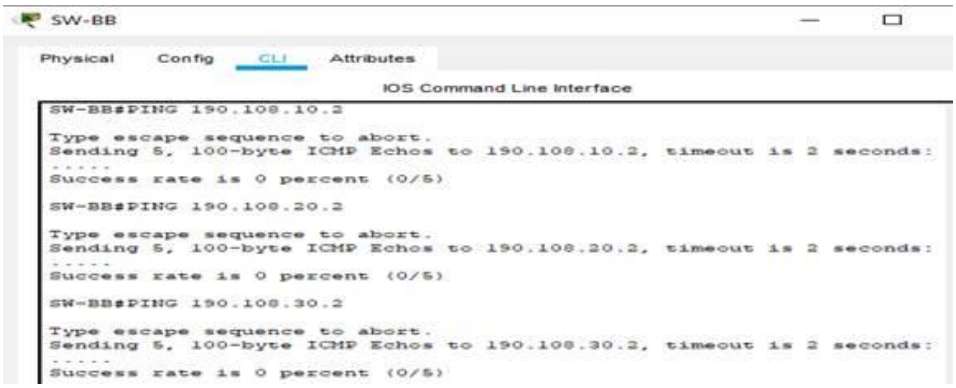


Figura 39. Validación ping SW-CC a Pc7-Pc8 y Pc9

CONCLUSIONES

He podido conocer y comprender como realizar una configuración básica de computadores en una red LAN usando el emulador “CISCO PACKET TRACER”, siendo un tipo de red que se limita a un área relativamente pequeña tal como un cuarto, un edificio, una nave, o un avión; mediante dicho emulador pude simular una conexión de computadores con su respectiva configuración, la cual después de haber conocido el programa a fondo pude desarrollar hasta comprobaciones y verificaciones las cuales me permiten saber el estado correcto de la conexión.

Por medio de estos ejercicios de configuración de routers y switches, comprendemos 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 dependiendo de la topología de red y requerimiento del usuario.

Con el presente trabajo se desarrolló habilidades prácticas en routers y switches CISCO, para aplicarlos en el campo laboral, como futuros administradores de red y configurar una red en los escenarios propuestos, estableciendo los direccionamientos IP, protocolos de enrutamiento y seguridad.

BIBLIOGRAFIAS

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

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

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

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

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

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!AmIJYei-NT1IlnMfy2rhPZHwEoWx

Wallace, K. (2015). CISCO Press (Ed). CCNP Routing and Switching ROUTE 300-101 Official Cert Guide. Recuperado de https://1drv.ms/b/s!AgIGg5JUgUBthFx8WOxiq6LPJppl