INGENIERIA ELECTRÓNICA

DIPLOMADO DE PROFUNDIZACION CCNP

ANA ISABEL NUÑEZ SANCHEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
INGENIERÍA ELECTRÓNICA
DIPLOMADO CISCO CCNP
BOGOTÁ
2019

EVALUACIÓN PRUEBA DE HABILIDADES PRÁCTICAS CCNP

ANA ISABEL NUÑEZ SANCHEZ

Diplomado de profundización cisco CCNP
prueba de habilidades prácticas

Gerardo Granados Acuña
Magíster en Telemática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
INGENIERÍA ELECTRÓNICA
DIPLOMADO CISCO CCNP
BOGOTÁ
2019

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____
_____

_____
Gerardo Granados Acuña

_____
Juan Carlos Vesga Ferreira

_____
Martha Fabiola Contreras Higuera

Bogotá 16 de octubre de 2019

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

BGP: Significa Border Gateway Protocol, es un protocolo que utiliza el sistema para comunicarse entre grandes nodos en el internet y transfiere información muy grande entre dos puntos de la red.

CISCO: Es una empresa de los Estados Unidos que fabrica, vende y da capacitaciones en quipos de comunicaciones y programas en los cuales de manera virtual ofrece al estudiante una manera práctica de entender sobre las redes y sus configuraciones.

CCNP: En ingles significa Certified Network Professional (CCNP). CISCO ofrece unas certificaciones que van por niveles y en este caso pertenece al nivel intermedio.

Comando: Es una orden que el usuario ingresa en un programa por ejemplo cuando se está trabajando en el programa Packet Tracer e ingresamos a un router para dar su configuración de que debe hacer, se hace a través de comandos.

IP: Es una dirección que nos indica la identificación de manera jerárquica una interfaz por ejemplo cuando ingresamos a una página en específico, ella tiene un numero asignado y nosotros accedemos a ella

Interfaz: es un dispositivo o programa que permite la conexión y comunicación para realizar cambio de información puede ser de equipos, programas e incluso para que el usuario tenga un acceso amigable.

Loopback: Es una interfaz de red pero virtual que maneja direcciones del rango 127.0.0.0

Mascara: ayuda a identificar, más bien a diferencias las direcciones IP, pero de una manera más amigable, ya que las máscaras de subred son por ejemplo 255.255.255.0 y no cientos de 1 y 0 que es el sistema binario por el que realmente trabajan las computadoras atrás de estos números.

Packet Tracer: Es un programa de simulación que pertenece a CISCO, en el cual se puede practicar de manera muy fácil el comportamiento de las redes, la

configuración de los equipos y a la vez se puede decir que es como un laboratorio virtual de comunicaciones.

Puerto: Es la puerta de conexión para las interfaces y puede ser físico o también un software, a través de ellos es donde existe la transmisión de datos entre computadoras u otros equipos.

Routers: Esta palabra en español traduce Enrutador y es un equipo que ayuda a la conexión entre computadoras inmersas en una red, la función de este aparato es buscar la ruta para cada paquete de datos

Red: Existen muchas topologías de red, pero en sistemas de comunicaciones una red es la interconexión de que existe entre varios computadores y es vital para aprovechar los recursos de correos electrónicos, el internet, video llamadas, teleconferencias entre otros muchos recursos informáticos.

Switches: La traducción de esta palabra es conmutador, es un dispositivo que sirve para la interconexión de un servidor a varios computadores por ejemplo en las empresas grandes existe el servidor que es donde se almacena toda la información y este va a un conmutador el cual sale para varios equipos entre ellas puede ser también una impresora.

Topología: Es el dibujo físico de las redes. Existe topología de Bus, Estrella, Anillo; árbol.

RESUMEN

Este trabajo contiene 3 escenarios cada uno de ellos muestran 3 imágenes diferentes en las cuales están plasmados diferentes tipos de redes y a continuación explico en que consiste cada una sin el detalle, ya que CISCO en su forma de enseñar es muy detallista con el paso a paso de cada ejercicio con la finalidad de entender e interiorizar cada una.

En el primer escenario se debe realizar configuraciones iniciales de enrutamiento y protocolo, crear interfaces de Loopback; en el escenario 2 se hace la configuración de routers partiendo de información como numero de Interfaz, Dirección IP y Numero de Mascara, por ultimo está el escenario 3 en el cual se debe configurar con VTP los Conmutadores y computadores que se muestran en la figura del escenario.

Palabras Clave: Conmutador, Computadores, VTP, Configurar, Routers, CISCO, Redes, Protocolo.

INTRODUCCIÓN

El presente trabajo tiene por objeto realizar la presentación de los ejercicios relacionados a la Prueba de habilidades que está conformada por tres (3) escenarios**,** utilizando los programas Packet Tracer o GNS3, en la cual se busca identificar el nivel de conocimientos adquiridos por el estudiante para resolver problemas con el **Networking.**

A continuación se presenta la solución para los tres escenarios planteados para este trabajo final, relacionando pantallazos de los resultados acuerdo los lineamientos que fueron otorgados por la guía académica de actividades las cuales son dadas a conocer de primero y posteriormente se muestran las soluciones.

Evaluación – Prueba de habilidades prácticas CCNP

Descripción general de la prueba de habilidades

La evaluación denominada “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.

Para esta actividad, el estudiante dispone de cerca de dos semanas para realizar las tareas asignadas en cada uno de los tres (3) escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos **ping, traceroute, show ip Route, entre otros.**

Teniendo en cuenta que la Prueba de habilidades está conformada por tres (3) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: **Packet Tracer** o **GNS3**.

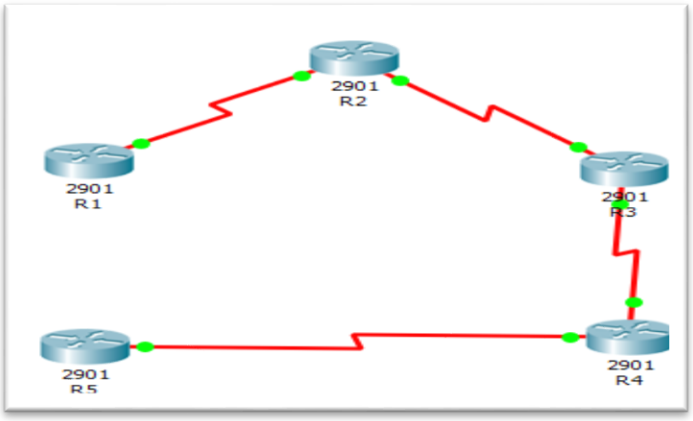
- Es muy importante mencionar que esta actividad es de carácter **INDIVIDUAL y OBLIGATORIA.**

- Toda evidencia de **copy-paste o plagio (de la web o de otros informes)** será penalizada con severidad.

Descripción de escenarios propuestos para la prueba de habilidades

ESCENARIO 1

Figura 1. Escenario 1.



1. Aplique las configuraciones iniciales y los protocolos de enrutamiento para los Routers R1, R2, R3, R4 y R5 según el diagrama. No asigne passwords en los Routers. Configurar las interfaces con las direcciones que se muestran en la topología de red.

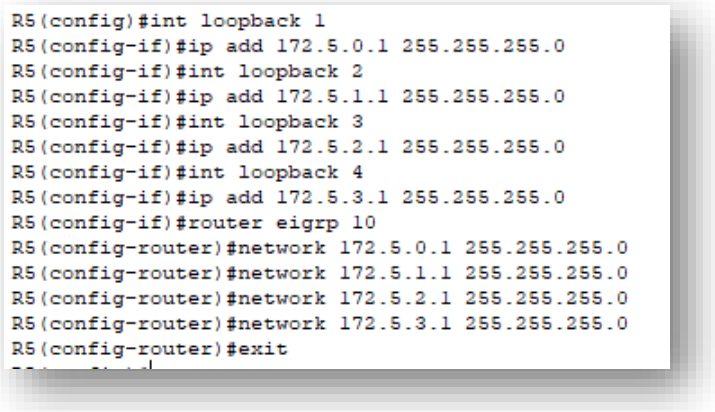
2. Cree cuatro nuevas interfaces de Loopback en R1 utilizando la asignación de direcciones 10.1.0.0/22 y configure esas interfaces para participar en el área 0 de OSPF.

Figura 2. Interfaces de Loopback en R1.

```
R1(config)#int loopback 1
R1(config-if)#ip add 10.1.0.1 255.255.255.0
R1(config-if)#int loopback 2
R1(config-if)#ip add 10.1.1.1 255.255.255.0
R1(config-if)#int loopback 3
R1(config-if)#ip add 10.1.2.1 255.255.255.0
R1(config-if)#int loopback 4
R1(config-if)#ip add 10.1.3.1 255.255.255.0
R1(config-if)#router ospf 1
R1(config-router)#network 10.1.0.0 255.255.255.0 area 0
R1(config-router)#network 10.1.1.0 255.255.255.0 area 0
R1(config-router)#network 10.1.2.0 255.255.255.0 area 0
R1(config-router)#network 10.1.3.0 255.255.255.0 area 0
R1(config-router)#exit
```

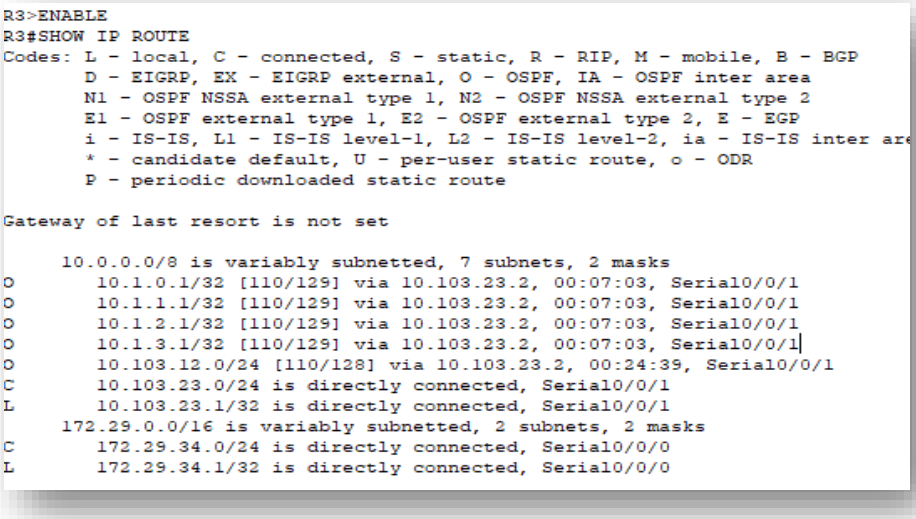
3. Cree cuatro nuevas interfaces de Loopback en R5 utilizando la asignación de direcciones 172.5.0.0/22 y configure esas interfaces para participar en el Sistema Autónomo EIGRP 10.

Figura 3. Interfaces de Loopback en R5.



4. Analice la tabla de enrutamiento de R3 y verifique que R3 está aprendiendo las nuevas interfaces de Loopback mediante el comando ***show ip Route***.

Figura 4. Verificación de interfaces Loopback con comando show ip Route***.***



5. Configure R3 para redistribuir las rutas EIGRP en OSPF usando el costo de 50000 y luego redistribuya las rutas OSPF en EIGRP usando un ancho de banda T1 y 20,000 microsegundos de retardo.

Figura 5. Configuración de R3 con OSPF

```
R3(config)#ROUTER OSPF 1
R3(config-router)#NETWORK 10.103.23.0 0.0.0.255 AREA 0
```

Figura 6. Configuración de Interfaz.

```
interface Serial0/0/0
 ip address 172.29.34.1 255.255.255.0
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.103.23.1 255.255.255.0
 clock rate 64000
```

6. Verifique en R1 y R5 que las rutas del sistema autónomo opuesto existen en su tabla de enrutamiento mediante el comando ***show ip route***.

Figura 7. Pantallazo comando show ip route.

```
R3(config)#ROUTER OSPF 1
R3(config-router)#NETWORK 10.103.23.0 0.0.0.255 AREA 0
```

Figura 8. Pantallazo comando show ip route para R1.

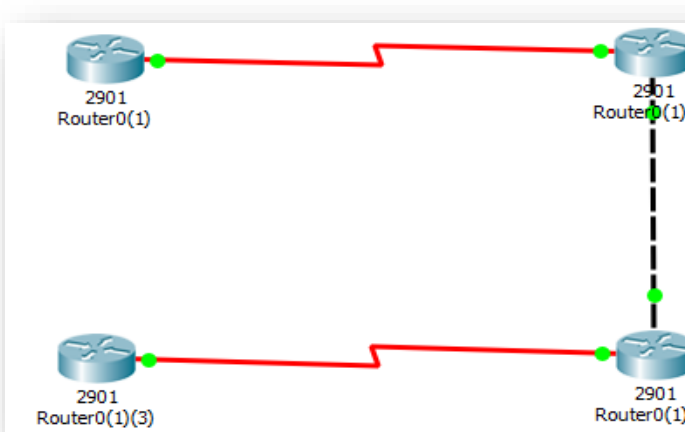
```
R1(config)#int loopback 1
R1(config-if)#ip add 10.1.0.1 255.255.255.0
R1(config-if)#int loopback 2
R1(config-if)#ip add 10.1.1.1 255.255.255.0
R1(config-if)#int loopback 3
R1(config-if)#ip add 10.1.2.1 255.255.255.0
R1(config-if)#int loopback 4
R1(config-if)#ip add 10.1.3.1 255.255.255.0
R1(config-if)#router ospf 1
R1(config-router)#network 10.1.0.0 255.255.255.0 area 0
R1(config-router)#network 10.1.1.0 255.255.255.0 area 0
R1(config-router)#network 10.1.2.0 255.255.255.0 area 0
R1(config-router)#network 10.1.3.0 255.255.255.0 area 0
```

Figura 9. Pantallazo comando show ip route para R5.

```
R5(config)#int loopback 1
R5(config-if)#ip add 172.5.0.1 255.255.255.0
R5(config-if)#int loopback 2
R5(config-if)#ip add 172.5.1.1 255.255.255.0
R5(config-if)#int loopback 3
R5(config-if)#ip add 172.5.2.1 255.255.255.0
R5(config-if)#int loopback 4
R5(config-if)#ip add 172.5.3.1 255.255.255.0
R5(config-if)#router eigrp 10
R5(config-router)#network 172.5.0.1 255.255.255.0
R5(config-router)#network 172.5.1.1 255.255.255.0
R5(config-router)#network 172.5.2.1 255.255.255.0
R5(config-router)#network 172.5.3.1 255.255.255.0
R5(config-router)#exit
```

ESCENARIO 2

Figura 10. Escenario 2.



Información para configuración de los Routers

Tabla 1. Configuración Routers

	Interfaz	Dirección IP	Máscara
R1	**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
	Interfaz	**Dirección IP**	**Máscara**
R2	**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
	Interfaz	**Dirección IP**	**Máscara**
R3	**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 11.11.11.11 para R1 y como 22.22.22.22 para R2. Presente el paso a con los comandos utilizados y la salida del comando ***show ip route.***

```
hostname R1
!
```

Figura 11. Configuración vecino de R1 y R2 con BGP

```
!
interface Loopback0
 ip address 1.1.1.1 255.0.0.0
!
interface Loopback1
 ip address 11.1.0.1 255.255.0.0
!
```

Figura 12. Configuración vecino R1 y R2 con BGP

```
router bgp 2
 bgp router-id 22.22.22.22
 bgp log-neighbor-changes
 no synchronization
 neighbor 192.1.12.1 remote-as 1
 neighbor 192.1.23.3 remote-as 3
 network 2.0.0.0
 network 12.1.0.0 mask 255.255.0.0
!
```

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 33.33.33.33. Presente el paso a con los comandos utilizados y la salida del comando ***show ip route.***

Figura 13. Configuración vecino de R2 y R3 con BGP

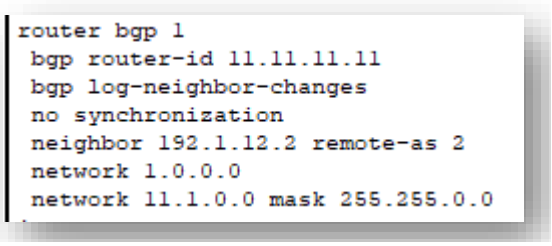


Figura 14. Configuración vecino de R2 y R3 con BGP

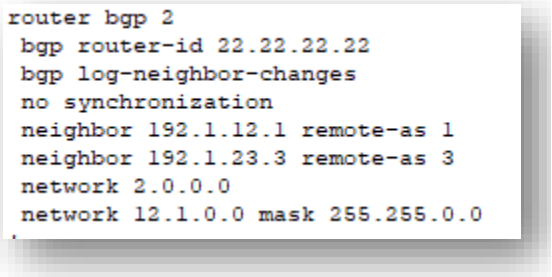
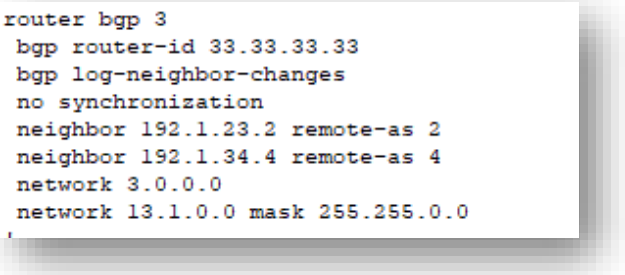


Figura 15. Configuración router R3 con 33.33.33.33.



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 44.44.44.44. 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.***

Figura 16. Configuración vecino de R3 y R4 con BGP.

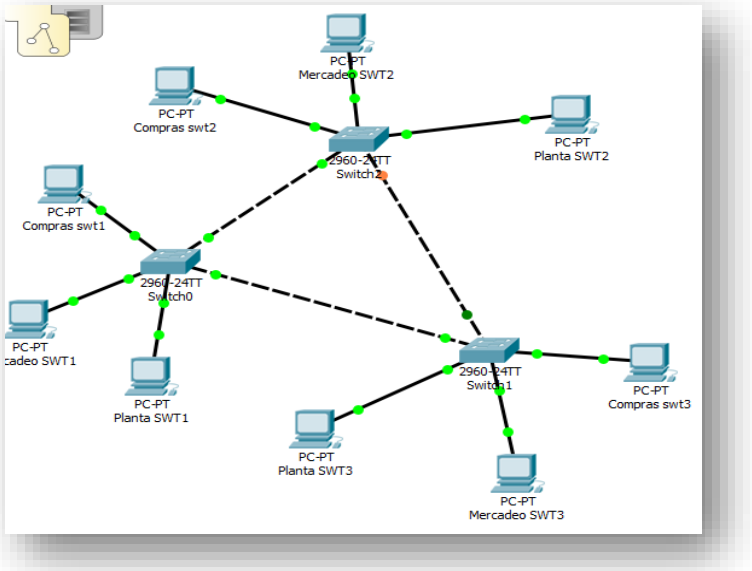
```
interface Loopback0
 ip address 4.4.4.4 255.0.0.0
!
interface Loopback1
 ip address 14.1.0.1 255.255.0.0
!
```

Figura 17. Configuración vecino de R3 y R4 con BGP

```
router bgp 4
 bgp router-id 44.44.44.44
 bgp log-neighbor-changes
 no synchronization
 neighbor 192.1.34.3 remote-as 3
 network 4.0.0.0
 network 14.1.0.0 mask 255.255.0.0
!
```

ESCENARIO 3

Figura 18. Escenario 3



A. Configurar VTP

1. Todos los switches se configurarán para usar VTP para las actualizaciones de VLAN. El switch SWT2 se configurará como el servidor. Los switches SWT1 y SWT3 se configurarán como clientes. Los switches estarán en el dominio VPT llamado CCNP y usando la contraseña cisco.

Figura 19. Configuracion switch SWT2 como servidor.

```
SWT2(config)#hostname SWT2
SWT2(config)#vtp mode server
Device mode already VTP SERVER.
SWT2(config)#vtp domain CCNP
Domain name already set to CCNP.
SWT2(config)#vtp pass cisco
```

Figura 20. Configuración switch SWT1 como cliente.

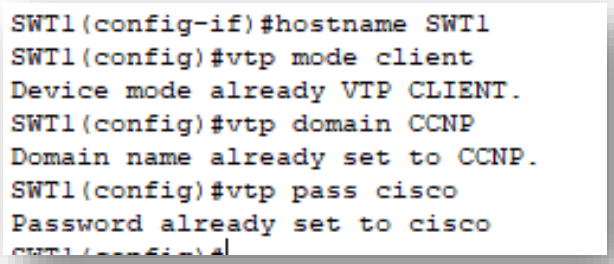


Figura 21. Configuración switch SWT3 como cliente.

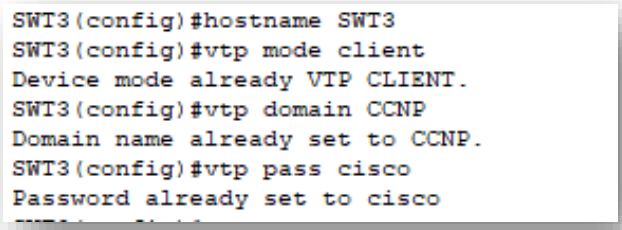
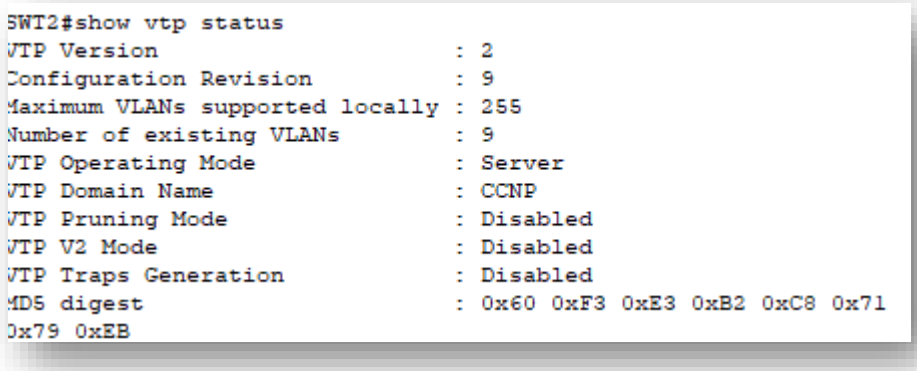


Figura 22. Switches en el dominio VPT.

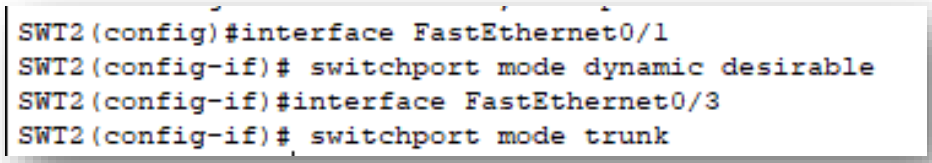


2. Verifique las configuraciones mediante el comando ***show vtp status***.

B. Configurar DTP (Dynamic Trunking Protocol)

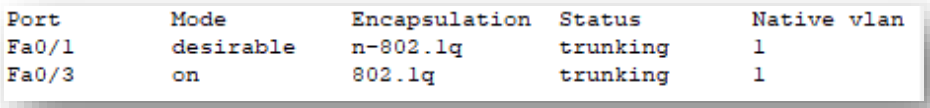
1. Configure un enlace troncal ("trunk") dinámico entre SWT1 y SWT2. Debido a que el modo por defecto es ***dynamic auto***, solo un lado del enlace debe configurarse como ***dynamic desirable***.

Figura 23. Configuración enlace TRUNK SWT1 y SWT2.



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

Figura 24. Verificación de Trunk entre SWT1 y SWT2



3. Entre SWT1 y SWT3 configure un enlace "trunk" estático utilizando el comando switchport ***mode trunk*** en la interfaz F0/3 de SWT1.

Figura 25. Configuración de enlace "trunk" estático entre SWT1 y SWT3

```
SWT3(config)#int fa 0/3
SWT3(config-if)#sw mo tr
SWT3(config-if)#int fa 0/1
SWT3(config-if)#sw mo tr
```

Figura 26. Configuración de enlace "trunk" estático entre SWT1 y SWT3 .

```
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/3       on           802.1q         trunking      1
```

4. Configure un enlace "trunk" permanente entre SWT2 y SWT3.

Figura 27. Configuración enlace Trunk entre SWT2 y SWT3.

```
SWT2(config)#interface FastEthernet0/1
SWT2(config-if)# switchport mode dynamic desirable
SWT2(config-if)#interface FastEthernet0/3
SWT2(config-if)# switchport mode trunk
```

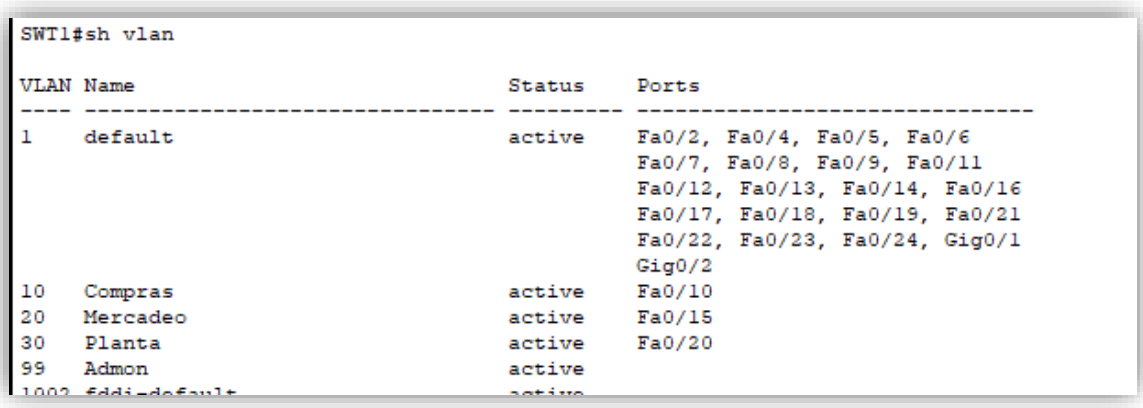
Figura 28. Configuración enlace Trunk entre SWT2 y SWT3.

```
SWT3(config)#int fa 0/3
SWT3(config-if)#sw mo tr
SWT3(config-if)#int fa 0/1
SWT3(config-if)#sw mo tr
```

C. Agregar VLANs y asignar puertos.

1. En STW1 agregue la VLAN 10. En STW2 agregue las VLANS Compras (10), Mercadeo (20), Planta (30) y Admon (99)

Figura 29. VLAN 10 en STW1.

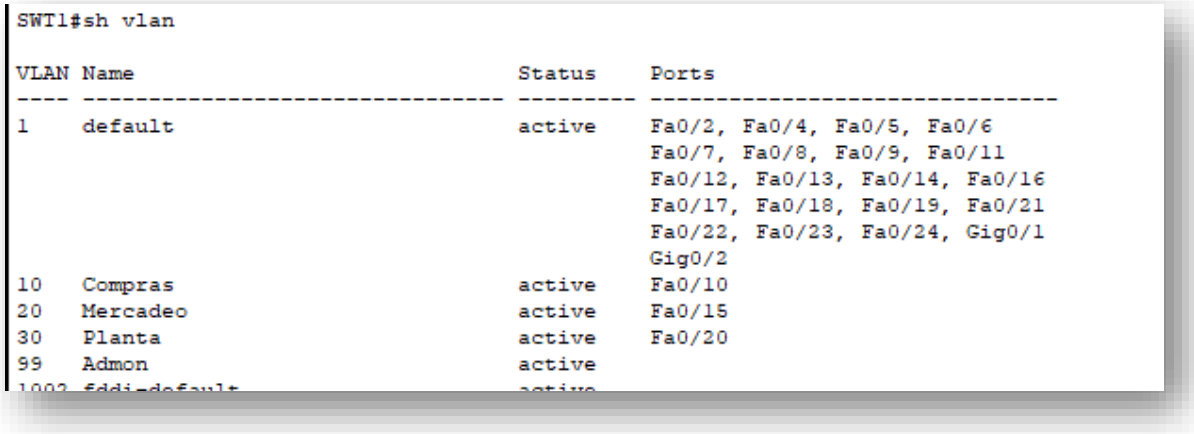


```
SWT1#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
10   Compras                          active    Fa0/10
20   Mercadeo                         active    Fa0/15
30   Planta                           active    Fa0/20
99   Admon                            active
1002 fddi-default                     active
```

2. Verifique que las VLANs han sido agregadas correctamente.

Figura 30. Verificación de VLANs correctas.



```
SWT1#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
10   Compras                          active    Fa0/10
20   Mercadeo                         active    Fa0/15
30   Planta                           active    Fa0/20
99   Admon                            active
1002 fddi-default                     active
```

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

Tabla 2.Direcciones IP

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

X = número de cada PC particular

Figura 31. Asociación de puertos VLAN.

```
SWT2(config-vlan)#vlan 10
SWT2(config-vlan)#name Compras
SWT2(config-vlan)#vlan 20
SWT2(config-vlan)#name Mercadeo
SWT2(config-vlan)#vlan 30
SWT2(config-vlan)#name Planta
SWT2(config-vlan)#vlan 99
SWT2(config-vlan)#name Admon
```

4. Configure el puerto F0/10 en modo de acceso para SWT1, SWT2 y SWT3 y asígnelo a la VLAN 10.

Figura 32. Configuración de puerto F0/10 a SWT1.

```
SWT1(config)#interface FastEthernet0/10
SWT1(config-if)# switchport access vlan 10
SWT1(config-if)#interface FastEthernet0/15
SWT1(config-if)# switchport access vlan 20
SWT1(config-if)#interface FastEthernet0/20
SWT1(config-if)# switchport access vlan 30
```

Figura 33. Configuración de puerto F0/10 a SWT2.

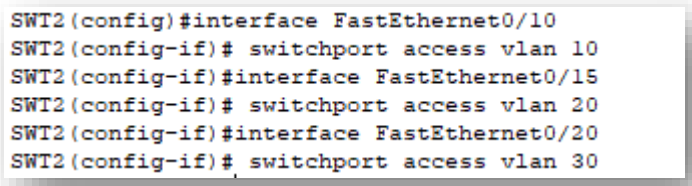
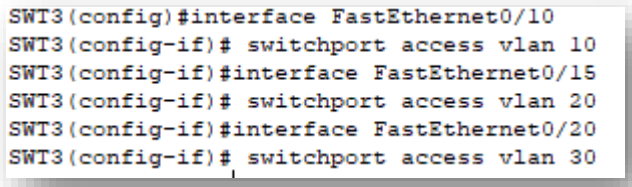


Figura 34. Configuración de puerto F0/10 a SWT3.



5. Repita el procedimiento para los puertos F0/15 y F0/20 en SWT1, SWT2 y SWT3. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

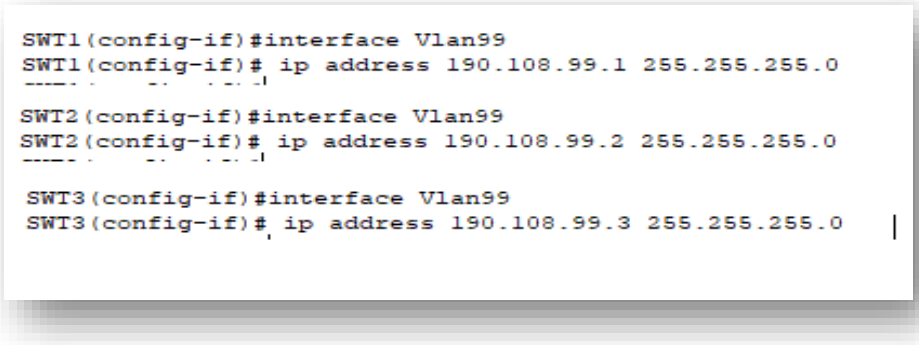
D. Configurar las direcciones IP en los Switches.

1. 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 3. Direccionamiento

Equipos	Interfaz	Dirección IP	Máscara
SWT1	VLAN 99	190.108.99.1	255.255.255.0
SWT2	VLAN 99	190.108.99.2	255.255.255.0
SWT3	VLAN 99	190.108.99.3	255.255.255.0

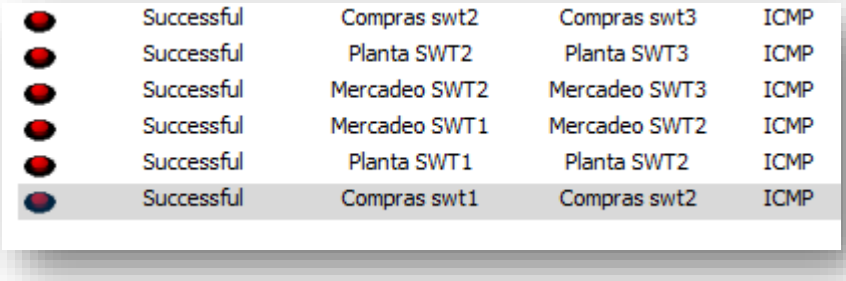
Figura 35. Asignación a SWT1, SWT2 y SWT3 la VLAN 99 con IP.



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

Figura 36. Ejecución de PING a cada PC y Switch.



CONCLUSIONES

Acuerdo los lineamientos de las guías académicas que se desarrollaron en el curso y por último la del presente trabajo, me permitió adquirir conocimientos desde lo más básico hasta la conformación y configuración de varios tipos de redes en las que se evidencia acuerdo los pantallazos, que el objetivo de las guías de CISCO las cuales son muy didácticas y tienen una forma de llevar al estudiante de la mano para aprender de una manera virtual y llevarlo a la vida laboral, puedo concluir que se superó la meta y es una puerta hacia un nuevo conocimiento para mí ya que en la Ingeniería Electrónica he tenido la oportunidad de desempeñarme en la parte de Metrología Variables Eléctricas y no en la parte de comunicaciones, lo cual para mí es un referente importante y un nuevo conocimiento que espero pueda aplicar cuando se me presente la oportunidad en el campo laboral.

BIBLIOGRAFIA

PING y TRACER como estrategias en procesos de Networking Este Objeto Virtual de Aprendizaje, titulado Video – Ping y Tracer como estrategias en procesos de Networking, tiene como objetivo, orientar al estudiante sobre el uso de las herramientas ping y tracer para la resolución de problemas de networking

UNAD (2014). Ping y Tracer como estrategias en procesos de Networking [OVA]. Recuperado dehttps://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf

Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de http://gonda.nic.in/swangonda/pdf/ccna1.pdf

CISCO. (2014). Exploración de la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1