PRUEBA DE HABILIDADES PRÁCTICAS CISCO CCNP

EDIER ALFONSO MURCIA ARREDONDO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA - ECTBI
INGENIERÍA DE ELECTRÓNICA
DIPLOMADO CISCO CCNP
PITALITO - HUILA
2019

PRUEBA DE HABILIDADES PRÁCTICAS CISCO CCNP

EDIER ALFONSO MURCIA ARREDONDO

Diplomado de profundización cisco CCNP pruebas de
Habilidades prácticas

Gerardo Granados Acuña
Magíster en Telemática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA - ECTBI
INGENIERÍA DE ELECTRÓNICA
DIPLOMADO CISCO CCNP
PITALITO - HUILA
2019

NOTA DE ACEPTACION

_____
_____
_____
_____
_____
_____

_____
Presidente del jurado

_____
Jurado

_____
Jurado

Pitalito – Huila Mayo de 2019

AGRADECIMIENTOS

Deseo agradecer a nuestro tutor Gerardo Granados y cada tutor que han aportado de forma considerable a un crecimiento profesional y personal en alcanzar metas de enriquecimiento en el conocimiento logrando culminar este proceso de una forma exitosa.

TABLA DE CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

GLOSARIO

CISCO PACKET TRACER: es un potente programa de simulación de red que permite a los estudiantes experimentar con el comportamiento de la red. Packet Tracer complementa equipo físico en el aula, al permitir a los estudiantes a crear una red con un número casi ilimitado de dispositivos, fomentar la práctica, el descubrimiento y solución de problemas.

RED: es un conjunto de equipos nodos y software conectados entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios

ROUTER: permite interconectar computadoras que funcionan en el marco de una red, se encarga de establecer qué ruta se destinará a cada paquete de datos dentro de una red informática.

SWITCH: que son los encargados de la interconexión de equipos dentro de una misma red, o lo que es lo mismo, son los dispositivos que, junto al cableado, constituyen las redes de área local o LAN.

RESUMEN

En el siguiente Informe, se desarrollaron los escenarios correspondientes a la configuración de los escenarios propuestos en la prueba de habilidades prácticas del diplomado de profundización cisco CCNP, en ellas encontramos una descripción clara y precisa de las configuraciones utilizadas en el desarrollo de nuestros laboratorios con su respectiva evidencia de su correcto funcionamiento.

Es importante resaltar la importancia que tienen las redes en nuestra actualidad y en constante crecimiento en todas las aplicaciones que se requieren para una mayor seguridad y rapidez en la obtención de información. En nuestro presente informe se presentara algunos de los métodos que hemos aprendido en el trascurso del diplomado CISCO

ABSTRACT

In the following report, the results corresponding to the configuration of the proposed results were developed in the CCNP's practice of deepening diplomacy practices, in which there is a clear and precise description of the functions used in the development of our laboratories. with your Respect for its correct functioning.

It is important to highlight the importance of networks in our present and constantly growing in all applications that are required for greater security and speed in obtaining information. In our present report we present some of the methods we have learned in the course of the CISCO course.

Palabras clave: Cisco, Router, Switch,

INTRODUCCIÓN

Podemos visualizar en nuestro entorno cotidiano la necesidad por las comunicaciones y la importancia de generar una mayor seguridad a nuestros datos como la facilidad de los mismos en cualquier lugar en que los requerimos, tanto en lo individual como en una organización o empresa.

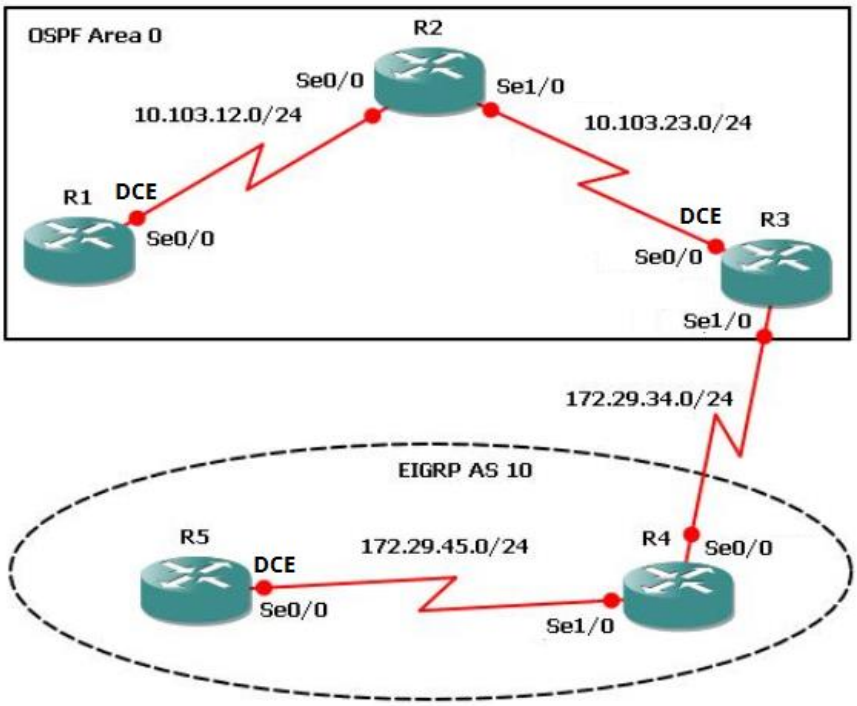
Vemos esta gran necesidad de las redes de datos y su respectivo crecimiento en el mundo de las comunicaciones donde nos enfrentamos a un crecimiento diario en lo cual nosotros estamos en la responsabilidad de afrontar estos desafíos que nos ofrece el diario vivir en nuestra ingeniería en lo cual nos fortalecemos en el aprendizaje de un mayor conocimiento para implementar protocolos efectivos de enrutamiento y seguridad de las redes WAN, LAN, PAN, CAN, MAN, SAN, VLAN, etc.

En nuestro trabajo final de enrutamiento vamos a implementar o profundizar en los dispositivos de routers y Switch los cuales son equipos que tienen sus diferentes actividades pero con un mismo fin de trasmitir o enrutar nuestros datos en los cuales nos ayudan optimizar los errores y a facilitar el viaje de datos de un dispositivo a otro hasta direccionar a su destino final. Estos equipos los podemos configurar según nuestra necesidad y su función requerida por una comunidad o empresa como tal.

En nuestro trabajo desarrollado podemos ver los conocimientos adquiridos en nuestro curso de CCNP en lo cual encontramos tres ejercicios con sus respectivas configuraciones requeridas y simulado en de Packet tracer.

1 ESCENARIO 1

Figura 1. Descripción Escenario 1



1.1 ACTIVIDAD

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.

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.

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***.

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.

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***.

1.2 DESARROLLO

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.

1.2.1 Configuración R1

```
Router>
Router>enable                    /  Se configura el ingreso a modo privilegiado
Router#configure terminal     /  Se configura el Ingreso a modo de configuración
Router(config)#hostname R1       /  Se configura para asignar nombre al router
R1(config)#router ospf 1            /  Se asigna protocolo ospf
R1(config-router)#router-d 1.1.1.1/La configuración nos permite Identificar el router
R1(config-router)#network 10.103.12.0 255.255.255.0 area 0 / Asignamos configuración IP
R1(config-router)#exit
R1(config)#interface s0/0           /  La Configuración del interfaz serial 0
R1(config-if)description to R2
R1(config-if)#ip address 10.103.12.1 255.255.255.0
R1(config-if)#clock rate 128000    /  Asignamos configuración de clock rate
R1(config-if)#bandwidth 128        /  Se asigna bandwidth
R1(config-if)#no shutdown          /  Activamos interfaz
R1(config-if)#exit
R1(config)#end
R2#wr
```

1.2.2 Configuración R2

```
Router>
Router>enable                    /  Se configura el ingreso a modo privilegiado
Router#configure                 /  Se configura el Ingreso a modo de configuración
Router(config)#hostname R2       /  Se configura para asignar nombre al router
R2(config)#router ospf 1         /  Se asigna protocolo ospf
R2(config-router)#router-id 2.2.2.2  /  La configuración nos permite Identificar el
router
R2(config-router)#network 10.103.12.0 255.255.255.0 area 0 / Asignamos
configuración IP
R2(config-router)#network 10.103.23.0 255.255.255.0 area 0
R2(config-router)#exit
R2(config)#interface s0/0        /  La Configuración del interfaz serial 0
R2(config-if)description to R1
R2(config-if)#ip address 10.103.12.2 255.255.255.0
R2(config-if)#no shutdown        /  Activamos interfaz

R2(config-if)#exit
R2(config)#interface s0/1        / Ingresamos interfaz
R2(config-if)description to R3
R2(config-if)#ip address 10.103.23.1 255.255.255.0  / Asignamos configuración IP
R2(config-if)#no shutdown        /  Activamos interfaz
R2(config-if)#exit
R2(config)#end
R2#wr
```

1.2.3 Configuración R3

```
Router>
Router>enable                    /  Se configura el ingreso a modo privilegiado
Router#configure                 /  Se configura el Ingreso a modo de configuración
Router(config)#hostname R3       /  Se configura para asignar nombre al router
R3(config)#router ospf 1         /  Se asigna protocolo ospf
R3(config-router)#router-id 3.3.3.3 /  La configuración nos permite Identificar el
router
R3(config-router)#network 10.103.23.0 255.255.255.0 area 0 / Asignamos
configuración IP
R3(config-router)#exit
R3(config)#interface s0/0        /  La Configuración del interfaz serial 0
R3(config-if)description to R2
R3(config-if)#ip address 10.103.23.2 255.255.255.0
R3(config-if)#clock rate 128000  /  Asignamos configuración de clock rate
R3(config-if)#bandwidth 128      /  Se asigna bandwidth
R3(config-if)#no shutdown        /  Activamos interfaz
```

R3(config-if)#exit
R3(config)#interface s0/1 / La Configuración del interfaz serial 1
R3(config-if)description to R4
R3(config-if)#ip address 172.29.34.1 255.255.255.0 / Asignamos configuración IP
R3(config-if)#no shutdown / Activamos interfaz
R3(config-if)#exit
R3(config)#end
R3#wr
R3#configure / Se configura el ingreso a modo privilegiado
R3(config)#router eigrp 10 / Configuramos protocolo eigrp
R3(config-rtr)#eigrp router-id 3.3.3.3 / La configuración nos permite Identificar el router
R3(config-rtr)#network 172.29.34.0 255.255.255.0
R3(config-rtr)#exit
R3(config)#end
R3#wr

1.2.4 Configuración R4

Router>
Router>enable / Se configura el ingreso a modo privilegiado
Router#configure / Se configura el Ingreso a modo de configuración
Router(config)#hostname R4 / Se configura para asignar nombre al router
R4(config)#router eigrp 10 / Configuramos protocolo eigrp
R4(config-rtr)#eigrp router-id 4.4.4.4 / La configuración nos permite Identificar el router
R4(config-rtr)#network 172.29.34.0 255.255.255.0 / Asignamos configuración IP
R4(config-rtr)#network 172.29.45.0 255.255.255.0
R4(config-rtr)#exit
R4(config)#interface s0/0 / La Configuración del interfaz serial 0
R4(config-if)#ip address 172.29.34.2 255.255.255.0
R5(config-if)#no shutdown / Activamos interfaz
R4(config-if)#exit
R4(config)#interface s0/1 / La Configuración del interfaz serial 1
R4(config-if)#ip address 172.29.45.1 255.255.255.0
R5(config-if)#no shutdown / Activamos interfaz
R4(config-if)#exit
R4(config)#end
R4#wr

1.2.5 Configuración R5

Router>
Router>enable / Se configura el ingreso a modo privilegiado

```
Router#configure                    /    Se configura el Ingreso a modo de configuración
Router(config)#hostname R5          /    Se configura para asignar nombre al router
R5(config)#router eigrp 10          /    Configuramos Protocolo eigrp
R5(config-rtr)#eigrp router-id 5.5.5.5  /    La configuración nos permite Identificar el
router
R4(config-rtr)#network 172.29.45.0 255.255.255.0
R5(config)#interface s0/0           /    La Configuración del interfaz serial 0
R5(config-if)#ip address 172.29.45.2 255.255.255.0 / Asignamos configuración IP
R5(config-if)#no shutdown           /    Activamos interfaz
R5(config-if)#exit
R5(config)#end
R5#wr
```

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.

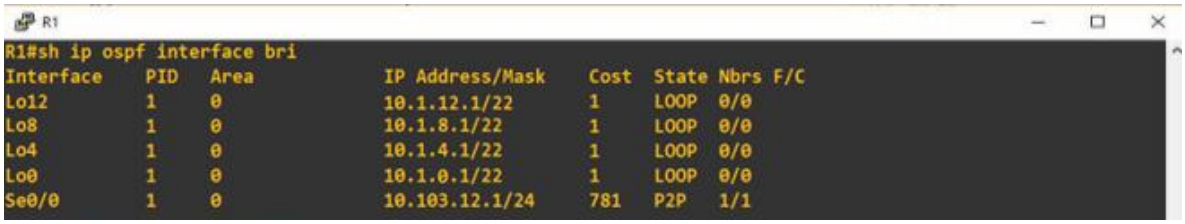
1.2.6 Realización de interfaces de Loopback en R1

Creamos cuatro interfaces Loopback en R1, en lo cual tenemos la máscara de sub red 255.255.252.0, En esta configuración ingresamos a la interfaz Loopback 0, 4, 8, y 12 a cada una se les asigna una dirección ip.

1.2.7 Loopback en R1

```
R1#conf t
R1(config)#interface loopback 0     / Configuramos y creamos la interfaz loopback 0
R1(config-if)#ip address 10.1.0.1 255.255.252.0 / Asignamos configuración IP
R1(config-if)#ip ospf 1 area 0      /    Configuramos en  OSPF
R1(config-if)#exit
R1(config)# interface loopback 4    / Configuramos y creamos la interfaz loopback 4
R1(config-if)#ip address 10.1.4.1 255.255.252.0 / Asignamos configuración IP
R1(config-if)#ip ospf 1 area 0    /    configuración en OSPF
R1(config-if)#exit
R1(config)# interface loopback 8 /Configuramos y creamos la interfaz loopback 8
R1(config-if)#ip address 10.1.8.1 255.255.252.0 / Asignamos configuración IP
R1(config-if)#ip ospf 1 area 0   /    configuración en OSPF
R1(config-if)#exit
R1(config)# interface loopback 12 /Configuramos y creamos la interfaz loopback 12
R1(config-if)#ip address 10.1.12.1 255.255.252.0 / Asignamos configuración IP
R1(config-if)#ip ospf 1 area 0      /    configuración en OSPF
R1(config-if)#exit
R1(config)#end
R1#wr
```

Figura 2. Loopback en R1

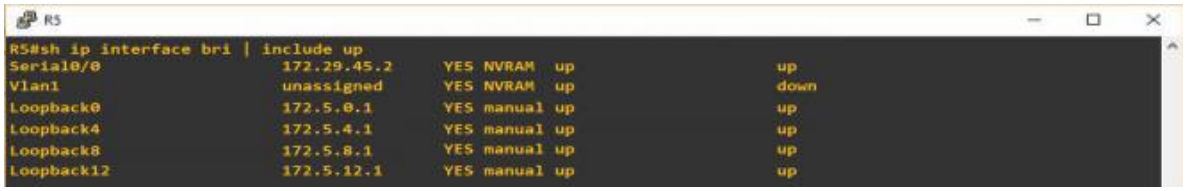


3- Cree cuatro nuevas interfaces de Loopback en R5 utilizando la asignación de direcciones 172.5.0.0/22 y configure esas interfaces para participar en el Sistema Autónomo EIGRP 10.

1.2.8 Loopback en R5

R5#conf t
R5(config)#interface loopback 0 / Configuramos y creamos la interfaz loopback 0
R5(config-if)#ip address 172.5.0.1 255.255.252.0 / Asignamos configuración IP
R5(config-if)#exit
R5(config)#int lo 4 / Configuramos y creamos la interfaz loopback 4
R5(config-if)#ip address 172.5.4.1 255.255.252.0 / Asignamos configuración IP
R5(config-if)#exit
R5(config)#int lo 8 / Configuramos y creamos la interfaz loopback 8
R5(config-if)#ip address 172.5.8.1 255.255.252.0 / Asignamos configuración IP
R5(config-if)#exit
R5(config)#int lo 12 / Configuramos y creamos la interfaz loopback 12
R5(config-if)#ip address 172.5.12.1 255.255.252.0 / Asignamos configuración IP
R5(config-if)#exit

Figura 3. Loopback en R5

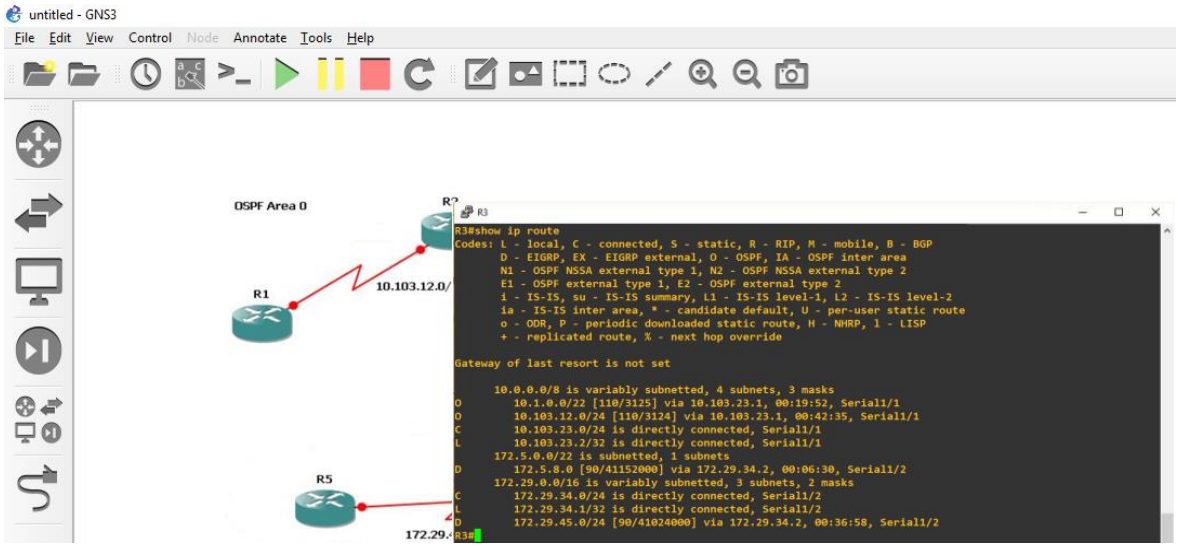


4- Analice la tabla de enrutamiento de R3 y verifique que R3 está aprendiendo las nuevas interfaces de Loopback mediante el comando ***show ip route***.

El comando ***show ip route*** nos arroja el siguiente resultado:

1.2.9 Comando show ip route

Figura 4. Interfaces de Loopback R3



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.

1.2.10 Distribuir las rutas OSPF en EIGRP

R3(config)#router eigrp 10 / Configuramos Protocolo eigrp
R3(config-router)#redistribute ospf 1 metric 100000 20000 255 255 1500 / Configuramos la distribución de las rutas EIGRP
R3(config-router)#exit
R3(config)#router ospf 1 / Se asigna protocolo ospf
R3(config-router)#redistribute eigrp 10 metric 50000 subnets
R3(config-router)#exit
R3(config)#end
R3#wr

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***.

1.2.11 Configurados los comando show ip route

Figura 5. Configuración R1

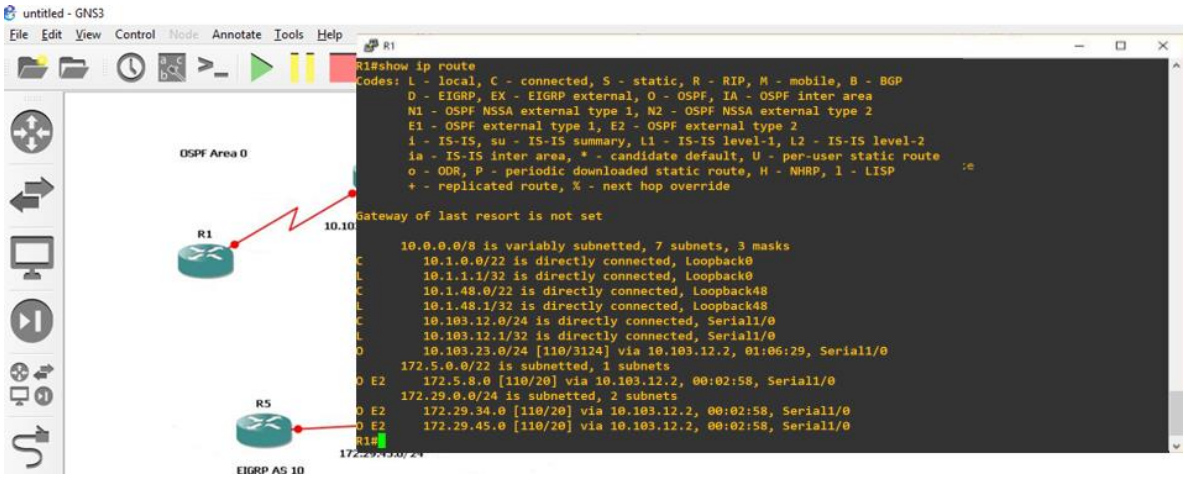
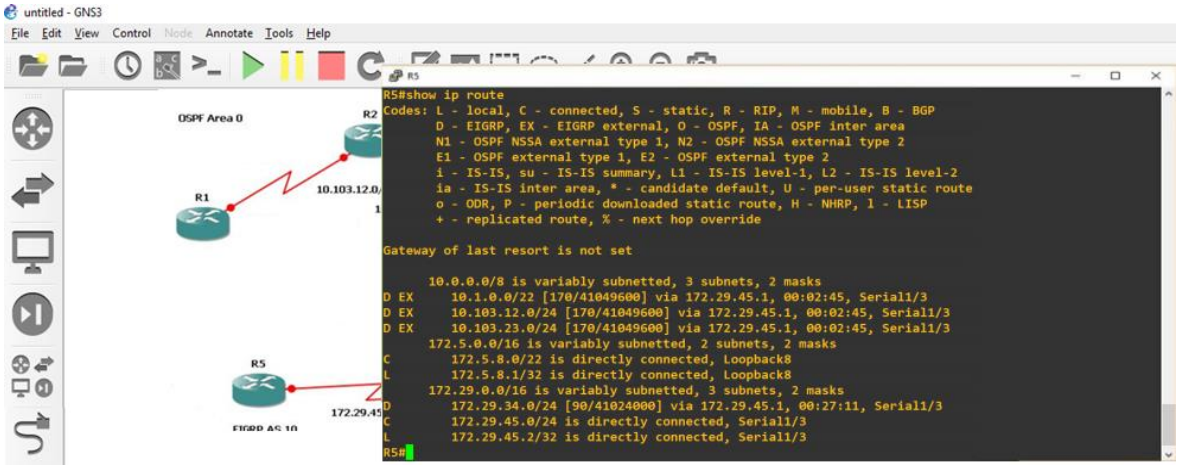
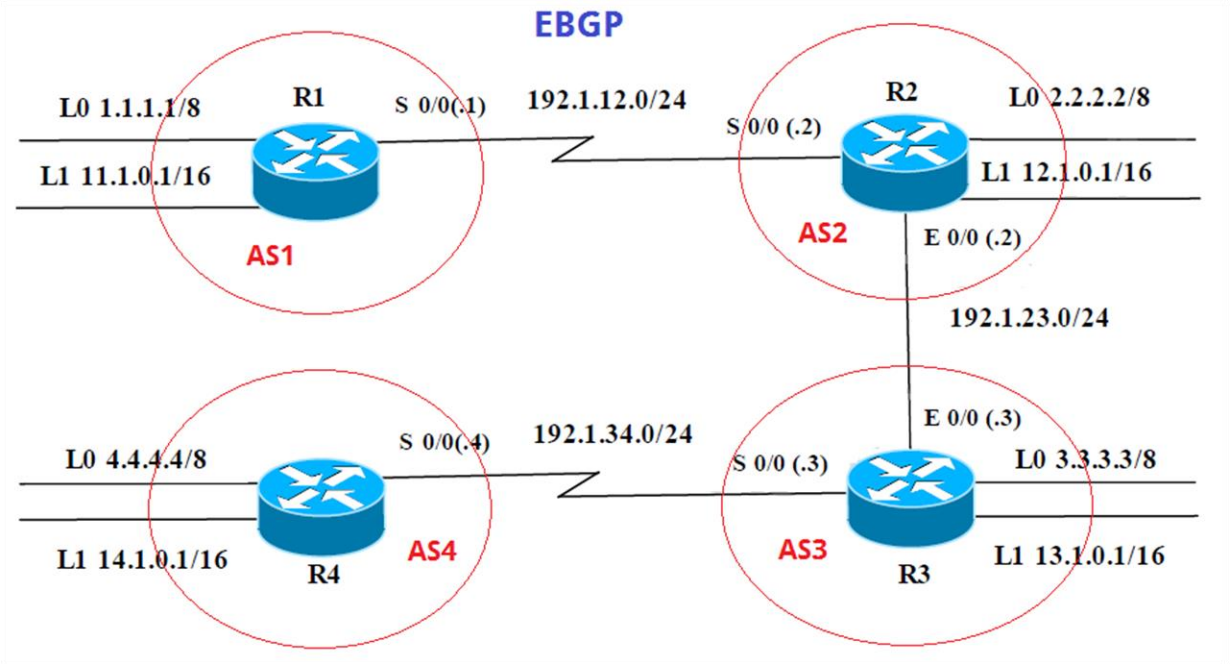


Figura 6. Configuración R5



2 ESCENARIO 2

Figura 7. Descripción Escenario 2



2.1 CONFIGURACIÓN DE LOS ROUTERS

Tabla 1. Configuración R1, R2, R3, R4

	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

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

2.2 ACTIVIDAD

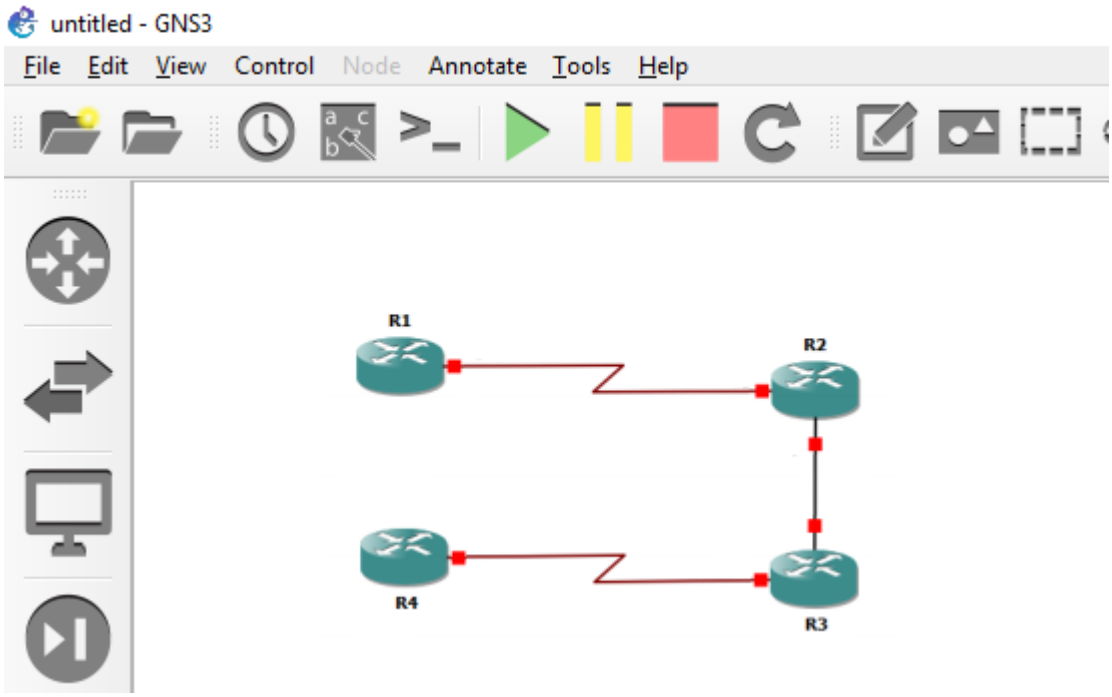
1- Configure una relación de vecino BGP entre R1 y R2. R1 debe estar en **AS1** y R2 debe estar en **AS2**. Anuncie las direcciones de Loopback en BGP. Codifique los ID para los routers BGP como 11.11.11.11 para R1 y como 22.22.22.22 para R2. Presente el paso a con los comandos utilizados y la salida del comando ***show ip route.***

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.***

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.***

2.3 DESARROLLO

Figura 8. Montaje Escenario 2.



Vamos a configurar los routers según la tabla que tenemos, creamos los loopBack.

2.3.1 Configuración R1

Router>
Router>enable / Se configura el ingreso a modo privilegiado
Router#configure terminal / Se configura el Ingreso a modo de configuración
Router(config)#hostname R1 / Se configura para asignar nombre al router
R1(config)#interface Loopback0 / Configuramos y creamos la interfaz loopback 0
R1(config-if)#ip address 1.1.1.1 255.0.0.0 / Asignamos configuración IP
R1(config-if)#exit
R1(config)#interface Loopback1 / Configuramos y creamos la interfaz loopback 1
R1(config-if)#ip address 11.1.0.1 255.255.0.0 / Asignamos configuración IP
R1(config-if)#exit
R1(config)#interface serial 0/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#clock rate 128000 / Asignamos configuración de clock rate
R1(config-if)#no shutdown / Activamos interfaz
R1(config-if)#exit

R1(config)#

2.3.2 Configuración R2

```
Router>
Router>enable                    /   Se configura el ingreso a modo privilegiado
Router#configure terminal        /   Se configura el Ingreso a modo de configuración
Router(config)#hostname R2       /   Se configura para asignar nombre al router
R2(config)#interface Loopback0       / Configuramos y creamos la interfaz loopback
0
R2(config-if)#ip address 2.2.2.2 255.255.255.0      / Asignamos configuración IP
R2(config-if)#exit
R2(config)#interface Loopback1                  / Configuramos y creamos la interfaz
loopback 1
R2(config-if)#ip address 12.1.0.1 255.255.0.0    / Asignamos configuración IP
R2(config-if)#exit
R2(config)#interface serial 0/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown       /    Activamos interfaz
R2(config-if)#exit
R2(config)#interface FastEthernet 0/0      /    Se Configura la interface
R2(config-if)#ip address 192.1.23.2 255.255.255.0   / Asignamos configuración IP
R2(config-if)#no shutdown       /    Activamos interfaz
R2(config-if)#exit
R2(config)#
```

2.3.3 Configuración R3

```
Router>
Router>enable                    /   Se configura el ingreso a modo privilegiado
Router#configure terminal        /   Se configura el Ingreso a modo de configuración
Router(config)#hostname R3       /   Se configura para asignar nombre al router
R3(config)#interface Loopback0       / Configuramos y creamos la interfaz loopback
0
R3(config-if)#ip address 3.3.3.3 255.255.255.0    / Asignamos configuración IP
R3(config-if)#exit
R3(config)#interface Loopback1       / Configuramos y creamos la interfaz loopback
1
R3(config-if)#ip address 13.1.0.1 255.255.0.0 / Asignamos configuración IP
R3(config-if)#exit
R3(config)#interface serial 0/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0     / Asignamos configuración IP
R3(config-if)#clock rate 128000       /   Asignamos configuración de clock rate
R3(config-if)#no shutdown        /    Activamos interfaz
```

```
R3(config-if)#exit
R3(config)#interface FastEthernet 0/0          /     Se Configura la interface
R3(config-if)#ip address 192.1.23.3 255.255.255.0      / Asignamos configuración IP
R3(config-if)#n
```

2.3.4 Configuración R4

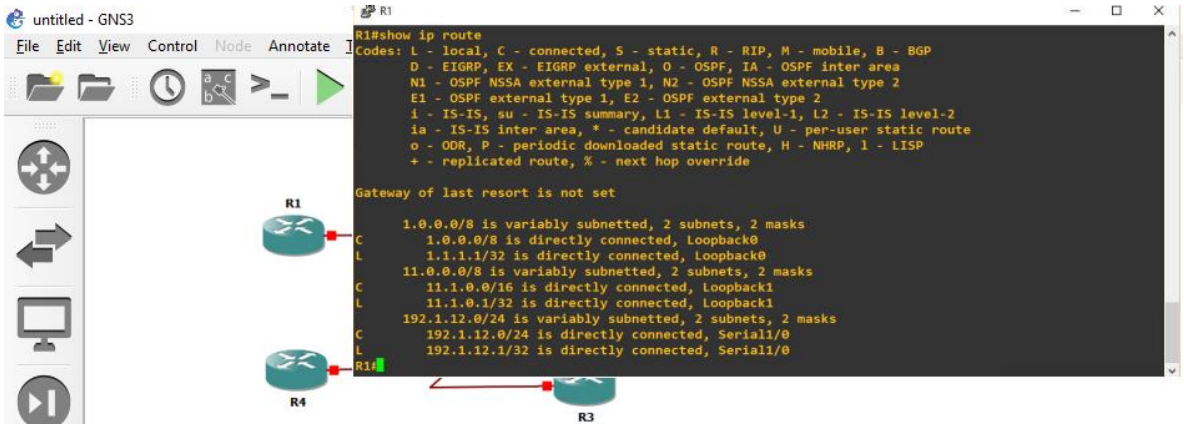
```
Router>
Router>enable                    /    Se configura el ingreso a modo privilegiado
Router#configure terminal        /    Se configura el Ingreso a modo de configuración
Router(config)#hostname R3       /     Se configura para asignar nombre al router
R4(config)#interface Loopback0       / Configuramos y creamos la interfaz loopback
0
R4(config-if)#ip address 4.4.4.4 255.255.255.0      / Asignamos configuración IP
R4(config-if)#exit
R4(config)#interface Loopback1       / Configuramos y creamos la interfaz loopback
1
R4(config-if)#ip address 14.1.0.1 255.255.0.0    / Asignamos configuración IP
R4(config-if)#exit
R4(con fig)#interface serial 0/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0    / Asignamos configuración IP
R4(config-if)#no shutdown        /      Activamos interfaz
R4(config-if)#exit
R4(config)#
```

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.***

2.3.5 Simulación y configuración de R1

```
R1(config)#router bgp 1
R1(config-router)#bgp router-id 11.11.11.11
R1(config-router)#neighbor 192.1.12.2 remote-as 2
R1(config-router)#network 1.1.1.0 mask 255.255.255.0
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router)#exit
R1(config)#
```

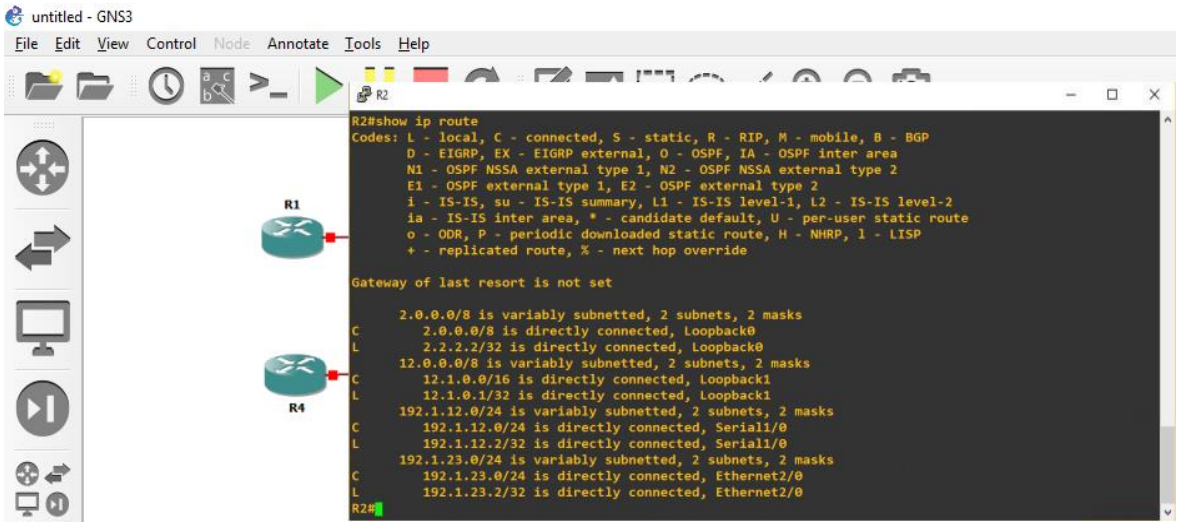
Figura 9. Simulación y configuración de R1



2.3.6 Simulación y configuración de R2

```
R2(config)#router bgp 2
R2(config-router)#bgp router-id 22.22.22.22
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#neighbor 192.1.23.3 remote-as 3
R2(config-router)#network 2.2.2.0 mask 255.255.255.0
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
R2(config-router)#
```

Figura 10. Simulación y configuración de 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 33.33.33.33. Presente el paso a con los comandos utilizados y la salida del comando ***show ip route.***

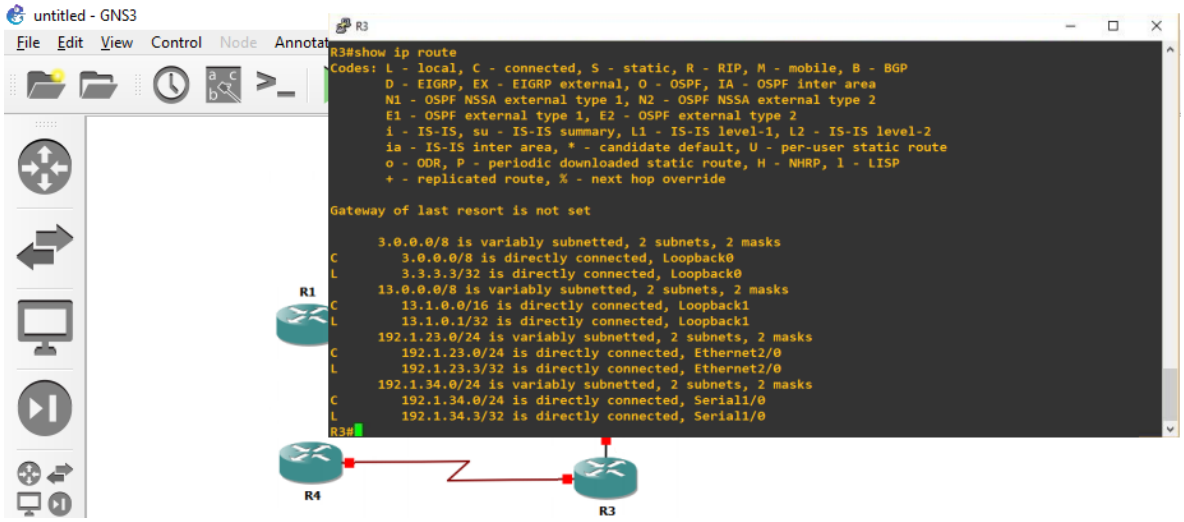
2.3.7 Configuración entre R2 y R3

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router bgp 2
R2(config-router)#neighbor 192.1.23.3 remote-as 3
```

2.3.8 Configuración entre R3 y R2

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router bgp 3
R3(config-router)#neighbor 192.1.23.3 remote-as 3
R3(config-router)#router rip
R3(config-router)#network 2.2.2.2
R3(config-router)#redistribute bgp 4
R3(config-router)#router bgp 4
R3(config-router)#neighbor 33.33.33.33 remote-as 3
R3(config-router)#neighbor 33.33.33.33 distribute-list 1 out
R3(config-router)#redistribute rip
R3(config-router)#access-list 1 permit 2.2.2.2 255.0.0.0
```

Figura 11. Configuración Entre R3 y 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 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.***

2.3.9 Realizamos la configuración entre R3 y R4

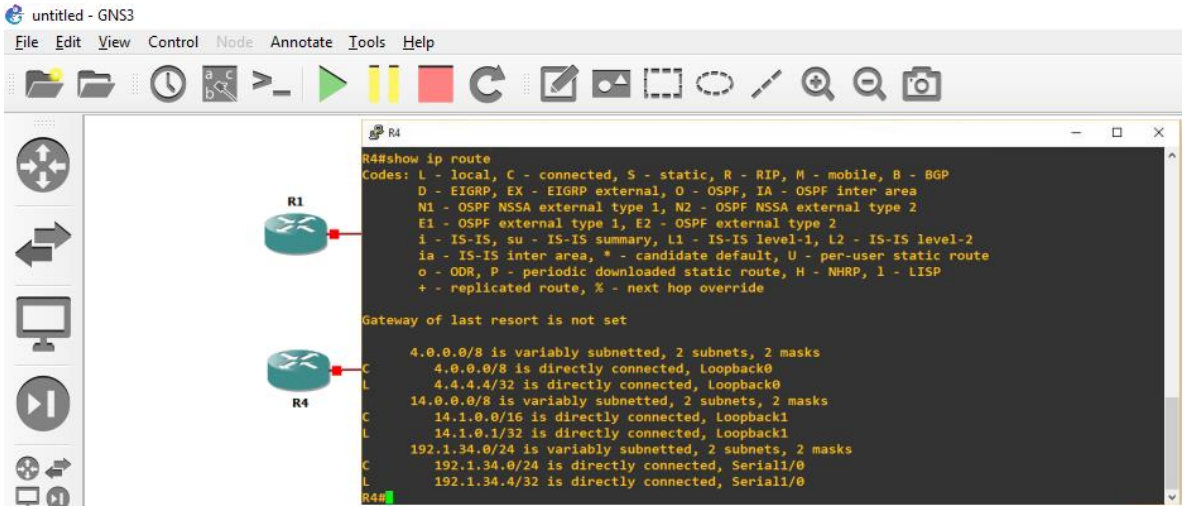
```
Router>enable
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router bgp 3
R3(config-router)#neighbor 192.1.34.2 remote-as 4
R3(config-router)#network 4.4.4.4
```

2.3.10 Realizamos la configuración entre R4 y R3

```
Router>enable
R4#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#router bgp 4
R4(config-router)#neighbor 192.1.34.2 remote-as 3
R4(config-router)#network 3.3.3.3
```

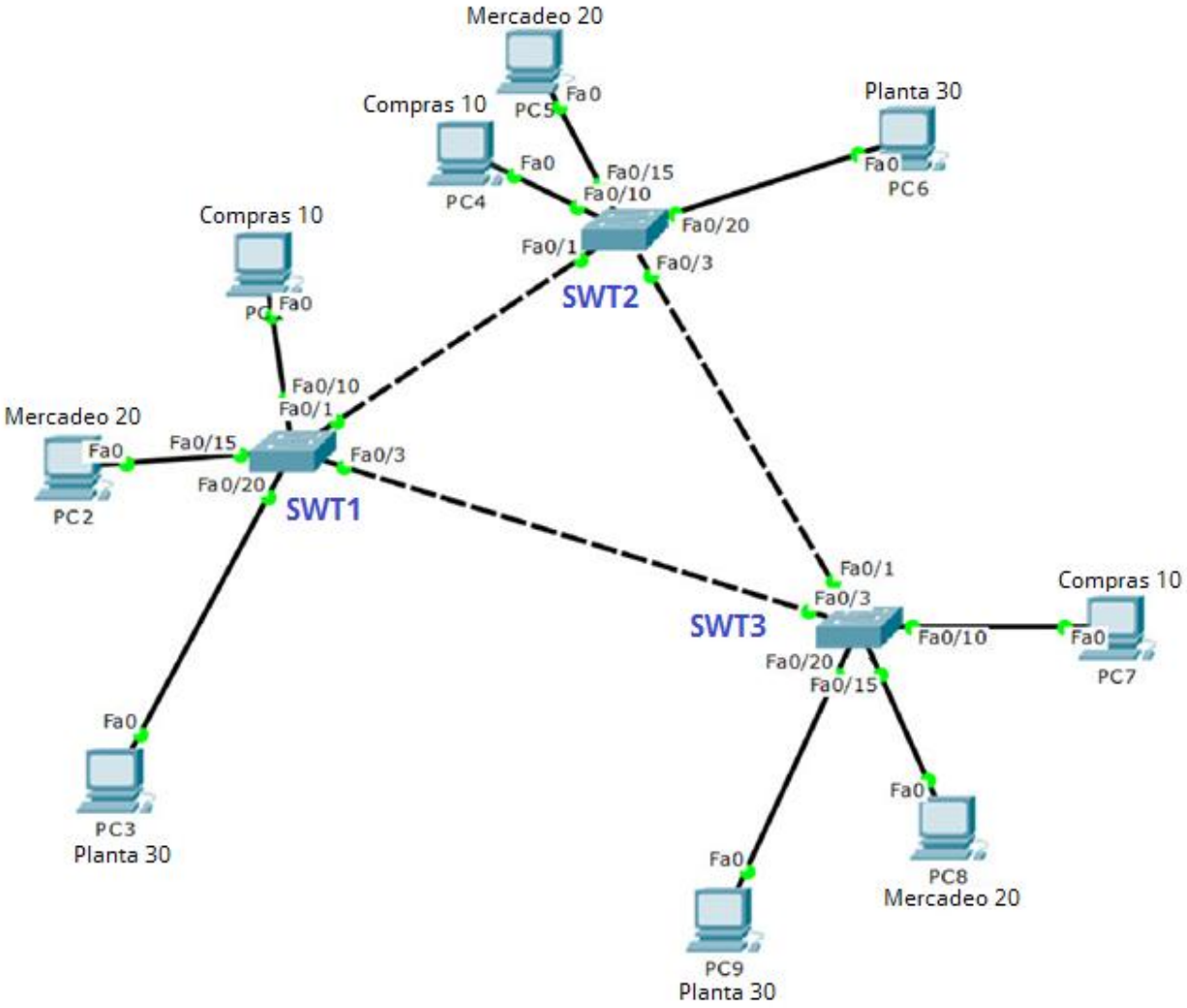
```
R4(config-router)#router rip
R4(config-router)#network 3.3.3.3
R4(config-router)#redistribute bgp 4
R4(config-router)#router bgp 4
R4(config-router)#
R4(config-router)#neighbor 44.44.44.44 remote-as 3
R4(config-router)#neighbor 44.44.44.44 distribute-list 1 out
R4(config-router)#access-list 1 permit 3.3.3.3 255.0.0.0
```

Figura 12. Configuración Entre R4 y R3



3 ESCENARIO 3

Figura 13. Descripción Escenario 3



3.1 ACTIVIDAD

A. Configurar VTP

B. Configurar DTP (Dynamic Trunking Protocol)

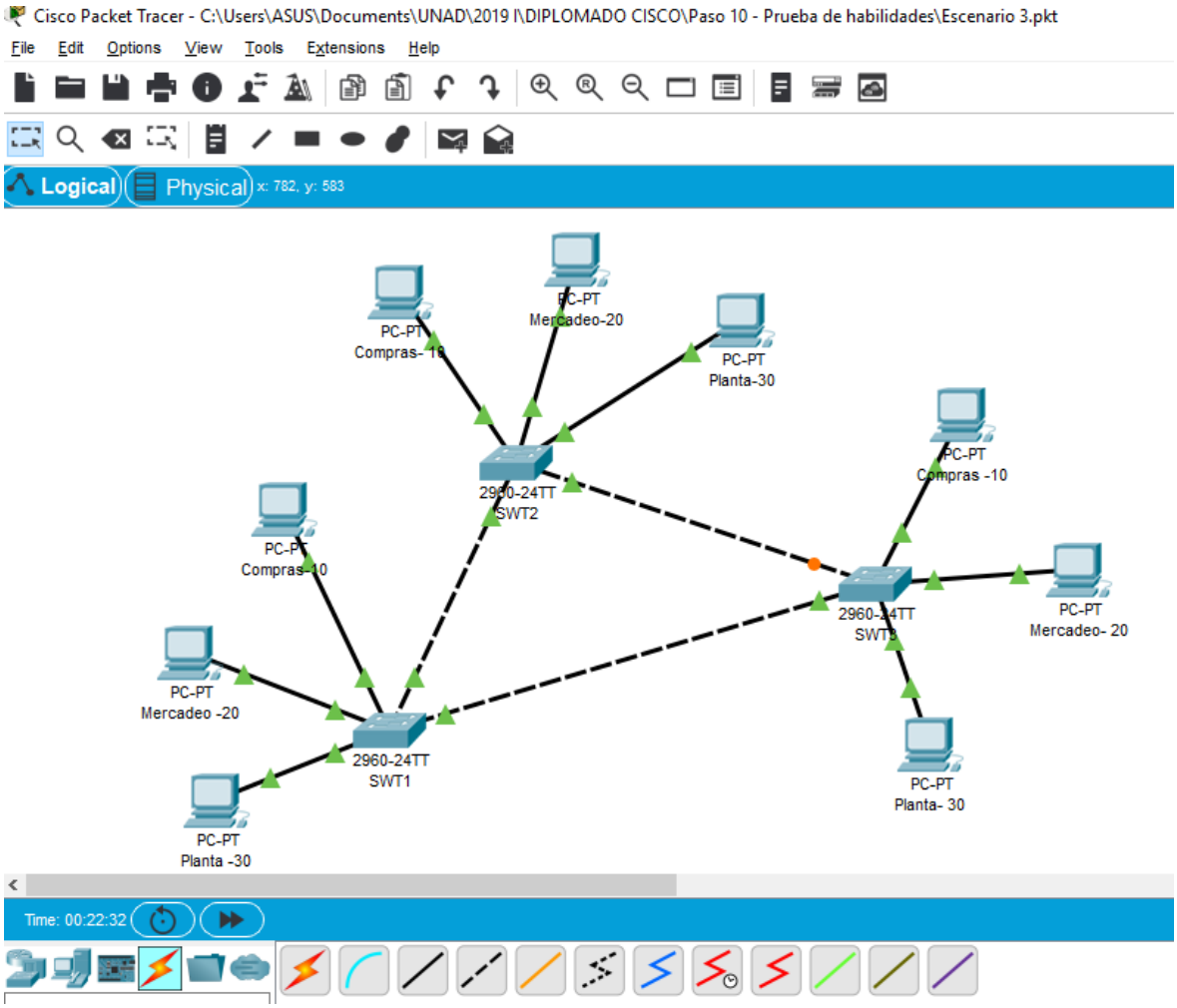
C. Agregar VLANs y asignar puertos.

D. Configurar las direcciones IP en los Switches.

E. Verificar la conectividad Extremo a Extremo

3.2 DESARROLLO

Figura 14. Montaje Escenario 3



3.2.1 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.

3.2.1.1 Configuración SWT2

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SWT2
SWT2(config)#vtp domain CCNP
Changing VTP domain name from NULL to
CCNP SWT2(config)#vtp version 2
SWT2(config)#vtp mode server Device mode
already VTP SERVER.
SWT2(config)#vtp password cisco
Setting device VLAN database password to
cisco SWT2(config)#
```

3.2.1.2 Configuración SWT1

```
Switch>enable
Switch#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SWT1
SWT1(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SWT1(config)#vtp version 2
SWT1(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWT1(config)#vtp password cisco
Setting device VLAN database password to cisco
SWT1(config)#
```

3.2.1.3 Configuración SWT3

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SWT3
SWT3(config)#vtp domain CCNP
Changing VTP domain name from NULL to
```

CCNP SWT3(config)#vtp version 2
SWT3(config)#vtp mode client Setting device to
VTP CLIENT mode.
SWT3(config)#vtp password cisco
Setting device VLAN database password to
cisco SWT3(config)#

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

3.2.1.4 Verificación de comandos “TRunk” entre swt1 y swt2

Figura 15. Switch SWT1

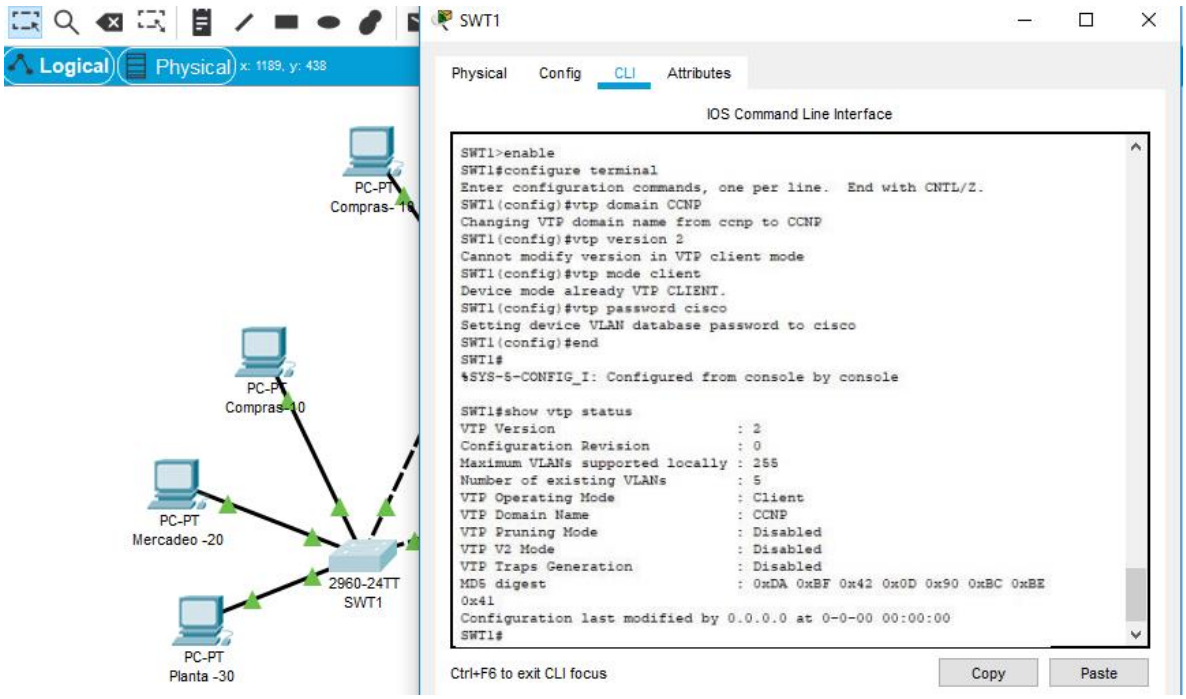


Figura 16. Switch SWT2

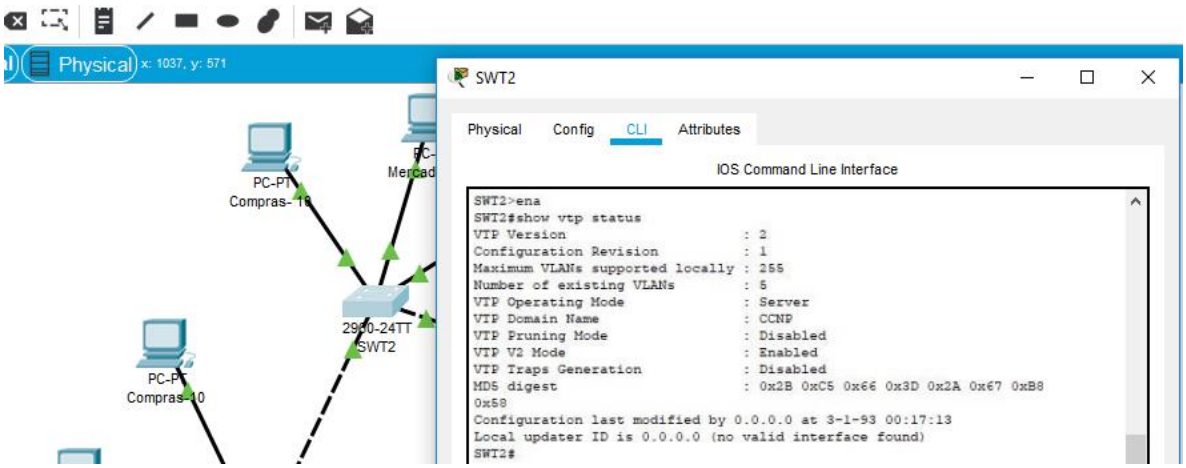
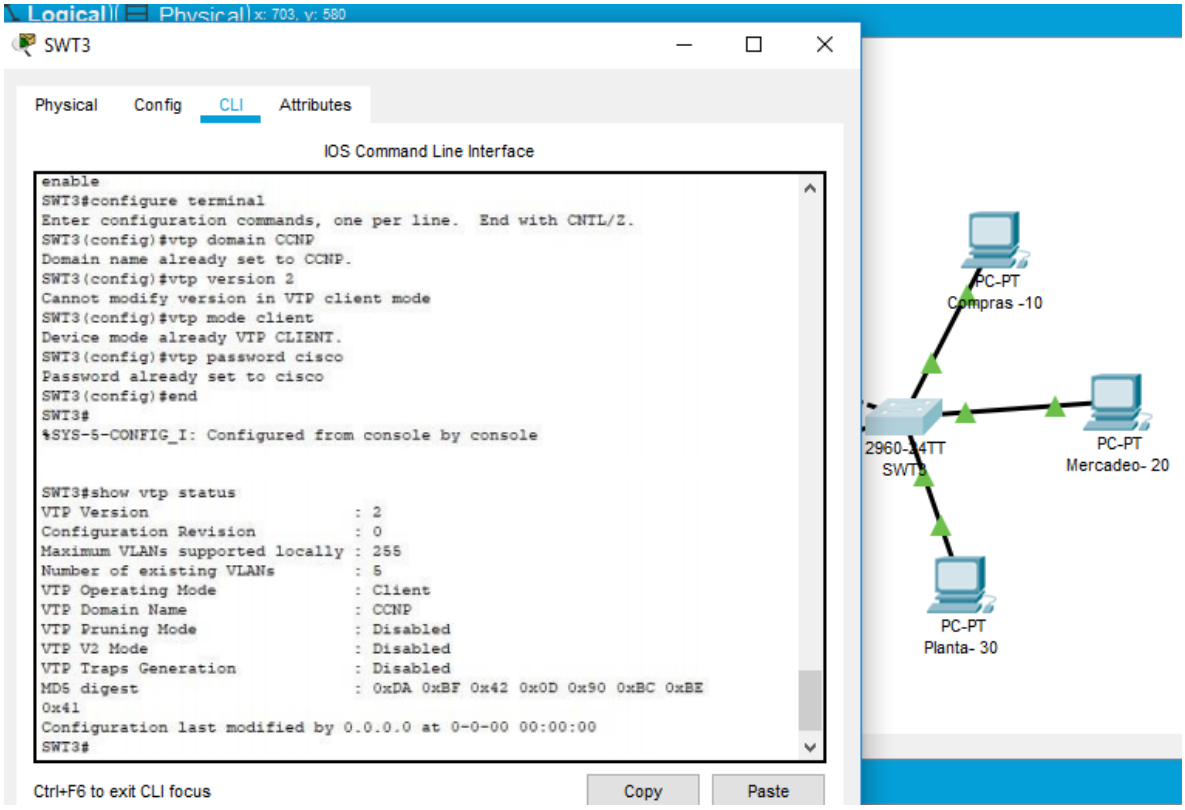


Figura 17. Switch SWT3



3.2.2 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***.

3.2.2.1 Switch SWT1

Switch>enable / Se configura el ingreso a modo privilegiado
SWT1#configure terminal / Se configura el Ingreso a modo de configuración
SWT1(config)#interface range ethernet0/0 - 1
SWT1(config-if-range)#switchport trunk encapsulation dot1q / Habilitamos el trunk standar SWT1(config-if-range)#switchport mode trunk / Habilitamos el modo trunk en la int.
SWT1(config-if-range)#switchport mode dynamic desirable / Configuramos dynamic desirable SWT1(config-if-range)#no shutdown / Activamos interfaz
SWT1(config-if-range)#exit
SWT1(config)#end
SWT1#wr

3.2.2.2 Switch SWT2

Switch>enable / Se configura el ingreso a modo privilegiado
SWT2#configure terminal / Se configura el Ingreso a modo de configuración
SWT2(config)#interface range ethernet0/0
SWT2(config-if-range)#switchport trunk encapsulation dot1q / Habilitamos el trunk standar SWT2(config-if-range)#switchport mode trunk / Habilitamos el modo trunk en la int. SWT2(config-if-range)#switchport mode dynamic desirable / Configuramos el modo dynamic desirable
SWT2(config-if-range)#no shutdown / Activamos interfaz
SWT2(config-if-range)#exit
SWT2(config)#interface range ethernet0/2
SWT2(config-if-range)#switchport trunk encapsulation dot1q / Activamos interfaz
SWT2(config-if-range)#switchport mode trunk / Habilitamos el modo trunk en la int.
SWT2(config-if-range)#switchport mode dynamic desirable / Configuramos el modo dynamic desirable
SWT2(config-if-range)#no shutdown / Activamos interfaz
SWT2(config-if-range)#exit
SWT2(config)#end
SWT2#wr

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

3.2.2.3 Verificación de enlace "trunk" entre SWT1 y SWT2

Figura 18. Enlace de trunk en STW1

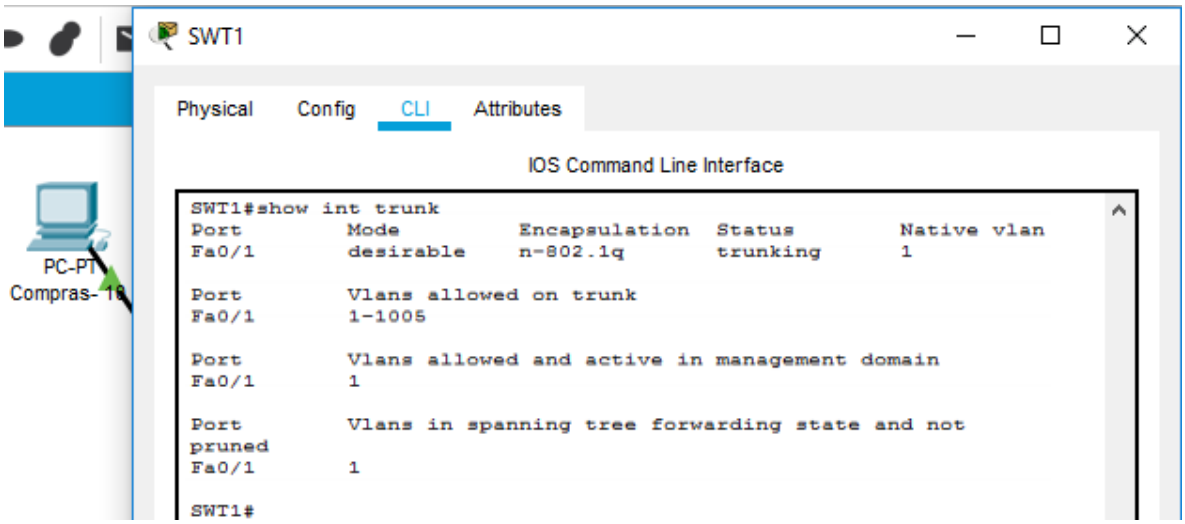
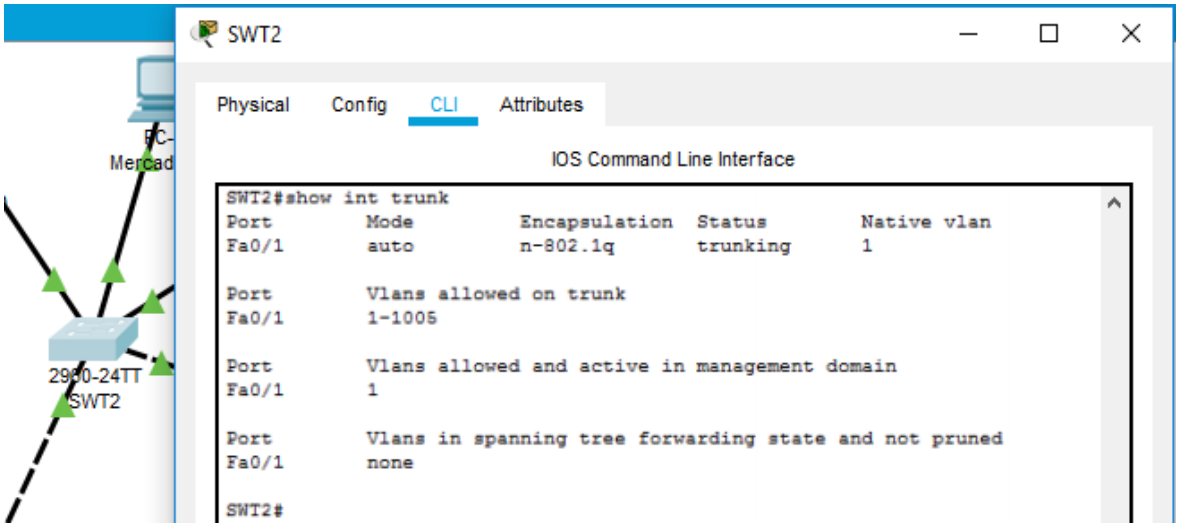


Figura 19. Enlace de trunk en STW2



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

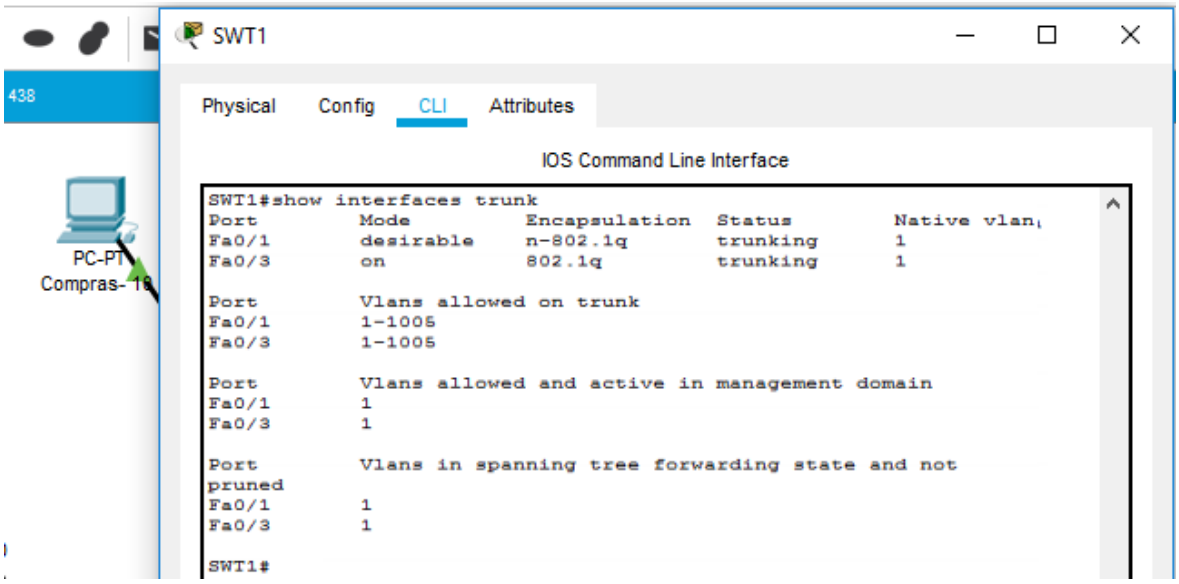
3.2.2.4 Entre SWT1 y SWT3 configuración en enlace "trunk"

Switch>enable / Se configura el ingreso a modo privilegiado
SWT3#configure terminal / Se configura el Ingreso a modo de configuración
SWT3(config)#interface range ethernet0/1
SWT3(config-if-range)#switchport trunk encapsulation dot1q / Habilitamos el trunk standar SWT3(config-if-range)#switchport mode trunk / Habilitamos el modo trunk en la int..
SWT3(config-if-range)#no shutdown / Activamos interfaz
SWT3(config-if-range)#exit
SWT3(config)#end
SWT3#wr

4. Verifique el enlace "trunk" el comando ***show interfaces trunk*** en SWT1.

3.2.2.5 Verifique el enlace "trunk"

Figura 20. Interface trunk en SWT1



5. Configuración de enlace "trunk" permanente entre SWT2 y SWT3.

3.2.2.6 Configuración de enlace "trunk" permanente entre SWT2 y SWT3

SWT2(config)#interface FastEthernet 0/3
SWT2(config-if)#switchport mode trunk
SWT2(config-if)#no shut

SWT3(config)#interface FastEthernet 0/3
SWT3(config-if)#switchport mode trunk
SWT3(config-if)#no shut

Figura 21. Enlace Trunk SWT2

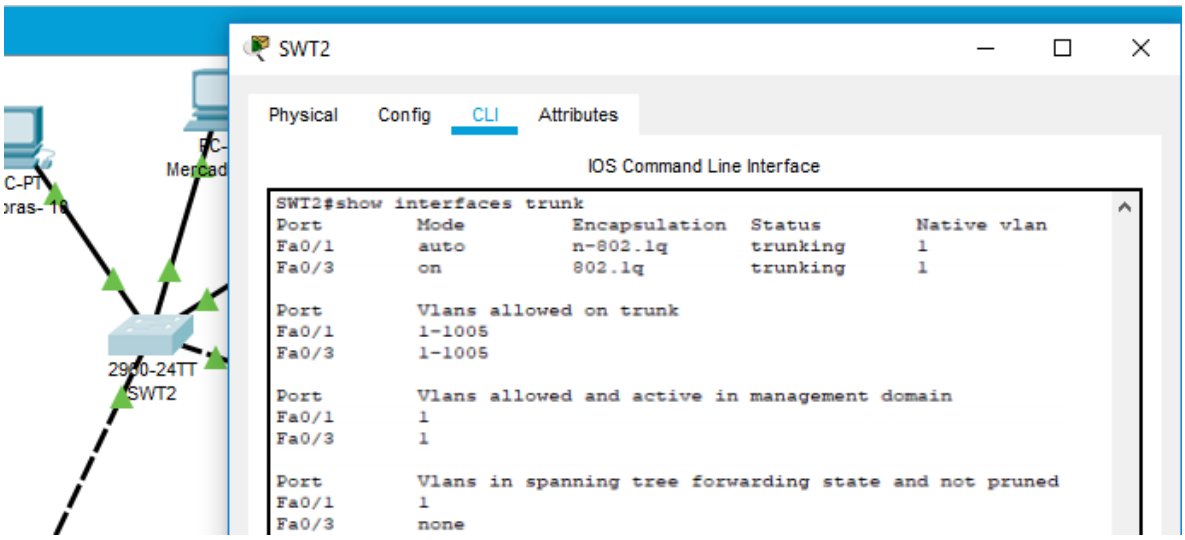
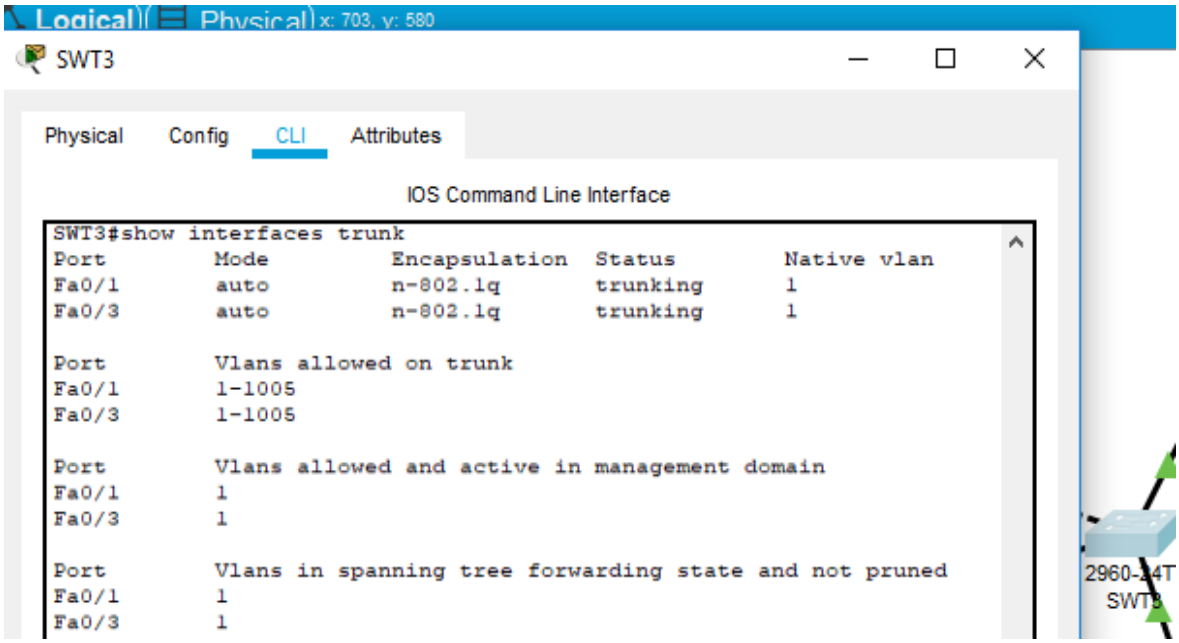


Figura 22. Enlace Trunk SWT3



3.2.3 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)

3.2.3.1 Configuración SWT1

```
SWT1>enable
SWT1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWT1(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
SWT1(config)#
```

3.2.3.2 Configuración SWT2

```
SWT2>enable
SWT2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWT2(config)#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
SWT2(config-vlan)#exit
SWT2(config)#
```

2. Verifique que las VLANs han sido agregadas correctamente.

3.2.3.3 Verificación que las VLANs

Figura 23. VLANs en SWT1

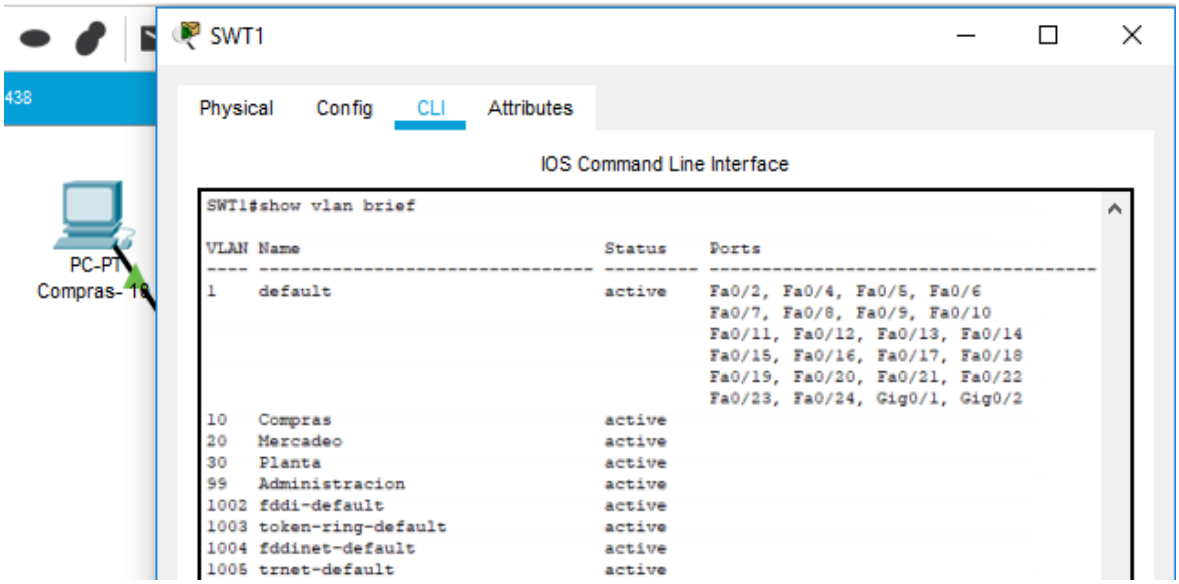
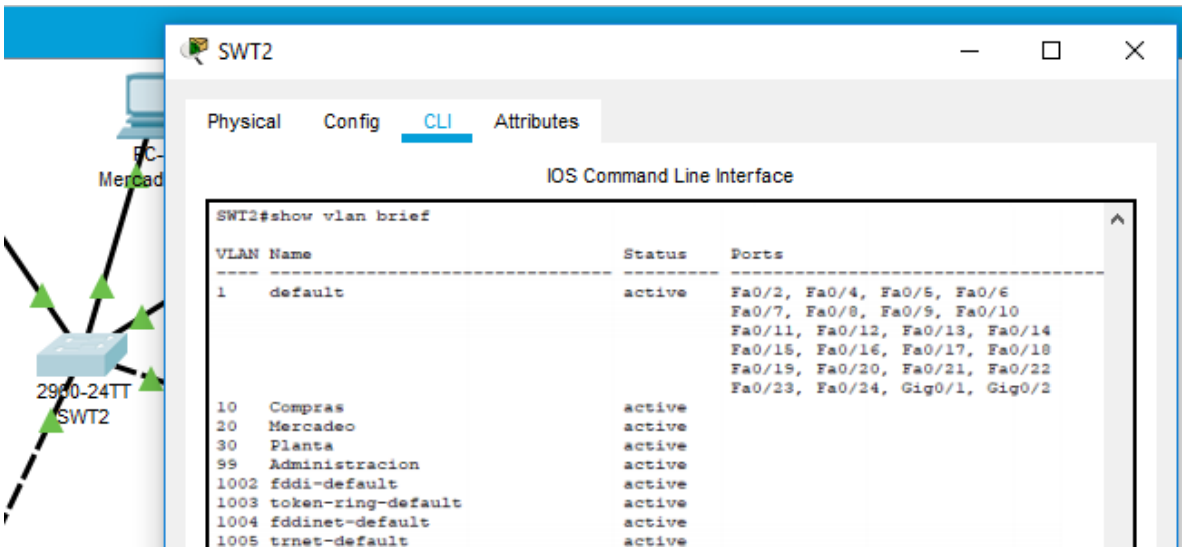


Figura 24. VLANs en SWT2



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

3.2.3.4 Configuración de direcciones IP con puertos VLAN

Tabla 2. Configuración 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

3.2.3.5 Configuramos Puertos VLAN SWT1

SWT1>enable
SWT1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWT1(config)#interface vlan 10
SWT1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
SWT1(config-if)#ip address 190.108.10.1 255.255.255.0 / Obtenemos las IP de cada PC
SWT1(config-if)#exit
SWT1(config)#interface vlan 20
SWT1(config-if)# %LINK-5-CHANGED: Interface Vlan20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
SWT1(config-if)#ip address 190.108.20.1 255.255.255.0 / Obtenemos las IP de cada PC
SWT1(config-if)#exit
SWT1(config)#interface vlan 30
SWT1(config-if)# %LINK-5-CHANGED: Interface Vlan30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up
SWT1(config-if)#ip address 190.108.30.1 255.255.255.0 / Obtenemos las IP de cada PC
SWT1(config-if)#exit

3.2.3.6 Configuramos Puertos VLAN SWT2

SWT2>enable
SWT2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWT2(config)#interface vlan 10
SWT2(config-if)#ip address 190.108.10.2 255.255.255.0 / Obtenemos las IP de cada PC

SWT2(config-if)#exit
SWT2(config)#interface vlan 20
SWT2(config-if)#ip address 190.108.20.2 255.255.255.0 / Obtenemos las IP de cada PC
SWT2(config-if)#exit
SWT2(config)#interface vlan 30
SWT2(config-if)#ip address 190.108.30.2 255.255.255.0 / Obtenemos las IP de cada PC
SWT2(config-if)#exit

3.2.3.7 Configuramos Puertos VLAN SWT3

SWT3>enable
SWT3#configure terminal Enter configuration commands, one per line. End with CNTL/Z. SWT3(config)#interface vlan 10
SWT3(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
SWT3(config-if)#ip address 190.108.10.3 255.255.255.0 / Obtenemos las IP de cada PC

SWT3(config-if)#exit
SWT3(config)#interface vlan 20
SWT3(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
SWT3(config-if)#ip address 190.108.20.3 255.255.255.0 / Obtenemos las IP de cada PC

SWT3(config-if)#exit
SWT3(config)#interface vlan 30
SWT3(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up
%LINEPROTO-5- UPDOWN: Line protocol on Interface Vlan30, changed state to up
SWT3(configif)#ip address 190.108.30.3 255.255.255.0 / Obtenemos las IP de cada PC
SWT3(config-if)#exit

Tabla 3. Direcciones IP de los PCs.

Swist	VLAN	Direcciones Ip de los PCs.
SWT1	VLAN10	190.108.10.1 / 24
SWT1	VLAN20	190.108.20.1 / 24
SWT1	VLAN30	190.108.30.1 / 24

SWT2	VLAN10	190.108.10.2 / 24
SWT2	VLAN20	190.108.20.2 / 24
SWT2	VLAN30	190.108.30.3 / 24
SWT3	VLAN10	190.108.10.3 / 24
SWT3	VLAN20	190.108.20.3 / 24
SWT3	VLAN30	190.108.30.3/ 24

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

3.2.3.8 Configuración del puerto F0/10 en modo de acceso para SWT1, SWT2 y SWT3 y asignación a la VLAN 10

SWT1

SWT1>enable
SWT1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWT1(config)#interface fa
SWT1(config)#interface fastEthernet 0/10
SWT1(config-if)#switchport mode access
SWT1(config-if)#switchport access vlan 10
SWT1(config-if)#exit
SWT1(config)#exit
SWT1#

SWT2:
SWT2(config)#interface fa
SWT2(config)#interface fastEthernet 0/10
SWT2(config-if)#switchport mode access
SWT2(config-if)#switchport access vlan 10
SWT2(config-if)#exit
SWT2(config)#
SWT2#

SWT3:
SWT3>enable
SWT3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWT3(config)#interface fa
SWT3(config)#interface fastEthernet 0/10
SWT3(config-if)#switchport mode access
SWT3(config-if)#switchport access vlan 10
SWT3(config-if)#exit

SWT3(config)#exit
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.

3.2.3.9 Procedimiento de los puertos F0/15 y F0/20 en SWT1, SWT2 y SWT3. Según la tabla 3.

SWT1:

```
SWT1>enable
SWT1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWT1(config)#interface fa
SWT1(config)#interface fastEthernet 0/15
SWT1(config-if)#switchport mode access
SWT1(config-if)#switchport access vlan 20
SWT1(config-if)#exit
SWT1(config)#interface fa
SWT1(config)#interface fastEthernet 0/20
SWT1(config-if)#switchport mode access
SWT1(config-if)#switchport access vlan 30
SWT1(config-if)#exit
SWT1(config)#exit
SWT1#
```

SWT2:

```
SWT2>enable
SWT2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWT2(config)#interface fa
SWT2(config)#interface fastEthernet 0/15
SWT2(config-if)#switchport mode access
SWT2(config-if)#switchport access vlan 20
SWT2(config-if)#no shut
SWT2(config-if)#exit
SWT2(config)#interface fa
SWT2(config)#interface fastEthernet 0/20
SWT2(config-if)#switchport mode access
SWT2(config-if)#switchport access vlan 30
SWT2(config-if)#end
SWT2#
```

SWT3:

```
 SWT3>enable
SWT3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWT3(config)#interface fa
SWT3(config)#interface fastEthernet 0/15
SWT3(config-if)#switchport mode access
SWT3(config-if)#switchport access vlan 20
SWT3(config-if)#exit
SWT3(config)#interface fa
SWT3(config)#interface fastEthernet 0/20
SWT3(config-if)#switchport mode access
SWT3(config-if)#switchport access vlan 30
SWT3(config-if)#exit
SWT3(config)#exit
SWT3#
```

3.2.4 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.

3.2.4.1 Asignación de direcciones IP al SVI a cada Switches según la tabla 4.

Tabla 4. Tabla de direccionamiento

Equipo	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

SWT1:

```
SWT1>enable
SWT1#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWT1(config)#interface vlan99
SWT1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
SWT1(config-if)#ip address 190.108.99.1 255.255.255.0
SWT1(config-if)#exit
SWT1(config)#

Figura 25. SWT1

```
interface Vlan99
 mac-address 0003.e443.bb01
 ip address 190.108.99.1 255.255.255.0
```

SWT2:
SWT2>enable
SWT2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWT2(config)#interface vlan 99
SWT2(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
SWT2(config-if)#ip address 190.108.99.2 255.255.255.0
SWT2(config-if)#exit

Figura 26. SWT2

```
interface Vlan99
 mac-address 00d0.9754.7601
 ip address 190.108.99.2 255.255.255.0
```

SWT3:
SWT3>enable
SWT3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWT3(config)#interface vlan 99
SWT3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
SWT3(config-if)#ip address 190.108.99.3 255.255.255.0
SWT3(config-if)#exit
SWT3(config)#end
SWT3#
Figura 27. SWT3

```
interface Vlan99
 mac-address 0004.9a84.7101
 ip address 190.108.99.3 255.255.255.0
```

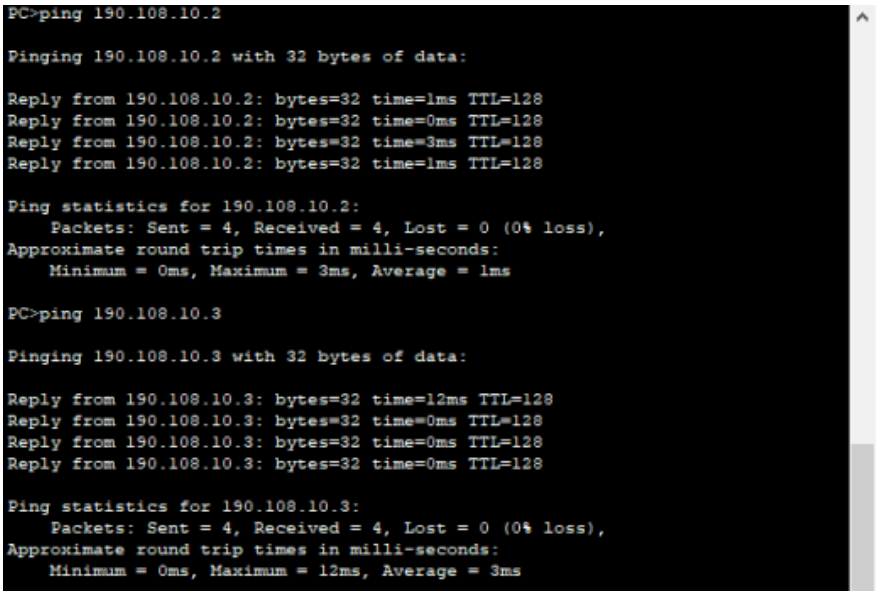
3.2.5 E. Verificar la conectividad Extremo a Extremo

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

3.2.5.1 Verificación de un Ping a cada PC

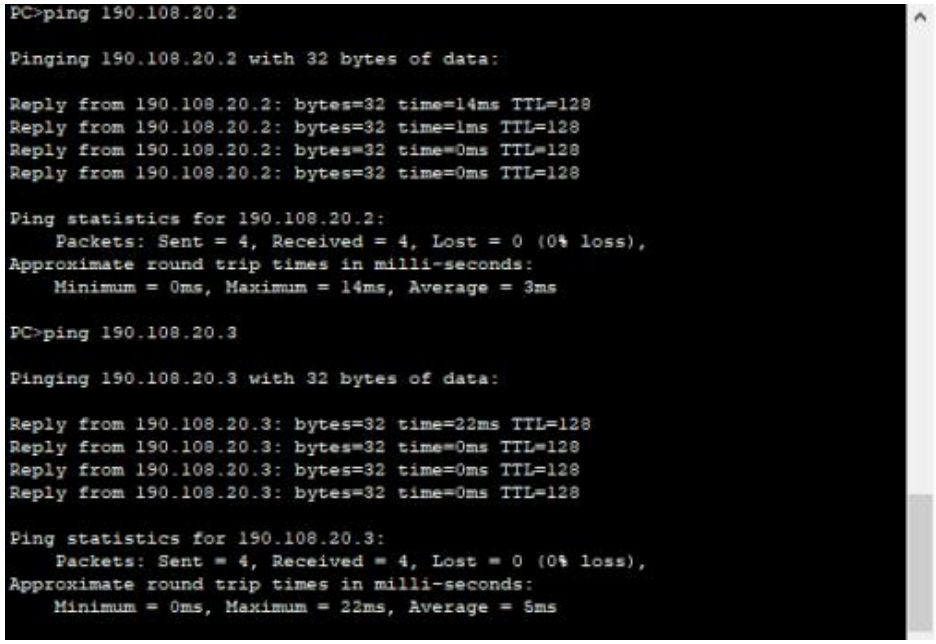
En SWT1 en el PC compras, en la realización de Ping a PCs Compras de SWT2 y SWT3 es exitoso

Figura 28. Comprobación exitosa de SWT1 Compras entre compras de SWT2 y SWT3



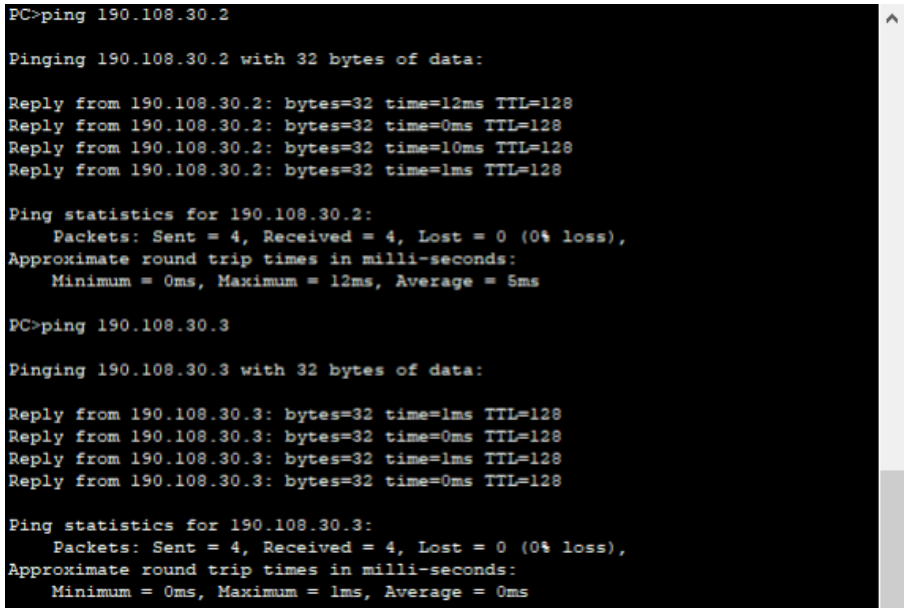
En SWT1 en el PC Mercadeo, en la realización de Ping a PCs Mercadeo de SWT2 y SWT3 es exitoso

Figura 29. Comprobación exitosa de SWT1 Mercadeo entre Mercadeo de SWT2 y SWT3



En SWT1 en el PC Planta, en la realización de Ping a PCs Planta de SWT2 y SWT3 es exitoso

Figura 30. Comprobación exitosa de SWT1 Planta entre Planta de SWT2 y SWT3



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

3.2.5.2 Verificación de cada Ping a cada Switch

Figura 31. Verificación SWT1

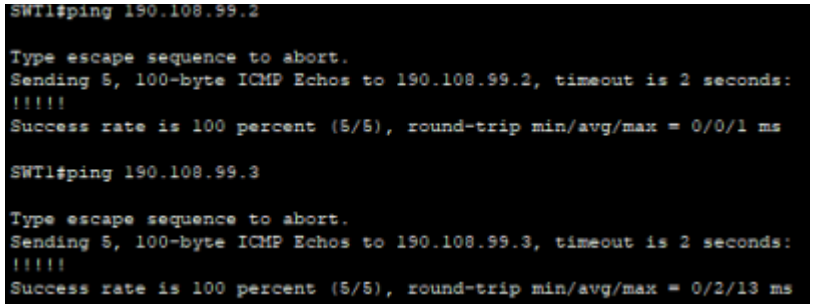


Figura 32. Verificación SWT2

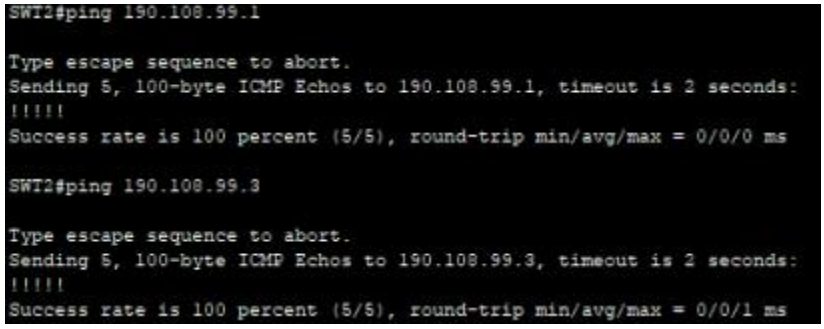
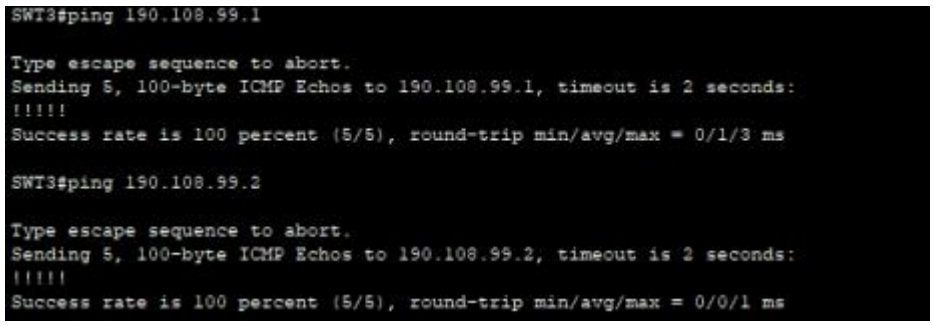


Figura 33. Verificación SWT3



Vemos que al generar Ping entre los Swist obtenemos respuesta por lo que la conexión es exitosa

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

3.2.5.3 Verificación de cada Ping a cada Switch a cada PC.

Figura 34. Verificación SWT1

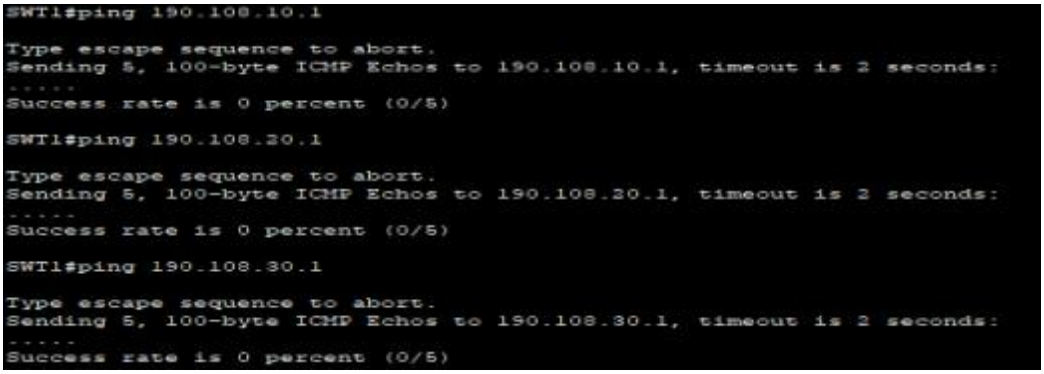


Figura 35. Verificación SWT2

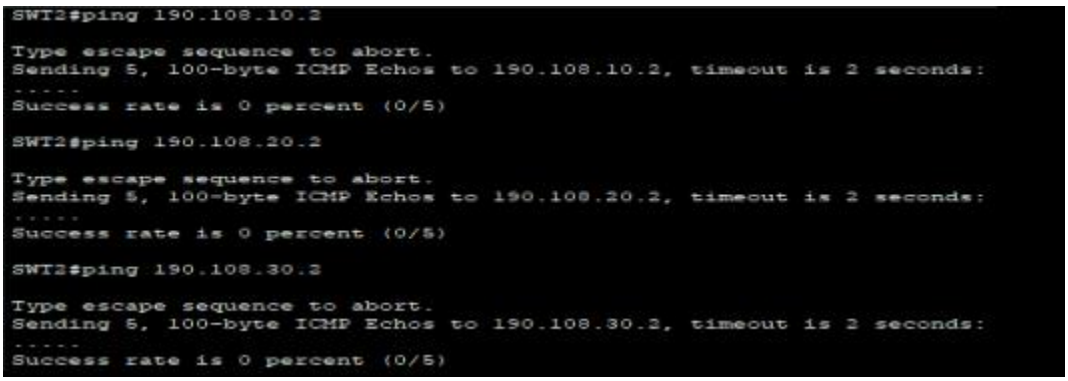
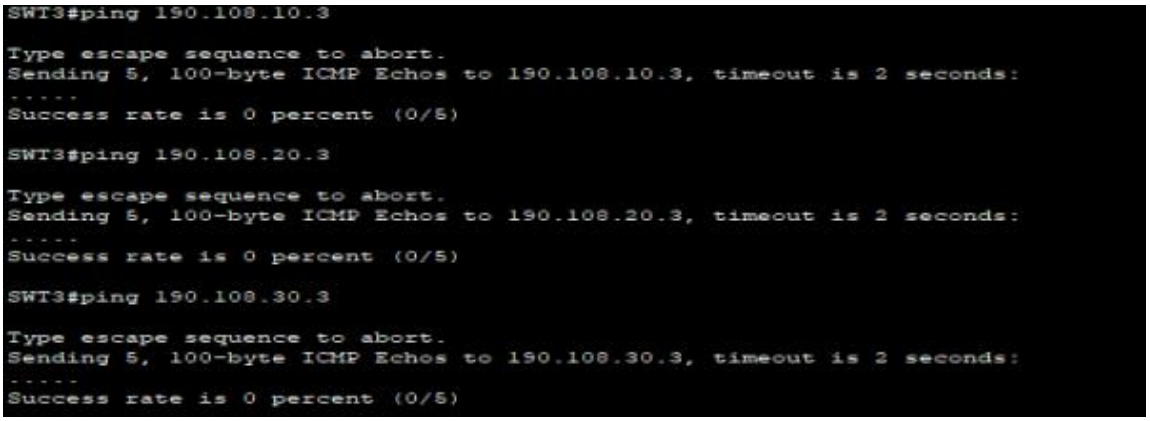


Figura 36. Verificación SWT3



Con los Ping de los Pc se nos ha presentado un inconveniente en la programación por lo cual no nos permite obtener una respuesta exitosa

CONCLUSIONES

En nuestro trabajo individual el cual hemos recopilado algunos de los conocimientos adquiridos en el curso de CCNP establecemos la funcionalidad de comandos detallados paso a paso generando cada una de las etapas durante de nuestra desarrollo del laboratorio practico, y en el cual hemos desarrollado tales como el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

Nuestro diplomado de CCNP nos permite adquirir el conocimiento necesario para el desarrollo de habilidades y competencias útiles en la configuración de redes y su diferentes dispositivos de red, en especial la adminitración de estos equipos tales como los switches y enrutadores lo cual son bases fundamentales para las redes.

En el desarrollo de nuestro escenario 3 donde utilizamos el funcionamiento de las VLANs las cuales son compuertas lógicas de dispositivos donde nos permite administrar los swichest implementamos los protocolos VTP para su importante administración de cada Swicht y llevar cada ip a su respectivo pc para octener un mayor beneficio en las redes tanto locales como de la nube.

Mediante el desarrollo del diplomado profundización CCNP, nos brinda los conocimientos prácticos y teóricos, CCNP Routing & Switching y su aplicabilidad con el plan de adquirir las capacidades necesarias para proyectar, implementar, asegurar, mantener y solucionar problemas de redes empresariales. Tan bien cabe destacar los programas asimilados durante nuestro trabajo de habilidades prácticas como lo son el GNS3 y el Packet Tracer los cuales son una gran herramienta para entender mejor las redes y sus protocolos de enrutamiento como su profundización más precisa para una mayor comprensión del vital funcionamiento de las redes en nuestro día a día.

REFERENCIAS BIBLIOGRÁFICAS

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

datos, C. (5 de mayo de 2010). https://sites.google.com. Obtenido de https://sites.google.com: https://sites.google.com/site/comdatosgrupo4/contenidos/cap4_conmutacionenrutamiento#TOC-PRINCIPIOS-DE-CONMUTACION-Y-ENRUTAMIENTO

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!AmIJYeiNT1IlnMfy2rhPZHwEoWx

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

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Introducción a la configuración de Switches y Routers. [OVA] Bogotá: UNAD, 2015. Recuperado de: https://1drv.ms/u/s!AmIJYei- NT1IhgL9QChD1m9EuGqC

trabajos, t. y. (5 de Noviembre de 2012). https://es.slideshare.net. Obtenido de https://es.slideshare.net: https://es.slideshare.net/TecnologiaTrabajos/enrutamientodinamico?next_slideshow=1