

PRUEBA DE HABILIDADES PRACTICAS CISCO CCNP

VLADIMIR ARROYO LOPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECTBI
INGENIERIA ELECTRONICA
MEDELLIN
2019

PRUEBA DE HABILIDADES PRACTICAS CISCO CCNP

VLADIMIR ARROYO LOPEZ

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

DIRECTOR:
MG. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECTBI
INGENIERIA ELECTRONICA
MEDELLIN
2019

Nota de Aceptación:

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Medellín, 5 de junio de 2019

AGRADECIMIENTOS

Gracias al tutor Gerardo Granados y toda la red de tutores de la universidad que nos ayudaron con esta fase de aprendizaje para alcanzar los objetivos y metas durante este largo proceso que culminamos con éxito.

Agradecerle a mi familia y especialmente a mi madre por ser de apoyo moral para sacar este proyecto de curso

CONTENIDO

	Pág.
LISTA DE TABLAS.....	6
LISTA DE FIGURAS.....	8
GLOSARIO.....	9
RESUMEN.....	14
INTRODUCCION.....	15
ESCENARIO 1.....	16
ESCENARIO 2.....	26
ESCENARIO 3.....	34
CONCLUSIONES.....	56
REFERENCIAS BIBLIOGRAFICAS.....	57

LISTA DE TABLAS

	Pág.
Tabla 1. Router R1.....	14
Tabla 2. Router R2.....	15
Tabla 3. Router R3.....	16
Tabla 4. Router R4.....	17
Tabla 5. Router R5.....	17
Tabla 6. Loopback R1.....	18
Tabla 7. Configuración R1.....	18
Tabla 8. Loopback R5.....	19
Tabla 9. Configuración R5.....	23 - 24
Tabla 10. Configuración De Los Routers R1-R5.....	25
Tabla 11. Configuración R1 a R5.....	26
Tabla 12. Vecino BGP Entre R1 y R2.....	27
Tabla 13. Vecino BGP Entre R2 y R3.....	33
Tabla 14. Vecino BGP R3.....	34
Tabla 15. Vecino BGP R4.....	34
Tabla 16. Configuración SWT1.....	37
Tabla 17. Configuración SWT2.....	37
Tabla 18. Configuración SWT1 y SWT3.....	39
Tabla 19. Enlace Troncal SWT1 y SWT3.....	40
Tabla 20 VLAN puerto configuración SWT1.....	41
Tabla 21 VLAN puerto configuración SWT2	41
Tabla 22. Configuración puertos VLAN SWT1.....	43
Tabla 23. Configuración puertos VLAN SWT2.....	43
Tabla 24. Configuración puertos VLAN SWT3.....	44
Tabla 25. Configure el puerto F0/10.....	44
Tabla 26. Configure el puerto F0/10 para SWT1.....	45
Tabla 27. Configure el puerto F0/10 para SWT2.....	45
Tabla 28. Configure el puerto F0/10 para SWT3.....	45

Tabla 29. Configuración Puerto F0/15 y F0/20 para SWT1.....	46
Tabla 30. Configuración Puerto F0/15 y F0/20 para SWT2.....	46
Tabla 31. Configuración Puerto F0/15 y F0/20 para SWT3.....	47
Tabla 32. Direccionamiento VLAN 99.....	47
Tabla 33. Direccionamiento VLAN 99 SWT1.....	47
Tabla 34. Direccionamiento VLAN 99 SWT2.....	48
Tabla 35. Direccionamiento VLAN 99 SWT3.....	48

LISTA DE FIGURAS

	Pág.
Figura 1. Descripción Escenario 1.....	13
Figura 2. Montaje escenario 1.....	13
Figura 3. Figura 3 Configuración Router #5.....	20
Figura 4. Resultado show Ip Route.....	20
Figura 5. Show Ip Route R1 y R 5.....	21
Figura 6. Configuración R5.....	22
Figura 7. Configuración en R5.....	22
Figura 8. Montaje escenario 2.....	23
Figura 9. Configuración routers lookback	24
Figura 10. Simulación y configuración	27
Figura 11. Simulación y configuración R1.....	28
Figura 12. Simulación y configuración R2.....	29
Figura 13. Configuración entre R3 y R2.....	30
Figura 14. Configuración entre R4 y R3.....	32
Figura 15. Descripción Escenario 3.....	32
Figura 16. Enlace "trunk" SWT1 comando <i>show interfaces trunk</i>	35
Figura 17. Enlace "trunk" SWT2 comando <i>show interfaces trunk</i>	35
Figura 18. Enlace "trunk" SWT3 comando <i>show interfaces trunk</i>	36
Figura 19. Enlace de trunk en STW1.....	38
Figura 20. Enlace de trunk en STW2.....	38
Figura 21. Verificación Interface trunk en SWT1.....	39
Figura 22. Enlace "trunk" permanente entre SWT2.....	40
Figura 23. Enlace "trunk" permanente entre SWT3.....	41
Figura 24. Configuración SWT2 VLANs en SWT1.....	42
Figura 25. Configuración SWT2 VLANs en SWT2.....	42
Figura 26 Conectividad SWT1 Ping a PCs Compras de SWT2 y SWT3.....	49

Figura 27 Conectividad SWT1 Ping a PCs Mercadeo de SWT2 y SWT3.....	49
Figura 28 Conectividad SWT1 Ping a PCs Planta de SWT2 y SWT3.....	50
Figura 29 Ping desde cada Switch (SWT1).....	50
Figura 30 Ping desde cada Switch (SWT2).....	51
Figura 31 Ping desde cada Switch (SWT3).....	51
Figura 32 Ping desde cada Switch (SWT1).....	51
Figura 33 Ping desde cada Switch (SWT2)	52
Figura 34 Ping desde cada Switch (SWT3).....	52

GLOSARIO

ADSL: línea de Suscripción Asimétrica Digital. Tecnología que mejora el ancho de banda de los hilos del cableado telefónico convencional que transporta hasta 16Mbps (megabits por segundo) gracias a una serie de métodos de compresión.

ASCII: american Standard Code for Information Interchange, es un estándar para el código utilizado por computadoras para representar todas las letras mayúsculas, minúsculas, letras latinas, números, signos de puntuación, etc.

BACKBONE: la parte de la red que transporta el tráfico más denso: conecta LANs, ya sea dentro de un edificio o a través de una ciudad o región.

BIT: dígito Binario. Unidad mínima de almacenamiento de la información cuyo valor puede ser 0 ó 1 (falso o verdadero respectivamente). Hay 8 bits en un byte.

BRIDGE: en redes de computadoras, un "bridge" (puente), conecta dos o más redes de área local (LAN) y WLAN entre sí.

CCNP: certificación intermedia de los diferentes cursos entregados por CISCO, tanto Enrutamiento (ROUTE) como en Conmutación (SWITCH)

CABLEADO: columna vertebral de una red la cual utiliza un medio físico de cable, casi siempre del tipo de red de área local (LAN), de forma que la información se transmite de un nodo a otro.

LAN: una red de área local, red local o LAN (del inglés local área network) es la interconexión de una o varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, con repetidores.

RESUMEN

El certificado me permitió profundizar y aprender todo lo relacionado con la introducción a las redes, gracias a su material multimedia y actividades prácticas, logre aprender a configurar e interconectar dispositivo y que logran comunicarse entre sí, el trabajo colaborativo me permitió aprender de mis compañeros y coordinar las actividades para obtener un buen resultado y aprender algo nuevo durante el proceso. Por otro lado, los exámenes pusieron a prueba lo investigado en los módulos del curso y encontrar las falencias que tenía en el momento para así mismo solucionarlas

ABSTRACT

The certified allowed me to deepen and learn everything related to the introduction to networks, thanks to its multimedia material and practical activities, I managed to learn how to configure and interconnect device and that they managed to communicate with each other, the collaborative works allowed me to learn from my colleagues and coordinate activities to obtain a good result and learn something new during the process. On the other hand, the exams put to the test what was investigated in the modules of the course and find the flaws that it had in the moment to solve them

INTRODUCCION

El presente trabajo da a conocer los resultados obtenidos tras el desarrollo del ejercicio planteado en el espacio indicado por el tutor, este tenía como objeto hacer que los estudiantes aplicaran los conocimientos adquiridos durante el semestre, logrando desarrollar paso a paso el ejercicio usando herramientas como Cisco Packet.

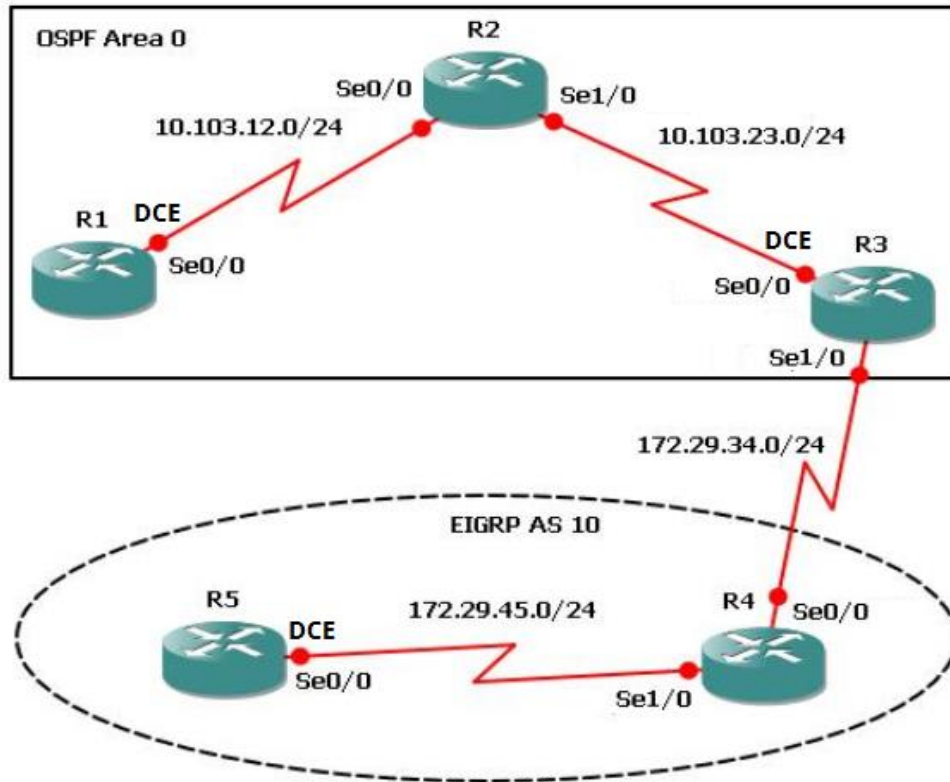
Se puede mostrar en nuestro entorno cotidiano la necesidad por las comunicaciones y la importancia de generar una mayor seguridad a nuestros datos como la facilidad de estos en cualquier lugar en que los requerimos, tanto en lo individual como en una entidad empresarial.

Vemos que se necesitan 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 obstáculos 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, etc.

En la actividad final de enrutamiento vamos a implementar o profundizar en los dispositivos de routers y Switch estos son equipos que tienen sus diferentes actividades, pero con un mismo fin de transmitir 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.

ESCENARIO 1

Figura 1. Descripción 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. Configure las interfaces con las direcciones que se muestran en la topología de red.

Tabla 1. Router R1

R1
Router> Tabla 1
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 área 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

Tabla 2. Router R2

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
```

Tabla 3. Router R3

R3
<pre> 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 </pre>

Tabla 4. Router R4

R4
<pre> 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 </pre>

Tabla 5. Router R5

R5
<pre> 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 </pre>

- 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.

Creamos cuatro interfaces Loopback en R1, en lo cual tenemos la máscara de subred 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.

Tabla 6. Loopback R1

Loopback11	10.1.0.1/22
Loopback12	10.1.4.1/22
Loopback13	10.1.8.1/22
Loopback14	10.1.12.1/22

Tabla 7. Configuración R1

ROUTER NUMBER 1 CONFIGURATION
<pre> 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 </pre>

Figura 2. Configuración R1

```

R1#sh ip ospf interface bri
Interface  PID  Area      IP Address/Mask  Cost  State Nbrs F/C
Lo12      1    0         10.1.12.1/22     1     LOOP  0/0
Lo8       1    0         10.1.8.1/22      1     LOOP  0/0
Lo4       1    0         10.1.4.1/22      1     LOOP  0/0
Lo0       1    0         10.1.0.1/22      1     LOOP  0/0
Se0/0    1    0         10.103.12.1/24   781   P2P   1/1
  
```

- 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.

Tabla 8. Loopback R5

Loopback51	172.5.0.1
Loopback52	172.5.4.1
Loopback53	172.5.8.1
Loopback54	172.5.12.1

Tabla 9. Configuración R5

```

ROUTER NUMBER 5 CONFIGURATION
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. Configuración Router #5

```

R5#sh ip interface bri | include up
Serial0/0      172.29.45.2      YES NVRAM up      up
Vlan1          unassigned       YES NVRAM up      down
Loopback0     172.5.0.1        YES manual up      up
Loopback4     172.5.4.1        YES manual up      up
Loopback8     172.5.8.1        YES manual up      up
Loopback12    172.5.12.1       YES manual up      up
  
```

- 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. Resultado show Ip Route

```

R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
O   10.1.0.0/22 [110/3125] via 10.103.23.1, 00:19:52, Serial1/1
O   10.103.12.0/24 [110/3124] via 10.103.23.1, 00:42:35, Serial1/1
C   10.103.23.0/24 is directly connected, Serial1/1
L   10.103.23.2/32 is directly connected, Serial1/1
172.5.0.0/22 is subnetted, 1 subnets
D   172.5.8.0 [90/41152000] via 172.29.34.2, 00:06:30, Serial1/2
C   172.29.0.0/16 is variably subnetted, 3 subnets, 2 masks
L   172.29.34.0/24 is directly connected, Serial1/2
L   172.29.34.1/32 is directly connected, Serial1/2
D   172.29.45.0/24 [90/41024000] via 172.29.34.2, 00:36:58, Serial1/2
  
```

- 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.

En este paso vamos a distribuir las rutas OSPF en EIGRP

R3 (config)#router eigrp 10 / Configuramos Protocolo eigrp

R3 (config)#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)#redistribuye 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*.

Ya encontramos configurados los comandos *show ip route*

Figura 5. Show Ip Route R1 y R5

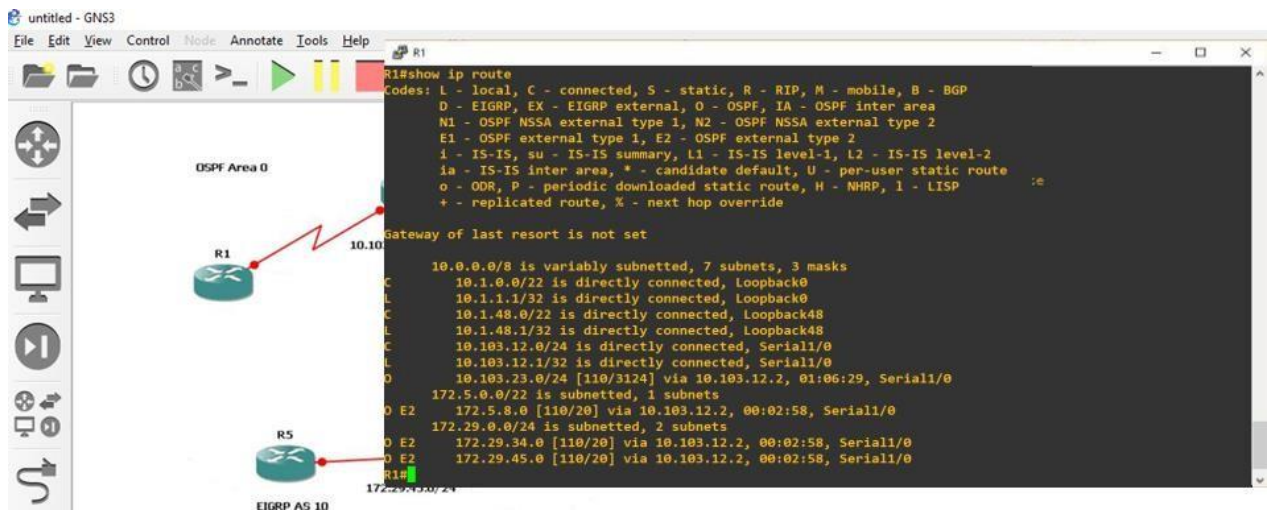


Figura 6. Configuración R5

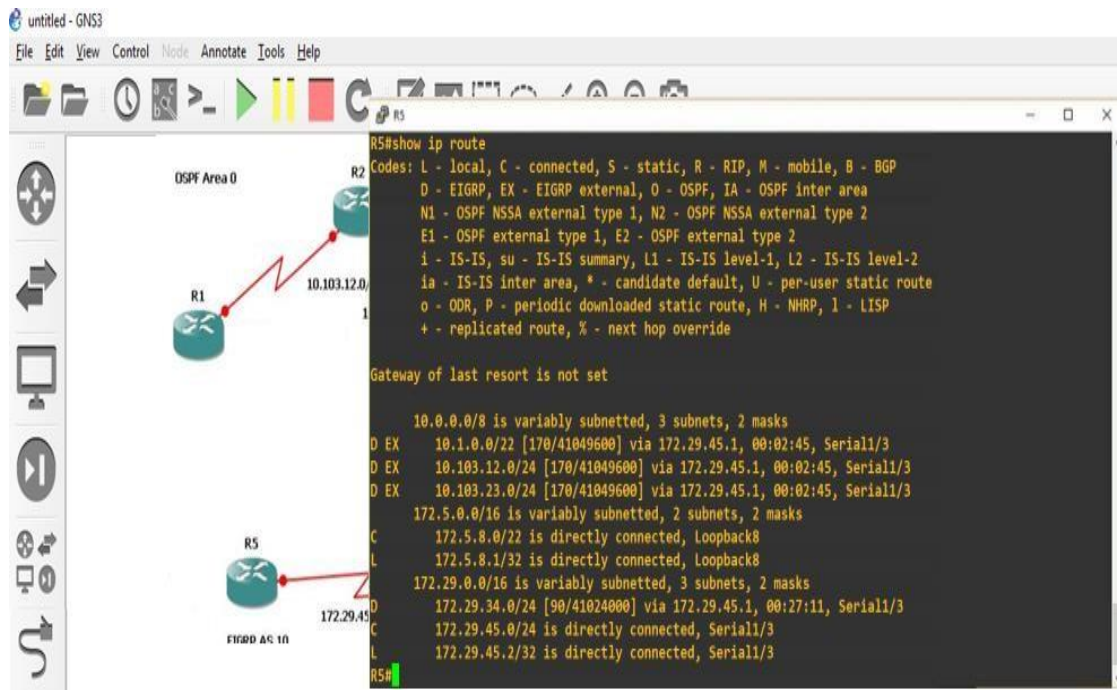
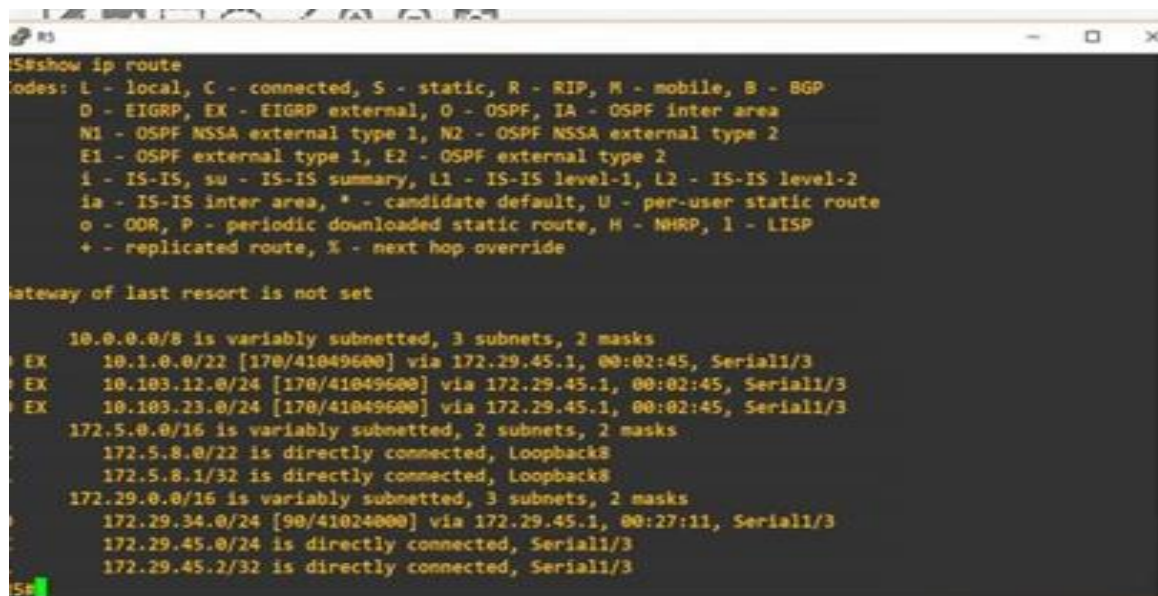


Figura 7. Configuración R5



ESCENARIO 2

Figura 8. Montaje escenario 2

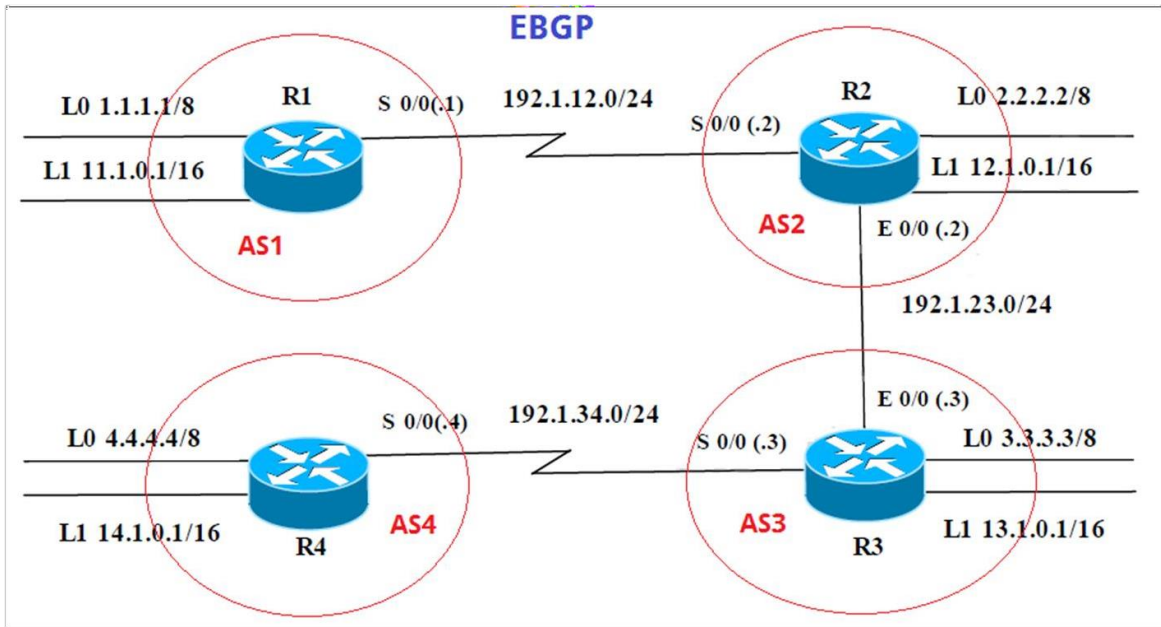


Tabla 10. Información para configuración de los Routers

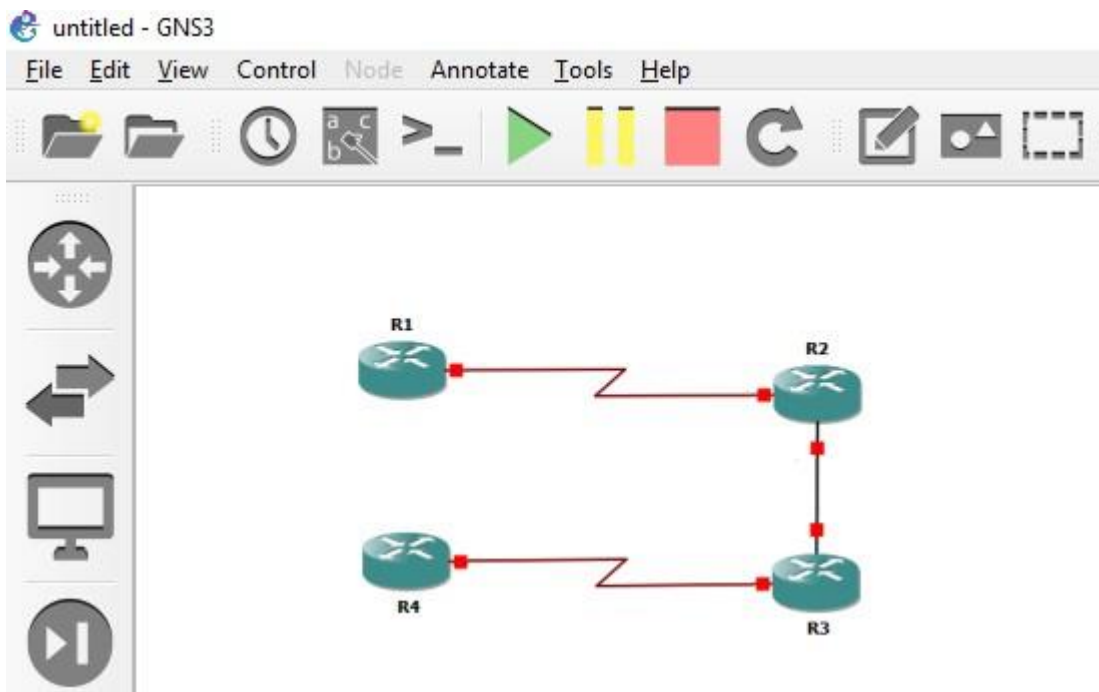
Interfaz	Dirección IP	Máscara
Loopback 0	1.1.1.1	255.0.0.0
Loopback 1	11.1.0.1	255.255.0.0
S 0/0	192.1.12.1	255.255.255.0

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

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
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

Figura 9. Configuración routers lookback



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**.

Tabla 11. Configuración R1 a R5

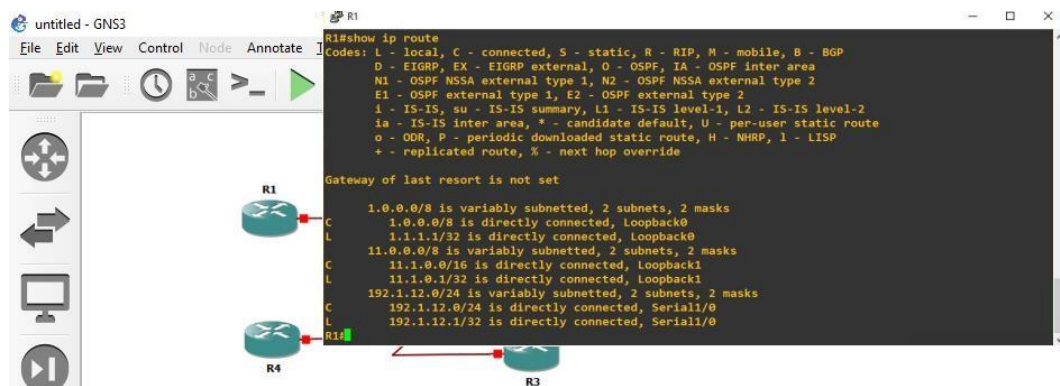
R1	<pre> Router> Router>enable / Se configura el ingreso a modo privilegiado Router#configure terminal / Se configura el Ingreso a modo de configuración Router(config)#hostname R1 / Se configura para asignar nombre al router R1(config)#interface Loopback0 / Configuramos y creamos la interfaz loopback 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)# </pre>
R2	<pre> 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 / Configuramos y creamos la interfaz Loopback0 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 </pre>

	<pre>R2(config-if)#exit R2(config)#</pre>
R3	<pre>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</pre>
R4	<pre>Router> Router>enable / Se configura el ingreso a modo privilegiado Router#configure terminal / Se configura el Ingreso a modo de Router(config)#hostnameR3 /Se configura para asignar nombre al router 4 (config)#interface Loopback0 / Configuramos y creamos la interfaz loopback 0 4 (config-if)#ip address 4.4.4.4 255.255.255.0/ Asignamos configuración IP 4 (config-if)#exit 4 (config)#interface Loopback1 / Configuramos y creamos la interfaz loopback 1 4 (config-if)#ip address 14.1.0.1 255.255.0.0 / Asignamos configuración IP 4 (config-if)#exit 4 (config)#interface serial 0/0 4 (config-if)#ip address 192.1.34.4 255.255.255.0 / Asignamos configuración IP 4 (config-if)#no shutdown/ Activamos interfaz 4 (config-if)#exit 4 (config)#</pre>

Tabla 12. Vecino BGP Entre R1 y R2

VECINO BGP ENTRE R1 y R2
<pre> 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)# </pre>

Figura 10. Simulación y configuración

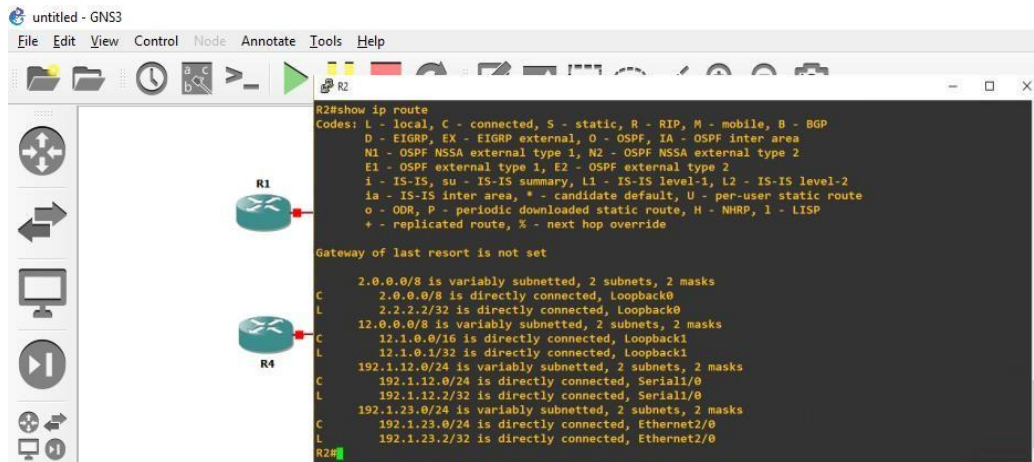


SIMULACIÓN Y CONFIGURACION DE R2

```

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

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**.

Realizamos la 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
```

Realizamos la 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 12. Simulación y configuración 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.

Realizamos la configuración entre R3 y R4

```
Router>enable R3#configure terminal
```

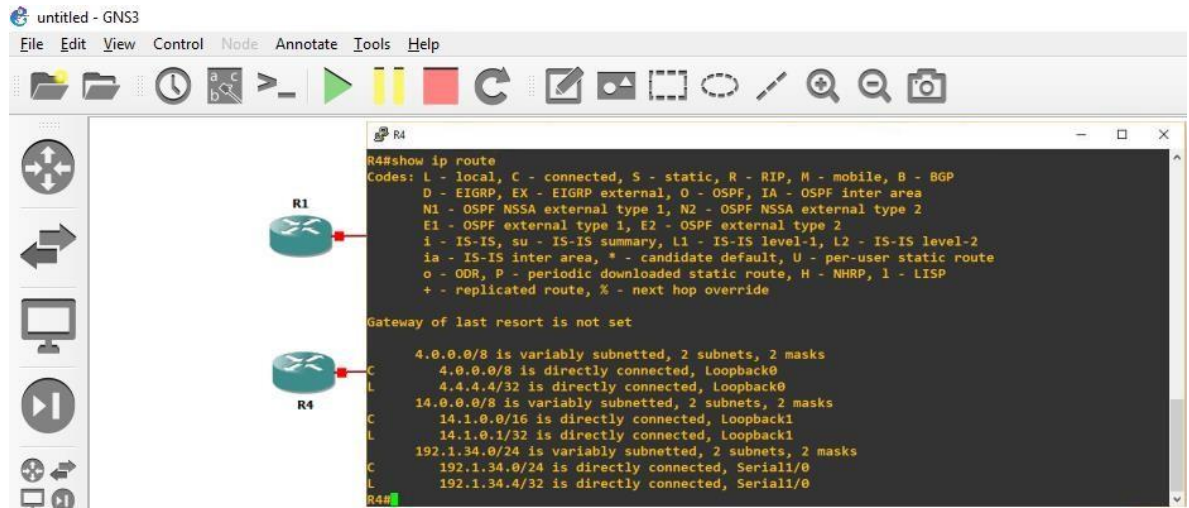
Enter configuration commands, one per line.
End with CNTL/Z. R3(config)#router bgp 3
R3(config-router)#neighbor 192.1.34.2 remote-as 4
R3(config-router)#network 4.4.4.4

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 13. Configuración entre R3 y R2



ESCENARIO 3

Figura 14. Configuración Entre R4 y R3

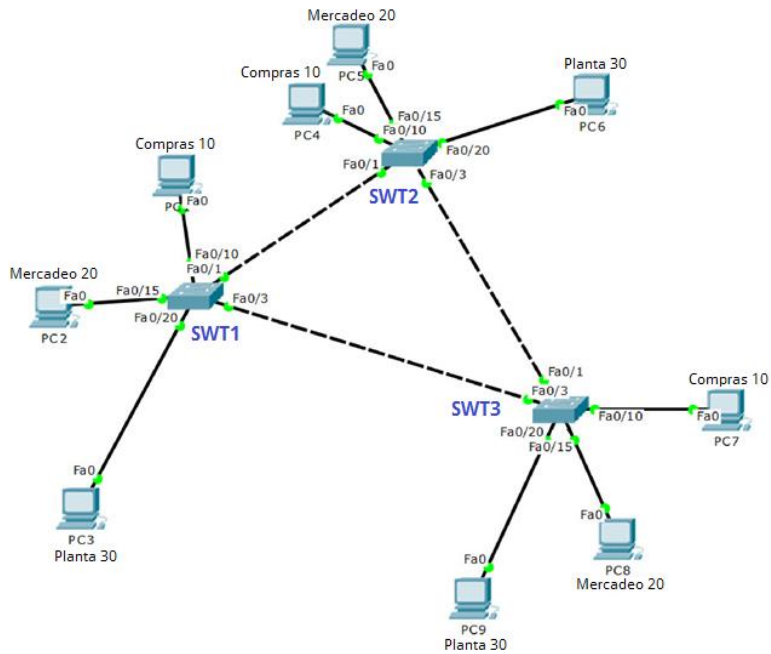
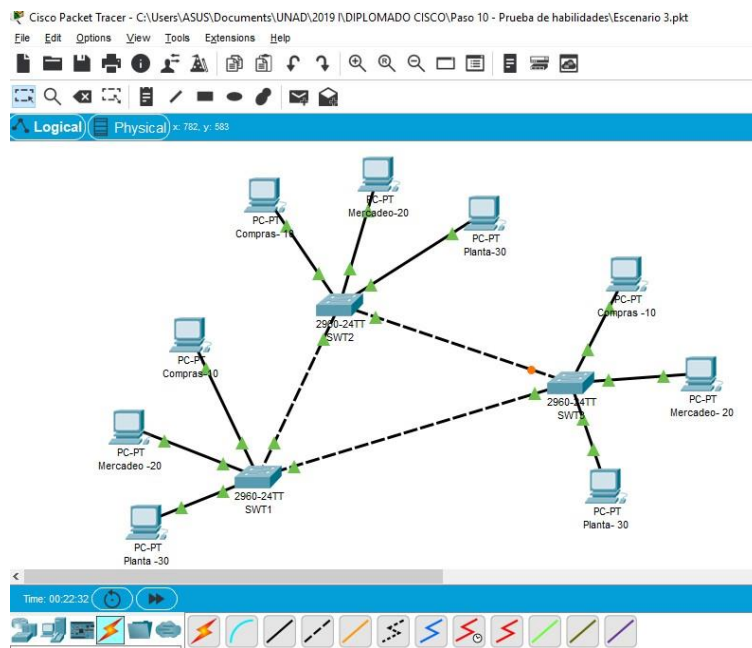


Figura 15. Descripción Escenario 3



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.

Tabla 13. Vecino BGP Entre R2 y R3

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)#

Tabla 14. Vecino BGP R3

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)#

Tabla 15. Vecino BGP R4

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 las configuraciones mediante el comando *show vtp status*.

Figura 16. Enlace "trunk" SWT1 comando **show interfaces trunk**

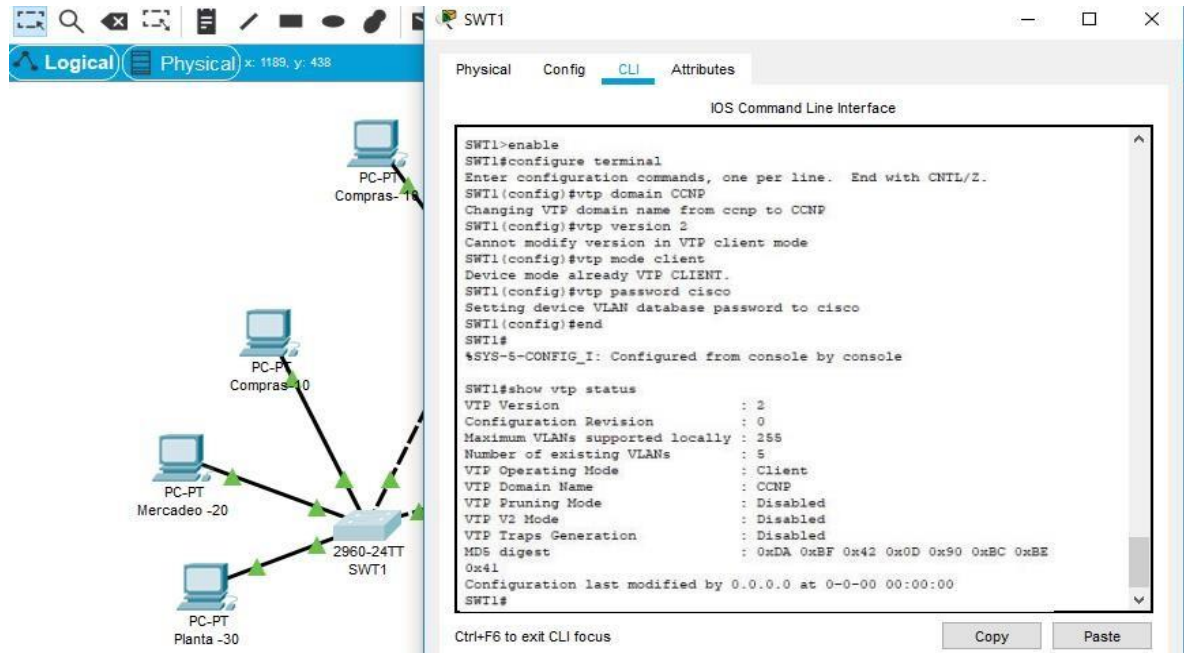


Figura 17. Enlace "trunk" SWT2 comando show interfaces trunk Switch SW2

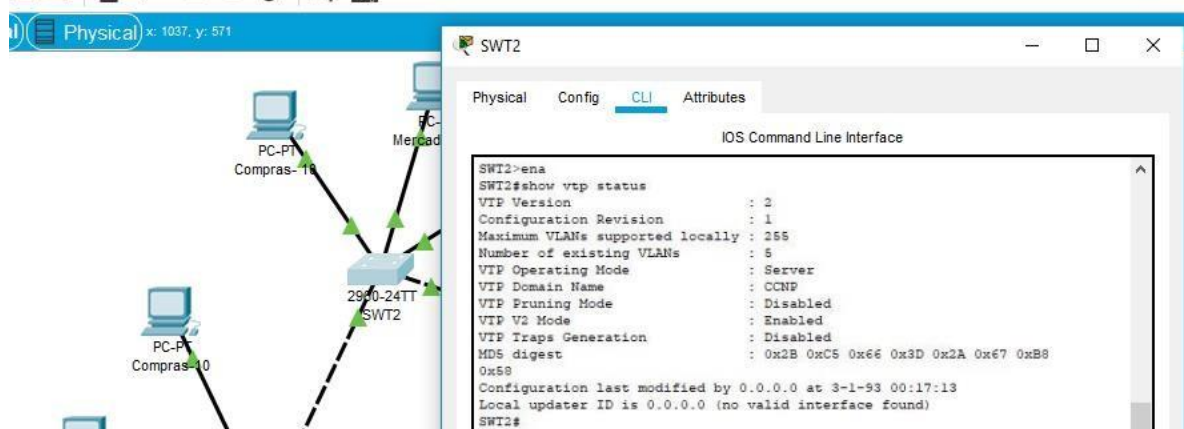


Figura 18 Enlace "trunk" SWT3 comando show interfaces trunk

The screenshot displays the configuration and status of a trunk link on switch SW3. The CLI window shows the following commands and output:

```
enable
SWT3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWT3(config)#vtp domain CCNP
Domain name already set to CCNP.
SWT3(config)#vtp version 2
Cannot modify version in VTP client mode
SWT3(config)#vtp mode client
Device mode already VTP CLIENT.
SWT3(config)#vtp password cisco
Password already set to cisco
SWT3(config)#end
SWT3#
%SYS-5-CONFIG_I: Configured from console by console

SWT3#show vtp status
VTP Version          : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode    : Client
VTP Domain Name       : CCNP
VTP Pruning Mode      : Disabled
VTP V2 Mode           : Disabled
VTP Traps Generation : Disabled
MD5 digest            : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE
0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SWT3#
```

The network diagram on the right shows a central switch labeled "2960-24TT SWT3" connected to three PCs: "PC-PT Compras -10", "PC-PT Mercadeo- 20", and "PC-PT Planta- 30".

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**.

Tabla 16. Configuración SWT1

Switch SWT1
<pre> 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 </pre>

Tabla 17. Configuración SWT2

Switch SWT2
<pre> 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 </pre>

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

Figura 19. Enlace Trunk entre SWT1

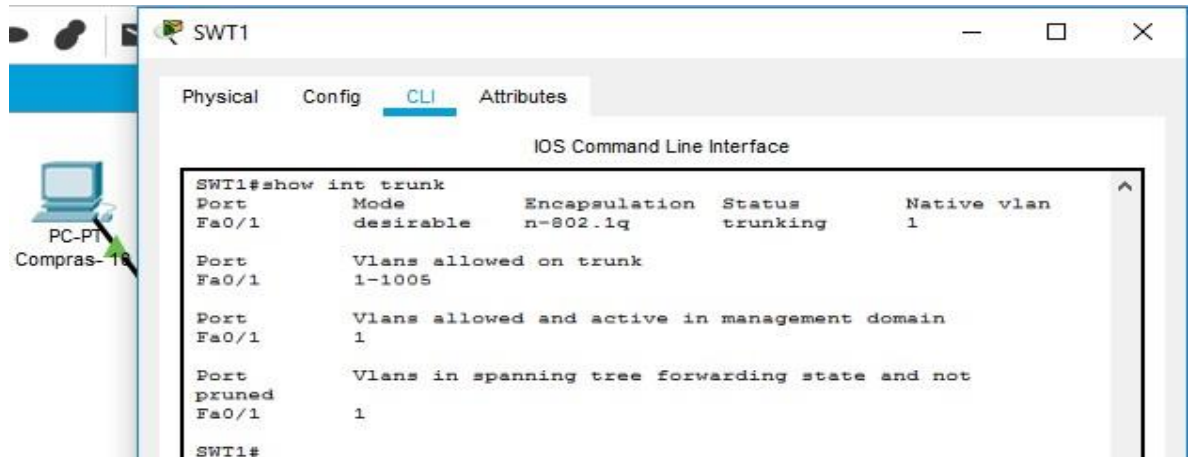
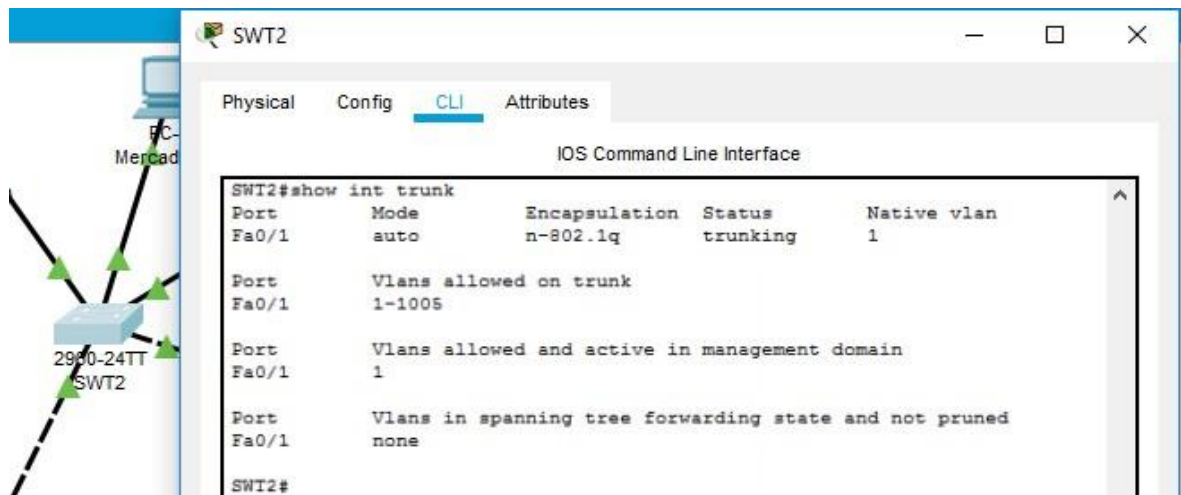


Figura 20. Enlace Trunk entre SWT2



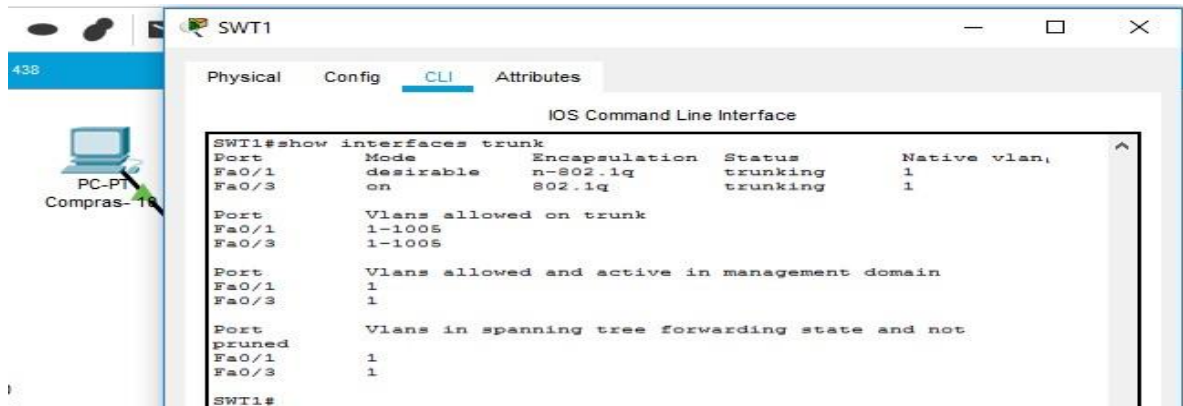
- Entre SWT1 y SWT3 configure un enlace "trunk" estático utilizando el comando *switchport mode trunk* en la interfaz F0/3 de SWT1

Tabla 18. Configuración SWT1 Y SWT3

ENTRE SWITCH 1 Y SWITCH 3
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 standard 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

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

Figura 21. Verificación Interface trunk en SWT1



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

Tabla 19. Enlace Troncal SWT1 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 22. Enlace Trunk SWT3

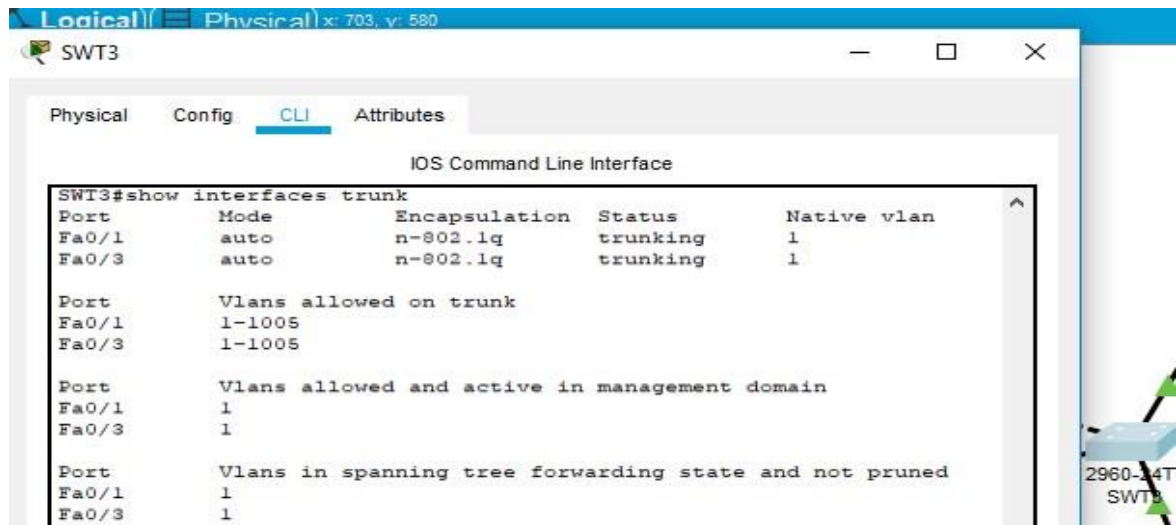
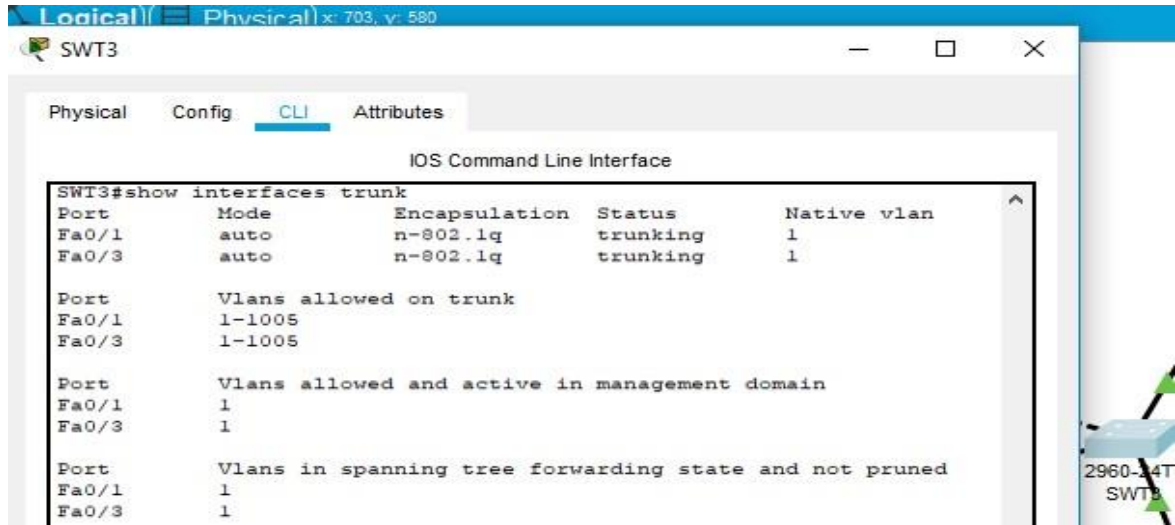


Figura 23. Enlace Trunk SWT3



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)

Tabla 20. VLAN puerto configuración SWT1

Configuración SWT1
<pre> 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)# </pre>

Tabla 21 VLAN puerto configuración SWT2

Configuración SWT2
<pre> 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 </pre>

2. Verifique que las VLANs han sido agregadas correctamente.

Figura 24. Configuración SW2 Vlan en SW1

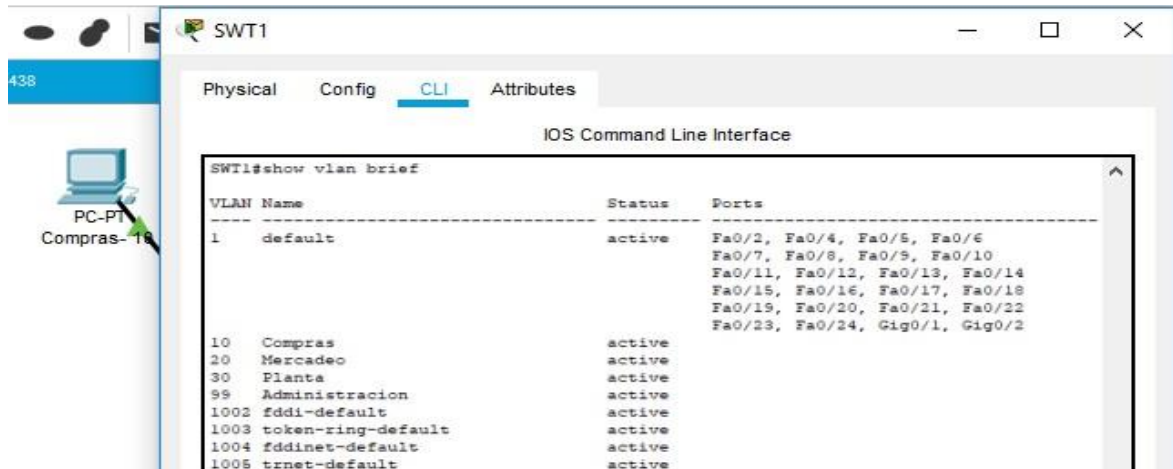
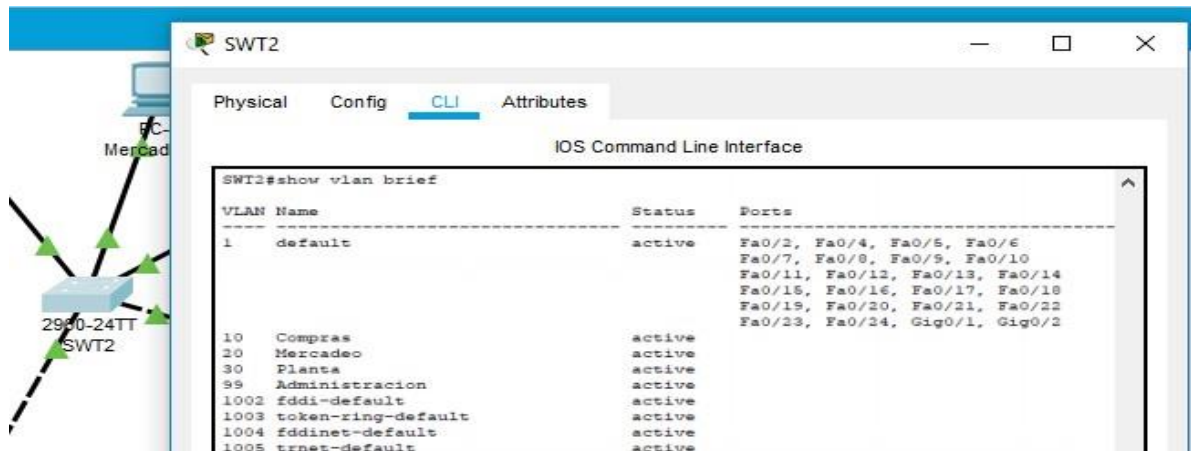


Figura 25. Configuración SW2 Vlan en SW2



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

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

X = número de cada PC particular

Tabla 22. Configuración puertos VLAN SWT1

Configuramos Puertos VLAN SWT1
<pre> 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 </pre>

Tabla 23. Configuración puertos VLAN SWT2

Configuramos Puertos VLAN SWT2
<pre> 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 </pre>

Tabla 24. Configuración puertos VLAN SWT3

CONFIGURAMOS PUERTOS VLAN SWT3	
<pre> 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(config-if)#ip address 190.108.30.3 255.255.255.0/Obtenemos las IP de cada PC SWT3(config-if)#exit </pre>	

Tabla 25. Configure el puerto F0/10

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.

Tabla 26. configuración Puerto F0/10 para SWT1

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#

Tabla 27. configuración Puerto F0/10 para SWT2

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#

Tabla 28. configuración Puerto F0/10 para SWT3

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.

Tabla 29. Configuración Puerto F0/15 y F0/20 para SWT1

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 (config-if)#exit SWT1(config)#exit SWT1#

Tabla 30. configuración Puerto F0/15 y F0/20 para SWT2

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#

Tabla 31. configuración Puerto F0/15 y F0/20 para SWT3

```

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#
    
```

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 32. Direccionamiento VLAN 99

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

Tabla 33. Direccionamiento VLAN 99 SWT1

```

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)#
```

Tabla 34. Direccionamiento VLAN 99 SWT2

```
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
```

Tabla 35. Direccionamiento VLAN 99 SWT3

```
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#
```


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.

Figura 26 Conectividad SWT1 Ping a PCs Compras de SWT2 y SWT3

```
PC>ping 190.108.10.2
Pinging 190.108.10.2 with 32 bytes of data:

Reply from 190.108.10.2: bytes=32 time=1ms TTL=128
Reply from 190.108.10.2: bytes=32 time=0ms TTL=128
Reply from 190.108.10.2: bytes=32 time=3ms TTL=128
Reply from 190.108.10.2: bytes=32 time=1ms TTL=128

Ping statistics for 190.108.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

PC>ping 190.108.10.3
Pinging 190.108.10.3 with 32 bytes of data:

Reply from 190.108.10.3: bytes=32 time=12ms TTL=128
Reply from 190.108.10.3: bytes=32 time=0ms TTL=128
Reply from 190.108.10.3: bytes=32 time=0ms TTL=128
Reply from 190.108.10.3: bytes=32 time=0ms TTL=128

Ping statistics for 190.108.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 3ms
```

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

Figura 27. Conectividad SWT1 Ping a PCs Mercadeo de SWT2 y SWT3

```
PC>ping 190.108.20.2
Pinging 190.108.20.2 with 32 bytes of data:

Reply from 190.108.20.2: bytes=32 time=14ms TTL=128
Reply from 190.108.20.2: bytes=32 time=1ms TTL=128
Reply from 190.108.20.2: bytes=32 time=0ms TTL=128
Reply from 190.108.20.2: bytes=32 time=0ms TTL=128

Ping statistics for 190.108.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 3ms

PC>ping 190.108.20.3
Pinging 190.108.20.3 with 32 bytes of data:

Reply from 190.108.20.3: bytes=32 time=22ms TTL=128
Reply from 190.108.20.3: bytes=32 time=0ms TTL=128
Reply from 190.108.20.3: bytes=32 time=0ms TTL=128
Reply from 190.108.20.3: bytes=32 time=0ms TTL=128

Ping statistics for 190.108.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 22ms, Average = 5ms
```

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

Figura 28. Conectividad SWT1 Ping a PCs Planta de SWT2 y SWT3

```
PC>ping 190.108.30.2
Pinging 190.108.30.2 with 32 bytes of data:

Reply from 190.108.30.2: bytes=32 time=12ms TTL=128
Reply from 190.108.30.2: bytes=32 time=0ms TTL=128
Reply from 190.108.30.2: bytes=32 time=10ms TTL=128
Reply from 190.108.30.2: bytes=32 time=1ms TTL=128

Ping statistics for 190.108.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 5ms

PC>ping 190.108.30.3
Pinging 190.108.30.3 with 32 bytes of data:

Reply from 190.108.30.3: bytes=32 time=1ms TTL=128
Reply from 190.108.30.3: bytes=32 time=0ms TTL=128
Reply from 190.108.30.3: bytes=32 time=1ms TTL=128
Reply from 190.108.30.3: bytes=32 time=0ms TTL=128

Ping statistics for 190.108.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

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

Figura 29. Ping desde cada Switch (SWT1)

```
SWT1#ping 190.108.99.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

SWT1#ping 190.108.99.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/13 ms
```

Figura 30. Ping desde cada Switch (SWT2)

```
SWT2#ping 190.108.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

SWT2#ping 190.108.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Figura 31. Ping desde cada Switch (SWT3)

```
SWT3#ping 190.108.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms

SWT3#ping 190.108.99.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

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.

Figura 32. Ping desde cada Switch (SWT1)

```
SWT1#ping 190.108.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SWT1#ping 190.108.20.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SWT1#ping 190.108.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Figura 33. Ping desde cada Switch (SWT2)

```
SWT2#ping 190.108.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SWT2#ping 190.108.20.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SWT2#ping 190.108.30.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Figura 34. Ping desde cada Switch (SWT3)

```
SWT3#ping 190.108.10.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SWT3#ping 190.108.20.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SWT3#ping 190.108.30.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

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

Ante todo, doy la gracias a este curso y al tutor por su diligencia y a la vez orientación, también a los creadores de la plataforma y permitirnros estas prácticas para desarrollarnos en la parte profesional.

Hacer que el profesional aplique los conocimientos y sobre adquiridos a lo largo del curso de Profundización Cisco todo relacionados con el protocolo de enrutamiento a los dispositivos de red, configurando una prioridad de routers, desactivando las actualizaciones de enrutamiento en las interfaces adecuadas y verificando la conectividad entre los dispositivos de la topología.

Adquirimos 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 nuestro 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.

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

REFERENCIAS BIBLIOGRAFICAS

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/site/comdatosgrupo4/contenidos/cap4_conmutacionenrutamiento# TOC-PRINCIPIOS-DE-CONMUTACION-Y-ENRUTAMIENTO](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/TecnologiaTrabajos/enrutamientodinamico?next_slideshow=1