

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

SEBASTIAN RESTREPO LÓPEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRÓNICA
BOGOTÁ
2019

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

SEBASTIAN RESTREPO LÓPEZ

Diplomado de profundización cisco CCNP
Prueba de habilidades prácticas

Gerardo Granados Acuña
Director

Efraín Alejandro Pérez
Tutor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRÓNICA
BOGOTÁ
2019

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 27 de julio de 2019

Dedicatoria

A Dios por la bendición de vida, sabiduría y fuerzas para culminar mis estudios, a mi familia quienes fueron mi mayor motivo de esfuerzo y lucha para superar todos los objetivos propuestos por el plan de estudio sin importar el grado de dificultad, ya que siempre estaba esa voz de aliento y palabras de superación para lograr esta nueva meta.

Agradecimiento

A mi gran compañero y ángel ingeniero Edwin López quien me guió para finalizar con gran éxito mi ingeniería y a todas esas personas (Erika, Leidy, Zulai, Oscar, Steven, Deyvis) que en algún momento pasaron por mi vida aportando ese granito de arena para dar grandes avances y lograr llegar a este nuevo logro.

Con gran aprecio a los tutores, directores y líderes de la UNAD quienes me entregaron todo su conocimiento, apoyo y dedicación para yo lograr esta nueva meta en mi campo profesional.

CONTENIDO

	pág.
INTRODUCCIÓN	11
ESCENARIO 1	12
ESCENARIO 2	18
ESCENARIO 3	24
CONCLUSIONES	35
BIBLIOGRÁFICA	36

LISTA DE TABLAS

	pág.
Tabla 1. Interfaces Loopback en R1.	14
Tabla 2. Interfaces Loopback en R5.	15
Tabla 3. Direcciones IP.	29
Tabla 4. Direcciones IP para VLAN 99.	31

LISTA DE FIGURAS

	pág.
Figura 1. Escenario 1.	12
Figura 2. Tabla de enrutamiento R3.	16
Figura 3. Tabla de enrutamiento R1.	17
Figura 4. Tabla de enrutamiento R5.	17
Figura 5. Escenario 2.	18
Figura 6. Información para configurar los Routers.	18
Figura 7. Show IP Route para R2.	21
Figura 8. Show ip Route para R3.	22
Figura 9. Show ip Router para R4.	23
Figura 10. Escenario 3.	24
Figura 11. Show VTP Status a SWT2.	25
Figura 12. Show VTP Status a SWT3.	26
Figura 13. Show interfaces a SWT.	27
Figura 14. Show interfaces a SWT2.	27
Figura 15. Show interfaces trunk SWT1.	28
Figura 16. Show VLAN SWT1.	29
Figura 17. Ping entre PC.	33
Figura 18. Ping entre Switchs.	34
Figura 19. Ping entre Switch a los PC.	34

GLOSARIO

BGP (*Protocolo Border Gateway*): es un protocolo de puerta de enlace exterior estandarizado diseñado para intercambiar información de enrutamiento y accesibilidad entre sistemas autónomos AS en Internet.

CISCO CERTIFIED NETWORK PROFESSIONAL: nivel intermedio de CNNP, para obtener esta certificación se debe superar varios exámenes, clasificados según la empresa en 3 módulos. Esta certificación, es la intermedia de las certificaciones generales de Cisco, no está tan valorada como el CCIE

EMULADOR: es un *hardware* o *software* que permite que un sistema informático llamado *host* se *coporte* como otro sistema informático llamado *guest*.

El emulador trata de modelar de forma precisa un dispositivo de manera que este funcione como si estuviese siendo usado en el aparato original.

GNS3: es un emulador de software de red que permite la combinación de dispositivos virtuales y reales, utilizados para simular redes complejas.

ROUTER: dispositivo de red que envía paquetes de datos entre redes de computadoras. Los enrutadores realizan las funciones de dirección de tráfico en Internet. Los datos enviados a través de Internet, como una página web o correo electrónico, se encuentran en forma de paquetes de datos.

SIMULADOR: solo trata de reproducir el comportamiento del programa.

VTP: transporta información de VLAN a todos los *switches* en su dominio.

RESUMEN

Las actividades concluidas para cada objetivo propuesto por el diplomado de profundización CCNP, se presentan de manera detallada en tres escenarios en los cuales se referencia el conocimiento y competencias adquiridas durante la ejecución de cada prueba realizada en el diplomado.

El primer escenario trata de las configuraciones iniciales y los protocolos de enrutamiento para *Routers*, en estas configuraciones se hace uso de las interfaces *Loopback*, del protocolo de red más corto para el direccionamiento de datos y el protocolo de enrutamiento del tipo vector distancia avanzado EIGRP.

En el segundo escenario se continúa con la configuración de *Routers* por medio del protocolo de puerta de enlace, en el que se intercambia información de enrutamiento probando la infraestructura de comunicación que se realiza en los *Routers*.

El tercer escenario está compuesto por la configuración de *switches*, esta configuración se hace por medio de la implementación de marcos de capa 2 para administrar la adición, eliminación y cambio de nombre de las VLAN con el modo VTP, se habilita los puertos de los *switches* por medio de DTP y como en este escenario se trata de *switches* en una red de área local, la cual se puede observar mediante la estructura y lógica de los componentes se crea las redes lógicas por medio de VLANs, en la que se define los tipos de nivel que son necesarios para la habilitación de los puertos.

Palabras Clave: CCNP, OSPF, EIGRP, VTP, DTP y VLANs.

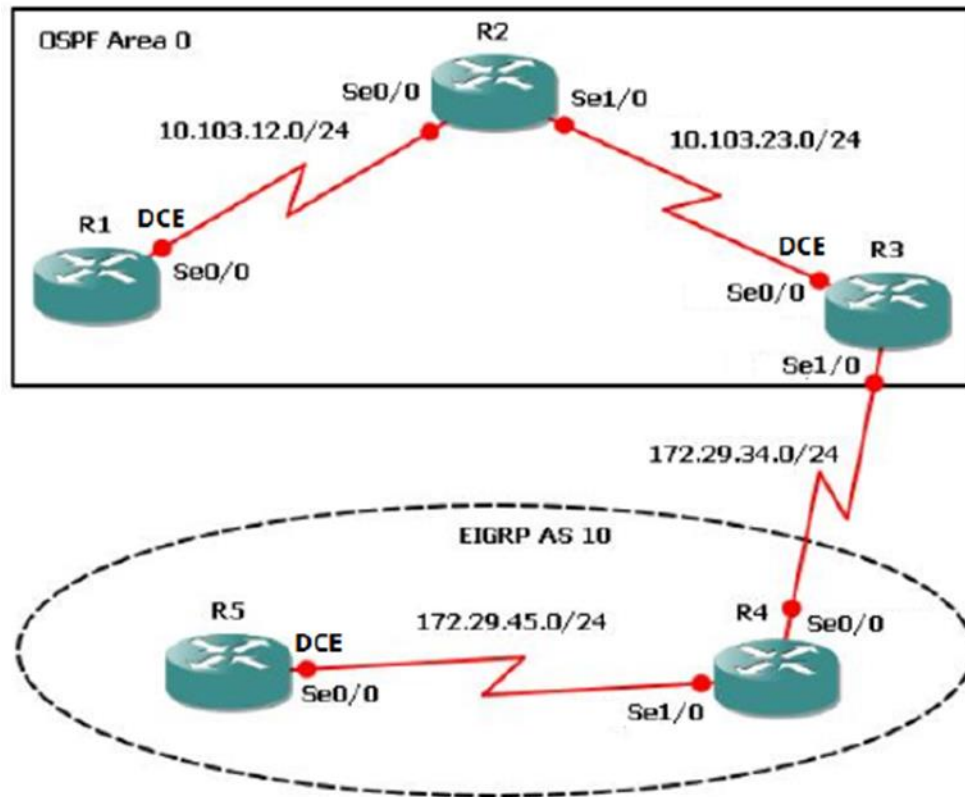
INTRODUCCIÓN

Las prácticas que contiene el actual trabajo comprende la importancia de la configuración de redes mediante Cisco, donde se implementa un conocimiento avanzado sobre redes y *networking* como requerimiento para la certificación de CCNA. Con los conocimientos adquiridos y certificaciones que nos otorga Cisco a través de la UNAD, obtenemos la competitividad de configurar e implementar redes con infraestructuras de gran tamaño y complejidad. También se cuenta con la capacidad de brindar soluciones de enrutamiento en redes LAN y WAN, bajo los protocolos de enlaces de un sistema a otro, contando con las características de compatibilidad de cada puerto y logrando un envío de datos forma segura y eficaz como lo requiere cada escenario en estas pruebas de habilidades.

En las configuraciones de los *Routers* y *switches* se implementan los protocolos de enrutamientos más importantes para redes de área local VLANs, complementándolos con algunos comandos como *ping*, *traceroute*, *show ip route*, que nos garantizan y facilita una conexión exitosa entre los componentes. Con estas configuraciones se tiene las herramientas básicas y técnicas tanto en protocolos de enrutamiento, seguridad y especificaciones técnicas para las conexiones de los diferentes equipos que conforman las redes de comunicaciones, soportado en los estándares de compatibilidad para él envío de datos que nos otorga Cisco.

ESCENARIO 1

Figura 1. Escenario 1.



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

CONFIGURACION R1

```
Router>en
Router#conf t
Router(config)#hostname R1
R1(config)#int s0/0/0
R1(config-if)#ip add 10.103.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#end
```

CONFIGURACION R2

```
Router>en
Router#conf t
Router(config)#hostname R2
R2(config)#int s 0/0/0
R2(config-if)#ip add 10.103.12.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#exit
R2(config)#int s 0/0/1
R2(config-if)#ip add 10.103.23.1 255.255.255.0
R2(config-if)#no sh
R2(config-if)#end
```

CONFIGURACION R3

```
Router>en
Router#conf t
Router(config)#hostname R3
R3(config)#int s 0/0/0
R3(config-if)#ip add 10.103.23.2 255.255.255.0
R3(config-if)#no sh
R3(config-if)#exit
R3(config)#int s 0/0/1
R3(config-if)#ip add 172.29.34.1 255.255.255.0
R3(config-if)#no sh
R3(config-if)#end
```

CONFIGURACION R4

```
Router>en
Router#conf t
Router(config)#hostname R4
R4(config)#int s 0/0/0
R4(config-if)#ip add 172.29.34.2 255.255.255.0
R4(config-if)#no sh
R4(config-if)#exit
R4(config)#int s 0/0/1
R4(config-if)#ip add 172.29.45.1 255.255.255.0
R4(config-if)#no sh
R4(config-if)#end
```

CONFIGURACION R5

```
Router>en
```

```

Router#conf t
Router(config)#hostname R5
R5(config)#int s 0/0/0
R5(config-if)#ip add 172.29.45.2 255.255.255.0
R5(config-if)#no sh
R5(config-if)#end

```

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.

Tabla 1. Interfaces Loopback en R1.

Cuatro Interfaces Loopback en R1	
Loopback1	10.1.0.1
Loopback2	10.1.1.1
Loopback3	10.1.2.1
Loopback4	10.1.3.1

CONFIGURACION EN R1

```

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

```

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

Tabla 2. Interfaces Loopback en R5.

Cuatro Interfaces Loopback	
Loopback1	172.5.0.1
Loopback2	172.5.1.1
Loopback3	172.5.2.1
Loopback4	172.5.3.1

CONFIGURACION EN R5

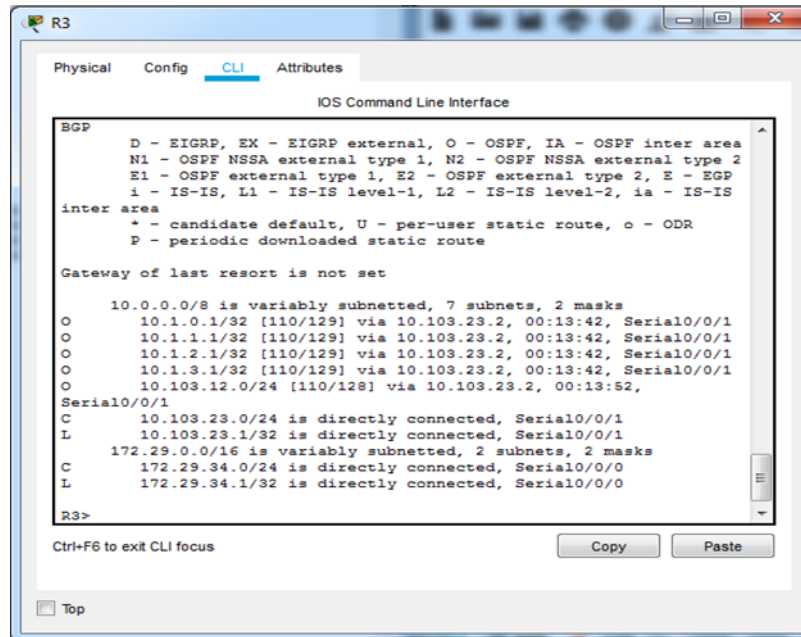
```

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

```

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 2. Tabla de enrutamiento R3.



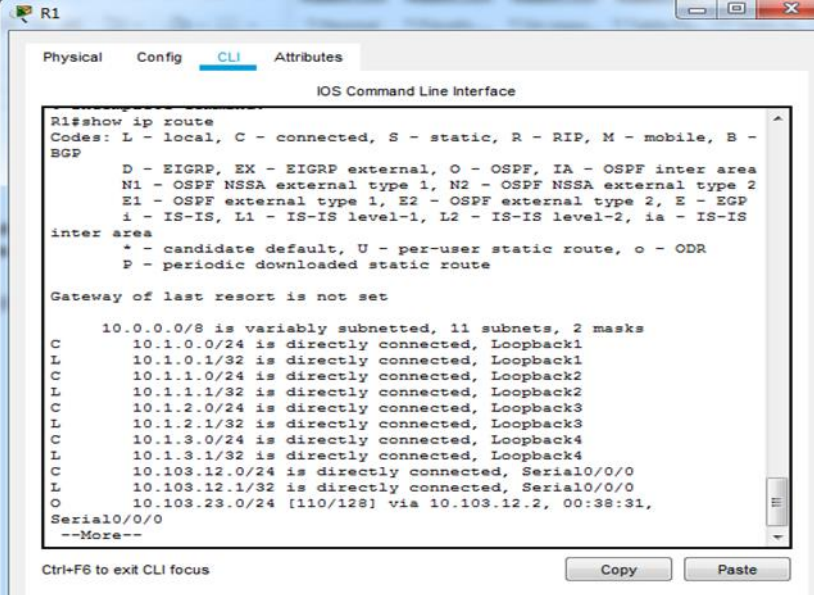
5. Configure R3 para redistribuir las rutas EIGRP en OSPF usando el costo de 50000 y luego redistribuya las rutas OSPF en EIGRP usando un ancho de banda T1 y 20,000 microsegundos de retardo.

```
R3(config)#router eigrp 10
R3(config-router)#redistribute ospf 1 metric 50000 100 255 1 500
R3(config)#router ospf 1
R3(config-router)#redistribute eigrp 10 metric 64 subnets
```

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**.

show ip route en R1

Figura 3. Tabla de enrutamiento R1.



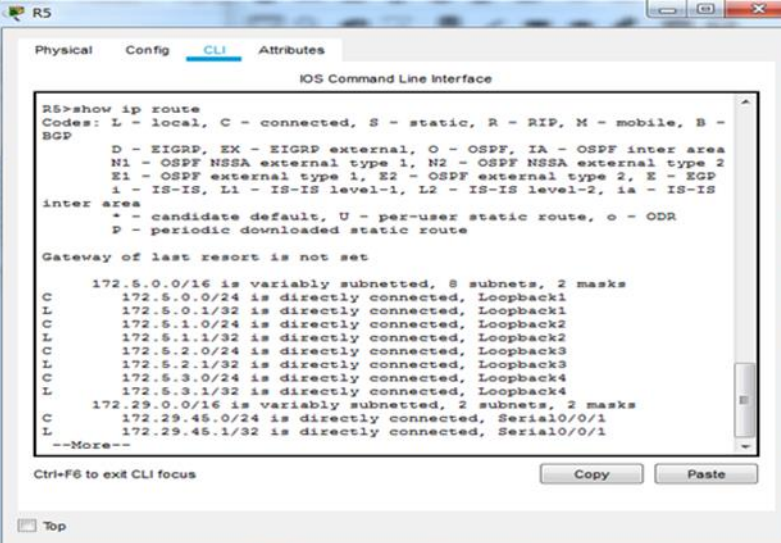
```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, 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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 11 subnets, 2 masks
C       10.1.0.0/24 is directly connected, Loopback1
L       10.1.0.1/32 is directly connected, Loopback1
C       10.1.1.0/24 is directly connected, Loopback2
L       10.1.1.1/32 is directly connected, Loopback2
C       10.1.2.0/24 is directly connected, Loopback3
L       10.1.2.1/32 is directly connected, Loopback3
C       10.1.3.0/24 is directly connected, Loopback4
L       10.1.3.1/32 is directly connected, Loopback4
C       10.103.12.0/24 is directly connected, Serial0/0/0
L       10.103.12.1/32 is directly connected, Serial0/0/0
O       10.103.23.0/24 [110/128] via 10.103.12.2, 00:38:31,
Serial0/0/0
--More--
```

show ip route en R5

Figura 4. Tabla de enrutamiento R5.



```
R5>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, E - EGP
       i - IS-IS, 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

Gateway of last resort is not set

     172.5.0.0/16 is variably subnetted, 8 subnets, 2 masks
C       172.5.0.0/24 is directly connected, Loopback1
L       172.5.0.1/32 is directly connected, Loopback1
C       172.5.1.0/24 is directly connected, Loopback2
L       172.5.1.1/32 is directly connected, Loopback2
C       172.5.2.0/24 is directly connected, Loopback3
L       172.5.2.1/32 is directly connected, Loopback3
C       172.5.3.0/24 is directly connected, Loopback4
L       172.5.3.1/32 is directly connected, Loopback4
C       172.29.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.29.45.0/24 is directly connected, Serial0/0/1
L       172.29.45.1/32 is directly connected, Serial0/0/1
--More--
```

ESCENARIO 2

Figura 5. Escenario 2.

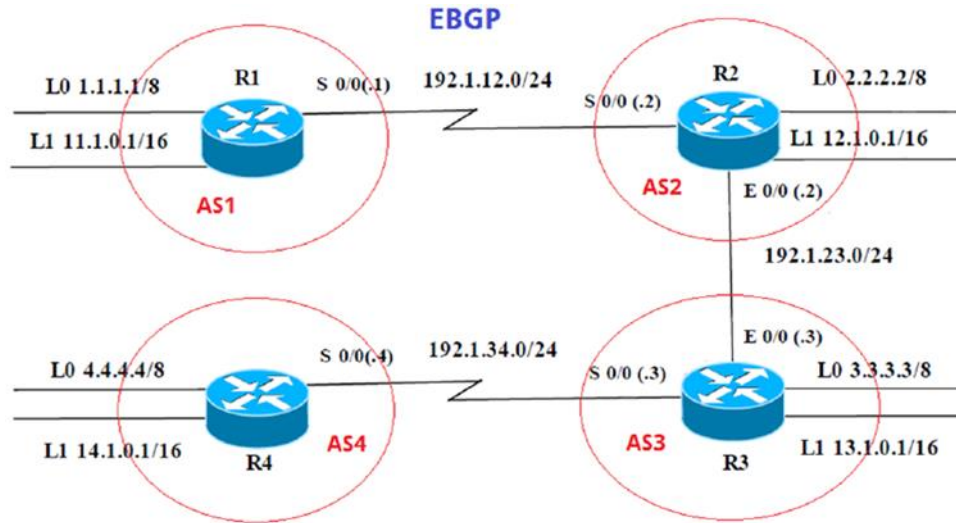


Figura 6. Información para configurar los Routers.

	Interfaz	Dirección IP	Máscara
R1	Loopback 0	1.1.1.1	255.0.0.0
	Loopback 1	11.1.0.1	255.255.0.0
	S 0/0	192.1.12.1	255.255.255.0
R2	Loopback 0	2.2.2.2	255.0.0.0
	Loopback 1	12.1.0.1	255.255.0.0
	S 0/0	192.1.12.2	255.255.255.0
	E 0/0	192.1.23.2	255.255.255.0
R3	Loopback 0	3.3.3.3	255.0.0.0
	Loopback 1	13.1.0.1	255.255.0.0
	E 0/0	192.1.23.3	255.255.255.0
	S 0/0	192.1.34.3	255.255.255.0
R4	Loopback 0	4.4.4.4	255.0.0.0
	Loopback 1	14.1.0.1	255.255.0.0
	S 0/0	192.1.34.4	255.255.255.0

Configuraciones iniciales:

EN R1

```
Router>en
Router#conf t
Router(config)#hostname R1
R1(config)#int s0/0/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#int loopback0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config)#int loopback1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#exit
```

EN R2

```
Router>en
Router#conf t
Router(config)#hostname R2
R2(config)#int loopback0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config)#int loopback1
R2(config-if)#ip add 12.1.0.1 255.255.0.0
R2(config-if)#exit
R2(config)#int s0/0/0
R2(config-if)#ip add 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#int G0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
```

EN R3

```
Router>en
Router#conf t
Router(config)#hostname R3
R3(config)#int loopback0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
```

```
R3(config)#int loopback1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#exit
R3(config)#int g0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#exit
R3(config)#int s0/0/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
```

EN R4

```
Router>en
Router#conf t
Router(config)#hostname R4
R4(config)#int loopback0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config)#int loopback1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#exit
R4(config)#int s0/0/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#clock rate 64000
R4(config-if)#no shutdown
R4(config-if)#exit
```

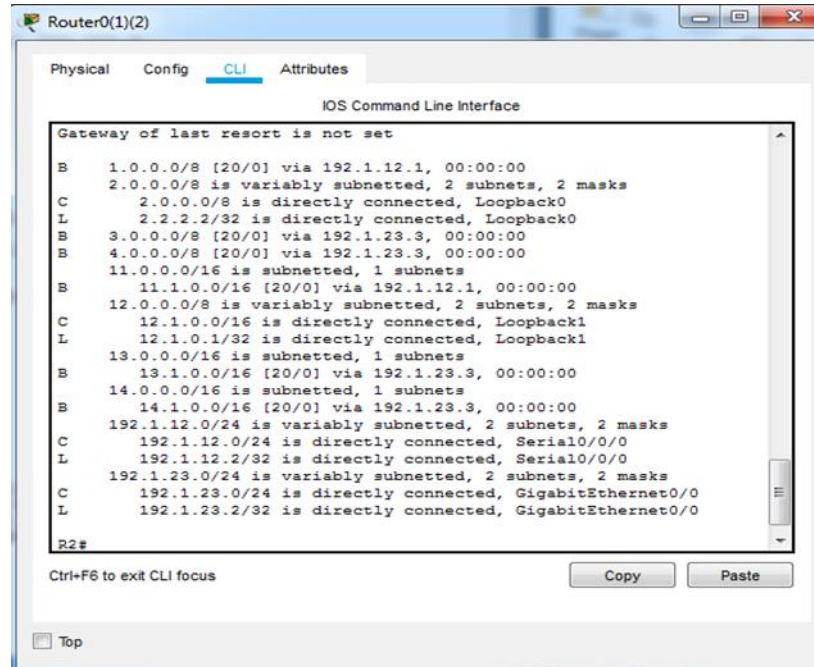
1. Configure una relación de vecino BGP entre R1 y R2. R1 debe estar en **AS1** y R2 debe estar en **AS2**. Anuncie las direcciones de *Loopback* en BGP. Codifique los ID para los *routers* BGP como 11.11.11.11 para R1 y como 22.22.22.22 para R2. Presente el paso a con los comandos utilizados y la salida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

EN R2

```
R2>en
R2#conf t
R2(config)#router bgp 2
R2(config-router)#no synchronization
R2(config-router)#bgp router-id 22.22.22.22
R2(config-router)#bgp log-neighbor-changes
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 2.0.0.0 mask 255.0.0.0
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
```

Figura 7. Show IP Route para 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**.

R1

```
R1>en
```

```
R1#conf t
```

```
R1(config)#router bgp 1
```

```
R1(config-router)#no synchronization
```

```
R1(config-router)#bgp router-id 11.11.11.11
```

```
R1(config-router)#bgp log-neighbor-changes
```

```
R1(config-router)#neighbor 192.1.12.2 remote-as 2
```

```
R1(config-router)#network 1.0.0.0 mask 255.0.0.0
```

```
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
```

R3

```
R3>en
```

```
R3#conf t
```

```
R3(config)#router bgp 3
```

```
R3(config-router)#bgp router-id 33.33.33.33
```

```
R3(config-router)#bgp log-neighbor-changes
```

```
R3(config-router)#no synchronization
```

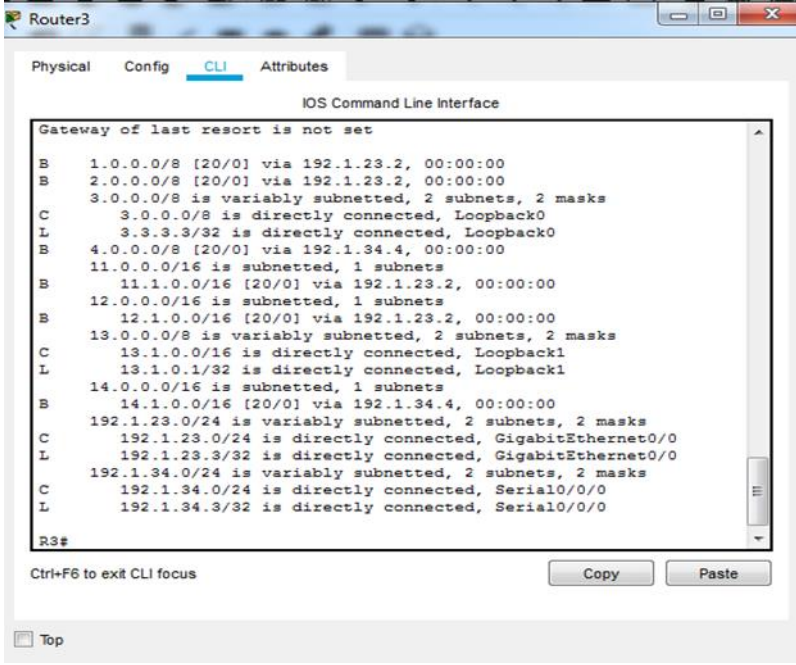
```
R3(config-router)#neighbor 192.1.23.2 remote-as 2
```

```
R3(config-router)#neighbor 192.1.34.4 remote-as 4
```

```
R3(config-router)#network 3.0.0.0 mask 255.0.0.0
```

```
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
```

Figura 8. Show ip Route para R3.



```
Router3
Physical Config CLI Attributes
IOS Command Line Interface
Gateway of last resort is not set
B 1.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
B 2.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 3.0.0.0/8 is directly connected, Loopback0
L 3.3.3.3/32 is directly connected, Loopback0
B 4.0.0.0/8 [20/0] via 192.1.34.4, 00:00:00
11.0.0.0/16 is subnetted, 1 subnets
B 11.1.0.0/16 [20/0] via 192.1.23.2, 00:00:00
12.0.0.0/16 is subnetted, 1 subnets
B 12.1.0.0/16 [20/0] via 192.1.23.2, 00:00:00
13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 13.1.0.0/16 is directly connected, Loopback1
L 13.1.0.1/32 is directly connected, Loopback1
14.0.0.0/16 is subnetted, 1 subnets
B 14.1.0.0/16 [20/0] via 192.1.34.4, 00:00:00
192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.1.23.0/24 is directly connected, GigabitEthernet0/0
L 192.1.23.3/32 is directly connected, GigabitEthernet0/0
192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.1.34.0/24 is directly connected, Serial10/0/0
L 192.1.34.3/32 is directly connected, Serial10/0/0
R3#
Ctrl+F6 to exit CLI focus Copy Paste
Top
```

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**.

EN R3

```
R3(config)#router bgp 3
```

```
R3(config-router)#neighbor 192.1.34.4 remote-as 4
```

EN R4

```
R4(config)#router bgp 4
```

```
R4(config-router)#bgp router-id 44.44.44.44
```

```
R4(config-router)#bgp log-neighbor-changes
```

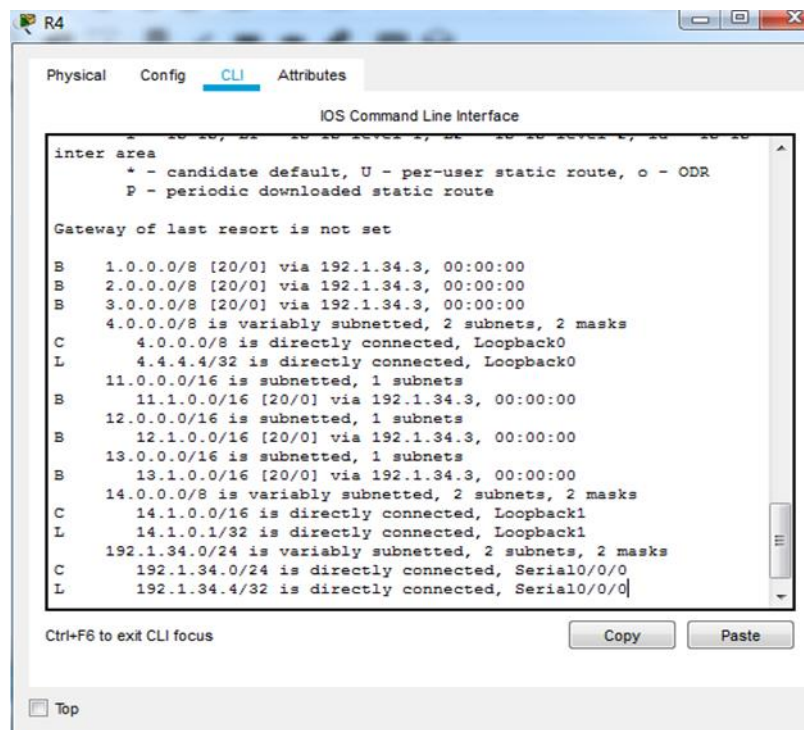
```
R4(config-router)#no synchronization
```

```
R4(config-router)#neighbor 192.1.34.3 remote-as 3
```

```
R4(config-router)#network 4.0.0.0 mask 255.0.0.0
```

```
R4(config-router)#network 14.1.0.0 mask 255.255.0.0
```

Figura 9. Show ip Router para R4.



```
R4
Physical Config CLI Attributes
IOS Command Line Interface
inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

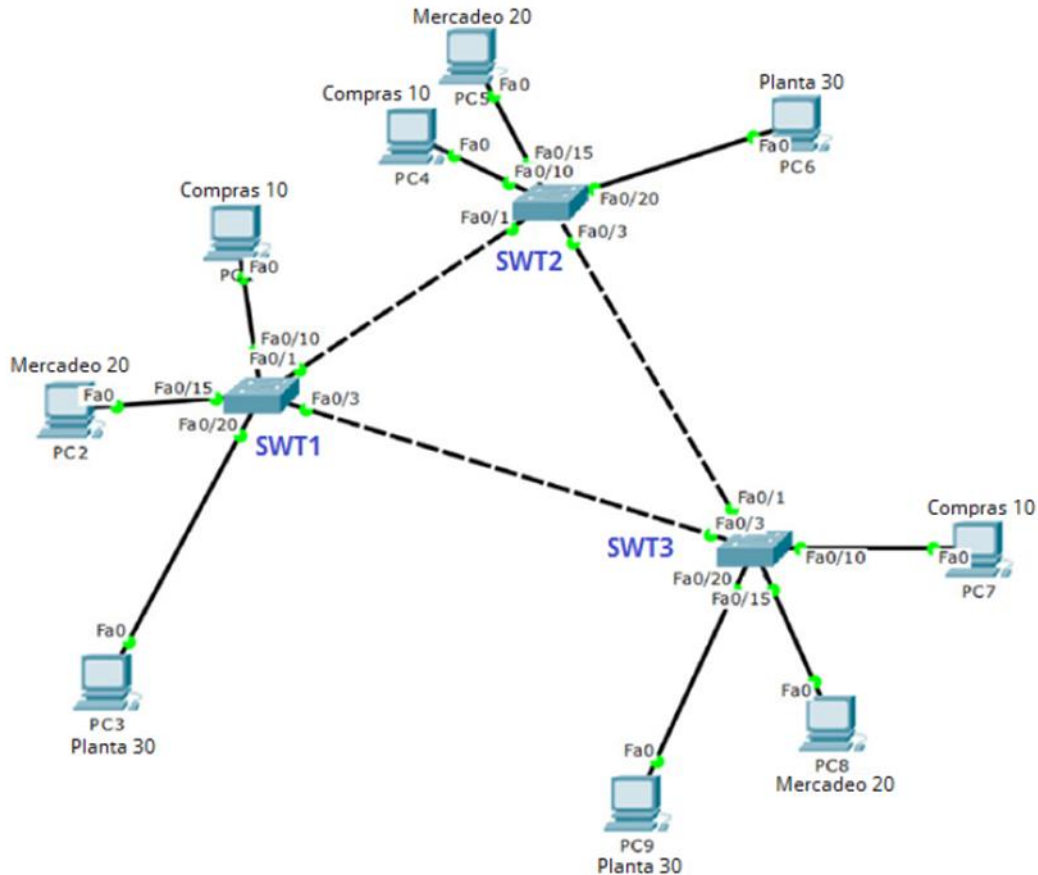
Gateway of last resort is not set

B 1.0.0.0/8 [20/0] via 192.1.34.3, 00:00:00
B 2.0.0.0/8 [20/0] via 192.1.34.3, 00:00:00
B 3.0.0.0/8 [20/0] via 192.1.34.3, 00:00:00
4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 4.0.0.0/8 is directly connected, Loopback0
L 4.4.4.4/32 is directly connected, Loopback0
11.0.0.0/16 is subnetted, 1 subnets
B 11.1.0.0/16 [20/0] via 192.1.34.3, 00:00:00
12.0.0.0/16 is subnetted, 1 subnets
B 12.1.0.0/16 [20/0] via 192.1.34.3, 00:00:00
13.0.0.0/16 is subnetted, 1 subnets
B 13.1.0.0/16 [20/0] via 192.1.34.3, 00:00:00
14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 14.1.0.0/16 is directly connected, Loopback1
L 14.1.0.1/32 is directly connected, Loopback1
192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.1.34.0/24 is directly connected, Serial0/0/0
L 192.1.34.4/32 is directly connected, Serial0/0/0

Ctrl+F6 to exit CLI focus Copy Paste
Top
```


ESCENARIO 3

Figura 10. 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.

SWT1

```
Switch>en
Switch#conf t
Switch(config)#hostname SWT1
SWT1(config)#vtp domain CCNP
```



```
SWT1(config)#vtp mode client
SWT1(config)#vtp pass cisco
SWT1(config)#vtp versión 2
```

SWT2

```
Switch>en
Switch#conf t
Switch(config)#hostname SWT2
SWT2(config)#vtp domain CCNP
SWT2(config)#vtp mode server
SWT2(config)#vtp pass cisco
SWT2(config)#vtp versión 2
```

SWT3

```
Switch>en
Switch#conf t
Switch(config)#hostname SWT3
SWT3(config)#vtp domain CCNP
SWT3(config)#vtp mode client
SWT3(config)#vtp pass cisco
SWT3(config)#vtp versión 2
```

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

Figura 11. Show VTP Status a SWT2.

```
SWT2#show vtp status
VTP Version                : 2
Configuration Revision     : 16
Maximum VLANs supported locally : 255
Number of existing VLANs   : 9
VTP Operating Mode         : Server
VTP Domain Name            : CCNP
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                  : 0xD9 0x09 0x9C 0xF9 0x3B 0x4E 0xD9
                             0x4B
```

Figura 12. Show VTP Status a SWT3.

```
SWT3>en
SWT3#show vtp status
VTP Version                : 2
Configuration Revision     : 16
Maximum VLANs supported locally : 255
Number of existing VLANs   : 9
VTP Operating Mode         : Client
VTP Domain Name            : CCNP
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                  : 0xD9 0x09 0x9C 0xF9 0x3B 0x4E 0xD9
0x4B
```

B. Configurar DTP (Dynamic Trunking Protocol).

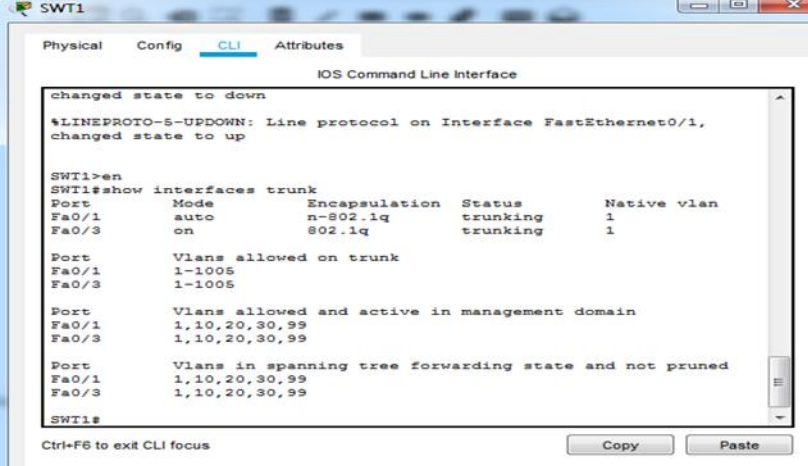
1. Configure un enlace troncal ("*trunk*") dinámico entre SWT1 y SWT2. Debido a que el modo por defecto es ***dynamic auto***, solo un lado del enlace debe configurarse como ***dynamic desirable***.

STW2

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

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

Figura 13. Show interfaces a SWT.



```
changed state to down
%LINEPROTO-S-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up

SW1>en
SW1#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     auto      n-802.1q       trunking    1
Fa0/3     on        802.1q         trunking    1

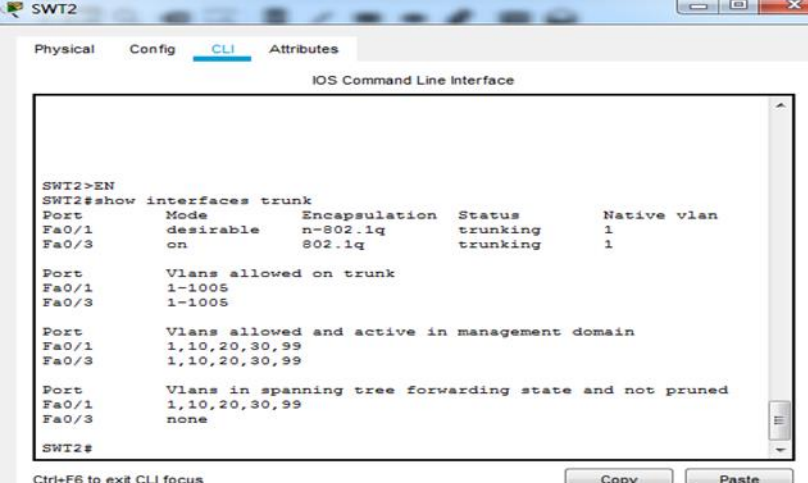
Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/3     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1,10,20,30,99
Fa0/3     1,10,20,30,99

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1,10,20,30,99
Fa0/3     1,10,20,30,99

SW1#
```

Figura 14. Show interfaces a SWT2.



```
SWI2>EN
SWI2#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     desirable n-802.1q       trunking    1
Fa0/3     on        802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/3     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1,10,20,30,99
Fa0/3     1,10,20,30,99

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1,10,20,30,99
Fa0/3     none

SWI2#
```

- Entre SW1 y SW3 configure un enlace "trunk" estático utilizando el comando **switchport mode trunk** en la interfaz F0/3 de SW1.

SW3

```
SW3(config-if)#int fa 0/3
SW3(config-if)#switchport mode trunk
SW3(config-if)#int fa 0/1
```

SWT3(config-if)#switchport mode trunk

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

Figura 15. Show interfaces trunk SWT1.

```
SWT1>en
SWT1#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     auto      n-802.1q       trunking    1
Fa0/3     on        802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/3     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1,10,20,30,99
Fa0/3     1,10,20,30,99

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1,10,20,30,99
Fa0/3     1,10,20,30,99
```

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

STW2

```
SWT2(config-if)#int fa 0/1
SWT2(config-if)#switchport mode dynamic desirable
SWT2(config-if)#int fa 0/3
SWT2(config-if)#switchport mode trunk
```

STW3

```
SWT3(config-if)#int fa 0/3
SWT3(config-if)#switchport mode trunk
SWT3(config-if)#int fa 0/1
SWT3(config-if)#switchport mode trunk
```

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).

SWT2

```
SWT2(config)#vlan 10
```

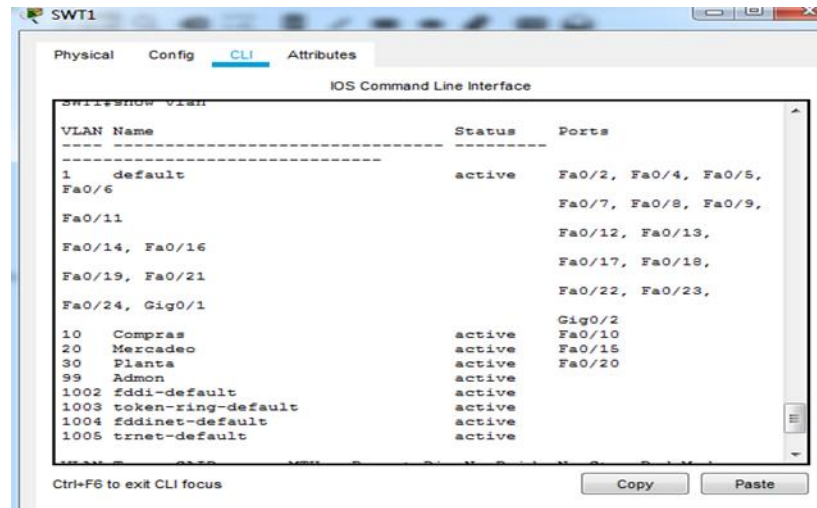
```

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

```

2. Verifique que las VLANs han sido agregadas correctamente.

Figura 16. Show VLAN SWT1.



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

Tabla 3. Direcciones IP.

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

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

STW1

```
SWT1(config-if)#int fa0/10
SWT1(config-if)#switchport access vlan 10
SWT1(config-if)#int fa0/15
SWT1(config-if)#switchport access vlan 20
SWT1(config-if)#int fa0/20
SWT1(config-if)#switchport access vlan 30
```

STW2

```
SWT2(config-if)#int fa0/10
SWT2(config-if)#switchport access vlan 10
SWT2(config-if)#int fa0/15
SWT2(config-if)#switchport access vlan 20
SWT2(config-if)#int fa0/20
SWT2(config-if)#switchport access vlan 30
```

STW3

```
SWT2(config-if)#int fa0/10
SWT2(config-if)#switchport access vlan 10
SWT2(config-if)#int fa0/15
SWT2(config-if)#switchport access vlan 20
SWT2(config-if)#int fa0/20
SWT2(config-if)#switchport access vlan 30
```

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.

SWT1

```
SWT1(config)#int fa0/15
SWT1(config-if)#switchport acces vlan 20
SWT1(config)#int fa0/20
SWT1(config-if)#switchport acces vlan 30
```

SWT2

```
SWT2(config-if)#int fa0/15
SWT2(config-if)#switchport mode access vlan 20
SWT2(config)#int fa0/20
```

```
SWT2(config-if)#switchport acces vlan 30
```

STW3

```
SWT3(config-if)#int f0/15  
SWT3(config-if)# switchport acces vlan 20  
SWT3(config-if)#int f0/20  
SWT3(config-if)# switchport acces vlan 30
```

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 4. Direcciones IP para 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

Configuración en STW1

```
SWT1(config)#int vlan 99  
SWT1(config-if)#ip add 190.108.99.1 255.255.255.0  
SWT1(config-if)#no sh  
"Los puertos que no están en uso se deshabilitan"  
SWT1(config)#int fa0/2  
SWT1(config)#shutdown  
SWT1(config)#exit  
SWT1(config)#int range fa0/4-9  
SWT1(config)#shutdown  
SWT1(config)#exit  
SWT1(config)#int range fa0/11-14  
SWT1(config)#shutdown  
SWT1(config)#exit  
SWT1(config)#int range fa0/16-19  
SWT1(config)#shutdown  
SWT1(config)#exit
```

```
SWT1(config)#int range fa0/21-24
SWT1(config)#shutdown
```

Configuración en STW2

```
SWT2(config)#int vlan 99
SWT2(config-if)#ip add 190.108.99.2 255.255.255.0
SWT2(config-if)#no sh
"Los puertos que no están en uso se deshabilitan"
SWT2(config)#int fa0/2
SWT2(config)#shutdown
SWT2(config)#exit
SWT2(config)#int range fa0/4-9
SWT2(config)#shutdown
SWT2(config)#exit
SWT2(config)#int range fa0/11-14
SWT2(config)#shutdown
SWT2(config)#exit
SWT2(config)#int range fa0/16-19
SWT2(config)#shutdown
SWT2(config)#exit
SWT2(config)#int range fa0/21-24
SWT2(config)#shutdown
```

Configuración en STW3

```
SWT3(config)#int vlan 99
SWT3(config-if)#ip add 190.108.99.3 255.255.255.0
SWT3(config-if)#no sh
"Los puertos que no están en uso se deshabilitan"
SWT3(config)#int fa0/2
SWT3(config)#shutdown
SWT3(config)#exit
SWT3(config)#int range fa0/4-9
SWT3(config)#shutdown
SWT3(config)#exit
SWT3(config)#int range fa0/11-14
SWT3(config)#shutdown
SWT3(config)#exit
SWT3(config)#int range fa0/16-19
SWT3(config)#shutdown
SWT3(config)#exit
SWT3(config)#int range fa0/21-24
```


SWT3(config)#shutdown

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 17. Ping entre PC.

```
Packet Tracer PC Command Line 1.0
C:\>ping 190.108.20.3

Pinging 190.108.20.3 with 32 bytes of data:

Reply from 190.108.20.3: bytes=32 time=3ms TTL=128
Reply from 190.108.20.3: bytes=32 time=3ms TTL=128
Reply from 190.108.20.3: bytes=32 time=10ms TTL=128
Reply from 190.108.20.3: bytes=32 time<1ms 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 = 10ms, Average = 4ms

C:\>ping 190.108.10.3

Pinging 190.108.10.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.10.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

El *ping* tiene éxito cuando se envía a los PC que están en la misma VLAN en este caso los de mercadeo, si intentamos enviar ping a otros departamentos sale negativo el *ping* ya que es otra VLAN.

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

Figura 18. Ping entre Switchs.

```
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 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

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
```

El *ping* fue exitoso ya que están en la misma VLAN y cada *Switch* posee su IP

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

Figura 19. Ping entre Switch a los PC.

```
SWT2>en
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)

SWT2#ping 190.108.20.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SWT2#
```

El *ping* no tuvo éxito los *switch* no tiene IP en la VLAN

CONCLUSIONES

- En las configuraciones y paso a paso que se realizó para cada escenario, se encontró un grado de complejidad al momento de tener conectividad en cada topología y sus componentes. Se calculó el direccionamiento de acuerdo a la solicitud planteada por medio de los protocolos de enrutamiento para cada interface, evidenciando la importancia del tipo de enrutamiento compatible entre el emisor y receptor, en lo que se planteó de acuerdo a las bases y conocimiento obtenido en las actividades del diplomado, cada configuración para el enrutamiento de datos en el paso a paso de las redes de comunicación.
- Con el primer escenario se presentaron los conocimientos adquiridos a lo largo del curso de profundización para la configuración y enrutamientos de *routers*, donde se implementó las interfaces *Loopback* para la transmisión de datos, la cual se determina en la práctica que esta interface dirige el tráfico en los mismo *routers* y se asocia a los procesos OSPF para no tener el riesgo de perder la sesión configurada.
- En el segundo escenario trato de configurar *routers* a través de la relación de vecino BGP, comprendiendo que los *routers* deben de ser compatibles con el protocolo de puerta de enlace para intercambiar la información de dirección entre las redes IP. Con esta configuración en los *routers* se garantiza una entrega fiable de la información y comprendemos que los sistemas autónomos están conectados por enlaces virtuales.
- Para la práctica realizada en el tercer escenario aplicamos los conceptos para la configuración de *switches* tomados en el curso, afianzando nuestro conocimiento y garantizando las competencias en la implementación de redes de comunicación con la configuración y administración de VLAN, con la definición de los tipos de nivel que son necesarios para habilitar los puertos entre los PC y los *switches*. Donde se tuvo que tener presente que los *switches* estaban en el dominio VPT llamado CCNP y se tenía que hacer uso de la contraseña cisco.

BIBLIOGRÁFICA

- Bibing. (2008). Fundamentos de BGP. Consultado el 06 de diciembre de 2018 del sitio web <http://bibing.us.es/proyectos/abreproy/11359/fichero/BGP%252F5.+Fundamentos+de+BGP.pdf>.
- Cisco. (2014). Configurando el VLAN Trunk Protocol (VTP). Consultado el 08 de diciembre de 2018 del sitio web https://www.cisco.com/c/es_mx/support/docs/lan-switching/vtp/98154-conf-vlan.html.
- From, 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!AmIJYei-NT1IlnWR0hoMxgBNv1CJ>