SOLUCIÓN DE ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

DIEGO FERNANDO GARCIA MARIN

Diplomado de Profundización CCNP

Mg. Gerardo Granados Acuña

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA
POPAYAN
2018

INTRODUCCIÓN

Internet es una red amplia de equipos y servidores que permite difundir y compartir información de gran variedad, por su crecimiento constante es indispensable el manejo adecuado para evitar filtración de información sensible a destinatarios no autorizados y así controlar el flujo adecuado, además, un control que permita mantener un flujo constante de los datos, dando fiabilidad y velocidad.

Por esta razón, es indispensable disponer de personal capacitado que pueda implementar las tecnologías apropiadas para construir una red escalable basada en routers, construir redes del tipo "campus" utilizando tecnologías de "switching multilayer", mejorar los flujos de tráfico de datos, seguridad, redundancia y rendimiento de LANs de campus o WANs basadas en routers y switches, así como acceso remoto a redes y crear, desarrollar intranets globales, con capacidad de resolución de incidencias en entornos basados en routers y switches de Cisco para servicios y hosts multiprotocolo.

En ente trabajo se puede observar como el estudiante luego del entrenamiento recibido durante el diplomando de profundización CCNP demuestra los conocimientos adquiridos sobre cómo instalar, configurar y operar redes locales y de área amplia, para brindar servicios de acceso por marcación a organizaciones que tienen redes desde 100 hasta 500 nodos con protocolos y tecnologías tales como TCP/IP, OSPF, EIGRP, BGP, STP y VTP mediante el desarrollo de tres ejercicios que abarcan algunos de los temas vistos durante el diplomado y el desarrollo de sus habilidades caza fallas de trouble-shooting.

CONTENIDO

ESCENARIO 1

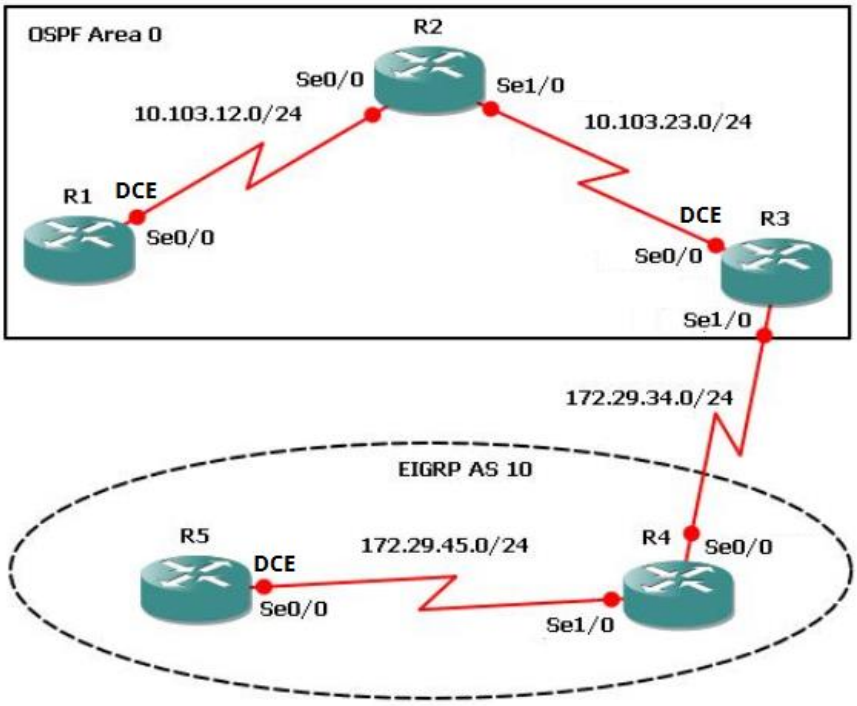

Figura 1, topología de red caso 1

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.

DESARROLLO PUNTO 1 CASO 1

Como configuración inicial, es necesario asignar nombre a cada uno de los routers, direcciones de las interfaces y protocolos de comunicación correspondientes con el siguiente código.

Configuración para Router 1

Dentro de las configuraciones iniciales que se deben aplicar a todo router está el asignar nombre a este para una fácil identificación en la topología, para este caso se debe usar el comando *hostname,* aplicar el tipo de protocolo a implementar que puede ser ejecutado mediante el comando *router protocolo área,* en este caso debe ser *OSPF 1.* Luego es necesario asignar una identificación al router dentro del

protocolo, para lo cual está el comando *router id #,*en este punto ya es posible agregar las redes que intervendrán en el protocolo.

Teniendo en cuenta lo anterior, se debe aplicar los siguientes comandos para configurar el router 1 según la especificación de la topología.

```
Router>
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 10.103.12.0 255.255.255.0 area 0
R1(config-router)#exit
R1(config)#interface s0/0
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
R1(config-if)#bandwidth 128
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#end
R2#wr
```

Es necesario tener presente que para activar las interfaces se debe aplicar el comando *shutdown,* de lo contrario permanecerá apagada.

Configuración para Router 2

Al igual que en la configuración del router anterio, se debe asignar nombre, aplicar el protocolo de comunicación e ingresar las interfaces que intervendrán en el mismo. Para ello, es necesario que se apliquen los comandos siguientes:

```
Router>
Router>enable
Router#configure terminal
Router(config)#hostname R2
```

```
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 10.103.12.0 255.255.255.0 area 0
R2(config-router)#network 10.103.23.0 255.255.255.0 area 0
R2(config-router)#exit
R2(config)#interface s0/0
R2(config-if)description to R1
R2(config-if)#ip address 10.103.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface s0/1
R2(config-if)description to R3
R2(config-if)#ip address 10.103.23.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#end
R2#wr
```

Es necesario guardar cada vez que se cambie algo en la configuración mediante el comando *wr,* toda vez que al apagar el router y reiniciarlo se perderá toda la información que no haya sido guardada.

Configuración para Router 3

Igual que en los routers 1 y 2, se debe aplicar los comandos siguientes como configuración inicial.

```
Router>
Router>enable
Router#configure terminal
Router(config)#hostname R3
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 10.103.23.0 255.255.255.0 area 0
R3(config-router)#exit
R3(config)#interface s0/0
```

```
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
R3(config-if)#bandwidth 128
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface s0/1
R3(config-if)description to R4
R3(config-if)#ip address 172.29.34.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#end
R3#wr
```

No olvidar que cuando un puerto tenga conexión DCE, es necesario configurar el reloj.

Con el objetivo de permitir comunicación con ambos protocolos y teniendo en cuenta que R4 en el puerto serial 0 se configura con un protocolo diferente como es el caso de *EIGRP*, se procede a configurar el puerto serial 1 de R3 para que intervenga en *eigrp*. Por tanto, se aplican los comandos presentados a continuación:

```
R3#configure terminal
R3(config)#router eigrp 10
R3(config-rtr)#eigrp router-id 3.3.3.3
R3(config-rtr)#network 172.29.34.0 255.255.255.0
R3(config-rtr)#exit
R3(config)#end
R3#wr
```

Como se observa en los comandos anteriores, para que el puerto ejecute este protocolo se debe utilizar el comando *router eigrp área*, así mismo se asigna un número para identificarlo y como es el router 3 se ha decidido dejar como 3.3.3.3

Configuración para Router 4

Para los routers 4 y 5 el protocolo de comunicación es el *eigrp* en el sistema autónomo 10, se identifican de acuerdo a su numeración para fácil uso, es decir el router 4 como 4.4.4.4 y el router 5 como 5.5.5.5, para anexar las interfaces que intervienen en este protocolo se usa el comando *network* seguido de la dirección ip correspondiente. Por tanto, para una apropiada configuración del router 4 se aplican los comandos presentados a continuación:

```
Router>
Router>enable
Router#configure terminal
Router(config)#hostname R4
R4(config)#router eigrp 10
R4(config-rtr)#eigrp router-id 4.4.4.4
R4(config-rtr)#network 172.29.34.0 255.255.255.0
R4(config-rtr)#network 172.29.45.0 255.255.255.0
R4(config-rtr)#exit
R4(config)#interface s0/0
R4(config-if)#ip address 172.29.34.2 255.255.255.0
R5(config-if)#no shutdown
R4(config-if)#exit
R4(config)#interface s0/1
R4(config-if)#ip address 172.29.45.1 255.255.255.0
R5(config-if)#no shutdown
R4(config-if)#exit
R4(config)#end
R4#wr
```

Es esencial aplicar el comando *no shutdown* cada vez que se configure coda interfaz para encenderla.

Configuración para Router 5

De acuerdo a la topología, se configuran las interfaces correspondientes según se muestra en la figura 1 para el router 5 con los comandos presentados a continuación:

```
Router>
Router>enable
Router#configure terminal
Router(config)#hostname R5
R5(config)#router eigrp 10
R5(config-rtr)#eigrp router-id 5.5.5.5
R4(config-rtr)#network 172.29.45.0 255.255.255.0
R5(config)#interface s0/0
R5(config-if)#ip address 172.29.45.2 255.255.255.0
R5(config-if)#no shutdown
R5(config-if)#exit
R5(config)#end
R5#wr
```

Con esto quedan configurados todos los routers según el punto 1 solicitado

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.

DESARROLLO PUNTO 2 CASO 1

Para crear una interfaz loopback solo se debe usar el comando *interface loopback,* es muy importante identificar la máscara de red la cual está dada por "***/22***" que corresponde a 255.255.252.0, por esta razón, para desarrollar este punto se debe aplicar los siguientes comandos en el router 1.

```
R1#conf t
R1(config)#interface loopback 4
R1(config-if)#ip address 10.1.4.1 255.255.252.0
R1(config-if)#ip ospf 1 area 0
R1(config-if)#exit
R1(config)# interface loopback 8
R1(config-if)#ip address 10.1.8.1 255.255.252.0
R1(config-if)#ip ospf 1 area 0
R1(config-if)#exit
```

```
R1(config)# interface loopback 12
R1(config-if)#ip address 10.1.12.1 255.255.252.0
R1(config-if)#ip ospf 1 area 0
R1(config-if)#exit
R1(config)# interface loopback 16
R1(config-if)#ip address 10.1.16.1 255.255.252.0
R1(config-if)#ip ospf 1 area 0
R1(config-if)#exit
R1(config)#end
R1#wr
```

Es necesario poner a participar estas interfaces en el protocolo sugerido, para ello se debe usar el comando *ip ospf 1 area 0*, según se solicita.

Con el objetivo de verificar que las nuevas interfaces loopback hayan quedado configuradas para participar en el protocolo OSPF se puede utilizar el comando ***show ip ospf brief***, el cual muestra el siguiente resultado como se puede evidenciar en la figura 2:

```
R1#sh ip ospf interface bri
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Lo16         1     0               10.1.16.1/22       1     LOOP  0/0
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
Se0/0        1     0               10.103.12.1/24     781   P2P   1/1
```

Figura 2, pantallazo router 1 loobacks

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.

DESARROLLO PUNTO 3 CASO 1

Para desarrollar este punto es indispensable identificar la máscara de red la cual está dada por el “/22” que corresponde a 255.255.252.0. Teniendo esto claro se deben crear las loopbacks correspondientes y asignarles las direcciones. En este caso, para crear cada loopback es necesario utilizar el comando *interface loopback*

número, de ahí que se puede usar las líneas de comando siguientes para cumplir con dicho objetivo:

R5#configure terminal Ingreso a modo de configuración
R5(config)#int lo 4
R5(config-if)#ip address 172.5.4.1 255.255.252.0
R5(config-if)#exit
R5(config)#int lo 8
R5(config-if)#ip address 172.5.8.1 255.255.252.0
R5(config-if)#exit
R5(config)#int lo 12
R5(config-if)#ip address 172.5.12.1 255.255.252.0
R5(config-if)#exit
R5(config)#int lo 16
R5(config-if)#ip address 172.5.16.1 255.255.252.0
R5(config-if)#exit

Con el objetivo de verificar que hayan sido creadas las interfaces loopback, se puede usar el comando **show ip interfaces brief | include up** que muestra el siguiente dato:

```
R5#sh ip interface bri | include up
Serial0/0                  172.29.45.2     YES NVRAM  up                    up
Vlan1                      unassigned      YES NVRAM  up                    down
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
Loopback16                 172.5.16.1      YES manual up                    up
```

Figura 3, pantallazo router 5 loobacks

Como se observa en la figura 3, las 4 loopback han sido creadas, por tanto, se agregan estas redes para que participen en el protocolo EIGRP, para esto se utiliza el comando *router eigrp 10* de la siguiente manera.

R5(config)#router eigrp 10
R5(config-router)#no auto-sumary
R5(config-router)#network 172.5.4.0 255.255.255.0
R5(config-router)#network 172.5.8.0 255.255.255.0

```
R5(config-router)#network 172.5.12.0 255.255.255.0
R5(config-router)#network 172.5.16.0 255.255.255.0
R5(config-router)#network 172.29.45.0 255.255.255.0
R5(config-router)#exit
R5(config)#end
R5#wr
```

Para verificar que las interfaces loopback hayan quedado integradas al protocolo EIGRP es posible utilizar el comando **show ip eigrp interfaces.**

```
R5#sh ip eigrp int
IP-EIGRP interfaces for process 10

                        Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable   Flow Timer   Routes
Se0/0              1        0/0        18       0/15          83           0
Lo4                0        0/0         0       0/1            0           0
Lo8                0        0/0         0       0/1            0           0
Lo12               0        0/0         0       0/1            0           0
Lo16               0        0/0         0       0/1            0           0
```

Figura 4, pantallazo router 5 interfaces eigrp

Como se puede evidenciar en la figura 4, las 4 nuevas interfaces de loopback ya participan en EIGRP.

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**.

DESARROLLO PUNTO 4 CASO 1

Se ejecuta el comando **show ip route**, el cual arroja la información siguiente:

```
R3#show ip route
Codes: 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

Gateway of last resort is not set

     172.5.0.0/22 is subnetted, 4 subnets
D       172.5.8.0 [90/2809856] via 172.29.34.2, 00:12:09, Serial0/1
D       172.5.12.0 [90/2809856] via 172.29.34.2, 00:12:01, Serial0/1
D       172.5.4.0 [90/2809856] via 172.29.34.2, 00:14:21, Serial0/1
D       172.5.16.0 [90/2809856] via 172.29.34.2, 00:11:52, Serial0/1
     172.29.0.0/24 is subnetted, 2 subnets
C       172.29.34.0 is directly connected, Serial0/1
D       172.29.45.0 [90/2681856] via 172.29.34.2, 08:37:06, Serial0/1
     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
O       10.1.8.1/32 [110/846] via 10.103.23.1, 06:05:23, Serial0/0
O       10.1.12.1/32 [110/846] via 10.103.23.1, 06:04:45, Serial0/0
O       10.1.4.1/32 [110/846] via 10.103.23.1, 08:11:52, Serial0/0
O       10.1.16.1/32 [110/846] via 10.103.23.1, 06:04:14, Serial0/0
O       10.103.12.0/24 [110/845] via 10.103.23.1, 08:37:24, Serial0/0
```

Figura 5, pantallazo router 3 rutas

De la información anterior, se evidencia que el router R3 ha aprendido las 8 nuevas interfaces de loopback de ambos protocolos de la siguiente manera:

```
     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
O       10.1.8.1/32 [110/846] via 10.103.23.1, 06:05:23, Serial0/0
O       10.1.12.1/32 [110/846] via 10.103.23.1, 06:04:45, Serial0/0
O       10.1.4.1/32 [110/846] via 10.103.23.1, 08:11:52, Serial0/0
O       10.1.16.1/32 [110/846] via 10.103.23.1, 06:04:14, Serial0/0
O       10.103.12.0/24 [110/845] via 10.103.23.1, 08:37:24, Serial0/0
```

Figura 6, pantallazo router 1 ospf

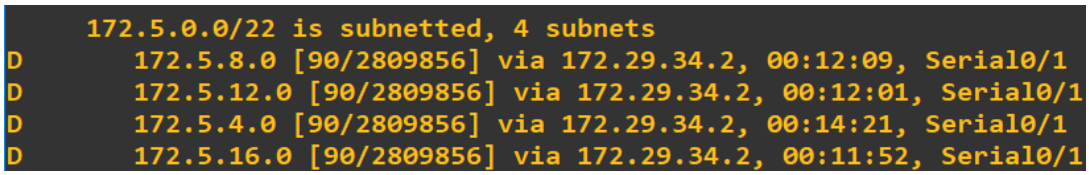

Figura 7 , pantallazo router 5 eigrp

En la figura 6 se observan las interfaces que participan en el protocolo OSPF, mientras que en la figura 7 se muestras las interfaces que participan en el protocolo EIGRP, por tanto, el router 3 tiene la información de todas la interfaces de ambos protocolos de comunicación.

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.

DESARROLLO PUNTO 5 CASO 1

Comandos necesarios para la distribución:

Es necesario tener presente la siguiente fórmula;

$$\text{Costo} = \frac{100000}{\text{BW(Kbps)}}$$

Se ingresa las líneas de comando siguientes para cumplir con lo requerido, teniendo en cuenta que el comando *redistribute* se utiliza para redistribuir en ambos protocolos, solo se debe especificar el mismo a aplicar, como se ilustra a continuación:

$$redistribute[protocolo]\ metric\ [(ancho\ de\ banda)(demora)(confiabiliad)(carga)(MTU)]$$

Para comprender mejor este comando se detallan a continuación cada una de sus partes:

Protocolo: Corresponde al protocolo de comunicación, en este caso puntual OSPF e EIGRP

Ancho de banda: En unidades de kilobites/segundo, 10000 para ethernet

Demora: En unidades de decenas de microsegundos, para ethernet es 100*10 microsegundos que es igual a 1ms.

Confiabilidad: Rango entre 0 y 255 donde 255 significa 100% de confiabilidad.

Carga: Es la carga efectiva en el link expresada entre 0 y 255, donde 255 es la carga a 100%

MTU: MTU (Unidad de Transmisión Básica) para la trayectoria, generalmente iguales que ethernet que es de 1500 bytes.

Con esta información, se ingresan las siguientes líneas de comando al router.

```
R3(config)#router eigrp 10
R3(config-router)#redistribute ospf 1 metric 100000 20000 255 255 1500
R3(config-router)#exit
R3(config)#router ospf 1
R3(config-router)#redistribute eigrp 10 metric 50000 subnets
R3(config-router)#exit
R3(config)#end
R3#wr
```

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

DESARROLLO PUNTO 6 CASO 1

Se aplica el comando *show ip route en cada uno de los routers:*

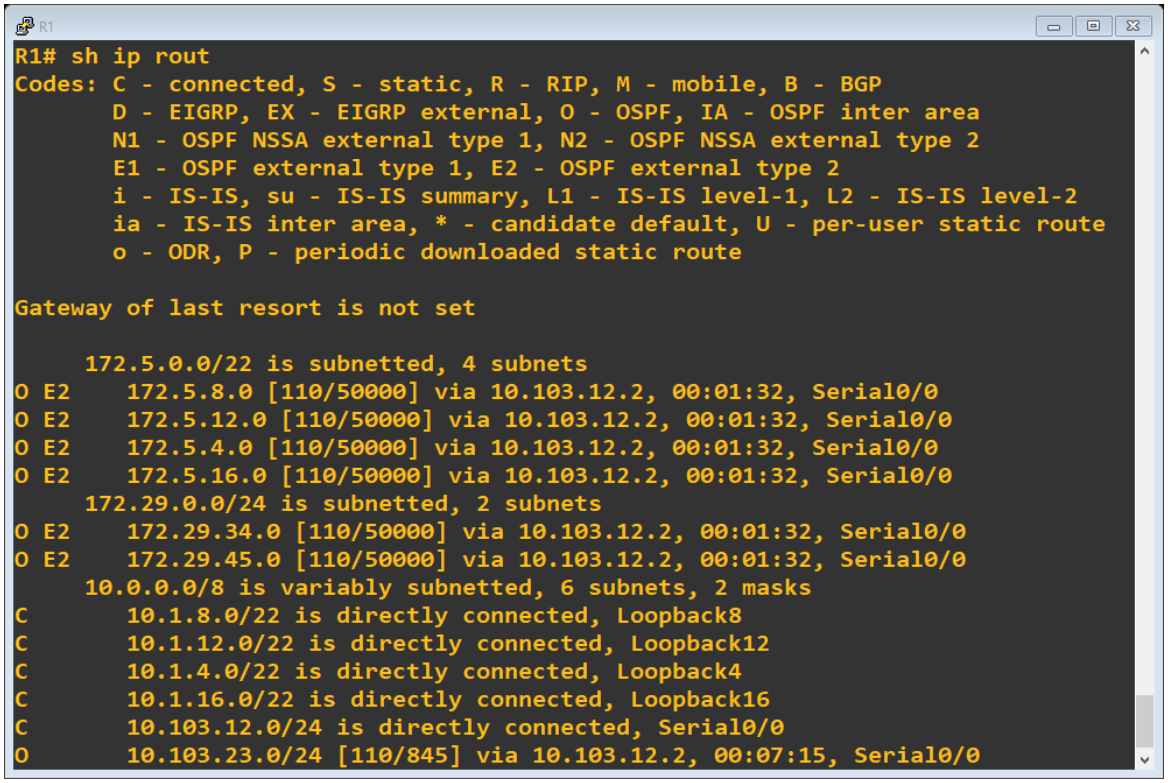

Figura 8, pantallazo router 1 (rutas)

Como se puede observar en figura 8, en el router R1 ya aparecen las loopbacks creadas en R5.

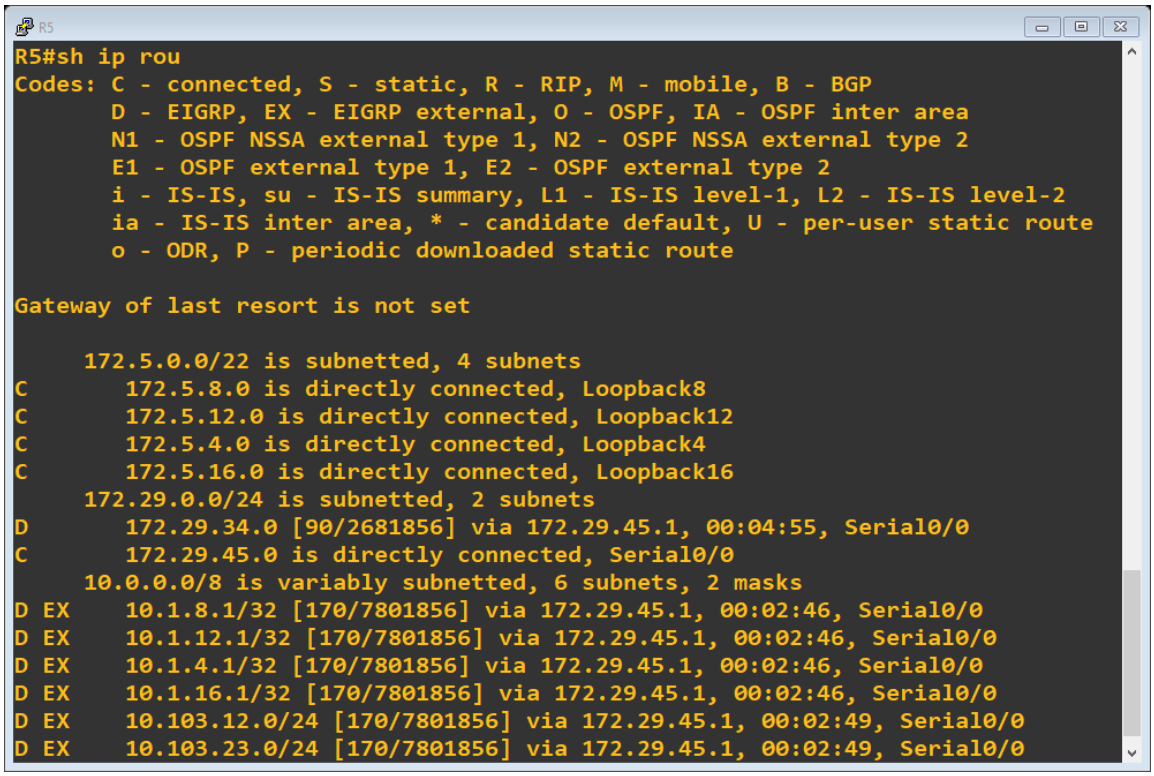

Figura 9, pantallazo router 5 rutas

Igualmente se puede observar en la figura 9 que el router R5 ya tiene aprendidas las loopbacks creadas en R1.

De esta forma los hosts en ambos protocolos pueden comunicarse entre sí.

ESCENARIO 2

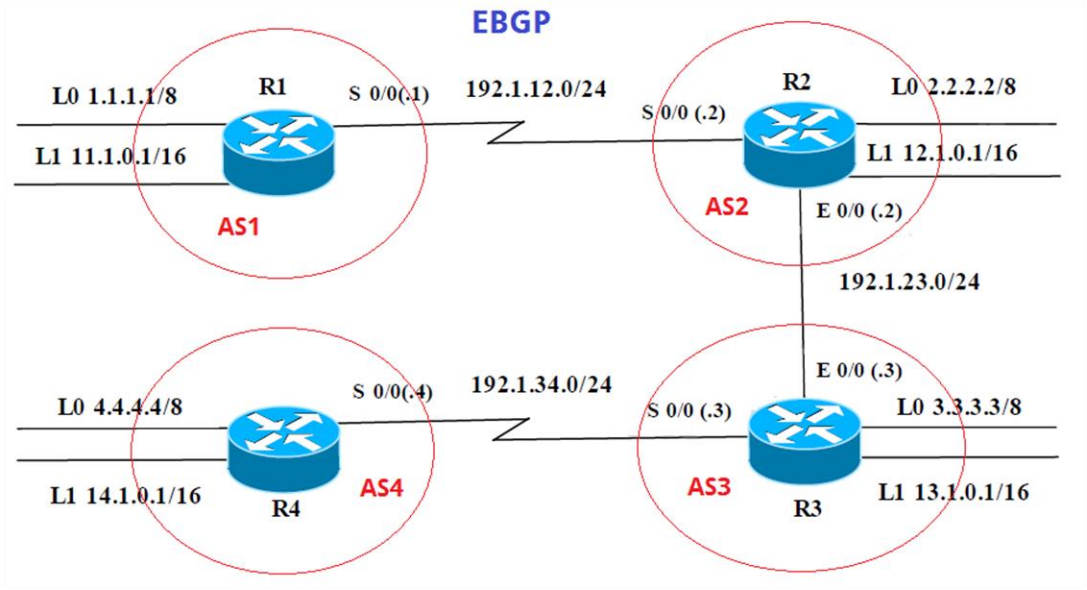

Figura 10, topología de red caso 2

Información para la configuración de los Routers

ROUTER 1

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

Tabla 1, configuración puerto serial y loobacks

Se ingresan las siguientes líneas de comandos con el fin de agregar las interfaces correspondientes:

R1#configure terminal

R1(config)#interface loopback 0

R1(config-if)#ip address 1.1.1.1 255.0.0.0

R1(config-if)#exit

R1(config)# interface loopback 1

R1(config-if)#ip address 11.1.0.1 255.255.0.0

R1(config-if)#exit

R1(config)# interface serial 0/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#exit
R1(config)#end
R1#wr

```
R1#sh ip int bri | include up
Serial0/0                  192.1.12.1      YES manual up                    up

Vlan1                      unassigned      YES unset  up                    down

Loopback0                  1.1.1.1         YES manual up                    up

Loopback1                  11.1.0.1        YES manual up                    up
```

Figura 11, interfaces en R1

En la figura 11 se puede constatar que las interfaces han sido agregadas.

ROUTER 2

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

Tabla 2, configuración puertos y loobacks

Se procede a configurar el router R2 mediante las siguientes líneas de comando:

R2#configure terminal
R2(config)#interface loopback 0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#exit
R2(config)# interface loopback 1
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#exit
R2(config)# interface serial 0/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#exit

R2(config)# interface fastethernet 0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#exit
R2(config)#end
R2#wr

```
R2#sh ip interface bri | include up
FastEthernet0/0            192.1.23.2      YES manual up                    up

Serial0/0                  192.1.12.2      YES manual up                    up

Vlan1                      unassigned      YES unset  up                    down

Loopback0                  2.2.2.2         YES manual up                    up

Loopback1                  12.1.0.1        YES manual up                    up
```

Figura 12, interfaces en R2

En la figura 12 se muestran las interfaces ya configuradas en el router R2 mediante el comando *show ip interface brief* | *include up*

ROUTER 3

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

Tabla 3, configuración puertos y loobacks

Se ingresan las siguientes líneas de comando en el router R3 para configurar las interfaces correspondientes:

R3#configure terminal
R3(config)#interface loopback 0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#exit
R3(config)# interface loopback 1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#exit

R3(config)# interface serial 0/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#exit
R3(config)# interface fastethernet 0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#exit
R3(config)#end
R3#wr

```
R3#sho ip int bri | include up
FastEthernet0/0            192.1.23.3      YES manual up                    up

Serial0/0                  192.1.34.3      YES manual up                    down

Vlan1                      unassigned      YES unset  up                    down

Loopback0                  3.3.3.3         YES manual up                    up

Loopback1                  13.1.0.1        YES manual up                    up
```

Figura 13, interfaces en R3

En la figura 13 se constata que las interfaces hayan sido creadas en el router R3 mediante el comando *show ip interface brief* | *include up.*

ROUTER 4

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

Tabla 4, configuración puerto serial y loobacks

Se ingresan las siguientes líneas de comando en el router R3 para configurar las interfaces correspondientes:

R4#configure terminal
R4(config)#interface loopback 0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#exit
R4(config)# interface loopback 1

R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#exit
R4(config)# interface serial 0/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#exit
R4(config)#end
R4#wr

```
R4#show ip int bri | in up
Serial0/0                  192.1.34.4      YES manual up                    up
Vlan1                      unassigned      YES unset  up                    down
Loopback0                  4.4.4.4         YES manual up                    up
Loopback1                  14.1.0.1        YES manual up                    up
```

Figura 14, interfaces en R4

En la figura 14 se constata que las interfaces hayan sido creadas en el router R3 mediante el comando *show ip interface brief* | *include up.*

PUNTOS A DESARROLLAR CASO 2

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.**

DESARROLLO PUNTO 1 CASO 2

Con el fin de configurar la relación de vecinos entre R1 y R2 se utiliza el comando *neigbor,* luego se agreagn las redes que participarán, de esta manera se agregan las líneas de comando al router R1 como se muestra a continuación:

R1#configure terminal
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 1.1.1.1 mask 255.0.0.0

R1(config-router)# network 11.1.0.1 mask 255.255.0.0
R1(config-router)#exit
R1(config)#end
R1#wr

```
R1#sh ip route
Codes: 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

Gateway of last resort is not set

C    192.1.12.0/24 is directly connected, Serial0/0
C    1.0.0.0/8 is directly connected, Loopback0
     11.0.0.0/16 is subnetted, 1 subnets
C       11.1.0.0 is directly connected, Loopback1
R1#
*Mar  1 00:00:42.987: %BGP-5-ADJCHANGE: neighbor 192.1.12.2 Up
```

Figura 15, rutas en R1

Mediante el comando *show ip route* se verifica que se haya activado la vecindad como lo muestra la figura 15.

Igualmente se activa el protocolo bgp y la relación de vecino en el router R2 mediante las siguientes líneas de comando:

R2#configure terminal
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)# network 2.2.2.2 mask 255.0.0.0
R2(config-router)# network 12.1.0.1 mask 255.255.0.0
R2(config-router)#exit
R2(config)#end
R2#wr

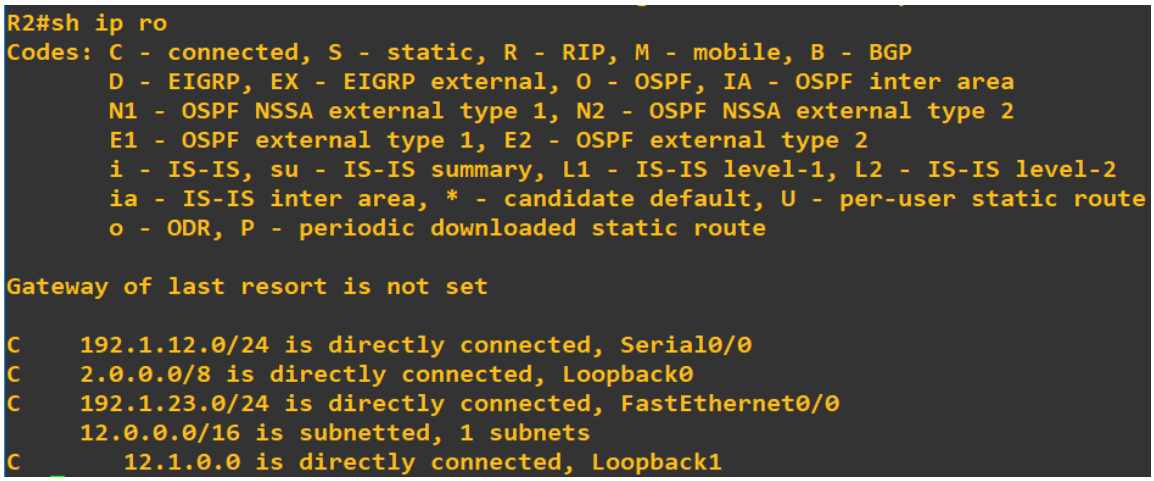

Figura 16, interfaces en R2

En la figura 16 se constata que la configuración haya sido efectiva.

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.**

DESARROLLO PUNTO 2 CASO 2

Primero se debe activar el protocolo bgp mediante el comando *router bgp (número),* luego se configura la relación de vecinos entre R2 y R3 con el comando *neighbor* mediante las líneas de comando siguientes:

R3#configure terminal
R3(config)# router bgp 3
R3(config-router)#bgp router-id 33.33.33.33
R3(config-router)# neighbor 192.1.23.2 remote-as 2
R3(config-router)# network 3.3.3.3 mask 255.0.0.0
R3(config-router)# network 13.1.0.1 mask 255.255.0.0
R3(config-router)#exit
R3(config)#end
R3#wr

```
R3#sh ip ro
Codes: 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

Gateway of last resort is not set

C    3.0.0.0/8 is directly connected, Loopback0
C    192.1.23.0/24 is directly connected, FastEthernet0/0
C    192.1.34.0/24 is directly connected, Serial0/0
     13.0.0.0/16 is subnetted, 1 subnets
C       13.1.0.0 is directly connected, Loopback1
```

Figura 17, interfaces en R3

En la figura 17 se observan las configuraciones guardadas.

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.**

DESARROLLO PUNTO 3 CASO 2

Mediante las siguientes líneas de comando se ejecutan las cofiguracione correspondientes:

R4#configure terminal
R4(config)# router bgp 4
R4(config-router)#bgp router-id 44.44.44.44
R4(config-router)# neighbor 192.1.34.3 remote-as 3
R4(config-router)# network 4.4.4.4 mask 255.0.0.0
R4(config-router)# network 14.1.0.1 mask 255.255.0.0
R4(config-router)#exit
R4(config)#end
R4#wr

```
R4#sh ip ro
Codes: 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

Gateway of last resort is not set

C    4.0.0.0/8 is directly connected, Loopback0
C    192.1.34.0/24 is directly connected, Serial0/0
     14.0.0.0/16 is subnetted, 1 subnets
C       14.1.0.0 is directly connected, Loopback1
```

Figura 18, interfaces en R4

En la figura 18 se evidencian las configuraciones correspondientes ya activas.

ESCENARIO 3

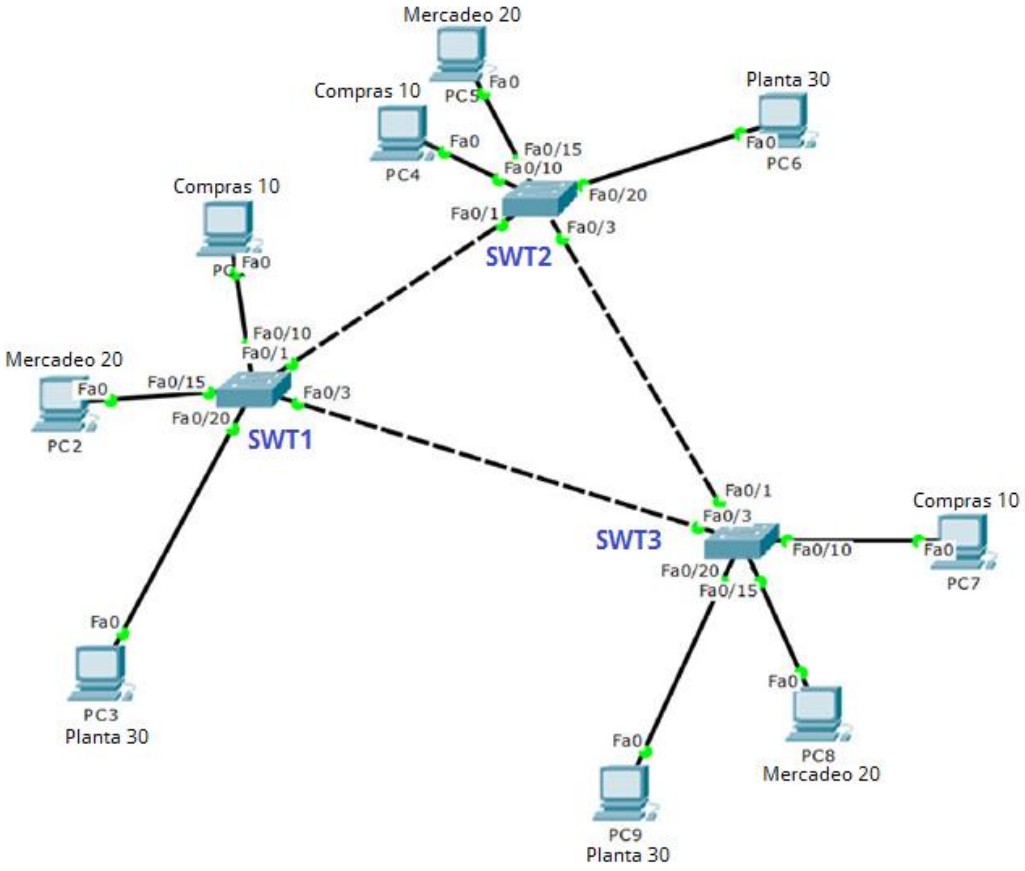

Figura 19, Topología de red caso 3

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.

DESARROLLO PARTE A PUNTO 1 CASO 3

Para activar la configuración VTP usamos el comando *vtp domain ***,* donde los astericos corresponden al nombre CCNP, para activar el modo cliente o servidor solo es necesario utilizar el comando *vtp mode (client/server)* dependiendo la opción

a utilizar. Es necesario recordar que en modo servidor es donde se pueden agregar las redes para que sean reconocidos en todos los switches. Para lograr lo anterior se aplica el siguiente código en cada uno de los switches:

Switch SWT1

```
IOU1#configure terminal
IOU1(config)#hostname SWT1
SWT1(config)#vtp domain CCNP
SWT1(config)#vtp mode client
SWT1(config)#vtp password cisco
SWT1(config)#exit
SWT1#wr
```

Switch SWT2

```
IOU1#configure terminal
IOU1(config)#hostname SWT2
SWT1(config)#vtp domain CCNP
SWT1(config)#vtp mode server
SWT1(config)#vtp password cisco
SWT1(config)#exit
SWT1#wr
```

Switch SWT3

```
IOU1#configure terminal
IOU1(config)#hostname SWT3
SWT1(config)#vtp domain CCNP
SWT1(config)#vtp mode client
SWT1(config)#vtp password cisco
SWT1(config)#exit
SWT1#wr
```

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

DESARROLLO PARTE A PUNTO 2 CASO 3

Se aplica el comando *show vtp status en cada unos de los switches* como se puede observar en las figuras 20 a 22.

Switch SWT1

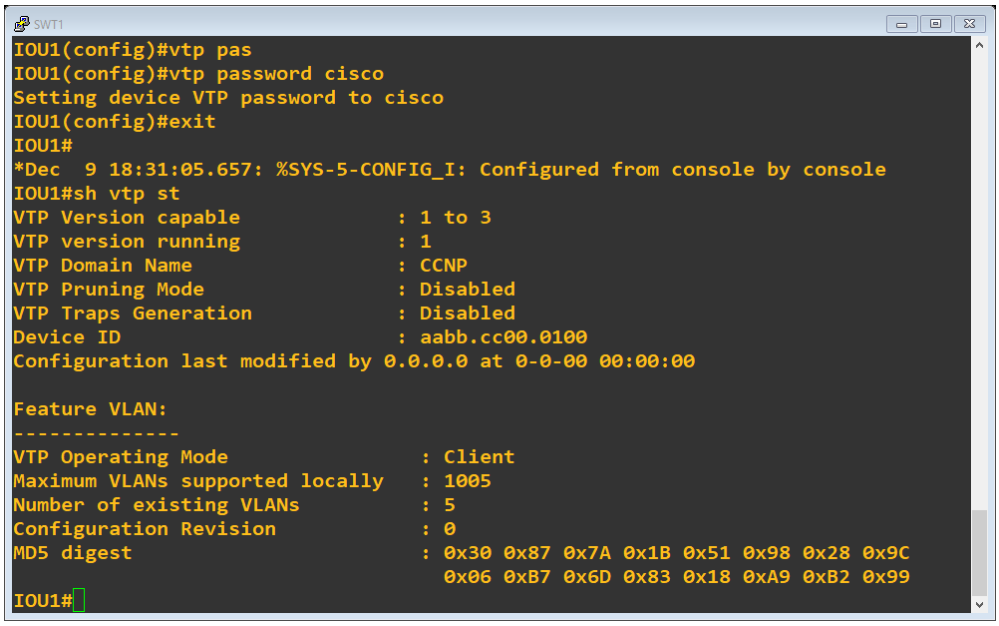

Figura 20, vtp en switch 1

Switch SWT2

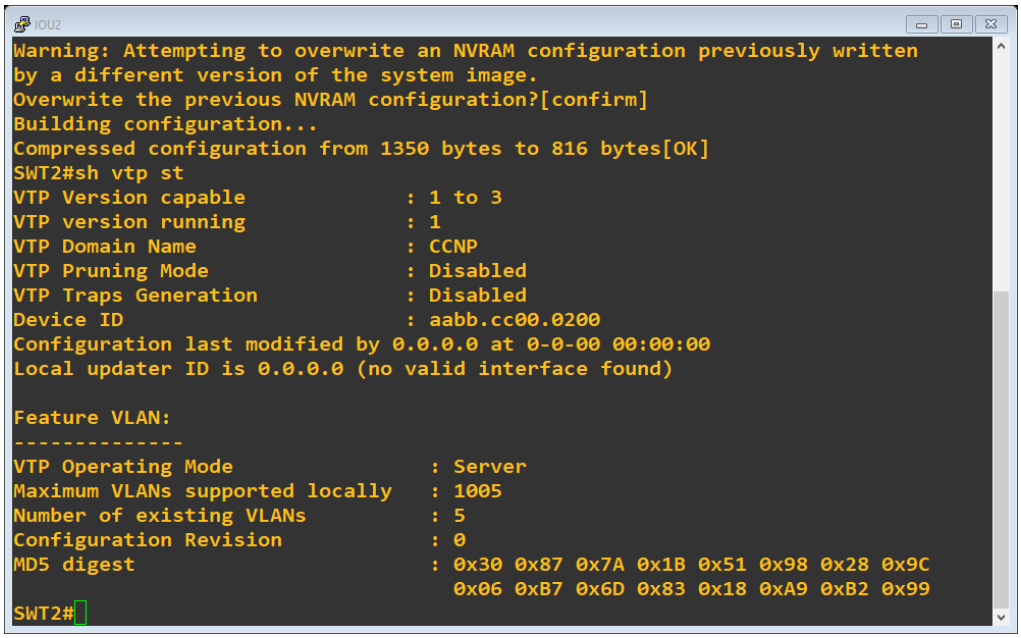

Figura 21, vtp en switch 2

Switch SWT3

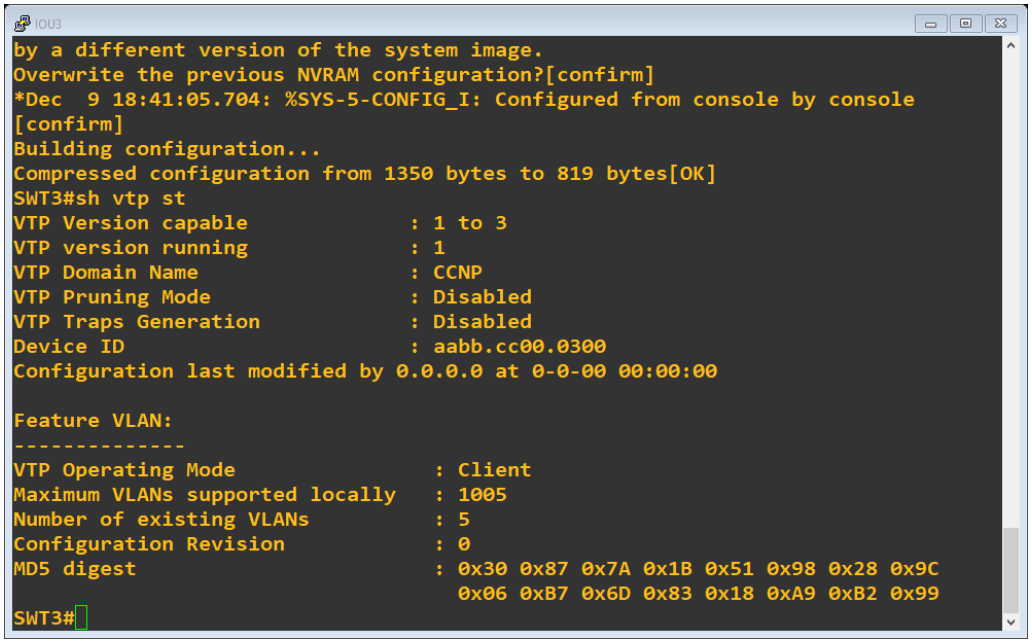

Figura 22, vtp en switch 3

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*.

DESARROLLO PARTE B PUNTO 1 CASO 3

Para configurar **Dynamic desirable** se debe utilizar el comando **switchport mode Dynamic desirable** en ambos switches, para ello se aplican las siguientes líneas de comando en cada uno.

Switch SWT1

```
SWT1#configure terminal
SWT1(config)#interface range ethernet0/0 - 1
SWT1(config-if-range)#switchport trunk encapsulation dot1q
SWT1(config-if-range)#switchport mode trunk
SWT1(config-if-range)#switchport mode dynamic desirable
SWT1(config-if-range)#no shutdown
SWT1(config-if-range)#exit
SWT1(config)#end
SWT1#wr
```

Switch SWT2

```
SWT2#configure terminal
SWT2(config)#interface range ethernet0/0
SWT2(config-if-range)#switchport trunk encapsulation dot1q
SWT2(config-if-range)#switchport mode trunk
SWT2(config-if-range)#switchport mode dynamic desirable
SWT2(config-if-range)#no shutdown
SWT2(config-if-range)#exit
SWT2(config)#interface range ethernet0/2
SWT2(config-if-range)#switchport trunk encapsulation dot1q
SWT2(config-if-range)#switchport mode trunk
SWT2(config-if-range)#switchport mode dynamic desirable
SWT2(config-if-range)#no shutdown
```

SWT2(config-if-range)#exit
SWT2(config)#end
SWT2#wr

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

DESARROLLO PARTE B PUNTO 2 CASO 3

Se aplica el comando *show interfaces trunk en cada switch* para verificar los enlaces como lo muestras las figuras 23 y 24:

Switch SWT1

```
IOU1#sh int trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       desirable        802.1q         trunking      1
Et0/1       desirable        802.1q         trunking      1
```

Figura 23, trunk en switch 1

Switch SWT2

```
SWT2#sh int trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       desirable        802.1q         trunking      1
Et0/2       desirable        802.1q         trunking      1
```

Figura 24, trunk en switch 2

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

DESARROLLO PARTE B PUNTO 3 CASO 3

En el punto anterior ya fue configurado la interfaz del SWT1, teniendo presente que es la interfaz etehernet 0/1, se procede con la configuración solicitada aplicando el comando *switchport mode trunk* en la interfaz F0/3 y se aplica el siguiente código:

Switch SWT3

SWT3#configure terminal

SWT3(config)#interface range ethernet0/1

SWT3(config-if-range)#switchport trunk encapsulation dot1q Activación del protocolo trunk standar

SWT3(config-if-range)#switchport mode trunk Activación del modo trunk en la interface

SWT3(config-if-range)#no shutdown

SWT3(config-if-range)#exit

SWT3(config)#end

SWT3#wr

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

DESARROLLO PARTE B PUNTO 4 CASO 3

Se verifica el enlace mediante el comando show interfaces trunk en el switch SWT1 como se muestra en la figura 25

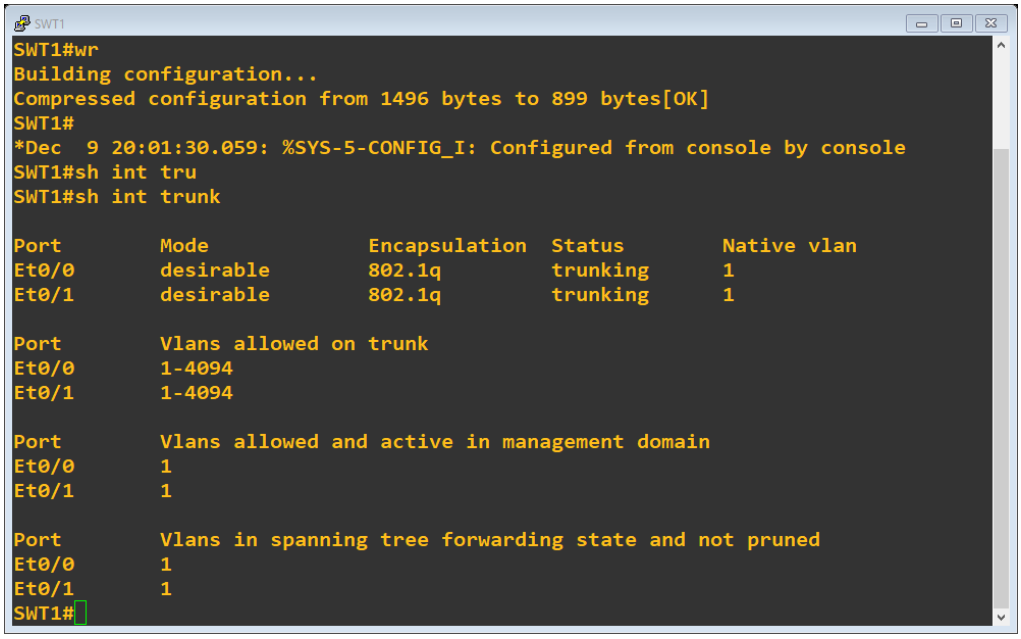

Figura 25, interfaces trunk en switch 1

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

DESARROLLO PARTE B PUNTO 5 CASO 3

Se aplican las siguientes líneas de comando para configurar el enlace teniendo presente que en el SWT2 ya fue configurado en el punto anterior.

Switch SWT3

SWT3#configure terminal
SWT3(config)#interface ethernet0/2
SWT3(config-if-range)#switchport trunk encapsulation dot1q
SWT3(config-if-range)#switchport mode trunk
SWT3(config-if-range)#no shutdown
SWT3(config-if-range)#exit
SWT3(config)#end
SWT3#wr

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)

DESARROLLO PARTE C PUNTO 1 CASO 3

Para crear la VLAN 10 en el switch SWT1 se debe crear en el switch SWT2 ya que es el que funciona en el modo servidor y es en este modo donde se pueden crear o agregar las vlan's, ya que en modo client no es posible. Se aplican las siguientes líneas de comando a fin de agregarlas.

SWT2#configure terminal	
SWT2(config)#vlan 10	Creación de la vlan 10
SWT2(config-vlan)#name Compras	Asignación de nombre
SWT2(config-vlan)#exit	
SWT2(config)#vlan 20	Creación de la vlan 20
SWT2(config-vlan)#name Mercadeo	Asignación de nombre
SWT2(config-vlan)#exit	
SWT2(config)#vlan 30	Creación de la vlan 30
SWT2(config-vlan)#name Planta	Asignación de nombre
SWT2(config-vlan)#exit	
SWT2(config)#vlan 99	Creación de la vlan 99
SWT2(config-vlan)#name Admon	Asignación de nombre
SWT2(config-vlan)#exit	
SWT2(config)#exit	
SWT2#wr	

2. Verifique que las VLANs han sido agregadas correctamente.

DESARROLLO PARTE C PUNTO 2 CASO 3

Para verificar lasVLANS creadas se utiliza el comando **show vlan brief** como se muestra en la figura 26.

SWT2

```
SWT2#sh vlan bri

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/1, Et0/3, Et1/0, Et1/1
                                                Et1/2, Et1/3, Et2/0, Et2/1
                                                Et2/2, Et2/3, Et3/0, Et3/1
                                                Et3/2, Et3/3
10   Compras                          active
20   Mercadeo                         active
30   Planta                           active
99   Admon                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Figura 26, VLANs en switch 2

SWT1

```
SWT1#sh vlan bri

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/2, Et0/3, Et1/0, Et1/1
                                                Et1/2, Et1/3, Et2/0, Et2/1
                                                Et2/2, Et2/3, Et3/0, Et3/1
                                                Et3/2, Et3/3
10   Compras                          active
20   Mercadeo                         active
30   Planta                           active
99   Admon                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Figura 27, VLANs en switch 1

Se constata que en el switch SWT1 ya aparecen las VLAN mediante el comando *show vlan brief* como lo muestra la figura 27.

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

Tabla 5, configuración interfaces y PC's

X = número de cada PC particular

DESARROLLO PARTE C PUNTO 3 CASO 3

Debido que los puertos usados en los switches son diferentes a los que se utilizaron en el laboratorio, se ha creado la tabla de acuerdo a la topología implementada.

Interfaz	VLAN	Direcciones IP de los PCs
E1/0	VLAN 10	190.108.10.1 / 24
E1/1	VLAN 20	190.108.20.2 /24
E1/2	VLAN 30	190.108.30.3 /24
E1/0	VLAN 10	190.108.10.4 / 24
E1/1	VLAN 20	190.108.20.5 /24
E1/2	VLAN 30	190.108.30.6 /24
E1/0	VLAN 10	190.108.10.7 / 24
E1/1	VLAN 20	190.108.20.8 /24
E1/2	VLAN 30	190.108.30.9 /24

Tabla 6, configuración interfaces VLAN y PC's

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

DESARROLLO PARTE C PUNTO 4 CASO 3

Se aplican las siguientes líneas de comando según el switch a configurar para asignar el puerto F0/10 a la VLAN10:

Configuración para el switch SWT1

SWT1#configure terminal

SWT1(config)#interface ethernet 1/0 Ingreso al puerto

SWT1(config-vlan)#switchport mode access Configuración del modo de acceso

SWT1(config-vlan)#switchport access vlan 10 Asinación de la VLAN10 al puerto

SWT1(config-vlan)#exit

Configuración para el switch SWT2

SWT2#configure terminal

SWT2(config)#interface ethernet 1/0 Ingreso al puerto

SWT2(config-vlan)#switchport mode access Configuración del modo de acceso

SWT2(config-vlan)#switchport access vlan 10 Asinación de la VLAN10 al puerto

SWT2(config-vlan)#exit

Configuración para el switch SWT3

SWT3#configure terminal

SWT3(config)#interface ethernet 1/0 Ingreso al puerto

SWT3(config-vlan)#switchport mode access Configuración del modo de acceso

SWT3(config-vlan)#switchport access vlan 10 Asinación de la VLAN10 al puerto

SWT3(config-vlan)#exit

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.

DESARROLLO PARTE C PUNTO 5 CASO 3

Se procede a configurar los puertos a su VLAN asignada correspondientemente:

Configuración para el switch SWT1 de los puertos E1/1-2

SWT1#configure terminal	
SWT1(config)#interface ethernet 1/1	Ingreso al puerto
SWT1(config-vlan)#switchport mode access	Configuración del modo de acceso
SWT1(config-vlan)#switchport access vlan 20	Asinación de la VLAN20 al puerto
SWT1(config-vlan)#exit	
SWT1(config)#interface ethernet 1/2	Ingreso al puerto
SWT1(config-vlan)#switchport mode access	Configuración del modo de acceso
SWT1(config-vlan)#switchport access vlan 30	Asinación de la VLAN30 al puerto
SWT1(config-vlan)#exit	
SWT1(config)#end	
SWT1#wr	Guardado de la configuración

Configuración para el switch SWT2 de los puertos E1/1-2

SWT2#configure terminal	
SWT2(config)#interface ethernet 1/1	Ingreso al puerto
SWT2(config-vlan)#switchport mode access	Configuración del modo de acceso
SWT2(config-vlan)#switchport access vlan 20	Asinación de la VLAN20 al puerto
SWT2(config-vlan)#exit	
SWT2(config)#interface ethernet 1/2	Ingreso al puerto
SWT2(config-vlan)#switchport mode access	Configuración del modo de acceso
SWT2(config-vlan)#switchport access vlan 30	Asinación de la VLAN30 al puerto
SWT2(config-vlan)#exit	

SWT2(config)#end

SWT2#wr Guardado de la configuración

Configuración para el switch SWT3 de los puertos E1/1-2

SWT3#configure terminal

SWT3(config)#interface ethernet 1/1 Ingreso al puerto

SWT3(config-vlan)#switchport mode access Configuración del modo de acceso

SWT3(config-vlan)#switchport access vlan 20 Asinación de la VLAN20 al puerto

SWT3(config-vlan)#exit

SWT3(config)#interface ethernet 1/2 Ingreso al puerto

SWT3(config-vlan)#switchport mode access Configuración del modo de acceso

SWT3(config-vlan)#switchport access vlan 30 Asinación de la VLAN30 al puerto

SWT3(config-vlan)#exit

SWT3(config)#end

SWT3#wr Guardar

Se procede a asignar las IP's correspondientes a las VPC's mediante las líneas de comando según el caso:

Asignación IP a VPC 01

PC-1>ip 190.108.10.1/24

```
PC-1> show

NAME   IP/MASK              GATEWAY           MAC               LPORT  RHOST:PO
RT
PC-1   190.108.10.1/24      0.0.0.0           00:50:79:66:68:00  10013  127.0.0.
1:10014
       fe80::250:79ff:fe66:6800/64
```

Figura 28, configuración ip de pc1

Asignación IP a VPC 02

PC-2>ip 190.108.20.2/24

```
PC-2> sh

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PO
RT
PC-2   190.108.20.2/24      0.0.0.0           00:50:79:66:68:01  10009  127.0.0.
1:10010
       fe80::250:79ff:fe66:6801/64
```

Figura 29, configuración ip de pc2

Asignación IP a VPC 03

PC-3>ip 190.108.30.3/24

```
PC-3> sh

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PO
RT
PC-3   190.108.30.3/24      0.0.0.0           00:50:79:66:68:02  10011  127.0.0.
1:10012
       fe80::250:79ff:fe66:6802/64
```

Figura 30, configuración ip de pc3

Asignación IP a VPC 04

PC-4>ip 190.108.10.4/24

```
PC-4> sh

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PO
RT
PC-4   190.108.10.4/24      0.0.0.0           00:50:79:66:68:03  10015  127.0.0.
1:10016
       fe80::250:79ff:fe66:6803/64
```

Figura 31, configuración ip de pc4

Asignación IP a VPC 05

PC-5>ip 190.108.20.5/24

```
PC-5> sh

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PO
RT
PC-5   190.108.20.5/24      0.0.0.0           00:50:79:66:68:04  10017  127.0.0.
1:10018
       fe80::250:79ff:fe66:6804/64
```

Figura 32, configuración ip de pc5

Asignación IP a VPC 06

PC-6>ip 190.108.30.6/24

```
PC-6> sh

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PO
RT
PC-6   190.108.30.6/24      0.0.0.0           00:50:79:66:68:05  10019  127.0.0.
1:10020
       fe80::250:79ff:fe66:6805/64
```

Figura 33, configuración ip de pc6

Asignación IP a VPC 07

PC-7>ip 190.108.10.7/24

```
PC-7> sh

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PO
RT
PC-7   190.108.10.7/24      0.0.0.0           00:50:79:66:68:06  10021  127.0.0.
1:10022
       fe80::250:79ff:fe66:6806/64
```

Figura 34, configuración ip de pc7

Asignación IP a VPC 08

PC-8>ip 190.108.20.8/24

```
PC-8> sh

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PO
RT
PC-8   190.108.20.8/24      0.0.0.0           00:50:79:66:68:07  10023  127.0.0.
1:10024
       fe80::250:79ff:fe66:6807/64
```

Figura 35, configuración ip de pc8

Asignación IP a VPC 09

PC-9>ip 190.108.30.9/24

```
PC-9> sh

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PO
RT
PC-9   190.108.30.9/24      0.0.0.0           00:50:79:66:68:08  10025  127.0.0.
1:10026
       fe80::250:79ff:fe66:6808/64
```

Figura 36, configuración ip de pc9

En las figuras 28 a 36 se observan que las IP quedan todas configuradas en las VPC's.

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.

...po	Interfaz	Dirección IP	Máscara
...T1	VLAN 99	190.108.99.1	255.255.255.0
...T2	VLAN 99	190.108.99.2	255.255.255.0
...T3	VLAN 99	190.108.99.3	255.255.255.0

Tabla 7, configuración VLAN en los switches

DESARROLLO PARTE D PUNTO 1 CASO 3

Para configurar VLAN99 para el switch SWT1 se aplican las líneas de comando siguientes:

```
SWT1#configure terminal
SWT1(config)#interface vlan 99                    Ingreso a la vlan
SWT1(config-vlan)#ip address 190.108.99.1 255.255.255.0   Configuro
SWT2(config-vlan)#no shutdown
SWT1(config-vlan)#exit
SWT1(config)#end
SWT1#wr                                           Guardar
```

Para configurar VLAN99 para el switch SWT2 se procede de la siguiente forma:

```
SWT2#configure terminal
SWT2(config)#interface vlan 99                    Ingreso a la vlan
SWT2(config-vlan)#ip address 190.108.99.2 255.255.255.0
SWT2(config-vlan)#no shutdown
SWT2(config-vlan)#exit
SWT2(config)#end
SWT2#wr                                                 Guardar
```

Para configurar VLAN99 para el switch SWT3 se procede de la siguiente forma:

```
SWT3#configure terminal
SWT3(config)#interface vlan 99                    Ingreso a la vlan
SWT3(config-vlan)#ip address 190.108.99.3 255.255.255.0
SWT3(config-vlan)#no shutdown
SWT3(config-vlan)#exit
SWT3(config)#end
SWT3#wr                                           Guardar
```

E. Verificar la conectividad Extremo a Extremo

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

VERIFICACIÓN DE CONECTIVIDAD DE EXTREMO A EXTREMO

VERIFICACIÓN DE PING ENTRE PC's									
PC	1	2	3	4	5	6	7	8	9
1	X	NO	NO	**Satisfactorio**	NO	NO	**Satisfactorio**	NO	NO
2	NO	X	NO	NO	**Satisfactorio**	NO	NO	**Satisfac**	NO
3	NO	NO	X	NO	NO	**Satisfactorio**	NO	NO	**Satisfactorio**
4	**Satisfactorio**	NO	NO	X	NO	NO	**Satisfactorio**	NO	NO
5	NO	**Satisfactorio**	NO	NO	X	NO	NO	**Satisfac**	NO
6	NO	NO	**Satisfactorio**	NO	NO	X	NO	NO	**Satisfactorio**
7	**Satisfactorio**	NO	NO	**Satisfactorio**	NO	NO	X	NO	NO
8	NO	**Satisfactorio**	NO	NO	**Satisfactorio**	NO	NO	X	NO
9	NO	NO	**Satisfactorio**	NO	NO	**Satisfactorio**	NO	NO	X

Tabla 8, verificación de ping entre equipos

En las figuras 37 y 45 se puede constatar la conectividad de extremo a extremo.

PC1

Ping entre PC1 y PC4, PC1 y PC7

```
PC-1> ping 190.108.10.4
84 bytes from 190.108.10.4 icmp_seq=1 ttl=64 time=3.890 ms
84 bytes from 190.108.10.4 icmp_seq=2 ttl=64 time=3.885 ms
84 bytes from 190.108.10.4 icmp_seq=3 ttl=64 time=3.877 ms
84 bytes from 190.108.10.4 icmp_seq=4 ttl=64 time=3.898 ms
84 bytes from 190.108.10.4 icmp_seq=5 ttl=64 time=3.865 ms

PC-1> ping 190.108.10.7
84 bytes from 190.108.10.7 icmp_seq=1 ttl=64 time=3.909 ms
84 bytes from 190.108.10.7 icmp_seq=2 ttl=64 time=3.909 ms
84 bytes from 190.108.10.7 icmp_seq=3 ttl=64 time=0.000 ms
84 bytes from 190.108.10.7 icmp_seq=4 ttl=64 time=3.896 ms
84 bytes from 190.108.10.7 icmp_seq=5 ttl=64 time=0.000 ms
```

Figura 37, verificación de ping

Ping entre PC1 a PC2, PC5, PC8

```
PC-1> ping 190.108.20.2
No gateway found

PC-1> ping 190.108.20.5
No gateway found

PC-1> ping 190.108.20.8
No gateway found
```

Figura 38, verificación de ping

Ping entre PC1 a PC3, PC6, PC9

```
PC-1> ping 190.108.30.3
No gateway found

PC-1> ping 190.108.30.6
No gateway found

PC-1> ping 190.108.30.9
No gateway found
```

Figura 39, verificación de ping

Observaciones:

No es posible realizar ping con las PC's que pertenecen a otra VLAN diferente a la VLAN 10, ya que este sistema busca aislar el tráfico de un segmento de la red promoviendo mayor velocidad y seguridad en la información.

PC2

Ping entre PC2 y PC5, PC1 y PC8

```
PC-2> ping 190.108.20.5
84 bytes from 190.108.20.5 icmp_seq=1 ttl=64 time=0.000 ms
84 bytes from 190.108.20.5 icmp_seq=2 ttl=64 time=0.000 ms
84 bytes from 190.108.20.5 icmp_seq=3 ttl=64 time=0.000 ms
84 bytes from 190.108.20.5 icmp_seq=4 ttl=64 time=0.000 ms
84 bytes from 190.108.20.5 icmp_seq=5 ttl=64 time=0.000 ms

PC-2> ping 190.108.20.8
84 bytes from 190.108.20.8 icmp_seq=1 ttl=64 time=3.865 ms
84 bytes from 190.108.20.8 icmp_seq=2 ttl=64 time=3.865 ms
84 bytes from 190.108.20.8 icmp_seq=3 ttl=64 time=3.883 ms
84 bytes from 190.108.20.8 icmp_seq=4 ttl=64 time=3.922 ms
84 bytes from 190.108.20.8 icmp_seq=5 ttl=64 time=3.881 ms
```

Figura 40, verificación de ping

Ping entre PC2 a PC1, PC4, PC7

```
PC-2> ping 190.108.10.1
No gateway found

PC-2> ping 190.108.10.4
No gateway found

PC-2> ping 190.108.10.7
No gateway found
```

Figura 41, verificación de ping

Ping entre PC2 a PC3, PC6, PC9

```
PC-2> ping 190.108.30.3
No gateway found

PC-2> ping 190.108.30.6
No gateway found

PC-2> ping 190.108.30.9
No gateway found
```

Figura 42, verificación de ping

Observaciones:

No es posible realizar ping con las PC's que pertenecen a otra VLAN diferente a la VLAN 20, ya que este sistema busca aislar el tráfico de un segmento de la red promoviendo mayor velocidad y seguridad en la información.

PC3

Ping entre PC3 y PC6, PC1 y PC9

```
PC-3> ping 190.108.30.6
84 bytes from 190.108.30.6 icmp_seq=1 ttl=64 time=3.885 ms
84 bytes from 190.108.30.6 icmp_seq=2 ttl=64 time=3.883 ms
84 bytes from 190.108.30.6 icmp_seq=3 ttl=64 time=3.922 ms
84 bytes from 190.108.30.6 icmp_seq=4 ttl=64 time=3.882 ms
84 bytes from 190.108.30.6 icmp_seq=5 ttl=64 time=0.000 ms

PC-3> ping 190.108.30.9
84 bytes from 190.108.30.9 icmp_seq=1 ttl=64 time=0.000 ms
84 bytes from 190.108.30.9 icmp_seq=2 ttl=64 time=0.000 ms
84 bytes from 190.108.30.9 icmp_seq=3 ttl=64 time=0.000 ms
84 bytes from 190.108.30.9 icmp_seq=4 ttl=64 time=0.000 ms
84 bytes from 190.108.30.9 icmp_seq=5 ttl=64 time=0.000 ms
```

Figura 43, verificación de ping

Ping entre PC3 a PC1, PC4, PC7

```
PC-3> ping 190.108.10.1
No gateway found

PC-3> ping 190.108.10.4
No gateway found

PC-3> ping 190.108.10.7
No gateway found
```

Figura 44, verificación de ping

Ping entre PC3 a PC2, PC5, PC8

```
PC-3> ping 190.108.20.2
No gateway found

PC-3> ping 190.108.20.5
No gateway found

PC-3> ping 190.108.20.8
No gateway found
```

Figura 45, verificación de ping

Observaciones:

No es posible realizar ping con las PC's que pertenecen a otra VLAN diferente a la VLAN 30, ya que este sistema busca aislar el tráfico de un segmento de la red promoviendo mayor velocidad y seguridad en la información.

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

RESPUESTA PREGUNTA 2 PARTE E CASO 3

Este switch no es de capa 3, no tiene capacidades de routing.

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

RESPUESTA PREGUNTA 3 PARTE E CASO 3

Debido a que no son switches de capa 3, el switch no puede realizar ping a los pc y no tiene sentido hacerlo.

CONCLUSIONES

- El comando *redistrubte* permite que diferentes protocolos de ruteo que son los encargados de que cada paquete de Información llege a su correcto destino puedan compartir información y cominicar hosts a pesar de no estar configurdos con el mismo protocol.
- El escenario 3 muestra los veneficios de utilizar VLAN en redes, tales como garantizar seguridad de datos sensibles que pueden ser separados del resto de la red, reducción del tráfico innecesario en la red.
- BGP es un protocolo de routing path vector.
- En el escenario 2 evidencia la utilidad de BGP al permitir intecambiar información de encaminamiento entre sistemas autónomos.

BIBLIOGRAFÍA

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx

Cisco. (2018). Cisco Networking Academy. *Packet Tracer: Configuring IPv6 ACLs*

Cisco Networking Academy. (s.f.). *Capítulo 7: Routing dinámico.* Recuperado el 15 de Noviembre de 2017, de UNIDAD 4 Enrutamiento en soluciones de red. Disponible en https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

Cisco Networking Academy, (s.f.). *Capítulo 9: Listas de control de acceso.* Recuperado el 15 de Noviembre de 2017, de UNIDAD 4 Enrutamiento en soluciones de red. Disponible en https://static-course assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

UNAD (2015). Introducción a la configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC