

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JORGE ARMANDO SOTO GARCÍA

**Universidad Nacional Abierta y a Distancia UNAD
Escuela de Ciencias Básicas Tecnología e Ingeniería – ECBTI
Programa de Ingeniería de Telecomunicaciones
Bogotá D.C.
2019**

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JORGE ARMANDO SOTO GARCÍA

**Informe de prueba de habilidades prácticas del Diplomado de Profundización
Cisco CCNP para optar al título de Ingeniero de Telecomunicaciones**

Director: Ing. GERARDO GRANADOS ACUÑA MSc.

**Universidad Nacional Abierta y a Distancia UNAD
Escuela de Ciencias Básicas Tecnología e Ingeniería – ECBTI
Programa de Ingeniería de Telecomunicaciones
Bogotá D.C.
2019**

CONTENIDO

	pág.
0. INTRODUCCIÓN	10
1. PRUEBA DE HABILIDADES PRÁCTICAS CCNP	11
1.1 ESCENARIO #1	11
1.2 ESCENARIO #2	24
1.3 ESCENARIO #3	36
CONCLUSIONES	60
BIBLIOGRAFÍA	61

LISTA DE FIGURAS

	pág.
Figura 1. Escenario 1	11
Figura 2. Topología implementada para el escenario 1	11
Figura 3. Escenario 1 - Direccionamiento IP implementado en R1	14
Figura 4. Escenario 1 - Direccionamiento IP implementado en R2	14
Figura 5. Escenario 1 - Direccionamiento IP implementado en R3	14
Figura 6. Escenario 1 - Direccionamiento IP implementado en R4	14
Figura 7. Escenario 1 - Direccionamiento IP implementado en R5	14
Figura 8. Escenario 1 - Rutas OSPF aprendidas en R1	15
Figura 9. Escenario 1 - Rutas OSPF aprendidas en R2	15
Figura 10. Escenario 1 - Rutas OSPF aprendidas en R3	15
Figura 11. Escenario 1 - Rutas OSPF aprendidas en R4	16
Figura 12. Escenario 1 - Rutas OSPF aprendidas en R5	16
Figura 13. Escenario 1 – Interfaces loopback en R1	17
Figura 14. Escenario 1 – Verificación de interfaces loopback participantes en proceso OSPF en R1	17
Figura 15. Escenario 1 – Interfaces loopback en R5	18
Figura 16. Escenario 1 – Verificación de interfaces loopback participantes en proceso EIGRP en R5	18
Figura 17. Escenario 1 – Verificación de nuevas interfaces loopback aprendidas en R3	19
Figura 18. Escenario 1 – Interfaces loopback aprendidas como ruta de red /24 en R3	20

Figura 19. Escenario 1 – Verificación de aprendizaje de rutas OSPF redistribuidas en R1	21
Figura 20. Escenario 1 – Verificación de aprendizaje de rutas EIGRP redistribuidas en R5	21
Figura 21. Escenario 1 – Tabla de enrutamiento final en R1	22
Figura 22. Escenario 1 – Tabla de enrutamiento final en R1	23
Figura 23. Escenario 1 – Ping exitoso desde R1 hacia R5	23
Figura 24. Escenario 1 – Ping exitoso desde R5 hacia R1	23
Figura 25. Escenario 2	24
Figura 26. Topología implementada para el escenario 2	25
Figura 27. Escenario 2 - Direccionamiento IP implementado en R1	26
Figura 28. Escenario 2 - Direccionamiento IP implementado en R2	27
Figura 29. Escenario 2 - Direccionamiento IP implementado en R3	27
Figura 30. Escenario 2 - Direccionamiento IP implementado en R4	27
Figura 31. Escenario 2 - Rutas BGP aprendidas en R1	28
Figura 32. Escenario 2 - Rutas BGP aprendidas en R2	28
Figura 33. Escenario 2 – BGP router ID y rutas BGP consolidadas en R1	28
Figura 34. Escenario 2 – BGP router ID y rutas BGP consolidadas en R2	29
Figura 35. Escenario 2 - Rutas BGP de R3 añadidas en R2	30
Figura 36. Escenario 2 - Rutas BGP aprendidas en R3	30
Figura 37. Escenario 2 – BGP router ID y rutas BGP consolidadas en R2	31
Figura 38. Escenario 2 – BGP router ID y rutas BGP consolidadas en R3	31
Figura 39. Escenario 2 - Rutas BGP aprendidas en R1	32
Figura 40. Escenario 2 - Rutas BGP aprendidas en R2	33

Figura 41. Escenario 2 - Rutas BGP aprendidas en R3	33
Figura 42. Escenario 2 - Rutas BGP aprendidas en R4	34
Figura 43. Escenario 2 – BGP router ID y rutas BGP consolidadas en R1	34
Figura 44. Escenario 2 – BGP router ID y rutas BGP consolidadas en R2	35
Figura 45. Escenario 2 – BGP router ID y rutas BGP consolidadas en R3	35
Figura 46. Escenario 2 – BGP router ID y rutas BGP consolidadas en R4	35
Figura 47. Escenario 3	36
Figura 48. Topología implementada para el escenario 3	36
Figura 49. Escenario 3 – Estado de VTP en SW1	37
Figura 50. Escenario 3 – Estado de VTP en SW2	38
Figura 51. Escenario 3 – Estado de VTP en SW3	38
Figura 52. Escenario 3 – Estado de enlaces troncales en SW1	39
Figura 53. Escenario 3 – Estado de enlaces troncales en SW2	39
Figura 54. Escenario 3 – Estado de enlaces troncales en SW1	40
Figura 55. Escenario 3 – Configuración de interfaz f0/3 en SW2 para enlace troncal	40
Figura 56. Escenario 3 – Error al agregar VLAN en VTP cliente en SW1	41
Figura 57. Escenario 3 – Verificación de VLAN en SW2	41
Figura 58. Escenario 3 – Verificación de VLAN en SW1	42
Figura 59. Escenario 3 – Verificación de VLAN en SW3	42
Figura 60. Escenario 3 – Verificación de conectividad entre PCs VLAN Compras	45
Figura 61. Escenario 3 – Verificación de conectividad entre VLAN Compras y VLAN Mercadeo	46

Figura 62. Escenario 3 – Verificación de conectividad entre VLAN Compras y VLAN Planta	47
Figura 63. Escenario 3 – Verificación de conectividad entre PCs VLAN Mercadeo	48
Figura 64. Escenario 3 – Verificación de conectividad entre VLAN Mercadeo y VLAN Compras	49
Figura 65. Escenario 3 – Verificación de conectividad entre VLAN Mercadeo y VLAN Planta	50
Figura 66. Escenario 3 – Verificación de conectividad entre PCs VLAN Planta	51
Figura 67. Escenario 3 – Verificación de conectividad entre VLAN Planta y VLAN Compras	52
Figura 68. Escenario 3 – Verificación de conectividad entre VLAN Mercadeo y VLAN Compras	53
Figura 69. Escenario 3 – Verificación de conectividad entre switches desde SW1	54
Figura 70. Escenario 3 – Verificación de conectividad entre switches desde SW1	54
Figura 71. Escenario 3 – Verificación de conectividad entre switches desde SW1	54
Figura 72. Escenario 3 – Verificación de conectividad desde SW1 a VLAN Compras	55
Figura 73. Escenario 3 – Verificación de conectividad desde SW1 a VLAN Mercadeo	56
Figura 74. Escenario 3 – Verificación de conectividad desde SW1 a VLAN Planta	56
Figura 75. Escenario 3 – Verificación de conectividad desde SW2 a VLAN Compras	57
Figura 76. Escenario 3 – Verificación de conectividad desde SW2 a VLAN Mercadeo	57

Figura 77. Escenario 3 – Verificación de conectividad desde SW2 a VLAN Mercadeo	58
Figura 78. Escenario 3 – Verificación de conectividad desde SW3 a VLAN Compras	58
Figura 79. Escenario 3 – Verificación de conectividad desde SW3 a VLAN Mercadeo	59
Figura 80. Escenario 3 – Verificación de conectividad desde SW3 a VLAN Planta	59

LISTA DE TABLAS

	pág.
Tabla 1. Escenario 2 - Direccionamiento IP a configurar en enrutadores	24
Tabla 2. Escenario 3 - Configuración de PCs e interfaces del <i>switch</i>	42
Tabla 3. Escenario 3 - Configuración de PCs e interfaces en SW1, SW2 y SW3	44
Tabla 4. Escenario 3 - Configuración de SVI para VLAN de administración en SW1, SW2 y SW3	44

0. INTRODUCCIÓN

El currículo y certificación CCNP R&S (*Cisco Certified Network Professional Routing and Switching*) ofrecido por Cisco Systems complementa varios conceptos teóricos de enrutamiento y conmutación (switching) tratados desde el currículo CCNA precedente, lo cual permite revisar, apropiar conceptos y realizar prácticas de nivel avanzado en temas tales como protocolos de enrutamiento, conmutación, IPv6, MPLS, entre otros.

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNP, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de *networking*.

1. PRUEBA DE HABILIDADES PRÁCTICAS CCNP

1.1 ESCENARIO #1

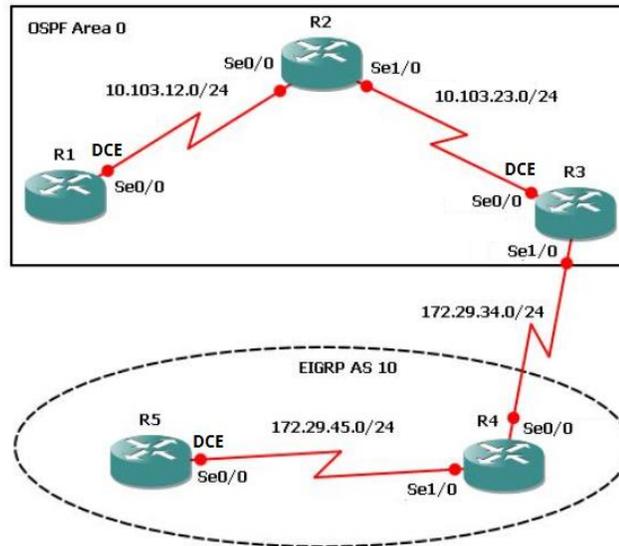


Figura 1. Escenario 1. Tomado de https://1drv.ms/w/s!AgIGg5JUgUBthGdCOlggFa_kkWCT

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.

Topología base implementada (Software: Cisco Packet Tracer v7.2.1.0128):

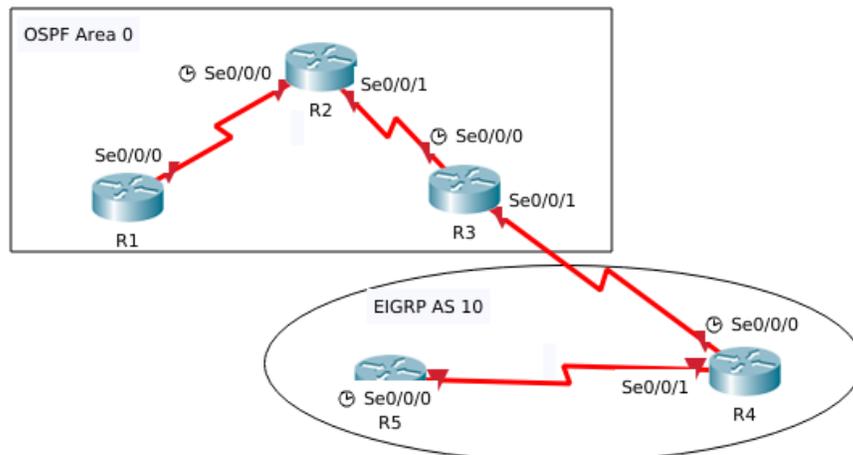


Figura 2. Topología implementada para el escenario 1. Elaboración propia.

```
Router>enable
Router#configure terminal
Router (config) #hostname R1
R1 (config) #interface serial 0/0/0
R1 (config-if) #ip address 10.103.12.1 255.255.255.0
R1 (config-if) #no shutdown
R1 (config-if) #exit
R1 (config) #router ospf 1
R1 (config-router) #network 10.103.12.0 0.0.0.255 area 0
R1 (config-router) #network 10.103.23.0 0.0.0.255 area 0
R1 (config-router) #do wr
R1 (config-router) #end
```

```
Router>enable
Router#configure terminal
Router (config) #hostname R2
R2 (config) #interface serial 0/0/0
R2 (config-if) #ip address 10.103.12.2 255.255.255.0
R2 (config-if) #clock rate 64000
R2 (config-if) #no shutdown
R2 (config-if) #exit
R2 (config) #interface serial 0/0/1
R2 (config-if) #ip address 10.103.23.1 255.255.255.0
R2 (config-if) #no shutdown
R2 (config-if) #exit
R2 (config) #router ospf 1
R2 (config-router) #network 10.103.12.0 0.0.0.255 area 0
R2 (config-router) #network 10.103.23.0 0.0.0.255 area 0
R2 (config-router) #do wr
R2 (config-router) #end
```

```
Router>enable
Router#configure terminal
Router (config) #hostname R3
R3 (config) #interface serial 0/0/0
R3 (config-if) #ip address 10.103.23.2 255.255.255.0
R3 (config-if) #clock rate 64000
R3 (config-if) #no shutdown
R3 (config-if) #exit
R3 (config) #interface serial 0/0/1
R3 (config-if) #ip address 172.29.34.1 255.255.255.0
R3 (config-if) #no shutdown
R3 (config-if) #exit
R3 (config) #router ospf 1
```

```
R3 (config-router) #network 10.103.12.0 0.0.0.255 area 0
R3 (config-router) #network 10.103.23.0 0.0.0.255 area 0
R3 (config-router) #exit
R3 (config) #router eigrp 10
R4 (config-router) #network 172.29.45.0 0.0.0.255
R4 (config-router) #network 172.29.34.0 0.0.0.255
R3 (config-router) #do wr
R3 (config-router) #end
```

```
Router>enable
Router#configure terminal
Router (config) #hostname R4
R4 (config) #interface serial 0/0/0
R4 (config-if) #ip address 172.29.34.2 255.255.255.0
R4 (config-if) #clock rate 64000
R4 (config-if) #no shutdown
R4 (config-if) #exit
R4 (config) #interface serial 0/0/1
R4 (config-if) #ip address 172.29.45.1 255.255.255.0
R4 (config-if) #no shutdown
R4 (config-if) #exit
R4 (config) #router eigrp 10
R4 (config-router) #network 172.29.45.0 0.0.0.255
R4 (config-router) #network 172.29.34.0 0.0.0.255
R4 (config-router) #do wr
R4 (config-router) #end
```

```
Router>enable
Router#configure terminal
Router (config) #hostname R5
R5 (config) #interface serial 0/0/0
R5 (config-if) #ip address 172.29.45.2 255.255.255.0
R5 (config-if) #clock rate 64000
R5 (config-if) #no shutdown
R5 (config-if) #exit
R5 (config) #router eigrp 10
R5 (config-router) #network 172.29.45.0 0.0.0.255
R5 (config-router) #network 172.29.34.0 0.0.0.255
R5 (config-router) #do wr
R5 (config-router) #end
```

Verificación de direccionamiento implementado:

```
R1>sh ip int br
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0 unassigned      YES unset  administratively down  down
GigabitEthernet0/1 unassigned      YES unset  administratively down  down
Serial0/0/0        10.103.12.1    YES manual up                up
Serial0/0/1        unassigned      YES unset  administratively down  down
Vlan1              unassigned      YES unset  administratively down  down
```

Figura 3. Escenario 1 - Direccionamiento IP implementado en R1. Elaboración propia.

```
R2>sh ip int br
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0 unassigned      YES unset  administratively down  down
GigabitEthernet0/1 unassigned      YES unset  administratively down  down
Serial0/0/0        10.103.12.2    YES manual up                up
Serial0/0/1        10.103.23.1    YES manual up                up
Vlan1              unassigned      YES unset  administratively down  down
```

Figura 4. Escenario 1 - Direccionamiento IP implementado en R2. Elaboración propia.

```
R3>sh ip int br
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0 unassigned      YES unset  administratively down  down
GigabitEthernet0/1 unassigned      YES unset  administratively down  down
Serial0/0/0        10.103.23.2    YES manual up                up
Serial0/0/1        172.29.34.1    YES manual up                up
Vlan1              unassigned      YES unset  administratively down  down
```

Figura 5. Escenario 1 - Direccionamiento IP implementado en R3. Elaboración propia.

```
R4>sh ip int br
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0 unassigned      YES unset  administratively down  down
GigabitEthernet0/1 unassigned      YES unset  administratively down  down
Serial0/0/0        172.29.34.2    YES manual up                up
Serial0/0/1        172.29.45.1    YES manual up                up
Vlan1              unassigned      YES unset  administratively down  down
```

Figura 6. Escenario 1 - Direccionamiento IP implementado en R4. Elaboración propia.

```
R5>sh ip int br
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0 unassigned      YES unset  administratively down  down
GigabitEthernet0/1 unassigned      YES unset  administratively down  down
Serial0/0/0        172.29.45.2    YES manual up                up
Serial0/0/1        unassigned      YES unset  administratively down  down
Vlan1              unassigned      YES unset  administratively down  down
```

Figura 7. Escenario 1 - Direccionamiento IP implementado en R5. Elaboración propia.

Verificación de enrutamiento implementado:

```
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, 3 subnets, 2 masks
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, 02:19:35, Serial0/0/0
```

Figura 8. Escenario 1 - Rutas OSPF aprendidas en R1. Elaboración propia.

```
R2>sh 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, 4 subnets, 2 masks
C    10.103.12.0/24 is directly connected, Serial0/0/0
L    10.103.12.2/32 is directly connected, Serial0/0/0
C    10.103.23.0/24 is directly connected, Serial0/0/1
L    10.103.23.1/32 is directly connected, Serial0/0/1
```

Figura 9. Escenario 1 - Rutas OSPF aprendidas en R2. Elaboración propia.

```
R3>sh 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, 3 subnets, 2 masks
O    10.103.12.0/24 [110/128] via 10.103.23.1, 02:20:04, Serial0/0/0
C    10.103.23.0/24 is directly connected, Serial0/0/0
L    10.103.23.2/32 is directly connected, Serial0/0/0
172.29.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.29.34.0/24 is directly connected, Serial0/0/1
L    172.29.34.1/32 is directly connected, Serial0/0/1
```

Figura 10. Escenario 1 - Rutas OSPF aprendidas en R3. Elaboración propia.

```

R4#sh 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

      172.29.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       172.29.34.0/24 is directly connected, Serial0/0/0
L       172.29.34.2/32 is directly connected, Serial0/0/0
C       172.29.45.0/24 is directly connected, Serial0/0/1
L       172.29.45.1/32 is directly connected, Serial0/0/1

```

Figura 11. Escenario 1 - Rutas OSPF aprendidas en R4. Elaboración propia.

```

R5#sh 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

      172.29.0.0/16 is variably subnetted, 3 subnets, 2 masks
D       172.29.34.0/24 [90/2681856] via 172.29.45.1, 00:04:05, Serial0/0/0
C       172.29.45.0/24 is directly connected, Serial0/0/0
L       172.29.45.2/32 is directly connected, Serial0/0/0

```

Figura 12. Escenario 1 - Rutas OSPF aprendidas en R5. Elaboración propia.

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.

```

R1#configure terminal
R1(config)#interface lo0
R1(config-if)#ip address 10.1.0.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface lo1
R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface lo2
R1(config-if)#ip address 10.1.2.1 255.255.255.0
R1(config-if)#exit
R1(config)#interface lo3
R1(config-if)#ip address 10.1.3.1 255.255.255.0
R1(config-if)#exit

```

```

R1 (config) #router ospf 1
R1 (config-router) #network 10.1.0.0 0.0.3.255 area 0
R1 (config-router) #end

```

Verificación de interfaces *loopback*:

```

R1#sh ip int brief | include Loopback
Loopback0          10.1.0.1          YES manual up      up
Loopback1          10.1.1.1          YES manual up      up
Loopback2          10.1.2.1          YES manual up      up
Loopback3          10.1.3.1          YES manual up      up

```

Figura 13. Escenario 1 – Interfaces *loopback* en R1. Elaboración propia.

Verificación de participación de interfaces *loopback* en proceso OSPF:

```

R1#show ip ospf interface

Serial0/0/0 is up, line protocol is up
 Internet address is 10.103.12.1/24, Area 0
 Process ID 1, Router ID 10.103.12.1, Network Type POINT-TO-POINT, Cost: 64
 Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:02
 Index 1/1, flood queue length 0
 Next 0x0(0)/0x0(0)
 Last flood scan length is 1, maximum is 1
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 1 , Adjacent neighbor count is 1
   Adjacent with neighbor 10.103.12.2
 Suppress hello for 0 neighbor(s)
Loopback0 is up, line protocol is up
 Internet address is 10.1.0.1/24, Area 0
 Process ID 1, Router ID 10.103.12.1, Network Type LOOPBACK, Cost: 1
 Loopback interface is treated as a stub Host
Loopback1 is up, line protocol is up
 Internet address is 10.1.1.1/24, Area 0
 Process ID 1, Router ID 10.103.12.1, Network Type LOOPBACK, Cost: 1
 Loopback interface is treated as a stub Host
Loopback2 is up, line protocol is up
 Internet address is 10.1.2.1/24, Area 0
 Process ID 1, Router ID 10.103.12.1, Network Type LOOPBACK, Cost: 1
 Loopback interface is treated as a stub Host
Loopback3 is up, line protocol is up
 Internet address is 10.1.3.1/24, Area 0
 Process ID 1, Router ID 10.103.12.1, Network Type LOOPBACK, Cost: 1
 Loopback interface is treated as a stub Host

```

Figura 14. Escenario 1 – Verificación de interfaces *loopback* participantes en proceso OSPF en R1. Elaboración propia.

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.

```
R5#configure terminal
R5 (config) #interface lo0
R5 (config-if) #ip address 172.5.0.1 255.255.255.0
R5 (config-if) #exit
R5 (config) #interface lo1
R5 (config-if) #ip address 172.5.1.1 255.255.255.0
R5 (config-if) #exit
R5 (config) #interface lo2
R5 (config-if) #ip address 172.5.2.1 255.255.255.0
R5 (config-if) #exit
R5 (config) #interface lo3
R5 (config-if) #ip address 172.5.3.1 255.255.255.0
R5 (config-if) #exit
R5 (config) #router eigrp 10
R5 (config-router) #network 172.5.0.0 0.0.3.255
R5 (config-router) #end
```

Verificación de interfaces *loopback*:

```
R5#sh ip int br | include Loopback
Loopback0      172.5.0.1      YES manual up      up
Loopback1      172.5.1.1      YES manual up      up
Loopback2      172.5.2.1      YES manual up      up
Loopback3      172.5.3.1      YES manual up      up
```

Figura 15. Escenario 1 – Interfaces *loopback* en R5. Elaboración propia.

Verificación participación de interfaces *loopback* en proceso EIGRP:

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

Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Se0/0/0	1	0/0	1236	0/10	0	0
Lo0	0	0/0	1236	0/10	0	0
Lo1	0	0/0	1236	0/10	0	0
Lo2	0	0/0	1236	0/10	0	0
Lo3	0	0/0	1236	0/10	0	0

Figura 16. Escenario 1 – Verificación de interfaces *loopback* participantes en proceso EIGRP en R5. Elaboración propia.

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*.

```
R3>sh 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, 7 subnets, 2 masks
O       10.1.0.1/32 [110/129] via 10.103.23.1, 00:00:27, Serial0/0/0
O       10.1.1.1/32 [110/129] via 10.103.23.1, 00:00:02, Serial0/0/0
O       10.1.2.1/32 [110/129] via 10.103.23.1, 00:00:02, Serial0/0/0
O       10.1.3.1/32 [110/129] via 10.103.23.1, 00:00:02, Serial0/0/0
O       10.103.12.0/24 [110/128] via 10.103.23.1, 04:04:29, Serial0/0/0
C       10.103.23.0/24 is directly connected, Serial0/0/0
L       10.103.23.2/32 is directly connected, Serial0/0/0
    172.5.0.0/24 is subnetted, 4 subnets
D       172.5.0.0/24 [90/2809856] via 172.29.34.2, 00:18:31, Serial0/0/1
D       172.5.1.0/24 [90/2809856] via 172.29.34.2, 00:18:31, Serial0/0/1
D       172.5.2.0/24 [90/2809856] via 172.29.34.2, 00:18:31, Serial0/0/1
D       172.5.3.0/24 [90/2809856] via 172.29.34.2, 00:18:31, Serial0/0/1
    172.29.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.29.34.0/24 is directly connected, Serial0/0/1
L       172.29.34.1/32 is directly connected, Serial0/0/1
D       172.29.45.0/24 [90/2681856] via 172.29.34.2, 00:18:31, Serial0/0/1
```

Figura 17. Escenario 1 – Verificación de nuevas interfaces loopback aprendidas en R3. Elaboración propia.

Se realiza la verificación de la tabla de enrutamiento en R3. Se evidencia que fueron aprendidas las rutas hacia las interfaces loopback creadas en R1 y propagadas mediante OSPF, así como las interfaces loopback creadas en R5 y propagadas a través de EIGRP. Se evidencia también que las interfaces loopback en R1 publicadas mediante OSPF están participando como rutas de host (/32) y no de red, por lo tanto, se debe cambiar el tipo de red por defecto, de loopback a punto-a-punto:

```
R1#configure terminal
R1 (config) #interface lo0
R1 (config-if) #ip ospf network point-to-point
R1 (config-if) #exit
R1 (config) #interface lo1
R1 (config-if) # ip ospf network point-to-point
R1 (config-if) #exit
R1 (config) #interface lo2
R1 (config-if) # ip ospf network point-to-point
```

```

R1 (config-if) #exit
R1 (config) #interface lo3
R1 (config-if) # ip ospf network point-to-point
R1 (config-if) #exit

```

Se realiza nueva verificación, encontrando que en la tabla de enrutamiento de R3 las interfaces *loopback* de R1 se muestran como rutas de red /24 y no de *host* /32:

```

R3#sh 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, 7 subnets, 2 masks
O       10.1.0.0/24 [110/129] via 10.103.23.1, 00:15:02, Serial0/0/0
O       10.1.1.0/24 [110/129] via 10.103.23.1, 00:14:52, Serial0/0/0
O       10.1.2.0/24 [110/129] via 10.103.23.1, 00:14:36, Serial0/0/0
O       10.1.3.0/24 [110/129] via 10.103.23.1, 00:14:26, Serial0/0/0
O       10.103.12.0/24 [110/128] via 10.103.23.1, 03:52:35, Serial0/0/0
C       10.103.23.0/24 is directly connected, Serial0/0/0
L       10.103.23.2/32 is directly connected, Serial0/0/0
    172.5.0.0/24 is subnetted, 4 subnets
D       172.5.0.0/24 [90/2809856] via 172.29.34.2, 00:06:37, Serial0/0/1
D       172.5.1.0/24 [90/2809856] via 172.29.34.2, 00:06:37, Serial0/0/1
D       172.5.2.0/24 [90/2809856] via 172.29.34.2, 00:06:37, Serial0/0/1
D       172.5.3.0/24 [90/2809856] via 172.29.34.2, 00:06:37, Serial0/0/1
    172.29.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.29.34.0/24 is directly connected, Serial0/0/1
L       172.29.34.1/32 is directly connected, Serial0/0/1
D       172.29.45.0/24 [90/2681856] via 172.29.34.2, 00:06:37, Serial0/0/1

```

Figura 18. Escenario 1 – Interfaces *loopback* aprendidas como ruta de red /24 en R3. Elaboración propia.

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

En primer lugar se realiza la redistribución de rutas EIGRP dentro de OSPF con los parámetros indicados:

```

R3#configure terminal
R3 (config) #router ospf 1
R3 (config-router) #redistribute eigrp 10 metric 50000 subnets
R3 (config-router) #end

```

Se verifica la tabla de enrutamiento en R1. Posterior a la ejecución del comando de redistribución, R1 debe haber aprendido las rutas hacia las redes o interfaces publicadas en R5 a través de EIGRP, y aparecen como rutas OSPF Externas tipo 2 (O E2):

```

R1#sh ip route ospf
    10.0.0.0/8 is variably subnetted, 11 subnets, 2 masks
O    10.103.23.0 [110/128] via 10.103.12.2, 04:22:37, Serial0/0/0
    172.5.0.0/24 is subnetted, 4 subnets
O E2  172.5.0.0 [110/50000] via 10.103.12.2, 00:07:12, Serial0/0/0
O E2  172.5.1.0 [110/50000] via 10.103.12.2, 00:07:12, Serial0/0/0
O E2  172.5.2.0 [110/50000] via 10.103.12.2, 00:07:12, Serial0/0/0
O E2  172.5.3.0 [110/50000] via 10.103.12.2, 00:07:12, Serial0/0/0
    172.29.0.0/24 is subnetted, 2 subnets
O E2  172.29.34.0 [110/50000] via 10.103.12.2, 00:07:12, Serial0/0/0
O E2  172.29.45.0 [110/50000] via 10.103.12.2, 00:07:12, Serial0/0/0

```

Figura 19. Escenario 1 – Verificación de aprendizaje de rutas OSPF redistribuidas en R1. Elaboración propia.

Posteriormente, se realiza la redistribución de rutas OSPF dentro de EIGRP con los parámetros indicados (el ancho de banda para una conexión T1 es de 1544 Mbps) con la estructura típica de las métricas K: OSPF>Area>Metrica>BW>Retardo (en unidades de 10 ms)>Confiabilidad>BW Efectivo>MTU:

```

R3#configure terminal
R3 (config) #router eigrp 10
R3 (config-router) #redistribute ospf 1 metric 1544 2000 255 1
1500
R3 (config-router) #end

```

Se verifica la tabla de enrutamiento en R5. Posterior a la ejecución del comando de redistribución, R5 debe haber aprendido las rutas hacia las redes o interfaces publicadas en R1 a través de OSPF, y aparecen como rutas EIGRP Externas (D EX):

```

R5>sh ip route | include EX
    D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
D EX  10.1.0.1/32 [170/3193856] via 172.29.45.1, 00:02:04, Serial0/0/0
D EX  10.1.1.1/32 [170/3193856] via 172.29.45.1, 00:02:04, Serial0/0/0
D EX  10.1.2.1/32 [170/3193856] via 172.29.45.1, 00:02:04, Serial0/0/0
D EX  10.1.3.1/32 [170/3193856] via 172.29.45.1, 00:02:04, Serial0/0/0
D EX  10.103.12.0/24 [170/3193856] via 172.29.45.1, 00:02:04, Serial0/0/0
D EX  10.103.23.0/24 [170/3193856] via 172.29.45.1, 00:02:04, Serial0/0/0

```

Figura 20. Escenario 1 – Verificación de aprendizaje de rutas EIGRP redistribuidas en R5. Elaboración propia.

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*.

Se observan la salida completa del comando *show ip route* en R1 y R5, donde se evidencia la correcta configuración de redistribución de rutas, ya que los sistemas autónomos publicados en OSPF y EIGRP son reconocidos por su opuesto en el extremo de la red:

Tabla de enrutamiento completa en R1:

```
R1>sh 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, Loopback0
L       10.1.0.1/32 is directly connected, Loopback0
C       10.1.1.0/24 is directly connected, Loopback1
L       10.1.1.1/32 is directly connected, Loopback1
C       10.1.2.0/24 is directly connected, Loopback2
L       10.1.2.1/32 is directly connected, Loopback2
C       10.1.3.0/24 is directly connected, Loopback3
L       10.1.3.1/32 is directly connected, Loopback3
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, 04:38:25, Serial0/0/0
    172.5.0.0/24 is subnetted, 4 subnets
O E2    172.5.0.0/24 [110/50000] via 10.103.12.2, 00:23:00, Serial0/0/0
O E2    172.5.1.0/24 [110/50000] via 10.103.12.2, 00:23:00, Serial0/0/0
O E2    172.5.2.0/24 [110/50000] via 10.103.12.2, 00:23:00, Serial0/0/0
O E2    172.5.3.0/24 [110/50000] via 10.103.12.2, 00:23:00, Serial0/0/0
    172.29.0.0/24 is subnetted, 2 subnets
O E2    172.29.34.0/24 [110/50000] via 10.103.12.2, 00:23:00, Serial0/0/0
O E2    172.29.45.0/24 [110/50000] via 10.103.12.2, 00:23:00, Serial0/0/0
```

Figura 21. Escenario 1 – Tabla de enrutamiento final en R1. Elaboración propia.

Tabla de enrutamiento completa en R5:

```
R5>sh 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, 6 subnets, 2 masks
D EX   10.1.0.1/32 [170/3193856] via 172.29.45.1, 00:05:10, Serial0/0/0
D EX   10.1.1.1/32 [170/3193856] via 172.29.45.1, 00:05:10, Serial0/0/0
D EX   10.1.2.1/32 [170/3193856] via 172.29.45.1, 00:05:10, Serial0/0/0
D EX   10.1.3.1/32 [170/3193856] via 172.29.45.1, 00:05:10, Serial0/0/0
D EX   10.103.12.0/24 [170/3193856] via 172.29.45.1, 00:05:10, Serial0/0/0
D EX   10.103.23.0/24 [170/3193856] via 172.29.45.1, 00:05:10, Serial0/0/0
    172.5.0.0/16 is variably subnetted, 8 subnets, 2 masks
C       172.5.0.0/24 is directly connected, Loopback0
L       172.5.0.1/32 is directly connected, Loopback0
C       172.5.1.0/24 is directly connected, Loopback1
L       172.5.1.1/32 is directly connected, Loopback1
C       172.5.2.0/24 is directly connected, Loopback2
L       172.5.2.1/32 is directly connected, Loopback2
C       172.5.3.0/24 is directly connected, Loopback3
L       172.5.3.1/32 is directly connected, Loopback3
    172.29.0.0/16 is variably subnetted, 3 subnets, 2 masks
D       172.29.34.0/24 [90/2681856] via 172.29.45.1, 02:19:26, Serial0/0/0
C       172.29.45.0/24 is directly connected, Serial0/0/0
L       172.29.45.2/32 is directly connected, Serial0/0/0
```

Figura 22. Escenario 1 – Tabla de enrutamiento final en R1. Elaboración propia.

Bonus: Pruebas de conectividad de extremo a extremo

Ping desde R1 a R5:

```
R1>ping 172.5.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.5.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/9/15 ms
```

Figura 23. Escenario 1 – Ping exitoso desde R1 hacia R5. Elaboración propia.

Ping desde R5 hacia R1:

```
R5>ping 10.1.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/11/24 ms
```

Figura 24. Escenario 1 – Ping exitoso desde R5 hacia R1. Elaboración propia.

1.2 ESCENARIO #2

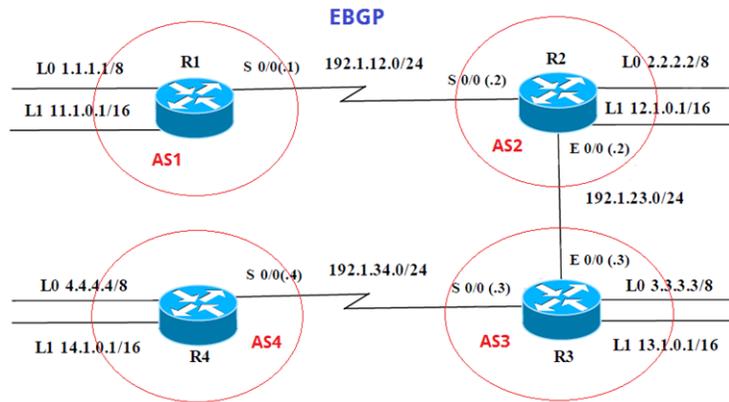


Figura 25. Escenario 2. Tomado de https://1drv.ms/w/s!AglGg5JUgUBthGdCOlggFa_kkWCT

Información para configuración de los enrutadores:

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

Tabla 1. Escenario 2 - Direccionamiento IP a configurar en enrutadores. Tomado de https://1drv.ms/w/s!AglGg5JUgUBthGdCOlggFa_kkWCT

Topología base implementada (Software: GNS3 v2.1.14):

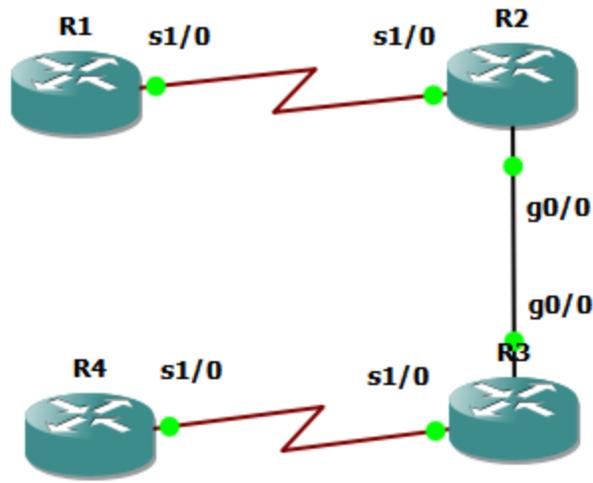


Figura 26. Topología implementada para el escenario 2. Elaboración propia.

Se realiza la configuración de direccionamiento IP en las diferentes interfaces de los enrutadores:

```
R1#configure terminal
R1 (config) #interface serial 1/0
R1 (config-if) #ip address 192.1.12.1 255.255.255.0
R1 (config-if) #no shutdown
R1 (config-if) #exit
R1 (config) #interface lo0
R1 (config-if) #ip address 1.1.1.1 255.0.0.0
R1 (config-if) #exit
R1 (config) #interface lo1
R1 (config-if) #ip address 11.1.0.1 255.255.0.0
R1 (config-if) #do wr
R1 (config-if) #end
```

```
R2#configure terminal
R2 (config) #interface serial 1/0
R2 (config-if) #ip address 192.1.12.2 255.255.255.0
R2 (config-if) #clock rate 64000
R2 (config-if) #no shutdown
R2 (config-if) #exit
R2 (config) #interface gigabitEthernet 0/0
R2 (config-if) #ip address 192.1.23.2 255.255.255.0
R2 (config-if) #no shutdown
R2 (config-if) #exit
R2 (config) #interface lo0
```

```

R2 (config-if) #ip address 2.2.2.2 255.0.0.0
R2 (config-if) #exit
R2 (config) #interface lo1
R2 (config-if) #ip address 12.1.0.1 255.255.0.0
R2 (config-if) #do wr
R2 (config-if) #end

R3#configure terminal
R3 (config) #interface serial 1/0
R3 (config-if) #ip address 192.1.34.3 255.255.255.0
R3 (config-if) #no shutdown
R3 (config-if) #exit
R3 (config) #interface gigabitEthernet 0/0
R3 (config-if) #ip address 192.1.23.3 255.255.255.0
R3 (config-if) #no shutdown
R3 (config-if) #exit
R3 (config) #interface lo0
R3 (config-if) #ip address 3.3.3.3 255.0.0.0
R3 (config-if) #exit
R3 (config) #interface lo1
R3 (config-if) #ip address 13.1.0.1 255.255.0.0
R3 (config-if) #do wr
R3 (config-if) #end

R4#configure terminal
R4 (config) #interface serial 1/0
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
R4 (config) #interface lo0
R4 (config-if) #ip address 4.4.4.4 255.0.0.0
R4 (config-if) #exit
R4 (config) #interface lo1
R4 (config-if) #ip address 14.1.0.1 255.255.0.0
R4 (config-if) #do wr
R4 (config-if) #end

```

Verificación de configuración de direccionamiento:

```

R1#sh ip int br | include manual
Serial1/0          192.1.12.1      YES manual up    up
Loopback0         1.1.1.1        YES manual up    up
Loopback1         11.1.0.1       YES manual up    up

```

Figura 27. Escenario 2 - Direccionamiento IP implementado en R1. Elaboración propia.

```

R2#sh ip int br | include manual
GigabitEthernet0/0      192.1.23.2      YES manual up      up
Serial1/0                192.1.12.2      YES manual up      up
Loopback0                2.2.2.2        YES manual up      up
Loopback1                12.1.0.1       YES manual up      up

```

Figura 28. Escenario 2 - Direccionamiento IP implementado en R2. Elaboración propia.

```

R3#sh ip int br | include manual
GigabitEthernet0/0      192.1.23.3      YES manual up      up
Serial1/0                192.1.34.3      YES manual up      up
Loopback0                3.3.3.3        YES manual up      up
Loopback1                13.1.0.1       YES manual up      up

```

Figura 29. Escenario 2 - Direccionamiento IP implementado en R3. Elaboración propia.

```

R4#sh ip int br | include manual
Serial1/0                192.1.34.4      YES manual up      up
Loopback0                4.4.4.4        YES manual up      up
Loopback1                14.1.0.1       YES manual up      up

```

Figura 30. Escenario 2 - Direccionamiento IP implementado en R4. Elaboración propia.

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*.

```

R1#configure terminal
R1 (config) #router bgp 1
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
R1 (config-router) # bgp router-id 11.11.11.11
R1 (config-router) # do wr
R1 (config-router) # end

```

```

R2#configure terminal
R2 (config) #router bgp 2
R2 (config-router) # neighbor 192.1.12.1 remote-as 1
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
R2 (config-router) # bgp router-id 22.22.22.22
R2 (config-router) # do wr
R2 (config-router) # end

```

Verificación de rutas propagadas a través de BGP para R1 y R2:

```
R1#sh ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B      2.0.0.0/8 [20/0] via 192.1.12.2, 00:02:57
       12.0.0.0/16 is subnetted, 1 subnets
B      12.1.0.0 [20/0] via 192.1.12.2, 00:02:57
```

Figura 31. Escenario 2 - Rutas BGP aprendidas en R1. Elaboración propia.

```
R2#sh ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B      1.0.0.0/8 [20/0] via 192.1.12.1, 00:02:59
       11.0.0.0/16 is subnetted, 1 subnets
B      11.1.0.0 [20/0] via 192.1.12.1, 00:02:59
```

Figura 32. Escenario 2 - Rutas BGP aprendidas en R2. Elaboración propia.

Verificación mediante comando *show bgp* en R1 y R2, en el cual se evidencian además de las rutas aprendidas y publicadas el *router ID* definido:

```
R1#show bgp
BGP table version is 9, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network          Next Hop          Metric LocPrf Weight Path
*> 1.0.0.0          0.0.0.0           0         32768 i
*> 2.0.0.0          192.1.12.2        0         0 2 i
*> 11.1.0.0/16      0.0.0.0           0         32768 i
*> 12.1.0.0/16      192.1.12.2        0         0 2 i
```

Figura 33. Escenario 2 - BGP router ID y rutas BGP consolidadas en R1. Elaboración propia.

```

R2#show bgp
BGP table version is 5, local router ID is 22.22.22.22
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network          Next Hop          Metric LocPrf Weight Path
*> 1.0.0.0          192.1.12.1         0             0 1 i
*> 2.0.0.0          0.0.0.0            0             32768 i
*> 11.1.0.0/16     192.1.12.1         0             0 1 i
*> 12.1.0.0/16     0.0.0.0            0             32768 i

```

Figura 34. Escenario 2 – BGP router ID y rutas BGP consolidadas en R2. Elaboración propia.

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*.

```

R2#configure terminal
R2 (config) #router bgp 2
R2 (config-router) # neighbor 192.1.23.3 remote-as 3
R2 (config-router) # do wr
R2 (config-router) # end

```

```

R3#configure terminal
R3 (config) #router bgp 3
R3 (config-router) # neighbor 192.1.23.2 remote-as 2
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
R3 (config-router) # bgp router-id 33.33.33.33
R3 (config-router) # do wr
R3 (config-router) # end

```

Verificación de rutas propagadas a través de BGP para R2 y R3:

```
R2#sh ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B     1.0.0.0/8 [20/0] via 192.1.12.1, 00:18:54
B     3.0.0.0/8 [20/0] via 192.1.23.3, 00:00:10
      11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.12.1, 00:18:54
      13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0 [20/0] via 192.1.23.3, 00:00:10
```

Figura 35. Escenario 2 - Rutas BGP de R3 añadidas en R2. Elaboración propia.

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

Gateway of last resort is not set

B     1.0.0.0/8 [20/0] via 192.1.23.2, 00:00:08
B     2.0.0.0/8 [20/0] via 192.1.23.2, 00:00:08
      11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.23.2, 00:00:08
      12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.23.2, 00:00:08
```

Figura 36. Escenario 2 - Rutas BGP aprendidas en R3. Elaboración propia.

Verificación mediante *comando show bgp* en R2 y R3, en el cual se evidencian además de las rutas aprendidas y publicadas, el *router ID* definido. En este punto R2 ya conoce las redes propagadas desde R1 y R3, y R3 reconoce incluso las rutas propagadas desde R1. Se observa también el incremento de número de versión de la tabla BGP respecto al paso anterior:

```

R2#show bgp
BGP table version is 7, local router ID is 22.22.22.22
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network          Next Hop          Metric LocPrf Weight Path
*>  1.0.0.0          192.1.12.1         0             0 1 i
*>  2.0.0.0           0.0.0.0            0             32768 i
*>  3.0.0.0          192.1.23.3         0             0 3 i
*>  11.1.0.0/16      192.1.12.1         0             0 1 i
*>  12.1.0.0/16      0.0.0.0            0             32768 i
*>  13.1.0.0/16      192.1.23.3         0             0 3 i

```

Figura 37. Escenario 2 – BGP router ID y rutas BGP consolidadas en R2. Elaboración propia.

```

R3#show bgp
BGP table version is 7, local router ID is 33.33.33.33
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network          Next Hop          Metric LocPrf Weight Path
*>  1.0.0.0          192.1.23.2         0             0 2 1 i
*>  2.0.0.0          192.1.23.2         0             0 2 i
*>  3.0.0.0           0.0.0.0            0             32768 i
*>  11.1.0.0/16      192.1.23.2         0             0 2 1 i
*>  12.1.0.0/16      192.1.23.2         0             0 2 i
*>  13.1.0.0/16      0.0.0.0            0             32768 i

```

Figura 38. Escenario 2 – BGP router ID y rutas BGP consolidadas en R3. Elaboración propia.

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*.

```

R3#configure terminal
R3 (config) #router bgp 3
R3 (config-router) #neighbor 192.1.34.4 remote-as 4
R3 (config-router) #do wr
R3 (config-router) #end

```

```

R4#configure terminal
R4 (config) #router bgp 4

```

```

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
R4 (config-router) # bgp router-id 44.44.44.44
R4 (config-router) # do wr
R4 (config-router) # end

```

Verificación de rutas propagadas a través de BGP para todos los enrutadores:

```

R1#sh ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B       2.0.0.0/8 [20/0] via 192.1.12.2, 02:29:38
B       3.0.0.0/8 [20/0] via 192.1.12.2, 02:10:49
B       4.0.0.0/8 [20/0] via 192.1.12.2, 00:35:41
       12.0.0.0/16 is subnetted, 1 subnets
B         12.1.0.0 [20/0] via 192.1.12.2, 02:29:38
       13.0.0.0/16 is subnetted, 1 subnets
B         13.1.0.0 [20/0] via 192.1.12.2, 02:10:49
       14.0.0.0/16 is subnetted, 1 subnets
B         14.1.0.0 [20/0] via 192.1.12.2, 00:35:41

```

Figura 39. Escenario 2 - Rutas BGP aprendidas en R1. Elaboración propia.

```

R2#sh ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B     1.0.0.0/8 [20/0] via 192.1.12.1, 02:30:12
B     3.0.0.0/8 [20/0] via 192.1.23.3, 02:11:28
B     4.0.0.0/8 [20/0] via 192.1.23.3, 00:36:20
      11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.12.1, 02:30:12
      13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0 [20/0] via 192.1.23.3, 02:11:28
      14.0.0.0/16 is subnetted, 1 subnets
B       14.1.0.0 [20/0] via 192.1.23.3, 00:36:20

```

Figura 40. Escenario 2 - Rutas BGP aprendidas en R2. Elaboración propia.

```

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

Gateway of last resort is not set

B     1.0.0.0/8 [20/0] via 192.1.23.2, 02:12:15
B     2.0.0.0/8 [20/0] via 192.1.23.2, 02:12:15
B     4.0.0.0/8 [20/0] via 192.1.34.4, 00:37:07
      11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.23.2, 02:12:15
      12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.23.2, 02:12:15
      14.0.0.0/16 is subnetted, 1 subnets
B       14.1.0.0 [20/0] via 192.1.34.4, 00:37:07

```

Figura 41. Escenario 2 - Rutas BGP aprendidas en R3. Elaboración propia.

```

R4#sh ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B       1.0.0.0/8 [20/0] via 192.1.34.3, 00:37:42
B       2.0.0.0/8 [20/0] via 192.1.34.3, 00:37:41
B       3.0.0.0/8 [20/0] via 192.1.34.3, 00:37:41
       11.0.0.0/16 is subnetted, 1 subnets
B         11.1.0.0 [20/0] via 192.1.34.3, 00:37:41
       12.0.0.0/16 is subnetted, 1 subnets
B         12.1.0.0 [20/0] via 192.1.34.3, 00:37:41
       13.0.0.0/16 is subnetted, 1 subnets
B         13.1.0.0 [20/0] via 192.1.34.3, 00:37:41

```

Figura 42. Escenario 2 - Rutas BGP aprendidas en R4. Elaboración propia.

Verificación mediante comando *show bgp* en todos los enrutadores:

```

R1#show bgp
BGP table version is 13, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network          Next Hop          Metric LocPrf Weight Path
*> 1.0.0.0          0.0.0.0           0             32768 i
*> 2.0.0.0          192.1.12.2        0             0 2 i
*> 3.0.0.0          192.1.12.2        0             0 2 3 i
*> 4.0.0.0          192.1.12.2        0             0 2 3 4 i
*> 11.1.0.0/16     0.0.0.0           0             32768 i
*> 12.1.0.0/16     192.1.12.2        0             0 2 i
*> 13.1.0.0/16     192.1.12.2        0             0 2 3 i
*> 14.1.0.0/16     192.1.12.2        0             0 2 3 4 i

```

Figura 43. Escenario 2 - BGP router ID y rutas BGP consolidadas en R1. Elaboración propia.

```

R2#show bgp
BGP table version is 9, local router ID is 22.22.22.22
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network          Next Hop          Metric LocPrf Weight Path
*> 1.0.0.0          192.1.12.1         0             0 1 i
*> 2.0.0.0          0.0.0.0            0            32768 i
*> 3.0.0.0          192.1.23.3         0             0 3 i
*> 4.0.0.0          192.1.23.3         0             0 3 4 i
*> 11.1.0.0/16     192.1.12.1         0             0 1 i
*> 12.1.0.0/16     0.0.0.0            0            32768 i
*> 13.1.0.0/16     192.1.23.3         0             0 3 i
*> 14.1.0.0/16     192.1.23.3         0             0 3 4 i

```

Figura 44. Escenario 2 – BGP router ID y rutas BGP consolidadas en R2. Elaboración propia.

```

R3#show bgp
BGP table version is 9, local router ID is 33.33.33.33
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network          Next Hop          Metric LocPrf Weight Path
*> 1.0.0.0          192.1.23.2         0             0 2 1 i
*> 2.0.0.0          192.1.23.2         0             0 2 i
*> 3.0.0.0          0.0.0.0            0            32768 i
*> 4.0.0.0          192.1.34.4         0             0 4 i
*> 11.1.0.0/16     192.1.23.2         0             0 2 1 i
*> 12.1.0.0/16     192.1.23.2         0             0 2 i
*> 13.1.0.0/16     0.0.0.0            0            32768 i
*> 14.1.0.0/16     192.1.34.4         0             0 4 i

```

Figura 45. Escenario 2 – BGP router ID y rutas BGP consolidadas en R3. Elaboración propia.

```

R4#show bgp
BGP table version is 9, local router ID is 44.44.44.44
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network          Next Hop          Metric LocPrf Weight Path
*> 1.0.0.0          192.1.34.3         0             0 3 2 1 i
*> 2.0.0.0          192.1.34.3         0             0 3 2 i
*> 3.0.0.0          192.1.34.3         0             0 3 i
*> 4.0.0.0          0.0.0.0            0            32768 i
*> 11.1.0.0/16     192.1.34.3         0             0 3 2 1 i
*> 12.1.0.0/16     192.1.34.3         0             0 3 2 i
*> 13.1.0.0/16     192.1.34.3         0             0 3 i
*> 14.1.0.0/16     0.0.0.0            0            32768 i

```

Figura 46. Escenario 2 – BGP router ID y rutas BGP consolidadas en R4. Elaboración propia.

1.3 ESCENARIO #3

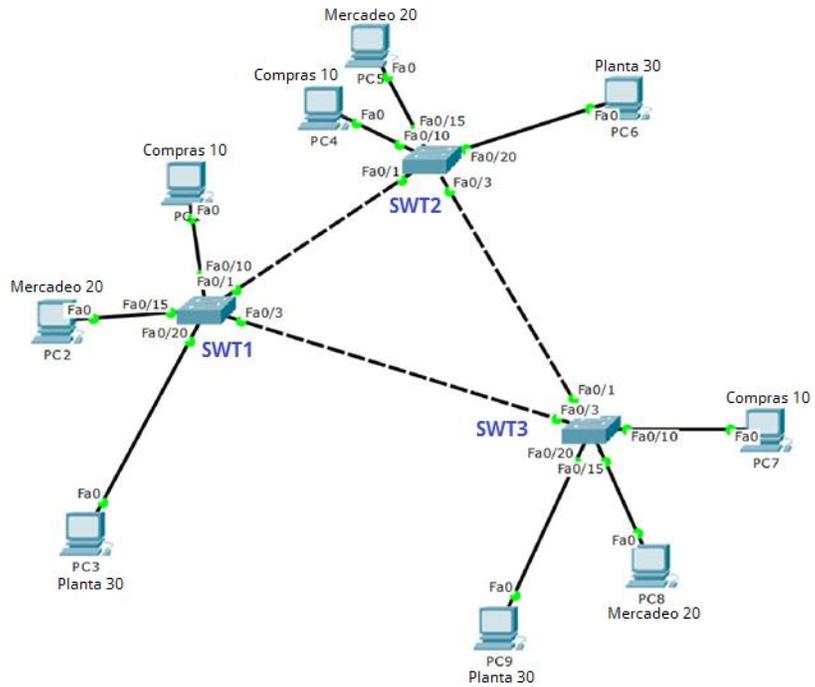


Figura 47. Escenario 3. Tomado de https://1drv.ms/w/s!AglGg5JUgUBthGdCOlggFa_kkWCT

Topología base implementada (Software: Cisco Packet Tracer v7.2.1.0128):

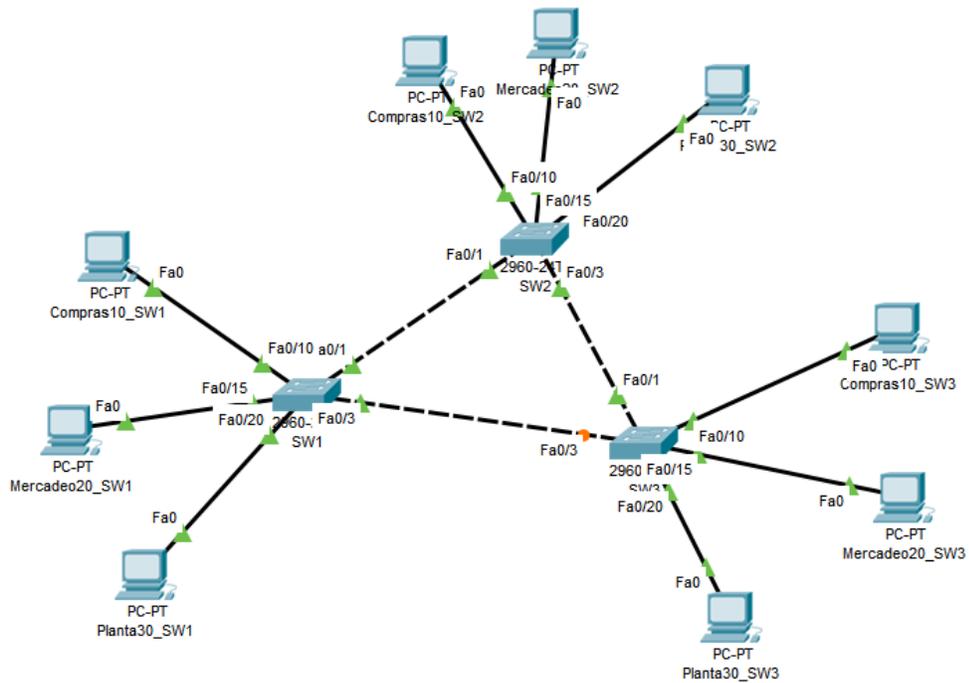


Figura 48. Topología implementada para el escenario 3. Elaboración propia.

A. Configurar VTP

1. Todos los *switches* se configurarán para usar VTP para las actualizaciones de VLAN. El *switch* SW2 se configurará como el servidor. Los *switches* SW1 y SW3 se configurarán como clientes. Los *switches* estarán en el dominio VTP llamado CCNP y usando la contraseña cisco.

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW1
SW1(config)#vtp mode client
SW1(config)#vtp domain CCNP
SW1(config)#vtp password cisco
SW1(config)#do wr
SW1(config)#end
```

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW2
SW2(config)#vtp domain CCNP
SW2(config)#vtp password cisco
SW2(config)#do wr
SW2(config)#end
```

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW3
SW3(config)#vtp mode client
SW3(config)#vtp domain CCNP
SW3(config)#vtp password cisco
SW3(config)#do wr
SW3(config)#end
```

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

```
SW1#sh vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 255
Number of existing VLANs   : 5
VTP Operating Mode         : Client
VTP Domain Name            : CCNP
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Figura 49. Escenario 3 – Estado de VTP en SW1. Elaboración propia.

```

SW2#sh vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 255
Number of existing VLANs   : 5
VTP Operating Mode        : Server
VTP Domain Name           : CCNP
VTP Pruning Mode          : Disabled
VTP V2 Mode               : Disabled
VTP Traps Generation      : Disabled
MD5 digest                 : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

```

Figura 50. Escenario 3 – Estado de VTP en SW2. Elaboración propia.

```

SW3#sh vtp status
VTP Version                : 2
Configuration Revision     : 0
Maximum VLANs supported locally : 255
Number of existing VLANs   : 5
VTP Operating Mode        : Client
VTP Domain Name           : CCNP
VTP Pruning Mode          : Disabled
VTP V2 Mode               : Disabled
VTP Traps Generation      : Disabled
MD5 digest                 : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

```

Figura 51. Escenario 3 – Estado de VTP en SW3. Elaboración propia.

B. Configurar DTP (*Dynamic Trunking Protocol*)

1. Configure un enlace troncal ("*trunk*") dinámico entre SW1 y SW2. Debido a que el modo por defecto es *dynamic auto*, solo un lado del enlace debe configurarse como *dynamic desirable*.

```

SW1#configure terminal
SW1 (config) #interface FastEthernet 0/1
SW1 (config-if) #switchport mode trunk
SW1 (config-if) #switchport mode dynamic desirable

```

```

SW2#configure terminal
SW2 (config) #interface FastEthernet 0/1
SW2 (config-if) #switchport mode trunk
SW2 (config-if) #switchport mode dynamic auto

```

2. Verifique el enlace "*trunk*" entre SW1 y SW2 usando el comando *show interfaces trunk*.

```
SW1#sh int tr
Port      Mode           Encapsulation  Status        Native vlan
Fa0/1     desirable     n-802.1q       trunking      1

Port      Vlans allowed on trunk
Fa0/1     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1
```

Figura 52. Escenario 3 – Estado de enlaces troncales en SW1. Elaboración propia.

```
SW2#sh int tr
Port      Mode           Encapsulation  Status        Native vlan
Fa0/1     auto           n-802.1q       trunking      1

Port      Vlans allowed on trunk
Fa0/1     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1
```

Figura 53. Escenario 3 – Estado de enlaces troncales en SW2. Elaboración propia.

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

```
SW1#configure terminal
SW1(config)#interface FastEthernet 0/3
SW1(config-if)#switchport mode trunk
```

4. Verifique el enlace "trunk" el comando *show interfaces trunk* en SW1.

```
SW1#sh int 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
Fa0/3     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1
Fa0/3     1
```

Figura 54. Escenario 3 – Estado de enlaces troncales en SW1. Elaboración propia.

5. Configure un enlace "trunk" permanente entre SW2 y SW3.

```
SW2#configure terminal
SW2 (config) #interface FastEthernet 0/3
SW2 (config-if) #switchport mode trunk
SW2 (config-if) #switchport nonegotiate

SW3#configure terminal
SW3 (config) #interface FastEthernet 0/1
SW3 (config-if) #switchport mode trunk
SW3 (config-if) #switchport nonegotiate
```

Verificación: Dado que se configure un enlace troncal permanente en la interfaz FastEthernet 0/3 de SW2, la salida del comando *show interfaces FastEthernet 0/3 switchport* debe mostrar que el valor de "Administrative Mode" debe ser "trunk":

```
SW2#show interfaces fastEthernet 0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
```

Figura 55. Escenario 3 – Configuración de interfaz f0/3 en SW2 para enlace troncal. Elaboración propia.

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).

```
SW1#configure terminal
SW1 (config) #vlan 10
```

No es posible crear la VLAN en SW1 toda vez que está operando en modo VTP cliente:

```
SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1 (config) #vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
```

Figura 56. Escenario 3 – Error al agregar VLAN en VTP cliente en SW1. Elaboración propia.

```
SW2#configure terminal
SW2 (config) #vlan 10
SW2 (config-vlan) #name Compras
SW2 (config) #vlan 20
SW2 (config-vlan) #name Mercadeo
SW2 (config) #vlan 30
SW2 (config-vlan) #name Planta
SW2 (config) #vlan 99
SW2 (config-vlan) #name Admon
SW2 (config-vlan) #end
```

2. Verifique que las VLANs han sido agregadas correctamente.

```
SW2#sh vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig0/1, Gig0/2
10	Compras	active	
20	Mercadeo	active	
30	Planta	active	
99	Admon	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Figura 57. Escenario 3 – Verificación de VLAN en SW2. Elaboración propia.

```
SW1#show vlan
```

```

VLAN Name                Status    Ports
-----
1    default                active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                           Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                           Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/23, Fa0/24, Gig0/1, Gig0/2

10   Compras                active
20   Mercadeo               active
30   Planta                 active
99   Admon                  active
1002 fddi-default           active
1003 token-ring-default   active
1004 fddinet-default       active
1005 trnet-default         active

```

Figura 58. Escenario 3 – Verificación de VLAN en SW1. Elaboración propia.

```
SW3#sh vlan
```

```

VLAN Name                Status    Ports
-----
1    default                active    Fa0/2, Fa0/4, Fa0/5, Fa0/6
                                           Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                           Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                           Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                           Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/23, Fa0/24, Gig0/1, Gig0/2

10   Compras                active
20   Mercadeo               active
30   Planta                 active
99   Admon                  active
1002 fddi-default           active
1003 token-ring-default   active
1004 fddinet-default       active
1005 trnet-default         active

```

Figura 59. Escenario 3 – Verificación de VLAN en SW3. Elaboración propia.

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

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

X = número de cada PC particular

Tabla 2. Escenario 3. Configuración de PCs e interfaces del switch. Tomado de https://1drv.ms/w/s!AgIGg5JUgUBthGdCOlggFa_kkWCT

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

```
SW1#configure terminal
SW1 (config) #interface FastEthernet 0/10
SW1 (config-if) #switchport mode access
SW1 (config-if) #switchport access vlan 10
```

```
SW2#configure terminal
SW2 (config) #interface FastEthernet 0/10
SW2 (config-if) #switchport mode access
SW2 (config-if) #switchport access vlan 10
SW3#configure terminal
SW3 (config) #interface FastEthernet 0/10
SW3 (config-if) #switchport mode access
SW3 (config-if) #switchport access vlan 10
```

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.

```
SW1#configure terminal
SW1 (config) #interface FastEthernet 0/15
SW1 (config-if) #switchport mode access
SW1 (config-if) #switchport access vlan 20
SW1 (config-if) #interface FastEthernet 0/20
SW1 (config-if) #switchport mode access
SW1 (config-if) #switchport access vlan 30
```

```
SW2#configure terminal
SW2 (config) #interface FastEthernet 0/15
SW2 (config-if) #switchport mode access
SW2 (config-if) #switchport access vlan 20
SW2 (config-if) #interface FastEthernet 0/20
SW2 (config-if) #switchport mode access
SW2 (config-if) #switchport access vlan 30
```

```
SW3#configure terminal
SW3 (config) #interface FastEthernet 0/15
SW3 (config-if) #switchport mode access
SW3 (config-if) #switchport access vlan 20
SW3 (config-if) #interface FastEthernet 0/20
SW3 (config-if) #switchport mode access
SW3 (config-if) #switchport access vlan 30
```

Se asignan las siguientes direcciones IP a los PCs:

SW	Interfaz	VLAN ID	Nombre VLAN	Nombre PC	Dirección IP
SW1	F0/10	10	Compras	Compras10_SW1	190.108.10.101
	F0/15	20	Mercadeo	Mercadeo20_SW1	190.108.20.101
	F0/20	30	Planta	Planta30_SW1	190.108.30.101
SW	Interfaz	VLAN ID	Nombre VLAN	Nombre PC	Dirección IP
SW2	F0/10	10	Compras	Compras10_SW2	190.108.10.102
	F0/15	20	Mercadeo	Mercadeo20_SW2	190.108.20.102
	F0/20	30	Planta	Planta30_SW2	190.108.30.102
SW	Interfaz	VLAN ID	Nombre VLAN	Nombre PC	Dirección IP
SW3	F0/10	10	Compras	Compras10_SW3	190.108.10.103
	F0/15	20	Mercadeo	Mercadeo20_SW3	190.108.20.103
	F0/20	30	Planta	Planta30_SW3	190.108.30.103

Tabla 3. Escenario 3 - Configuración de PCs e interfaces en SW1, SW2 y SW3. Tomado de https://1drv.ms/w/s!AglGg5JUgUBthGdCOlggFa_kkWCT

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.

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

Tabla 4. Escenario 3 - Configuración de SVI para VLAN de administración en SW1, SW2 y SW3. Tomado de https://1drv.ms/w/s!AglGg5JUgUBthGdCOlggFa_kkWCT

```
SW1#configure terminal
SW1 (config) #interface vlan 99
SW1 (config-if) #ip address 190.108.99.1 255.255.255.0
```

```
SW2#configure terminal
SW2 (config) #interface vlan 99
SW2 (config-if) #ip address 190.108.99.2 255.255.255.0
```

```
SW3#configure terminal
SW3 (config) #interface vlan 99
SW3 (config-if) #ip address 190.108.99.3 255.255.255.0
```

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.

Desde el PC Compras10_SW1 asignado a la VLAN Compras en el SW1 con dirección IP 190.108.10.101 es posible contactar a las otras dos direcciones IP que se encuentran en la misma VLAN, en los *switches* SW2 y SW3. No ocurre lo mismo cuando se intenta contactar con los PCs pertenecientes a las VLAN Mercadeo (190.108.20.x) y Planta (190.108.30.x) en SW1, SW2 y SW3:

```
Link-local IPv6 Address.....: FE80::2E0:8FFF:FE67:3935
IP Address.....: 190.108.10.101
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 190.108.10.1

Bluetooth Connection:

Link-local IPv6 Address.....: ::
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0

C:\>ping 190.108.10.102

Pinging 190.108.10.102 with 32 bytes of data:

Reply from 190.108.10.102: bytes=32 time=1ms TTL=128
Reply from 190.108.10.102: bytes=32 time<1ms TTL=128
Reply from 190.108.10.102: bytes=32 time<1ms TTL=128
Reply from 190.108.10.102: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.10.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 190.108.10.103

Pinging 190.108.10.103 with 32 bytes of data:

Reply from 190.108.10.103: bytes=32 time<1ms TTL=128
Reply from 190.108.10.103: bytes=32 time=1ms TTL=128
Reply from 190.108.10.103: bytes=32 time<1ms TTL=128
Reply from 190.108.10.103: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.10.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figura 60. Escenario 3 – Verificación de conectividad entre PCs VLAN Compras. Elaboración propia.

```
C:\>ping 10.108.20.101

Pinging 10.108.20.101 with 32 bytes of data:

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

Ping statistics for 10.108.20.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.108.20.102

Pinging 10.108.20.102 with 32 bytes of data:

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

Ping statistics for 10.108.20.102:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.108.20.103

Pinging 10.108.20.103 with 32 bytes of data:

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

Ping statistics for 10.108.20.103:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 61. Escenario 3– Verificación de conectividad entre VLAN Compras y VLAN Mercadeo. Elaboración propia.

```
C:\>ping 10.108.30.101

Pinging 10.108.30.101 with 32 bytes of data:

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

Ping statistics for 10.108.30.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.108.30.102

Pinging 10.108.30.102 with 32 bytes of data:

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

Ping statistics for 10.108.30.102:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.108.30.103

Pinging 10.108.30.103 with 32 bytes of data:

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

Ping statistics for 10.108.30.103:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 62. Escenario 3 – Verificación de conectividad entre VLAN Compras y VLAN Planta. Elaboración propia.

Se realiza prueba desde el PC Mercadeo20_SW2, perteneciente a la VLAN Mercadeo (190.108.20.x) con dirección IP 190.108.20.102. Es posible alcanzar las direcciones IP que se encuentran dentro de la misma VLAN en SW1 y SW3, pero no es posible alcanzar las direcciones IP de los equipos de las VLAN de Compras (190.108.10.x) y Planta (190.108.30.x) en SW1, SW2 y SW3:

```
Link-local IPv6 Address.....: FE80::201:42FF:FE7D:855B
IP Address.....: 190.108.20.102
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 190.108.20.1

Bluetooth Connection:

Link-local IPv6 Address.....: ::
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0

C:\>ping 190.108.20.101

Pinging 190.108.20.101 with 32 bytes of data:

Reply from 190.108.20.101: bytes=32 time=1ms TTL=128
Reply from 190.108.20.101: bytes=32 time<1ms TTL=128
Reply from 190.108.20.101: bytes=32 time<1ms TTL=128
Reply from 190.108.20.101: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.20.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 190.108.20.103

Pinging 190.108.20.103 with 32 bytes of data:

Reply from 190.108.20.103: bytes=32 time=1ms TTL=128
Reply from 190.108.20.103: bytes=32 time<1ms TTL=128
Reply from 190.108.20.103: bytes=32 time<1ms TTL=128
Reply from 190.108.20.103: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.20.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figura 63. Escenario 3– Verificación de conectividad entre PCs VLAN Mercadeo. Elaboración propia.

```
C:\>ping 10.108.10.101

Pinging 10.108.10.101 with 32 bytes of data:

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

Ping statistics for 10.108.10.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.108.10.102

Pinging 10.108.10.102 with 32 bytes of data:

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

Ping statistics for 10.108.10.102:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.108.10.103

Pinging 10.108.10.103 with 32 bytes of data:

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

Ping statistics for 10.108.10.103:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 64. Escenario 3 – Verificación de conectividad entre VLAN Mercadeo y VLAN Compras. Elaboración propia.

```
C:\>ping 10.108.30.101

Pinging 10.108.30.101 with 32 bytes of data:

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

Ping statistics for 10.108.30.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.108.30.102

Pinging 10.108.30.102 with 32 bytes of data:

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

Ping statistics for 10.108.30.102:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 10.108.30.103

Pinging 10.108.30.103 with 32 bytes of data:

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

Ping statistics for 10.108.30.103:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 65. Escenario 3 – Verificación de conectividad entre VLAN Mercadeo y VLAN Planta. Elaboración propia.

Finalmente, se realiza prueba desde el PC Planta30_SW3, perteneciente a la VLAN Planta (190.108.30.x) con dirección IP 190.108.30.103. Es posible alcanzar las direcciones IP que se encuentran dentro de las misma VLAN en SW1 y SW2, pero no es posible alcanzar las direcciones IP de los equipos de las VLAN de Compras (190.108.10.x) y Mercadeo (190.108.20.x) en SW1, SW2 y SW3:

```

Link-local IPv6 Address.....: FE80::2D0:BAFF:FE56:D111
IP Address.....: 190.108.30.103
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 190.108.30.1

Bluetooth Connection:

Link-local IPv6 Address.....: ::
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0

C:\>ping 190.108.30.101

Pinging 190.108.30.101 with 32 bytes of data:

Reply from 190.108.30.101: bytes=32 time=1ms TTL=128
Reply from 190.108.30.101: bytes=32 time<1ms TTL=128
Reply from 190.108.30.101: bytes=32 time<1ms TTL=128
Reply from 190.108.30.101: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.30.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 190.108.30.102

Pinging 190.108.30.102 with 32 bytes of data:

Reply from 190.108.30.102: bytes=32 time=2ms TTL=128
Reply from 190.108.30.102: bytes=32 time<1ms TTL=128
Reply from 190.108.30.102: bytes=32 time<1ms TTL=128
Reply from 190.108.30.102: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.30.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

```

Figura 66. Escenario 3– Verificación de conectividad entre PCs VLAN Planta. Elaboración propia.

```
C:\>ping 190.108.10.101

Pinging 190.108.10.101 with 32 bytes of data:

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

Ping statistics for 190.108.10.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.10.102

Pinging 190.108.10.102 with 32 bytes of data:

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

Ping statistics for 190.108.10.102:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.10.103

Pinging 190.108.10.103 with 32 bytes of data:

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

Ping statistics for 190.108.10.103:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 67. Escenario 3 – Verificación de conectividad entre VLAN Planta y VLAN Compras. Elaboración propia.

```
C:\>ping 190.108.20.101

Pinging 190.108.20.101 with 32 bytes of data:

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

Ping statistics for 190.108.20.101:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.20.102

Pinging 190.108.20.102 with 32 bytes of data:

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

Ping statistics for 190.108.20.102:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.20.103

Pinging 190.108.20.103 with 32 bytes of data:

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

Ping statistics for 190.108.20.103:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 68. Escenario 3 – Verificación de conectividad entre VLAN Mercadeo y VLAN Compras. Elaboración propia.

No es posible hacer ping entre VLAN diferentes puesto que no existen SVIs para cada una de ellas que funcionen como puerta de enlace en cada segmento de red. En consecuencia, no pueden participar de un proceso de enrutamiento InterVLAN.

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

Desde SW1:

```
SW1#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 = 0/0/0 ms

SW1#ping 190.108.99.3

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

Figura 69. Escenario 3 – Verificación de conectividad entre switches desde SW1. Elaboración propia.

Desde SW2:

```
SW2#ping 190.108.99.1

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

SW2#ping 190.108.99.3

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

Figura 70. Escenario 3 – Verificación de conectividad entre switches desde SW1. Elaboración propia.

Desde SW3:

```
SW3#ping 190.108.99.1

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

SW3#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
```

Figura 71. Escenario 3 – Verificación de conectividad entre switches desde SW1. Elaboración propia.

Las pruebas de ping entre conmutadores resultan exitosas por varios factores: Porque cada *switch* mediante su respectiva SVI tiene una dirección IP dentro de la VLAN de administración (ID 99), porque en cada *switch* está creada la VLAN 99 y también, porque los enlaces troncales están correctamente configurados entre ellos.

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

Se intenta realizar un ping desde SW1 hacia las direcciones IP de los equipos en la VLAN Compras (190.108.10.x). Resultan no exitosos toda vez que el *switch* no tiene configurada una SVI dentro de dicha VLAN y, en consecuencia, no podrá participar del proceso de enrutamiento entre VLANs. Se observa el mismo comportamiento al hacer ping a las direcciones dentro de la VLAN de Mercado (190.108.20.x) y planta (190.108.30.x):

```
SW1>ping 190.108.10.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.101, timeout is 2
seconds:
-----
Success rate is 0 percent (0/5)

SW1>ping 190.108.10.102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.102, timeout is 2
seconds:
-----
Success rate is 0 percent (0/5)

SW1>ping 190.108.10.103

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.103, timeout is 2
seconds:
-----
Success rate is 0 percent (0/5)
```

Figura 72. Escenario 3 – Verificación de conectividad desde SW1 a VLAN Compras. Elaboración propia.

```
SW1>ping 190.108.20.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.101, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW1>ping 190.108.20.102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.102, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW1>ping 190.108.20.103

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.103, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
```

Figura 73. Escenario 3– Verificación de conectividad desde SW1 a VLAN Mercadeo. Elaboración propia.

```
SW1>ping 190.108.30.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.101, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW1>ping 190.108.30.102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.102, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW1>ping 190.108.30.103

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.103, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
```

Figura 74. Escenario 3– Verificación de conectividad desde SW1 a VLAN Planta. Elaboración propia.

Se repite el comportamiento al realizar la misma prueba desde SW2 y SW3.

SW2:

```
SW2>ping 190.108.10.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.101, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW2>ping 190.108.10.102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.102, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW2>ping 190.108.10.103

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.103, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
```

Figura 75. Escenario 3 – Verificación de conectividad desde SW2 a VLAN Compras. Elaboración propia.

```
SW2>ping 190.108.20.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.101, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW2>ping 190.108.20.102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.102, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW2>ping 190.108.20.103

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.103, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
```

Figura 76. Escenario 3 – Verificación de conectividad desde SW2 a VLAN Mercadeo. Elaboración propia.

```
SW2>ping 190.108.30.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.101, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW2>ping 190.108.30.102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.102, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW2>ping 190.108.30.103

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.103, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
```

Figura 77. Escenario 3– Verificación de conectividad desde SW2 a VLAN Mercadeo. Elaboración propia.

SW3:

```
SW3>ping 190.108.10.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.101, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW3>ping 190.108.10.102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.102, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW3>ping 190.108.10.103

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.103, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
```

Figura 78. Escenario 3– Verificación de conectividad desde SW3 a VLAN Compras. Elaboración propia.

```
SW3>ping 190.108.20.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.101, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW3>ping 190.108.20.102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.102, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW3>ping 190.108.20.103

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.103, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
```

Figura 79. Escenario 3– Verificación de conectividad desde SW3 a VLAN Mercadeo. Elaboración propia.

```
SW3>ping 190.108.30.101

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.101, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW3>ping 190.108.30.102

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.102, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW3>ping 190.108.30.103

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.103, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
```

Figura 80. Escenario 3– Verificación de conectividad desde SW3 a VLAN Planta. Elaboración propia.

CONCLUSIONES

- Es posible realizar redistribución de rutas de OSPF utilizando el protocolo EIGRP y viceversa, lo cual facilita la interconexión en ambientes con dispositivos de diferentes fabricantes, teniendo en cuenta que EIGRP es un protocolo de enrutamiento propietario de Cisco Systems.
- BGP es un protocolo de enrutamiento avanzado para la comunicación entre sistemas autónomos. Su implementación en términos generales es sencilla, sin embargo, al profundizar en sus diferentes funcionalidades se observa que es un protocolo muy robusto pero a la vez complejo de administrar. Al igual que los demás protocolos de enrutamiento, también permite hacer uso de opciones como *address families* para interoperabilidad IPv4/IPv6, y propagación de rutas por defecto.
- El uso de VLANs permite simplificar la administración de la red, al realizar segmentación lógica de hosts que serán susceptibles por ejemplo, a políticas de seguridad que no afectarán dispositivos en diferentes VLAN.
- VTP es un protocolo muy útil para un entorno en el cual exista un alto número de VLANs en producción, sin embargo, su implementación requiere un elevado nivel de atención al detalle dado que un error en su despliegue o configuración podría desencadenar por ejemplo, una pérdida total de la base de datos de VLANs y, en consecuencia, se perdería la conectividad hacia la red.

BIBLIOGRAFÍA

Macfarlane, J. (2014). Network Routing Basics : Understanding IP Routing in Cisco Systems. Recuperado de <http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live>.

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

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