

EVALUACION FINAL
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

AIDE YASMIN DAZA DORADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
INGENIERIA DE TELECOMUNICACIONES
DIPLOMADO CISCO CCNP
BORDO CAUCA
2019

EVALUACION PRUEBA DE HABILIDADES PRÁCTICAS CCNP

AIDE YASMIN DAZA DORADO

Diplomado de profundización cisco CCNP prueba de
Habilidades prácticas

Gerardo Granados Acuña
Magister en Telemática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
INGENIERIA DE TELECOMUNICACIONES
DIPLOMADO CISCO CCNP
BORDO CAUCA
2019

NOTA DE ACEPTACION

Presidente del jurado

Jurado

Jurado

Bordo Cauca 03 de julio de 2019

CONTENIDO

Introduccion.....	9
Desarrollo de los escenarios.....	10
Conclusiones.....	46
Referencias Bibliograficas.....	47

LISTA DE TABLAS

Tabla 1. Enrutamiento y configuracion de los routers escenario 2.....	20
Tabla 2. Direccionamiento IP para los PCs	33
Tabla 3. Direccionamiento IP para los PCs	34
Tabla 4. Direccionamiento IP para los SVI (<i>Switch Virtual Interface</i>).....	40
Tabla 5. Verificación comando ping.....	42

LISTA DE FIGURAS

Figura 1. Esquema escenario 1.....	10
Figura 2. Montaje en software GNS3 escenario 1.....	10
Figura 3. Resultado comando show ip ospf brief.....	15
Figura 4. Resultado comando show ip interfaces brief include up.....	16
Figura 5. Resultado comando show ip eigrp interfaces.....	16
Figura 6. Resultado comando show ip route.....	17
Figura 7. Protocolo OSPF en R1.....	17
Figura 8. Protocolo EIGRP en R5.....	17
Figura 9. En R1 se encuentran las loopbacks creadas en R5.....	18
Figura 10. En R5 se encuentran las loopbacks creadas en R1.....	19
Figura 11. Esquema escenario 2.....	19
Figura 12. Resultado comando show ip route.....	23
Figura 13. Resultado comando show ip route.....	23
Figura 14. Resultado comando show ip route.....	24
Figura 15. Resultado comando show ip route.....	24
Figura 16. Resultado comando show ip route.....	25
Figura 17. Esquema escenario 3.....	26
Figura 18. Resultado comando show vtp status.....	27
Figura 19. Resultado comando show vtp status.....	28
Figura 20. Resultado comando show vtp status.....	28
Figura 21. Resultado comando show interfaces trunk.....	30
Figura 22. Resultado comando show interfaces trunk.....	30
Figura 23. Resultado comando show interfaces trunk.....	31
Figura 24. Resultado Comando show vlan brief.....	33
Figura 25. Resultado Comando show vlan brief.....	33
Figura 26. Resultado comando show.....	37
Figura 27. Resultado comando show.....	37

Figura 28. Resultado comando show.....	37
Figura 29. Resultado comando show.....	38
Figura 30. Resultado comando show.....	38
Figura 31. Resultado comando show.....	38
Figura 32. Resultado comando show.....	39
Figura 33. Resultado comando show.....	39
Figura 34. Resultado comando show.....	40
Figura 35. Resultado comando ping.....	43
Figura 36. Resultado comando ping.....	43
Figura 37. Resultado comando ping.....	43
Figura 38. Resultado comando ping.....	44
Figura 39. Resultado comando ping.....	44
Figura 40. Resultado comando ping.....	44
Figura 41. Resultado comando ping.....	44
Figura 42. Resultado comando ping.....	45

RESUMEN

La importancia de las telecomunicaciones en la vida diaria de las personas, de las organizaciones y de los países es cada día mayor dado a que las telecomunicaciones fomentan el desarrollo social y económico, mejoran los servicios de salud, de educación, de gobierno y la democracia, estimulan la creación de empleos, contribuyen a preservar el medio ambiente, entre muchos otros beneficios. Por eso, no es posible imaginarse el presente o el futuro sin telecomunicaciones. A través del curso Diplomado de profundización Cisco CCNP se adquieren diferentes conceptos presentados en los contenidos de formación y que se asocian con el contexto de las telecomunicaciones respecto a su aplicación en las redes de área extendida, en la identificación y comprensión del uso que tienen las tecnologías en el desarrollo de proyectos de conectividad de redes empresariales.

Palabras Clave: NETWORKING, ENRUTAMIENTO, DIRECCIONAMIENTO, PROTOCOLO, CCNP, TELECOMUNICACIONES.

INTRODUCCION

La importancia de las telecomunicaciones en la vida diaria de las personas, de las organizaciones y de los países es cada día mayor dado a que las telecomunicaciones fomentan el desarrollo social y económico, mejoran los servicios de salud, de educación, de gobierno y la democracia, estimulan la creación de empleos, contribuyen a preservar el medio ambiente, entre muchos otros beneficios. Por eso, no es posible imaginarse el presente o el futuro sin telecomunicaciones. El INTERNET es la principal NTIC a la que estamos expuestos. Pero hay muchas otras que poco a poco nos van invadiendo, gracias al poder de las telecomunicaciones y la electrónica.

Por medio del curso Diplomado de profundización Cisco CCNP adquirimos nuevos conceptos presentados en los contenidos de formación y se asocian con el contexto de las telecomunicaciones respecto a su aplicación en las redes de área extendida e identificar y comprender el uso que tiene las tecnologías en el desarrollo de proyectos de conectividad de redes empresariales. Entre los conocimientos adquiridos a través del diplomado de profundización CCNP está la buena comprensión del modelo OSI de siete capas y del TCP/IP de 4 capas, configuración de routers y switches Cisco, conocimiento avanzado y configuración de diferentes protocolos de enrutamiento, incluyendo RIP v2, EIGRP, OSPF, BGP, IS-IS, y protocolos encaminados IP, así como teoría de los protocolos de encaminamiento en general, aunque en los últimos años, Cisco se ha centrado en el protocolo IP, debido a la tendencia de este protocolo, se ha incorporado el estudio de la versión 6 de IP (IPv6) desde el CCNA Exploration y en la versión 4.0 del BSCI. La última versión del currículo incluye temas avanzados de enrutamiento como MPLS, enrutamiento de Multicast y filtrado/manipulación de las actualizaciones de enrutamiento, conocimiento de varias tecnologías y protocolos usados en redes, tales como spanning tree, VLANs, VTP Domain, ACLs, HSRP, VRRP, agregación de enlaces con LACP/PAgP, VLANs privadas, filtrado entre Vlans, teoría y práctica de calidad de servicio (QoS).

En el presente informe se encuentra el desarrollo de tres escenarios correspondientes a la temática de implementación de soluciones soportadas en enrutamiento avanzado como etapa final del curso Diplomado de profundización Cisco CCNP haciendo uso del software Packet Tracer o GNS3.

DESARROLLO DE LOS ESCENARIOS

Escenario 1

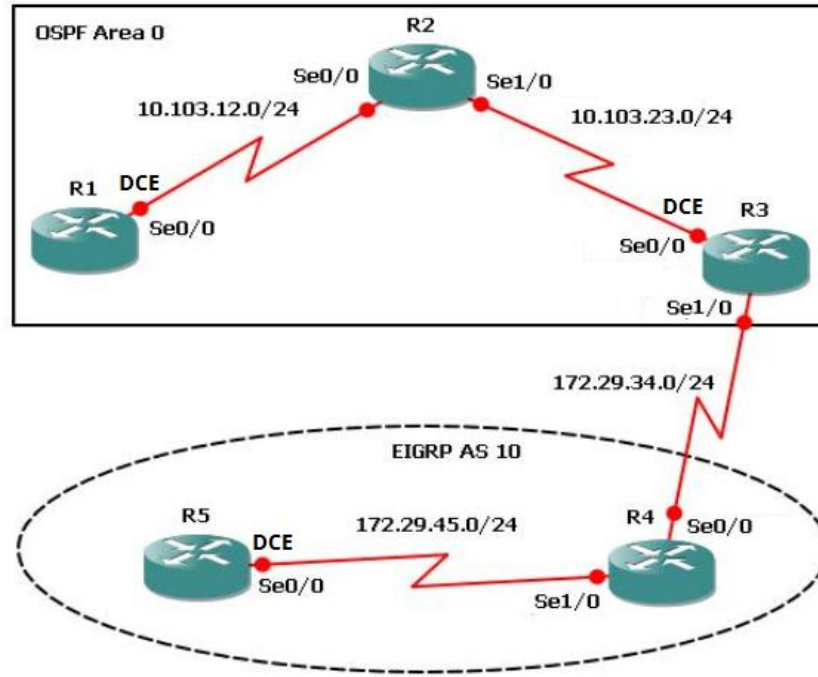


Figura 1. Esquema escenario 1.

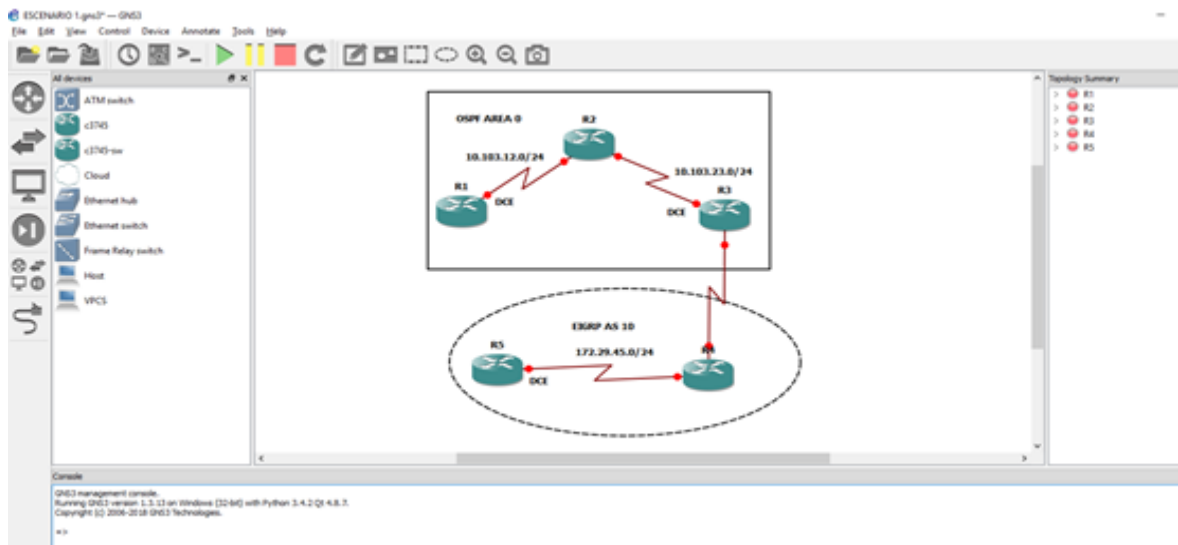


Figura 2. Montaje en software GNS3 escenario 1.

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

Para la configuración inicial, primeramente asignamos nombre a cada uno de los routers, direcciones de las interfaces y protocolos de comunicación haciendo uso del código:

Configuración R1

```
Router>
Router>enable                               Ingreso a modo privilegiado
Router#configure terminal                   Ingreso a modo de
configuración
Router(config)#hostname R1                 Asigno nombre al router
R1(config)#router ospf 1
R1(config-router)#router-d 1.1.1.1        Identifico el router
R1(config-router)#network 10.103.12.0 255.255.255.0 area 0
R1(config-router)#exit
R1(config)#interface s0/0                 Configuro interfaz serial 0
R1(config-if)#description to R2
R1(config-if)#ip address 10.103.12.1 255.255.255.0
R1(config-if)#clock rate 128000           Como es DCE se configura reloj
R1(config-if)#bandwidth 128
R1(config-if)#no shutdown                 Activo la interfaz
R1(config-if)#exit
R1(config)#end
R2#wr
```

Configuración R2

```
Router>
Router>enable                               Ingreso a modo privilegiado
Router#configure terminal                   Ingreso a modo de
configuración
Router(config)#hostname R2                 Asigno nombre al router
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2       Identifico el router
```

```

R2(config-router)#network 10.103.12.0 255.255.255.0 area 0
R2(config-router)#network 10.103.23.0 255.255.255.0 area 0
R2(config-router)#exit
R2(config)#interface s0/0                               Configuro interfaz serial 0
R2(config-if)#description to R1
R2(config-if)#ip address 10.103.12.2 255.255.255.0
R2(config-if)#no shutdown                               Activo la interfaz
R2(config-if)#exit
R2(config)#interface s0/1                               Configuro interfaz serial 0
R2(config-if)#description to R3
R2(config-if)#ip address 10.103.23.1 255.255.255.0
R2(config-if)#no shutdown                               Activo la interfaz
R2(config-if)#exit
R2(config)#end
R2#wr

```

Configuración R3

```

Router>
Router>enable                                           Ingreso a modo privilegiado
Router#configure terminal                               Ingreso a modo de
configuración
Router(config)#hostname R3                             Asigno nombre al router
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3                   Identifico el router
R3(config-router)#network 10.103.23.0 255.255.255.0 area 0
R3(config-router)#exit
R3(config)#interface s0/0                               Configuro interfaz serial 0
R3(config-if)#description to R2
R3(config-if)#ip address 10.103.23.2 255.255.255.0
R3(config-if)#clock rate 128000                       Como es DCE se configura reloj
R3(config-if)#bandwidth 128
R3(config-if)#no shutdown                               Activo la interfaz
R3(config-if)#exit
R3(config)#interface s0/1                               Configuro interfaz serial 1
R3(config-if)#description to R4
R3(config-if)#ip address 172.29.34.1 255.255.255.0
R3(config-if)#no shutdown                               Activo la interfaz
R3(config-if)#exit

```

```
R3(config)#end
```

```
R3#wr
```

Para permitir la comunicación con ambos protocolos y teniendo en cuenta que R4 en el puerto serial 0 se configura con eigrp, se procede a configurar igualmente el puerto serial 1 de R3.

```
R3#configure terminal          Ingreso a modo de
configuración
```

```
R3(config)#router eigrp 10    Configuro eigrp
```

```
R3(config-rtr)#eigrp router-id 3.3.3.3    Asigno identidad al router
```

```
R3(config-rtr)#network 172.29.34.0 255.255.255.0
```

```
R3(config-rtr)#exit
```

```
R3(config)#end
```

```
R3#wr
```

Configuración R4

```
Router>
```

```
Router>enable                Ingreso a modo privilegiado
```

```
Router#configure terminal    Ingreso a modo de
configuración
```

```
Router(config)#hostname R4   Asigno nombre al router
```

```
R4(config)#router eigrp 10   Configuro eigrp
```

```
R4(config-rtr)#eigrp router-id 4.4.4.4    Asigno identidad al router
```

```
R4(config-rtr)#network 172.29.34.0 255.255.255.0
```

```
R4(config-rtr)#network 172.29.45.0 255.255.255.0
```

```
R4(config-rtr)#exit
```

```
R4(config)#interface s0/0
```

```
R4(config-if)#ip address 172.29.34.2 255.255.255.0
```

```
R5(config-if)#no shutdown    Activo la interfaz
```

```
R4(config-if)#exit
```

```
R4(config)#interface s0/1
```

```
R4(config-if)#ip address 172.29.45.1 255.255.255.0
```

```
R5(config-if)#no shutdown    Activo la interfaz
```

```
R4(config-if)#exit
```

```
R4(config)#end
```

```
R4#wr
```

Configuración R5

```
Router>
Router>enable                               Ingreso a modo privilegiado
Router#configure terminal                   Ingreso a modo de
configuración
Router(config)#hostname R5                 Asigno nombre al router
R5(config)#router eigrp 10                 Configuro eigrp
R5(config-rtr)#eigrp router-id 5.5.5.5    Asigno identidad al router
R4(config-rtr)#network 172.29.45.0 255.255.255.0
R5(config)#interface s0/0
R5(config-if)#ip address 172.29.45.2 255.255.255.0
R5(config-if)#no shutdown                 Activo la interfaz
R5(config-if)#exit
R5(config)#end
R5#wr
```

2. Cree cuatro nuevas interfaces de Loopback en R1 utilizando la asignación de direcciones 10.1.0.0/22 y configure esas interfaces para participar en el área 0 de OSPF.

Primeramente creamos las interfaces Loopback, para lo cual, identifico que la máscara de red es 255.255.252.0

```
R1#conf t
R1(config)#interface loopback 4           Creo la interfaz lo 4
R1(config-if)#ip address 10.1.4.1 255.255.252.0 Establezco la dirección IP
R1(config-if)#ip ospf 1 area 0           Con este comando configuro
la int. En OSPF
R1(config-if)#exit
R1(config)# interface loopback 8         Creo la interfaz lo 8
R1(config-if)#ip address 10.1.8.1 255.255.252.0 Establezco la dirección IP
R1(config-if)#ip ospf 1 area 0           Con este comando configuro
la int. En OSPF
R1(config-if)#exit
R1(config)# interface loopback 12        Creo la interfaz lo 12
R1(config-if)#ip address 10.1.12.1 255.255.252.0 Establezco la dirección IP
R1(config-if)#ip ospf 1 area 0           Con este comando configuro
la int. En OSPF
```

```

R1(config-if)#exit
R1(config)# interface loopback 16          Creo la interfaz lo 16
R1(config-if)#ip address 10.1.16.1 255.255.252.0 Establezco la dirección IP
R1(config-if)#ip ospf 1 area 0           Con este comando configuro
la int. En OSPF
R1(config-if)#exit
R1(config)#end
R1#wr

```

Para verificar que las nuevas interfaces loopback hayan quedado configuradas para participar en el protocolo OSPF se hace uso del comando **show ip ospf brief** obteniendo como resultado (véase en la Figura 3):

```

R1#sh ip ospf interface bri
Interface      PID  Area      IP Address/Mask    Cost  State Nbrs F/C
Lo16           1    0         10.1.16.1/22      1     LOOP  0/0
Lo12           1    0         10.1.12.1/22      1     LOOP  0/0
Lo8            1    0         10.1.8.1/22       1     LOOP  0/0
Lo4            1    0         10.1.4.1/22       1     LOOP  0/0
Se0/0         1    0         10.103.12.1/24    781   P2P   1/1

```

Figura 3.Resultado comando show ip ospf brief.

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

```

Para verificar que hayan sido creadas las interfaces loopback, utilizo el comando **show ip interfaces brief | include up** obteniendo (véase en la Figura 4):

```
R5#sh ip interface bri | include up
Serial0/0          172.29.45.2      YES NVRAM  up          up
Vlan1              unassigned       YES NVRAM  up          down
Loopback4         172.5.4.1       YES manual up          up
Loopback8         172.5.8.1       YES manual up          up
Loopback12        172.5.12.1      YES manual up          up
Loopback16        172.5.16.1      YES manual up          up
```

Figura 4. Resultado comando show ip interfaces brief | include up.

```
R5(config)#router eigrp 10
R5(config-router)#no auto-summary
R5(config-router)#network 172.5.4.0 255.255.255.0
R5(config-router)#network 172.5.8.0 255.255.255.0
R5(config-router)#network 172.5.12.0 255.255.255.0
R5(config-router)#network 172.5.16.0 255.255.255.0
R5(config-router)#network 172.29.45.0 255.255.255.0
R5(config-router)#exit
R5(config)#end
R5#wr
```

Para verificar que las interfaces loopback hayan quedado integradas al protocolo EIGRP utilizo el comando **show ip eigrp interfaces**, obteniendo (véase en la Figura 5):

```
R5#sh ip eigrp int
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	1	0/0	18	0/15	83	0
Lo4	0	0/0	0	0/1	0	0
Lo8	0	0/0	0	0/1	0	0
Lo12	0	0/0	0	0/1	0	0
Lo16	0	0/0	0	0/1	0	0

Figura 5. Resultado comando show ip eigrp interfaces.

Se puede apreciar que las 4 nuevas interfaces de loopback ya hacen parte en EIGRP.

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

Se hace uso del comando **show ip route** y se obtiene (véase en la Figura 6):

```
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

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

Figura 6. Resultado comando show ip route.

Con lo anterior se puede evidenciar que el router R3 ha aprendido las 8 nuevas interfaces de loopback de ambos protocolos.

Protocolo OSPF en R1 (véase en la Figura 7).

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

Figura 7. Protocolo OSPF en R1.

Protocolo EIGRP en R5 (véase en la Figura 8).

```
    172.5.0.0/22 is subnetted, 4 subnets
D       172.5.8.0 [90/2809856] via 172.29.34.2, 00:12:09, Serial0/1
D       172.5.12.0 [90/2809856] via 172.29.34.2, 00:12:01, Serial0/1
D       172.5.4.0 [90/2809856] via 172.29.34.2, 00:14:21, Serial0/1
D       172.5.16.0 [90/2809856] via 172.29.34.2, 00:11:52, Serial0/1
```

Figura 8. Protocolo EIGRP en R5.

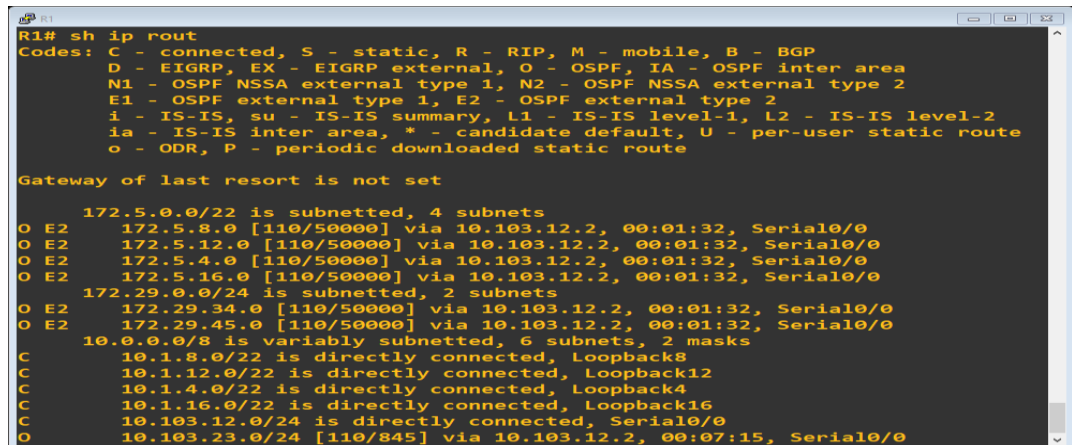
5. R3 para redistribuir las rutas EIGRP en OSPF usando el costo de 50000 y luego redistribuya las rutas OSPF en EIGRP usando un ancho de banda T1 y 20,000 microsegundos de retardo.

Primeramente se redistribuyen las rutas EIGRP en OSPF y viceversa utilizando los siguientes comandos:

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

6. Verifique en R1 y R5 que las rutas del sistema autónomo opuesto existen en su tabla de enrutamiento mediante el comando **show ip route** (véase en la Figura 9, Figura 10).

R1.



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

Gateway of last resort is not set

172.5.0.0/22 is subnetted, 4 subnets
O E2 172.5.8.0 [110/50000] via 10.103.12.2, 00:01:32, Serial0/0
O E2 172.5.12.0 [110/50000] via 10.103.12.2, 00:01:32, Serial0/0
O E2 172.5.4.0 [110/50000] via 10.103.12.2, 00:01:32, Serial0/0
O E2 172.5.16.0 [110/50000] via 10.103.12.2, 00:01:32, Serial0/0
172.29.0.0/24 is subnetted, 2 subnets
O E2 172.29.34.0 [110/50000] via 10.103.12.2, 00:01:32, Serial0/0
O E2 172.29.45.0 [110/50000] via 10.103.12.2, 00:01:32, Serial0/0
10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C 10.1.8.0/22 is directly connected, Loopback8
C 10.1.12.0/22 is directly connected, Loopback12
C 10.1.4.0/22 is directly connected, Loopback4
C 10.1.16.0/22 is directly connected, Loopback16
C 10.103.12.0/24 is directly connected, Serial0/0
O 10.103.23.0/24 [110/845] via 10.103.12.2, 00:07:15, Serial0/0
```

Figura 9. En R1 se encuentran las loopbacks creadas en R5.

R5

```
R5#sh ip rou
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

 172.5.0.0/22 is subnetted, 4 subnets
 C    172.5.8.0 is directly connected, Loopback8
 C    172.5.12.0 is directly connected, Loopback12
 C    172.5.4.0 is directly connected, Loopback4
 C    172.5.16.0 is directly connected, Loopback16
 172.29.0.0/24 is subnetted, 2 subnets
 D    172.29.34.0 [90/2681856] via 172.29.45.1, 00:04:55, Serial0/0
 C    172.29.45.0 is directly connected, Serial0/0
 10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
 D EX 10.1.8.1/32 [170/7801856] via 172.29.45.1, 00:02:46, Serial0/0
 D EX 10.1.12.1/32 [170/7801856] via 172.29.45.1, 00:02:46, Serial0/0
 D EX 10.1.4.1/32 [170/7801856] via 172.29.45.1, 00:02:46, Serial0/0
 D EX 10.1.16.1/32 [170/7801856] via 172.29.45.1, 00:02:46, Serial0/0
 D EX 10.103.12.0/24 [170/7801856] via 172.29.45.1, 00:02:49, Serial0/0
 D EX 10.103.23.0/24 [170/7801856] via 172.29.45.1, 00:02:49, Serial0/0
```

Figura 10. En R5 se encuentran las loopbacks creadas en R1.

Escenario 2

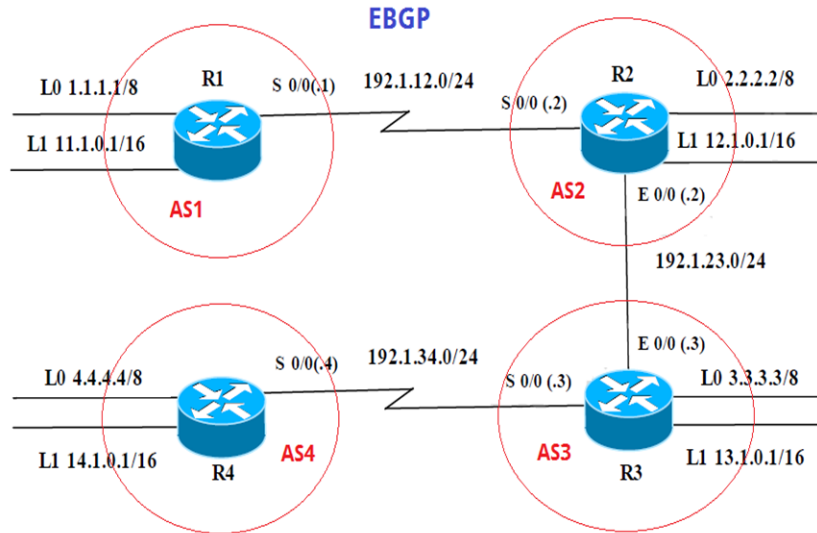


Figura 11. Esquema escenario 2.

Información para configuración de los Routers

Tabla 1. Tabla de enrutamiento y configuración de los Routers.

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

R1

```

enable
conf terminal
int lo 0
ip address 1.1.1.1 255.0.0.0
exit
int lo 1
ip address 11.1.0.1 255.255.0.0
exit
int s0/0
ip address 192.1.12.1 255.255.255.0
clockrate 64000
no shut
exit
end
wr

```

R2

```
enable
conf terminal
int lo 0
ip address 2.2.2.2 255.0.0.0
exit
int lo 1
ip address 12.1.0.1 255.255.0.0
exit
int s0/0
ip address 192.1.12.2 255.255.255.0
no shut
exit
int fastEthernet 0/0
ip address 192.1.23.2 255.255.255.0
no shut
```

R3

```
enable
conf terminal
int lo 0
ip address 3.3.3.3 255.0.0.0
exit
int lo 1
ip address 13.1.0.1 255.255.0.0
exit
int fastEthernet 0/0
ip address 192.1.23.3 255.255.255.0
no shut
exit
int s0/0
ip address 192.1.34.3 255.255.255.0
no shut
exit
end
```

R4

```
enable
```

```
conf terminal
int lo 0
ip address 4.4.4.4 255.0.0.0
exit
int lo 1
ip address 14.1.0.1 255.255.0.0
exit
int s0/0
ip address 192.1.34.4 255.255.255.0
clockrate 64000
no shut
exit
end
```

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

```
enable
conf terminal
router bgp 1
bgp router-id 11.11.11.11
neighbor 192.1.12.2 remote-as 2
network 1.0.0.0 mask 255.0.0.0
network 11.1.0.0 mask 255.255.0.0
```

R2

```
enable
conf terminal
router bgp 2
bgp router-id 22.22.22.22
neighbor 192.1.12.1 remote-as 1
network 2.0.0.0 mask 255.0.0.0
network 12.1.0.0 mask 255.255.0.0 (véase en la Figura 12, Figura 13)
```

```

*Mar 1 00:08:15.971: ASYS-5-CONFIG_I: Configured from console by console
R1#wr
Building configuration...
[OK]
R1#
*Mar 1 00:08:55.219: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
R1#enable
R1#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router bgp 1
R1(config-router)#bgp router-id 11.11.11.11
R1(config-router)#neighbor 193.1.12.2 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)#exit
R1(config)#exit
R1#
*Mar 1 00:27:16.783: ASYS-5-CONFIG_I: Configured from console by console
R1#wr
% Unknown command or computer name, or unable to find computer address
R1#wr
Building configuration...

```

Figura 12. Resultado comando *show ip route*.

```

R2#enable
R2#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router bgp 2
R2(config-router)#bgp router-id 22.22.22.22
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#network 2.0.0.0 mask 255.0.0.0
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
R2(config-router)#end
R2#
*Mar 1 00:30:07.327: ASYS-5-CONFIG_I: Configured from console by console
R2#wr

```

Figura 13. Resultado comando *show ip route*.

- 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** (véase en la Figura 14, Figura 15).

R2

```

enable
conf terminal
router bgp 2
neighbor 192.1.23.3 remote-as 3

```

R3

```

enable
conf terminal
router bgp 3
bgp router-id 33.33.33.33
neighbor 192.1.23.2 remote-as 2
network 3.0.0.0 mask 255.0.0.0
network 13.1.0.0 mask 255.255.0.0

```

```

[OK]
R3#enable
R3#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config-router)#router bgp 3
R3(config-router)#neighbor 192.1.23.3 remote-as 3
R3#
R3#
Building configuration...
*Mar 1 00:44:41.483: %SYS-5-CONFIG_I: Configured from console by console[OK]
R3#
*Mar 1 00:45:30.939: %BGP-5-ADJCHANGE: neighbor 192.1.23.3 Up
R3#
Building configuration...
[OK]
R3#show ip route
% Invalid input detected at '''' marker.
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       Ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C 192.1.22.0/24 is directly connected, Serial0/0
C 192.0.0/8 [20/0] via 192.1.23.3, 00:15:33
C 2.0.0.0/8 is directly connected, Loopback0
C 3.0.0.0/8 [20/0] via 192.1.23.3, 00:10:00
C 192.1.23.0/24 is directly connected, FastEthernet0/0
B 11.0.0.0/16 is summarized, 1 subnets
  11.0.0.0 [20/0] via 192.1.23.3, 00:15:33
C 12.0.0.0/16 is summarized, 1 subnets
  12.0.0.0 is directly connected, Loopback1
C 13.0.0.0/16 is summarized, 1 subnets
  13.0.0.0 [20/0] via 192.1.23.3, 00:10:11
R3#

```

Figura 14. Resultado comando *show ip route*.

```

R3
*Mar 1 00:15:25.407: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
R3#enable
R3#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config-router)#router bgp 3
R3(config-router)#bgp router-id 33.33.33.33
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#network 3.0.0.0 mask 255.0.0.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3#
R3#
*Mar 1 00:45:30.923: %BGP-5-ADJCHANGE: neighbor 192.1.23.2 Up
*Mar 1 00:45:31.539: %SYS-5-CONFIG_I: Configured from console by console
R3#
Building configuration...
[OK]
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       Ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

B 1.0.0.0/8 [20/0] via 192.1.23.2, 00:03:21
C 2.0.0.0/8 [20/0] via 192.1.23.2, 00:03:21
C 3.0.0.0/8 is directly connected, Loopback0
C 192.1.23.0/24 is directly connected, FastEthernet0/0
B 11.0.0.0/16 is summarized, 1 subnets
  11.0.0.0 [20/0] via 192.1.23.2, 00:02:21
C 192.1.34.0/24 is directly connected, Serial0/0
C 13.0.0.0/16 is summarized, 1 subnets
  13.1.0.0 [20/0] via 192.1.23.2, 00:02:21
  13.0.0.0/16 is summarized, 1 subnets
R3#

```

Figura 15. Resultado comando *show ip route*.

- 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** (véase en la Figura 16).

R3

```

enable
conf terminal
router bgp 3
neighbor 192.1.34.4 remote-as 4

```

R4

enable

conf terminal

router bgp 4

bgp router-id 44.44.44.44

neighbor 192.1.34.3 remote-as 3

network 4.0.0.0 mask 255.0.0.0

exit


ip route 3.0.0.0 255.0.0.0 192.1.34.3

router bgp 4

no network 4.0.0.0 mask 255.0.0.0

network 4.0.0.0 mask 255.0.0.0

network 14.1.0.0 mask 255.255.0.0



```
R4
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#int lo 0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#exit
R4(config)#int lo 1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#exit
R4(config)#int s0/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#clockrate 64000
R4(config-if)#no shut
R4(config-if)#exit
R4(config)#end
*Mar  1 00:15:22.495: %LINEPROTO-3-UPDOWN: Line protocol on Interface Loopback0, changed state to up
*Mar  1 00:15:22.839: %LINEPROTO-3-UPDOWN: Line protocol on Interface Loopback1, changed state to up
R4(config)#end
*Mar  1 00:15:24.463: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
R4(config)#end
*Mar  1 00:15:25.487: %LINEPROTO-3-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
R4(config)#end
R4#
*Mar  1 00:15:29.735: %SYS-5-CONFIG_I: Configured from console by console
R4#wr
Building configuration...
```

Figura 16. Resultado comando *show ip route*.

Escenario 3

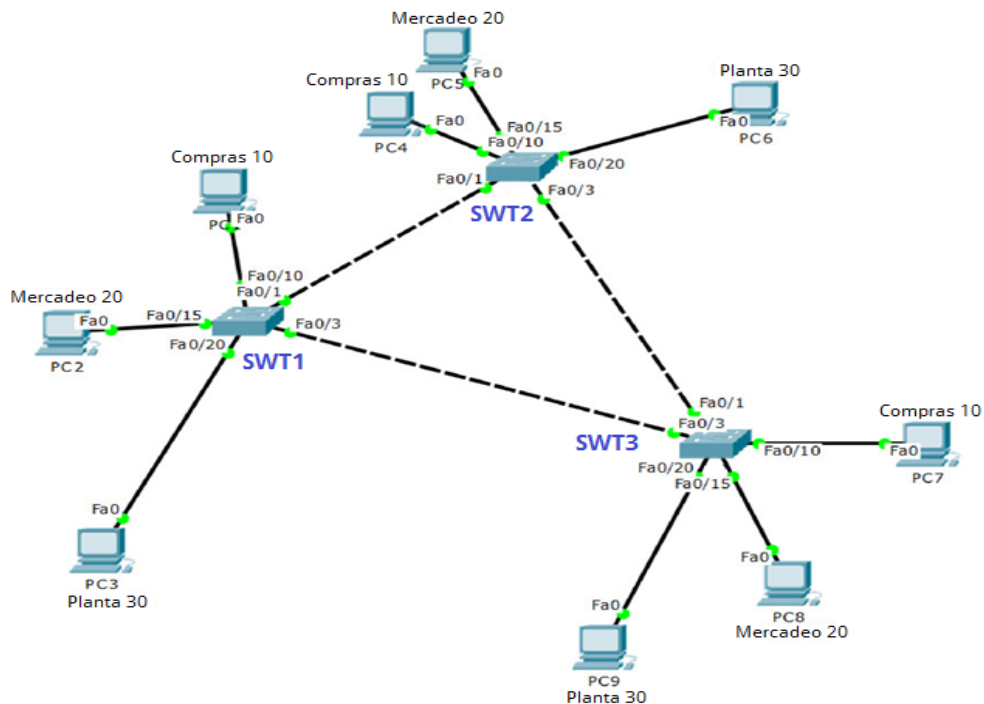


Figura 17. Esquema escenario 3.

A. Configurar VTP

1. Todos los switches se configurarán para usar VTP para las actualizaciones de VLAN. El switch SWT2 se configurará como el servidor. Los switches SWT1 y SWT3 se configurarán como clientes. Los switches estarán en el dominio VPT llamado CCNP y usando la contraseña cisco.

Primero que todo se utilizó el siguiente código para cada uno de los routers:

SWT1

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

SWT2

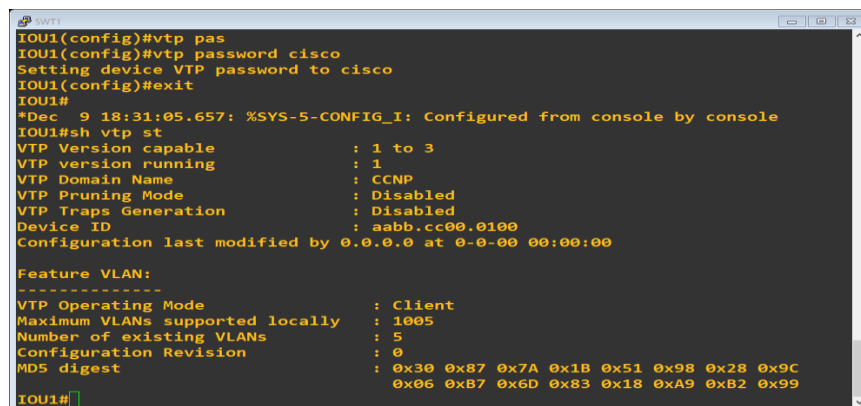
```
IOU1#configure terminal
IOU1(config)#hostname SWT2
SWT1(config)#vtp domain CCNP
SWT1(config)#vtp mode server
SWT1(config)#vtp password cisco
SWT1(config)#exit
SWT1#wr
```

SWT3

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

2. Verifique las configuraciones mediante el comando **show vtp status** (véase en la Figura 18, Figura 19, Figura 20).

SWT1



```
IOU1(config)#vtp pas
IOU1(config)#vtp password cisco
Setting device VTP password to cisco
IOU1(config)#exit
IOU1#
*Dec  9 18:31:05.657: %SYS-5-CONFIG_I: Configured from console by console
IOU1#sh vtp st
VTP Version capable      : 1 to 3
VTP version running     : 1
VTP Domain Name         : CCNP
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID                : aabb.cc00.0100
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN:
-----
VTP Operating Mode      : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs : 5
Configuration Revision  : 0
MD5 digest              : 0x30 0x87 0x7A 0x1B 0x51 0x98 0x28 0x9C
                       : 0x06 0xB7 0x6D 0x83 0x18 0xA9 0xB2 0x99

IOU1#
```

Figura 18. Resultado comando *show vtp status*.

SWT2

```
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 1350 bytes to 816 bytes[OK]
SWT2#sh vtp st
VTP Version capable      : 1 to 3
VTP version running      : 1
VTP Domain Name          : CCNP
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                 : aabb.cc00.0200
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)

Feature VLAN:
-----
VTP Operating Mode       : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 5
Configuration Revision   : 0
MD5 digest               : 0x30 0x87 0x7A 0x1B 0x51 0x98 0x28 0x9C
                        : 0x06 0xB7 0x6D 0x83 0x18 0xA9 0xB2 0x99
SWT2#
```

Figura 19. Resultado comando *show vtp status*.

SWT3

```
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
*Dec 9 18:41:05.704: %SYS-5-CONFIG_I: Configured from console by console
[confirm]
Building configuration...
Compressed configuration from 1350 bytes to 819 bytes[OK]
SWT3#sh vtp st
VTP Version capable      : 1 to 3
VTP version running      : 1
VTP Domain Name          : CCNP
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                 : aabb.cc00.0300
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN:
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs : 5
Configuration Revision   : 0
MD5 digest               : 0x30 0x87 0x7A 0x1B 0x51 0x98 0x28 0x9C
                        : 0x06 0xB7 0x6D 0x83 0x18 0xA9 0xB2 0x99
SWT3#
```

Figura 20. Resultado comando *show vtp status*.

B. Configurar DTP (Dynamic Trunking Protocol)

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

Se utilizó el comando **switchport mode Dynamic desirable** en ambos switches.

SWT1

```
SWT1#configure terminal
SWT1(config)#interface range ethernet0/0 - 1
SWT1(config-if-range)#switchport trunk encapsulation dot1q Habilito el trunk
standar
SWT1(config-if-range)#switchport mode trunk Habilito el modo
trunk en la int.
SWT1(config-if-range)#switchport mode dynamic desirable Configuro
dynamic desirable
SWT1(config-if-range)#no shutdown
SWT1(config-if-range)#exit
SWT1(config)#end
SWT1#wr
```

SWT2

```
SWT2#configure terminal
SWT2(config)#interface range ethernet0/0
SWT2(config-if-range)#switchport trunk encapsulation dot1q Habilito el trunk
standar
SWT2(config-if-range)#switchport mode trunk Habilito el modo
trunk en la int
SWT2(config-if-range)#switchport mode dynamic desirable Configuro
dynamic desirable
SWT2(config-if-range)#no shutdown
SWT2(config-if-range)#exit
SWT2(config)#interface range ethernet0/2
SWT2(config-if-range)#switchport trunk encapsulation dot1q Habilito el trunk
standar
SWT2(config-if-range)#switchport mode trunk Habilito el modo
trunk en la int
SWT2(config-if-range)#switchport mode dynamic desirable Configuro
dynamic desirable
SWT2(config-if-range)#no shutdown
SWT2(config-if-range)#exit
SWT2(config)#end
SWT2#wr
```

2. Verifique el enlace "trunk" entre SWT1 y SWT2 usando el comando **show interfaces trunk** (véase en la Figura 21, Figura 22).

SWT1

```
IOU1#sh int trunk
```

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

Figura 21. Resultado comando show interfaces trunk.

SWT2

```
SWT2#sh int trunk
```

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

Figura 22. Resultado comando show interfaces trunk.

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

Anteriormente se configuro la interfaz de SWT1, teniendo presente que es la interfaz ethernet 0/1

Para fvnnfSwitch SWT3

```
SWT3#configure terminal
```

```
SWT3(config)#interface range ethernet0/1
```

```
SWT3(config-if-range)#switchport trunk encapsulation dot1q Habilito el trunk standar
```



```
SWT3(config-if-range)#exit
SWT3(config)#end
SWT3#wr
```

C. Agregar VLANs y asignar puertos.

1. En STW1 agregue la VLAN 10. En STW2 agregue las VLANS Compras (10), Mercadeo (20), Planta (30) y Admon (99)

Se crea la VLAN 10 el switch SWT1 se deben crear en el switch SWT2 ya que es el que funciona en el modo servidor y es en este modo donde se pueden crear o agregar las vlan's, ya que en modo client no es posible.

```
SWT2#configure terminal
SWT2(config)#vlan 10                                Creo la vlan 10
SWT2(config-vlan)#name Compras                      Asigno el nombre
Compras
SWT2(config-vlan)#exit
SWT2(config)#vlan 20                                Creo la vlan 20
SWT2(config-vlan)#name Mercadeo                     Asigno el nombre
Mercadeo
SWT2(config-vlan)#exit
SWT2(config)#vlan 30                                Creo la vlan 30
SWT2(config-vlan)#name Planta                       Asigno el nombre
Planta
SWT2(config-vlan)#exit
SWT2(config)#vlan 99                                Creo la vlan 99
SWT2(config-vlan)#name Admon                        Asigno el nombre
Admon
SWT2(config-vlan)#exit
SWT2(config)#exit
SWT2#wr
```

2. Verifique que las VLANs han sido agregadas correctamente.

Comando show vlan brief (véase en la Figura 24, Figura 25)

```
SWT2#sh vlan bri
VLAN Name                Status    Ports
-----
1    default                active    Et0/1, Et0/3, Et1/0, Et1/1
      Et1/2, Et1/3, Et2/0, Et2/1
      Et2/2, Et2/3, Et3/0, Et3/1
      Et3/2, Et3/3
10   Compras                active
20   Mercadeo               active
30   Planta                 active
99   Admon                  active
1002 fddi-default           act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default         act/unsup
```

Figura 24. Resultado Comando show vlan brief.

SWT1

```
SWT1#sh vlan bri
VLAN Name                Status    Ports
-----
1    default                active    Et0/2, Et0/3, Et1/0, Et1/1
      Et1/2, Et1/3, Et2/0, Et2/1
      Et2/2, Et2/3, Et3/0, Et3/1
      Et3/2, Et3/3
10   Compras                active
20   Mercadeo               active
30   Planta                 active
99   Admon                  active
1002 fddi-default           act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default         act/unsup
```

Figura 25. Resultado Comando show vlan brief.

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

Tabla 2. Tabla de direccionamiento IP de los PCs.

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

Dado a que utilice puertos de los switches diferentes mi tabla queda de la siguiente forma:

Tabla 3. Tabla de direccionamiento IP de los PCs.

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

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

SWT1

```

SWT1#configure terminal
SWT1(config)#interface ethernet 1/0           Ingreso al puerto
SWT1(config-vlan)#switchport mode access     Configuro el modo
de acceso
SWT1(config-vlan)#switchport access vlan 10  Asino la VLAN10
al puerto
SWT1(config-vlan)#exit
    
```

SWT2

```

SWT2#configure terminal
SWT2(config)#interface ethernet 1/0           Ingreso al puerto
SWT2(config-vlan)#switchport mode access     Configuro el modo
de acceso
SWT2(config-vlan)#switchport access vlan 10  Asino la VLAN10
al puerto
SWT2(config-vlan)#exit
    
```

SWT3

```

SWT3#configure terminal
    
```

SWT3(config)#interface ethernet 1/0	Ingreso al puerto
SWT3(config-vlan)#switchport mode access	Configuro el modo
de acceso	
SWT3(config-vlan)#switchport access vlan 10	Asino la VLAN10
al puerto	
SWT3(config-vlan)#exit	

5. Repita el procedimiento para los puertos F0/15 y F0/20 en SWT1, SWT2 y SWT3. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

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

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

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

SWT2#configure terminal	
SWT2(config)#interface ethernet 1/1	Ingreso al puerto
SWT2(config-vlan)#switchport mode access	Configuro el modo
de acceso	
SWT2(config-vlan)#switchport access vlan 20	Asino la VLAN20
al puerto	

SWT2(config-vlan)#exit	
SWT2(config)#interface ethernet 1/2	Ingreso al puerto
SWT2(config-vlan)#switchport mode access	Configuro el modo
de acceso	
SWT2(config-vlan)#switchport access vlan 30	Asino la VLAN30
al puerto	
SWT2(config-vlan)#exit	
SWT2(config)#end	
SWT2#wr	Guardo
configuración	

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

SWT3#configure terminal	
SWT3(config)#interface ethernet 1/1	Ingreso al puerto
SWT3(config-vlan)#switchport mode access	Configuro el modo
de acceso	
SWT3(config-vlan)#switchport access vlan 20	Asino la VLAN20
al puerto	
SWT3(config-vlan)#exit	
SWT3(config)#interface ethernet 1/2	Ingreso al puerto
SWT3(config-vlan)#switchport mode access	Configuro el modo
de acceso	
SWT3(config-vlan)#switchport access vlan 30	Asino la VLAN30
al puerto	
SWT3(config-vlan)#exit	
SWT3(config)#end	
SWT3#wr	Guardo
configuración	

Asignación IP a VPC 01

PC-1>ip 190.108.10.1/24

Para confirmar que haya quedado asignada la IP, utilizo el comando show en la consola, la cual me indica los parámetros de IP (véase en la Figura 26).

```

PC-1> show
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC-1 190.108.10.1/24 0.0.0.0 00:50:79:66:68:00 10013 127.0.0.1:10014
fe80::250:79ff:fe66:6800/64

```

Figura 26. Resultado comando show.

Asignación IP a VPC 02

PC-1>ip 190.108.20.2/24

Para confirmar que haya quedado asignada la IP, utilizo el comando show en la consola, la cual me indica los parámetros de IP (véase en la Figura 27).

```

PC-2> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC-2 190.108.20.2/24 0.0.0.0 00:50:79:66:68:01 10009 127.0.0.1:10010
fe80::250:79ff:fe66:6801/64

```

Figura 27. Resultado comando show.

Asignación IP a VPC 03

PC-1>ip 190.108.30.3/24

Para confirmar que haya quedado asignada la IP, utilizo el comando show en la consola, la cual me indica los parámetros de IP (véase en la Figura 28).

```

PC-3> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC-3 190.108.30.3/24 0.0.0.0 00:50:79:66:68:02 10011 127.0.0.1:10012
fe80::250:79ff:fe66:6802/64

```

Figura 28. Resultado comando show.

Asignación IP a VPC 04

PC-1>ip 190.108.10.4/24

Para confirmar que haya quedado asignada la IP, utilizo el comando show en la consola, la cual me indica los parámetros de IP (véase en la Figura 29).

```
PC-4> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC-4 190.108.10.4/24 0.0.0.0 00:50:79:66:68:03 10015 127.0.0.1:10016
fe80::250:79ff:fe66:6803/64
```

Figura 29. Resultado comando show.

Asignación IP a VPC 05

PC-1>ip 190.108.20.5/24

Para confirmar que haya quedado asignada la IP, utilizo el comando show en la consola, la cual me indica los parámetros de IP (véase en la Figura 30).

```
PC-5> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC-5 190.108.20.5/24 0.0.0.0 00:50:79:66:68:04 10017 127.0.0.1:10018
fe80::250:79ff:fe66:6804/64
```

Figura 30. Resultado comando show.

Asignación IP a VPC 06

PC-1>ip 190.108.30.6/24

Para confirmar que haya quedado asignada la IP, utilizo el comando show en la consola, la cual me indica los parámetros de IP (véase en la Figura 31).

```
PC-6> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
PC-6 190.108.30.6/24 0.0.0.0 00:50:79:66:68:05 10019 127.0.0.1:10020
fe80::250:79ff:fe66:6805/64
```

Figura 31. Resultado comando show.

Asignación IP a VPC 07

PC-1>ip 190.108.10.7/24

Para confirmar que haya quedado asignada la IP, utilizo el comando show en la consola, la cual me indica los parámetros de IP (véase en la Figura 32).

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

Figura 32. Resultado comando show.

Asignación IP a VPC 08

PC-1>ip 190.108.20.8/24

Para confirmar que haya quedado asignada la IP, utilizo el comando show en la consola, la cual me indica los parámetros de IP (véase en la Figura 33).

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

Figura 33. Resultado comando show.

Asignación IP a VPC 09

PC-1>ip 190.108.30.9/24

Para confirmar que haya quedado asignada la IP, utilizo el comando show en la consola, la cual me indica los parámetros de IP (véase en la Figura 34).

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

Figura 34. Resultado comando show.

D. Configurar las direcciones IP en los Switches.

1. En cada uno de los Switches asigne una dirección IP al SVI (*Switch Virtual Interface*) para VLAN 99 de acuerdo con la siguiente tabla de direccionamiento y active la interfaz.

Tabla 4. Direccionamiento IP para los SVI (*Switch Virtual Interface*).

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

Se configura VLAN99 para el switch SWT1:

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

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

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

SWT3#configure terminal

```
SWT3(config)#interface vlan 99                               Ingreso a la vlan
SWT3(config-vlan)#ip address 190.108.99.3 255.255.255.0   Configuro
```

```
SWT3(config-vlan)#no shutdown
SWT3(config-vlan)#exit
SWT3(config)#end
SWT3#wr
configuración
```

Guardo

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.

Para entender mejor he realizado una tabla identificando los PCS de cada Vlan con colores diferentes, quedando de la siguiente forma:

Vlan10 = Color Azul

Vlan20 = Color Amarillo

Vlan30 = Color Rojo

Tabla 4. Verificación comando ping.

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

PC1

Ping entre PC1 y PC4, PC1 y PC7 (véase en la Figura 31) Ping entre PC1 a PC2, PC5, PC8 (véase en la Figura 35, figura 36)

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

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

Figura 35. Resultado comando ping.

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

PC-1> ping 190.108.20.5
No gateway found

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

Figura 36. Resultado comando ping.

Ping entre PC1 a PC3, PC6, PC9 (véase en la Figura 37).

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

PC-1> ping 190.108.30.6
No gateway found

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

Figura 37. Resultado comando ping.

Al realizar ping con las PC's que pertenecen a otra VLAN diferente estos no son posibles de realizar.

PC2

Ping entre PC2 y PC5, PC1 y PC8 (véase en la Figura 34) Ping entre PC2 a PC1, PC4, PC7 (véase en la Figura 38, figura 39).

```

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

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

```

Figura 38. Resultado comando ping.

```

PC-2> ping 190.108.10.1
No gateway found

PC-2> ping 190.108.10.4
No gateway found

PC-2> ping 190.108.10.7
No gateway found

```

Figura 39. Resultado comando ping.

Ping entre PC2 a PC3, PC6, PC9 (véase en la Figura 40).

```

PC-2> ping 190.108.30.3
No gateway found

PC-2> ping 190.108.30.6
No gateway found

PC-2> ping 190.108.30.9
No gateway found

```

Figura 40. Resultado comando ping.

Al realizar ping con las PC's que pertenecen a otra VLAN diferente estos no son posibles de realizar.

PC3

Ping entre PC3 y PC6, PC1 y PC9 (véase en la Figura 37) Ping entre PC3 a PC1, PC4, PC7 (véase en la Figura 41).

```

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

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

```

Figura 41. Resultado comando ping.

Ping entre PC3 a PC2, PC5, PC8 (véase en la Figura 43).

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

PC-3> ping 190.108.20.5
No gateway found

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

Figura 42. Resultado comando ping.

Al realizar ping con las PC's que pertenecen a otra VLAN diferente estos no son posibles de realizar.

CONCLUSIONES

Con el desarrollo de los tres escenarios solicitados se logra evidenciar la implementación de la temática aprendida a lo largo del curso Diplomado de profundización Cisco CCNP.

Se detalla el paso a paso y el uso de los diferentes comandos en cada una de las etapas realizadas y el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

El curso Diplomado de profundización Cisco CCNP me permitió apropiarme de los conceptos presentados en los contenidos de formación y que se asocian con el contexto de las telecomunicaciones respecto a su aplicación en las redes de área extendida e identificar y comprender el uso que tiene las tecnologías en el desarrollo de proyectos de conectividad de redes empresariales.

REFERENCIAS BIBLIOGRAFICAS

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing IPv6 in the Enterprise Network. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Fundamentals Review. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>

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-NT1InMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Switching Features and Technologies. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>