

EVALUACIÓN FINAL
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DUVAN FERNEY RODRIGUEZ FORIGUA

CC 1075676802

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
INGENIERÍA DE TELECOMUNICACIONES
DIPLOMADO CISCO CCNP
ZIPAQUIRA
2019

EVALUACIÓN PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DUVAN FERNEY RODRIGUEZ FORIGUA
CC 1075676802

Diplomado de profundización cisco CCNP prueba de
Habilidades prácticas

Gerardo Granados
Magister En Telemática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
INGENIERÍA DE TELECOMUNICACIONES
DIPLOMADO CISCO CCNP
ZIAPAQUIRA
2019

NOTA DE ACEPTACION

Presidente del jurado

Jurado

Jurado

Zipaquirá 03 de junio de 2019

CONTENIDO

INTRODUCCIÓN	9
ESCENARIO 1	10
ESCENARIO 2	17
ESCENARIO 3	25
CONCLUSIONES	38
BIBLIOGRAFÍA	39

LISTADO DE TABLAS

Tabla 1 Direccionamiento Routers	18
Tabla 2 Direccionamiento Vlans	31
Tabla 3 Direccionamiento ip Switches	34

LISTA DE FIGURAS

Figura 1. Escenario 1	10
Figura 2. tabla enrutamiento R3	15
Figura 3. Tabla enrutamiento R5	16
Figura 4. Tabla de enrutamiento R1	16
Figura 5. Prueba conectividad R5	17
Figura 6. Prueba conectividad R1	17
Figura 7. Escenario 2	17
Figura 8. Configuración R1	21
Figura 9. Configuración R2	21
Figura 10. Configuración R3	23
Figura 11. Configuración R4	24
Figura 12. Escenario 3	25
Figura 13. Configuración SWT1	27
Figura 14. Configuración SWT2	27
Figura 15. Verificación interfaces SWT1	28
Figura 16. Verificación interfaces SWT2	28
Figura 17. Verificación interfaces trunk SWT1	29
Figura 18. Verificación Vlans	30
Figura 19. Verificación conexión extremo a extremo	35
Figura 20. Conexión switch SWT1	35
Figura 21. Conexión switch SWT2	35
Figura 22. Conexión switch SWT3	36
Figura 23. Ping SWT1	36
Figura 24. Ping SWT2	37
Figura 25. Ping SWT3	37

GLOSARIO

CCNP: (Cisco Certified Network Professional) es el nivel intermedio de certificación de la compañía .3 Para obtener esta certificación, se han de superar varios exámenes, clasificados según la empresa en 3 módulos. Esta certificación, es la intermedia de las certificaciones generales de Cisco, no está tan valorada como el CCIE, pero sí, mucho más que el CCNA.

Gns3: Es un simulador gráfico de red que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos. Para permitir completar simulaciones, GNS3 está estrechamente vinculada con: Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarios imágenes IOS de Cisco Systems

Networking: Es una red de computadoras, también llamada red de ordenadores, red de comunicaciones de datos o red informática conjunto de equipos informáticos y software reconectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Protocolos de red: Conjunto de normas standard que especifican el método para enviar y recibir datos entre varios ordenadores. Es una convención que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales

Vlan: Es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local

RESUMEN

Se realiza la presentación de este trabajo para agregarlo al repositorio de la UNAD donde quedara registro del desarrollo del diplomado cisco CCNP el cual nos permitió adquirir nuevo conocimiento en cuanto a la gran variedad de tecnologías que existen en el networking. Además de conocer diferentes plataformas con las cuales interactuamos de una manera más profesional en este ámbito de las telecomunicaciones

INTRODUCCIÓN

Se realiza el desarrollo del siguiente trabajo con el fin de colocar en práctica todos los conceptos vistos en el diplomado cisco CCNP el trabajo constara de tres laboratorios lo cuales contienen temáticas vistas en este curso

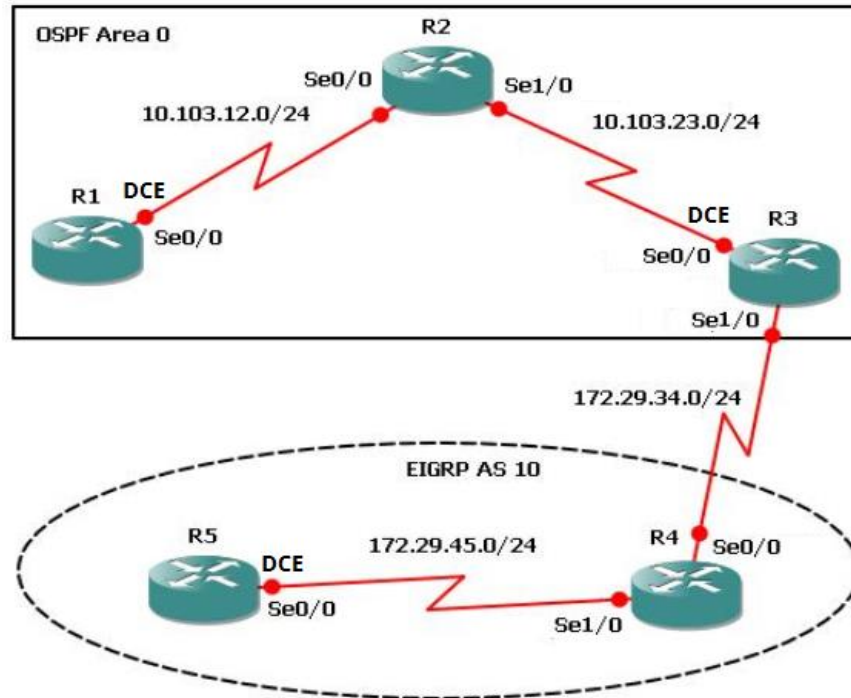
En el primer laboratorio se realizara la configuración de una topología de red donde estarán involucrados los protocolos de enrutamiento OSPF y EIGRP realizando la redistribución de las respectivas rutas para un correcto funcionamiento

El segundo laboratorio se realiza la configuración del protocolo BGP en una topología que consta de 4 routers en la cual se tendrá que tener conexión entre estos cuatro dispositivos

En el tercer escenario se realizara la configuración de 3 switch con el protocolo VTP el cual nos permite administrar VLANs tendrá que haber conexión entre Vlans

ESCENARIO 1

Figura 1. Escenario 1



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

```
R1(config)#no ip domain lookup
```

```
R1(config)#interface s 0/0
```

```
R1(config-if)#ip address 10.103.12.1 255.255.255.0
```

```
R1(config-if)#no shutdown
```

```
R1(config-if)#clock rate 64000
```

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

R1(config-router)#network 10.103.12.0 0.0.0.255 area 0

R2(config)#no ip domain lookup

R2(config)#interface s 0/0

R2(config-if)#ip address 10.103.12.2 255.255.255.0

R2(config-if)#no shutdown

R2(config-if)#exit

R2(config)#interfac s 1/0

R2(config-if)#ip address 10.103.23.1 255.255.255.0

R2(config-if)#no shutdown

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

R3(config)#no ip domain lookup

R3(config)#interface s 0/0

R3(config-if)#ip address 10.103.23.2 255.255.255.0

R3(config-if)#no shutdown

R3(config-if)#clock rate 64000

R3(config)#interface s 1/0

R3(config-if)#ip address 172.29.34.1 255.255.255.0

R3(config-if)#no shutdown

R3(config)#router ospf 1

R3(config-router)#network 10.103.23.0 0.0.0.255 area 0

R3(config-router)#network 172.29.34.0 0.0.0.255 area 0

R3(config)#router eigrp 10

R3(config-router)#network 172.29.34.0

R3(config-router)#no auto-summary

R4(config)#no ip domain lookup

R4(config)#interface s0/0

R4(config-if)#ip address 172.29.34.2 255.255.255.0

R4(config-if)#no shutdown

R4(config-if)#clock rate 64000

R4(config)#interface s 1/0

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 172.29.34.0

```
R4(config-router)#network 172.29.45.0
```

```
R4(config-router)#no auto-summary
```

```
R5(config-if)#ip address 172.29.45.2 255.255.255.0
```

```
R5(config-if)#no shutdown
```

```
R5(config-if)#clock rate 64000
```

```
R5(config)#router eigrp 10
```

```
R5(config-router)#network 172.29.45.0
```

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(config)#interface loopback 1
```

```
R1(config-if)#ip address 10.1.0.1 255.255.252.0
```

```
R1(config-if)#ip ospf network point-to-point
```

```
R1(config)#interface loopback 2
```

```
R1(config-if)#ip address 10.1.4.1 255.255.252.0
```

```
R1(config-if)#ip ospf network point-to-point
```

```
R1(config-if)#exit
```

```
R1(config)#interface loopback 3
```

```
R1(config-if)#ip address 10.1.8.1 255.255.252.0
```

```
R1(config-if)#ip ospf network point-to-point
```

```
R1(config-if)#exit
```

```
R1(config)#interface loopback 4
```

```
R1(config-if)#ip address 10.1.12.1 255.255.252.0
```

```
R1(config-if)#ip ospf network point-to-point
```

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

```
R1(config-router)#network 10.1.0.0 0.0.3.255 area 0
```

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(config)#interface loopback 5
```

```
R5(config-if)#ip address 172.5.0.1 255.255.252.0
```

```
R5(config)#interface loopback 6
```

```
R5(config-if)#ip address 172.5.4.1 255.255.252.0
```

```
R5(config)#interface loopback 7
```

```
R5(config-if)#ip address 172.5.8.1 255.255.252.0
```

```
R5(config)#interface loopback 8
```

```
R5(config-if)#ip address 172.5.12.1 255.255.252.0
```

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

Figura 2. Tabla enrutamiento R3

```
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, 00:00:11, Serial1/0
D       172.5.12.0 [90/2809856] via 172.29.34.2, 00:00:11, Serial1/0
D       172.5.0.0 [90/2809856] via 172.29.34.2, 00:00:11, Serial1/0
D       172.5.4.0 [90/2809856] via 172.29.34.2, 00:00:11, Serial1/0
172.29.0.0/24 is subnetted, 2 subnets
C       172.29.34.0 is directly connected, Serial1/0
D       172.29.45.0 [90/2681856] via 172.29.34.2, 00:16:45, Serial1/0
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O       10.1.0.0/22 [110/129] via 10.103.23.1, 00:16:36, Serial0/0
O       10.103.12.0/24 [110/128] via 10.103.23.1, 00:16:36, Serial0/0
C       10.103.23.0/24 is directly connected, Serial0/0
```

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

```
R3(config)#router ospf 1
```

```
R3(config-router)#redistribute eigrp 10 subnets
```

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

```
R3(config-router)#redistribute ospf 1 metric 1544 100 255 1 1500
```

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**.

Figura 3. Tabla enrutamiento R5

```
R5#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
      C      172.5.8.0 is directly connected, Loopback7
      C      172.5.12.0 is directly connected, Loopback8
      C      172.5.0.0 is directly connected, Loopback5
      C      172.5.4.0 is directly connected, Loopback6
    172.29.0.0/24 is subnetted, 2 subnets
      D      172.29.34.0 [90/2681856] via 172.29.45.1, 00:37:34, Serial0/0
      C      172.29.45.0 is directly connected, Serial0/0
    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
      D EX   10.1.0.0/22 [170/2707456] via 172.29.45.1, 00:10:16, Serial0/0
      D EX   10.103.12.0/24 [170/2707456] via 172.29.45.1, 00:10:16, Serial0/0
      D EX   10.103.23.0/24 [170/2707456] via 172.29.45.1, 00:10:16, Serial0/0
R5#
```

Figura 4. Tabla de enrutamiento R1

```
R1#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
      O E2   172.5.8.0 [110/20] via 10.103.12.2, 00:13:44, Serial0/0
      O E2   172.5.12.0 [110/20] via 10.103.12.2, 00:13:44, Serial0/0
      O E2   172.5.0.0 [110/20] via 10.103.12.2, 00:13:43, Serial0/0
      O E2   172.5.4.0 [110/20] via 10.103.12.2, 00:13:43, Serial0/0
    172.29.0.0/24 is subnetted, 2 subnets
      O      172.29.34.0 [110/192] via 10.103.12.2, 00:13:56, Serial0/0
      O E2   172.29.45.0 [110/20] via 10.103.12.2, 00:13:43, Serial0/0
    10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
      C      10.1.8.0/22 is directly connected, Loopback3
      C      10.1.12.0/22 is directly connected, Loopback4
      C      10.1.0.0/22 is directly connected, Loopback1
      C      10.1.4.0/22 is directly connected, Loopback2
      C      10.103.12.0/24 is directly connected, Serial0/0
      O      10.103.23.0/24 [110/128] via 10.103.12.2, 00:14:03, Serial0/0
R1#
```


Figura 5. Prueba conectividad R5

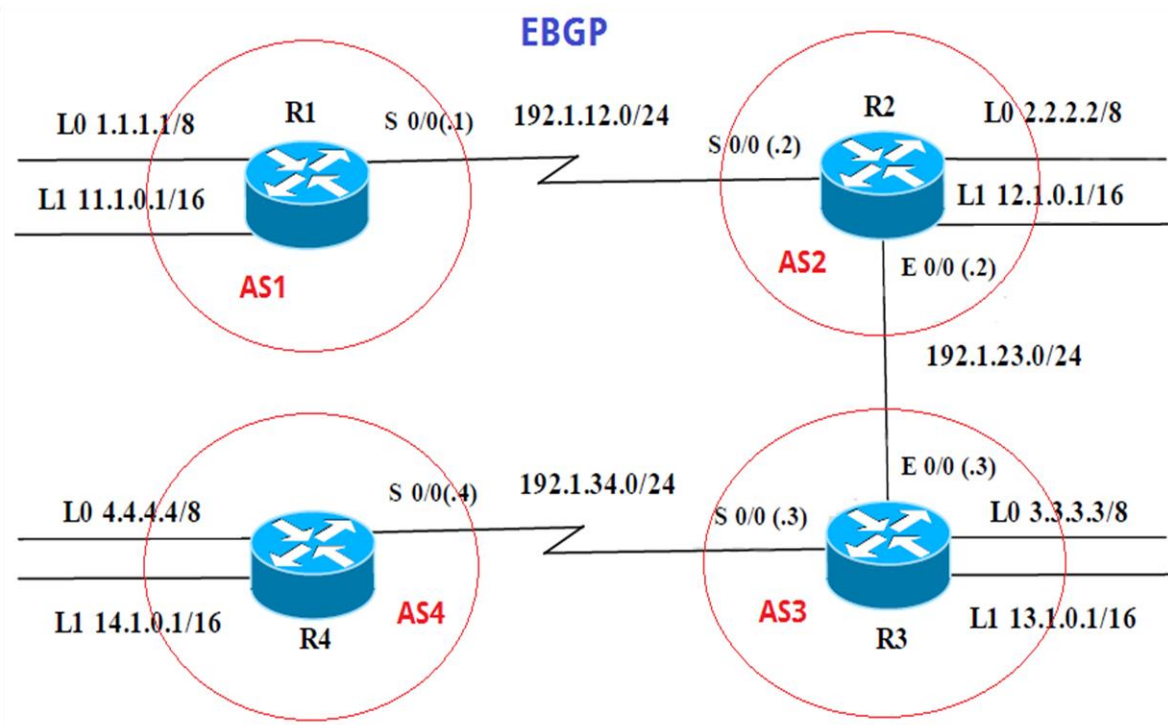
```
R5#ping 10.103.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.103.12.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 140/207/288 ms
R5#
```

Figura 6. Prueba conectividad R1

```
R1#ping 172.29.45.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.45.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 168/253/380 ms
R1#
```

ESCENARIO 2

Figura 7. Escenario 2



Información para configuración de los Routers

Tabla 1. Direccionamiento Routers

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

R1(config)#interface loopback 0

R1(config-if)#ip address 1.1.1.1 255.0.0.0

R1(config)#interface loopback 1

R1(config-if)#ip address 11.1.0.1 255.255.0.0

R1(config)#interface s 0/0

R1(config-if)#ip address 192.1.12.1 255.255.255.0

R1(config-if)#no shutdown

R2(config)#interface loopback 0

R2(config-if)#ip address 2.2.2.2 255.0.0.0

R2(config)#interface loopback 1

R2(config-if)#ip address 12.1.0.1 255.255.0.0

R2(config)#interface f 0/0

R2(config-if)#ip address 192.1.23.2 255.255.255.0

R2(config-if)#no shutdown

R3(config)#interface loopback 0

R3(config-if)#ip address 3.3.3.3 255.0.0.0

R3(config)#interface loopback 1

R3(config-if)#ip address 13.1.0.1 255.255.0.0

R3(config)#interface f0/0

R3(config-if)#ip address 192.1.23.3 255.255.255.0

R3(config-if)#no shutdown

R3(config)#interface s 0/0

```
R3(config-if)#ip address 192.1.34.3 255.255.255.0
```

```
R3(config-if)#no shutdown
```

```
R4(config)#interface loopback 0
```

```
R4(config-if)#ip address 4.4.4.4 255.0.0.0
```

```
R4(config)#interface loopback 1
```

```
R4(config-if)#ip address 14.1.0.1 255.255.0.0
```

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

```
R4(config-if)#ip address 192.1.34.4 255.255.255.0
```

```
R4(config-if)#no shutdown
```

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(config)#router bgp 1
```

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

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

```
R1(config-router)#network 1.1.1.1 mask 255.0.0.0
```

```
R1(config-router)#network 11.1.0.1 mask 255.255.0.0
```

Figura 8. Configuración R1

```
R1# 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    1.0.0.0/8 is directly connected, Loopback0
     11.0.0.0/16 is subnetted, 1 subnets
C      11.1.0.0 is directly connected, Loopback1
```

```
R2(config)#router bgp 2
```

```
R2(config-router)#bgp router-id 22.22.22.22
```

```
R2(config-router)#neighbor 192.1.12.1 remote-as 1
```

```
R2(config-router)#neighbor 192.1.34.3 remote-as 3
```

```
R2(config-router)#neighbor 192.1.23.3 remote-as 3
```

```
R2(config-router)#network 2.0.0.0 mask 255.0.0.0
```

```
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
```

Figura 9. Configuración R2

```
R2#sho 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    2.0.0.0/8 is directly connected, Loopback0
C   192.1.23.0/24 is directly connected, FastEthernet0/0
     12.0.0.0/16 is subnetted, 1 subnets
C      12.1.0.0 is directly connected, Loopback1
R2#
R2#
```

2. Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en **AS2** y R3 debería estar en **AS3**. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 33.33.33.33. Presente el paso a con los comandos utilizados y la salida del comando **show ip route**.

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

```
R3(config-router)#neighbor 192.1.12.2 remote-as 2
```

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

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

```
R3(config-router)#network 4.0.0.0 mask 255.0.0.0
```

```
R3(config-router)#network 14.1.0.0 mask 255.255.0.0
```

```
R3(config-router)#network 2.0.0.0 mask 255.0.0.0
```

```
R3(config-router)#network 12.1.0.0 mask 255.255.0.0
```

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

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

Figura 10. Configuración R3

```
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    2.0.0.0/8 [20/0] via 192.1.23.2, 00:00:33
C    3.0.0.0/8 is directly connected, Loopback0
C    192.1.23.0/24 is directly connected, FastEthernet0/0
C    192.1.34.0/24 is directly connected, Serial0/0
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.23.2, 00:00:33
     13.0.0.0/16 is subnetted, 1 subnets
C       13.1.0.0 is directly connected, Loopback1
R3#
```

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**.

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

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

```
R4(config-router)#neighbor 192.1.23.3 remote-as 3
```

```
R4(config-router)#neighbor 192.1.23.2 remote-as 2
```

```
R4(config-router)#neighbor 192.1.12.2 remote-as 2
```

```
R4(config-router)#neighbor 192.1.12.1 remote-as 1
```

```
R4(config-router)#network 3.0.0.0 mask 255.0.0.0
```

```
R4(config-router)#network 13.1.0.0 mask 255.255.0.0
```

```
R4(config-router)#network 12.1.0.0 mask 255.255.0.0
```

```
R4(config-router)#network 2.0.0.0 mask 255.0.0.0
```

```
R4(config-router)#network 11.1.0.0 mask 255.255.0.0
```

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

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

Figura 11. Configuración R4

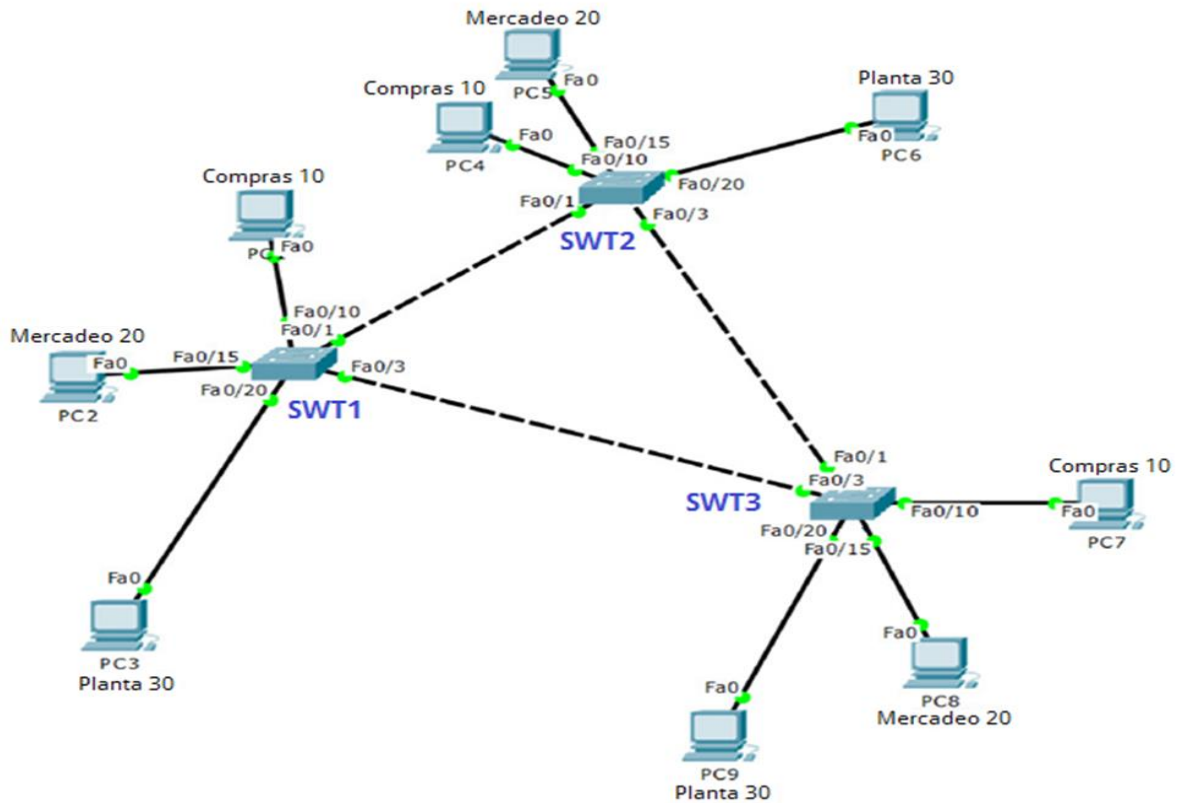
```
R4#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, 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    2.0.0.0/8 [20/0] via 192.1.34.3, 00:01:27
B    3.0.0.0/8 [20/0] via 192.1.34.3, 00:01:27
C    4.0.0.0/8 is directly connected, Loopback0
B    192.1.23.0/24 [20/0] via 192.1.34.3, 00:01:27
C    192.1.34.0/24 is directly connected, Serial0/0
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.34.3, 00:01:27
     13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0 [20/0] via 192.1.34.3, 00:01:27
     14.0.0.0/16 is subnetted, 1 subnets
C       14.1.0.0 is directly connected, Loopback1
R4#
```


ESCENARIO 3

Figura 12. Escenario 3



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

```
SWT1(config)#vtp domain CCNP
```

Changing VTP domain name from NULL to CCNP

```
SWT1(config)#vtp version 2
```

```
SWT1(config)#vtp mode client
```

Setting device to VTP CLIENT mode.

```
SWT1(config)#vtp pass
```

```
SWT1(config)#vtp password cisco
```

Setting device VLAN database password to cisco

```
SWT3(config)#vtp domain CCNP
```

Changing VTP domain name from NULL to CCNP

```
SWT3(config)#vtp version 2
```

```
SWT3(config)#vtp mode client
```

Setting device to VTP CLIENT mode.

```
SWT3(config)#vtp password cisco
```

Setting device VLAN database password to cisc

```
SWT2(config)#vtp domain
```

```
SWT2(config)#vtp domain CCNP
```

Changing VTP domain name from NULL to CCNP

```
SWT2(config)#vtp version 2
```

```
SWT2(config)#vtp mode server
```

Device mode already VTP SERVER.

SWT2(config)#vtp password cisco

Setting device VLAN database password to cisco

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

Figura 13. Configuración SWT1

```
SWT1(config)#
SWT1#show vtp status
VTP Version                : 2
Configuration Revision     : 1
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               : Enabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0xD3 0x6D 0xAB 0x8C 0xC3 0x75 0xBC 0xC3
Configuration last modified by 0.0.0.0 at 3-1-93 00:09:50
SWT1#
SWT1#
```

Figura 14. Configuración SWT2

```
SWT2#show vtp status
VTP Version                : 2
Configuration Revision     : 1
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               : Enabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0xB6 0xD8 0xF8 0xBB 0x5D 0xEC 0x23 0xF9
Configuration last modified by 0.0.0.0 at 3-1-93 00:09:41
Local updater ID is 0.0.0.0 (no valid interface found)
SWT3#show vtp status
VTP Version                : 2
Configuration Revision     : 1
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               : Enabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0xD3 0x57 0x37 0x9B 0x27 0x10 0x86 0x3B
Configuration last modified by 0.0.0.0 at 3-1-93 00:09:38
SWT3#
```

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**.

```
SWT1(config)#interface f 0/1
```

```
SWT1(config-if)#switchport mode dynamic desirable
```

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

Figura 15. Verificación interfaces SWT1

```
SWT1#show interface trunk
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     none

SWT1#
```

Figura 16. Verificación interfaces SWT2

```
SWT2#show interfaces trunk
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     none

SWT2#
```

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

```
SWT1(config)#INTERFACE F 0/3
```

```
SWT1(config-if)#SWItchport MODE TRUNK
```

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

Figura 17. Verificación interfaces trunk SWT1

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

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

Port      Vlans allowed and active in management domain
Fa0/1     1
Fa0/3     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1
Fa0/3     none
```

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

```
SWT2(config)#interface f 0/3
```

```
SWT2(config-if)#switchport mode trunk
```

```
SWT3(config)#interface f 0/1
```

```
SWT3(config-if)#switchport mode trunk
```

C. Agregar VLANs y asignar puertos.

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

```
SWT1(config)#vlan 10
```

VTP VLAN configuration not allowed when device is in CLIENT mode.

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

```
SWT2(config-vlan)#name Compras
```

```
SWT2(config-vlan)#vlan 20
```

```
SWT2(config-vlan)#name Mercadeo
```

```
SWT2(config-vlan)#vlan 30
```

```
SWT2(config-vlan)#name Planta
```

```
SWT2(config-vlan)#vlan 99
```

```
SWT2(config-vlan)#name Admon
```

2. Verifique que las VLANs han sido agregadas correctamente.

Figura 18. Verificación Vlan

```

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

```

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
30	enet	100030	1500	-	-	-	-	-	0	0
99	enet	100099	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

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

Tabla 2 .Direccionamiento Vlans

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

```
SWT1(config)#interface vlan 10
SWT1(config-if)#ip address 190.108.10.1 255.255.255.0
SWT1(config-if)#exit
SWT1(config)#interface vlan 20
SWT1(config-if)#ip address 190.108.20.1 255.255.255.0
SWT1(config-if)#exit
SWT1(config)#interface vlan 30
SWT1(config-if)#ip address 190.108.30.1 255.255.255.0
SWT1(config-if)#exit
```

```
SWT2(config)#interface vlan 10
SWT2(config-if)#ip address 190.108.10.2 255.255.255.0
SWT2(config-if)#exit
SWT2(config)#interface vlan 20
SWT2(config-if)#ip address 190.108.20.2 255.255.255.0
SWT2(config-if)#exit
SWT2(config)#interface vlan 30
SWT2(config-if)#ip address 190.108.30.2 255.255.255.0
SWT2(config-if)#exit
```

```
SWT3(config)#interface vlan 10
SWT3(config-if)#ip address 190.108.10.3 255.255.255.0
SWT3(config-if)#exit
SWT3(config)#interface vlan 20
SWT3(config-if)#ip address 190.108.20.3 255.255.255.0
SWT3(config-if)#exit
SWT3(config)#interface vlan 30
SWT3(config-if)#
SWT3(config-if)#ip address 190.108.30.3 255.255.255.0
SWT3(config-if)#exit
```

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

```
SWT1(config)#interface fastEthernet 0/10
SWT1(config-if)#switchport mode access
SWT1(config-if)#switchport access vlan 10
SWT1(config-if)#exit
```

```
SWT2(config)#interface fastEthernet 0/10
SWT2(config-if)#switchport mode access
SWT2(config-if)#switchport access vlan 10
```

```
SWT3(config)#interface fastEthernet 0/10
SWT3(config-if)#switchport mode access
SWT3(config-if)#switchport access vlan 10
SWT3(config-if)#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.


```
SWT1(config)#interface fastEthernet 0/15
SWT1(config-if)#switchport mode access
SWT1(config-if)#switchport access vlan 20
SWT1(config-if)#exit
SWT1(config)#interface fastEthernet 0/20
SWT1(config-if)#switchport mode access
SWT1(config-if)#switchport access vlan 30
SWT1(config-if)#exit
```

```
SWT2(config)#interface fastEthernet 0/15
SWT2(config-if)#switchport mode access
SWT2(config-if)#switchport access vlan 20
SWT2(config-if)#exit
SWT2(config)#interface fastEthernet 0/20
SWT2(config-if)#switchport mode access
SWT2(config-if)#switchport access vlan 30
```

```
SWT3(config)#interface fastEthernet 0/15
SWT3(config-if)#switchport mode access
SWT3(config-if)#switchport access vlan 20
SWT3(config-if)#exit
SWT3(config)#interface fastEthernet 0/20
SWT3(config-if)#switchport mode access
SWT3(config-if)#switchport access vlan 30
SWT3(config-if)#exit
```

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 3. Direccionamiento ip Switches

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

```
SWT1(config)#interface vlan 99
```

```
SWT1(config-if)#ip address 190.108.99.1 255.255.255.0
```

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

```
SWT2(config)#interface vlan 99
```

```
SWT2(config-if)#ip address 190.108.99.2 255.255.255.0
```

```
SWT2(config-if)#exit
```

```
SWT3(config)#interface vlan 99
```

```
SWT3(config-if)#ip address 190.108.99.3 255.255.255.0
```

```
SWT3(config-if)#
```

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.

El ping es correcto entre los equipos que están en la misma vlan

Si son De diferentes vlan el ping falla

Figura 19. Verificación conexión extremo a extremo

```
C:\>
C:\>ping 192.108.20.10

Pinging 192.108.20.10 with 32 bytes of data:

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

Ping statistics for 192.108.20.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

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

El ping es correcto porque esta configurada la vlan 99 vlan de administración

Figura 20. Conexión switch SWT1

```
SWT1#ping 190.108.99.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms

SWT1#ping 190.108.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms
```

Figura 21. Conexión switch SWT2

```
SWT2#ping 190.108.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms

SWT2#ping 190.108.99.3

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

-----
```

Figura 22. Conexión switch SWT3

```
SWT3#ping 190.108.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

SWT3#ping 190.108.99.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms

SWT3#
```

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

El ping es exitoso por que los swicht reconocen cada una de las vlans configuradas

Figura 23.Ping SWT1

```
SWT1#ping 190.108.20.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.11, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

SWT1#ping 190.108.30.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.11, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Figura 24 .Ping SWT2

```
SWT2#ping 190.108.20.22

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.22, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/9 ms

SWT2#ping 190.108.30.22

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.22, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Figura 25.Ping SWT3

```
SWT3#ping 190.108.20.33

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.33, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

SWT3#ping 190.108.30.33

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.33, timeout is 2
seconds:
!!!!
```

CONCLUSIONES

- ✓ Se conoció la funcionalidad de la redistribución como se pueden interconectar dos redes con diferentes protocolos de enrutamiento

- ✓ Se entiende la importancia de cada comando y cada proceso que se realiza al momento de configurar una red una debida documentación de cada paso que realicemos nos permitirá un mejor entendimiento de la red ya sea para saber su funcionamiento o para identificar errores futuros

- ✓ Se analiza la funcionalidad del protocolo vtp y como nos permite la administración de las vlans las cuales son de mucha utilidad para la gestión de una red

- ✓ Los conceptos aprendidos en el desarrollo del diplomado nos permiten realizar un análisis más profundo de las topologías de red que se nos presenten en nuestra vida laboral una mejor identificación de problemáticas ,visión mas amplia en el campo del networking

BIBLIOGRAFÍA

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-NT1IlnWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Campus Network Design Fundamentals. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Campus Network Architecture. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ>

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

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

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