

EVALUACIÓN FINAL  
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

YUL ALEXANDER HERNÁNDEZ AGUILAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
INGENIERIA DE TELECOMUNICACIONES  
DIPLOMADO CISCO CCNP  
SAN JOSE DEL GUAVIARE  
2019

# EVALUACIÓN PRUEBA DE HABILIDADES PRÁCTICAS CCNP

YUL ALEXANDER HERNÁNDEZ

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  
SAN JOSE DEL GUAVIARE  
2019

NOTA DE ACEPTACION

---

---

---

---

---

---

---

---

---

---

---

Presidente del Jurado

---

Jurado

---

Jurado

San José del Guaviare 05 de Junio de 2019

## CONTENIDO

INTRODUCCIÓN .....	9
ESCENARIO 1 .....	10
ESCENARIO 2 .....	19
ESCENARIO 3 .....	26
CONCLUSIONES.....	43
BIBLIOGRAFÍA .....	44

## LISTA DE FIGURAS

Figura 1 Escenario 1 .....	10
Figura 2 Escenario 1 Packet Tracer .....	10
Figura 3. Verificación de las nuevas interfaces en R1 .....	14
Figura 4. Verificación de las nuevas interfaces en R5 .....	15
Figura 5. Verificación de las interfaces loopback .....	16
Figura 6. R3 ha aprendido las nuevas 8 interfaces .....	16
Figura 7. Protocolo OSPF en R1 .....	17
Figura 8. Protocolo EIGRP en R5.....	17
Figura 9. Ruta de sistema autónomo R1 .....	18
Figura 10. Ruta de sistema autónomo R1 .....	18
Figura 11.Escenario 2.....	19
Figura 12.Escenario 2 Packet Tracer.....	19
Figura 13. Relación de vecino BGP entre R1 y R2 y R2 y R1 .....	23
Figura 14. Relación de vecino BGP entre R2 y R3 y R3 y R2 .....	24
Figura 15. Red loopback de R4 en BGP .....	25
Figura 16. Escenario 3.....	26
Figura 17. VTP Estatus escenario 3 SWT1 .....	27
Figura 18. VTP Estatus escenario 3 SWT2 .....	27
Figura 19. VTP Estatus escenario 3 SWT3 .....	28
Figura 20. VTP Enlace Trunk SWT1 .....	29
Figura 21. VTP Enlace Trunk SWT2 .....	29

Figura 22. Enlace TRUNK SWT1. ....	30
Figura 23. Verificación de VLANS creadas .....	32
Figura 24. Verificación en SWT1 .....	32
Figura 25. Utilización de comando show en PC1 .....	35
Figura 26. Utilización de comando show en PC2 .....	35
Figura 27. Utilización de comando show en PC3 .....	36
Figura 28. Utilización de comando show en PC4 .....	36
Figura 29. Utilización de comando show en PC5 .....	37
Figura 30. Utilización de comando show en PC6 .....	37
Figura 31. Utilización de comando show en PC7 .....	38
Figura 32. Utilización de comando show en PC8 .....	38
Figura 33. Utilización de comando show en PC9 .....	39
Figura 34. Ping ente PC1 y PC4, PC1 y PC7, Ping entre PC1 a PC2, PC5, PC8 .	41
Figura 35. Ping entre PC1 a PC3, PC6, PC9 .....	41
Figura 36 Ping entre PC2 y PC5, PC1 y PC8, Ping entre PC2 a PC1, PC4, PC7 .	41
Figura 37. Ping entre PC2 a PC3, PC6, PC9 .....	42
Figura 38. Ping entre PC3 y PC6, PC1 y PC9, Ping entre PC3 a PC1, PC4, PC7	42
Figura 39. Ping entre PC3 a PC2, PC5, PC8 .....	42

## LISTA DE TABLAS

Tabla 1. Información para configuración de los Routers .....	20
Tabla 2. Interfaces VLAN Escenario 3 .....	32
Tabla 3. Creación de los puertos .....	33
Tabla 4. Tabla de direccionamiento .....	39
Tabla 5. Ejecución de un ping desde cada PC.....	40

## RESUMEN

Durante el desarrollo del curso de profundización Diplomado CISCO CCNP, trabajamos sobre dos módulos CCNP ROUTE R&S V7 y CCNP SWITCH R&S V7, en el cual aprendimos a crear una red eficaz y escalable; así como a instalar, configurar, supervisar, y solucionar problemas en los equipos de una red convergente.

La herramienta que utilizamos para el desarrollo de los laboratorios y escenarios fue Packet Tracer en la cual trabajamos en los diferentes tipos de configuración de IPv6 y configuración de protocolos de enrutamiento como: RIPng, OSPFv3, EIGRP for IPv6 y MP-BGP

## INTRODUCCIÓN

Una vez adquiridos los conocimientos y habilidades en los diferentes protocolos, aplicaciones y características de los elementos Cisco (Router y Switch) se proponen tres escenarios en los cuales se aplicarán dichos conocimientos y habilidades permitiendo evaluar en qué nivel se encuentran estos e identificar los aspectos a mejorar para en un futuro afrontar los desafíos que se presentan en la vida laboral de un ingeniero de telecomunicaciones.

Este trabajo se realizó con el fin de llevar a cabo la Prueba de Habilidades Prácticas implementada como parte de las actividades evaluativas del Diplomado de Profundización CCNP, la cual busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado y poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking

En esta actividad se utilizan comandos de configuración avanzada en routers bajo diferentes tipos de configuración avanzada en routers bajo diferentes tipos de configuración de IPv6 y la configuración de protocolos de enrutamiento.

Se abordan temáticas como el enrutamiento dinámico a través de los protocolos OSPF y EIGRP, así como la configuración de áreas y sistemas autónomos respectivamente, el enrutamiento a través del protocolo BGP y el proceso de creación de adyacenticas en función del protocolo IPv4, del Router ID e interfaces Loopback.

Se evidencia la configuración de una pequeña red basada en Switches capa 2 y PCs, en la cual se configura el enrutamiento IPv4 respectivo, se implementa protocolos como VLAN Trunking Protocol y Dynamic Trunking Protocol, así como una parte inicial del enrutamiento InterVLAN.

# Descripción de escenarios para la prueba de habilidades

## ESCENARIO 1

Figura 1. Escenario 1

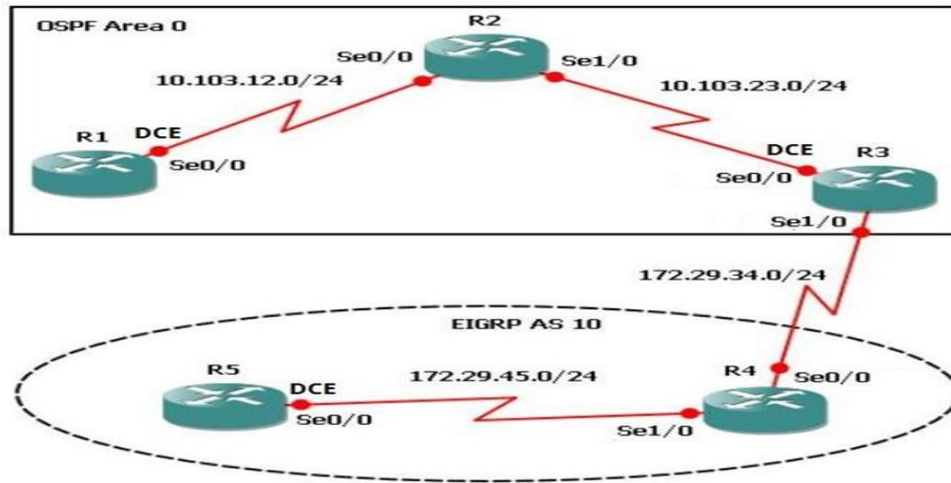
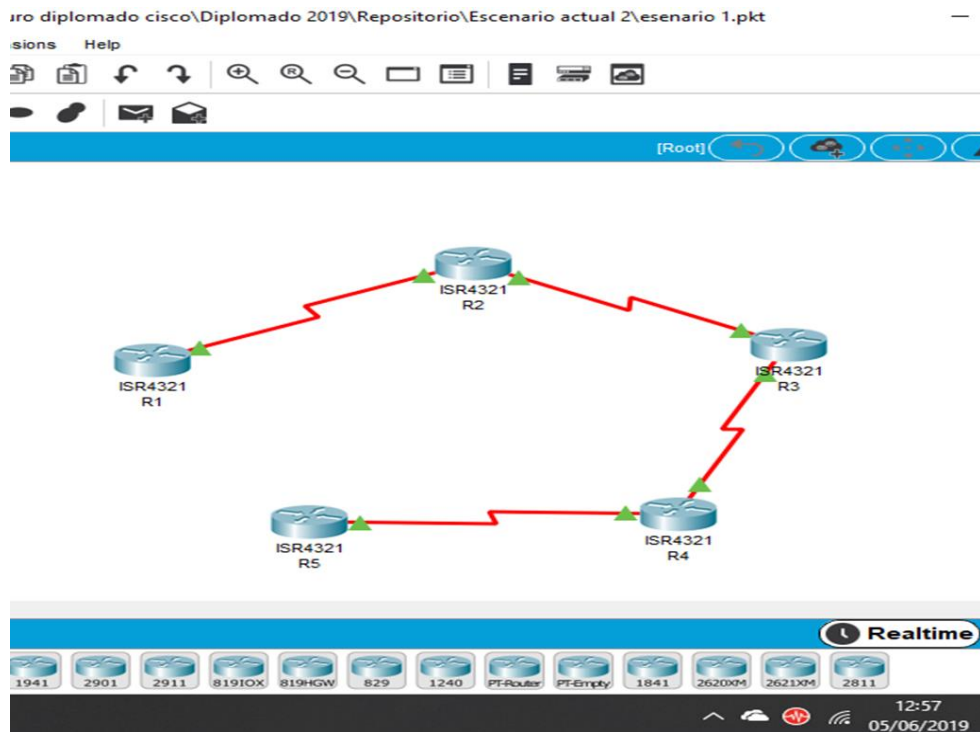


Figura 2 Escenario 1 Packet Tracer



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

Configuración inicial, asignamos nombre a cada uno de los routers, direcciones de las interfaces y protocolos de comunicación correspondientes con el siguiente código.

### Configuración R1

```
Router>
Router>enable      Ingreso a modo privilegiado
Router#configure terminal Ingreso a modo de configuración
Router(config)#hostname R1      Se asigna nombre lrouter
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
```

### 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
```

### 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
```

Con el objetivo de permitir 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>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.

Procedo a crear 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
```

Con el objetivo de verificar que las nuevas interfaces loopback hayan quedado configuradas para participar en el protocolo OSPF utilizo el comando show ip ospf brief, mostrando el siguiente resultado:

Figura 3. Verificación de las nuevas interfaces en R1

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	

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

```

Con el objetivo de verificar que hayan sido creadas las interfaces loopback, utilizo el comando show ip interfaces brief | include up arrojando el siguiente dato:

Figura 4. Verificación de las nuevas interfaces en R5

Interface	IP Address	Status	Other
Serial0/0	172.29.45.2	up	YES NVRAM
Vlan1	unassigned	down	YES NVRAM
Loopback4	172.5.4.1	up	YES manual
Loopback8	172.5.8.1	up	YES manual
Loopback12	172.5.12.1	up	YES manual
Loopback16	172.5.16.1	up	YES manual

```

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

```

Para verificar que las interfaces loopback hayan quedado integradas al protocolo EIGRP utilizo el comando show ip eigrp interfaces.

Figura 5. Verificación de las interfaces loopback

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

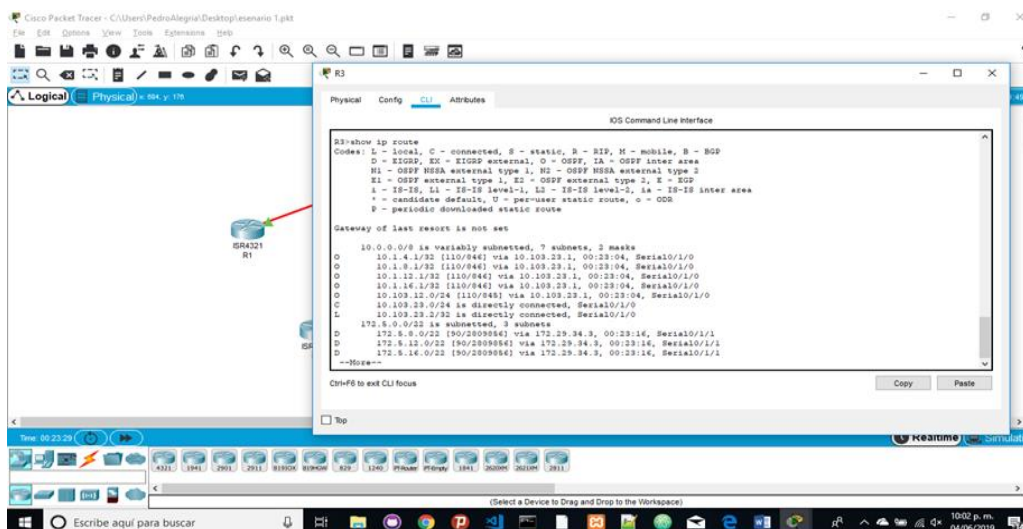
Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
Se0/0	1	0/0	18	0/15	83	0
Lo4	0	0/0	0	0/1	0	0
Lo8	0	0/0	0	0/1	0	0
Lo12	0	0/0	0	0/1	0	0
Lo16	0	0/0	0	0/1	0	0

Como se puede evidenciar, las 4 nuevas interfaces de loopback ya participan 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.

Para este punto ejecuto el comando show ip route el cual arroja los siguientes datos:

Figura 6. R3 ha aprendido las nuevas 8 interfaces



De la información anterior, se puede evidenciar que el router R3 ha aprendido las 8 nuevas interfaces de loopback de ambos protocolos.

Figura 7. Protocolo OSPF en R1

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

Figura 8. Protocolo EIGRP en R5

```
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
```

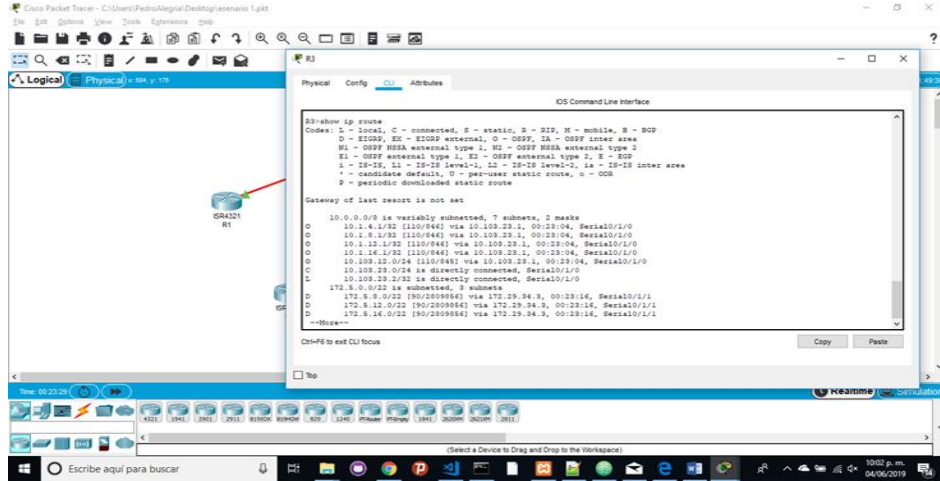
5. R3 para redistribuir las rutas EIGRP en OSPF usando el costo de 50000 y luego redistribuya las rutas OSPF en EIGRP usando un ancho de banda T1 y 20,000 microsegundos de retardo.

Para lograr redistribuir las rutas EIGRP en OSPF y viceversa utilizo 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
```

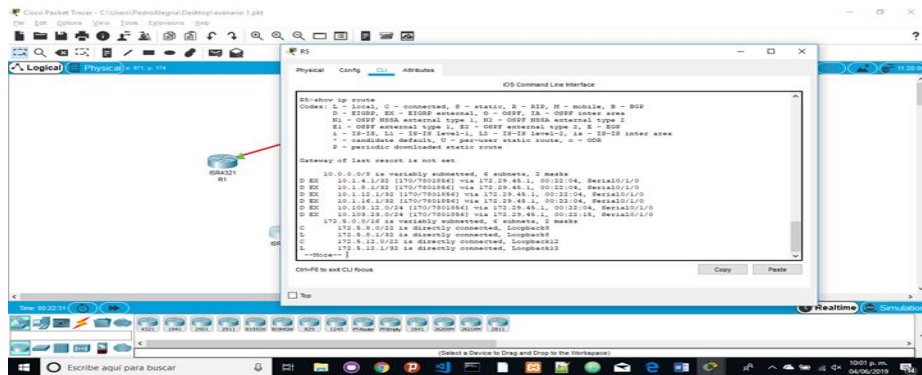
6. Verifique en R1 y R5 que las rutas del sistema autónomo opuesto existen en su tabla de enrutamiento mediante el comando show ip route.

Figura 9. Ruta de sistema autónomo R1



Se puede observar en R1 ya aparecen las loopbacks creadas en R5.

Figura 10. Ruta de sistema autónomo R1



Como se puede observar en R5 ya aparecen las loopbacks creadas en R1.

## ESCENARIO 2

Figura 11. Escenario 2

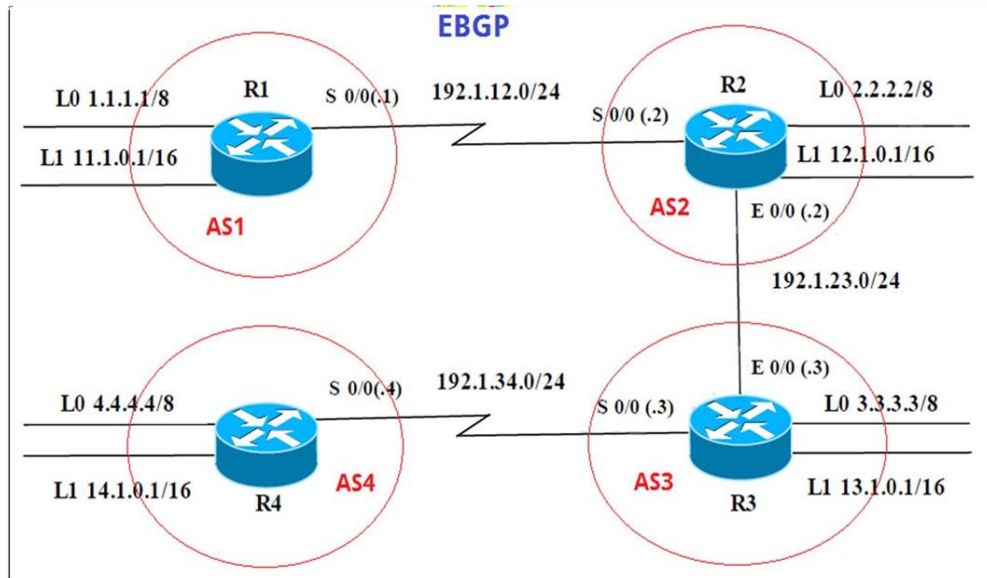


Figura 12. Escenario 2 Packet Tracer

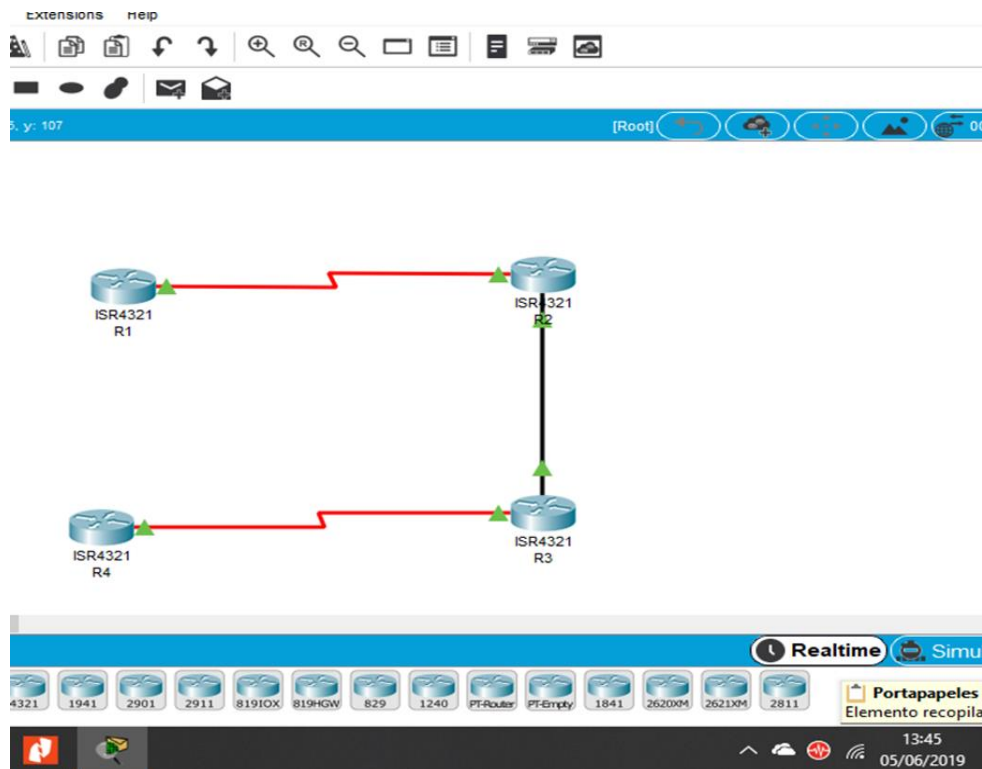


Tabla 1. Información para configuración de los Routers

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

```

R1
Router>EN
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int s0/0/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit
R1(config)#int Lo0
R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state
to up

```

```
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#exit
R1(config)#int Lo1
R1(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state
to up
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#exit
R1(config)#
```

### Configuración R2

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int Lo0
R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state
to up
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#exit
R2(config)#int Lo1
R2(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state
to up
```

### Configuración R3:

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#conf t
```

```

Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int Lo0
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state
to up
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#exit
R3(config)#int Lo1
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state
to up
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#exit
R3(config)#int f0/0/0
%Invalid interface type and number
R3(config)#int f0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#exit
R3(config)#int s0/0/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R3(config-if)#exit
R3(config)#

```

#### Configuración R4

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R4
R4(config)#END
R4#
%SYS-5-CONFIG_I: Configured from console by console
R4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#int Lo0
R4(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state
to up
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#exit

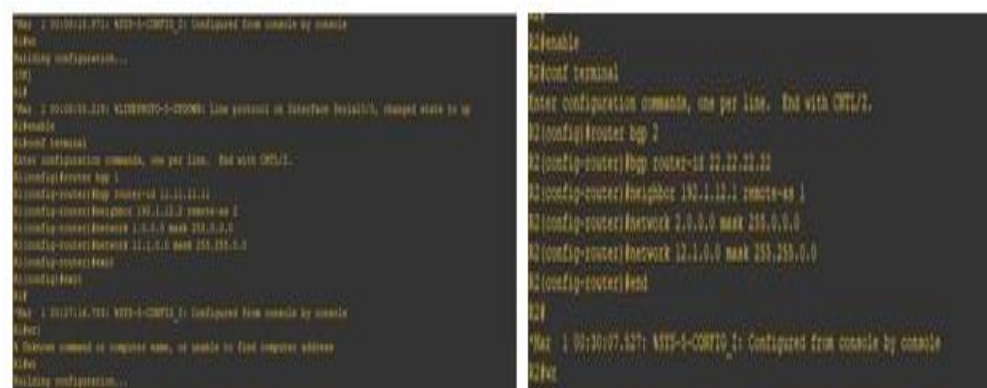
```

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

```
R1
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
```

Figura 13. Relación de vecino BGP entre R1 y R2 y R2 y R1



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

```

R2
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router bgp 200
R2(config-router)#network 192.1.12.2 mask 255.255.255.0
R2(config-router)#neighbor 192.1.12.3 remote-as 300
R2(config-router)#

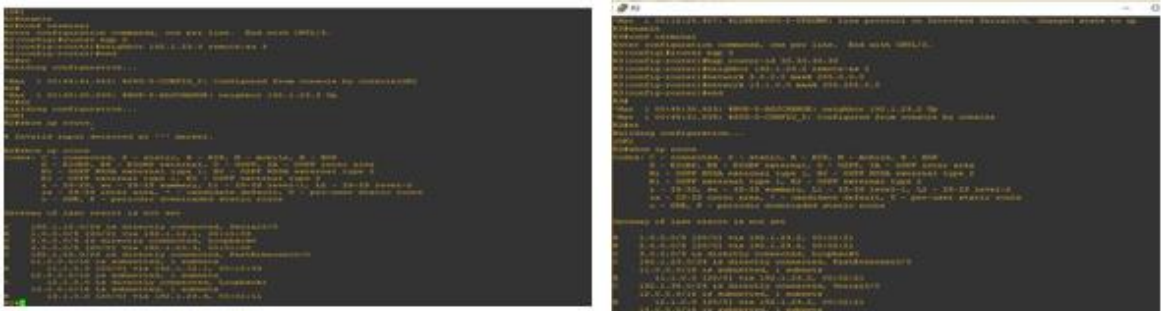
```

```

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

```

Figura 14. Relación de vecino BGP entre R2 y R3 y R3 y R2



- Configure una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en AS3 y R4 debería estar en AS4. Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como 44.44.44.44. Establezca las relaciones de vecino con base en las direcciones de Loopback 0. Cree rutas estáticas para alcanzar la Loopback 0 del otro router. No anuncie la Loopback 0 en BGP. Anuncie la red Loopback de R4 en BGP. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

```

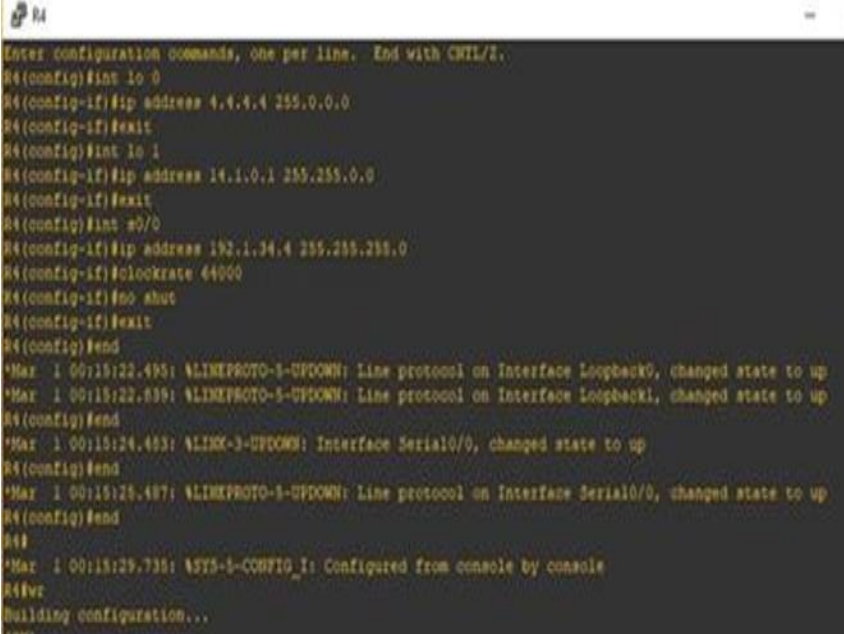
R3
enable
conf terminal router bgp 3
neighbor 192.1.34.4 remote-as 4

```

```
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
```

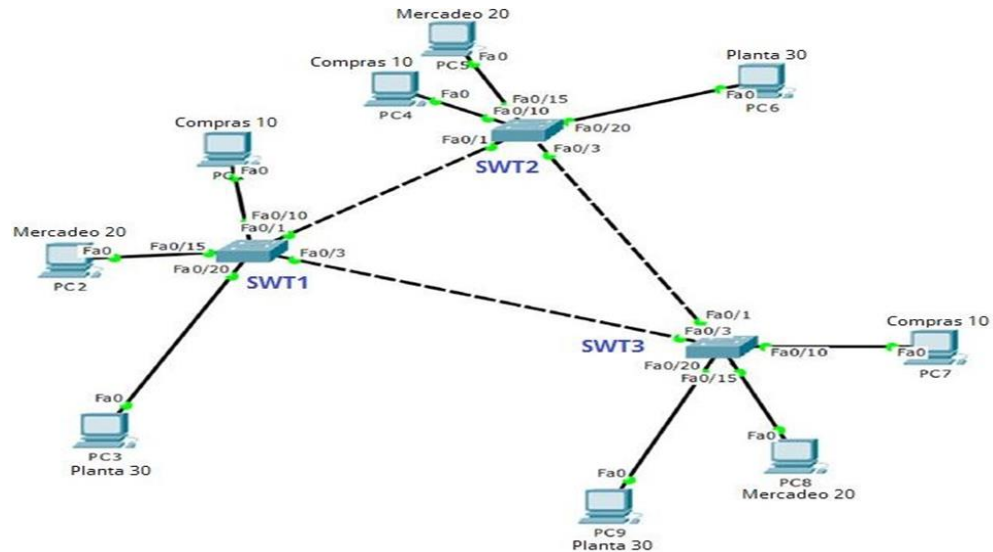
Figura 15. Red loopback de R4 en BGP



```
Enter configuration commands, one per line. End with CTRL/Z.
R4(config)#int lo 0
R4(config-if)#ip address 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 4000
R4(config-if)#no shut
R4(config-if)#exit
R4(config)#end
*Mar 1 00:13:22.495: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
*Mar 1 00:13:22.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
R4(config)#end
*Mar 1 00:13:24.483: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
R4(config)#end
*Mar 1 00:13:25.487: %LINKPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
R4(config)#end
R4#
*Mar 1 00:13:29.735: %SYS-5-CONFIG_I: Configured from console by console
R4#
Building configuration...
```

## ESCENARIO 3

Figura 16. 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.

Para ejecutar lo anterior aplico el siguiente código en 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
```

```
Switch
SWT2 IOU1#configure terminal
```

```

IOU1(config)#hostname SWT2
SWT1(config)#vtp domain CCNP
SWT1(config)#vtp mode server
SWT1(config)#vtp password cisco
SWT1(config)#exit
SWT1#wr
Switch SWT3
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.

Figura 17. VTP Estatus escenario 3 SWT1

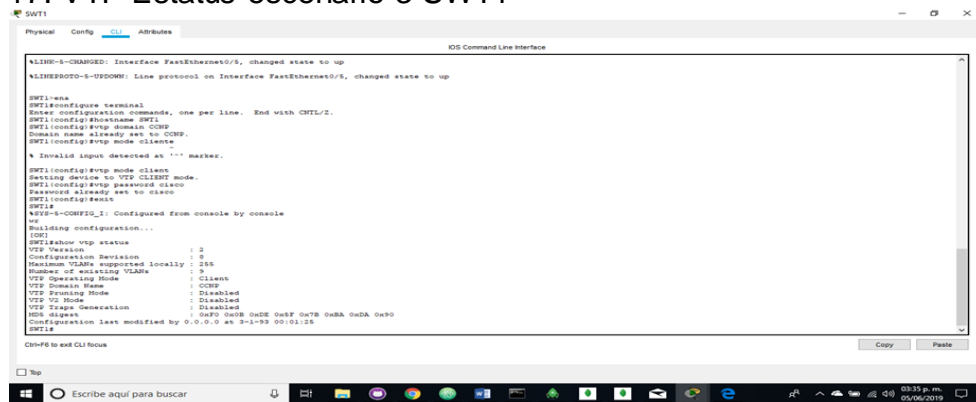


Figura 18. VTP Estatus escenario 3 SWT2

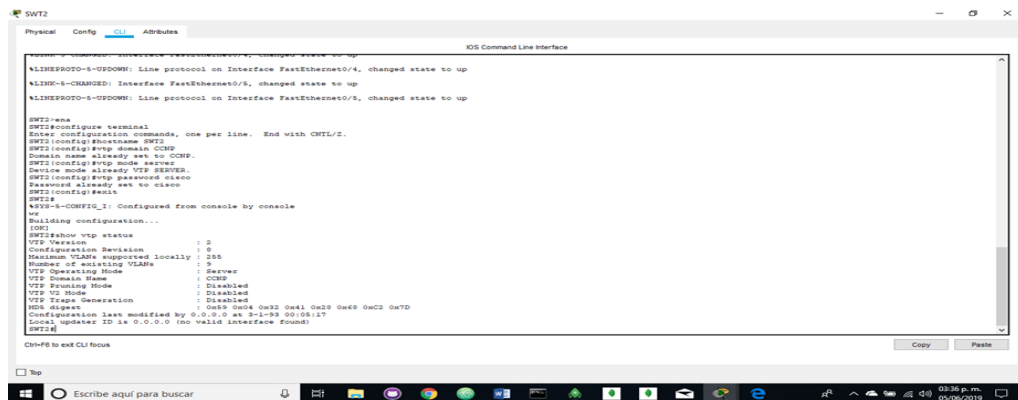
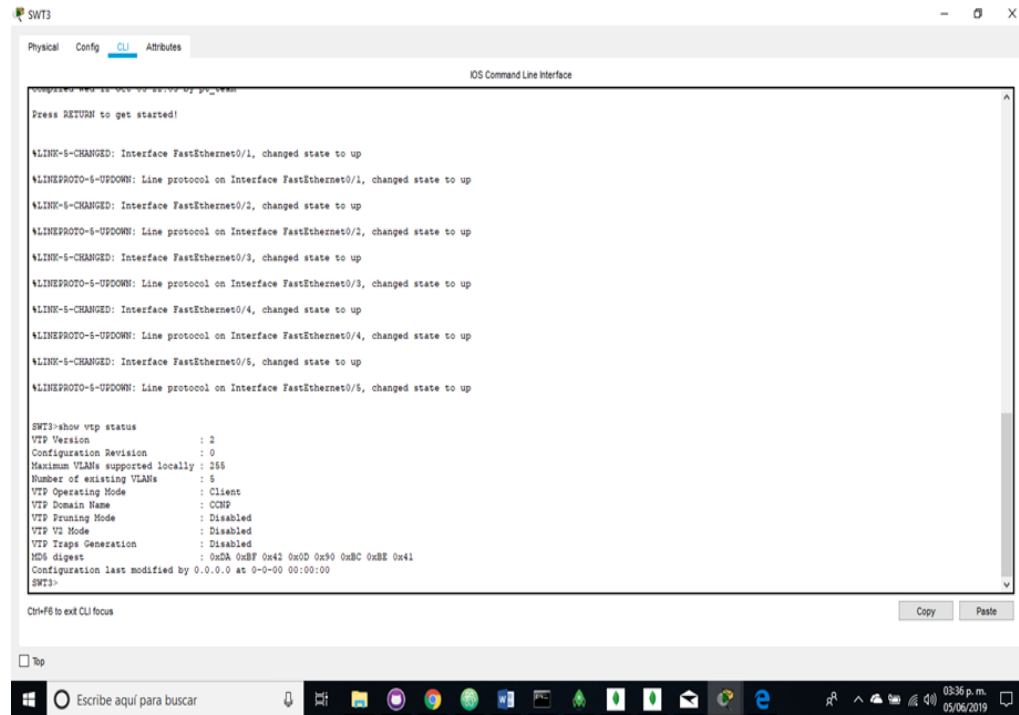


Figura 19. VTP Estatus escenario 3 SWT3



## 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.

Para configurar Dynamic desirable se utilizó el comando switchport mode Dynamic desirable en ambos switches.

Para Switch SWT1

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

```

SWT1#wr
Para Switch SWT2
SWT2#configure terminal
SWT2(config)#interface range ethernet0/0
SWT2(config-if-range)#switchport trunk encapsulation dot1q
SWT2(config-if-range)#switchport mode trunk
SWT2(config-if-range)#switchport mode dynamic desirable
SWT2(config-if-range)#no shutdown
SWT2(config-if-range)#exit
SWT2(config)#interface range ethernet0/2
SWT2(config-if-range)#switchport trunk encapsulation dot1q
SWT2(config-if-range)#switchport mode trunk
SWT2(config-if-range)#switchport mode dynamic desirable
SWT2(config-if-range)#no shutdown
SWT2(config-if-range)#exit
SWT2(config)#end
SWT2#wr

```

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

Figura 20. VTP Enlace Trunk 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. VTP Enlace 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

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

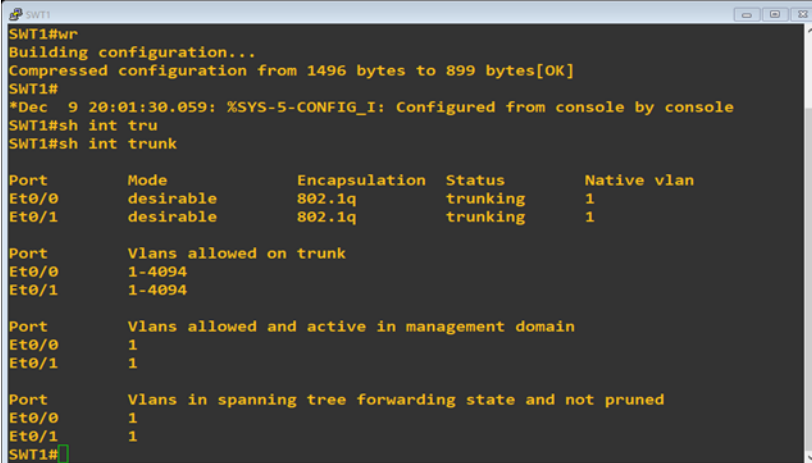
En el punto anterior ya configuré la interfaz del SWT1, teniendo presente que es la interfaz ethernet 0/1

Para Switch SWT3

```
SWT3#configure terminal
SWT3(config)#interface range ethernet0/1
SWT3(config-if-range)#switchport trunk encapsulation dot1q
SWT3(config-if-range)#switchport mode trunk
SWT3(config-if-range)#no shutdown
SWT3(config-if-range)#exit
SWT3(config)#end
SWT3#wr
```

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

Figura 22. Enlace TRUNK SWT1.



```
SWT1#wr
Building configuration...
Compressed configuration from 1496 bytes to 899 bytes[OK]
SWT1#
*Dec  9 20:01:30.059: %SYS-5-CONFIG_I: Configured from console by console
SWT1#sh int tru
SWT1#sh int trunk

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

Port      Vlans allowed on trunk
Et0/0     1-4094
Et0/1     1-4094

Port      Vlans allowed and active in management domain
Et0/0     1
Et0/1     1

Port      Vlans in spanning tree forwarding state and not pruned
Et0/0     1
Et0/1     1
SWT1#
```

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

En el punto anterior ya configuré la interfaz del SWT2, teniendo presente que es la interfaz ethernet 0/2

```

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

```

C. Agregar VLANs y asignar puertos.

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

Procedo a crear 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.

```

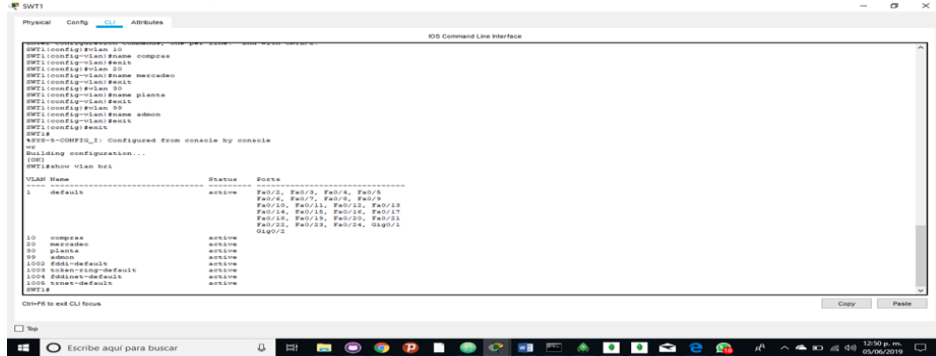
SWT2#configure terminal
SWT2(config)#vlan 10      Creo la vlan 10
SWT2(config-vlan)#name Compras      Asigno el nombre Compras
SWT2(config-vlan)#exit
SWT2(config)#vlan 20      Creo la vlan 20
SWT2(config-vlan)#name Mercadeo      Asigno el nombre Mercadeo
SWT2(config-vlan)#exit
SWT2(config)#vlan 30      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.

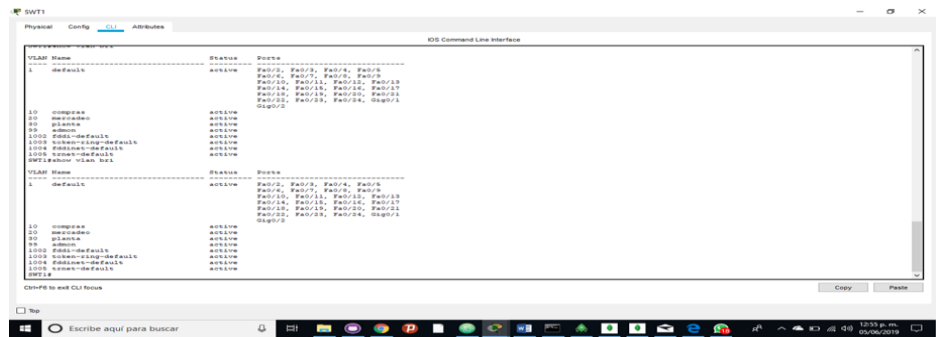
Para verificar las VLANS creadas utilizo el comando show vlan brief

Figura 23. Verificación de VLANs creadas



Para garantizar que las VLANs aparecen en el switch SW1 aplico el mismo comando en este.

Figura 24. Verificación en SW1



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

Tabla 2. Interfaces VLAN Escenario 3

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  
 Debido que los puertos usados en los switches son diferentes a los que estoy usando, creo la tabla de acuerdo a la topología implementada.

Tabla 3. Creación de los puertos

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.

Configuración para el switch 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

Configuración para el switch 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

Configuración para el switch 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  Asigno 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  Asigno la VLAN30 al puerto
SWT1(config-vlan)#exit
SWT1(config)#end
SWT1#wr    Se guarda la configuración
```

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

```
SWT2#configure terminal
SWT2(config)#interface ethernet 1/1    Ingreso al puerto
SWT2(config-vlan)#switchport mode access  Configuro el modo de acceso
SWT2(config-vlan)#switchport access vlan 20  Asigno 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  Asigno la VLAN30 al puerto
SWT2(config-vlan)#exit
SWT2(config)#end
SWT2#wr    Se guarda la configuración
```

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

```
SWT3#configure terminal
SWT3(config)#interface ethernet 1/1    Ingreso al puerto
SWT3(config-vlan)#switchport mode access  Configuro el modo de acceso
SWT3(config-vlan)#switchport access vlan 20  Asigno 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  Asigno la VLAN30 al puerto
SWT3(config-vlan)#exit
SWT3(config)#end
SWT3#wr    Se guarda la 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.

Figura 25. Utilización de comando show en PC1

```
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
```

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.

Figura 26. Utilización de comando show en PC2

```
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
```

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.

Figura 27. Utilización de comando show en PC3

```
PC-3> sh

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

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.

Figura 28. Utilización de comando show en PC4

```
PC-4> sh

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

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.

Figura 29. Utilización de comando show en PC5

```
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
```

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.

Figura 30. Utilización de comando show en PC6

```
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
```

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.

Figura 31. Utilización de comando show en PC7

```
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
```

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.

Figura 32. Utilización de comando show en PC8

```
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
```

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.

Figura 33. Utilización de comando show en PC9

```
PC-9> sh
NAME IP/MASK GATEWAY MAC LPORT RHOST:PORT
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
```

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. Tabla de direccionamiento

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

Para configurar VLAN99 para el switch SWT1 procedo de la siguiente forma:

```
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 Se guarda la 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 Se guarda la configuración

```

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.

Tabla 5. Ejecución de un ping desde cada PC

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

Equipos en VLAN 10  
Equipos en VLAN 20  
Equipos en VLAN 30

PC1

Figura 34. Ping entre PC1 y PC4, PC1 y PC7, Ping entre PC1 a PC2, PC5, PC8

```
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

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 35. Ping entre PC1 a PC3, PC6, PC9

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

PC-1> ping 190.108.30.6
No gateway found

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

Observaciones:

No es posible realizar ping con las PC's que pertenecen a otra VLAN diferente a la VLAN 10

PC2

Figura 36 Ping entre PC2 y PC5, PC1 y PC8, Ping entre PC2 a PC1, PC4, PC7

```
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

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 37. Ping entre PC2 a PC3, PC6, PC9

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

PC-2> ping 190.108.30.6
No gateway found

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

Observaciones:

No es posible realizar ping con las PC's que pertenecen a otra VLAN diferente a la VLAN 20,

PC3\*-

Figura 38. Ping entre PC3 y PC6, PC1 y PC9, Ping entre PC3 a PC1, PC4, PC7

```
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

PC-3> ping 190.108.10.1
No gateway found

PC-3> ping 190.108.10.4
No gateway found

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

Figura 39. Ping entre PC3 a PC2, PC5, PC8

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

PC-3> ping 190.108.20.5
No gateway found

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

Observaciones:

No es posible realizar ping con las PC's que pertenecen a otra VLAN diferente a la VLAN 30

## CONCLUSIONES

Con el desarrollo de esta actividad, se trabajó en tres escenarios, tuvimos la oportunidad de establecer y ver la funcionalidad de los comandos que se utilizaron en el paso a paso para la configuración de los equipos, mediante el registro de procesos de verificación de conectividad mediante el uso de los siguientes comandos, ping, traceroute, show ip route, entre otros.

Se llevó a cabo el desarrollo de la Prueba de Habilidades Prácticas implementada como parte de las actividades evaluativas del Diplomado de Profundización CISCO CCNP, mediante la cual identificamos el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del curso, poniendo a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking

## BIBLIOGRAFÍA

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. (Teare, 2015) Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>

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

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-NT1IlnMfy2rhPZHwEoWx>

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 (Froom, 2015)

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-NT1IlnWR0hoMxgBNv1CJ>