EVALUACIÓN FINAL

PRUEBA DE HABILIDADES PRÁCTICAS CCNP

EDGAR STIVEN MURCIA ROCHA

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

EVALUACIÓN PRUEBA DE HABILIDADES PRÁCTICAS
CCNP

EDGAR STIVEN MURCIA ROCHA

Diplomado de profundización cisco CCNP prueba de
Habilidades prácticas

Gerardo Granados Acuña
Magíster en Telemática

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

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

_____

_____

_____
Presidente del jurado

_____
Jurado

_____
Jurado

BOGOTA 17 de julio de 2019

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

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.

OSPF: Open Shortest Path First (OSPF), es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol para calcular la ruta más corta entre dos nodos. Su medida de métrica se denomina cost, y tiene en cuenta diversos parámetros tales como el ancho de banda y la congestión de los enlaces. OSPF mantiene actualizada la capacidad de encaminamiento entre los nodos de una red mediante la difusión de la topología de la red y la información de estado-enlace de sus distintos nodos.

EIGRP: Es un protocolo de encaminamiento de vector distancia, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de vector de distancia. Se considera un protocolo avanzado que se basa en las características normalmente asociadas con los protocolos del estado de enlace. Algunas de las mejores funciones de OSPF, como las actualizaciones parciales y la detección de vecinos, se usan de forma similar con EIGRP. Aunque no garantiza el uso de la mejor ruta, es bastante usado porque EIGRP es algo más fácil de configurar que OSPF. EIGRP mejora las propiedades de convergencia y opera con mayor eficiencia que IGRP.

BGP:(Border Gateway Protocol) es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Por ejemplo, los proveedores de servicio registrados en Internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.

VTP: VLAN Trunking Protocol, un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite centralizar y simplificar la administración en un dominio de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos. El protocolo VTP nace como una herramienta de administración para redes de cierto tamaño, donde la gestión manual se vuelve inabordable.

DTP: Dynamic Trunking Protocol es un protocolo propietario creado por Cisco Systems que opera entre switches Cisco, el cual automatiza la configuración de trunking (etiquetado de tramas de diferentes VLAN's con ISL o 802.1Q) en enlaces Ethernet.Dicho protocolo puede establecer los puertos ethernet en cinco modos diferentes de trabajo: AUTO, ON, OFF, DESIRABLE y NON-NEGOTIATE.

RESUMEN

En este trabajo se encuentran tres ejercicios donde se analizan y se aplican soluciones con base en los conocimientos adquiridos en el diplomado de cisco CCNP, en los cuales se explica el paso a paso y configuración que se aplicó a cada dispositivo con el objetivo de configurar cada escenario según lo solicitado en cada punto.

Con el desarrollo de estos ejercicios también se demuestra a nivel general el manejo de las herramientas trabajadas en el curso como lo son PACKET TRACER y GNS3.

Por ultimo aprendimos nueva terminología correspondiente al area de telecomunicaciones.

Palabras Clave: OSPF, EIGRP, VLAN,TRUNK, VTP,DTP

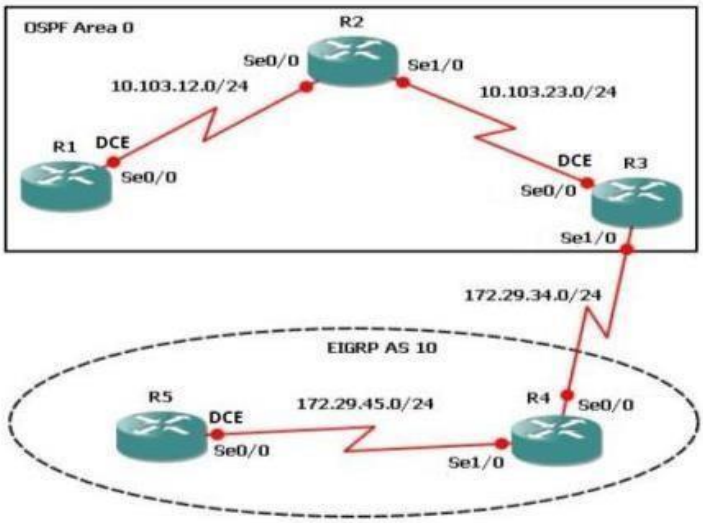
INTRODUCCIÓN

Este trabajo fue realizado con el fin de cumplir las Pruebas 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. Se requiere que los estudiantes para el desarrollo de las actividades planteadas, apliquen el contenido de las temáticas abordadas a lo largo del curso, correspondientes a Protocolos de Enrutamiento Avanzado, Implementación de soluciones soportadas en enrutamiento avanzado, configuración de sistemas de red soportados en VLANs, y Administración, Seguridad y Escalabilidad en redes conmutadas.

Se plantean 3 escenarios distintos sobre los cuales cada estudiante deberá realizar las tareas asignadas, y con base en ellas, sustentar con los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros., empleando cualquiera de las herramientas de Simulación: PACKET TRACER o GNS3. Finalmente, y con base en lo anterior, consolidarán el informe como evidencia del proceso de configuración realizado.

ESCENARIO 1

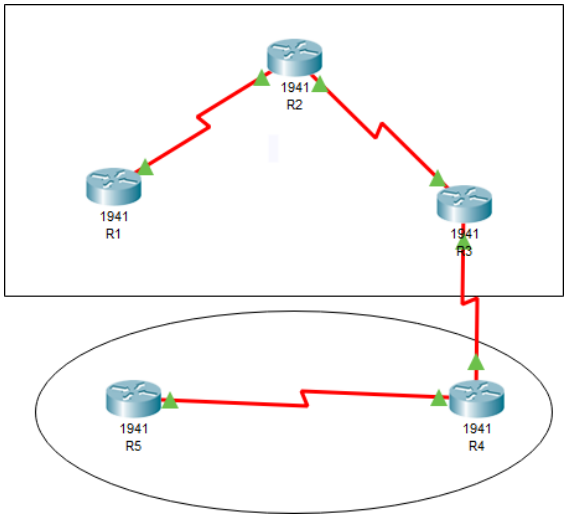
Figura 1. Ejemplo de topología a realizar.



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.

Se realiza la configuración inicial de las direcciones ip especificadas para cada router tal como se aprecia en la siguiente figura:

Figura 2. Topología escenario 1.



Se configuran las interfaces para cada router:

R1:
Router>enRouter#conf t
Router(config)#hostname R1
R1(config)#end
R1

R1#conf t
R1(config)#int s 0/0/0
R1(config-if)#ip address 10.103.12.1 255.255.255.0
R1(config-if)#clock rate 64000 R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#

Router>en
Router#conf t
Router(config)#hostname R2
R2(config)#end
R2#

R2#conf t
R2(config)#int s0/0/0
R2(config-if)#ip address 10.103.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#
R2(config-if)#exit
R2(config)#int s0/0/1
R2(config-if)#ip address 10.103.23.1 255.255.255.0
R2(config-if)#clock rate 64000
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#end
R2#

Router>en Router#conf t
Router(config)#hostname R3
R3(config)#end
R3#

```
R3#conf t
R3(config)#int s0/0/0
R3(config-if)#ip address 10.103.23.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#
R3(config-if)#exit
R3(config)#int s0/0/1
R3(config-if)#ip address
R3(config-if)#ip address 172.29.34.1 255.255.255.0
R3(config-if)#clock rate 64000
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#

Router>en Router#conf t
Router(config)#hostname R4
R4(config)#END
R4#

R4#conf t
R4(config)#int s0/0/0
R4(config-if)#ip address 172.29.34.2 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#
R4(config-if)#exit
R4(config)#int s0/0/1
R4(config-if)#
R4(config-if)#ip address 172.29.45.1 255.255.255.0
R4(config-if)#clock rate 64000
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#


Router>EN Router#conf t
Router(config)#hostname R5
R5(config)#end
R5#

R5#conf t
R5(config)#int s0/0/0
R5(config-if)#ip address 172.29.45.2 255.255.255.0
R5(config-if)#no shutdown
R5(config-if)#
```

```
R5(config-if)#exit
R5(config)#
```

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.

Se realiza la siguiente configuración en el Router R1 para las 4 interfaces con los siguientes comandos

```
R1#conf t
R1(config)#int Lo1
R1(config-if)#ip address 10.1.0.1 255.255.252.0
R1(config-if)#exit R1(config)#int Lo2
R1(config-if)#ip address 10.1.0.2 255.255.252.0
R1(config-if)#exit
R1(config)#int Lo3
R1(config-if)#
R1(config-if)#ipaddress 10.1.0.3 255.255.252.0
R1(config-if)#exit
R1(config)#int Lo4
R1(config-if)#
R1(config-if)#ip address 10.1.0.4 255.255.252.0
R1(config-router)#exit R1(config)#end
R1#
```

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.

Se realiza la siguiente configuración en el Router R5 utilizando las direcciones 172.5.0.0/22.

```
R5#conf t
R5(config)#int Lo1
R5(config-if)#
R5(config-if)#ip address 172.5.0.1 255.255.252.0
R5(config-if)#exit R5(config)#int Lo2
R5(config-if)#
R5(config-if)#ip address 172.5.0.2 255.255.252.0
R5(config-if)#exit
```

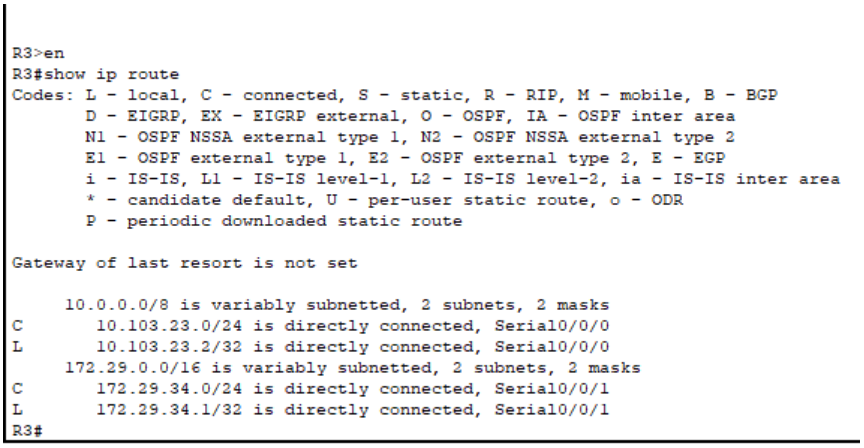
```
R5(config)#int Lo3 R5(config-if)#
R5(config-if)#ip address 172.5.0.3 255.255.252.0
R5(config-if)#exit
R5(config)#int Lo4
R5(config-if)#
R5(config-if)#ip address 172.5.0.4 255.255.252.0
R5(config-if)#exit
R5(config)#router eigrp 10
R5(config-router)#no auto-summary
R5(config-router)#network 172.5.0.0 0.0.3.255
R5(config-router)#exit
R5(config)#end
R5#
```

.

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

Utilizamos el comando show ip route en el R3 para validar:

Figura 3. Tabla de enrutamiento de R3.



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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.103.23.0/24 is directly connected, Serial0/0/0
L       10.103.23.2/32 is directly connected, Serial0/0/0
     172.29.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.29.34.0/24 is directly connected, Serial0/0/1
L       172.29.34.1/32 is directly connected, Serial0/0/1
R3#
```

Se puede observar que R3 ya reconoce la configuración Loopback configurada.

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

Se realiza la configuración en R3 con los siguientes comandos:

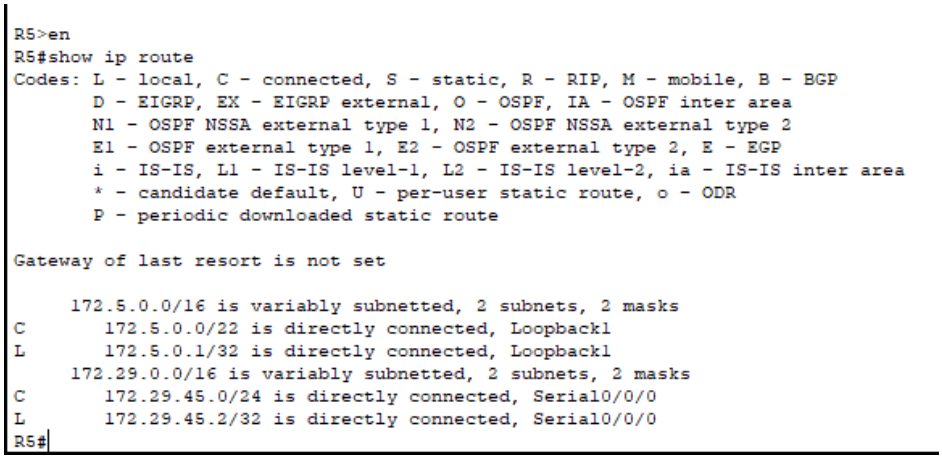
R3>en R3#conf t
R3(config)#router eigrp 10
R3(config-router)#redistribute ospf 1 metric 10000 100 255 1 1500
R3(config-router)#network 172.5.0.0 0.0.3.255
R3(config-router)#auto-summary
R3(config-router)#exit
R3(config)#router ospf 1
R3(config-router)#log-adjacency-changes
R3(config-router)#redistribute eigrp 10 subnets
R3(config-router)#network 10.1.0.0 0.0.3.255 area 0
R3(config-router)#exit
R3(config)#

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 4. Ruta de verificación de R1.

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

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks
C       10.1.0.0/22 is directly connected, Loopback1
L       10.1.0.1/32 is directly connected, Loopback1
C       10.103.12.0/24 is directly connected, Serial0/0/0
L       10.103.12.1/32 is directly connected, Serial0/0/0
R1#
```

Figura 5. Ruta de verificación de R5.

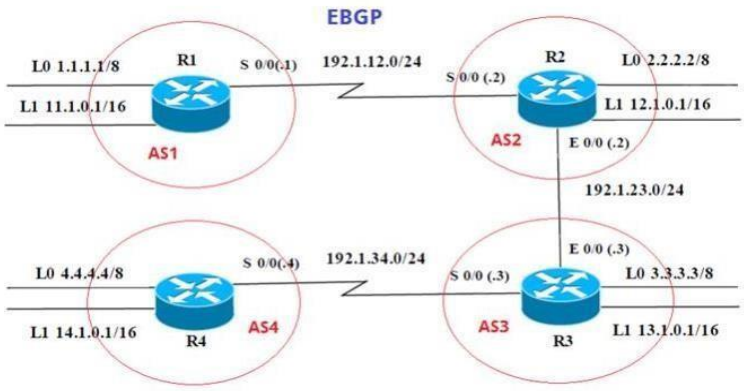


```
R5>en
R5#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2,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

Gateway of last resort is not set

     172.5.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.5.0.0/22 is directly connected, Loopback1
L       172.5.0.1/32 is directly connected, Loopback1
     172.29.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.29.45.0/24 is directly connected, Serial0/0/0
L       172.29.45.2/32 is directly connected, Serial0/0/0
R5#
```

Se realiza la validación en R1 y R5 mediante el comando show ip route y se verifica que estos routers contienen en su tabla de enrutamiento las interfaces configuradas.

ESCENARIO 2

Figura 6. Ejemplo de escenario 2.



Información para configuración de los routers:

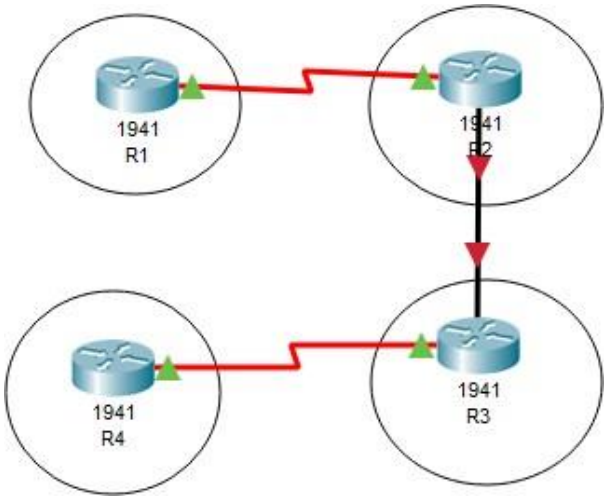
Tabla 1. Información para la configuración de los routers.

	Interfaz	Direccion IP	Mascara
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
	Interfaz	Direccion IP	Mascara
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	192.168.23.2	255.255.255.0
	Interfaz	Direccion IP	Mascara
R3	Loopback 0	3.3.3.3	255.0.0.0
	Loopback 1	13.1.0.1	255.255.0.0
	S 0/0	192.1.23.3	255.255.255.0
	E 0/0	192.168.34.3	255.255.255.0
	Interfaz	Direccion IP	Mascara
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

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 11.11.11.11para 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.

Figura 7. Topología de escenario 2.



Se realiza la configuración en los routers según la tabla 1

Router>EN Router#conf t
Router(config)#hostname R1
R1(config)#end
R1#

R1#conf t
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
R1(config-if)#exit
R1(config)#int Lo0
R1(config-if)#
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#exit
R1(config)#int Lo1 R1(config-if)#
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#exit
R1(config)#
Router>en Router#conf t
Router(config)#hostname R2

```
R2(config)#end
R2#

R2#conf t
R2(config)#int Lo0
R2(config-if)#
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#exit
R2(config)#int Lo1
R2(config-if)#
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#exit
R2(config)#int s0/0/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#
R2(config-if)#exit
R2(config)#int f0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#exit
R2(config)#


Router>en Router#conf t
Router(config)#hostname R3
R3(config)#exit
R3#

R3#conf t
R3(config)#int Lo0
R3(config-if)#
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#exit
R3(config)#int Lo1
R3(config-if)#
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#exit
R3(config)#int f0/0/0
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
```

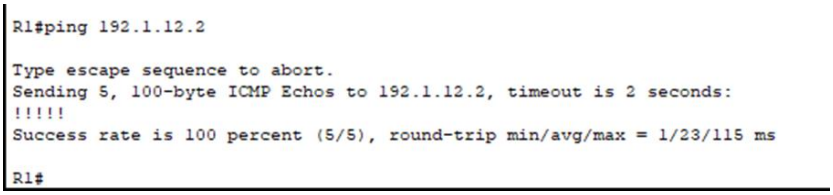
```
R3(config-if)#exit
R3(config)#


Router>en Router#conf t
 Router(config)#hostname R4
R4(config)#end
R4#

R4#conf t
R4(config)#int Lo0
R4(config-if)#
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#exit
R4(config)#int Lo1
R4(config-if)#
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#exit
R4(config)#int s0/0/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#clock rate 64000
R4(config-if)#no shutdown
R4(config-if)#
R4(config-if)#exit
R4(config)#
```

Se configure el vecino BGP para R1 y R2: R1:

```
R1#conf t
R1(config)#router bgp 100
R1(config-router)#network 192.1.12.1 mask 255.255.255.0
R1(config-router)#neighbor 192.1.12.2 remote-as 200
R1(config-router)#

R2#conf t
R2(config)#router bgp 200
R2(config-router)#network 192.1.12.2 mask 255.255.255.0
R2(config-router)#neighbor 192.1.12.1 remote-as 100
R2(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.12.1 Up
```

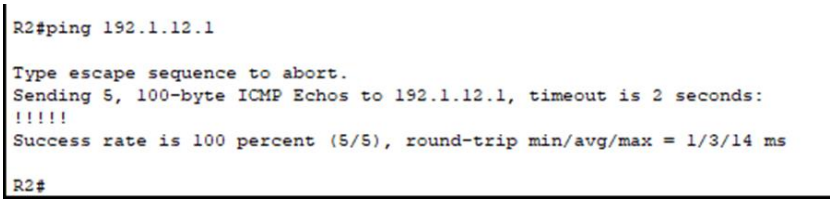
Se comprueba el funcionamiento de la relación BGP establecida:

Figura 8. Ping 192.1.12.2.



```
R1#ping 192.1.12.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/23/115 ms

R1#
```

Figura 9. Ping 192.1.12.1.



```
R2#ping 192.1.12.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.12.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/14 ms

R2#
```

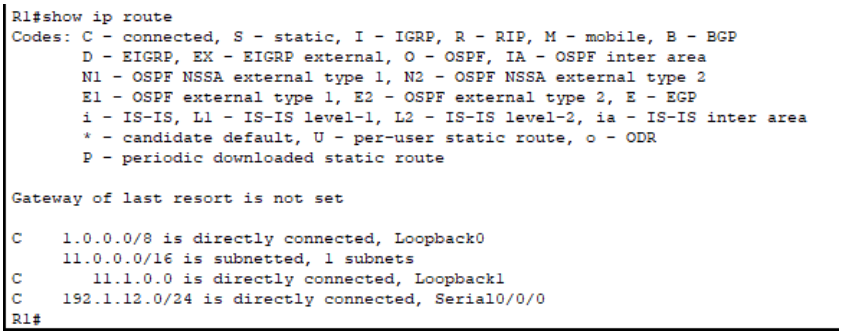
Con el comando ping a R1 y a R2 comprobamos el funcionamiento de la relación BGP establecida

Se codifican los ID para los routers BGP:

R1#conf t
R1(config)#router bgp 100
R1(config-router)#bgp router-id 11.11.11.11
R1(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.12.2 Up

R2#conf t
R2(config)#router bgp 200
R2(config-router)#bgp router-id 22.22.22.22
R2(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.12.1 Up

Figura 10. Show ip route.



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

Gateway of last resort is not set

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
C    192.1.12.0/24 is directly connected, Serial0/0/0
R1#
```

Utilizamos el comando Show ip router en R1 para confirmar la nueva configuración.

2. Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en AS2 y R3debería 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.

Se configura con los siguientes comandos:

R2#conf t
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#conf t
R3(config)#router bgp 300
R3(config-router)#network 192.1.12.3 mask 255.255.255.0
R3(config-router)#neighbor 192.1.12.2 remote-as 200 R3(config-router)#

Se codifica el ID para el router R3:

R3#CONF T
R3(config)#router bgp 300
R3(config-router)#bgp router-id 33.33.33.33 R3(config-router)#exit
R3(config)#end R3#

R3#show ip bgp
BGP table version is 1, local router ID is 33.33.33.33

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. Creerutas 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 delcomando show ip route.

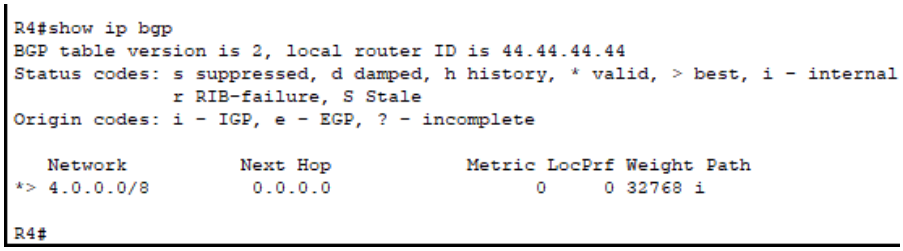
R3#conf t
R3(config)#router bgp 300
R3(config-router)#network 3.3.3.3 mask 255.0.0.0
R3(config-router)#neighbor 4.4.4.4 remote-as 400
R3(config-router)#exit
R3(config)#end

R3#

R4#conf t
R4(config)#router bgp 400
R4(config-router)#network 4.4.4.4 mask 255.0.0.0
R4(config-router)#neighbor 3.3.3.3 remote-as 300
R4(config-router)#exit
R4(config)#end
R4#

Se codifica el ID para el router R4:
R4#conf t
R4(config)#router bgp 400
R4(config-router)#bgp router-id 44.44.44.44
R4(config-router)#exit
R4(config)#end
R4(config)# router bgp 44
R4(config-router)#network 4.0.0.0 mask 255.0.0.0
R4(config-router)#network 14.1.0.0 mask 255.255.0.0
R4(config-router)#network 192.1.34.0 mask 255.255.255.0
exit
R4(config)# router bgp 44
R4(config-router)#neighbor 192.1.34.3 remote-as 33

Figura 11. Show ip bgp.



Con el comando show ip bgp en R4 confirmamos el ID como 44.44.44.44.

Ahora se crea la ruta estática para R3 y R4

Figura 12. Definiendo ruta estática en R3.

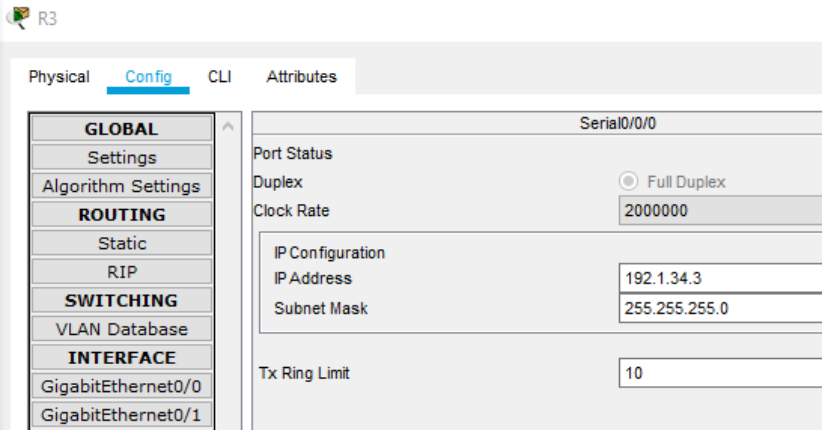
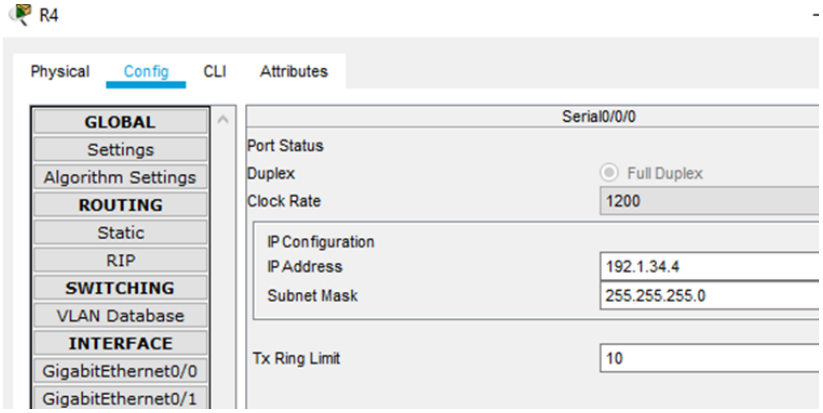


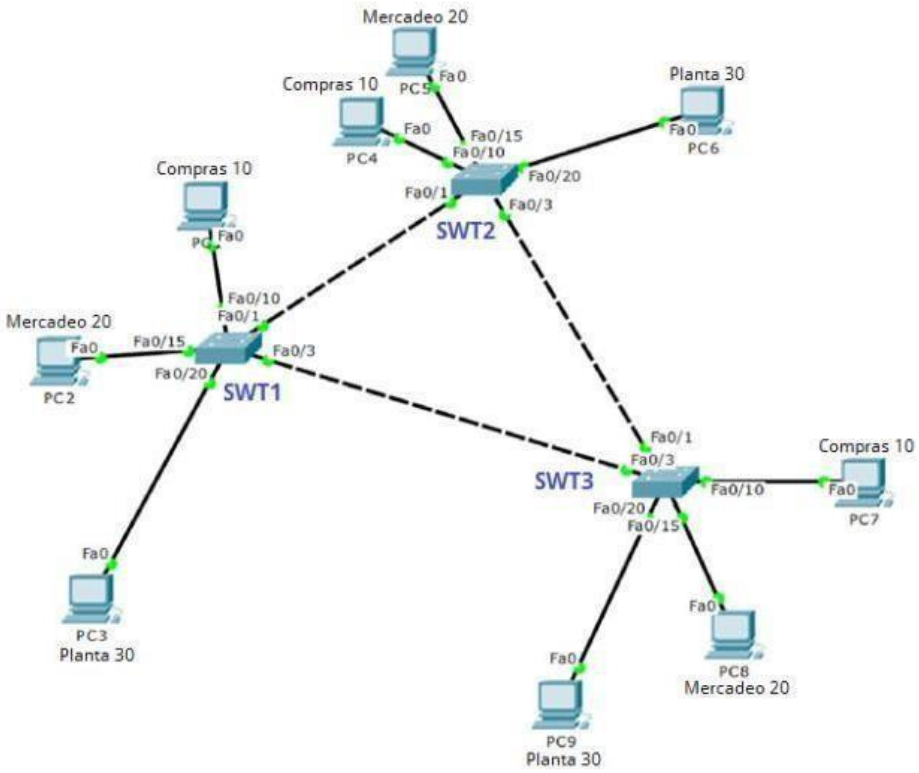
Figura 13. Definiendo ruta estática en R4.



Se procedió con la asignación de Ip´s fijas a R3 y R4 con el fin de completar la configuración.

ESCENARIO 3

Figura 14. Escenario 3.

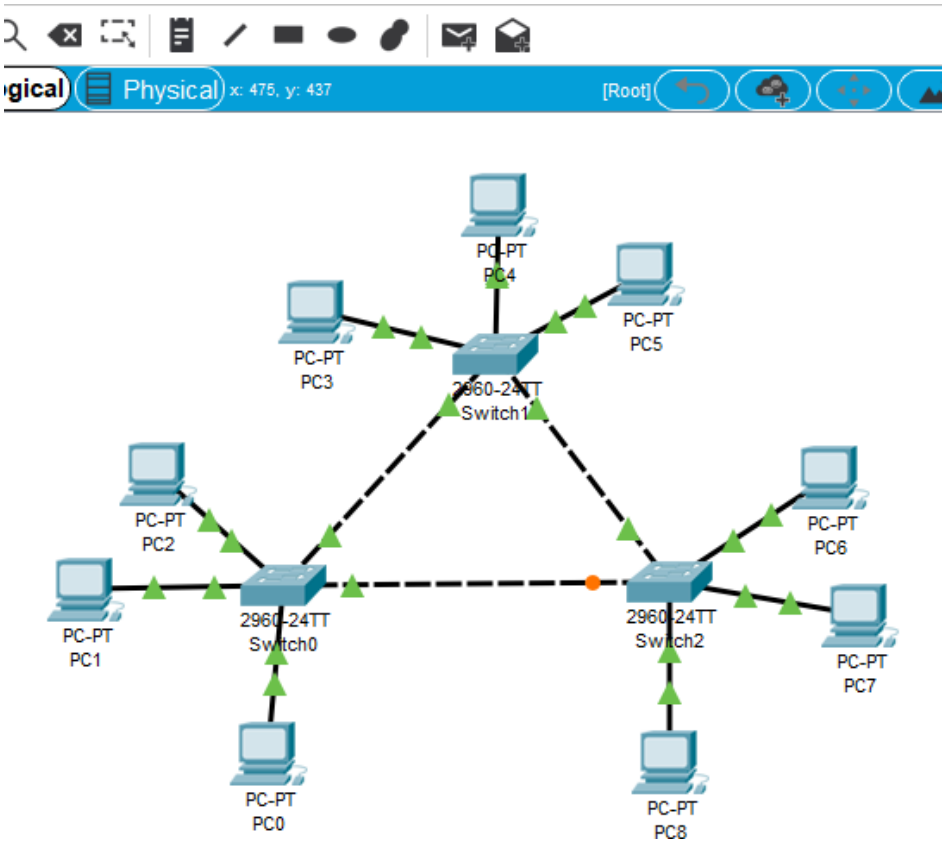


Configurar VTP

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.

Se realiza la simulación en packet tracer de la topología del escenario 3

Figura 15. Escenario 3 en Packet tracer.



Se procede a realizar la configuración de los SW1 y SW3 en modo cliente y el SW2 en modo servidor con los siguientes comandos:

SWT1(config)#vtp mode client
SWT1(config)#vtp domain CCNP
SWT1(config)#vtp password cisco

SWT2(config)#vtp mode server
SWT2(config)#vtp domain CCNP
SWT2(config)#vtp password cisco

SWT3(config)#vtp mode client
SWT3(config)#vtp domain CCNP
SWT3(config)#vtp password cisco

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

Figura 16. Configuración Swt1 a través del comando show vtp status.

```
SWT1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SWT1#
```

Figura 17. Configuración Swt2 a través del comando show vtp status.

```
SWT2#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
SWT2#
```

Figura 18. Configuración Swt3 a través del comando show vtp status.

```
SWT3#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SWT3#
```

Se muestra en cada switch la configuración que tiene en el momento.

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.Verifique el enlace "trunk" entre SWT1 y SWT2 usando el comando show interfaces trunk.
Se configuran los enlaces troncales con los siguientes comandos:

SWT1>EN

```
SWT1#conf t
SWT1(config)#int fa0/1
SWT1(config-if)#switchport mode dynamic desirable
SWT1(config-if)#
SWT1(config-if)#exit
SWT1(config)#end
SWT1#
```

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

Figura 19. Configuración de estatus truncado en 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
SWT1#
```

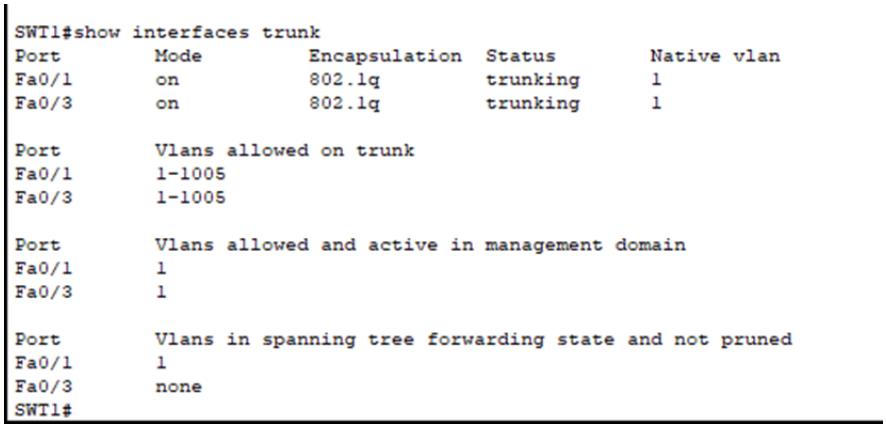
Se realiza la verificación en el SW1.

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

```
SWT1#conf t
SWT1(config)#int fa0/3
SWT1(config-if)#switchport mode trunk
SWT1(config-if)#
SWT1(config-if)#exit
SWT1(config)#end
SWT1#
```

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

Figura 20. Verificación de estatus truncado en Swt1.



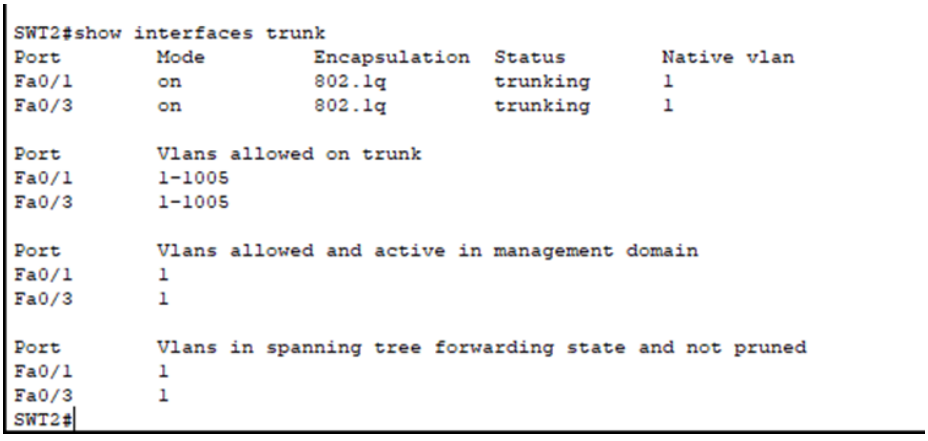
```
SWT1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/3       on           802.1q         trunking      1

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
SWT1#
```

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

Se aplican los siguientes comandos en SW2:

SWT2>en
SWT2#conf t
SWT2(config)#int fa0/3
SWT2(config-if)#switchport mode trunk
SWT2(config-if)#
SWT2(config-if)#exit
SWT2(config)#end
SWT2#

Figura 21. Configuración de estatus truncado en Swt2.



```
SWT2#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/3       on           802.1q         trunking      1

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

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

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
Fa0/3       1
SWT2#
```

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 agrega cada vlan de la siguiente manera:

```
SWT2>en
SWT2#conf t
SWT2(config)#vlan 10
SWT2(config-vlan)#name VLAN_Compras
SWT2(config-vlan)#exit
SWT2(config)#vlan 20
SWT2(config-vlan)#name VLAN_Mercadeo
SWT2(config-vlan)#exit
SWT2(config)#vlan 30
SWT2(config-vlan)#name VLAN_Planta
SWT2(config-vlan)#exit
SWT2(config)#vlan 99
SWT2(config-vlan)#name VLAN_Admon
SWT2(config-vlan)#exit
SWT2(config)#end
SWT2#
```

```
SWT1#conf t
SWT1(config)#int fa0/10
SWT1(config-if)#sw access vlan 10
SWT1(config-if)#exit
SWT1(config)#end
SWT1#
```

2. Verifique que las VLANs han sido agregadas correctamente.

Figura 22. Verificación de inclusión de las Vlans en el Swt1.

```
SWT1#show vlan

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

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
```

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

Tabla 2. Direccionamiento routers.

Interfaz	VLAN	Direcciones IP de los PCs
F 0/10	vlan 10	190.108.10.x/24
F 0/15	vlan 20	190.108.20.x/24
F 0/20	vlan 30	190.108.30.x/24

SWT1#conf t
SWT1(config)#int fa0/10
SWT1(config-if)#switchport mode access
SWT1(config-if)#switchport access vlan 10
SWT1(config-if)#exit
SWT1(config)#int fa0/15
SWT1(config-if)#
SWT1#

SWT1#conf t
SWT1(config)#int fa0/15

```
SWT1(config-if)#switchport mode access
SWT1(config-if)#switchport access vlan 20
SWT1(config-if)#exit
SWT1(config)#int fa0/20
SWT1(config-if)#switchport mode access
SWT1(config-if)#switchport access vlan 30
SWT1(config-if)#exit
SWT1(config)#end
SWT1#
```

Configure el puerto F0/10 en modo de acceso para SWT1, SWT2 y SWT3 y asígnelo a la VLAN 10.
5. Repita el procedimiento para los puertos F0/15 y F0/20 en SWT1, SWT2 y SWT3. Asigne las VLANs ylas direcciones IP de los PCs de acuerdo con la tabla de arriba.

Se realiza mediante los siguientes comandos para todos los SW:

```
interface range f0/10
switchport mode access
switchport access vlan 10
exit
interface range f0/15
switchport mode access
switchport access vlan 20
exit
interface range f0/20
switchport mode access
switchport access vlan 30
```

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 deacuerdo con la siguiente tabla de direccionamiento y active la interfaz.

Tabla 3. Direccionamiento IP.

Interfaz	VLAN	Direcciones IP de los PCs
F 0/10	vlan 10	190.108.10.x/24
F 0/15	vlan 20	190.108.20.x/24
F 0/20	vlan 30	190.108.30.x/24

Se configura para cada uno de los switches de la siguiente manera:

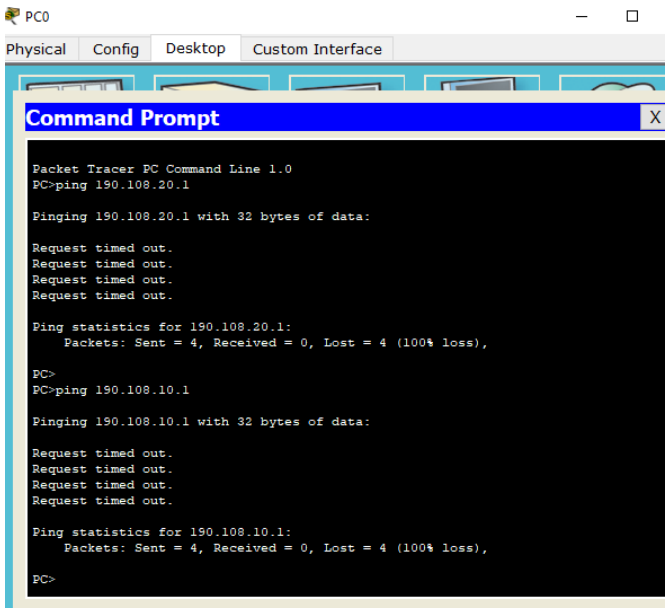
```
SWT1#conf t
SWT1(config)#int fa0/10
SWT1(config-if)#switchport mode access
SWT1(config-if)#switchport access vlan 10
SWT1(config-if)#exit
SWT1(config)#int fa0/15
SWT1(config-if)#
SWT1#

SWT1#conf t
SWT1(config)#int fa0/15
SWT1(config-if)#switchport mode access
SWT1(config-if)#switchport access vlan 20
SWT1(config-if)#exit
SWT1(config)#int fa0/20
SWT1(config-if)#switchport mode access
SWT1(config-if)#switchport access vlan 30
SWT1(config-if)#exit
SWT1(config)#end
SWT1#


SWT2#conf t
SWT2(config)#int fa0/10
SWT2(config-if)#switchport mode access
SWT2(config-if)#switchport access vlan 10
SWT2(config-if)#exit
SWT2(config)#int fa0/15
SWT2(config-if)#switchport mode access
SWT2(config-if)#switchport access vlan 20
SWT2(config-if)#exit
SWT2(config)#int fa0/20
SWT2(config-if)#switchport mode access
SWT2(config-if)#switchport access vlan 30
SWT2(config-if)#exit
```

```
SWT2(config)#end
SWT2#

SWT3#conf t
SWT3(config)#int fa0/10
SWT3(config-if)#switchport mode access
SWT3(config-if)#switchport access vlan 10
SWT3(config-if)#exit
SWT3(config)#int fa0/15
SWT3(config-if)#switchport mode access
SWT3(config-if)#switchport access vlan 20
SWT3(config-if)#exit
SWT3(config)#int fa0/20
SWT3(config-if)#switchport mode access
SWT3(config-if)#switchport access vlan 30
SWT3(config-if)#exit
SWT3(config)#end
SWT3#
```

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.

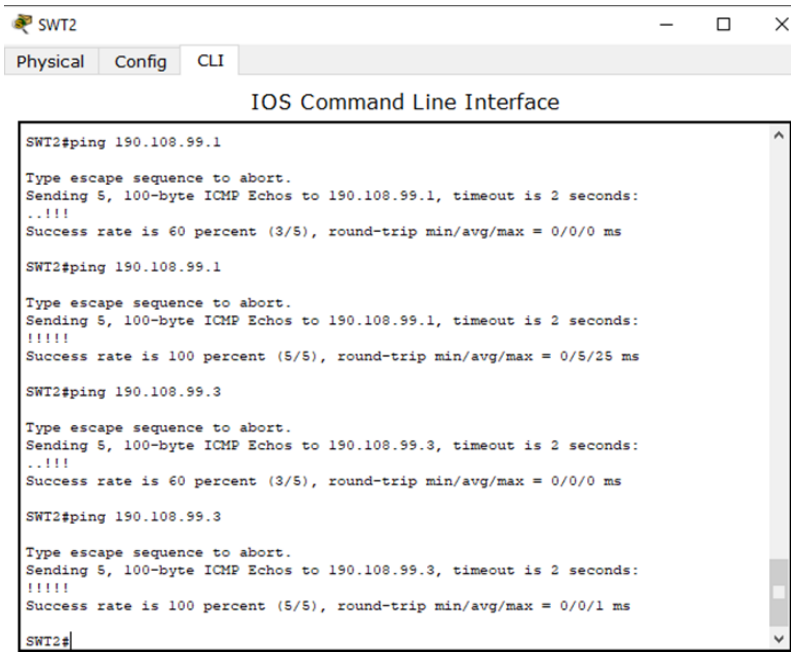
Figura 23. Verificación de ping de extremo a extremo.



Cuando se realiza ping a los demás equipos, estos no responden, ya que se encuentran en diferentes segmentos.

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

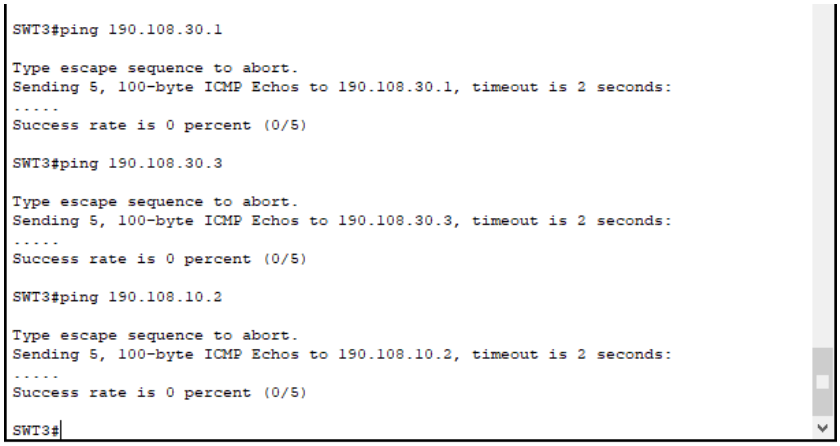
Figura 24. Ejecución de Píng desde cada Switch a los demás.



Si tiene éxito ya que se configura una VLAN común para todos, la de administración y en este caso se tiene comunicación desde allí.

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

Figura 25. Ejecución de Píng desde cada Switch a cada PC.



No se tuvo éxito ya que ni el switch ni el pc tienen configurada una dirección

ip, esto hace que los equipos no se encuentren dentro de la red. La dirección ip es primordial ya que permite a cada dispositivo ser reconocido dentro de la misma red y así poder enviar y recibir información.

CONCLUSIONES

Se llevó a cabo el desarrollo de la Prueba de Habilidades Prácticas implementada como parte de las actividades evaluativas del Diplomado de Profundización 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.

Se estableció relaciones de vecino BGP, anunciando las direcciones Loopback correspondientes, codificando los ID de los routers y comprobando el funcionamiento de las conexiones realizadas de acuerdo a los parámetros definidos para el escenario 2.

Se puso en práctica las temáticas abordadas a lo largo del curso, correspondientes a protocolos de Enrutamiento Avanzado, Implementación de soluciones soportadas en enrutamiento avanzado, configuración de sistemas de red soportados en VLANs, y Administración, Seguridad y Escalabilidad en redes conmutadas.

Se aplicó los procesos de configuración VTP para las actualizaciones de VLAN, empleando configuraciones de tipo servidor y cliente, y estableciendo dominios y contraseñas predeterminados. Adicional, se configuraron enlaces troncales dinámicos, estáticos y permanentes, con el

Se realizó procesos de configuración de protocolos de enrutamiento para routers, de interfaces Loopback, asignación de direcciones IP, configuración OSPF y EIGPR, y redistribución de rutas a partir de las topologías y criterios planteados para el escenario 1.

Finalmente, se sustentó el desarrollo de cada escenario con los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de los comandos requeridos para cada caso, empleando la herramienta de simulación Packet Tracer.

REFERENCIAS BIBLIOGRÁFICAS

Reyes, G. (2019). Fundamentos de BGP - Sea CCNA. Retrieved 2 August 2019, from https://www.seaccna.com/fundamentos-de-bgp/

UNAD (2019) 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

UNAD (2019) 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