DIPLOMADO CCNP - CISCO PRUEBA DE HABILIDADES CCNP

EYDER ALEXANDER CORTES ORTIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA DE SISTEMAS PALMIRA

2020

DIPLOMADO CCNP - CISCO PRUEBA DE HABILIDADES CCNP

EYDER ALEXANDER CORTES ORTIZ

Diplomado de profundización CISCO

Director /Tutor

MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA DE SISTEMAS PALMIRA

2020

NOTA DE ACEPTACIÓN:

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Palmira, (mayo 22, 2020)

AGRADECIMIENTO

Le agradezco a Dios por haberme acompañado y guiado a lo largo de mi carrera, por ser mi fortaleza en los momentos de debilidad y por brindarme una vida llena de aprendizajes, experiencias y sobre todo felicidad.

A mis padres por su cariño y apoyo incondicional, durante todo este proceso, por estar conmigo en todo momento gracias.

A toda mi familia porque con sus oraciones, consejos y palabras de aliento hicieron de mí una mejor persona y de una u otra forma me acompañan en todos mis sueños y metas.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Banda: Conjunto de las frecuencias comprendidas entre límites determinados y pertenecientes a un espectro o gama de mayor extensión. La clasificación adoptada internacionalmente está basada en bandas numeradas que van de la que se ubica de los 0.3 x 10n Hz a 3 x 10n Hz, en la cual n es el número de banda.

EGP: El Exterior Gateway Protocol (EGP) es un protocolo estándar usado para intercambiar información de encaminamiento entre sistemas autónomos. Las puertas de enlace o pasarelas EGP solamente pueden retransmitir información de accesibilidad para las redes de su sistema autónomo (AS).

Fibra multimodo: Un tipo de cable de fibra óptica con un diámetro de núcleo de entre 50 y 100 mm. En fibra multimodo, rayos diferentes de luz rebotan a lo largo de la fibra a diferentes ángulos cuando viajan por el núcleo. Esto resulta en algún grado de distorsión de la señal en el extremo receptor. La fibra multimodo puede ser de dos tipos: de índice graduado o de índice escalonado.

ICPM (Internet Control Message Protocol, Protocolo de mensajes de control de Internet): Es un protocolo que permite administrar información relacionada con errores de los equipos en red

ISP (Internet Services Provider/Proveedor de Servicios de Internet): Una compañía que proporciona a sus clientes acceso a Internet.

Loopbaak: El dispositivo de red loopback es una interfaz de red virtual. ...
También es posible hacer ping a la dirección de loopback para probar la configuración de TCP/IP en el host local. A pesar de que sólo se usa la dirección única ' 127.0.0.1 ', se reservan las direcciones desde la ' 127.0.0.0 ' hasta la ' 127.255.255.255 '.

TCP: (del inglés Transmission Control Protocol, Protocolo de Control de Transmisión). Protocolo que fue creado entre los años 1973 - 1974 (por Vint Cerf y Robert Kahn) es uno de los protocolos fundamentales en Internet. Muchos programas dentro de una red de datos compuesta por computadores pueden usar TCP para crear conexiones entre ellos a través de las cuales enviarse datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

WAN (del inglés Wide Area Network, Red de área amplia): Tipo de red de computadores capaz de cubrir distancias desde unos 100 hasta unos 1000 km, proveyendo de servicio a un país o un continente. Un ejemplo de este tipo de redes sería RedIRIS, Internet o cualquier red en la cual no estén en un mismo edificio todos sus miembros (sobre la distancia hay discusión posible). Muchas WAN son construidas por y para una organización o empresa particular y son de uso privado, otras son construidas por los proveedores de Internet (ISP) para proveer de conexión a sus clientes.

RESUMEN

El siguiente trabajo escrito se realizó para ilustrar los pasos con que se llevó a cabo la configuración de redes de los escenarios asignados en la prueba del diplomado de profundización CISCO CCNP. En el cual se explica el enrutamiento y conmutación para configurar dichos escenarios. La ingeniería electrónica de la universidad UNAD tiene como requisito la presentación de este trabajo para obtener el grado de ingeniero electrónico.

Palabras clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica

ASTRACT

The following written work was carried out to illustrate the steps with which the network configuration of the scenarios assigned in the CISCO CCNP deepening diploma test was carried out. In which the routing and switching are explained to configure these scenarios. The electronic engineering of the UNAD university has as a requirement the presentation of this work to obtain the degree of electronic engineer.

Keywords: CISCO, CCNP, Routing, Swicthing, Networking, Electronics.

INTRODUCCION

El presente documento constituye la evidencia del desarrollo total de las actividades propuestas para la prueba de habilidades prácticas del Diplomado de Profundización CISCO CCNP ofrecido como opción de grado en la Universidad Nacional Abierta y a Distancia – UNAD. Para el desarrollo de las actividades aquí plasmadas, se realizaron las respectivas consultas sobre la implementación de las diferentes soluciones soportadas para el enrutamiento avanzado.

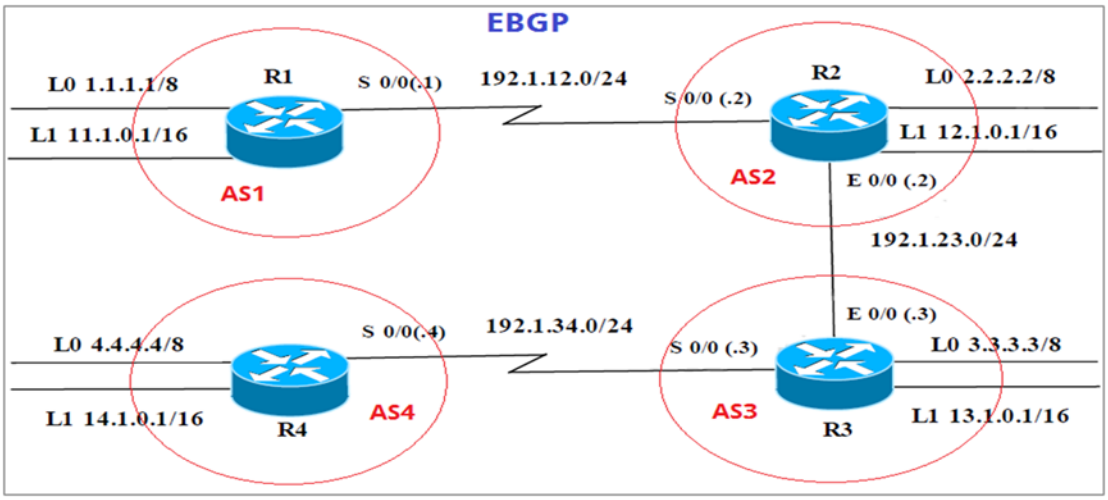
En las páginas siguientes se documentará detalladamente el desarrollo de cada una de las actividades indicadas; cada desarrollo incluye las respuestas a los interrogantes planteados y el informe cuenta con las correspondientes conclusiones inherentes a todo lo desarrollado.

Además, se pondrá en evidencia los conocimientos adquiridos durante la fase, el cual está conformado por el módulo; CCNP SWITCH donde se abordarán conceptos principales como operaciones y puertos de swtiches, NTP, SNMP, HSRP entre otros. Los laboratorios aquí plasmados, se realizarán mediante simuladores GNS3, Packet Tracer y SmartLab.

DESARROLLO DE LOS ESCENARIOS

Escenario 1

Figura 1. Escenario 2.



Fuente: Prueba de habilidades CCNP 2020, Cisco Academy.

Tabla 1. interfaz, dirección IP y máscara.

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	192.1.34.3	255.255.255.0

Fuente: Prueba de habilidades CCNP 2020, Cisco Academy.

Relación de vecino BGP entre R1 y R2

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 22.22.22.22 para R1 y como 33.33.33.33 para R2. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

```
R1(config)#hostname R1
R1(config)#interface Loopback 0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#interface Loopback 1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#interface serial 0/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router bgp 1
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#network 1.0.0.0 mask 255.0.0.0
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router)#network 192.1.12.0 mask 255.255.255.0
R1(config-router)#neighbor 192.1.12.2 remote-as 2
R1(config-router)#exit
R1(config)#do  wr
Building configuration...

R2(config)#hostname R2
R2(config)#interface Loopback 0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#interface Loopback 1
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#interface serial 0/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#interface e1/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router bgp 2
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#network 2.0.0.0 mask 255.0.0.0
```

Figura 2. Rutas vecinas entre R1 y R2.

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

Gateway of last resort is not set

C    192.1.12.0/24 is directly connected, Serial0/0
C    1.0.0.0/8 is directly connected, Loopback0
B    2.0.0.0/8 [20/0] via 192.1.12.2, 00:01:44
     11.0.0.0/16 is subnetted, 1 subnets
C       11.1.0.0 is directly connected, Loopback1
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.12.2, 00:01:44
R1#
```

Fuente: Elaboración propia.

Figura 3. Rutas vecinas entre R1 y R2.

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

Gateway of last resort is not set

C    192.1.12.0/24 is directly connected, Serial0/0
B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:02:53
C    2.0.0.0/8 is directly connected, Loopback0
C    192.1.23.0/24 is directly connected, Ethernet1/0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.12.1, 00:02:53
     12.0.0.0/16 is subnetted, 1 subnets
C       12.1.0.0 is directly connected, Loopback1
R2#
```

Fuente: Elaboración propia.

Relación de vecino BGP entre R2 y R3

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 44.44.44.44.

Presente el paso a con los comandos utilizados y la salida del comando show ip route.

```
R2(config)#router bgp 2
R2(config-router)#network 192.1.23.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.23.3 remote-as 3
R2(config-router)#do wr
Building configuration...


R3(config)#hostname R3
R3(config)#interface Loopback 0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#interface Loopback 1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#interface e1/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#interface serial 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 bgp 3
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#network 3.0.0.0 mask 255.0.0.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3(config-router)#network 192.1.23.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.23.2 remote-as 2
```

A continuación, se puede evidenciar en el resultado que se obtiene del comando show ip route, que el router R2 ha actualizado su tabla de enrutamiento y ahora contiene también las direcciones de Loopback configuradas en el router R3, por tanto, este dispositivo ha aprendido hasta este momento 4 rutas a través del protocolo BGP las cuales identifica con el código B. De otro lado, el router R3 contiene en su tabla de enrutamiento las redes que reconoce conectadas directamente, es decir, las configuradas en sus interfaces Loopback y las redes que lo comunican con los routers R3 y R4 mediante las interfaces fastEthernet

Figura 4. Rutas vecinas entre R2 y R3.

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

Gateway of last resort is not set

C    192.1.12.0/24 is directly connected, Serial0/0
B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:06:17
C    2.0.0.0/8 is directly connected, Loopback0
B    3.0.0.0/8 [20/0] via 192.1.23.3, 00:00:23
C    192.1.23.0/24 is directly connected, Ethernet1/0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.12.1, 00:06:17
     12.0.0.0/16 is subnetted, 1 subnets
C       12.1.0.0 is directly connected, Loopback1
     13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0 [20/0] via 192.1.23.3, 00:00:25
R2#
```

Fuente: Elaboración propia.

Figura 5. Rutas vecinas entre R2 y R3.

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

Gateway of last resort is not set

B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:01:06
B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:01:06
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:01:06
C    3.0.0.0/8 is directly connected, Loopback0
C    192.1.23.0/24 is directly connected, Ethernet1/0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.23.2, 00:01:06
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.23.2, 00:01:06
     13.0.0.0/16 is subnetted, 1 subnets
C       13.1.0.0 is directly connected, Loopback1
R3#
```

Fuente: Elaboración propia.

Relación de vecino BGP entre R3 y R4

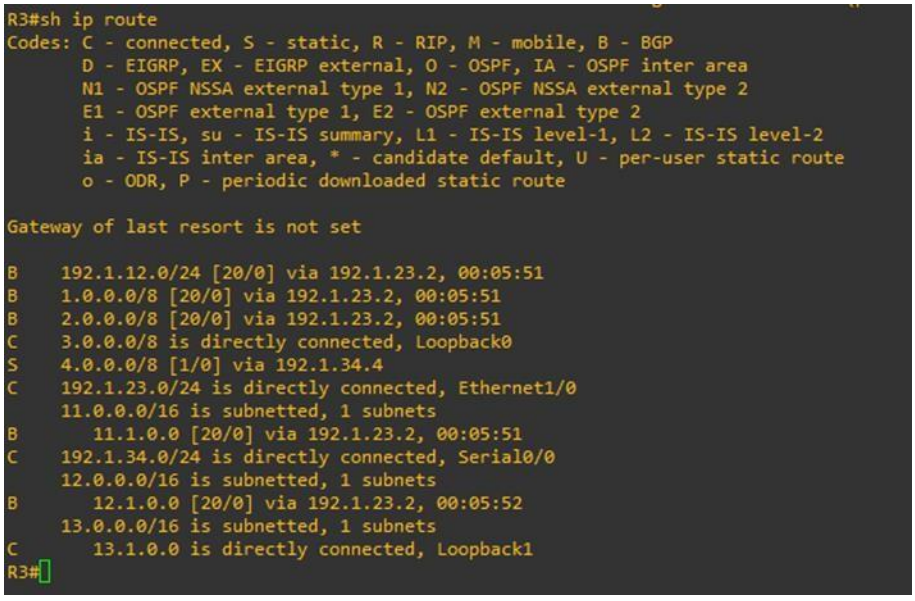
Configure una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en AS3 y R4 debería estar en AS4. Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como 66.66.66.66. Establezca las relaciones de vecino con base en las direcciones de Loopback 0. Cree rutas 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(config)#router bgp 3
R3(config-router)#network 192.1.34.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#ip route 4.0.0.0 255.0.0.0 192.1.34.4
R3(config)#router bgp 3
R3(config-router)#no neighbor 192.1.34.4
R3(config-router)#no network 3.0.0.0 mask 255.0.0.0
R3(config-router)#neighbor 4.4.4.4 remote-as 4
R3(config-router)#neighbor 4.4.4.4 update-source loopback 0
R3(config-router)# neighbor 4.4.4.4 ebgp-multihop
```

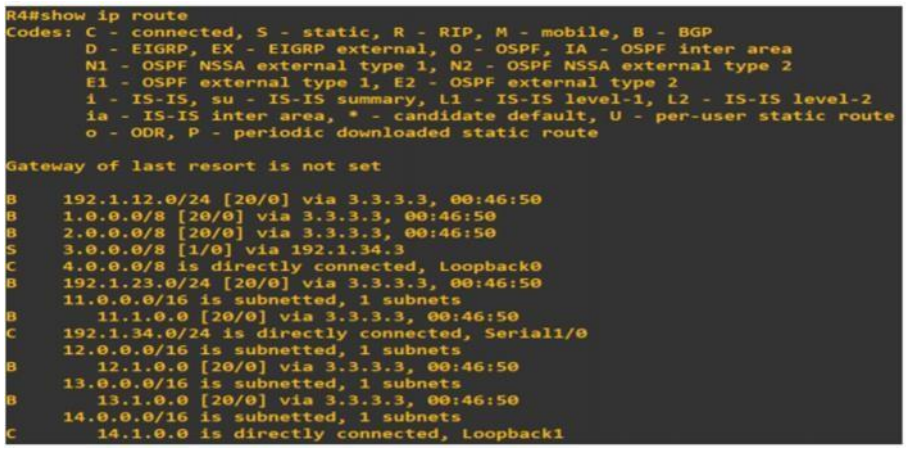
```
R4(config)#hostname R4
R4(config)#interface Loopback 0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#interface Loopback 1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#interface serial 0/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#router bgp 4
R4(config-router)#bgp router-id 66.66.66.66
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
R4(config-router)#neighbor 192.1.34.3 remote-as 3
R4(config-router)#exit
R4(config)#ip route 3.0.0.0 255.0.0.0 192.1.34.3
R4(config)#router bgp 4
R4(config-router)#no neighbor 192.1.34.3
R4(config-router)#neighbor 3.3.3.3 remote-as 4
R4(config-router)#neighbor 3.3.3.3 update-source loopback 0
R4(config-router)# neighbor 3.3.3.3 ebgp-multihop
R4(config-router)#do wr
Building configuration...
```

Figura 6. Rutas vecinas entre R3 y R4.



Fuente: Elaboración propia.

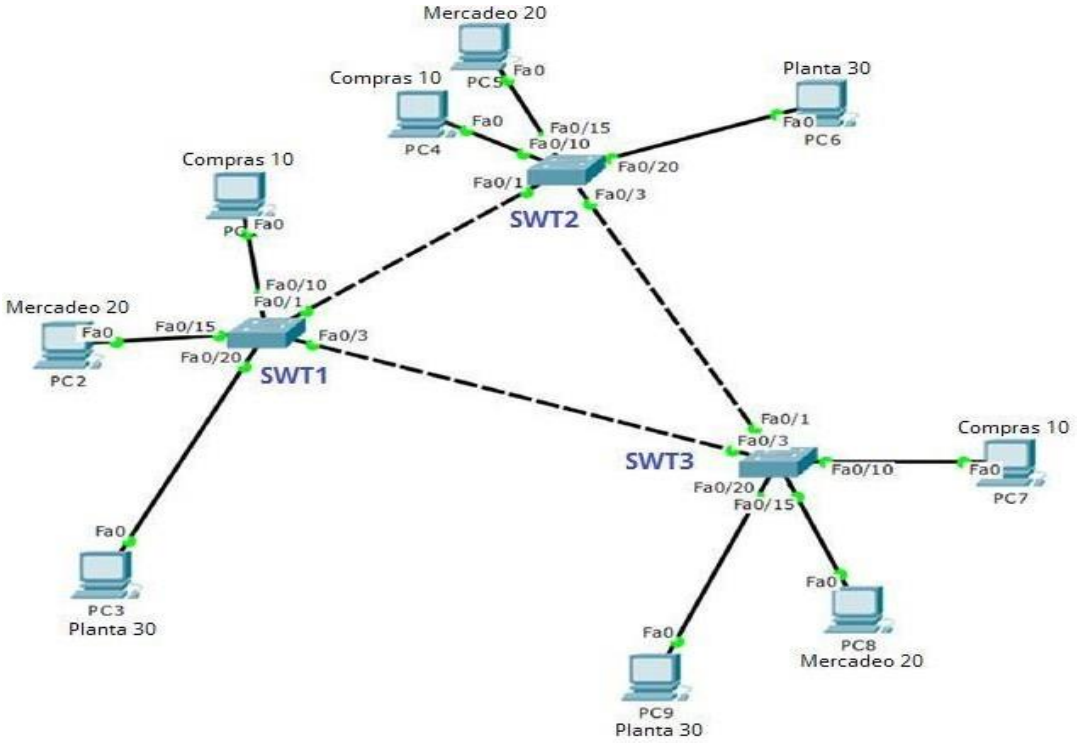
Figura 7. Rutas vecinas entre R3 y R4.



Fuente: Elaboración propia.

Escenario 2

Figura 8. Escenario 3.



Fuente: Prueba de habilidades CCNP 2020, Cisco Academy.

A. Configurar VTP

1. Todos los switches se configurarán para usar VTP para las actualizaciones de VLAN.

El switch SW-BB se configurará como el servidor. Los switches SW-AA y SW-CC se configurarán como clientes. Los switches estarán en el dominio VPT llamado CCNP y usando la contraseña cisco.

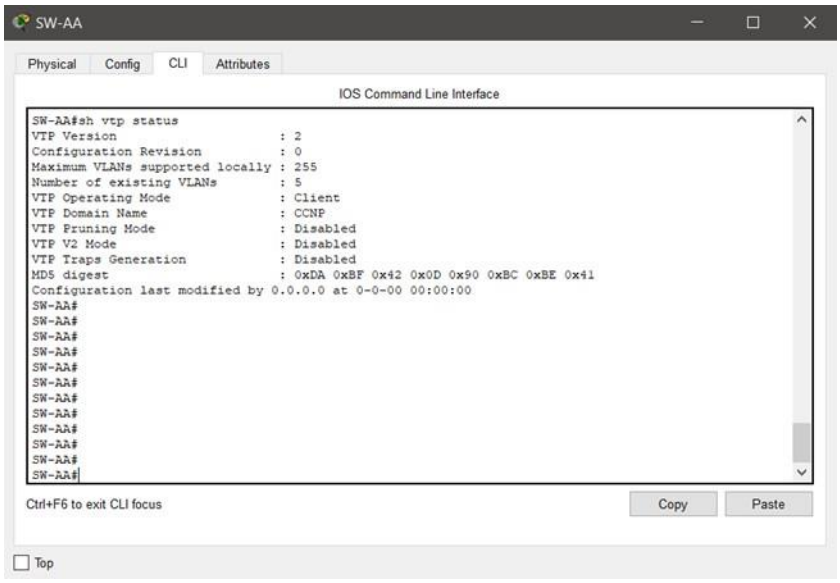
Switch 1

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-AA
SW-AA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-AA(config)#vtp domain CCNP
Domain name already set to CCNP.
```

```
SW-AA(config)#vtp password cisco
Password already set to cisco

Switch  2

Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-BB
SW-BB(config)#vtp mode server
Device mode already VTP SERVER.
SW-BB(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-BB(config)#vtp password cisco
Setting device VLAN database password to cisco


Switch  3

Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-CC
SW-CC(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-CC(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-CC(config)#vtp password cisco
Setting device VLAN database password to cisco
```

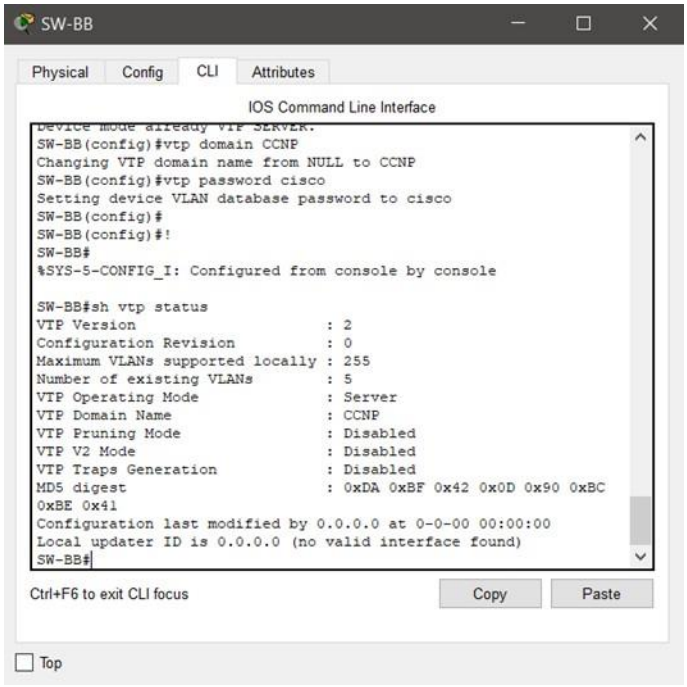
2. Verifique las configuraciones mediante el comando show vtp status.

Figura 9. Status del SW en VTP.



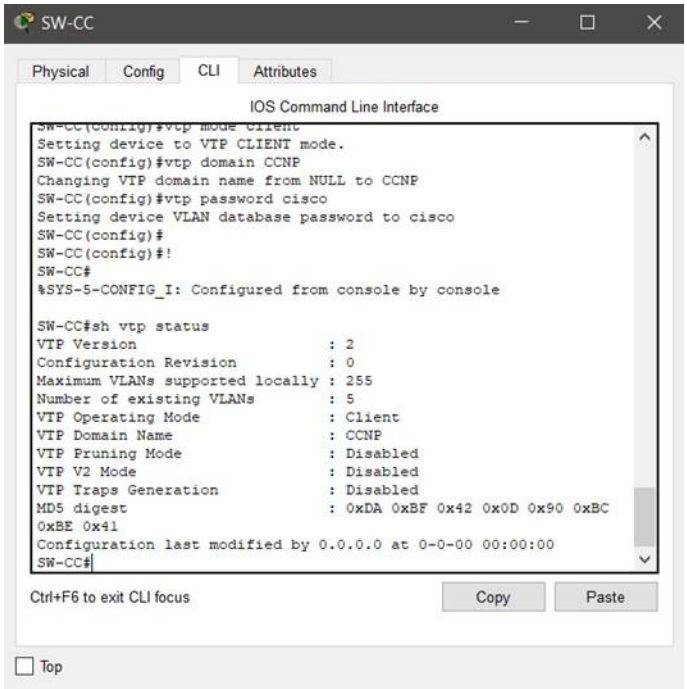
Fuente: Elaboración propia.

Figura 10. Status del SW en VTP.



Fuente: Elaboración propia.

Figura 11. Status del SW en VTP.



Fuente: Elaboración propia.

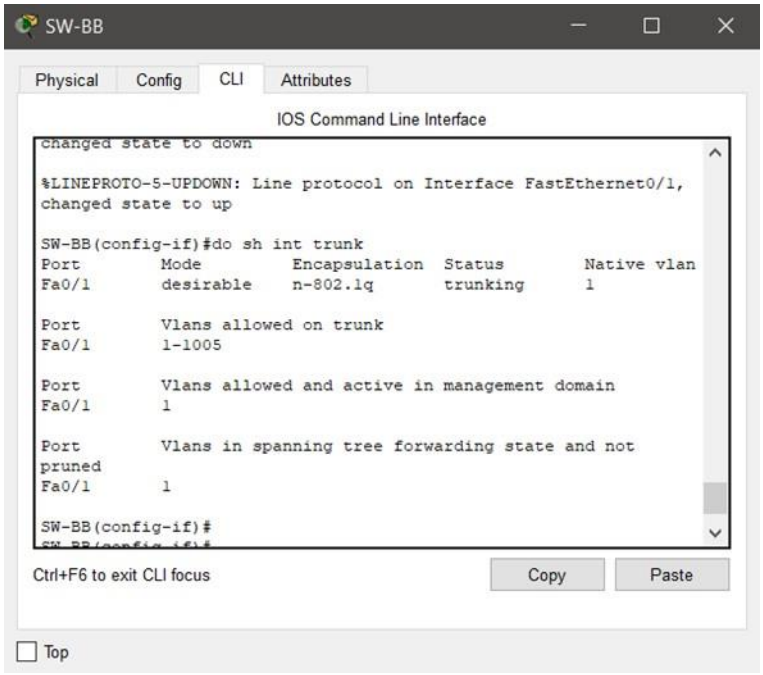
B. Configurar DTP (Dynamic Trunking Protocol)

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

```
SW-BB(config)#interface fastEthernet 0/1
SW-BB(config-if)#switchport mode dynamic desirable
```

2. Verifique el enlace "trunk" entre SW-AA y SW-BB usando el comando ***show interfaces trunk.***

Figura 12. Modo trunk de los puertos.



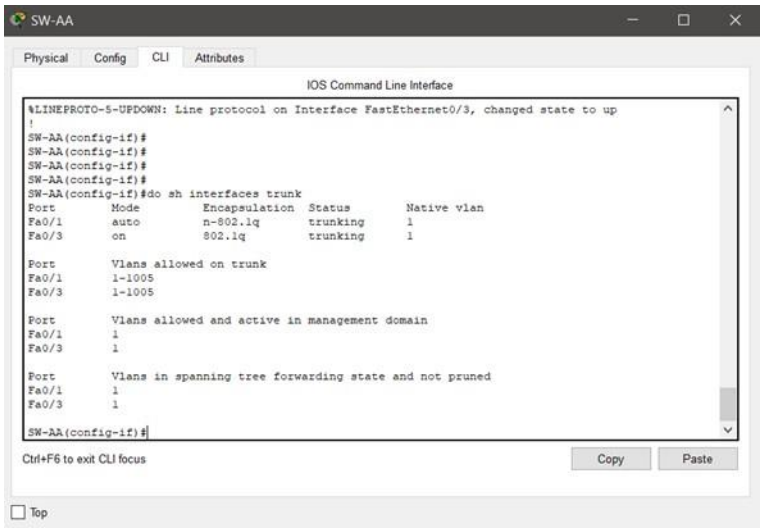
Fuente: Elaboración propia.

3. Entre SW-AA y SW-CC configure un enlace "trunk" estático utilizando el comando ***switchport mode trunk*** en la interfaz F0/3 de SW-AA.

```
SW-AA(config)#interface fastEthernet 0/3
SW-AA(config-if)#switchport mode trunk
```

4. Verifique el enlace "trunk" el comando ***show interfaces trunk*** en SW-AA.

Figura 13. Modo trunk de los puertos.

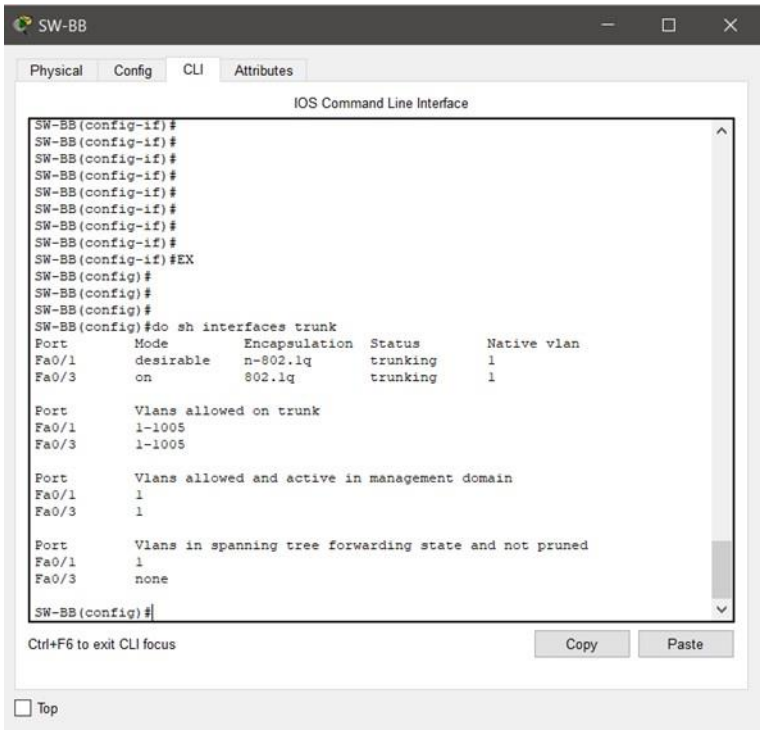


Fuente: Elaboración propia.

5. Configure un enlace "trunk" permanente entre SW-BB y SW-CC.

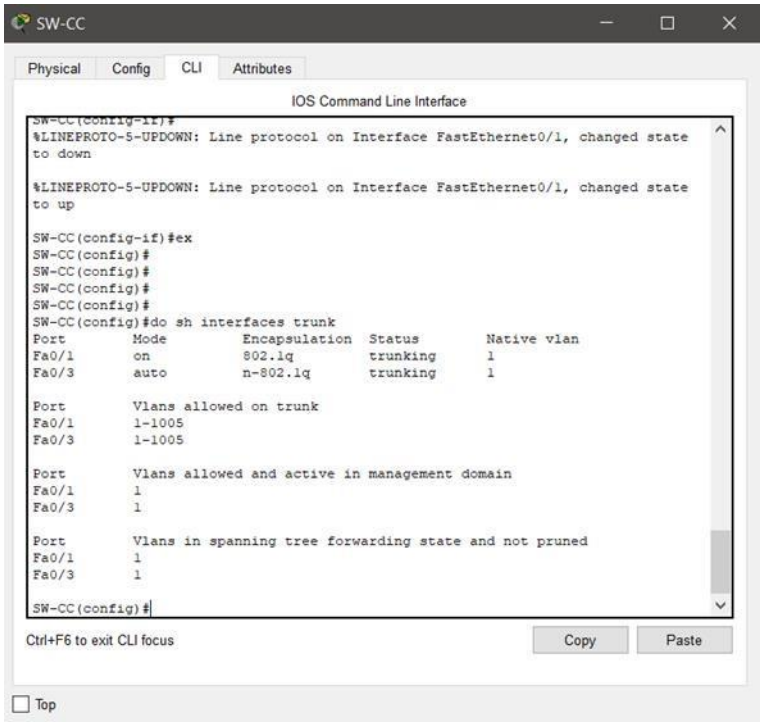
```
SW-CC(config)#interface fastEthernet 0/1
SW-CC(config-if)#switchport mode trunk

SW-BB(config)#interface fastEthernet 0/3
SW-BB(config-if)#switchport mode trunk
```

Figura 14. Modo trunk de los puertos.



Fuente: Elaboración propia.

Figura 15. Modo trunk de los puertos.



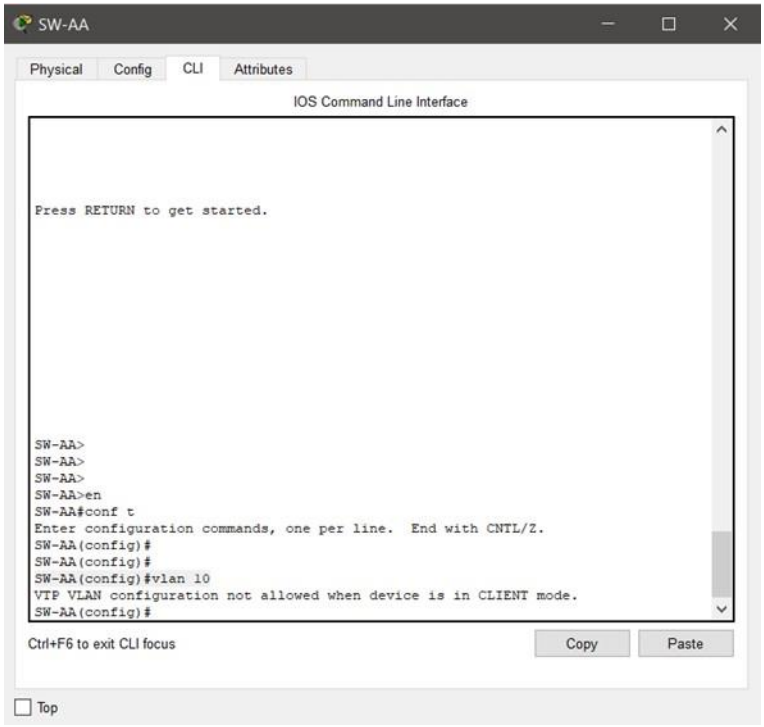
Fuente: Elaboración propia.

C. Agregar VLANs y asignar puertos.

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

```
SW-AA(config)#vlan 10
```

Figura 16. Error en creación de VLAN.

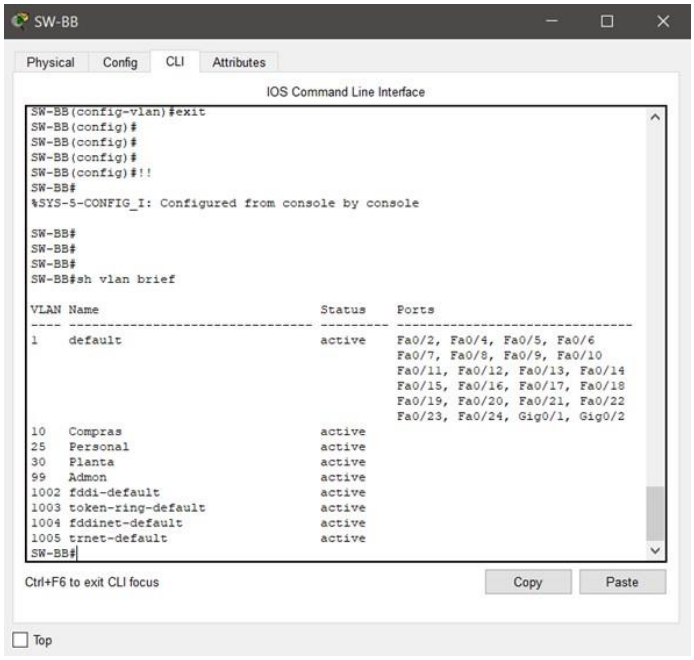


Fuente: Elaboración propia.

```
SW-BB#configure terminal
Enter configuration commands, one per line.   End with CNTL/Z.
SW-BB(config)#vlan 10
SW-BB(config-vlan)#name Compras
SW-BB(config-vlan)#vlan 25
SW-BB(config-vlan)#name Personal
SW-BB(config-vlan)#vlan 30
SW-BB(config-vlan)#name Planta
SW-BB(config-vlan)#vlan 99
SW-BB(config-vlan)#name Admon
SW-BB(config-vlan)#exit
```

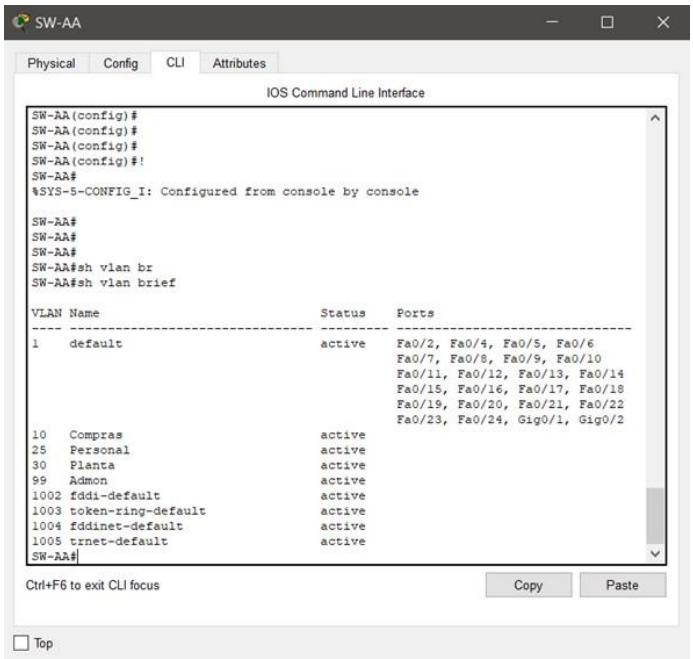
2. Verifique que las VLANs han sido agregadas correctamente.

Figura 17. VLAN creadas en el SW.



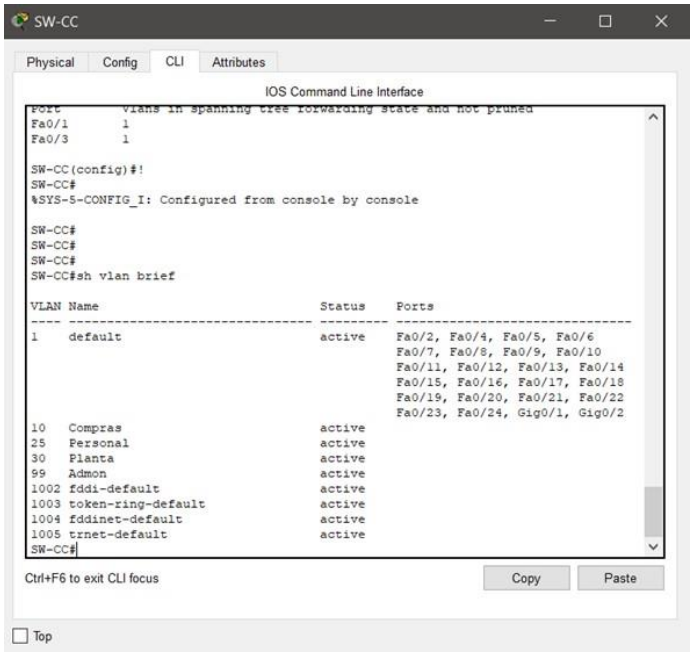
Fuente: Elaboración propia.

Figura 18. VLAN creadas por VTP en SW.



Fuente: Elaboración propia.

Figura 19. VLAN creadas por VTP en SW.



Fuente: Elaboración propia.

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

Tabla 2. Tabla de direcciones para PCS.

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.X /24
F0/15	VLAN 25	190.108.20.X /24
F0/20	VLAN 30	190.108.30.X /24

X = número de cada PC particular

Fuente: Prueba de habilidades CCNP 2020, Cisco Academy.

4. Configure el puerto F0/10 en modo de acceso para SW-AA, SW-BB y SW-CC y asígnelo a la VLAN 10.

```
SW-AA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-AA(config)#interface fastEthernet 0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#interface fastEthernet 0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#interface fastEthernet 0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
```

5. Repita el procedimiento para los puertos F0/15 y F0/20 en SW-AA, SW-BB y SW-CC.

```
SW-AA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-AA(config)#interface fastEthernet 0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#interface fastEthernet 0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#interface fastEthernet 0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30

SW-BB#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SW-BB(config)#interface fastEthernet 0/10
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#interface fastEthernet 0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#interface fastEthernet 0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30

SW-CC(config)#interface fastEthernet 0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#interface fastEthernet 0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#interface fastEthernet 0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30
```

Tabla 3. Tabla de direccionamiento de PC.

Pc	Vlan	Ip	Mascara
1	10	190.108.10.1	255.255.255.0
4	10	190.108.10.2	255.255.255.0
7	10	190.108.10.3	255.255.255.0
2	20	190.108.20.4	255.255.255.0
5	20	190.108.20.5	255.255.255.0
8	20	190.108.20.6	255.255.255.0
3	30	190.108.30.7	255.255.255.0
6	30	190.108.30.8	255.255.255.0
9	30	190.108.30.9	255.255.255.0

Fuente: Elaboración propia.

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 de los switch.

Equipo	Interfaz	Dirección IP	Máscara
SW-AA	VLAN 99	190.108.99.1	**255.255.255.**
SW-BB	VLAN 99	190.108.99.2	**255.255.255.**
SW-CC	**VLAN 99**	**190.108.99.3**	**255.255.255.**

Fuente: Elaboración propia.

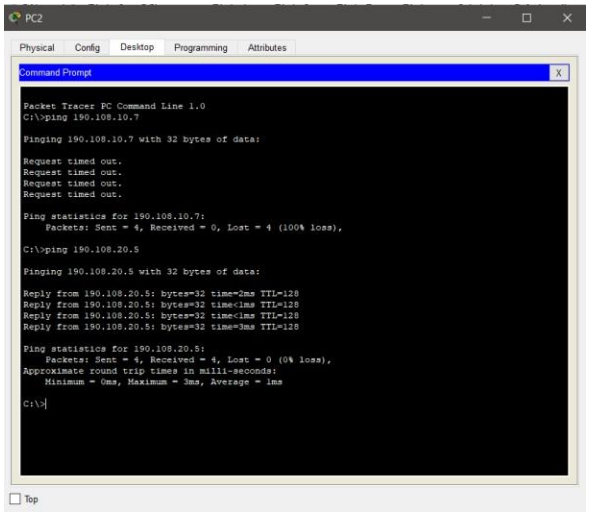
```
SW-AA(config)#interface vlan 99
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0

SW-BB(config)#interface vlan 99
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0

W-CC(config)#interface vlan 99
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0
```

E. Verificar la conectividad Extremo a Extremo

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

Ping de PC1 a PC4 y PC7

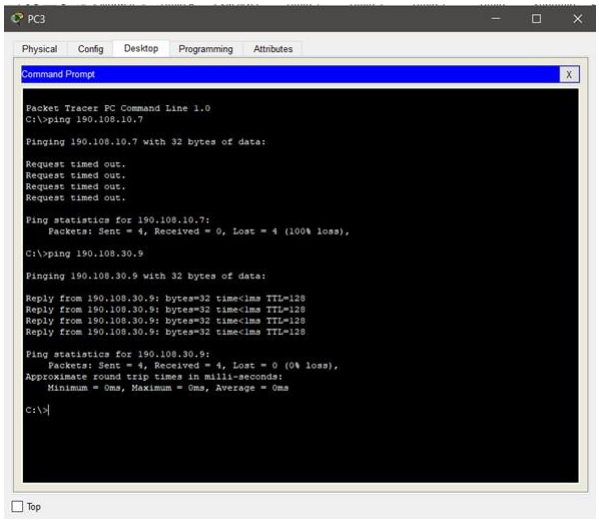
Figura 20. Prueba de conectividad.



Fuente: Elaboración propia.

Ping de PC6 a PC4 y PC9

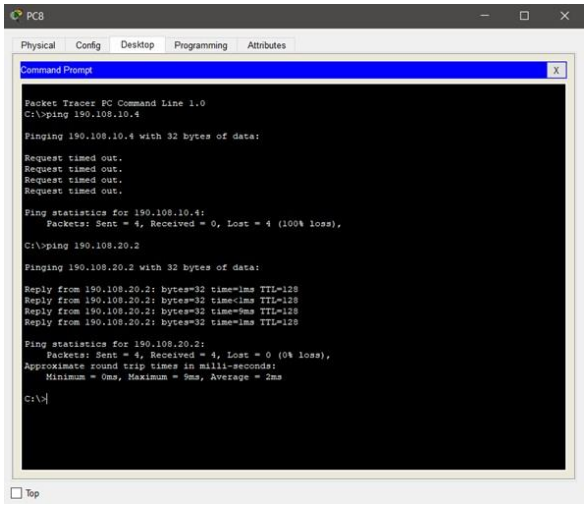
Figura 21. Prueba de conectividad.



Fuente: Elaboración propia.

Ping de PC8 a PC4 y PC2

Figura 22. Prueba de conectividad.

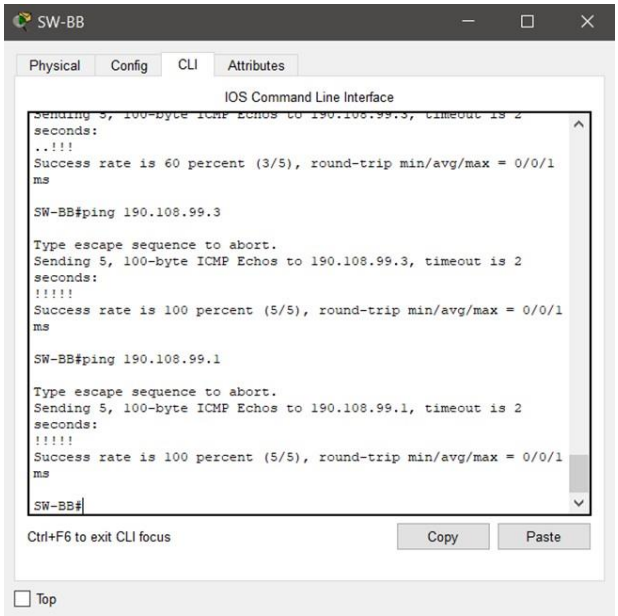


Fuente: Elaboración propia.

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

Ping de SW-BB a SW-AA Y SW-CC

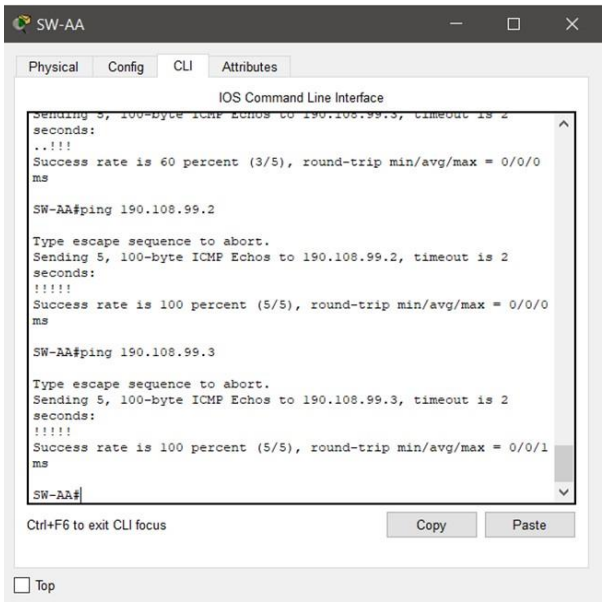
Figura 23. Prueba de conectividad.



Fuente: Elaboración propia.

Ping de SW-AA a SW-BB Y SW-CC

Figura 24. Prueba de Conectividad.

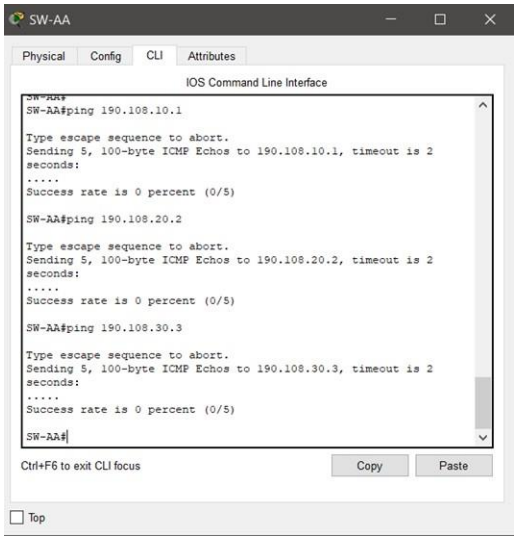


Fuente: Elaboración propia.

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

Ping de SW-AA a PC1-PC2 y PC3

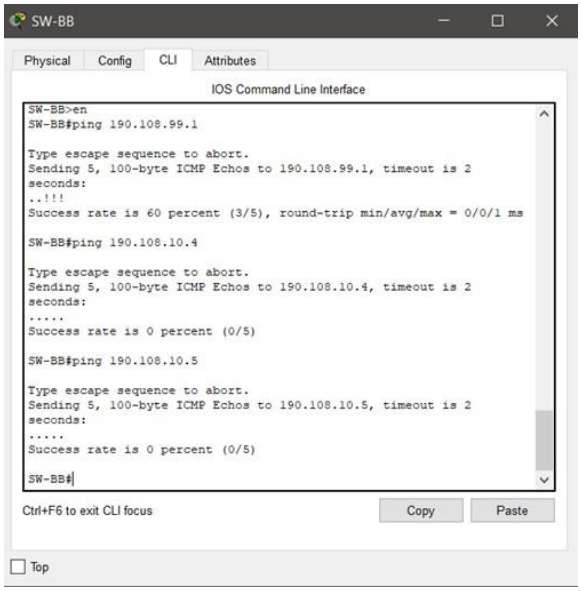
Figura 25. Prueba de conectividad.



Fuente: Elaboración propia.

Ping de SW-BB a PC4-PC5 y PC6

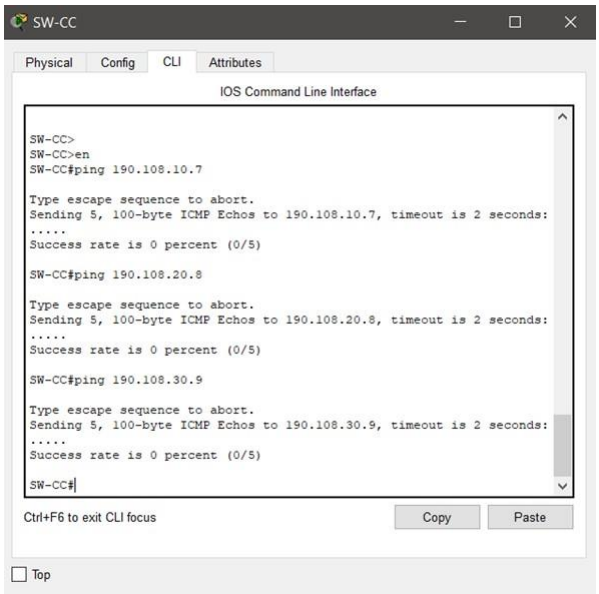
Figura 26. Prueba de conectividad.



Fuente: Elaboración propia.

Ping de SW-CC a PC7-PC8 y PC9

Figura 27.Prueba de conectividad.



Fuente: Elaboración propia.

Para los tres casos como se nombra anteriomente piden la misma justificación, y para los tres casos es la misma para este ejercicio no se configuran protocolos de enrutamiento, es la única forma que existe para comunicar segmentos de lan o vlan diferentes ya que la cabecera del

paquete no existe información de para comunicarse con la otra red, los comandos como vtp no están destinados para este fin, solo para enviar información en dispositivos de capa 2 y los comando de trunk permiten el trafico de varias vlan por el mismo camino pero no existe un protocolo que comunique redes diferentes.

CONCLUSIONES

A través del desarrollo de la prueba de habilidades practicas se desarrolla competencias, las cuales nos permitirán en el campo profesional implementar soluciones a este tipo de problemas en redes.

Se comprende el funcionamiento de un sistema de enrutamiento avanzado y su importancia a la hora de implementar en una red de datos.

Se observó por medio de práctica como el protocolo BGP (Protocolo de enlace de frontera), es un protocolo el cual se puede intercambiar información entre sistemas autónomos es decir una combinación entre protocolos de enrutamiento tanto internos como externo que en este caso es BGP.

OSPFv2 admite la autenticación de hash SHA usando cadenas de claves. Cisco se refiere a esto como la función de autenticación criptográfica OSPFv2. La función evita las actualizaciones de enrutamiento no autorizadas o no válidas en una red al autenticar los paquetes de protocolo OSPFv2 utilizando algoritmos HMAC-SHA.

BIBLIOGRAFIA

Casos Prácticos de BGP. (30 de Octubre de 2008). Obtenido de Cisco: https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html

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

Wallace, K. (2015). CISCO Press (Ed). CCNP Routing and Switching ROUTE 300-101 Official Cert Guide. Recuperado de https://1drv.ms/b/s!AgIGg5JUgUBthFx8WOxiq6LPJppl

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

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

García, V. S. (04 de Julio de 2017). *Diseño de Redes con BGP.* Obtenido de Universitat Politècnica de València: https://riunet.upv.es/bitstream/handle/10251/91691/S%C3%81NCHEZ%20-%20Dise%C3%B1o%20de%20redes%20con%20BGP.pdf?sequence=1