DIPLOMADO CCNP - CISCO PRUEBA DE HABILIDADES CCNP

FRANCISCO JAVIER VANEGAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA ESCUELA

DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA DE SISTEMAS MEDELLIN

2020

DIPLOMADO CCNP - CISCO PRUEBA DE HABILIDADES CCNP

FRANCISCO JAVIER VANEGAS

Diplomado de profundización CISCO

Director

Gerardo Granados Acuña

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA ESCUELA

DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

INGENIERÍA DE SISTEMAS MEDELLIN

2020

NOTA DE ACEPTACIÓN:

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Medellin, (mayo 10, 2020)

AGRADECIMIENTO

A Dios principalmente, por ser el gestor de mis logros, de levantarme cada vez que quería renunciar y por forjar el carácter perseverante que me define.

Gracias a mis padres por ser los principales promotores de mis sueños, gracias a ellos por cada día confiar y creer en mí y en mis expectativas, gracias a mi madre por estar dispuesta a acompañarme cada larga y agotadora noche de estudio, agotadoras noches en las que su compañía y la llegada de sus cafés era para mí como agua en el desierto; gracias a mi padre por siempre desear y anhelar siempre lo mejor para mi vida, gracias por cada consejo y por cada una de sus palabras que me guiaron durante mi vida.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Dirección IP: Una dirección en la red asignada a una in-terfaz de un nodo de la red y usada para identificar (localizar) en forma única el nodo dentro de la Internet. Dos versiones están actualmente implementadas: IPv4 e IPv6.

Dirección IPv4: Una dirección IP con base en el IPv4. Esas direcciones consisten en 32 bits (0 al 31) particionados en cuatro grupos de ocho bits cada uno (llamados octetos) y organizados en cinco clases (A a la E) con base en los valores de bits 0 al 3.

Dirección IPv6: Una dirección IP con base en IPv6. Una dirección IPv6 consiste en 128 bits y tiene 4000 millones X 4000 millones de veces el tamaño del espacio de dirección IPv4 (2128 vs. 232). A diferencia de las direcciones IPv4, las direcciones IPv6 usan dos puntos como delimitador (en vez de una notación “punto”), y ellas son escritas como ocho enteros de 16 bits expresados en forma hexadecimal.

Fibre Monomodo: Un tipo de cable de fibra óptica con un diámetro en su núcleo de entre 7 y 9 mm. En fibras de modo simple, sólo puede pasar un único rayo de luz, llamado rayo axial. Entonces, una onda de luz que entra a la fibra sale con muy poca distorsión, aún en muy largas distancias y muy altas velocidades de los datos.

LAN (del inglés Local Area Network, Red de Área Local): Una red local es la interconexión de varios computadores y periféricos. Su extensión esta limitada físicamente a un edificio o a un entorno de unos pocos kilómetros. Su aplicación más extendida es la interconexión de computadores personales y estaciones de trabajo en oficinas, fábricas, etc; para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen. El término red local incluye tanto el hardware como el software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

Network: Se le llama network o también red a aquellas series de ordenadores o dispositivos informáticos que se conectan por medio de cables, ondas, señales u otros mecanismos con el propósito de transmitir datos entre sí, además de recursos y servicios, con el fin de generar una experiencia de trabajo compartida, y ahorrar tiempo y dinero.

STP: (del inglés Spanning Tree Protocol) es un protocolo de red de capa 2 del modelo OSI (capa de enlace de datos). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice la eliminación de bucles.

Spoofing: es el uso de técnicas de suplantación de identidad generalmente para usos maliciosos. Se pueden clasificar sus ataques en función de la tecnología utilizada. Entre ellos el más extendido es el IP spoofing, aunque también existe el ARP spoofing, DNS spoofing, Web spoofing o email spoofing.

Switch: un switch o conmutador es un dispositivo de interconexión de redes informáticas. En computación y en informática de redes, un switch es el dispositivo analógico que permite interconectar redes operando en la capa 2 o de nivel de enlace de datos del modelo OSI u Open Systems Interconnection.

Trunking Protocol: es un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. El protocolo VTP nace como una herramienta de administración para redes de cierto tamaño, donde la gestión manual se vuelve inabordable.

RESUMEN

BGP es un protocolo tan complejo y robusto, que prácticamente permite que internet funcione, su énfasis en la seguridad y la escalabilidad lo hace esencial, en CCNP es abordado en profundidad junto a otras tecnologías de redes de datos y electrónicas como conmutación multicapa, redistribución de rutas y varios protocolos de enrutamiento. BGP es un protocolo de enrutamiento, en pocas palabras, dirige paquetes entre sistemas autónomos (AS): por ejemplo, redes administradas bajo tecnologías Cisco por una sola empresa o proveedor de servicios. El tráfico que se enruta dentro de una única red AS se conoce como BGP interno o **iBGP**. Más a menudo, BGP se utiliza para conectar un AS a otros sistemas autónomos, y luego se denomina BGP externo **eBGP**. La función principal de BGP es intercambiar información de capacidad de alcance de la red con otros sistemas BGP. El Protocolo de puerta de enlace de frontera construye un gráfico de sistemas autónomos basado en la información intercambiada entre routers BGP.

VTP son las siglas de VLAN Trunking Protocol, un protocolo de mensajes de nivel 2 usado en las tecnologías de swicthing para configurar y administrar VLANs en equipos Cisco. ... El protocolo VTP nace como una herramienta de administración para redes de cierto tamaño, donde la gestión manual se vuelve inabordable. Y se aborda en esta prueba para solucionar pruebas de conectividad entre los dispositivos mencionados

ASTRACT

BGP is such a complex and robust protocol that it practically allows the internet to work, its emphasis on security and scalability makes it essential, in CCNP it is addressed in depth alongside other electronics and data networking technologies such as multilayer switching, redistribution of routes and various routing protocols. BGP is a routing protocol, in a nutshell, it directs packets between autonomous systems (AS): for example, networks managed under Cisco technologies by a single company or service provider. Traffic that is routed within a single AS network is known as internal BGP or iBGP. Most often, BGP is used to connect an AS to other autonomous systems, and is then called an external BGP eBGP. The main function of BGP is to exchange network range capacity information with other BGP systems. The Border Gateway Protocol builds a graph of autonomous systems based on the information exchanged between BGP routers.

VTP stands for VLAN Trunking Protocol, a level 2 messaging protocol used in swicthing technologies to configure and manage VLANs on Cisco equipment. ... The VTP protocol was born as an administration tool for networks of a certain size, where manual management becomes unapproachable. And it is addressed in this test to solve connectivity tests between mentioned devices

INTRODUCCION

La siguiente actividad de habilidades prácticas es realizada con el fin de que el estudiante emplee herramientas de simulación y laboratorios de acceso remoto con el fin de establecer escenarios LAN/WAN que permitan realizar un análisis sobre el comportamiento de múltiples protocolos, evaluando el desempeño de los routers, mediante el uso de comandos de administración avanzados y bajo el uso de protocolos de vector distancia y estado enlace.

Durante el desarrollo de las actividades se trabajaron las temáticas de:

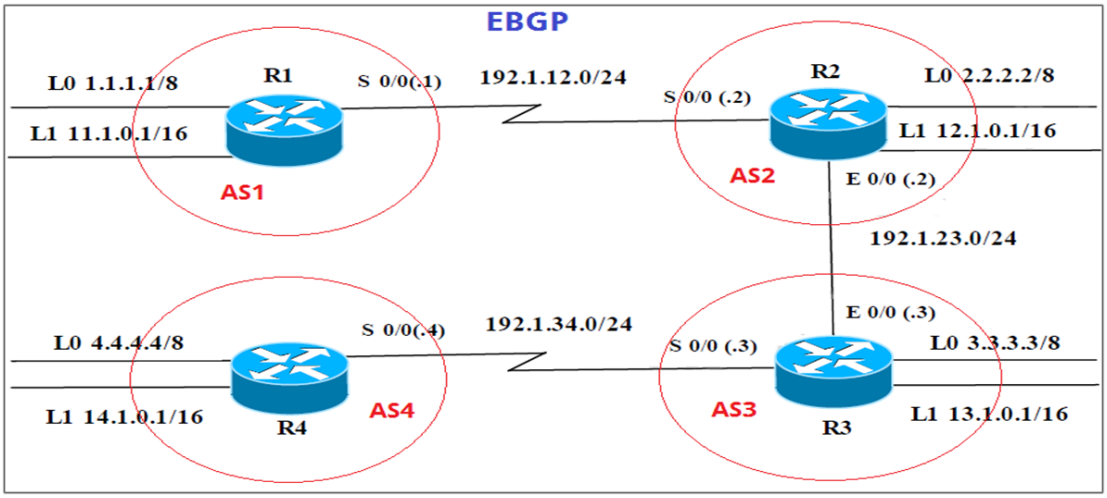
- Implementing a Border Gateway Protocol (BGP)
- Routers and Routing Protocol Hardening

Además, se utilizarán para las configuraciones el protocolo BGP, de Gateway exterior que se utiliza para el enrutamiento entre dominios de redes TCP/IP y sus dos casos de configuración, que son iBGP (dentro del sistema autónomo) y eBGP (entre sistemas autónomos).

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. R

```
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.

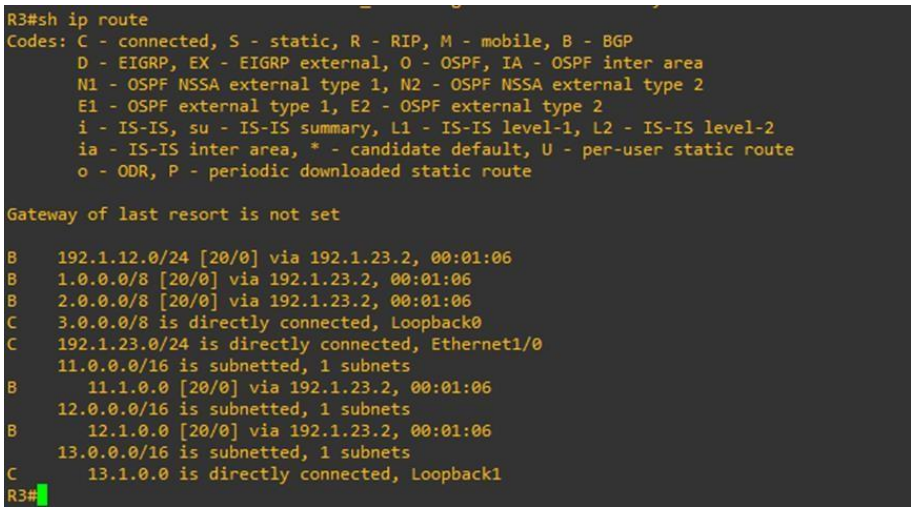
```
R2(config)#router bgp 2
R2(config-router)#network 192.1.23.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.23.3 remote-as 3
R2(config-router)#do wr
Building configuration...


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
```

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.



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.

```
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, 00:05:51
B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:05:51
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:05:51
C    3.0.0.0/8 is directly connected, Loopback0
S    4.0.0.0/8 [1/0] via 192.1.34.4
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, 00:05:51
C    192.1.34.0/24 is directly connected, Serial0/0
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.23.2, 00:05:52
     13.0.0.0/16 is subnetted, 1 subnets
C       13.1.0.0 is directly connected, Loopback1
R3#
```

Fuente: Elaboración propia.

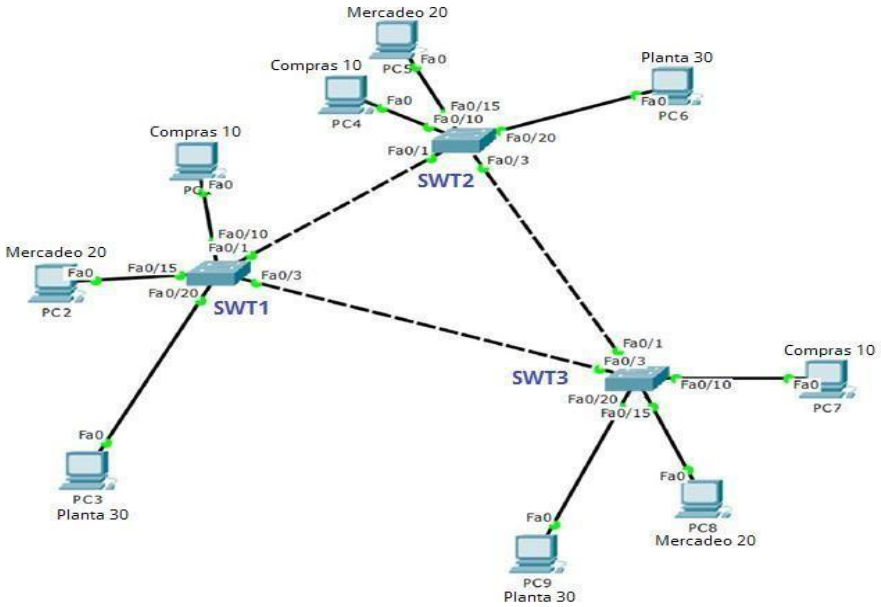
Figura 7. Rutas vecinas entre R3 y R4.

```
R4#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

B     192.1.12.0/24 [20/0] via 3.3.3.3, 00:46:50
B     1.0.0.0/8 [20/0] via 3.3.3.3, 00:46:50
B     2.0.0.0/8 [20/0] via 3.3.3.3, 00:46:50
S     3.0.0.0/8 [1/0] via 192.1.34.3
C     4.0.0.0/8 is directly connected, Loopback0
B     192.1.23.0/24 [20/0] via 3.3.3.3, 00:46:50
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 3.3.3.3, 00:46:50
C     192.1.34.0/24 is directly connected, Serial1/0
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 3.3.3.3, 00:46:50
      13.0.0.0/16 is subnetted, 1 subnets
B        13.1.0.0 [20/0] via 3.3.3.3, 00:46:50
      14.0.0.0/16 is subnetted, 1 subnets
C        14.1.0.0 is directly connected, Loopback1
```

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

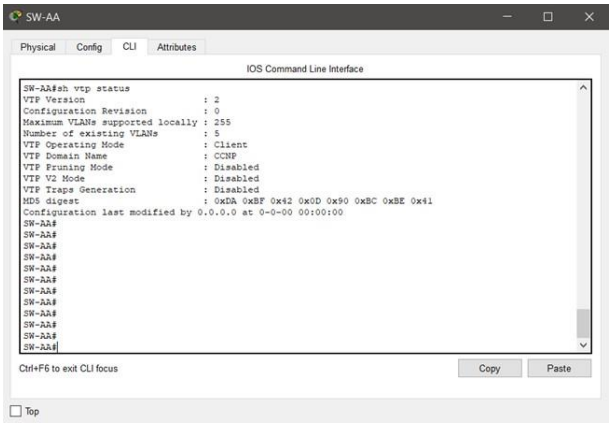
```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-BB
SW-BB(config)#vtp mode server
Device mode already VTP SERVER.
SW-BB(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-BB(config)#vtp password cisco
Setting device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

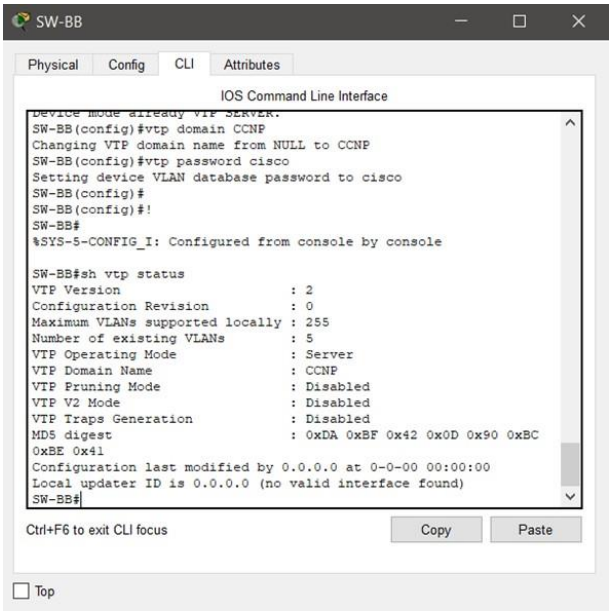
2. Verifique las configuraciones mediante el comando show vtp status.

Figura 9. Status del SW en VTP.



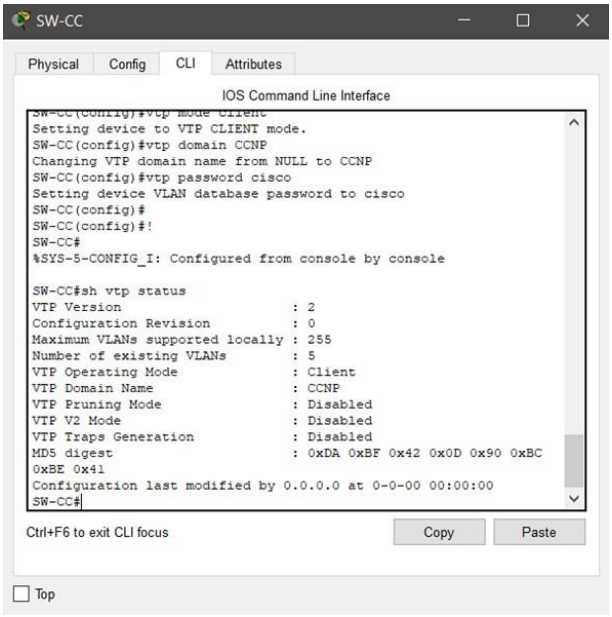
Fuente: Elaboración propia.

Figura 10. Status del SW en VTP.



Fuente: Elaboración propia. *Figura*

11. Status del SW en VTP.



Fuente: Elaboración propia.

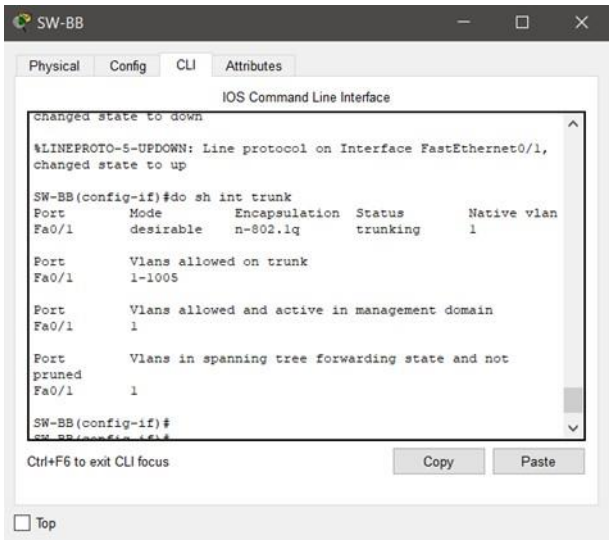
B. Configurar DTP (Dynamic Trunking Protocol)

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.



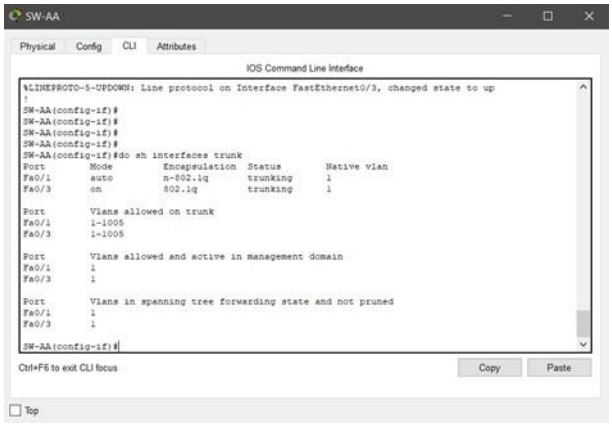
Fuente: Elaboración propia.

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.

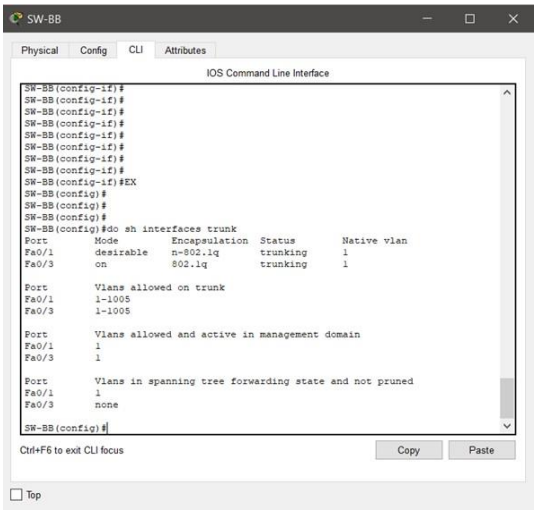


Fuente: Elaboración propia.

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

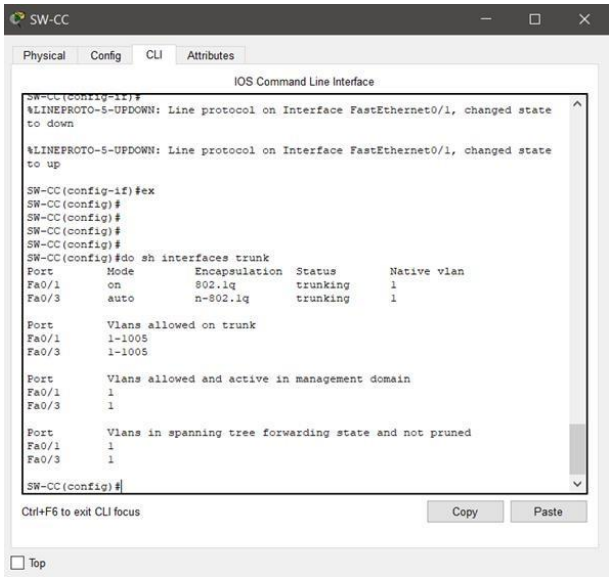
```
SW-CC(config)#interface fastEthernet 0/1
SW-CC(config-if)#switchport mode trunk

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.



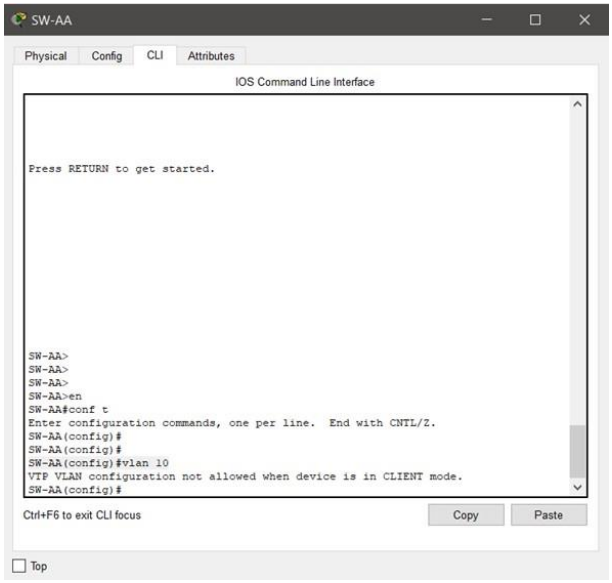
Fuente: Elaboración propia.

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.

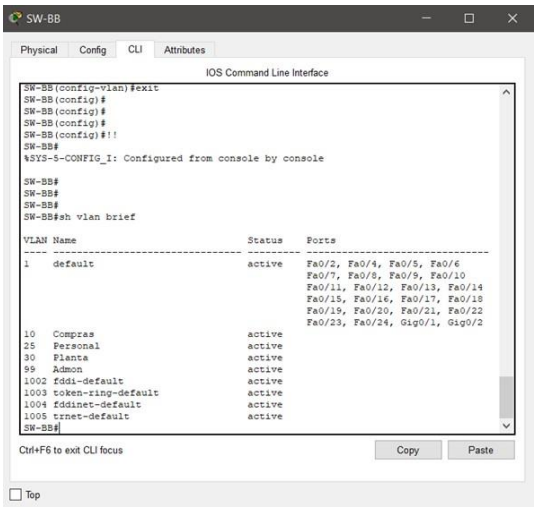


Fuente: Elaboración propia.

```
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
```

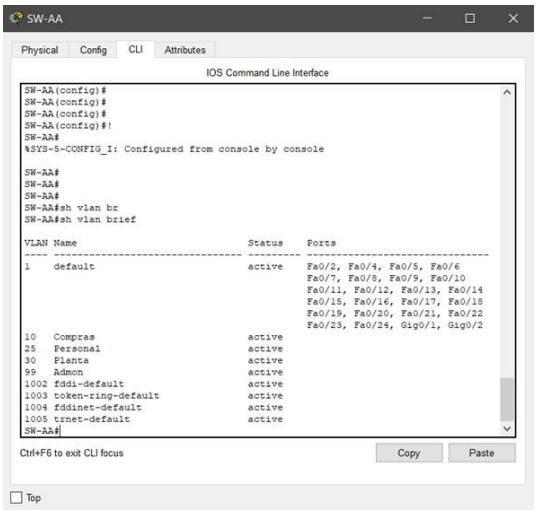
2. Verifique que las VLANs han sido agregadas correctamente.

Figura 17. VLAN creadas en el SW.



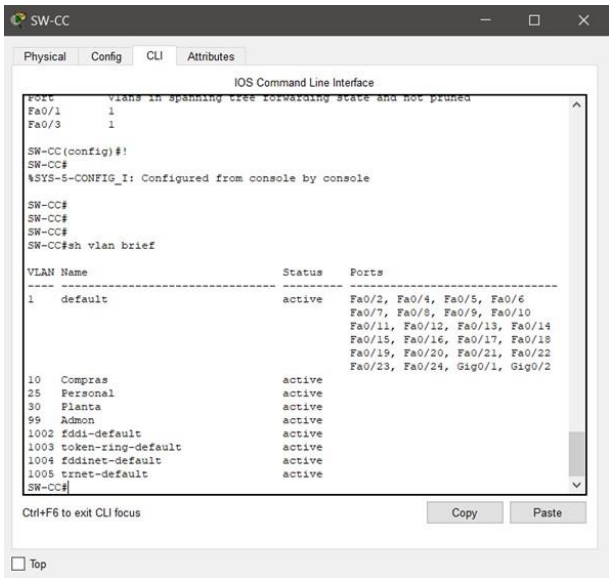
Fuente: Elaboración propia.

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

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.

Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

```
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
```

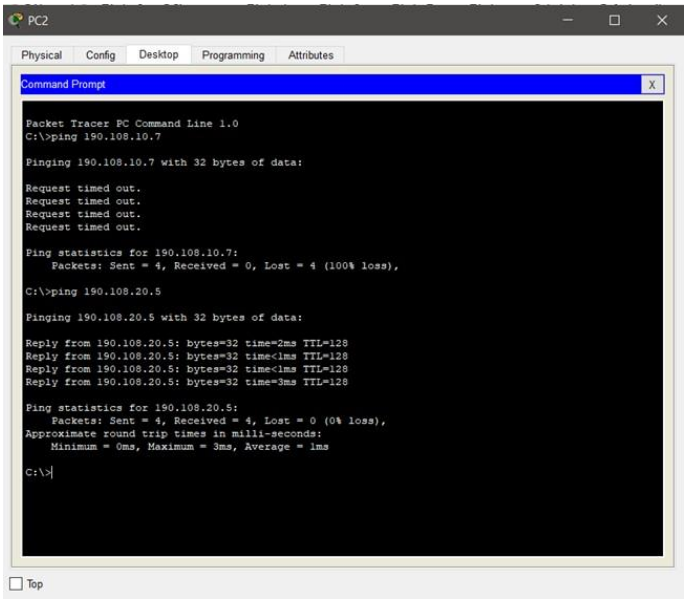
E. Verificar la conectividad Extremo a Extremo

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

Es un hecho que los paquetes enviados entre dispositivos de diferente subnet nunca van a funcionar si no hay protocolo y un dispositvo que enrute esos paquetes a otra red, es diferente en el caso de la misma vlan ya que a haber protocolos como trunking habilitados este permiten el paso de varias vlan sobre un mismo puerto de no se asi esos paquetes tampoco funcionarian

Ping de PC2 a PC5 y PC7

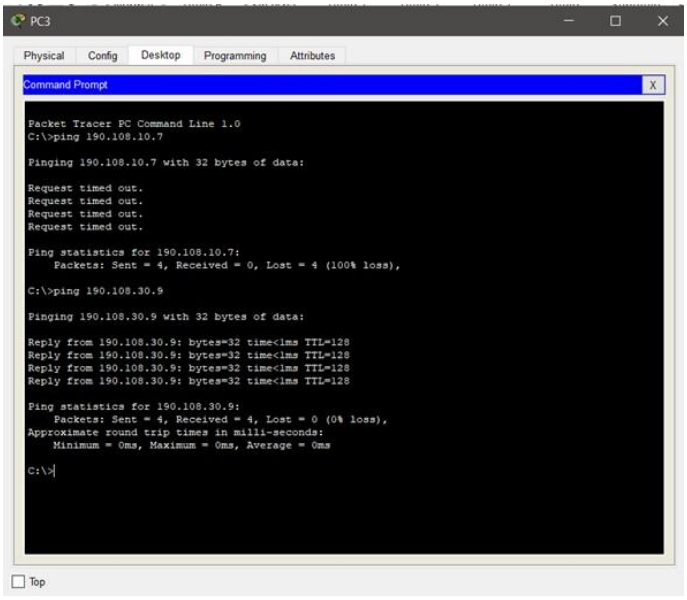
Figura 20. Prueba de conectividad.



Fuente: Elaboración propia.

Ping de PC3 a PC7 y PC9

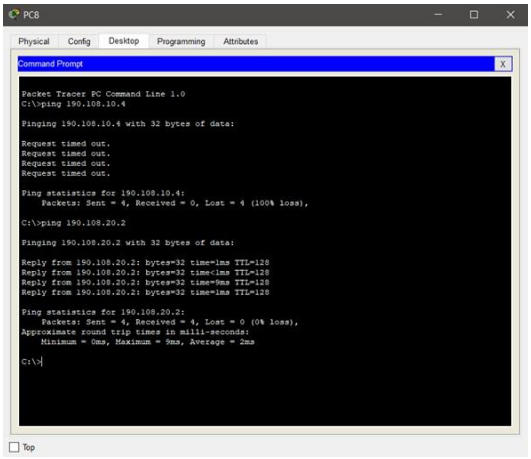
Figura 21. Prueba de conectividad.



Fuente: Elaboración propia.

Ping de PC8 a PC4 y PC2

Figura 22. Prueba de conectividad.



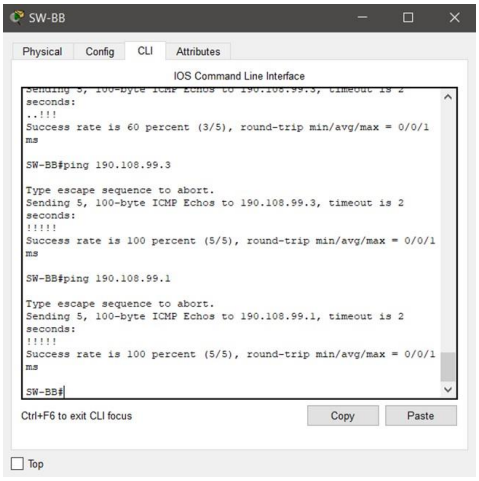
Fuente: Elaboración propia.

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

Para este caso si funcionaran ya que como mencione anteriormente al haber un protocolo de trunk va a permitir el paso de ellos y ya que se encuentran en la vlan administrativa los paquetes van a fluir sin problemas.

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

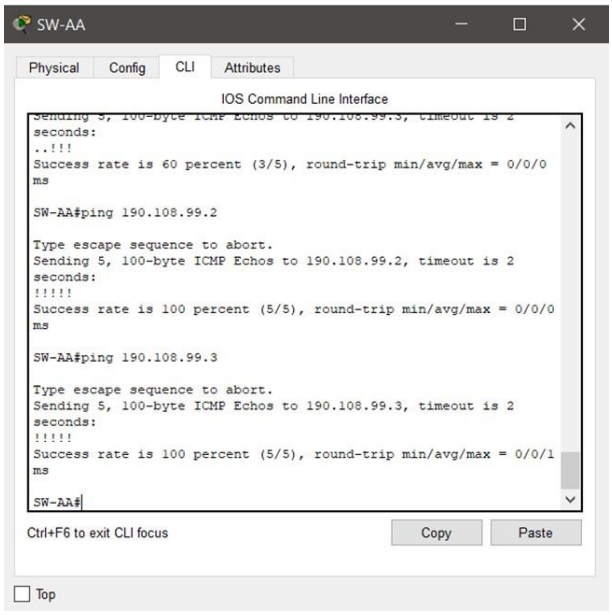
Figura 23. Prueba de conectividad.



Fuente: Elaboración propia.

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

Figura 24. Prueba de Conectividad.



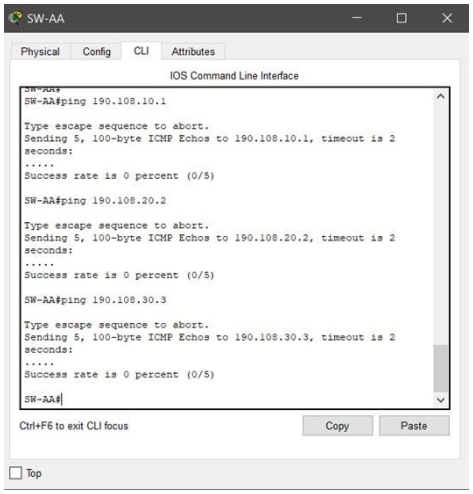
Fuente: Elaboración propia.

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

Es un hecho que los paquetes enviados entre dispositivos de diferente subnet nunca van a funcionar si no hay protocolo y un dispositvo que enrute esos paquetes a otra red, es diferente en el caso de la misma vlan ya que a haber protocolos como trunking habilitados este permiten el paso de varias vlan sobre un mismo puerto de no se asi esos paquetes tampoco funcionarian

Ping de SW-AA a PC1-PC2 y PC3

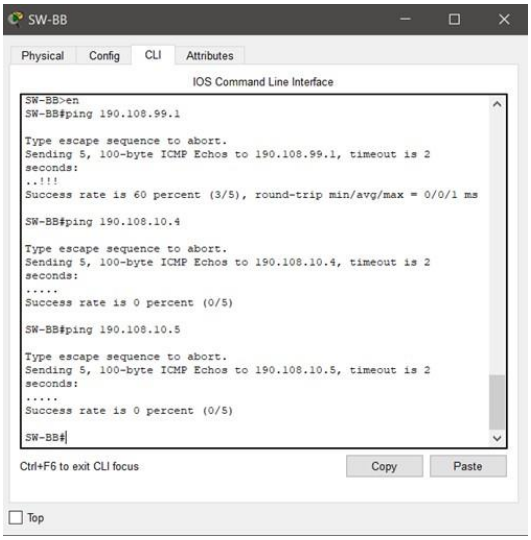
Figura 25. Prueba de conectividad.



Fuente: Elaboración propia.

Ping de SW-BB a PC4-PC5 y PC6

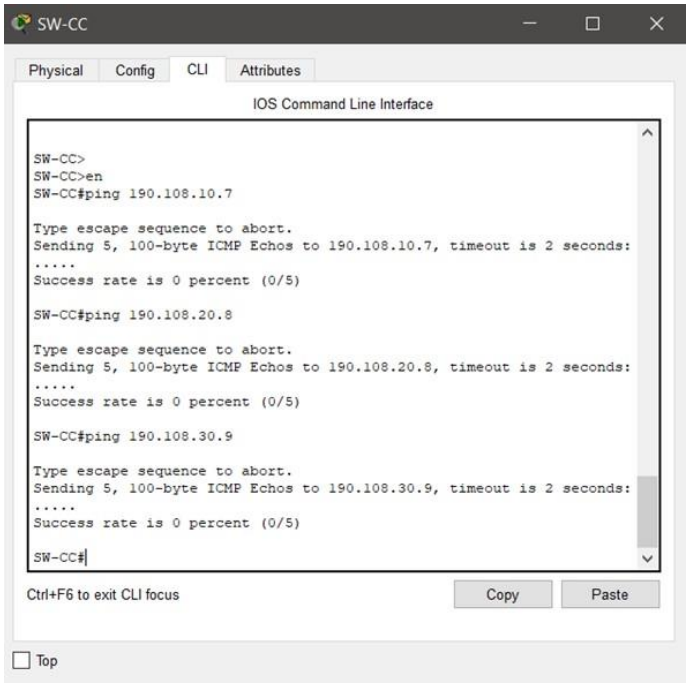
Figura 26. Prueba de conectividad.



Fuente: Elaboración propia.

Ping de SW-CC a PC7-PC8 y PC9

Figura 27.Prueba de conectividad.



Fuente: Elaboración propia.

CONCLUSIONES

Como resultado del desarrollo de los escenarios propuestos como parte de la evaluación final del curso, se logra contextualizar los conocimientos teóricos y las habilidades practicas construidas a través del curso mediante el uso de herramientas como GNS3, Packet Tracer y packet. En el contexto de la configuración de protocolos de enrutamiento dinámico, tales como BGP, sumado a la configuración de enrutamiento IPv4 en interfaces Seriales, FastEthernet y Loopback.

Tras completar las configuraciones requeridas para cada dispositivo, se logró contrastar los conocimientos adquiríos a lo largo del curso en referencia a los requerimientos y métricas que se tienen en cuenta para él envió de tráfico a través de OSPF, EIGRP y BGP, así como para la redistribución de rutas, creación de subredes, configuración del protocolo DTP (Dynamic Trunking Protocol) y del protocolo VTP. Estableciendo es este último caso, un dispositivo servidor a partir del cual se actualice la configuración de otros dispositivos, clientes, como parte del enrutamiento a través de redes de área local virtuales (Vlans).

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-NT1IlnW R0hoMxgBNv1CJ

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-NT1IlnW R0hoMxgBNv1CJ

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-NT1IlnW R0hoMxgBNv1CJ

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-NT1IlnW R0hoMxgBNv1CJ

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