

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JOSÉ ANDRÉS GÓMEZ MORANTES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA TELECOMUNICACIONES
BOGOTÁ DC
2020

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

JOSÉ ANDRÉS GÓMEZ MORANTES

Diplomado de opción de grado presentado para optar el título de INGENIERO EN
TELECOMUNICACIONES

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA TELECOMUNICACIONES
BOGOTÁ DC
2020

NOTA DE ACEPTACIÓN

Firma del presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá DC. 22 de mayo de 2020

AGRADECIMIENTOS

Agradezco a Dios por permitirme tener a mi familia, gracias a mis padres a mis hijos y a mi esposa por la comprensión y el cariño con el cual me apoyaron en el desarrollo de mi carrera profesional y en todos mis proyectos, gracias a mis compañeros en todos los trabajos en los cuales me desempeñe y me animaron y motivaron a seguir con mis proyectos, gracias a mis jefes y superiores que creyeron en mi y me exigieron para ser cada día más profesional, gracias a Dios por permitirme disfrutar de cada día de mi vida y darme salud y sabiduría.

El Camino no ha sido sencillo hasta ahora, pero gracias a sus aportes, a su amor a su inmensa bondad, lo imposible ha sido posible y la meta cada vez esta más cerca. Les agradezco y hago presente mi gran afecto hacia ustedes, mi valiosa familia y todo lo que yo emprenda es por mi y por mis hijos Felipe y Camilo.

CONTENIDO

LISTA DE TABLAS	6
LISTA DE FIGURAS	7
GLOSARIO	7
RESUMEN	9
ABSTRACT	9
INTRODUCCIÓN	10
DESARROLLO DEL ESCENARIO 1	11
DESARROLLO DEL ESCENARIO 2	19
CONCLUSIONES	32
BIBLIOGRAFÍA	33

LISTA DE TABLAS

	Pág
Tabla 1. Configuración de las interfaces de R1.....	11
Tabla 2. Configuración de las interfaces de R2.....	12
Tabla 3. Configuración de las interfaces de R3.....	12
Tabla 4. Configuración de las interfaces de R4.....	12
Tabla 5. Tabla de asociación de los puertos a las Vlan y las direcciones Ip.	24
Tabla 6. Configuración de las direcciones Ip de los Switches.	26

LISTA DE FIGURAS

	Pág
Figura 1. Topología del escenario 1.....	11
Figura 2. Topología del escenario 1 en GNS3.	12
Figura 3. Comando show ip route en R1.....	13
Figura 4. Comando show ip route en R2.....	15
Figura 5. Comando show ip route en R3.....	16
Figura 6. Comando show ip route en R3.....	17
Figura 7. Comando show ip route en R4.....	18
Figura 8. Ping desde R4 a R1 y R2.....	18
Figura 9. Topología escenario 2.	19
Figura 10. Diseño de la topología en Packet Tracer.	19
Figura 11. Comando show vtp status.....	20
Figura 12. Comando show vtp status.....	20
Figura 13. Comando show vtp status.....	21
Figura 14. Comando show interface trunk.....	21
Figura 15. Comando show interface trunk.....	21
Figura 16. Comando show interface trunk.....	22
Figura 17. Comando show vlan brief en SW-AA.	23
Figura 18.. Comando show vlan brief en SW-BB.	23
Figura 19. Comando show vlan brief en SW-BB.	23
Figura 20. Comando show vlan brief en SW-CC.....	24
Figura 21. Ping desde PC1.....	27
Figura 22. Ping desde PC2.....	28
Figura 23. Ping desde PC3.....	28
Figura 24. Ping desde SW-AA a SW-BB y SW-CC.....	29
Figura 25. Ping desde SW-BB a SW-AA y SW-CC.....	29
Figura 26. Ping desde SW-CC a SW-AA y SW-BB.....	29
Figura 27. Ping desde SW-CC a distintos PC.....	30
Figura 28. Ping desde SW-AA a distintos PC.	30

GLOSARIO

LAN

Una red de área local o LAN es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio..

VLAN

Una VLAN, acrónimo de virtual LAN, es un método para crear redes lógicas independientes dentro de una misma red física.

EIGRP

es un protocolo de encaminamiento de vector distancia, propiedad de Cisco Systems, que ofrece lo mejor de los algoritmos de Vector de distancias.

BGP

En telecomunicaciones, el protocolo de puerta de enlace de frontera o BGP es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos.

WLAN

Una red de área local inalámbrica, también conocida como WLAN, es un sistema de comunicación inalámbrico para minimizar las conexiones cableadas.

TERMINAL

Un(a) terminal o consola (hardware) es un dispositivo electrónico o electromecánico que se utiliza para interactuar con un(a) computador(a). Suele confundirse con su homónimo virtual, programado para emular las especificaciones de un terminal estándar

RESUMEN

La evaluación de habilidades prácticas es parte fundamental en el diplomado de profundización de CISCO – CCNP lo cual permite ampliar los conocimientos en las áreas de redes, telecomunicaciones y electrónica.

En este diplomado adquirimos los conocimientos necesarios para el diseño de redes LAN y WAN escalables con el fin de optimizar el rendimiento, el enrutamiento y la seguridad adoptando de manera adecuada el uso de tecnologías y protocolos de conmutación mejorados tales como WLAN, VLAN, BGP y EIGRP.

En la terminal de comandos de Cisco IOS se pudo implementar topologías de red correctamente y la comunicación entre los dispositivos en los dos escenarios propuestos para esta evaluación.

ABSTRACT

The evaluation of practical skills is a fundamental part of the CISCO - CCNP in-depth diploma, which allows expanding knowledge in the areas of networks, telecommunications and electronics.

In this course, we gain the knowledge to design scalable LAN and WAN networks to optimize performance, routing, and security by appropriately adopting the use of enhanced switching protocols and technologies such as WLAN, VLAN, BGP, and EIGRP.

In the Cisco IOS command terminal, network topologies and communication between devices were correctly implemented in the two scenarios proposed for this evaluation.

INTRODUCCIÓN

En el desarrollo del diplomado de profundización como opción de grado se adquirieron conocimientos y se formaron las capacidades necesarias para un posible futuro profesional de los estudiantes.

El principal objetivo de esta prueba de habilidades es alcanzar la máxima capacidad de análisis y comprensión del estudiante para desarrollar a satisfacción los dos escenarios propuestos

Estos se enfocan en llevar la parte práctica de todo el conocimiento teórico que se fue adquiriendo durante el diplomado, para el desarrollo de los escenarios se utilizaron herramientas como Packet Tracer y GNS3 para realizar las simulaciones y las configuraciones de los dos escenarios y poder ver el funcionamiento según las indicaciones dadas.

DESARROLLO DEL ESCENARIO 1

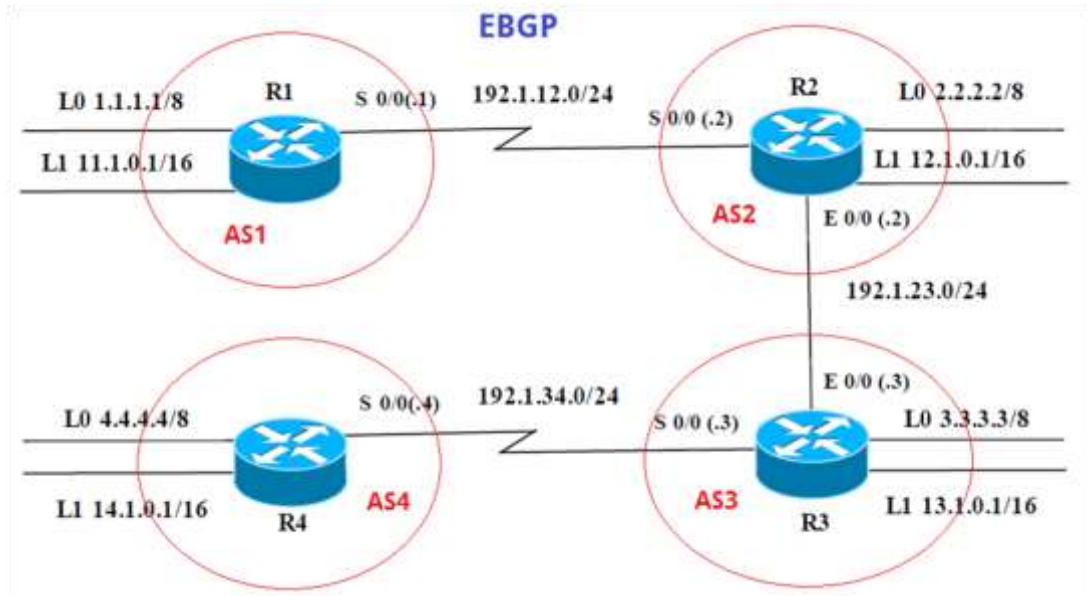


Figura 1. Topología del escenario 1.

	Interfaz	Dirección IP	Máscara
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

Tabla 1. Configuración de las interfaces de R1.

	Interfaz	Dirección IP	Máscara
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	192.1.23.2	255.255.255.0

Tabla 2. Configuración de las interfaces de R2.

	Interfaz	Dirección IP	Máscara
R3	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

Tabla 3. Configuración de las interfaces de R3.

	Interfaz	Dirección IP	Máscara
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

Tabla 4. Configuración de las interfaces de R4.

Diseño de la topología en GNS3

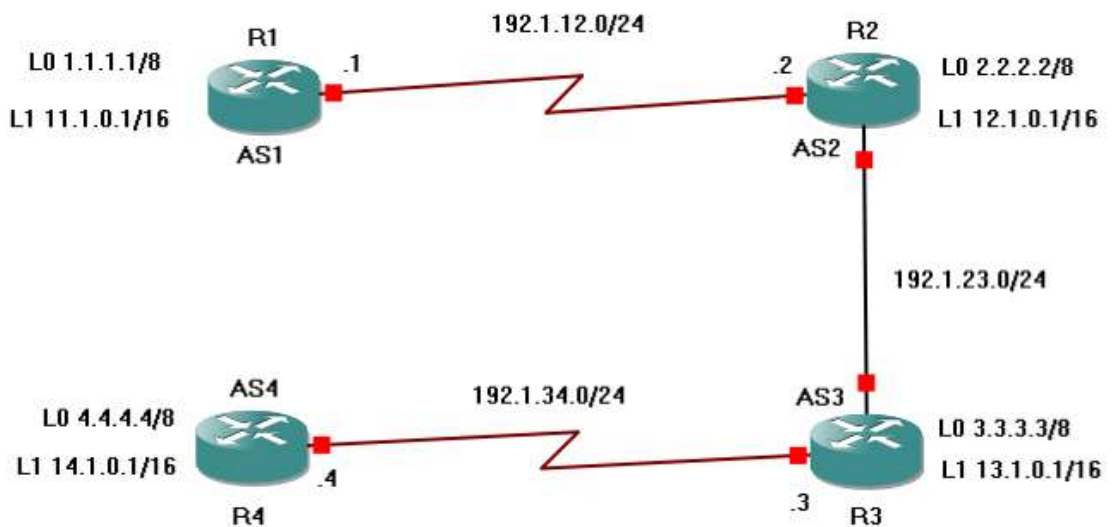
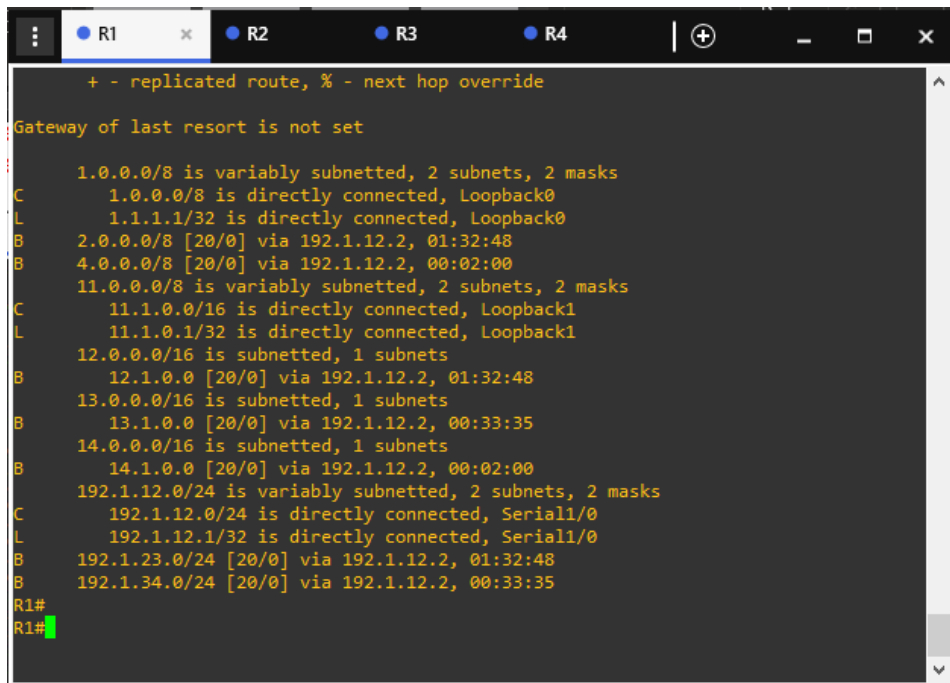


Figura 2. Topología del escenario 1 en GNS3.

1. Configure 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#configure terminal
R1(config)#interface loopback 0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config)#interface loopback 1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config)#interface s1/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#router bgp 1
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router)#network 1.0.0.0 mask 255.0.0.0
R1(config-router)#network 192.1.12.0 mask 255.255.255.0
R1(config-router)#neighbor 192.1.12.2 remote-as 2
```



```
+ - replicated route, % - next hop override
Gateway of last resort is not set

  1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    1.0.0.0/8 is directly connected, Loopback0
L    1.1.1.1/32 is directly connected, Loopback0
B    2.0.0.0/8 [20/0] via 192.1.12.2, 01:32:48
B    4.0.0.0/8 [20/0] via 192.1.12.2, 00:02:00
  11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    11.1.0.0/16 is directly connected, Loopback1
L    11.1.0.1/32 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, 01:32:48
  13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0 [20/0] via 192.1.12.2, 00:33:35
  14.0.0.0/16 is subnetted, 1 subnets
B    14.1.0.0 [20/0] via 192.1.12.2, 00:02:00
  192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.12.0/24 is directly connected, Serial1/0
L    192.1.12.1/32 is directly connected, Serial1/0
B    192.1.23.0/24 [20/0] via 192.1.12.2, 01:32:48
B    192.1.34.0/24 [20/0] via 192.1.12.2, 00:33:35
R1#
R1#
```

Figura 3. Comando *show ip route* en R1.

```

R2#configure terminal
R2(config)# interface loopback 0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config)# interface loopback 1
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config)#interface s1/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shut
R2(config)#interface f0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shut
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
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
R2(config-router)#network 192.1.12.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.12.1 remote-as 1
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)#exit

```

```

Gateway of last resort is not set

R  1.0.0.0/8 [20/0] via 192.1.12.1, 01:32:39
C  2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    2.0.0.0/8 is directly connected, Loopback0
L    2.2.2.2/32 is directly connected, Loopback0
B  4.0.0.0/8 [20/0] via 192.1.23.3, 00:01:51
C  11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 192.1.12.1, 01:32:39
C  12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    12.1.0.0/16 is directly connected, Loopback1
L    12.1.0.1/32 is directly connected, Loopback1
C  13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0 [20/0] via 192.1.23.3, 00:33:26
C  14.0.0.0/16 is subnetted, 1 subnets
B    14.1.0.0 [20/0] via 192.1.23.3, 00:01:51
B  192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.12.0/24 is directly connected, Serial1/0
L    192.1.12.2/32 is directly connected, Serial1/0
B  192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, FastEthernet0/0
L    192.1.23.2/32 is directly connected, FastEthernet0/0
B  192.1.34.0/24 [20/0] via 192.1.23.3, 00:33:26
R2#
R2#

```

Figura 4. Comando show ip route en R2.

2. Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en AS2 y R3 debería estar en AS3. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 44.44.44.44. Presente el paso a con los comandos utilizados y la salida del comando *show ip route*.

```
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)#exit
```

```
R3#configure terminal
R3(config)# interface loopback 0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config)# interface loopback 1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config)#interface s1/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config)#interface f0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#network 192.1.23.0 mask 255.255.255.0
R3(config-router)#network 3.0.0.0 mask 255.0.0.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3(config-router)#neighbor 192.1.23.2 remote-as 2
```

```

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:33:14
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:33:14
    3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    3.0.0.0/8 is directly connected, Loopback0
L    3.3.3.3/32 is directly connected, Loopback0
S    4.0.0.0/8 [1/0] via 192.1.34.4
    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 192.1.23.2, 00:33:14
    12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 192.1.23.2, 00:33:14
    13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    13.1.0.0/16 is directly connected, Loopback1
L    13.1.0.1/32 is directly connected, Loopback1
    14.0.0.0/16 is subnetted, 1 subnets
B    14.1.0.0 [20/0] via 192.1.34.4, 00:01:39
B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:33:14
    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, FastEthernet0/0
L    192.1.23.3/32 is directly connected, FastEthernet0/0
    192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial1/0
L    192.1.34.3/32 is directly connected, Serial1/0
R3#

```

Figura 5. Comando show ip route en R3.

- 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)#network 192.1.34.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#exit
R3(config)#ip route 4.0.0.0 255.0.0.0 192.1.34.4
R3(config)#router bgp 3
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
R3(config-router)#exit

```

```

R4#configure terminal

```



```

R4(config)# interface loopback 0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config)# interface loopback 1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config)#interface s1/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shut
R4(config-if)#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)#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)#neighbor 3.3.3.3 remote-as 3
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)#exit

```

```

R3# show ip route
B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:14:10
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:14:10
C    3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
L    3.0.0.0/8 is directly connected, Loopback0
L    3.3.3.3/32 is directly connected, Loopback0
S    4.0.0.0/8 [1/0] via 192.1.34.4
L    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 192.1.23.2, 00:14:10
L    12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 192.1.23.2, 00:14:10
C    13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
L    13.1.0.0/16 is directly connected, Loopback1
L    13.1.0.1/32 is directly connected, Loopback1
L    14.0.0.0/16 is subnetted, 1 subnets
B    14.1.0.0 [20/0] via 4.4.4.4, 00:01:34
B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:14:10
C    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
L    192.1.23.0/24 is directly connected, FastEthernet0/0
L    192.1.23.3/32 is directly connected, FastEthernet0/0
C    192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
L    192.1.34.0/24 is directly connected, Serial1/0
L    192.1.34.3/32 is directly connected, Serial1/0
R3#

```

Figura 6. Comando show ip route en R3.

```
Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 3.3.3.3, 00:02:20
B    2.0.0.0/8 [20/0] via 3.3.3.3, 00:02:20
S    3.0.0.0/8 [1/0] via 192.1.34.3
    4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    4.0.0.0/8 is directly connected, Loopback0
L    4.4.4.4/32 is directly connected, Loopback0
    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 3.3.3.3, 00:02:20
    12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 3.3.3.3, 00:02:20
    13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0 [20/0] via 3.3.3.3, 00:02:20
    14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    14.1.0.0/16 is directly connected, Loopback1
L    14.1.0.1/32 is directly connected, Loopback1
B    192.1.12.0/24 [20/0] via 3.3.3.3, 00:02:20
B    192.1.23.0/24 [20/0] via 3.3.3.3, 00:02:20
    192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, Serial1/0
L    192.1.34.4/32 is directly connected, Serial1/0
R4#
```

Figura 7. Comando show ip route en R4.

Las tablas de enrutamiento anexadas se muestran como evidencia que ya se encuentran actualizadas, primero se configuraron los Routers y después se comenzó a montar el documento con las evidencias.

En el numero 3 demuestro el cambio de la tabla de enrutamiento en el Router 3 por la modificación de las relaciones con los Routers vecinos con base a las direcciones de Loopback 0, se realizará un ping de extremo a extremo para verificar la conectividad.

```
R4#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 = 80/100/116 ms
R4#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 = 40/58/96 ms
R4#ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 108/132/188 ms
R4#ping 3.3.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/20/32 ms
R4#ping 11.1.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.1.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/104/160 ms
R4#
```

Figura 8. Ping desde R4 a R1 y R2.

DESARROLLO DEL ESCENARIO 2

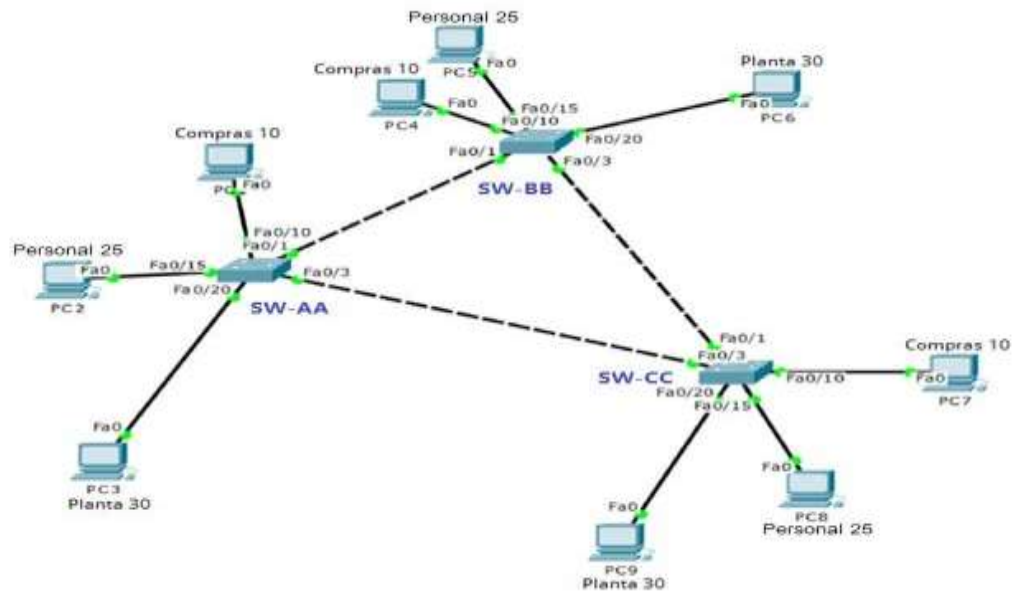


Figura 9. Topología escenario 2.

Diseño

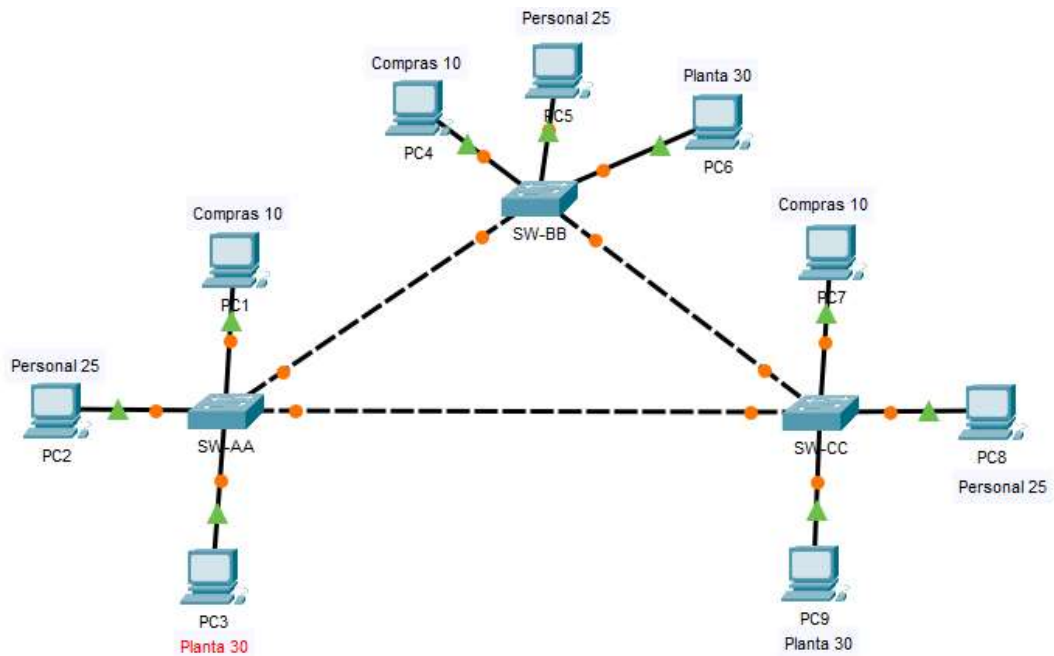


Figura 10. Diseño de la topología en Packet Tracer.

A. Configurar VTP

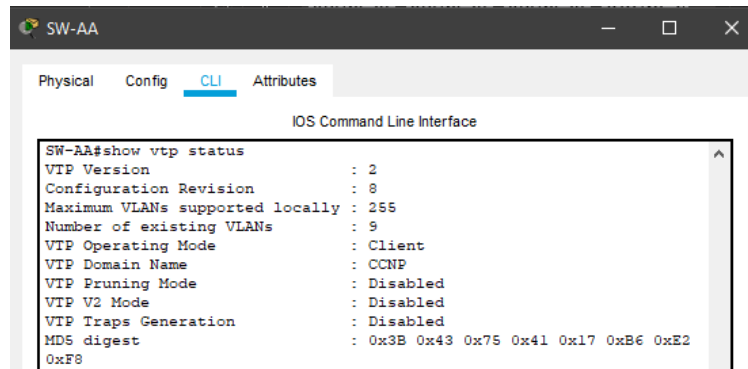
1. Todos los switches se configurarán para usar VTP para las actualizaciones de VLAN. El switch SW-BB se configurará como el servidor. Los switches SW-AA y SW-CC se configurarán como clientes. Los switches estarán en el dominio VTP llamado CCNP y usando la contraseña cisco.

```
SW-AA(config)#vtp mode client
SW-AA(config)#vtp domain CCNP
SW-AA(config)#vtp password cisco
```

```
SW-BB(config)#vtp mode server
SW-BB(config)#vtp domain CCNP
SW-BB(config)#vtp password cisco
```

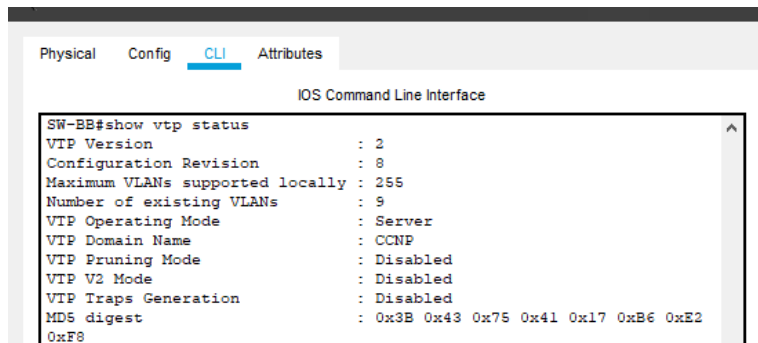
```
SW-CC(config)#vtp mode client
SW-CC(config)#vtp domain CCNP
SW-CC(config)#vtp password cisco
```

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

A screenshot of the SW-AA switch CLI interface. The window title is 'SW-AA'. The 'CLI' tab is selected. The command 'SW-AA#show vtp status' has been entered, and the output is displayed in a scrollable window. The output shows VTP Version 2, Configuration Revision 8, Maximum VLANs supported locally 255, Number of existing VLANs 9, VTP Operating Mode Client, VTP Domain Name CCNP, VTP Pruning Mode Disabled, VTP V2 Mode Disabled, VTP Traps Generation Disabled, and MDS digest 0x3B 0x43 0x75 0x41 0x17 0xB6 0xE2 0xF8.

```
SW-AA#show vtp status
VTP Version          : 2
Configuration Revision : 8
Maximum VLANs supported locally : 255
Number of existing VLANs : 9
VTP Operating Mode   : Client
VTP Domain Name      : CCNP
VTP Pruning Mode     : Disabled
VTP V2 Mode          : Disabled
VTP Traps Generation : Disabled
MDS digest           : 0x3B 0x43 0x75 0x41 0x17 0xB6 0xE2
0xF8
```

Figura 11. Comando show vtp status.

A screenshot of the SW-BB switch CLI interface. The window title is 'SW-BB'. The 'CLI' tab is selected. The command 'SW-BB#show vtp status' has been entered, and the output is displayed in a scrollable window. The output shows VTP Version 2, Configuration Revision 8, Maximum VLANs supported locally 255, Number of existing VLANs 9, VTP Operating Mode Server, VTP Domain Name CCNP, VTP Pruning Mode Disabled, VTP V2 Mode Disabled, VTP Traps Generation Disabled, and MDS digest 0x3B 0x43 0x75 0x41 0x17 0xB6 0xE2 0xF8.

```
SW-BB#show vtp status
VTP Version          : 2
Configuration Revision : 8
Maximum VLANs supported locally : 255
Number of existing VLANs : 9
VTP Operating Mode   : Server
VTP Domain Name      : CCNP
VTP Pruning Mode     : Disabled
VTP V2 Mode          : Disabled
VTP Traps Generation : Disabled
MDS digest           : 0x3B 0x43 0x75 0x41 0x17 0xB6 0xE2
0xF8
```

Figura 12. Comando show vtp status.

```
SW-CC#show vtp status
VTP Version          : 2
Configuration Revision : 8
Maximum VLANs supported locally : 255
Number of existing VLANs : 9
VTP Operating Mode   : Client
VTP Domain Name     : CCNP
VTP Pruning Mode    : Disabled
VTP V2 Mode         : Disabled
VTP Traps Generation : Disabled
MD5 digest          : 0x3B 0x43 0x75 0x41 0x17 0xB6 0xE2
0xF8
```

Figura 13. Comando show vtp status.

B. Configurar DTP (Dynamic Trunking Protocol)

1. Se configuro un enlace troncal 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#configure terminal
SW-BB(config)#interface f0/1
SW-BB(config-if)#switch mode dynamic desirable
SW-BB(config-if)#exit
```

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

```
SW-AA#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     auto      n-802.1q       trunking    1
```

Figura 14. Comando show interface trunk.

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

Figura 15. Comando show interface trunk.

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

```
SW-AA#configure terminal
SW-AA(config)#interface f0/3
SW-AA(config-if)#switchport mode trunk
```

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

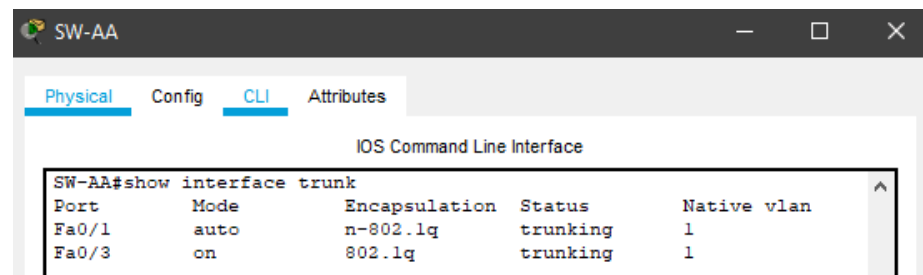


Figura 16. Comando `show interface trunk`.

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

```
SW-BB#configure terminal
SW-BB(config)#interface f0/3
SW-BB(config-if)#switchport mode trunk
```

C. Agregar VLANs y asignar puertos.

- En SW-AA agregue la VLAN 10. En SW-BB agregue las VLANs Compras (10), Personal (25), Planta (30) y Admon (99).

```
SW-AA#configure terminal
SW-AA(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
```

```
SW-BB#configure terminal
SW-BB(config)#vlan 10
SW-BB(config-vlan)#name Compras
SW-BB(config-vlan)#exit
SW-BB(config)#vlan 25
SW-BB(config-vlan)#name Personal
```

```

SW-BB(config-vlan)#exit
SW-BB(config)#vlan 30
SW-BB(config-vlan)#name Planta
SW-BB(config-vlan)#exit
SW-BB(config)#vlan 99
SW-BB(config-vlan)#name Admon
SW-BB(config-vlan)#exit

```

2. Se verifico que las VLANs han sido agregadas correctamente.

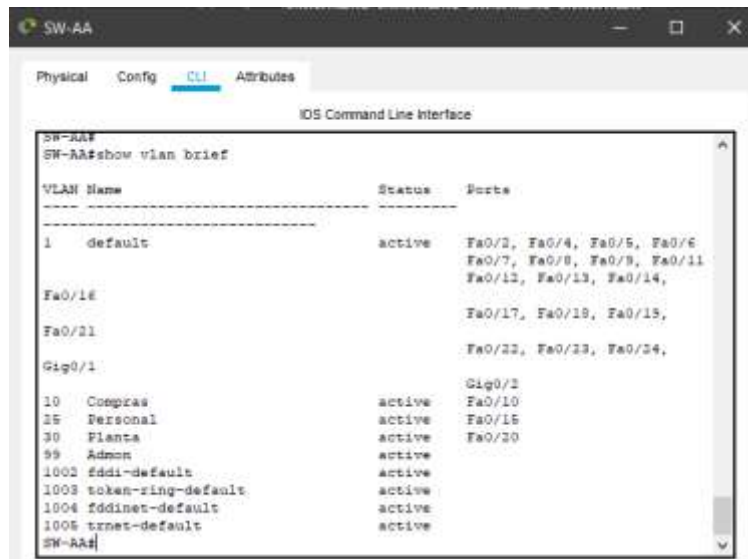


Figura 17. Comando show vlan brief en SW-AA.

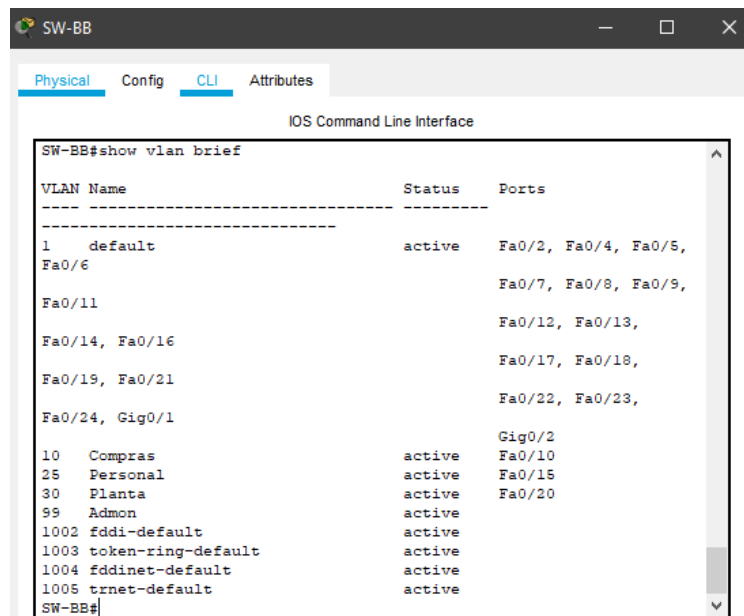


Figura 18.. Comando show vlan brief en SW-BB.

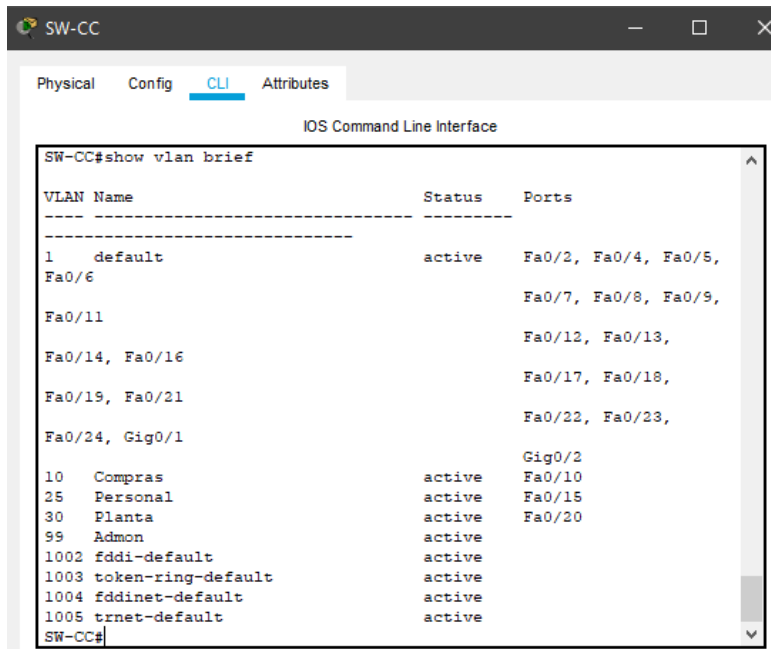


Figura 20. Comando show vlan brief en SW-CC.

- Se asociaron los puertos a las VLAN y se configuraron las direcciones IP de acuerdo con la siguiente tabla.

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

Tabla 5. Tabla de asociación de los puertos a las Vlan y las direcciones Ip. .

Se asigno una ip a cada uno de los computadores por medio de la tabla.

Antes de asignar las ip a los Pc se configuraron las direcciones Ip para asociar cada una de las interfaces.

```

SW-AA(config)#interface vlan 10
SW-AA(config-if)#ip address 190.108.10.1 255.255.255.0
SW-AA(config-if)#interface vlan 25
SW-AA(config-if)#ip address 190.108.20.1 255.255.255.0
SW-AA(config-if)#interface vlan 30
SW-AA(config-if)#ip address 190.108.30.1 255.255.255.0

```



```
SW-BB(config)#interface vlan 10
SW-BB(config-if)#ip address 190.108.10.2 255.255.255.0
SW-BB(config-if)#interface vlan 25
SW-BB(config-if)#ip address 190.108.20.2 255.255.255.0
SW-BB(config-if)#interface vlan 30
SW-BB(config-if)#ip address 190.108.30.2 255.255.255.0
```

```
SW-CC(config)#interface vlan 10
SW-CC(config-if)#ip address 190.108.10.3 255.255.255.0
SW-CC(config-if)#interface vlan 25
SW-CC(config-if)#ip address 190.108.20.3 255.255.255.0
SW-CC(config-if)#interface vlan 30
SW-CC(config-if)#ip address 190.108.30.3 255.255.255.0
```

9. Se configuro el puerto F0/10 en modo de acceso para SW-AA, SW-BB y SW-CC y asígnelo a la VLAN 10.
10. Se repite el procedimiento para los puertos F0/15 y F0/20 en SW-AA, SW-BB y SW-CC. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

```
SW-AA#configure terminal
SW-AA(config)#interface f0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#exit
SW-AA(config)#interface f0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#exit
SW-AA(config)#interface f0/20
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
```

```
SW-BB#configure terminal
SW-BB(config)#interface f0/10
SW-BB(config-if)#switchport mode access
```

```

SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#exit
SW-BB(config)#interface f0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#exit
SW-BB(config)#interface f0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30

```

```

SW-CC#configure terminal
SW-CC(config)#interface f0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#exit
SW-CC(config)#interface f0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#exit
SW-CC(config)#interface f0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30

```

D. Configurar las direcciones IP en los Switches.

14. En cada uno de los Switches se asignó una dirección IP al SVI (*Switch Virtual Interface*) para VLAN 99 de acuerdo con la siguiente tabla.

Equipo	Interfaz	Dirección IP	Máscara
SW-AA	VLAN 99	190.108.99.1	255.255.255.0
SW-BB	VLAN 99	190.108.99.2	255.255.255.0
SW-CC	VLAN 99	190.108.99.3	255.255.255.0

Tabla 6. Configuración de las direcciones Ip de los Switches.

```

SW-AA#configure terminal
SW-AA(config)#interface vlan 99
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
SW-BB#configure terminal

```

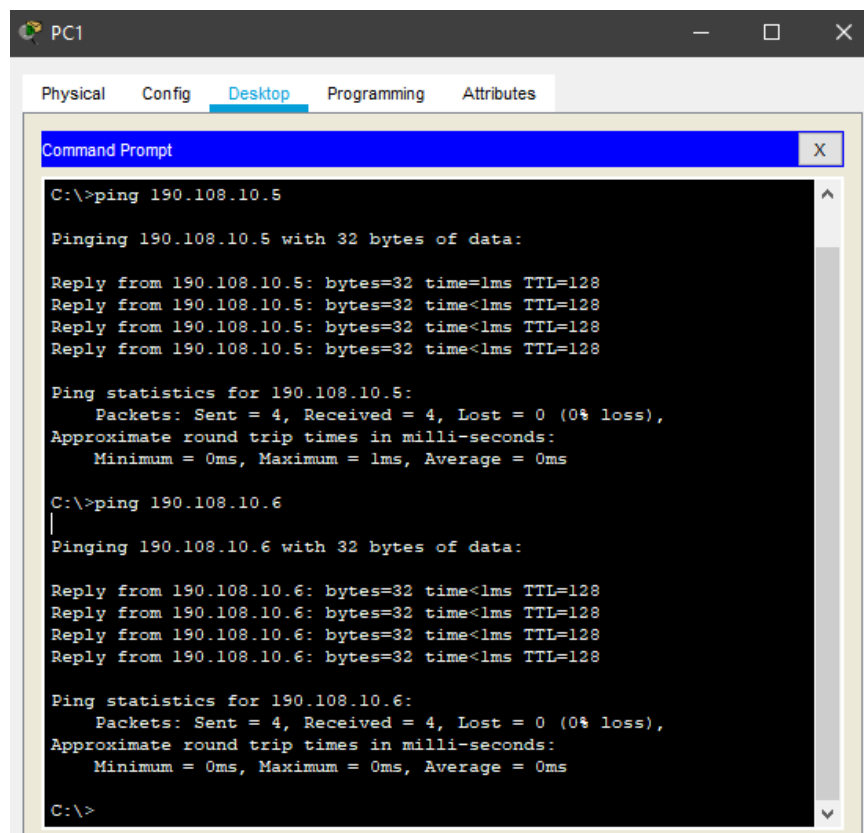
```
SW-BB(config)#interface vlan 99
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
```

```
SW-CC#configure terminal
SW-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. Se ejecuto un ping desde cada PC a los demás. Explique por qué el ping tuvo o no tuvo éxito.

Se ejecuto el ping desde los PC, se aclara que solo hará ping correctamente con los PC que estén en la misma Vlan, por ejemplo, en el PC1 hará ping con los PC4 y PC7 ya que estos pertenecen a la misma Vlan de lo contrario el resto fallara, como ejemplo se anexa los pings que pueden desarrollar cada uno de ellos.



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 190.108.10.5
Pinging 190.108.10.5 with 32 bytes of data:
Reply from 190.108.10.5: bytes=32 time<lms TTL=128
Reply from 190.108.10.5: bytes=32 time<lms TTL=128
Reply from 190.108.10.5: bytes=32 time<lms TTL=128
Reply from 190.108.10.5: bytes=32 time<lms TTL=128
Ping statistics for 190.108.10.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = lms, Average = 0ms
C:\>ping 190.108.10.6
Pinging 190.108.10.6 with 32 bytes of data:
Reply from 190.108.10.6: bytes=32 time<lms TTL=128
Reply from 190.108.10.6: bytes=32 time<lms TTL=128
Reply from 190.108.10.6: bytes=32 time<lms TTL=128
Reply from 190.108.10.6: bytes=32 time<lms TTL=128
Ping statistics for 190.108.10.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Figura 21. Ping desde PC1.

```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 190.108.20.5

Pinging 190.108.20.5 with 32 bytes of data:

Reply from 190.108.20.5: bytes=32 time<lms TTL=128
Reply from 190.108.20.5: bytes=32 time<lms TTL=128
Reply from 190.108.20.5: bytes=32 time<lms TTL=128
Reply from 190.108.20.5: bytes=32 time<lms TTL=128

Ping statistics for 190.108.20.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 190.108.20.6

Pinging 190.108.20.6 with 32 bytes of data:

Reply from 190.108.20.6: bytes=32 time=lms TTL=128
Reply from 190.108.20.6: bytes=32 time<lms TTL=128
Reply from 190.108.20.6: bytes=32 time<lms TTL=128
Reply from 190.108.20.6: bytes=32 time<lms TTL=128

Ping statistics for 190.108.20.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Figura 22. Ping desde PC2.

```
PC3
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 190.108.30.5

Pinging 190.108.30.5 with 32 bytes of data:

Reply from 190.108.30.5: bytes=32 time=lms TTL=128
Reply from 190.108.30.5: bytes=32 time=lms TTL=128
Reply from 190.108.30.5: bytes=32 time<lms TTL=128
Reply from 190.108.30.5: bytes=32 time<lms TTL=128

Ping statistics for 190.108.30.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 190.108.30.6

Pinging 190.108.30.6 with 32 bytes of data:

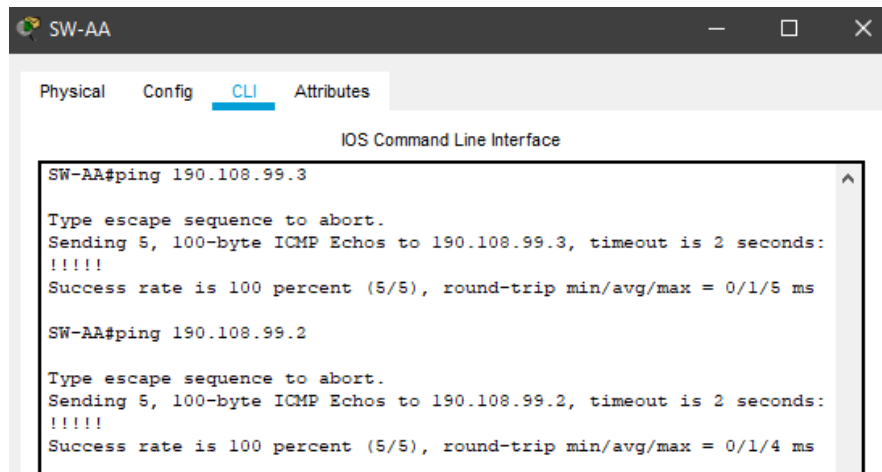
Reply from 190.108.30.6: bytes=32 time<lms TTL=128
Reply from 190.108.30.6: bytes=32 time=2ms TTL=128
Reply from 190.108.30.6: bytes=32 time<lms TTL=128
Reply from 190.108.30.6: bytes=32 time=3ms TTL=128

Ping statistics for 190.108.30.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>
```

Figura 23. Ping desde PC3.

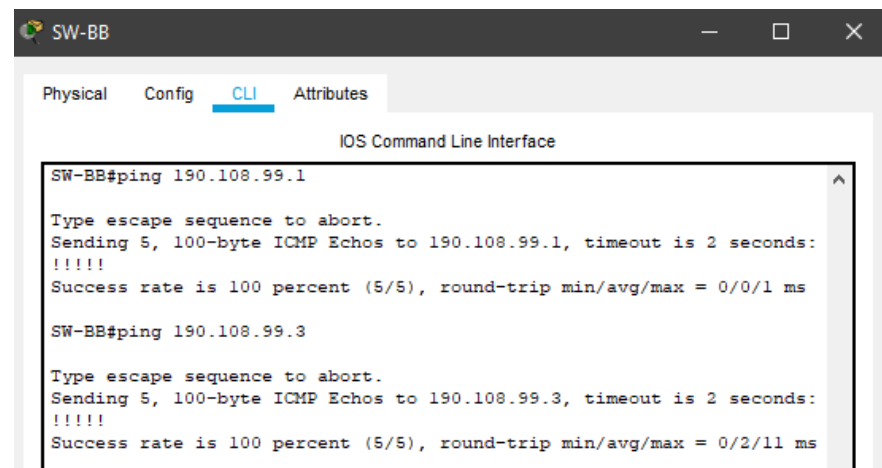
2. Se ejecuta un Ping desde cada Switch a los demás. Explique por qué el ping tuvo o no tuvo éxito.



```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
SW-AA#ping 190.108.99.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/5 ms

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

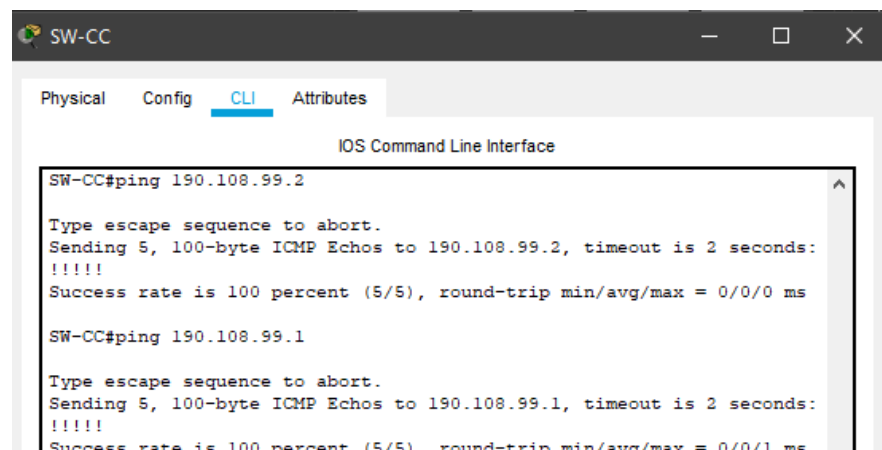
Figura 24. Ping desde SW-AA a SW-BB y SW-CC.



```
SW-BB
Physical Config CLI Attributes
IOS Command Line Interface
SW-BB#ping 190.108.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

SW-BB#ping 190.108.99.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/11 ms
```

Figura 25. Ping desde SW-BB a SW-AA y SW-CC.



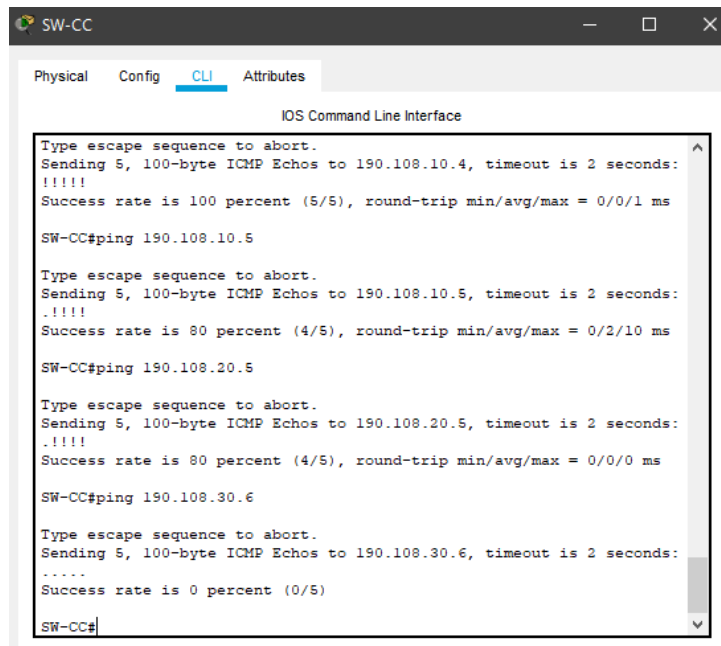
```
SW-CC
Physical Config CLI Attributes
IOS Command Line Interface
SW-CC#ping 190.108.99.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

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

Figura 26. Ping desde SW-CC a SW-AA y SW-BB.

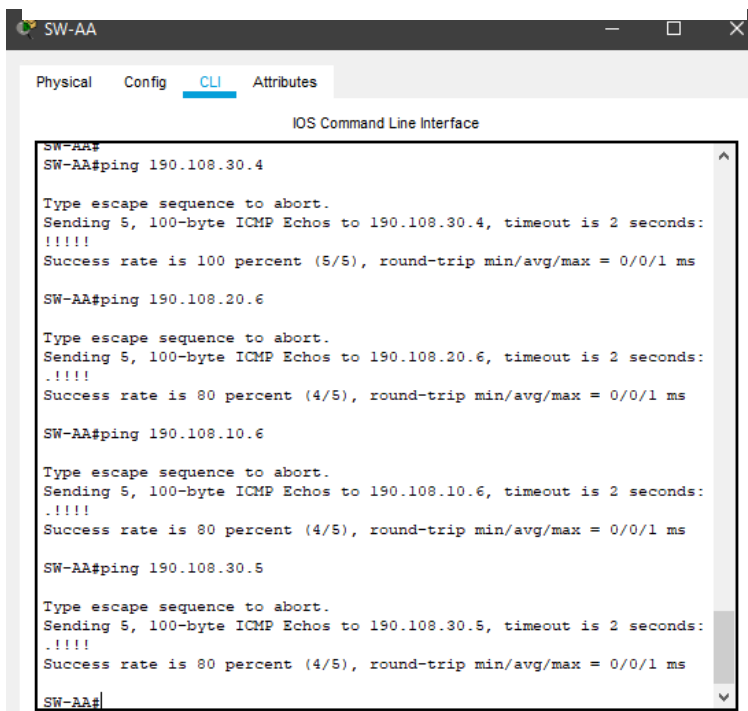
Los pings entre los Switches fueron satisfactorio gracias a la configuración que se realizo previamente del modo troncal entre las interfaces físicas conectadas.

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



```
SW-CC
Physical Config CLI Attributes
IOS Command Line Interface
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
SW-CC#ping 190.108.10.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.5, timeout is 2 seconds:
..!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/10 ms
SW-CC#ping 190.108.20.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.5, timeout is 2 seconds:
..!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
SW-CC#ping 190.108.30.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-CC#
```

Figura 27. Ping desde SW-CC a distintos PC.



```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
SW-AA#
SW-AA#ping 190.108.30.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
SW-AA#ping 190.108.20.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.6, timeout is 2 seconds:
..!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
SW-AA#ping 190.108.10.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.6, timeout is 2 seconds:
..!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
SW-AA#ping 190.108.30.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.5, timeout is 2 seconds:
..!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
SW-AA#
```

Figura 28. Ping desde SW-AA a distintos PC.

Con la configuración de enrutamiento IP en las Vlan creadas es posible realizar estos pings correctamente, en dado caso que no se configurara el enrutamiento IP en la Vlan al momento de realizar el ping entre los hosts esta acción no hubiera sido posible ya que es necesario configurar una dirección IP y una máscara de subredes en cada una de las interfaces de las Vlan la cual debe pertenecer al mismo segmento de red para que estos se puedan comunicar.

CONCLUSIONES

Se realizó un análisis y se desarrolló los conocimientos adquiridos durante el diplomado en cada uno de los escenarios, esto fue posible en esta práctica y en ella se puede evidenciar el conocimiento intelectual y lógico adquirido para solucionar todo tipo de problemas en diferentes aspectos de la administración de redes

Esta práctica permitió la implementación de diferentes procesos, en el escenario 1 se implementó enrutamiento Inter dominio BGP, donde se configuró la relación entre Routers vecinos, en cada uno de estos se codificó por medio de un ID, en el escenario 2 se configuró VTP de cada Switch para la comunicación y administración de datos, se conectaron por medio de troncales, por último, se crearon unas Vlan donde se configurara puertos, sus modos de acceso y direccionamiento en cada uno de los Switches.

Completado el desarrollo de la mejor manera en los escenarios propuestos por medio del diseño de en software de simulación como Packet Tracer y GNS3.

BIBLIOGRAFÍA

ANON., 2013. In : Cisco.com [en ligne]. 2013. [Consulté le 15 mai 2020]. Recuperado de: https://www.cisco.com/c/dam/en_us/training-events/netacad/demos/CCNP1v30/index/glossary/CCNP_v30_glossary.pdf.

Casos Prácticos de BGP. (30 de octubre de 2008). Recuperado de: https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocolbgp/26634-bgp-toc.html.

CISCO Press (Ed). CCNP Quick Reference. Recuperado de: <https://1drv.ms/b/s!AglGg5JUgUBthFt77ehzL5qp0OKD>

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!AmIJYeiNT1InWR0hoMxgBNv1CJ>.

Hucaby, D. (2015). CISCO Press (Ed). CCNP Routing and Switching SWITCH 300- 115 Official Cert Guide. Recuperado de <https://1drv.ms/b/s!AglGg5JUgUBthF16RWCSsCZnfDo2> Donohue, D. (2017).

Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de: <https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de: <https://1drv.ms/b/s!AmIJYei-NT1InMfy2rhPZHwEoWx>