

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

KEVIN LEONARDO RAMIREZ PADILLA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA DE
TELECOMUNICACIONES
CARTAGENA
2020

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

KEVIN LEONARDO RAMIREZ PADILLA

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA DE
TELECOMUNICACIONES
CARTAGENA
2020

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Cartagena, 22 de mayo de 2020

AGRADECIMIENTOS

Este proyecto de vida se lo agradezco principalmente a Dios por llenarme de salud y vida, para emprender cada uno de mis proyectos en el transcurso de mi existir. También a mis padres, hermano y familiares, con su apoyo incondicional y quienes han creído en mi a pesar de los cambios drásticos que nos da la vida, la cuales siempre buscamos el lado positivo y empeño de salir adelante. Por otra parte, agradezco a la Universidad Nacional Abierta y a Distancia, por permitirme capacitar en cada uno de los cursos de mi carrera como estudiante de Ingeniería de Telecomunicaciones, los cuales a través de los años no ha sido fácil, pero al adquirir estos conocimientos brindados por esta gran institución académica, hoy puedo decir que me llena de orgullo saber que estoy culminando este proyecto de vida, para graduarme como un futuro profesional.

Muchas gracias y bendiciones.

CONTENIDO

LISTA DE TABLAS.....	6
LISTA DE FIGURAS.....	7
GLOSARIO.....	8
RESUMEN.....	9
ABSTRACT	10
INTRODUCCIÓN.....	11
DESARROLLO PRUEBA DE HABILIDADES PRACTICAS CCNP	12
ESCENARIO 1	12
ESCENARIO 2	20
CONCLUSIONES.....	39
BIBLIOGRAFÍA.....	40

LISTA DE TABLAS

Tabla 1. Configuración Routers.....	12
Tabla 2. Puertos VLAN y Direcciones IP	30
Tabla 3. Equipos, Direcciones IP y Mascaras Asignadas.....	32
Tabla 4. Equipos, VLAN 99, Direcciones IP y Mascaras.	32

LISTA DE FIGURAS

Ilustración 1. Escenario 1	12
Ilustración 2. Simulación Escenario 1	13
Ilustración 3. Resultado aplicar comando show ip route R1	14
Ilustración 4. Resultado aplicar comando show ip route R2.....	15
Ilustración 5. Resultado aplicar comando show ip route R2.....	16
Ilustración 6. Resultado aplicar comando show ip route R3.....	17
Ilustración 7. Resultado aplicar comando show ip route R3.....	18
Ilustración 8. Resultado aplicar comando show ip route R4.....	19
Ilustración 9. Escenario 2	20
Ilustración 10. Simulación Escenario 2	20
Ilustración 11. Resultado aplicar comando show vtp SW-AA	22
Ilustración 12. Resultado aplicar comando show vtp SW-BB	22
Ilustración 13. Resultado aplicar comando show vtp SW-CC	23
Ilustración 14. Resultado aplicar comando show interfaces trunk SW-AA	24
Ilustración 15. Resultado aplicar comando show interfaces trunk SW-BB	24
Ilustración 16. Resultado aplicar comando show interfaces trunk SW-AA	25
Ilustración 17. Resultado aplicar comando show interfaces trunk SW-CC	26
Ilustración 18. Resultado aplicar comando show interfaces trunk SW-BB	27
Ilustración 19. Resultado al intentar entrar a la VLAN 10	27
Ilustración 20. Resultado aplicar comando show vlan SW-AA	28
Ilustración 21. Resultado aplicar comando show vlan SW-BB	29
Ilustración 22. Resultado aplicar comando show vlan SW-CC.....	29
Ilustración 23. Resultado aplicar ping en diferentes PC.....	34
Ilustración 24. Resultado hacer ping de SW-AA a SW-BB y SW-CC	35
Ilustración 25. Resultado hacer ping de SW-BB a SW-AA y SW-CC	35
Ilustración 26. Resultado hacer ping de SW-CC a SW-AA y SW-BB	36
Ilustración 27. Resultado hacer ping de SW-AA a PC1-PC2-PC3	37
Ilustración 28. Resultado hacer ping de SW-BB a PC4-PC5-PC6	37
Ilustración 29. Resultado hacer ping de SW-CC a PC7-PC8-PC9.....	38

GLOSARIO

Dirección IP

Es un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, laptop , teléfono inteligente) que utilice el protocolo o (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP

BGP

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

VLAN - Red de Área Local Virtual

Tipo de red que aparentemente parece ser una pequeña red de área local (LAN) cuando en realidad es una construcción lógica que permite la conectividad con diferentes paquetes de software. Sus usuarios pueden ser locales o estar distribuidos en diversos lugares

VTP

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

DTP

(Dynamic Trunking Protocol) es un protocolo propietario creado por Cisco Systems que opera entre switches Cisco, el cual automatiza la configuración de trunking (etiquetado de tramas de diferentes VLAN's con ISL o 802.1Q) en enlaces Ethernet.

Ancho de Banda – Bandwidth

Cantidad de datos que puede ser enviada o recibida durante un cierto tiempo a través de un determinado circuito de comunicación. Técnicamente, es la diferencia en hertzios (Hz) entre la frecuencia más alta y más baja de un canal de transmisión.

DHCP

Siglas del inglés "Dynamic Host Configuration Protocol." Protocolo Dinámico de configuración del Host. Un servidor de red usa este protocolo para asignar de forma dinámica las direcciones IP a las diferentes computadoras de la red

Gateway – Pasarela o puerta de acceso

es el dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos, y también posibilita compartir recursos entre dos o más ordenadores.

RESUMEN

A lo largo del tiempo la tecnología y la **electrónica** han evolucionado en diferentes aspectos, facilitando la comunicación y transporte de datos en el mundo, por lo cual debemos siempre mantenernos actualizados en el caso más específico, me permito presentar esta Prueba de Habilidades Prácticas, la cual es una actividad final que corresponde al Diplomado de Profundización **CCNP**, donde se busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado, en la cual **CISCO** a través de su plataforma <https://www.netacad.com/es>. Busca instruir a sus alumnos y personal interesado en la configuración de **redes** de telecomunicaciones, por lo tanto, lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de **redes**. Para esta actividad, el estudiante dispone de cerca de un (1) mes y quince (15) días para realizar las tareas asignadas en cada uno de los dos (2) escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros; para así, verificar proceso de **conmutación** estableciendo las vías o caminos entre los diferentes escenarios presentados en la prueba de habilidad.

En este caso, se realizó las diferentes configuraciones de los dos (2) escenarios propuestos con la herramienta de Packet Tracer, donde se aplican los conocimientos, destrezas y habilidades aprendidas durante el desarrollo del presente diplomado de **CCNP**. Colocando en práctica la destreza de desarrollar la capacidad de configurar y verificar operaciones básicas de **enrutamiento** de Gateway interior mediante el uso de comandos específicos del IOS con el fin identificar y resolver problemas de conectividad y actualización de tablas de **enrutamiento**.

Palabras Clave: CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

Over time, technology and **electronics** have evolved in different ways, facilitating the communication and transport of data in the world, so we must always keep updated in the most specific case, allow me to present this Practical Skills Test, which is a final activity corresponding to the **CCNP** Deepening Diploma, where it is sought to identify the degree of development of skills and abilities that were acquired throughout the diploma course, in which **CISCO** through its platform <https://www.netacad.com/es>. Seeks to instruct its students and staff interested in the configuration of telecommunications **networking**, therefore, the essential thing is to test the levels of understanding and troubleshooting related to various aspects of **networking**, For this activity, the student has about one (1) month and fifteen (15) days to perform the assigned tasks in each of the two (2) scenarios proposed, accompanied by the respective solution documentation processes, corresponding to the recording of the configuration of each device, the detailed step-by-step description of each of the steps taken during its development, the recording of the connectivity verification processes using ping commands, traceroute, show ip route, among others; for this, verify the **switching** process by establishing the pathways or pathways between the different scenarios presented in the skill test.

In this case, the different configurations of the two (2) scenarios proposed with the Packet Tracer tool were performed, where the knowledge is applied, skills and abilities learned during the development of the present **CCNP** diploma, Putting into practice the ability to develop the ability to configure and verify basic **routing** operations of internal Gateway by using specific IOS commands in order to identify and solve connectivity problems and update tables **routing**.

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

INTRODUCCIÓN

Los desafíos que presentan diariamente la Networking, son solucionados por los Ingenieros de Telecomunicaciones, por tal motivo, en esta prueba de Prueba de Habilidades Prácticas, se buscará poner en práctica los aprendidos al largo de este Diplomado de Profundización CCNP, dando solución a los dos (2) escenarios propuestos, Una vez adquiridos los conocimientos y habilidades en los diferentes protocolos, aplicaciones y características de los elementos Cisco (Router y Switch).

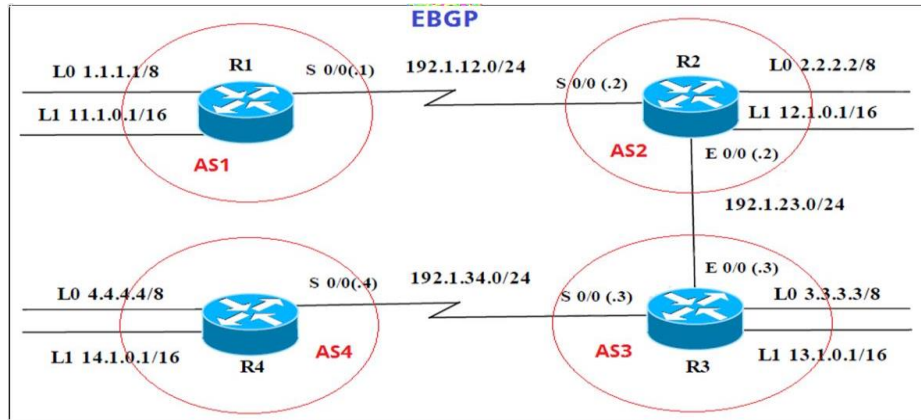
A lo largo del documento de guía se informa paso a paso el proceso realizado para dar solución a actividad planteada y el registro de los procesos de verificación de conectividad mediante el uso de comandos como ping, traceroute, show ip route, apoyándose en la práctica con el simulador Packet Tracer.

Para cumplir con los propósitos mencionados, se abordan temáticas como el enrutamiento dinámico, el enrutamiento a través del protocolo BGP y el proceso de creación de adyacentes en función del protocolo IPv4, del Router ID e interfaces Loopback. Por último, se evidencia la configuración de una pequeña red basada en Switches capa 2 y PCs, en la cual se configura el enrutamiento IPv4 respectivo, se implementa protocolos como VLAN Trunking Protocol y Dynamic Trunking Protocol, así como una parte inicial del enrutamiento InterVLAN.

DESARROLLO PRUEBA DE HABILIDADES PRACTICAS CCNP

ESCENARIO 1

Ilustración 1. Escenario 1

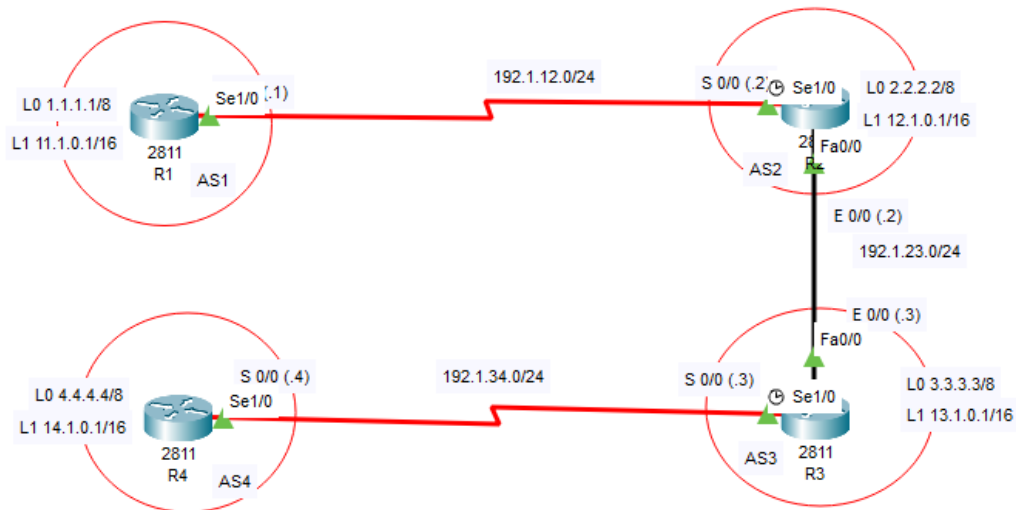


Información para la configuración de Routers.

Tabla 1. Configuración Routers

	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
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
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
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

Ilustración 2. Simulación Escenario 1



1. Configure una relación de vecino BGP entre R1 y R2. R1 debe estar en **AS1** y R2 debe estar en **AS2**. Anuncie las direcciones de Loopback en BGP. Codifique los ID para los routers BGP como 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**.

```

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(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 1/0
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 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)#exit
R1#

```

Ilustración 3. Resultado aplicar comando show ip route R1

```
R1
Physical Config CLI Attributes
IOS Command Line Interface
* > 192.1.12.0/24 0.0.0.0 0 0 32768 i
*
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

C 1.0.0.0/8 is directly connected, Loopback0
B 2.0.0.0/8 [20/0] via 192.1.12.2, 00:00:00
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, 00:00:00
C 192.1.12.0/24 is directly connected, Serial1/0

R1#
Ctrl+F6 to exit CLI focus Copy Paste
Top
```

```
Router>enable
Router#configure terminal
Router(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 1/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#interface fastethernet 0/0
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)#exit
R2(config)#exit
R2#
```

Ilustración 4. Resultado aplicar comando show ip route R2



```
Physical Config CLI Attributes
IOS Command Line Interface
*-> 192.1.12.0/24 0.0.0.0 0 0 32768 i
* 192.1.12.1 0 0 0 1 i

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

Gateway of last resort is not set

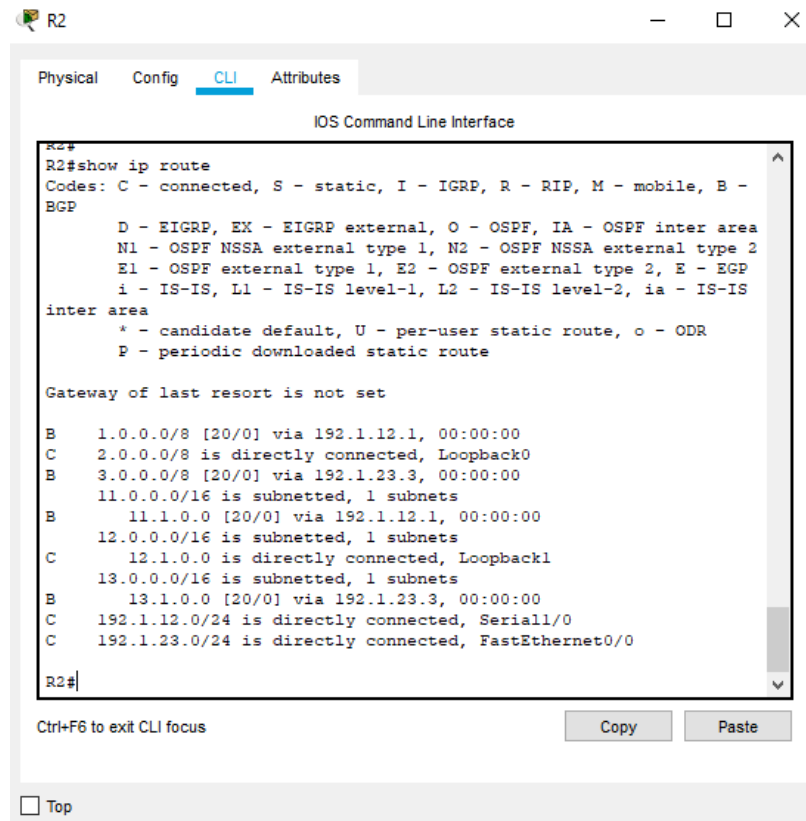
B 1.0.0.0/8 [20/0] via 192.1.12.1, 00:00:00
C 2.0.0.0/8 is directly connected, Loopback0
  11.0.0.0/16 is subnetted, 1 subnets
  11.1.0.0 [20/0] via 192.1.12.1, 00:00:00
B 12.0.0.0/16 is subnetted, 1 subnets
  12.1.0.0 is directly connected, Loopback1
C 192.1.12.0/24 is directly connected, Serial1/0

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 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)#exit
R2(config)#exit
R2#
```

Ilustración 5. Resultado aplicar comando show ip route R2



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

Gateway of last resort is not set

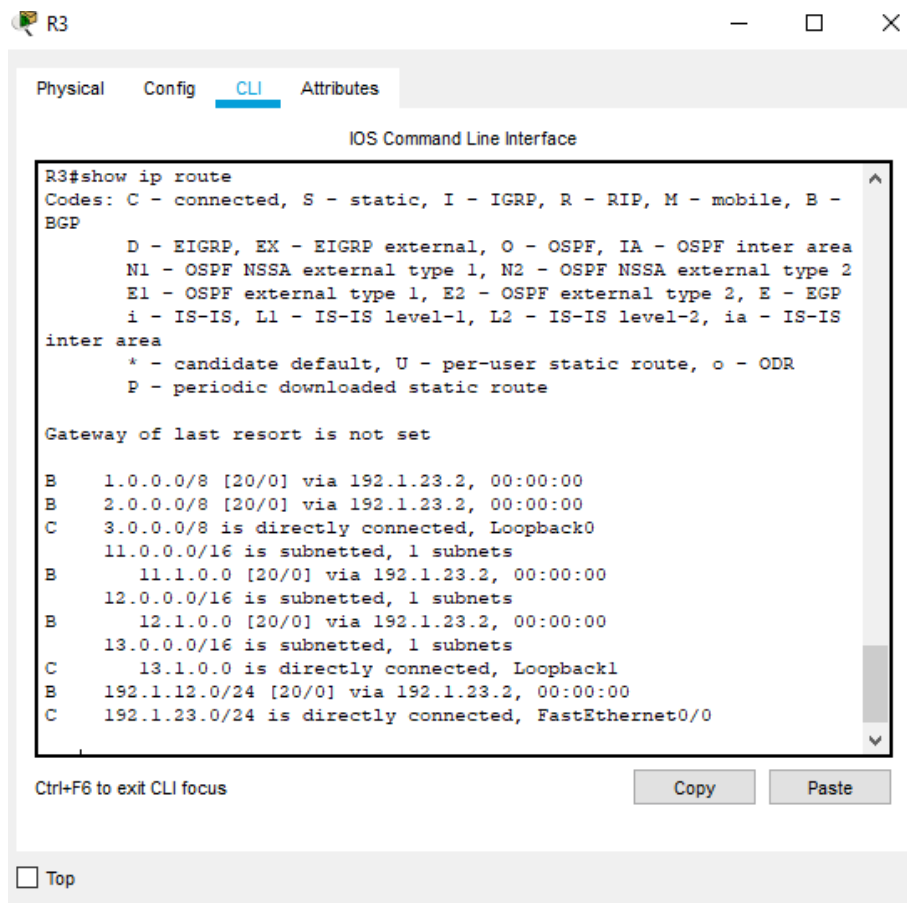
B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:00:00
C    2.0.0.0/8 is directly connected, Loopback0
B    3.0.0.0/8 [20/0] via 192.1.23.3, 00:00:00
     11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 192.1.12.1, 00:00:00
     12.0.0.0/16 is subnetted, 1 subnets
C    12.1.0.0 is directly connected, Loopback1
     13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0 [20/0] via 192.1.23.3, 00:00:00
C    192.1.12.0/24 is directly connected, Serial1/0
C    192.1.23.0/24 is directly connected, FastEthernet0/0

R2#
```

```
Router>enable
Router#configure terminal
Router(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 fastethernet 0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#interface serial 1/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shut
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
R3(config-router)#exit
R3(config)#exit
R3#
```

Ilustración 6. Resultado aplicar comando show ip route R3



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

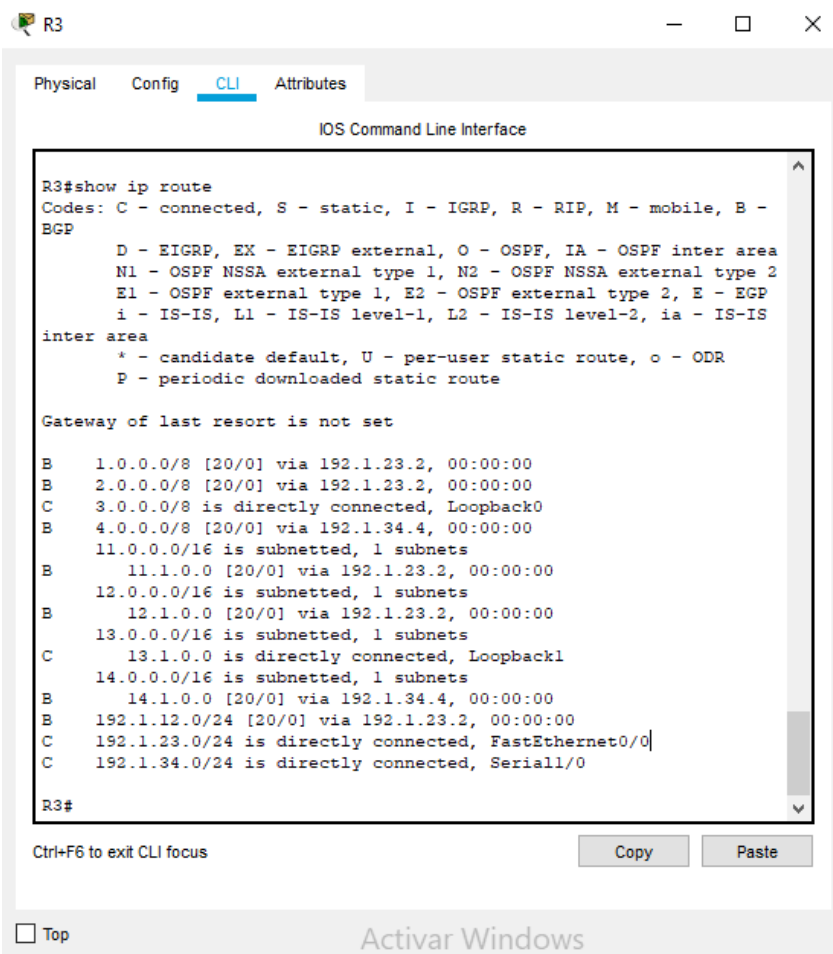
Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
C    3.0.0.0/8 is directly connected, Loopback0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.23.2, 00:00:00
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.23.2, 00:00:00
     13.0.0.0/16 is subnetted, 1 subnets
C       13.1.0.0 is directly connected, Loopback1
B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:00:00
C    192.1.23.0/24 is directly connected, FastEthernet0/0
```

3. Configure una relación de vecino BGP entre R3 y R4. R3 ya debería estar configurado en **AS3** y R4 debería estar en **AS4**. Anuncie las direcciones de Loopback de R4 en BGP. Codifique el ID del router R4 como 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
```

Ilustración 7. Resultado aplicar comando show ip route R3



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

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
C    3.0.0.0/8 is directly connected, Loopback0
B    4.0.0.0/8 [20/0] via 192.1.34.4, 00:00:00
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.23.2, 00:00:00
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.23.2, 00:00:00
     13.0.0.0/16 is subnetted, 1 subnets
C       13.1.0.0 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, 00:00:00
B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:00:00
C    192.1.23.0/24 is directly connected, FastEthernet0/0|
C    192.1.34.0/24 is directly connected, Serial1/0

R3#
```

```

Router>enable
Router#configure terminal
Router(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 1/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shut
R4(config-if)#exit
R4(config)#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)#exit

```

Ilustración 8. Resultado aplicar comando show ip route R4

```

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

Gateway of last resort is not set

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

R4#

```

ESCENARIO 2

Ilustración 9. Escenario 2

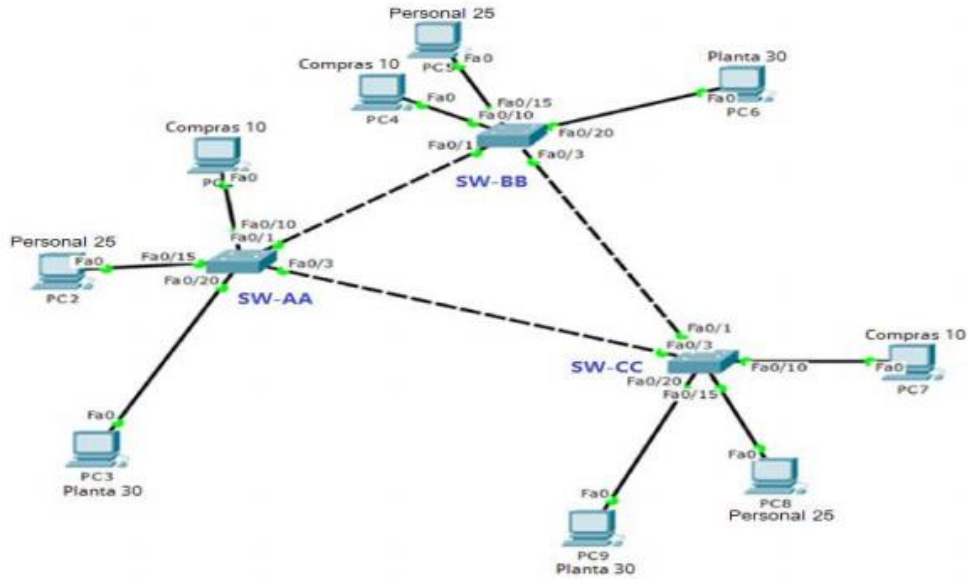
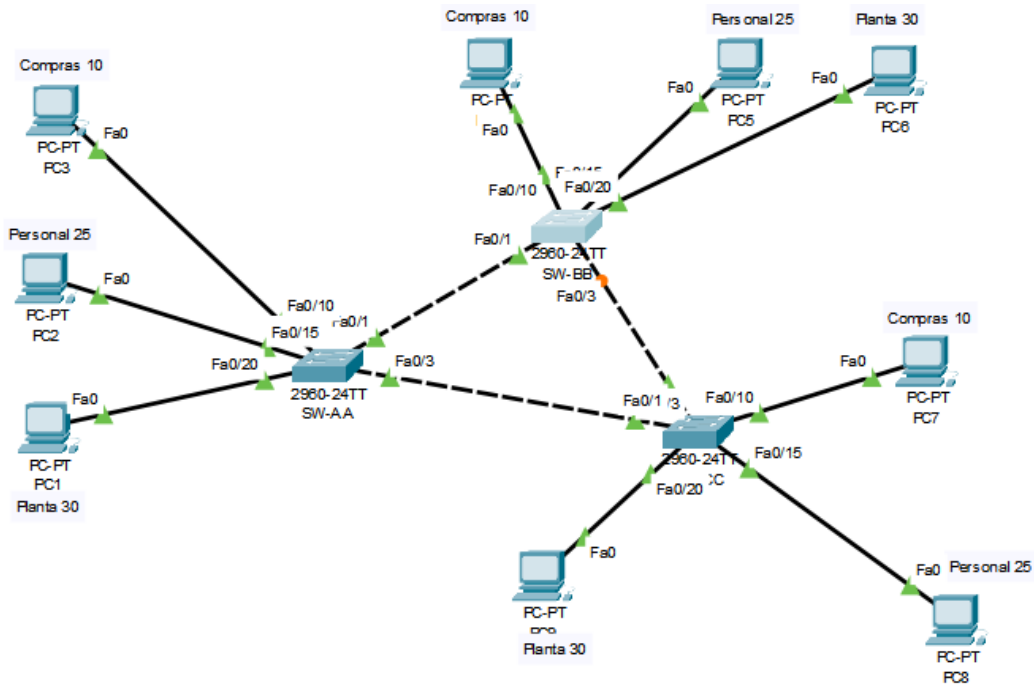


Ilustración 10. Simulación Escenario 2



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.

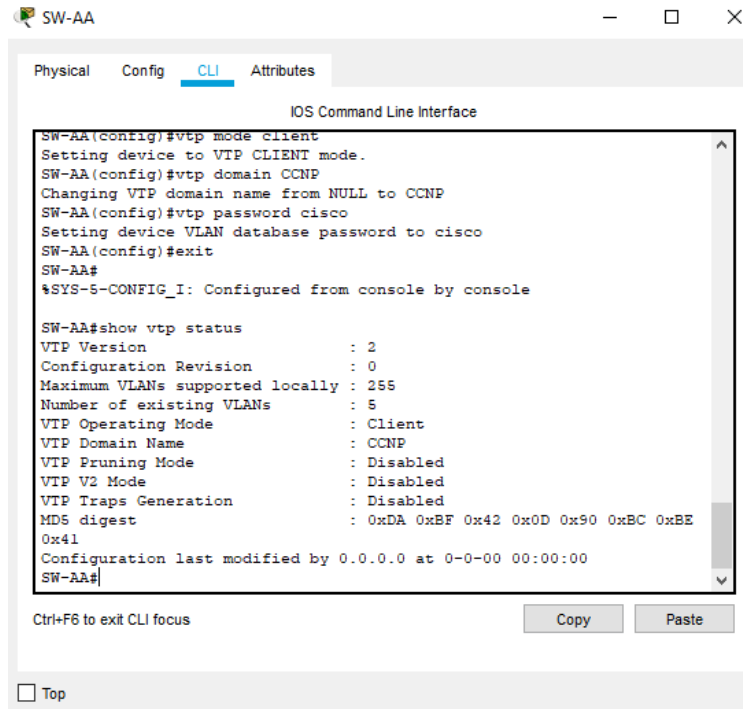
```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-AA
SW-AA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-AA(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-AA(config)#vtp password cisco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

```
Switch>enable
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
SW-BB(config)#
```

```
Switch>enable
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
SW-CC(config)#
```

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

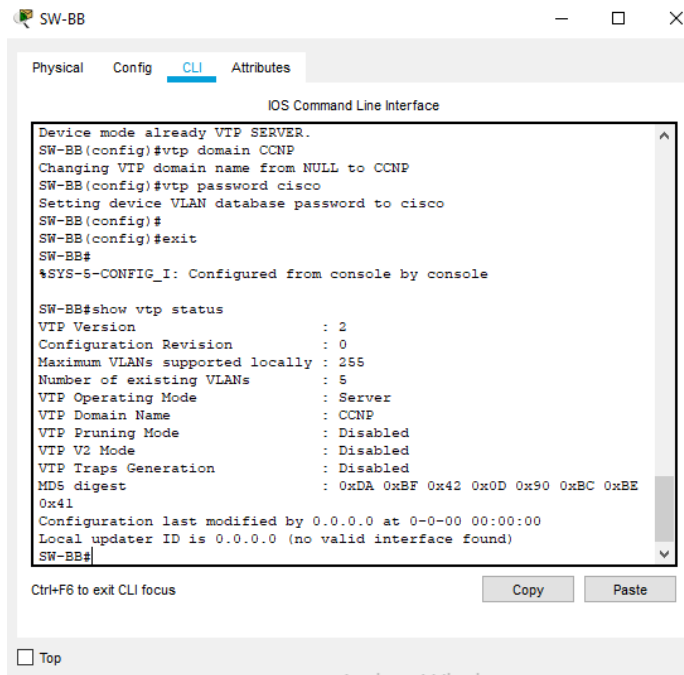
Ilustración 11. Resultado aplicar comando show vtp SW-AA



```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
SW-AA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-AA(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-AA(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-AA(config)#exit
SW-AA#
%SYS-5-CONFIG_I: Configured from console by console

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

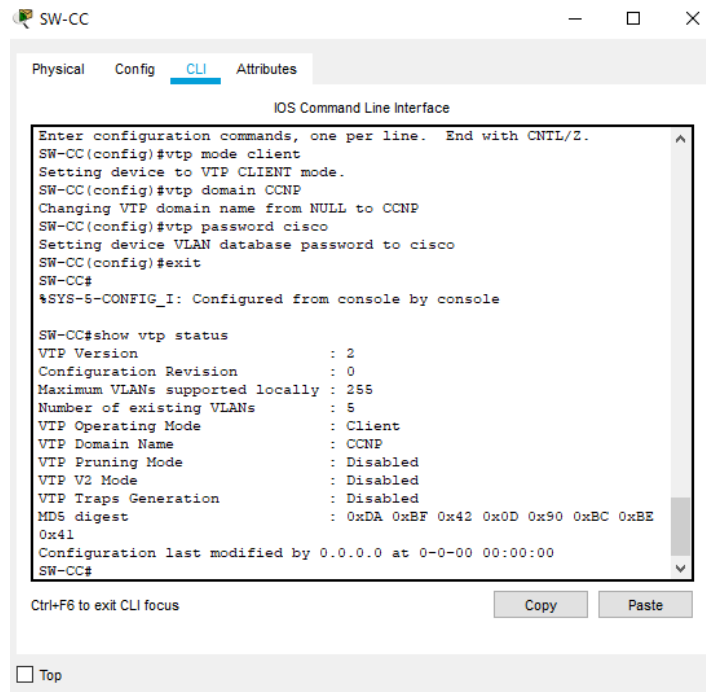
Ilustración 12. Resultado aplicar comando show vtp SW-BB



```
SW-BB
Physical Config CLI Attributes
IOS Command Line Interface
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
SW-BB(config)#
SW-BB(config)#exit
SW-BB#
%SYS-5-CONFIG_I: Configured from console by console

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

Ilustración 13. Resultado aplicar comando show vtp SW-CC



```
SW-CC
Physical Config CLI Attributes
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
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
SW-CC(config)#exit
SW-CC#
%SYS-5-CONFIG_I: Configured from console by console

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

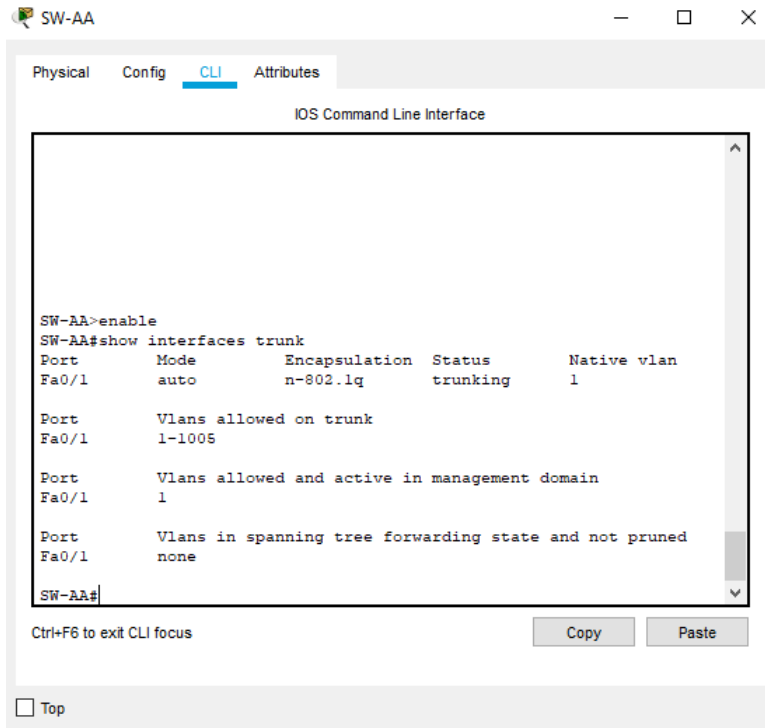
B. Configurar DTP (Dynamic Trunking Protocol)

4. 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 t
SW-BB(config)#interface fastethernet 0/1
SW-BB(config-if)#switchport mode dynamic desirable
SW-BB(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up
```

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

Ilustración 14. Resultado aplicar comando `show interfaces trunk` SW-AA



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

Port      Vlans allowed on trunk
Fa0/1     1-1005

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

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     none

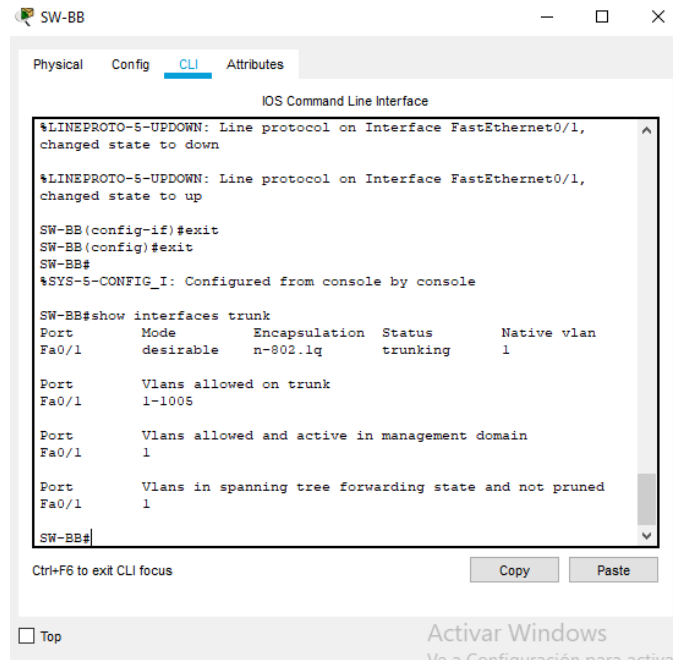
SW-AA#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Ilustración 15. Resultado aplicar comando `show interfaces trunk` SW-BB



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

Port      Vlans allowed on trunk
Fa0/1     1-1005

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

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1

SW-BB#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

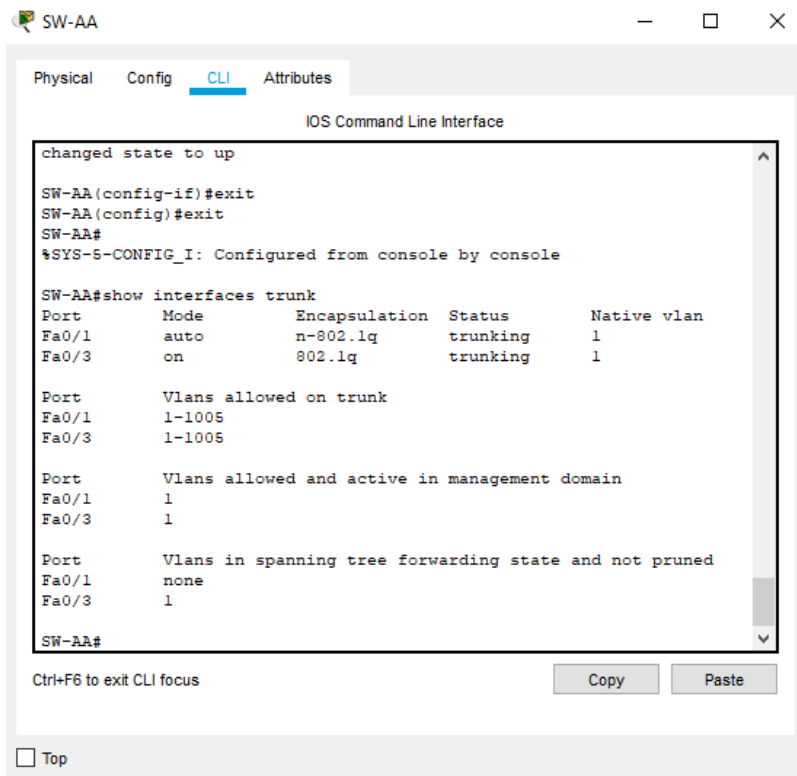
Activar Windows
Ve a Configuración para activar

6. 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#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface fastethernet 0/3
SW-AA(config-if)#switchport mode trunk
SW-AA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
state to up
SW-AA(config-if)#exit
SW-AA(config)#exit
SW-AA#
```

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

Ilustración 16. Resultado aplicar comando show interfaces trunk SW-AA



```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
changed state to up
SW-AA(config-if)#exit
SW-AA(config)#exit
SW-AA#
%SYS-5-CONFIG_I: Configured from console by console

SW-AA#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     auto     n-802.1q       trunking    1
Fa0/3     on       802.1q         trunking    1

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

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

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     none
Fa0/3     1

SW-AA#
```

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

```
SW-BB#conf t
SW-BB(config)#interface fastethernet 0/3
SW-BB(config-if)#switchport mode trunk
SW-BB(config-if)#exit
SW-BB(config)#exit
SW-BB#
```

```
SW-CC#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#interface fastethernet 0/1
SW-CC(config-if)#switchport mode trunk
SW-CC(config-if)#exit
SW-CC(config)#exit
SW-CC#
```

Ilustración 17. Resultado aplicar comando show interfaces trunk SW-CC

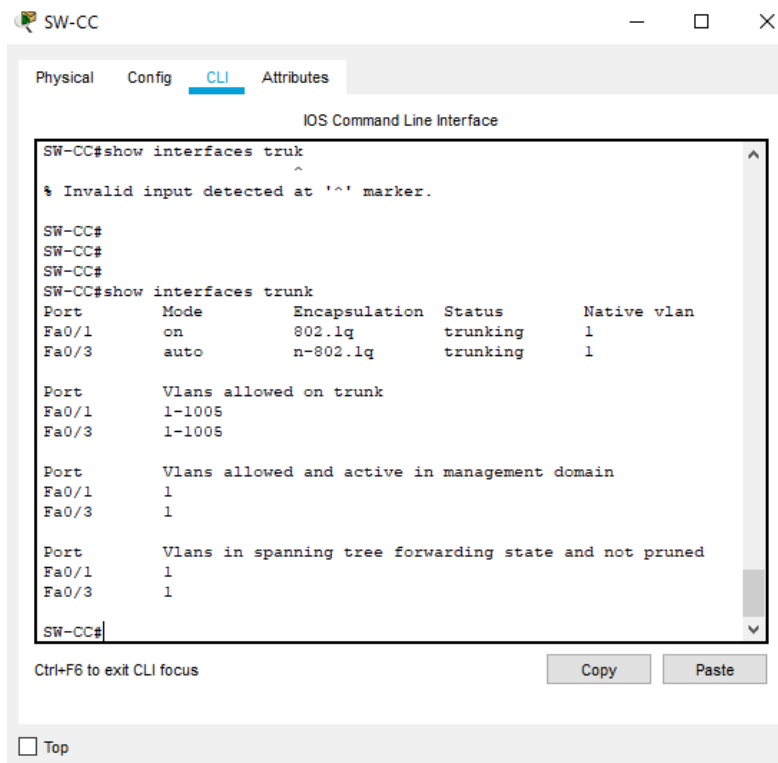
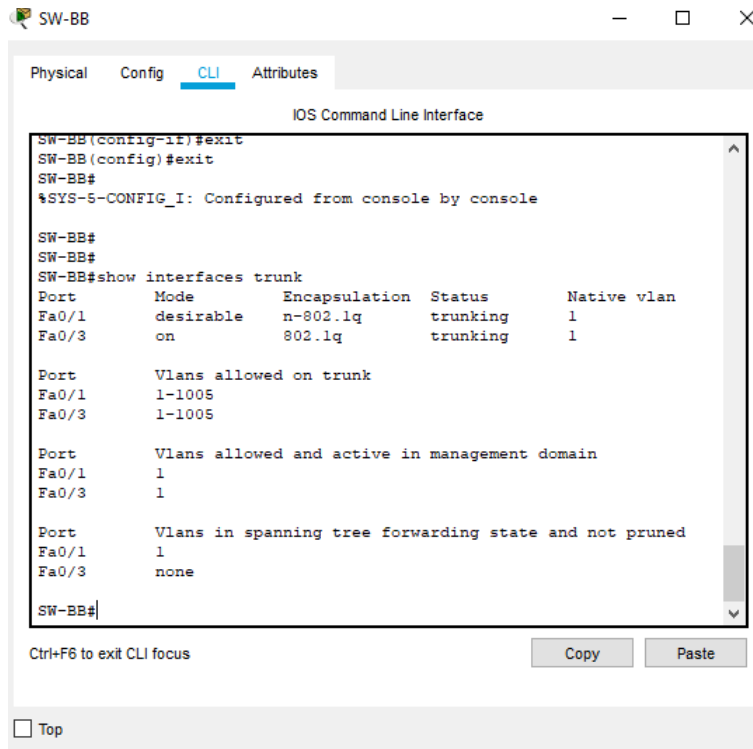


Ilustración 18. Resultado aplicar comando show interfaces trunk SW-BB



```
SW-BB
Physical Config CLI Attributes
IOS Command Line Interface
SW-BB(config-if)#exit
SW-BB(config)#exit
SW-BB#
%SYS-5-CONFIG_I: Configured from console by console

SW-BB#
SW-BB#
SW-BB#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     desirable n-802.1q       trunking    1
Fa0/3     on        802.1q         trunking    1

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

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

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1
Fa0/3     none
SW-BB#
```

C. Agregar VLANs y asignar puertos.

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

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

Ilustración 19. Resultado al intentar entrar a la VLAN 10



```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
SW-AA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
```

```

SW-BB#conf t
SW-BB(config-vlan)#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
SW-BB(config)#exit

```

10. Verifique que las VLANs han sido agregadas correctamente.

Ilustración 20. Resultado aplicar comando show vlan SW-AA

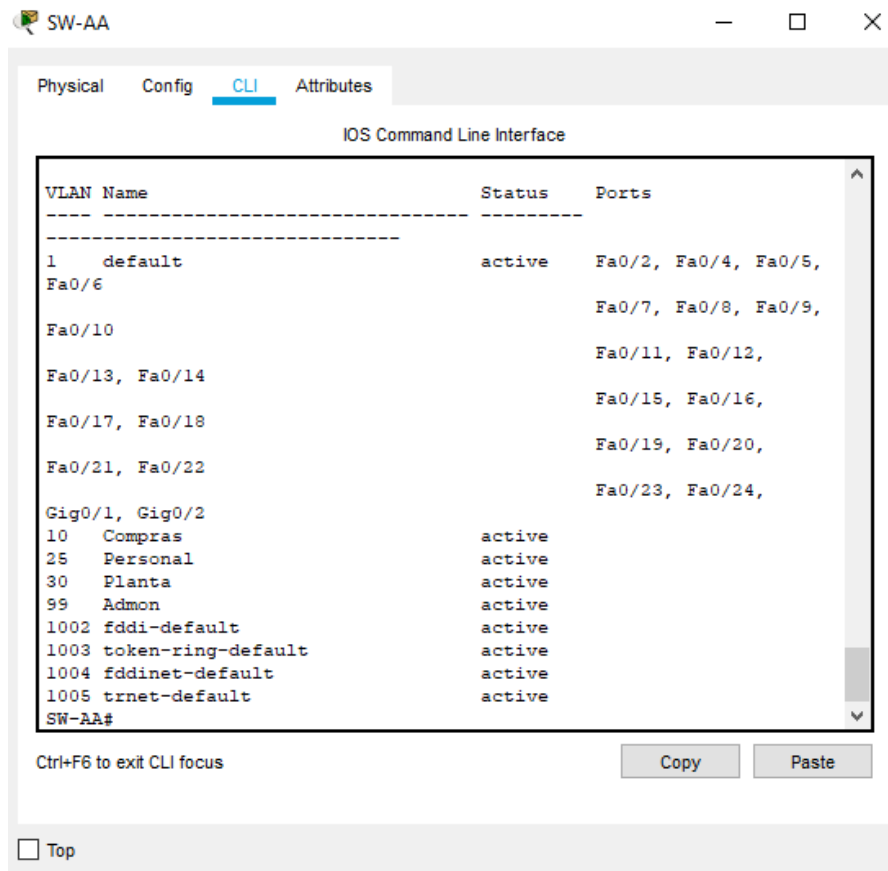
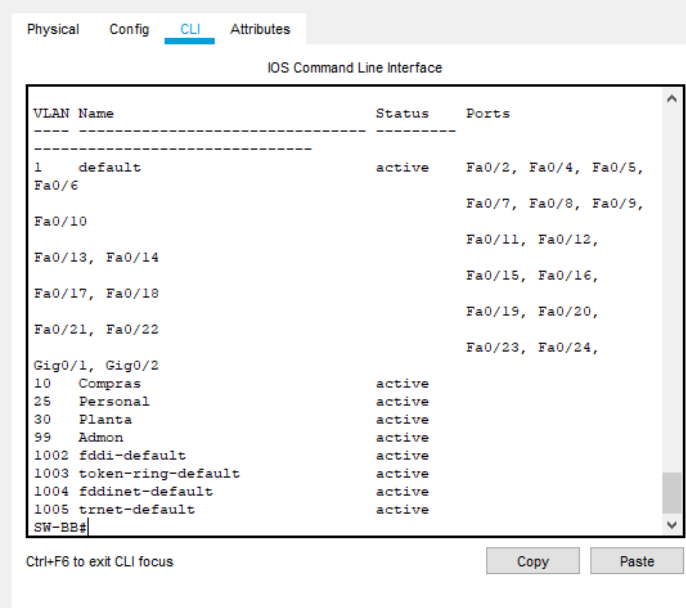


Ilustración 21. Resultado aplicar comando show vlan SW-BB



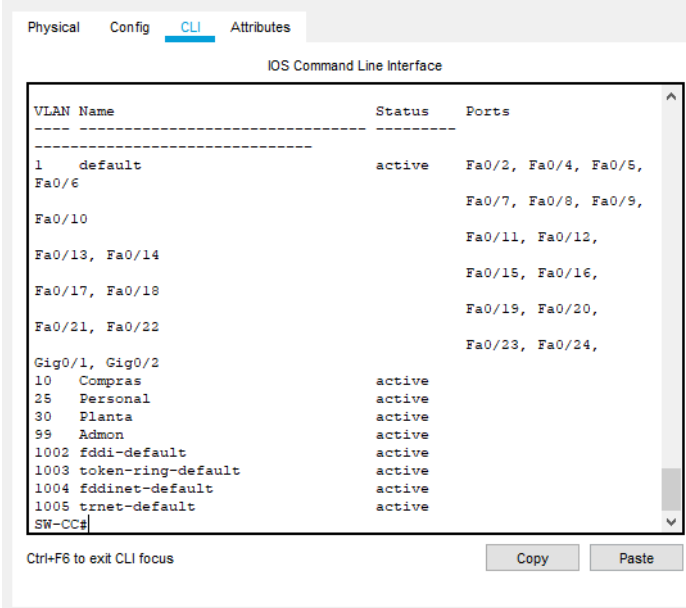
```
SW-BB
Physical Config CLI Attributes
IOS Command Line Interface
VLAN Name                Status  Ports
-----
1  default                active  Fa0/2, Fa0/4, Fa0/5,
Fa0/6                    Fa0/7, Fa0/8, Fa0/9,
Fa0/10                   Fa0/11, Fa0/12,
Fa0/13, Fa0/14           Fa0/15, Fa0/16,
Fa0/17, Fa0/18           Fa0/19, Fa0/20,
Fa0/21, Fa0/22           Fa0/23, Fa0/24,
Gig0/1, Gig0/2
10  Compras                active
25  Personal                active
30  Planta                  active
99  Admon                   active
1002 fddi-default           active
1003 token-ring-default   active
1004 fddinet-default       active
1005 trnet-default         active
SW-BB#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Ilustración 22. Resultado aplicar comando show vlan SW-CC



```
SW-CC
Physical Config CLI Attributes
IOS Command Line Interface
VLAN Name                Status  Ports
-----
1  default                active  Fa0/2, Fa0/4, Fa0/5,
Fa0/6                    Fa0/7, Fa0/8, Fa0/9,
Fa0/10                   Fa0/11, Fa0/12,
Fa0/13, Fa0/14           Fa0/15, Fa0/16,
Fa0/17, Fa0/18           Fa0/19, Fa0/20,
Fa0/21, Fa0/22           Fa0/23, Fa0/24,
Gig0/1, Gig0/2
10  Compras                active
25  Personal                active
30  Planta                  active
99  Admon                   active
1002 fddi-default           active
1003 token-ring-default   active
1004 fddinet-default       active
1005 trnet-default         active
SW-CC#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

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

Tabla 2. Puertos VLAN y Direcciones IP

Interfaz	VLAN	Direcciones IP de los PCs
F 0/10	VLAN 10	190.108.10.X / 24
F 0/15	VLAN 25	190.108.20.X / 24
F 0/20	VLAN 30	190.108.30.X / 24

X = número de cada PC particular

En SW-AA.

```
SW-AA>enable
SW-AA#configure terminal
SW-AA(config)#interface vlan 10
SW-AA(config-if)#
SW-AA(config-if)#ip address 190.108.10.1 255.255.255.0
SW-AA(config-if)#exit
SW-AA(config)#interface vlan 20
SW-AA(config-if)#
SW-AA(config-if)#ip address 190.108.20.1 255.255.255.0
SW-AA(config-if)#exit
SW-AA(config)#interface vlan 30
SW-AA(config-if)#
SW-AA(config-if)#ip address 190.108.30.1 255.255.255.0
SW-AA(config-if)#exit
```

En SW-BB

```
SW-BB>enable
SW-BB#configure terminal
SW-BB(config)#interface vlan 10
SW-BB(config-if)#ip address 190.108.10.2 255.255.255.0
SW-BB(config-if)#exit
SW-BB(config)#interface vlan 20
SW-BB(config-if)#ip address 190.108.20.2 255.255.255.0
SW-BB(config-if)#exit
SW-BB(config)#interface vlan 30
SW-BB(config-if)#ip address 190.108.30.2 255.255.255.0
SW-BB(config-if)#exit
```

En SW-CC

```
SW-CC>enable
SW-CC#configure terminal
SW-CC(config)#interface vlan 10
```

```
SW-CC(config-if)#
SW-CC(config-if)#ip address 190.108.10.3 255.255.255.0
SW-CC(config-if)#exit
SW-CC(config)#interface vlan 20
SW-CC(config-if)#ip address 190.108.20.3 255.255.255.0
SW-CC(config-if)#exit
SW-CC(config)#interface vlan 30
SW-CC(config-if)#ip address 190.108.30.3 255.255.255.0
SW-CC(config-if)#exit
```

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

13. Repita 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#conf t
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-AA(config-if)#exit
SW-AA(config)#exit
SW-AA#
```

```
SW-BB#conf t
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-BB(config-if)#exit
SW-BB(config)#exit
```

```

SW-CC#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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
SW-CC(config-if)#exit
SW-CC(config)#exit
SW-CC#

```

Tabla 3. Equipos, Direcciones IP y Mascaras Asignadas.

EQUIPO	DIRECCIÓN IP	MASCARA
PC1	190.108.10.10	255.255.255.0
PC2	190.108.20.20	255.255.255.0
PC3	190.108.30.30	255.255.255.0
PC4	190.108.10.4	255.255.255.0
PC5	190.108.20.5	255.255.255.0
PC6	190.108.30.6	255.255.255.0
PC7	190.108.10.7	255.255.255.0
PC8	190.108.20.8	255.255.255.0
PC9	190.108.30.9	255.255.255.0

D. Configurar las direcciones IP en los Switches.

14. 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. Equipos, VLAN 99, Direcciones IP y Mascaras.

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

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

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

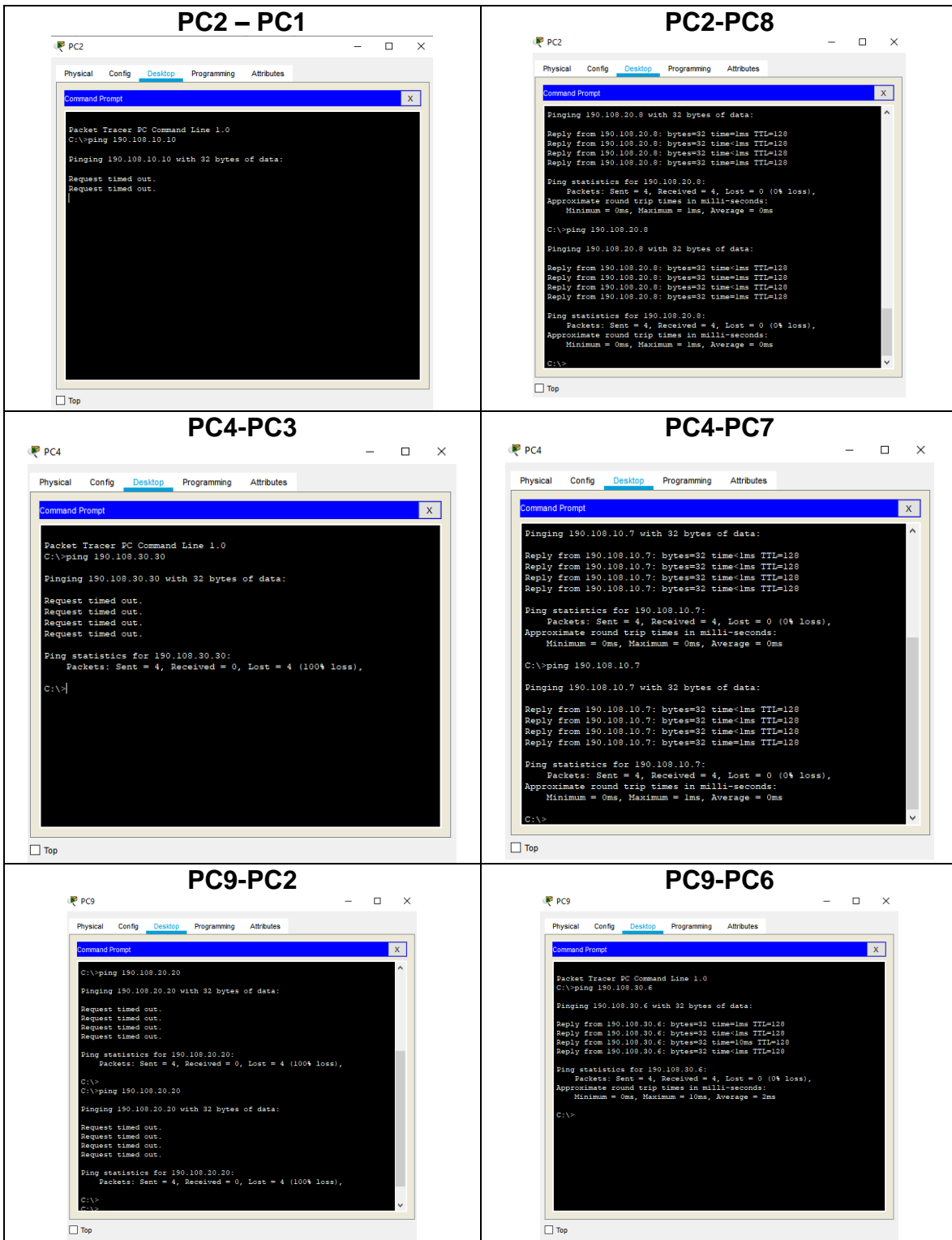
```
SW-CC#conf t
SW-CC(config)#interface vlan 99
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0
SW-CC(config-if)#exit
SW-CC(config)#exit
```

E. Verificar la conectividad Extremo a Extremo

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

El ping realizado entre los PCs pertenecientes a diferentes Vlans no tuvo éxito, sin embargo, los pings realizados a PCs que perteneces a la misma Vlan, si tuvieron éxito. El error en los PCs pertenecientes a diferentes Vlans se presenta ya que cada PC pertenece a un segmento de red diferente. Por tanto, para lograr establecer comunicación entre estos PCs, sería necesario incluir en la topología de la red un enrutador o un Switch de capa 3 (Switch Multicapa), los cuales tienen la funcionalidad intrínseca de enrutamiento entre VLANs, para así lograr comunicación entre todos los PCs.

Ilustración 23. Resultado aplicar ping en diferentes PC



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

El ping entre los tres switch es exitoso pues las direcciones ip que se les configuro están en una misma vlan y todos cuentan con puertos trunk lo que permite el paso de paquetes, pero se tiene que resaltar que en el SW-AA hay una perdida de paquete.

Ilustración 24. Resultado hacer ping de SW-AA a SW-BB y SW-CC



```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface

SW-AA>enable
SW-AA#ping 190.108.99.2

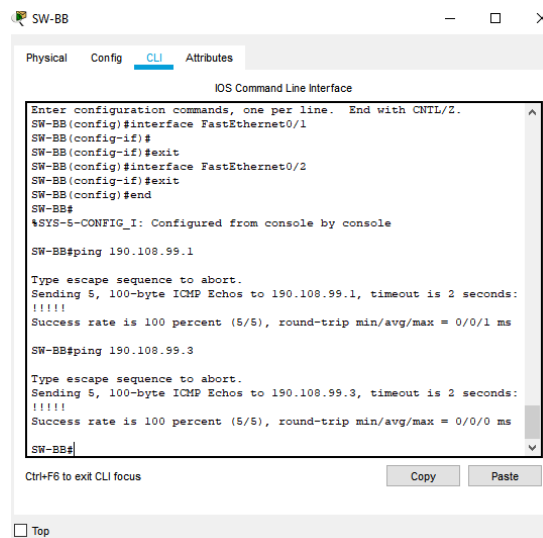
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/2/7 ms

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 60 percent (3/5), round-trip min/avg/max = 0/0/2 ms

SW-AA#
```

Ilustración 25. Resultado hacer ping de SW-BB a SW-AA y SW-CC



```
SW-BB
Physical Config CLI Attributes
IOS Command Line Interface

Enter configuration commands, one per line. End with CNTL/Z.
SW-BB (config)#interface FastEthernet0/1
SW-BB (config-if)#
SW-BB (config-if)#exit
SW-BB (config)#interface FastEthernet0/2
SW-BB (config-if)#exit
SW-BB (config)#end
SW-BB#
%SYS-5-CONFIG_I: Configured from console by console

SW-BB#ping 190.108.99.1

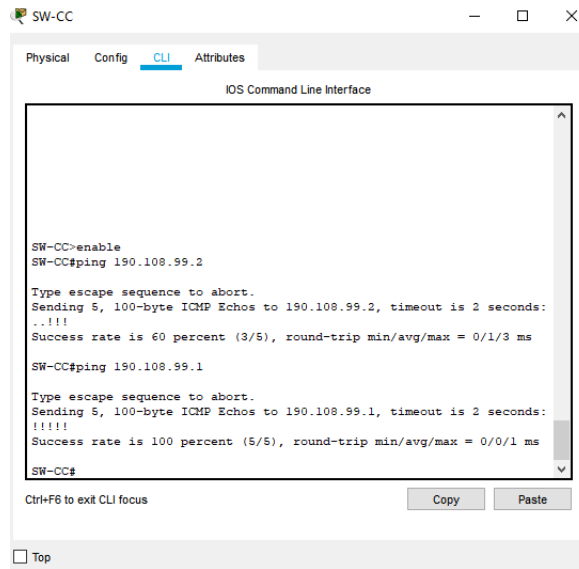
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

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 = 0/0/0 ms

SW-BB#
```

Ilustración 26. Resultado hacer ping de SW-CC a SW-AA y SW-BB



```
SW-CC>enable
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 60 percent (3/5), round-trip min/avg/max = 0/1/3 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

SW-CC#
```

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

Al ejecutar un ping entre un switch y los demás pc tiene éxito, debido a que cada pc está comunicado por sus troncales y las vlans fueron compartidas entre switches, por esta razón se puede efectuar un ping entre ellos.

Ilustración 27. Resultado hacer ping de SW-AA a PC1-PC2-PC3

```
SW-AA#ping 190.108.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.10, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.20.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.20, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

SW-AA#ping 190.108.30.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.30, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#
```

Ilustración 28. Resultado hacer ping de SW-BB a PC4-PC5-PC6

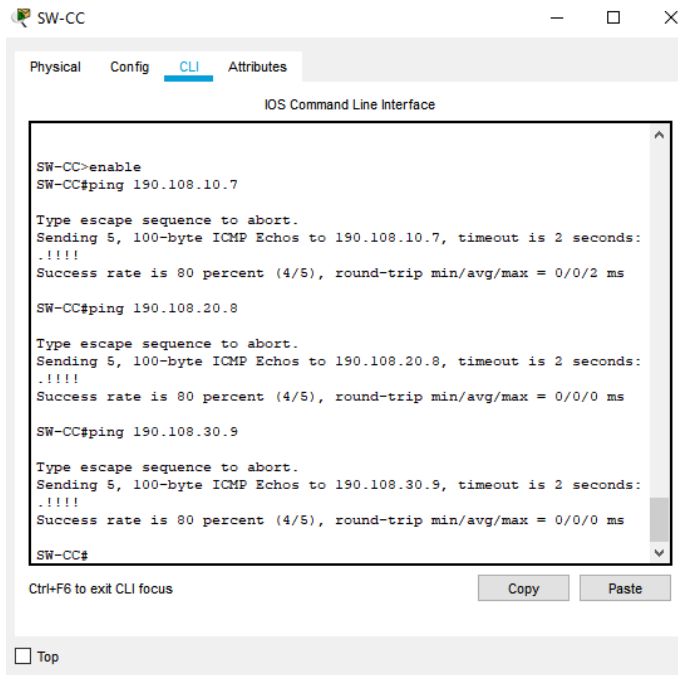
```
SW-BB>enable
SW-BB#ping 190.108.10.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.4, timeout is 2 seconds:
..!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

SW-BB#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-BB#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 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

SW-BB#
```

Ilustración 29. Resultado hacer ping de SW-CC a PC7-PC8-PC9



The screenshot shows a window titled "SW-CC" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following sequence of commands and results:

```
SW-CC>enable
SW-CC#ping 190.108.10.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.7, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/2 ms

SW-CC#ping 190.108.20.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.8, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

SW-CC#ping 190.108.30.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.9, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

SW-CC#
```

At the bottom of the CLI window, there is a "Ctrl+F6 to exit CLI focus" message and "Copy" and "Paste" buttons. Below the CLI window, there is a "Top" button.

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 prácticas construidas a través del curso mediante el uso de herramientas como GNS3, Packet Tracer y SmartLab de Cisco. En el contexto de la configuración de protocolos de enrutamiento dinámico, tales como configuración de enrutamiento IPv4 en interfaces Seriales, FastEthernet y Loopback, en dispositivos de enrutamiento, conmutación y acceso a la red por parte de usuarios finales. Así también, se logran determinar fallos y dar solución a estos, comprobando la configuración y la existencia de conexión lógica entre los dispositivos de las redes propuestas, empleando el protocolo ICMP y analizando el resultado obtenido con comandos show como: show running-config, show ip route, show interfaces trunk, show vtp status, show vlan brief. Entre otros.

En los diferentes módulos de diplomado de profundización en CCNP se abordaron diferentes temas importantes a la hora de configurar topologías de red, por ejemplo en CCNP ROUTE se tocaron temas relacionados a los protocolos como lo son: EIGRP, EBGP OSPF, redistribución de rutas; en el módulo de CCNP SWITCH se trataron diferentes conceptos como operaciones y puertos switches, spanning tree, Vlans y troncales, VTP, configuración de acceso a usuarios

Se aplicaron los conocimientos adquiridos a lo largo del diplomado en escenarios que pueden presentarse en el día a día de un ingeniero de telecomunicaciones encargado de las configuraciones de red de una compañía que utiliza dispositivos Cisco. Entre las características y ventajas que ofrecen los dispositivos Cisco se destaca la intercomunicación entre protocolos de enrutamiento diferentes teniendo en cuenta que la clave es el orden y la configuración de las interfaces y parámetros de los protocolos desplegados.

BIBLIOGRAFÍA

ARIGANELLO. Ernesto, BARRIENTOS SEVILLA. Enrique. Redes Cisco Guía de Estudio para la Certificación CCNP. Segunda Edición. Madrid: Editorial RA-MA. 2014. 369 p.

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYeiNT1InWR0hoMxgBNv1CJ>

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-NT1InWR0hoMxgBNv1CJ>

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

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://onedrive.live.com/?authkey=%21AB%5FLauE9kfAShbE&cid=483D35BEE8610962&id=483D35BEE8610962%212931&parId=483D35BEE8610962%212930&o=OneUp>