

**DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP**

MARLON ANDREY GIL JARAMILLO

**UNIVERSIDAD ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA ELECTRÓNICA
DOSQUEBRADAS
2020**

**DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP**

MARLON ANDREY GIL JARAMILLO

**Diplomado de Opción de Grado Presentado Para Optar El Título de
Ingeniero Electrónico**

DIRECTOR

MSc. GERARDO GRANADOS ACUÑA

**UNIVERSIDAD ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI
INGENIERÍA ELECTRÓNICA
DOSQUEBRADAS**

2020

FIRMAS DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

DOSQUEBRADAS, 22 de mayo de 2020

AGRADECIMIENTOS

Agradezco a Dios por permitir estudiar esta carrera la cual considero que es mi vocación y darme los medios de trabajo y pagar mis estudios. Agradezco a mi familia por el apoyo en este proceso y dedico este logro a mis padres.

CONTENIDO

FIRMAS DE ACEPTACIÓN.....	3
AGRADECIMIENTOS	4
CONTENIDO.....	5
LISTA DE TABLAS	6
LISTA DE FIGURAS	7
GLOSARIO.....	8
RESUMEN	9
ABSTRACT.....	10
INTRODUCCIÓN.....	11
DESARROLLO	12
Escenario 1	12
Escenario 2	20
Configurar VTP	20
B. Agregar VLANs y asignar puertos.....	27
C. Configurar las direcciones IP en los Switches.	31
CONCLUSIONES.....	38
REFERENCIAS BIBLIOGRÁFICAS	39

LISTA DE TABLAS

Tabla 1. Configuración de Routers	12
Tabla 2. Configuraciones ip y VLAN	30
Tabla 3. Configuraciones ip em Switchs	32

LISTA DE FIGURAS

Figura 1. Escenario 1.....	12
Figura 2. Esquema En CISCO Packet Tracer	13
Figura 3. R1 - Show ip roue	14
Figura 4. R1 - Show ip route.....	15
Figura 5. Configuración Show ip route R2.....	16
Figura 6. Configuración Show ip route R3	17
Figura 7. Actualización Por Show ip route R3	18
Figura 8. Actualización Por Show ip route R4.....	19
Figura 9. Escenraio 2.....	20
Figura 10. Esquema En CISCO Packet Tracer	20
Figura 11. SW-AA Show vtp status.....	21
Figura 12. SW-BB Show vtp status	22
Figura 13 SW-CC Show vtp status.....	23
Figura 14. Trunk SW-AA	24
Figura 15 Trunk SW-BB	24
Figura 16. Show interfaces Trunk SW-AA	25
Figura 17. Enlace Trunk SW-BB	26
Figura 18. Enlace Trunk SW-CC	26
Figura 19. VLAN 10 SW-AA	27
Figura 20. VLAN 10 SW-BB	28
Figura 21. VLAN 10 SW-BB	29
Figura 22. Ping de PC1 a PC3.....	32
Figura 23. Ping de PC1 a PC4.....	32
Figura 24. Ping de PC5 a PC8.....	33
Figura 25. Ping de PC5 a PC9.....	33
Figura 26. Ping de PC9 a PC2.....	34
Figura 27. Ping de PC9 a PC3.....	34
Figura 28. Ping de SW-AA a SW-BB y SW-CC	35
Figura 29. Ping de SW-AA a SW-BB y SW-CC	35
Figura 30. Ping de SW-AA a SW-BB y SW-CC	36
Figura 31. Ping SW-AA a PC1 / PC2 / PC3.....	36
Figura 32. Ping SW-CC a PC7 / PC8 / PC9.....	37

GLOSARIO

Sumarizar: es resumir los bits comunes de varias redes. De esa forma obtenemos una red con prefijo (el cual indicará los bits comunes, que forman la parte de red). Por supuesto hemos de tener en cuenta que para usar Supernetting tendremos que implementar un protocolo de enrutamiento dinámico sin clase que soporte VLSM y CIDR, como por ejemplo OSPF, RIP v2, IS-IS.

Router: es un dispositivo que opera en capa tres de nivel de 3. Así, permite que varias redes u ordenadores se conecten entre sí y, por ejemplo, compartan una misma conexión de Internet. Un router se vale de un protocolo de enrutamiento, que le permite comunicarse con otros enrutadores o encaminadores y compartir información entre sí para saber cuál es la ruta más rápida y adecuada para enviar datos.

Switch: es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).

Máscara De Subred: ayuda a identificar esas direcciones a simple vista iguales con un código que permitirá leerlas de manera más sencilla. Está compuesta del valor 255 para lo que está igual y del valor 0 cuando se diferencia. Es algo similar a 255.255.255.0.

Topología De Red: es la forma en que se conectan las computadoras para intercambiar datos entre sí. Es como una familia de comunicación, que define cómo se va a diseñar la red tanto de manera física, como de manera lógica.

RESUMEN

El curso de CISCO CCNP (Cisco Certified Network Professional), consta de etapas como (ROUTE) and (SWITCH), los cuales ofrecen conocimientos aplicativos a la conmutación, el enrutamiento de las redes. Estas competencias son Propias en el mundo de la electrónica como extensión a las ramas de conocimiento de la ingeniería en sistemas, ingeniería electrónica y afines. Se realiza la práctica aplicando los conocimientos adquiridos en Redes, tanto en Router como en Switching, evidenciando el manejo de los comandos adecuados para las respectivas configuraciones, se aplican las instrucciones necesarias para verificar conectividad e identificar fallas y proponer soluciones. La electrónica y las telecomunicaciones van de la mano ya que son dependientes, por todo lo que es el Hardware y las configuraciones del dispositivo.

El escenario 1, consta de configuraciones necesarias para el enrutamiento, el cual sirve para encontrar un camino entre las redes para garantizar la conectividad entre las topologías. Cabe denotar que la conmutación es la acción de establecer una vía, un camino, de extremo a extremo entre dos puntos, un emisor (Tx) y un receptor (Rx) a través de nodos o equipos de transmisión. En este escenario se evidencia cada una de estas directrices para la configuración de un Router y cómo por medio de comandos como show ip route se aprecia la comunicación entre ellos.

El Escenario 2, postula una configuración de Switch con VTP para las actualizaciones VLAN. Se emplea el comando show VTP status para verificar las configuraciones. Se configura el enlace troncal y se verifica respectivamente por medio del comando show interfaces trunk. Se agregan las VLAN correspondientes y se configuran sus respectivas ip; por último, se verifica la conectividad de extremo a extremo donde se procede a hacer un análisis y se explica como se pueden corregir errores de estas conexiones.

ABSTRACT

Through the activities applied to routing and switching, I have been able to demonstrate the knowledge acquired during the CISCO CCNP course, obtaining more solid skills in the world of networks. All the competencies evidenced by the activities recorded in this document, allow an integration between systems engineering and electronic engineering.

The proposed scenario to demonstrate the knowledge in routing, the necessary commands are carried out to configure the routers and verify the respective connections using the show ip route command, guaranteeing domain in this field of networks.

The scenario that shows the practice and knowledge in Switching, the respective VTP configurations and trunks are made through Switch with dynamic auto and the others with dynamic desirable, in order to be verified through the show interfaces trunk instruction. Subsequently, add the VLANs and IPs required to verify the connection and offer an analysis of these and possible solutions.

Networks allow people to communicate, collaborate, and interact in many ways. Therefore, the Networking application increases connectivity. Networks are used to access web pages, talk on IP phones, participate in video conferences, compete in interactive games, make purchases on the Internet, complete online courses and more. Electronics is applied and networks depend on the development of this science to implement different protocols and guarantee connections through developed hardware.

INTRODUCCIÓN

El diplomado CCNP fortalece los conocimientos sobre la importancia de establecer niveles de seguridad básicos mediante la definición de criterios y políticas de seguridad aplicadas a diversos escenarios de red, bajo el uso de estrategias hardware y software, con el fin de proteger la integridad de la información frente a cualquier tipo de ataque que se pueda presentar en un instante de tiempo determinado.

Se adquieren los conocimientos necesarios para el diseño de redes escalables mediante el uso del modelo jerárquico de tres niveles, con el fin de optimizar el rendimiento de la red e incorporar de manera adecuada el uso de tecnologías y protocolos de conmutación mejorados.

Se desarrolla la capacidad de configurar y administrar dispositivos de Networking orientados al diseño de redes escalables y de conmutación, mediante el estudio del modelo OSI, la arquitectura TCP/IP, y el uso de recursos y herramientas en función de los protocolos y servicios de la capa física como soporte de las comunicaciones a través de las redes de datos estableciendo alternativas a problemas de interconectividad.

Cada práctica evidencia el manejo de los conocimientos adquiridos de Router and Switching.

DESARROLLO

Escenario 1

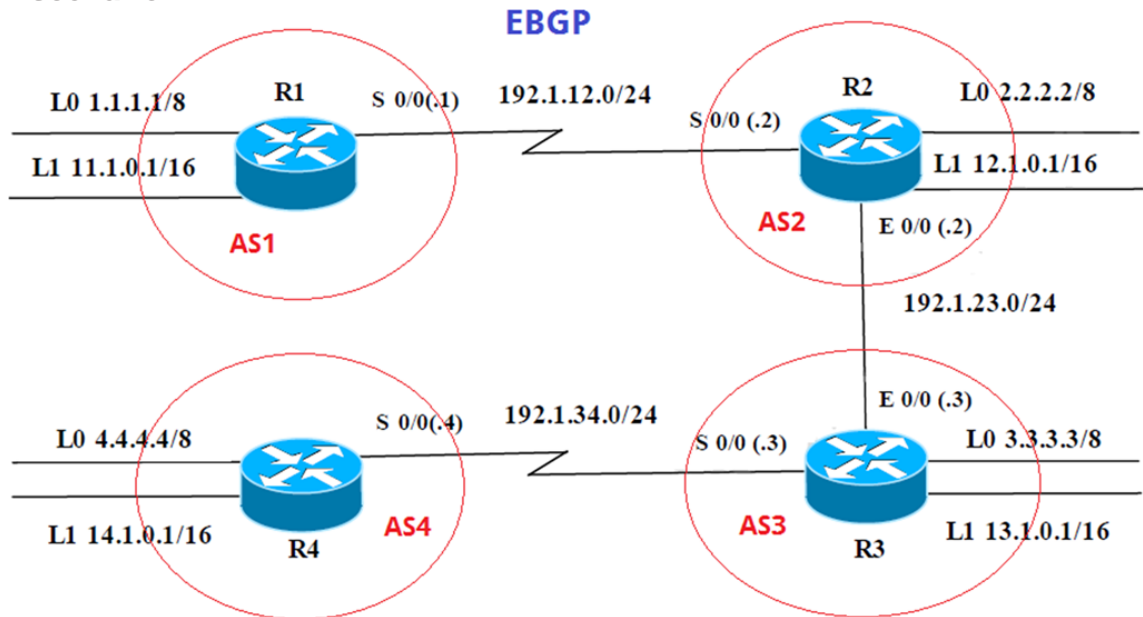


Figura 1. Escenario 1

Información para configuración de los 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

Tabla 1. Configuración de Routers

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.

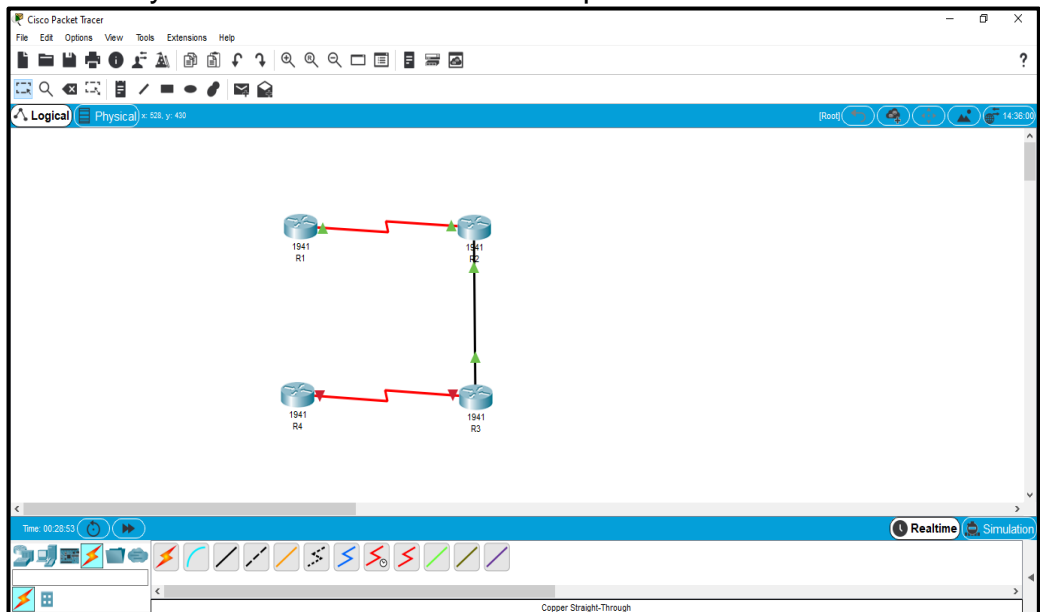


Figura 2. Esquema En CISCO Packet Tracer

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

```
R2#configure terminal
R2 (config)#interface Loopback 0
R2 (config-if)#ip address 2.2.2.2 255.0.0.0
R2 (config-if)#interface Loopback 1
R2 (config-if)#ip address 12.1.0.1 255.255.0.0
R2 (config-if)#interface serial 0/0/0
R2 (config-if)#ip address 192.1.12.2 255.255.255.0
```

```

R2 (config-if) #no shutdown
R2 (config-if) #interface gigabitEthernet 0/0
R2 (config-if) #ip address 192.1.23.2 255.255.255.0
R2 (config-if) #no shutdown
R2 (config-if) #exit
R2 (config) #router bgp 2
R2 (config-router) #bgp router-id 33.33.33.33
R2 (config-router) #network 2.0.0.0 mask 255.0.0.0
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

```

Ahora se evidencia la conexión entre los 2 routers ejecutando el comando:

show ip route

R1

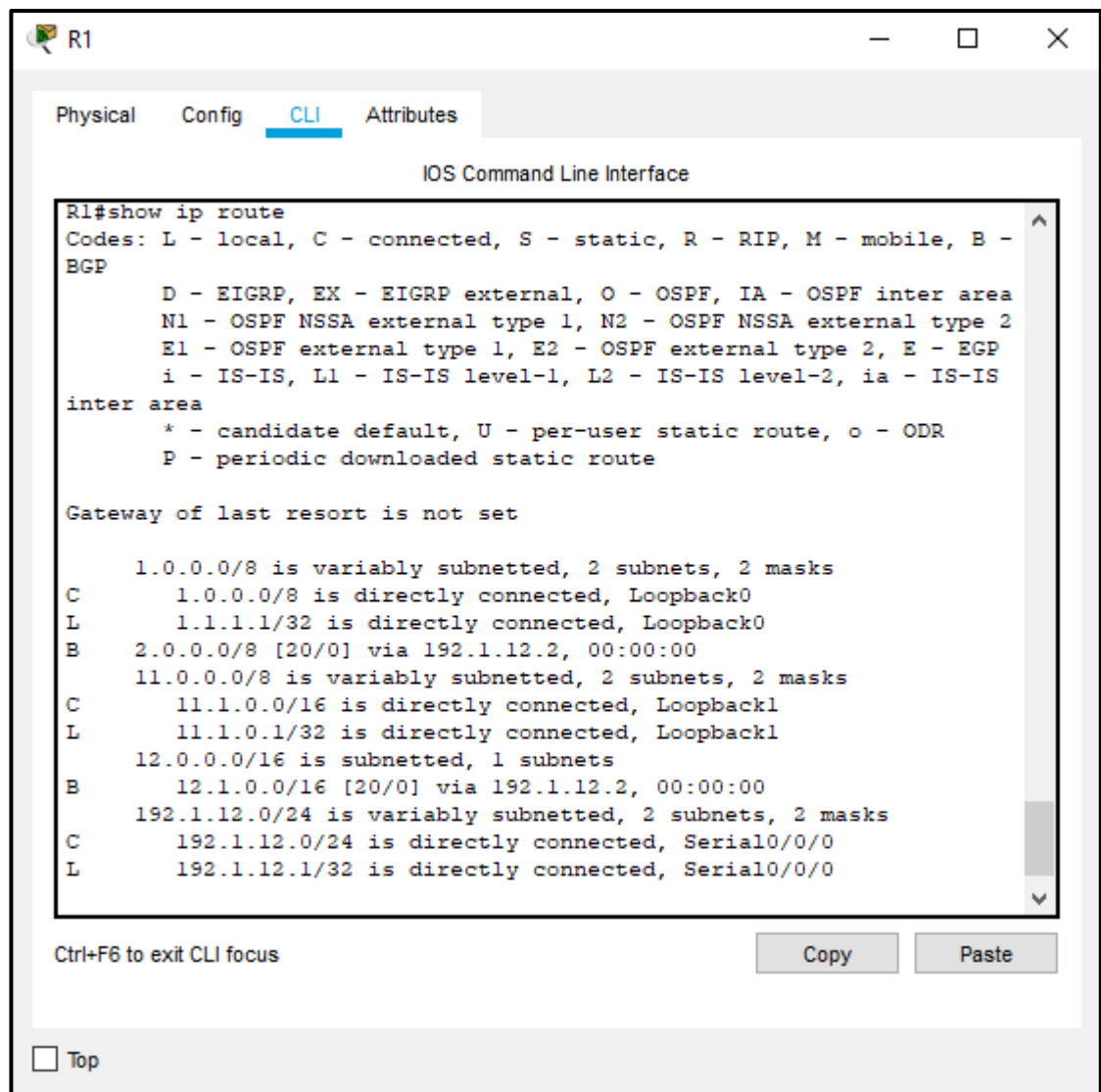
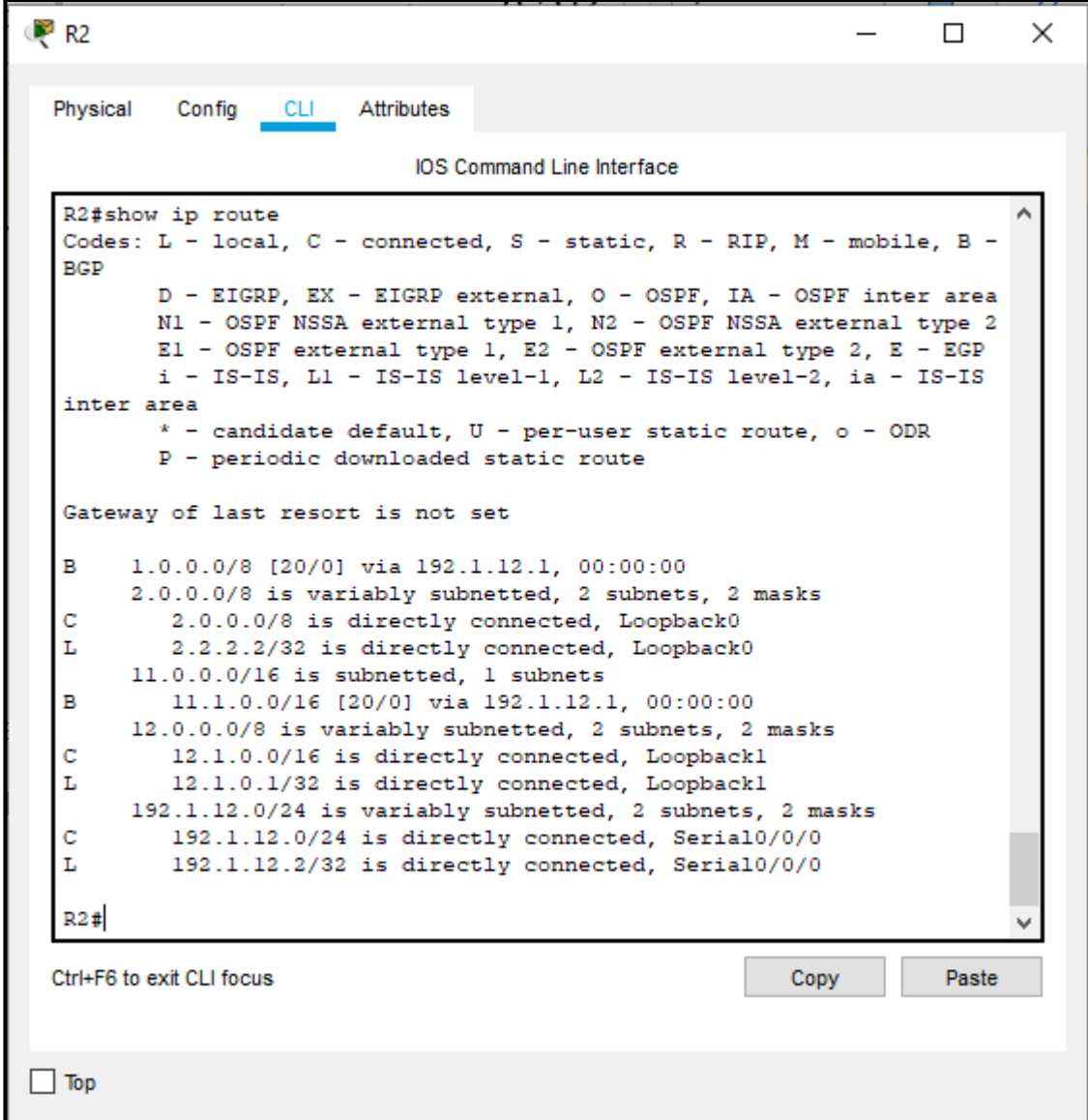


Figura 3. R1 - Show ip route

R2



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

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:00:00
     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
     11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0/16 [20/0] via 192.1.12.1, 00:00:00
     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
     192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.12.0/24 is directly connected, Serial0/0/0
L    192.1.12.2/32 is directly connected, Serial0/0/0

R2#
```

Figura 4. R1 - Show ip route

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#configure terminal
R2(config)#router bgp 2
```

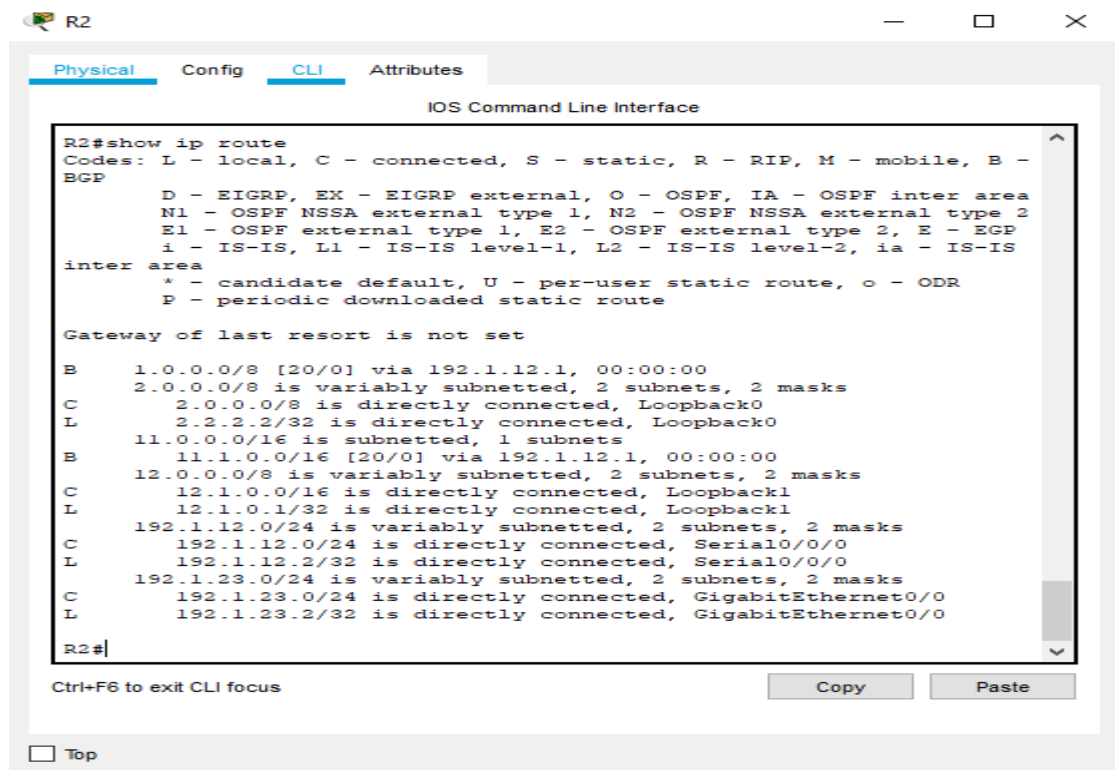
```
R2(config-router)#network 192.1.23.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.23.3 remote-as 3
```

```
R3#configure terminal
```

```
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 gigabitEthernet 0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#interface serial 0/0/1
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router bgp 3
R3(config-router)#bgp router-id 33.33.33.33
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
```

Ahora ejecuta el comando show ip route en:

R2



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

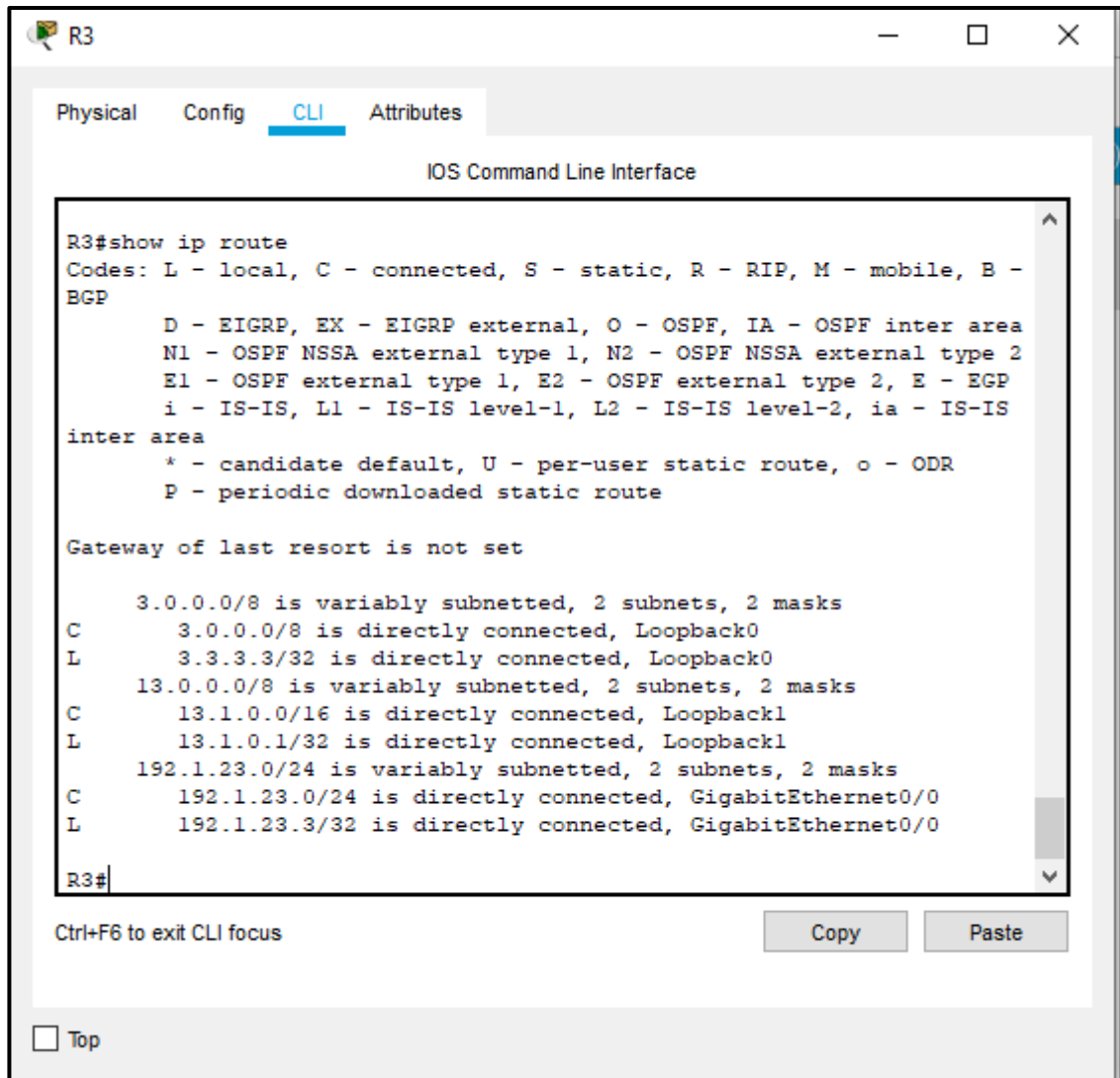
Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:00:00
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
L    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0/16 [20/0] via 192.1.12.1, 00:00:00
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
L    192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.12.0/24 is directly connected, Serial0/0/0
L    192.1.12.2/32 is directly connected, Serial0/0/0
C    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.23.0/24 is directly connected, GigabitEthernet0/0
L    192.1.23.2/32 is directly connected, GigabitEthernet0/0

R2#
```

Figura 5. Configuración Show ip route R2

R3



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

Gateway of last resort is not set

      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
      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
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.23.0/24 is directly connected, GigabitEthernet0/0
L       192.1.23.3/32 is directly connected, GigabitEthernet0/0

R3#
```

Figura 6. Configuración Show ip route R3

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#configure terminal
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
```

```

R4#configure terminal
R4 (config) #interface Loopback 0
R4 (config-if) #ip address 4.4.4.4 255.0.0.0
R4 (config-if) #interface Loopback 1
R4 (config-if) #ip address 14.1.0.1 255.255.0.0
R4 (config-if) #interface serial 0/0/0
R4 (config-if) #ip address 192.1.34.4 255.255.255.0
R4 (config-if) #no shutdown
R4 (config-if) #exit
R4 (config) #router bgp 4
R4 (config-router) #bgp router-id 66.66.66.66
R4 (config-router) #network 4.0.0.0 mask 255.0.0.0
R4 (config-router) #network 14.1.0.0 mask 255.255.0.0
R4 (config-router) #network 192.1.34.0 mask 255.255.255.0
R4 (config-router) #neighbor 192.1.34.3 remote-as 3

```

Ahora se configuran los parámetros para los vecinos:

```

R3#configure terminal
R3 (config) #ip route 4.0.0.0 255.0.0.0 192.1.34.4
R3 (config) #router bgp 3
R3 (config-router) #no neighbor 192.1.34.4
R3 (config-router) #no network 3.0.0.0 mask 255.0.0.0
R3 (config-router) #neighbor 4.4.4.4 remote-as 4
R3 (config-router) #neighbor 4.4.4.4 update-source loopback 0
R3 (config-router) # neighbor 4.4.4.4 ebgp-multihop

```

```

R4 (config) #ip route 3.0.0.0 255.0.0.0 192.1.34.3
R4 (config) #router bgp 4
R4 (config-router) #no neighbor 192.1.34.3
R4 (config-router) #neighbor 3.3.3.3 remote-as 4
R4 (config-router) #neighbor 3.3.3.3 update-source loopback 0
R4 (config-router) # neighbor 3.3.3.3 ebgp-multihop

```

Ahora ejecutando el comando show ip route, muestra que R3 se actualiza la tabla de enrutamiento y esta conectado con R4.



Figura 7. Actualización Por Show ip route R3

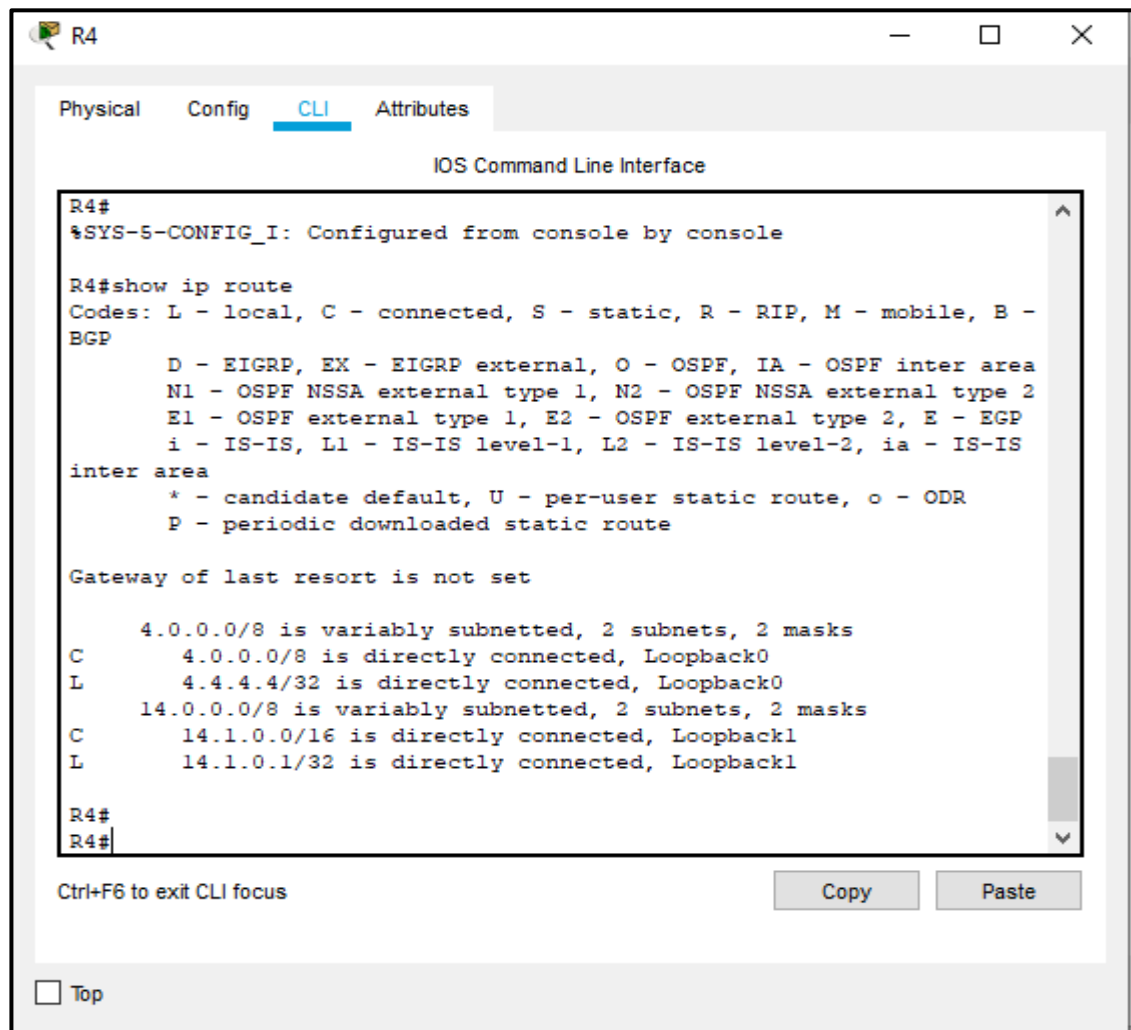


Figura 8. Actualización Por Show ip route R4

Escenario 2

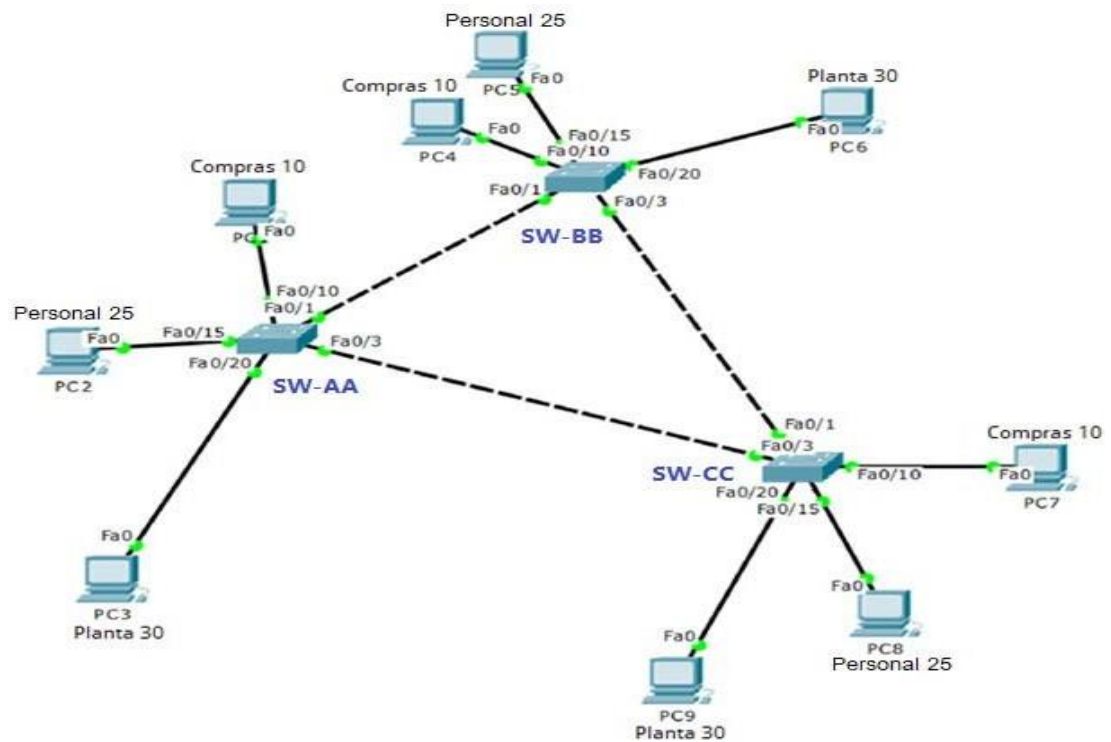


Figura 9. Escenario 2

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.

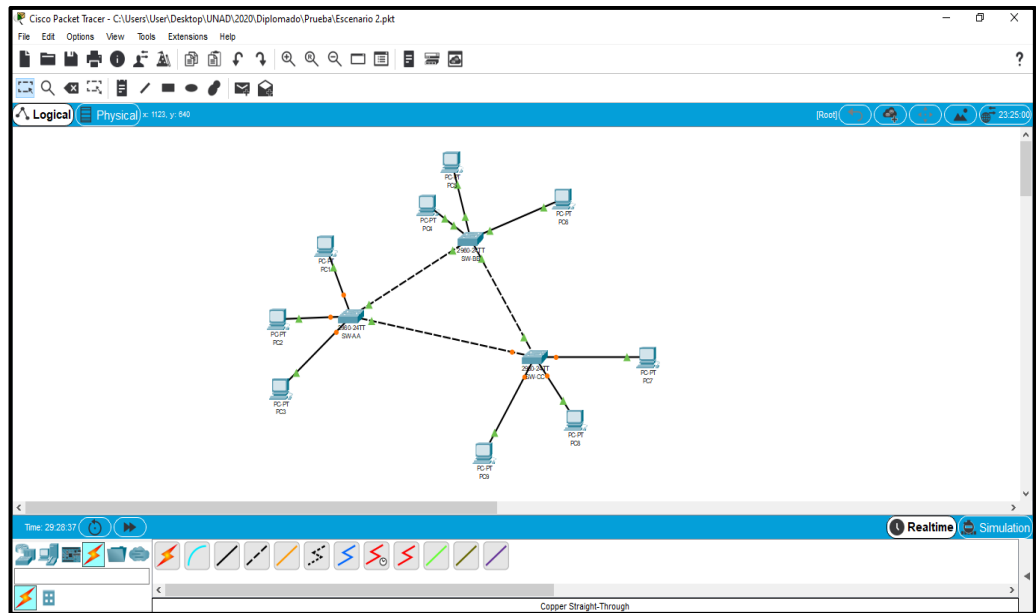


Figura 10. Esquema En CISCO Packet Tracer

```

SW-AA#configure terminal
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

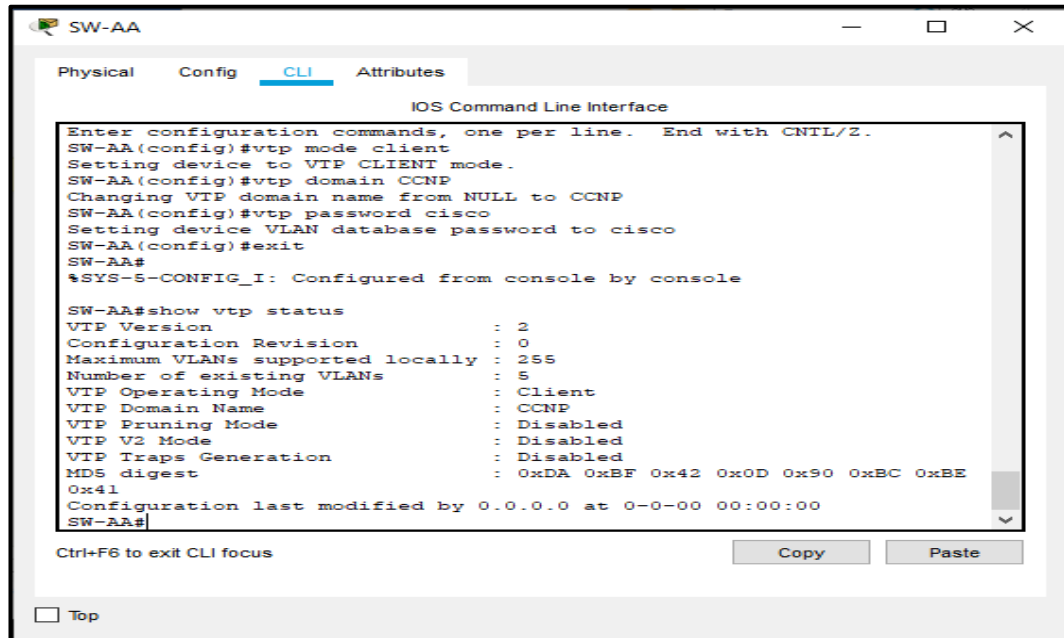
SW-BB#configure terminal
SW-BB(config)#vtp mode server
Setting device to VTP SERVER mode.
SW-BB(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-BB(config)#vtp password cisco
Setting device VLAN database password to cisco

SW-CC #configure terminal
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-BB(config)#vtp password cisco
Setting device VLAN database password to cisco

```

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

SW-AA

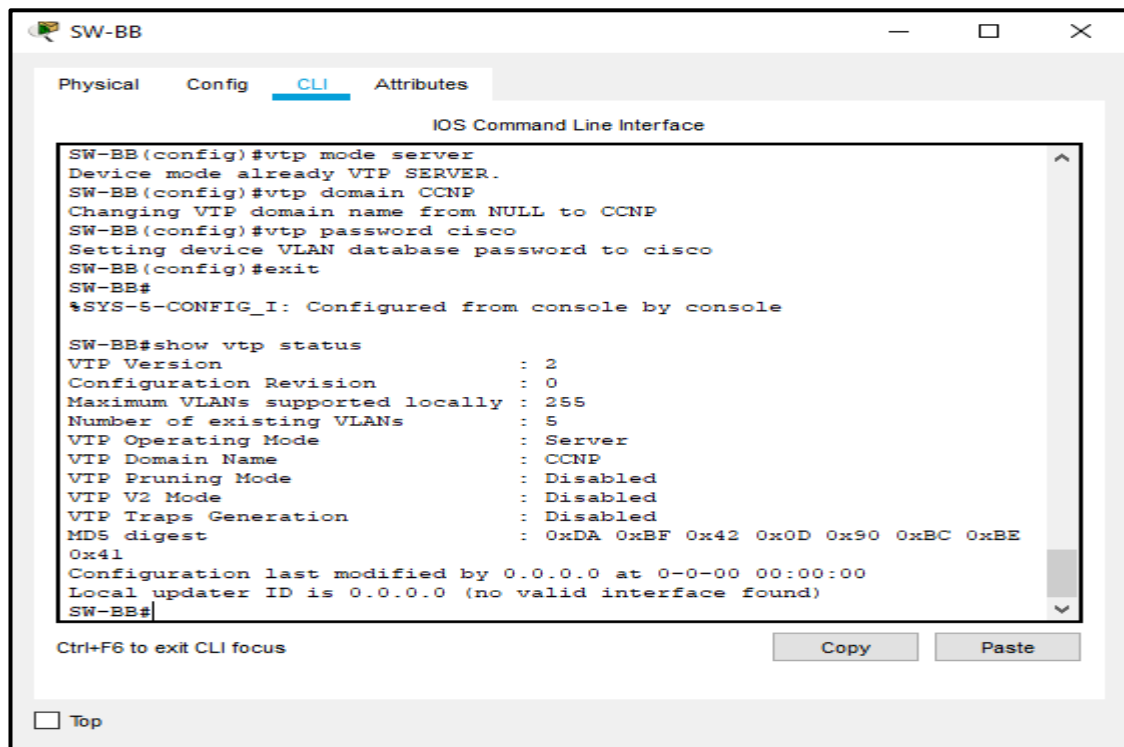


```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#vtp mode client
Setting device to VIP CLIENT mode.
SW-AA(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-AA(config)#vtp password cisco
Setting 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
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-AA#
```

Figura 11. SW-AA Show vtp status

SW-BB



```
SW-BB
Physical Config CLI Attributes
IOS Command Line Interface
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)#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
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
Local updater ID is 0.0.0.0 (no valid interface found)
SW-BB#
```

Figura 12. SW-BB Show vtp status

SW-CC

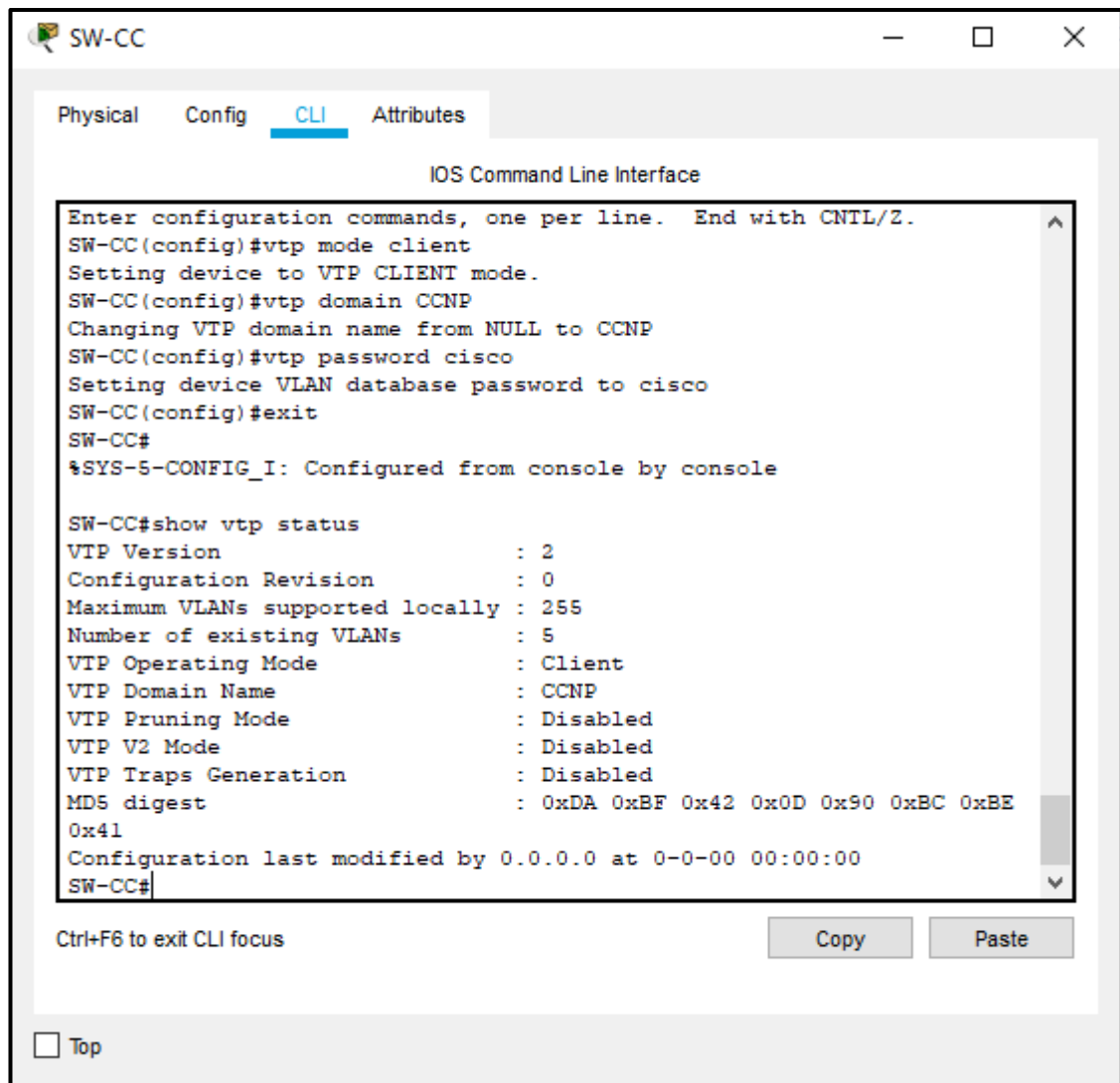


Figura 13. SW-BB Show vtp status

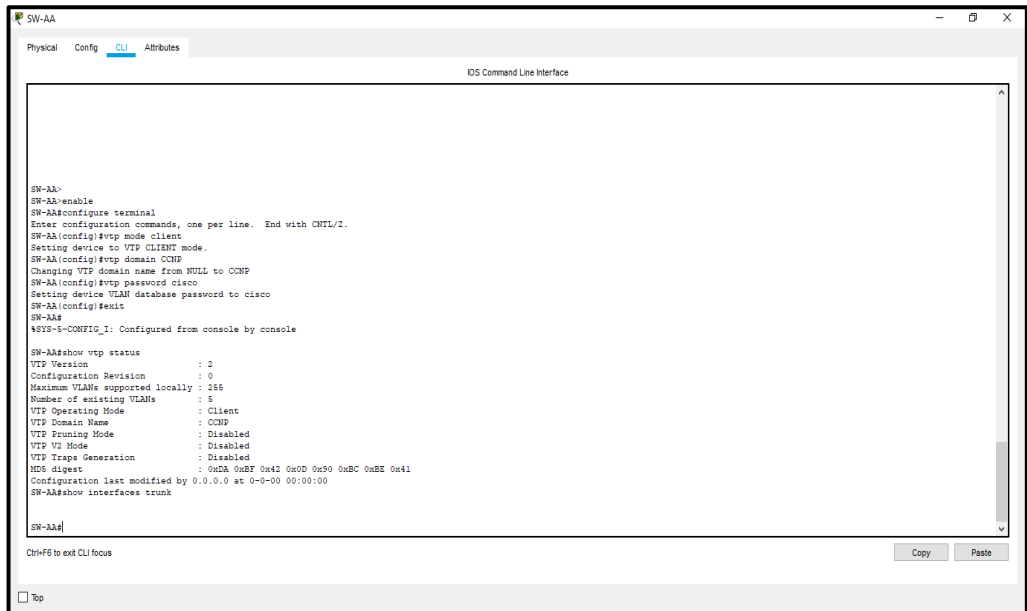
A. Configurar DTP (Dynamic Trunking Protocol)

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

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

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

SW-AA



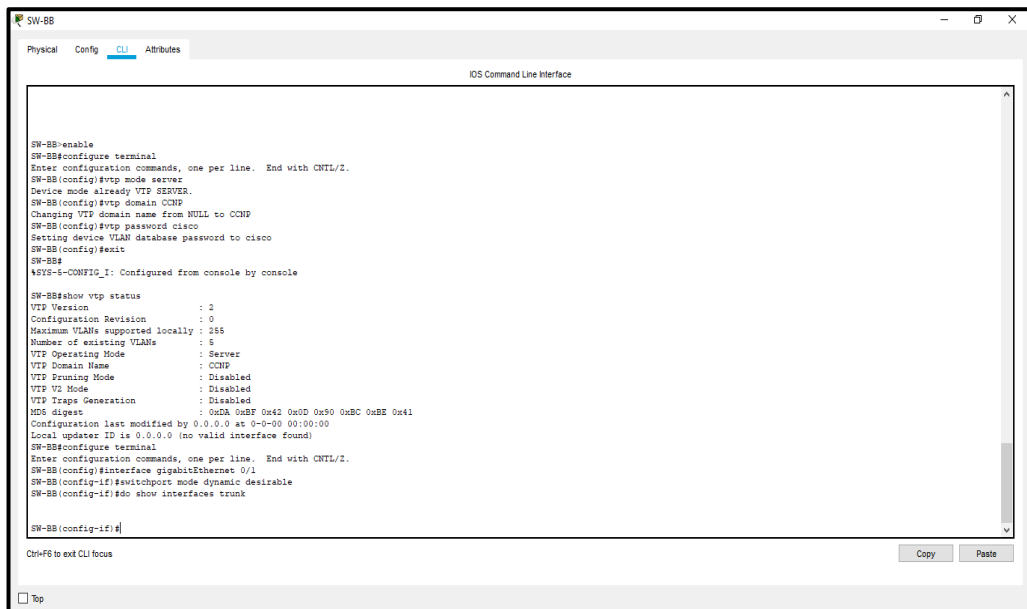
```
SW-AA>
SW-AA#enable
SW-AA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-AA(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-AA(config)#vtp password cisco
Setting device VLAN 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
MDS digest           : 0x2B 0xBF 0x43 0xD0 0x50 0xBC 0xBE 0x11
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SW-AA#show interfaces trunk

SW-AA#
```

Figura 14. Trunk SW-AA

SW-BB



```
SW-BB>
SW-BB#enable
SW-BB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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)#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
MDS digest           : 0xDA 0xBF 0x43 0xD0 0x50 0xBC 0xBE 0x11
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#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#interface gigabitEthernet 0/1
SW-BB(config-if)#switchport mode dynamic desirable
SW-BB(config-if)#do show interfaces trunk

SW-BB (config-if)#
```

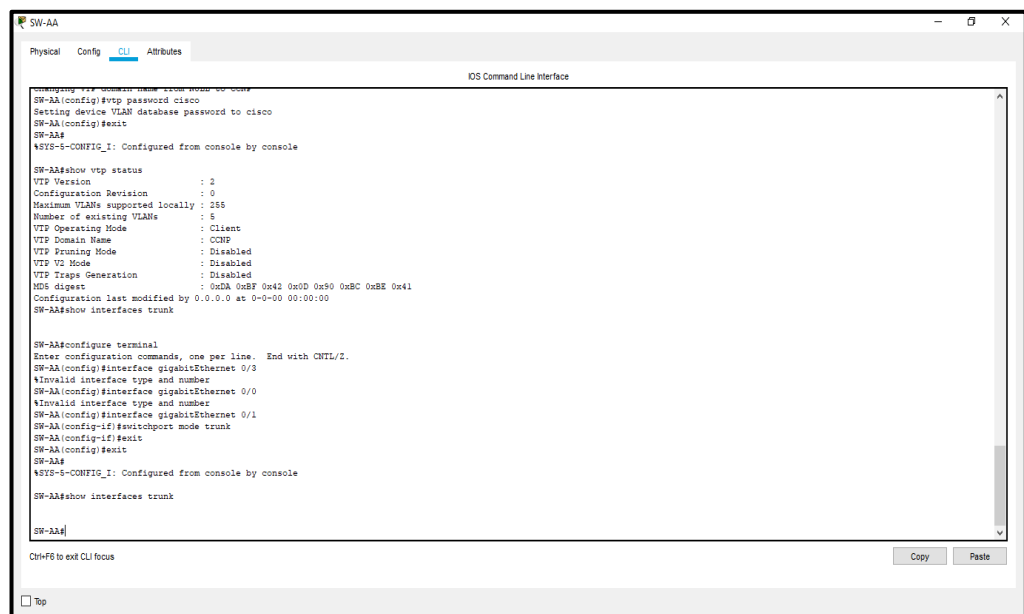
Figura 15. Trunk SW-BB

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

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

SW-AA



```
SW-AA  
Physical Config CLI Attributes  
IOS Command Line Interface  
Changing vtp domain name from none to cisco  
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  
MDS digest : 0x0A 0x0E 0x41 0x0D 0x50 0x8C 0x8E 0x41  
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00  
SW-AA#show interfaces trunk  
  
SW-AA#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
SW-AA(config)#interface gigabitEthernet 0/3  
%Invalid interface type and number  
SW-AA(config)#interface gigabitEthernet 0/0  
%Invalid interface type and number  
SW-AA(config)#interface gigabitEthernet 0/1  
SW-AA(config-if)#switchport mode trunk  
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  
  
SW-AA#
```

Figura 16. Show interfaces Trunk SW-AA

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

```
SW-BB#configure terminal  
SW-BB (config)#interface gigabitEthernet 0/1  
SW-BB (config-if)#switchport mode trunk
```

SW-BB

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

SW-BB>enable
SW-BB(config)#vtp password cisco
Setting device VLAN database password to cisco
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 : 155
Number of existing VLANs : 5
VTP Operating Mode   : Server
VTP Domain Name     : CNRP
VTP Pruning Mode    : Disabled
VTP V2 Mode         : Disabled
VTP Traps Generation : Disabled
MDS digest          : 0x0A 0x0F 0x43 0x0D 0x50 0xBC 0x8E 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#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#interface gigabitEthernet 0/1
SW-BB(config-if)#switchport mode dynamic desirable
SW-BB(config-if)#do show interfaces trunk

SW-BB(config-if)#exit
SW-BB(config)#interface gigabitEthernet 0/1
SW-BB(config-if)#switchport mode trunk
SW-BB(config-if)#exit
SW-BB(config)#exit
SW-BB#
%SYS-5-CONFIG_I: Configured from console by console

SW-BB#show interfaces trunk

SW-BB#
Ctrl+F6 to exit CLI focus
Copy Paste
Top
```

Figura 17. Enlace Trunk SW-BB

SW-CC

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

SW-CC>enable
SW-CC#configure terminal
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 CNRP
Changing VTP domain name from NULL to CNRP
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 : 155
Number of existing VLANs : 5
VTP Operating Mode   : Client
VTP Domain Name     : CNRP
VTP Pruning Mode    : Disabled
VTP V2 Mode         : Disabled
VTP Traps Generation : Disabled
MDS digest          : 0x0A 0x0F 0x43 0x0D 0x50 0xBC 0x8E 0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SW-CC#show interfaces trunk

SW-CC#
SW-CC#
Ctrl+F6 to exit CLI focus
Copy Paste
Top
```

Figura 18. Enlace Trunk SW-CC

B. Agregar VLANs y asignar puertos.

1. 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
```

2. Verifique que las VLANs han sido agregadas correctamente.

SW-AA

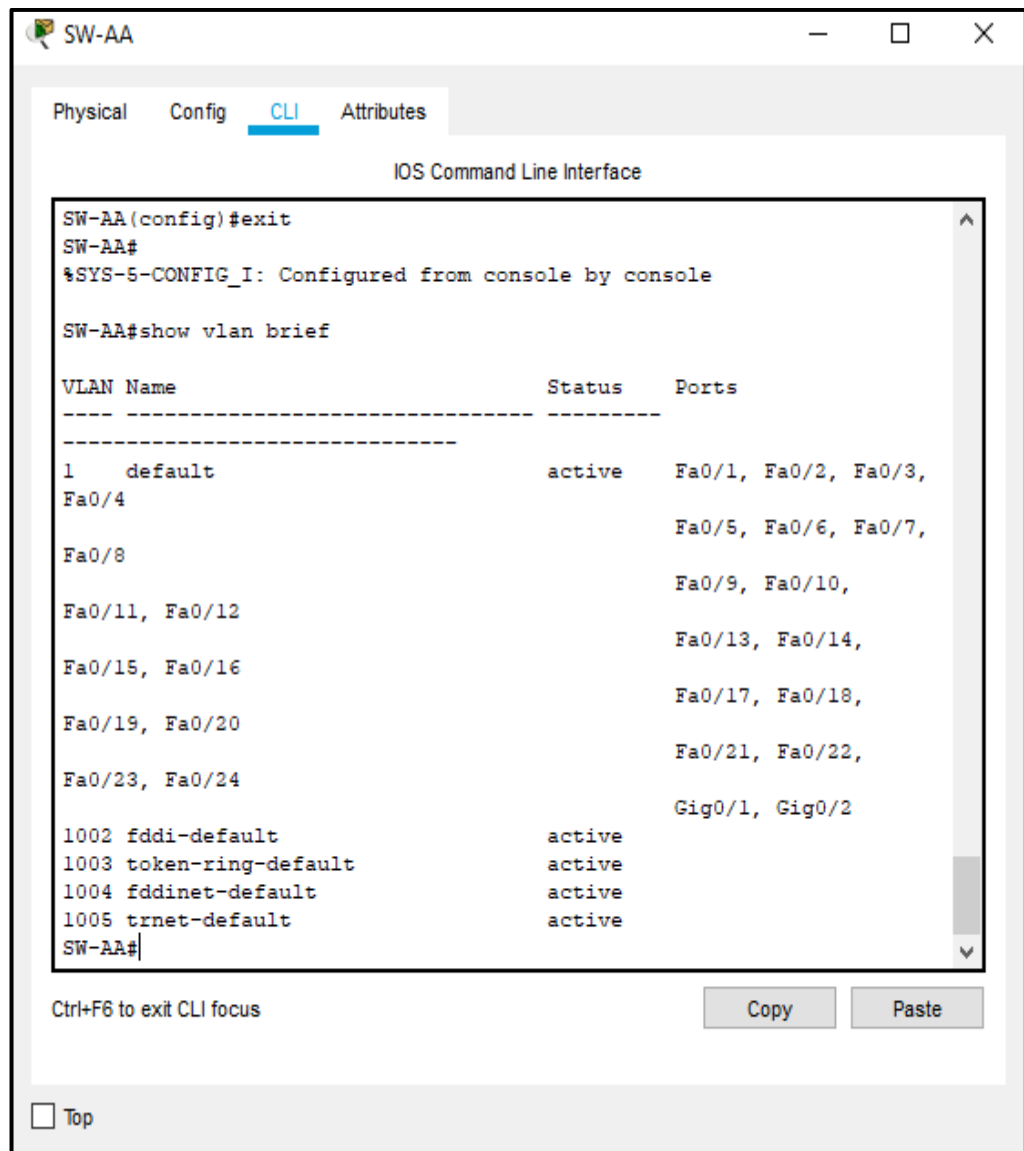
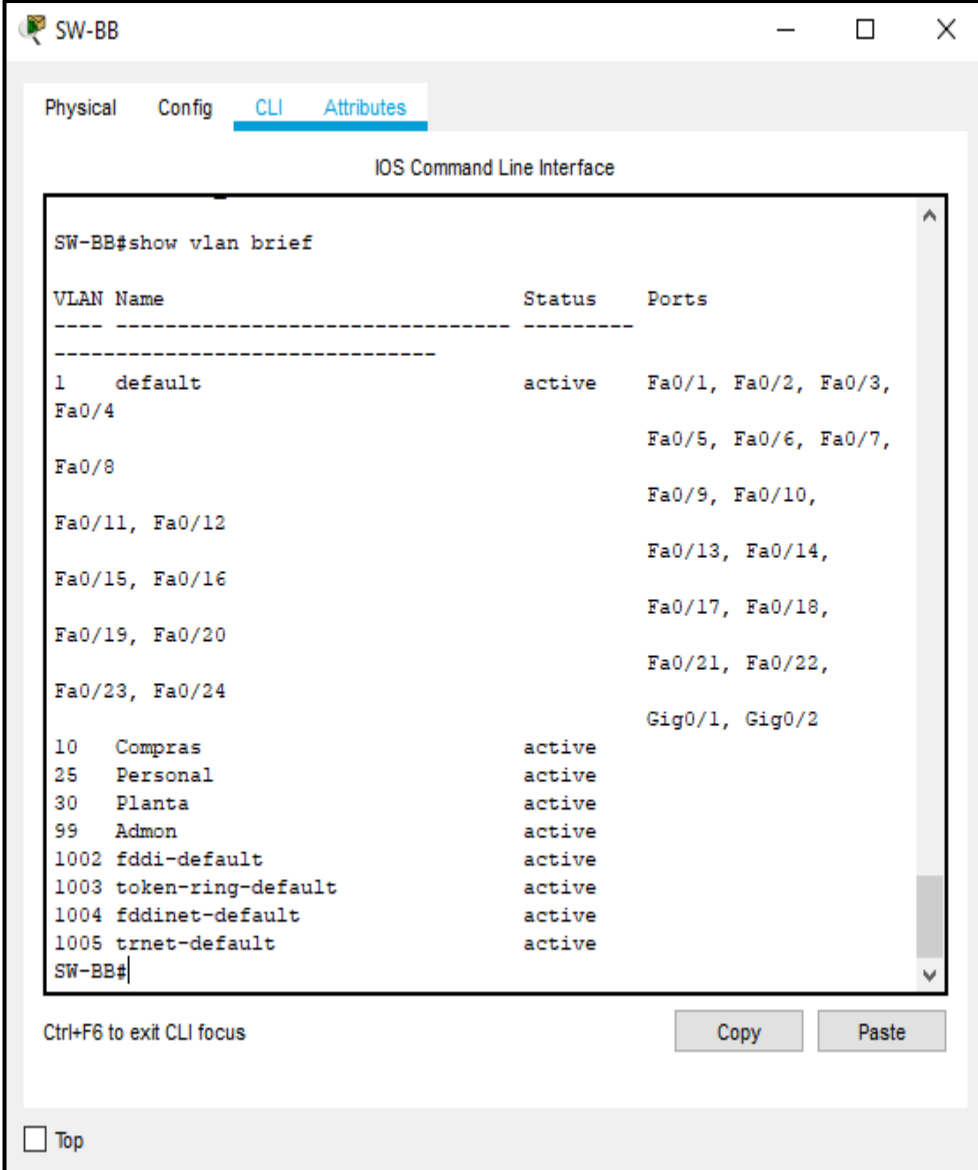


Figura 19. VLAN 10 SW-AA

SW-BB



SW-BB

Physical Config **CLI** Attributes

IOS Command Line Interface

```
SW-BB#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, 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

Figura 20. VLAN 10 SW-BB

SW-CC

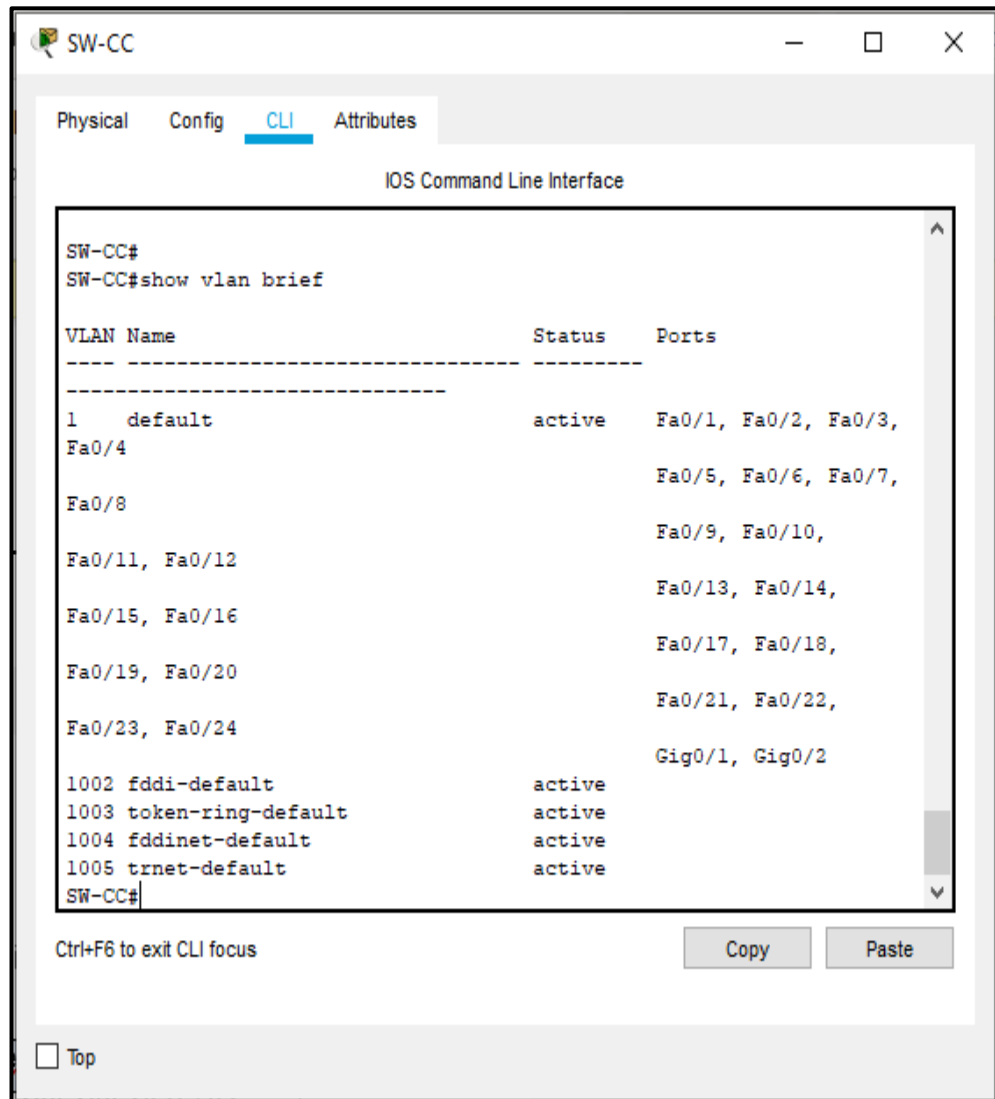


Figura 21. VLAN 10 SW-CC

3. Asocie los puertos a las VLAN y configure 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

X = número de cada PC particular

Tabla 2. Configuraciones ip y VLAN

4. Configure el puerto F0/10 en modo de acceso para SW-AA, SW-BB y SW-CC y asígnelo a la VLAN 10.
5. 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.

```
SWT1#configure terminal
SWT1 (config)#interface fastEthernet 0/10
SWT1 (config-if)#switchport mode access
SWT1 (config-if)#switchport access vlan 10
SWT1 (config)#interface fastEthernet 0/15
SWT1 (config-if)#switchport mode access
SWT1 (config-if)#switchport access vlan 20
SWT1 (config)#interface fastEthernet 0/20
SWT1 (config-if)#switchport mode access
SWT1 (config-if)#switchport access vlan 30
```

```
SWT2#configure terminal
SWT2 (config)#interface fastEthernet 0/10
SWT2 (config-if)#switchport mode access
SWT2 (config-if)#switchport access vlan 10
SWT2 (config)#interface fastEthernet 0/15
SWT2 (config-if)#switchport mode access
SWT2 (config-if)#switchport access vlan 25
SWT2 (config)#interface fastEthernet 0/20
SWT2 (config-if)#switchport mode access
SWT2 (config-if)#switchport access vlan 30
```

```
SWT3#configure terminal
SWT3 (config)#interface fastEthernet 0/10
SWT3 (config-if)#switchport mode access
SWT3 (config-if)#switchport access vlan 10
SWT3 (config)#interface fastEthernet 0/15
SWT3 (config-if)#switchport mode access
SWT3 (config-if)#switchport access vlan 20
SWT3 (config)#interface fastEthernet 0/20
SWT3 (config-if)#switchport mode access
SWT3 (config-if)#switchport access vlan 30
```

```
PC1: ip address 190.108.10.1 255.255.255.0
PC2: ip address 190.108.20.2 255.255.255.0
PC3: ip address 190.108.30.3 255.255.255.0
PC4: ip address 190.108.10.4 255.255.255.0
PC5: ip address 190.108.20.5 255.255.255.0
PC6: ip address 190.108.30.6 255.255.255.0
PC7: ip address 190.108.10.7 255.255.255.0
```

PC8: **ip address 190.108.20.8 255.255.255.0**
PC9: **ip address 190.108.30.9 255.255.255.0**

C. Configurar las direcciones IP en los Switches.

1. En cada uno de los Switches asigne una dirección IP al SVI (Switch Virtual Interface) para VLAN 99 de acuerdo con la siguiente tabla de direccionamiento y active la interfaz.

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 3. Configuraciones ip en Switchs

```
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
```

D. Verificar la conectividad Extremo a Extremo

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

Se realizan los diferentes Ping's y se nota que los Pings a diferentes VLAN's no fueron satisfactorias, en cambio, los que se realizaron con las mismas VLAN's si fueron satisfactorias. Los errores son por los segmentos diferentes de red.

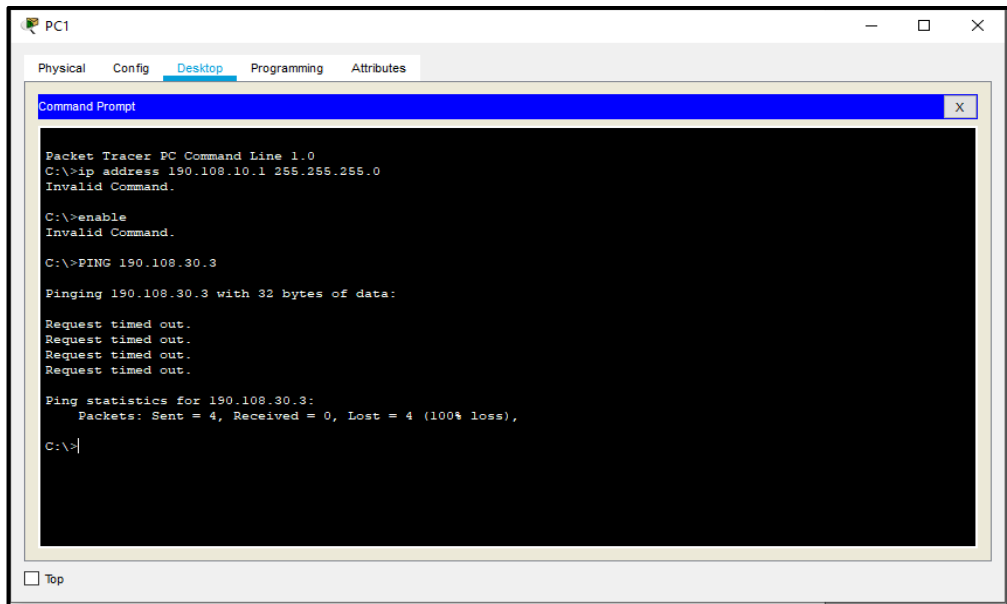


Figura 22. Ping de PC1 a PC3

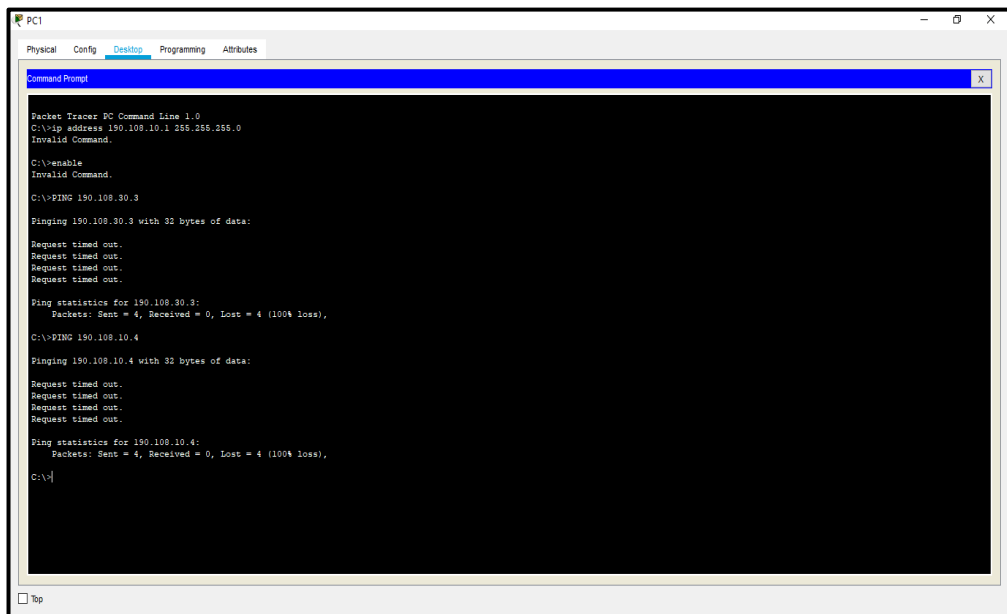
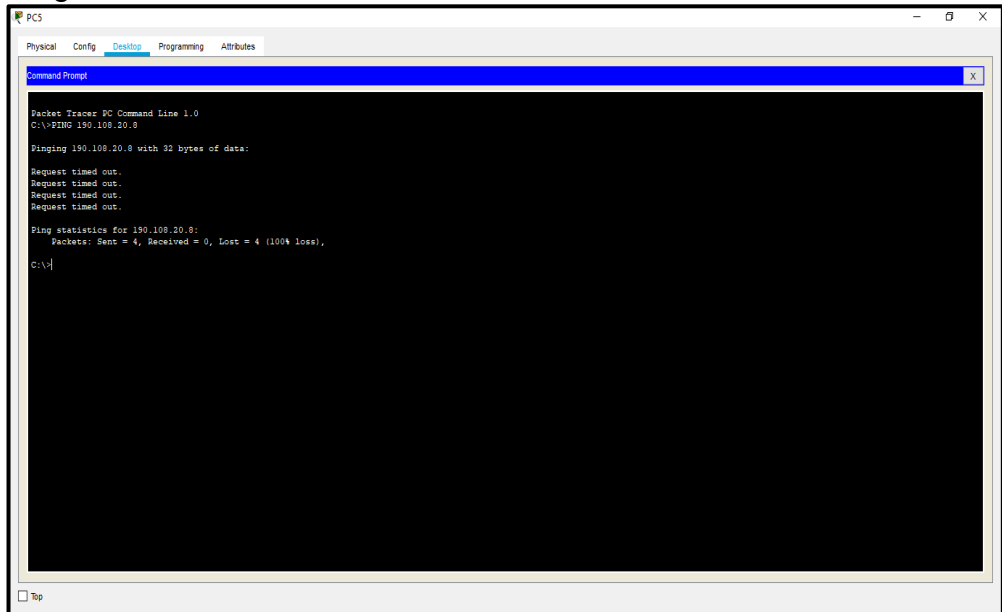


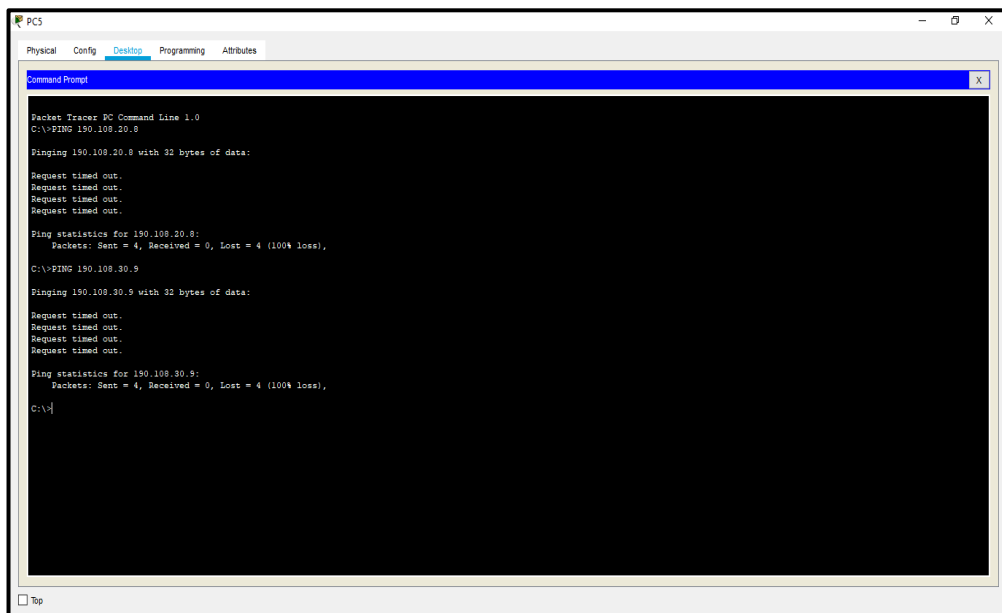
Figura 23. Ping de PC1 a PC4

Ping de PC5 a PC8



```
PC5
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>PING 190.108.20.8
Pinging 190.108.20.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.20.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

Figura 24. Ping de PC5 a PC8



```
PC5
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>PING 190.108.20.8
Pinging 190.108.20.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.20.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>PING 190.108.30.9
Pinging 190.108.30.9 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 190.108.30.9:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

Figura 25. Ping de PC5 a PC9

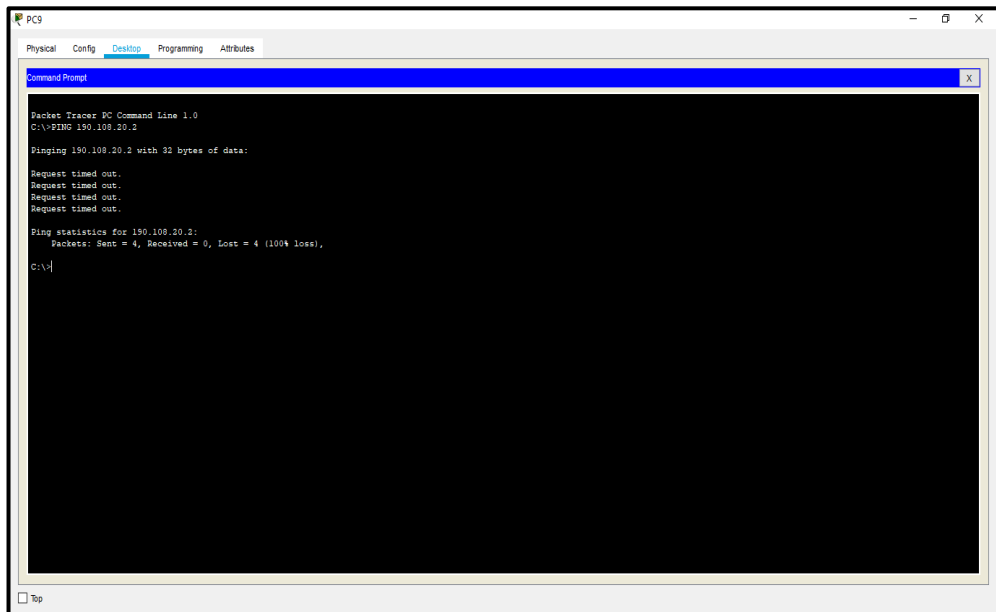


Figura 26. Ping de PC9 a PC2

Ping de PC9 a PC3

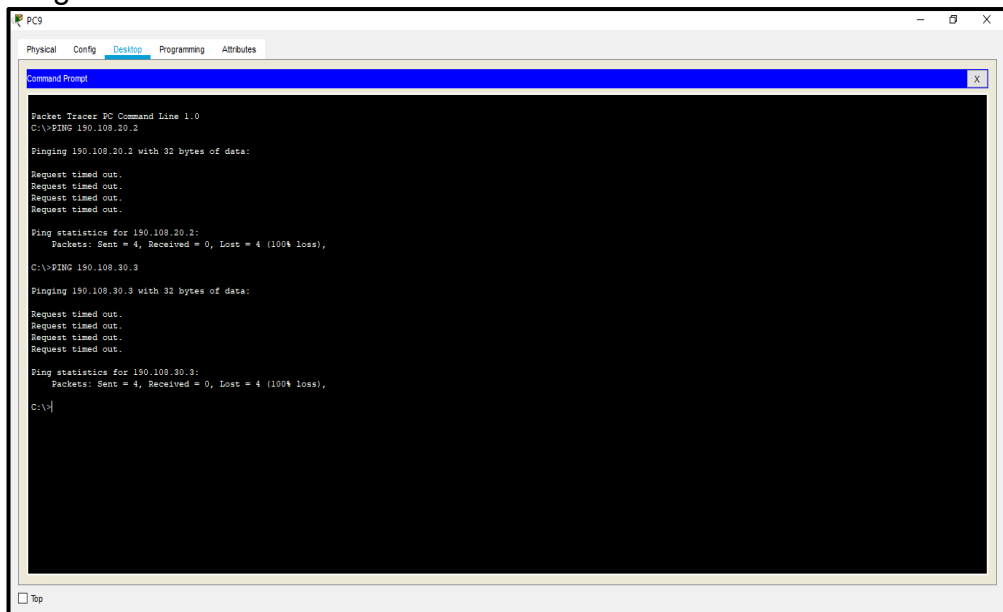


Figura 27. Ping de PC9 a PC3

2. Ejecute un Ping desde cada Switch a los demás. Explique por qué el ping tuvo o no tuvo éxito.
Los comandos Ping de Switch a Switch fueron ejecutados con éxito. Las configuraciones en modo troncal entre los Switch's permitieron la labor del protocolo ICMP.



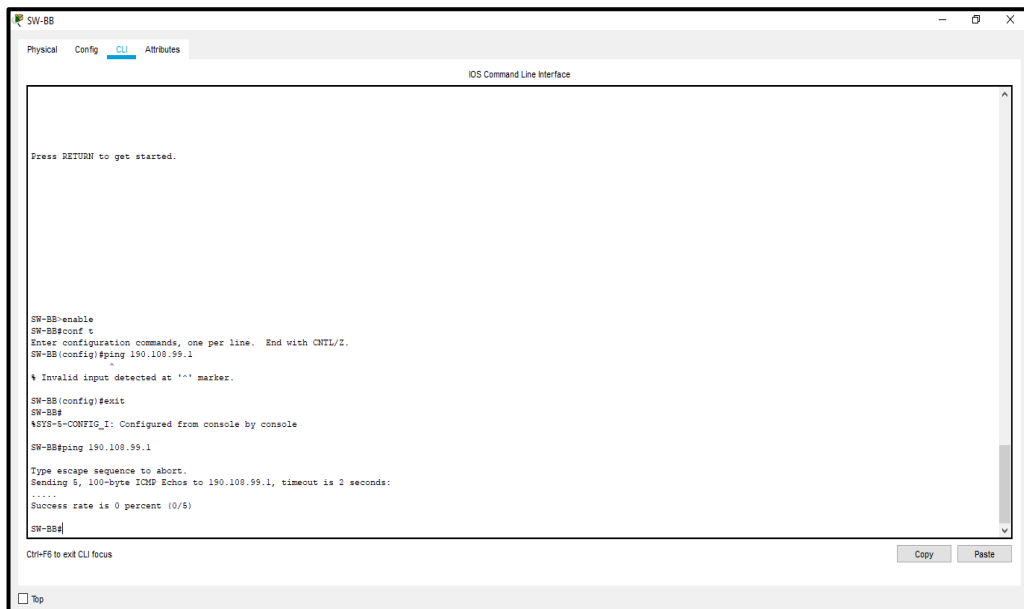
```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface

SW-AA con0 is now available

Press RETURN to get started.

SW-AA-enable
SW-AA#ping 150.108.99.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.108.99.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-AA#
SW-AA#
```

Figura 28. Ping de SW-AA a SW-BB y SW-CC



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

Press RETURN to get started.

SW-BB-enable
SW-BB#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#ping 150.108.99.1
% Invalid input detected at '^' marker.
SW-BB(config)#exit
SW-BB#
%SYS-5-CONFIG_I: Configured from console by console
SW-BB#ping 150.108.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 150.108.99.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#
```

Figura 29. Ping de SW-AA a SW-BB y SW-CC

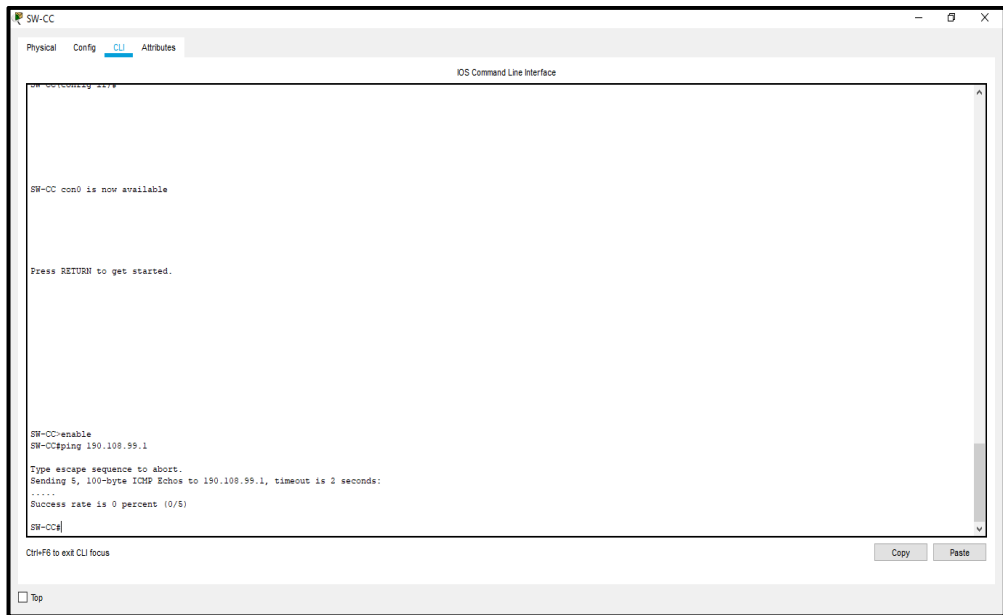


Figura 30. Ping de SW-AA a SW-BB y SW-CC

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

Los comandos Ping's en combinación entre Switch's y PC's no fue exitosa, debido a las VLAN's diversas por medio del protocolo VTP, por tanto, cada PC entra según sus respectivas VLAN's programadas.

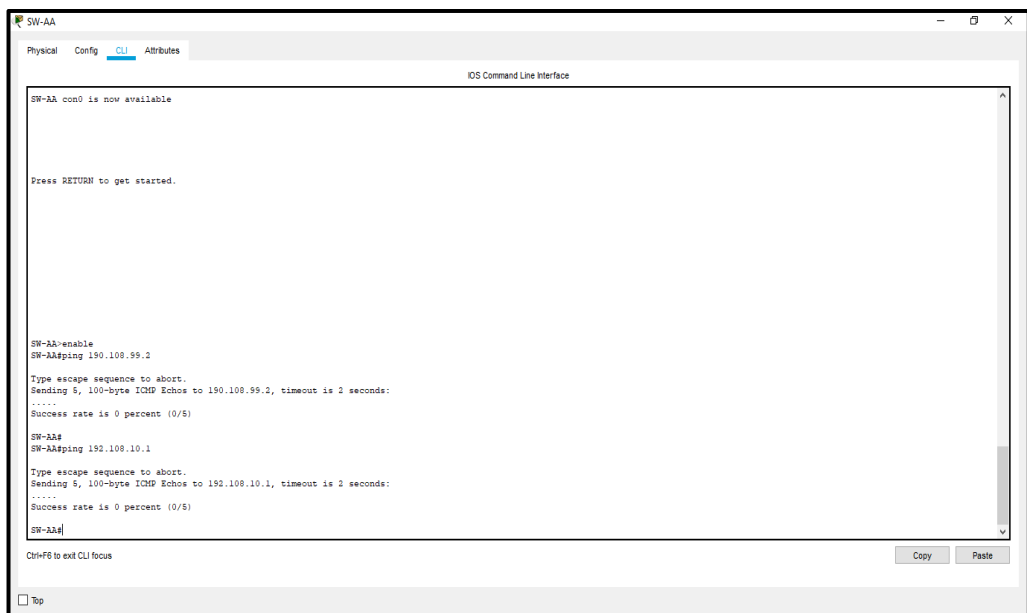


Figura 31. Ping SW-AA a PC1 / PC2 / PC3

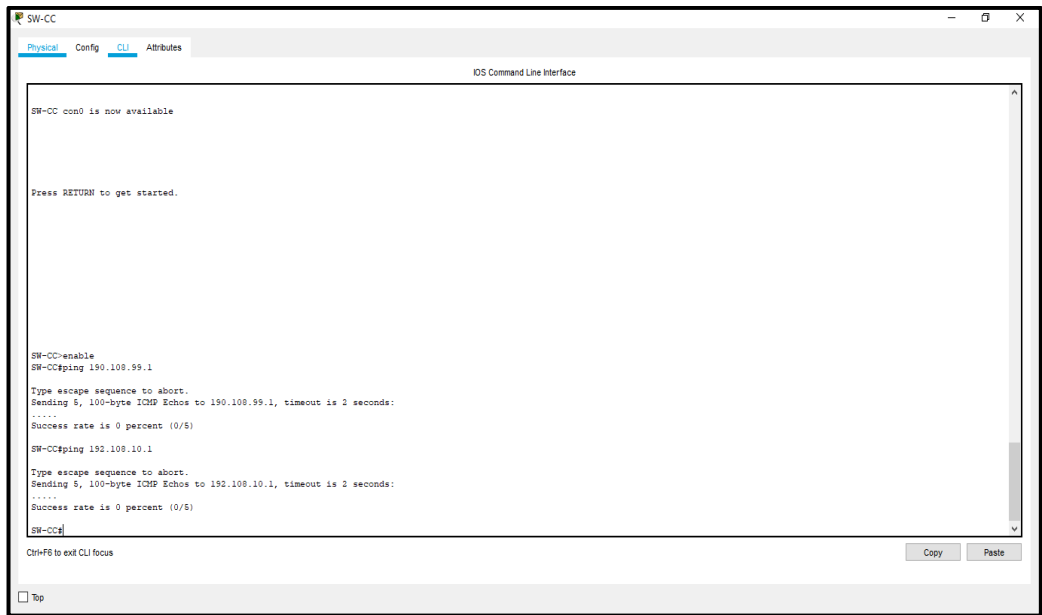


Figura 32. Ping SW-CC a PC7 / PC8 / PC9

CONCLUSIONES

Desarrollando las actividades propuestas, se evidencia los conocimientos adquiridos a través del curso utilizando Software prácticos como Packet Tracer y GNS.

Por medio del análisis de los comandos dados como show ip route, show interfaces trunk o show vlan brief, se detectan fallas y con los conocimientos adquiridos se proponen soluciones.

Cuando se realiza la revisión de conexión de extremo a extremo, se evidencia el manejo de cada una de las competencias adquiridas en el curso, identificando falencias y problemas en data y conexiones, señalando ajustes necesarios en las configuraciones de los elementos implicados y ofrecer una solución adecuada para la solución de fallas dadas.

REFERENCIAS BIBLIOGRÁFICAS

RAMÍREZ, José. (2020). Disponible en: Culturación - Topología de Red. Artículo en Línea. Disponible en: <http://culturacion.com/topologia-de-red-malla-estrella-arbol-bus-y-anillo/>

ABADÍA, Carlos. (2020). Disponible en: Router. Artículo en Línea. Disponible en: <https://www.definicionabc.com/tecnologia/router.php>

MARQUEZ, Iván. (2020). Disponible en: Sumarización. Artículo en Línea. Disponible en: <https://bloggspace.wordpress.com/2016/03/04/que-es-sumarizar-y-como-realiza-y-calcular/>

SANTOS GONZÁLES, Manuel. Disponible en: El Switch: cómo funciona y sus principales características. Artículo en Línea. Disponible en: <http://redestematicas.com/el-switch-como-funciona-y-sus-principales-caracteristicas/>

SOTO, Luis. (2020). Disponible en: Tecno Derecho - Máscara de Subred. Artículo en Línea. Disponible en: <https://sistemas.tecnoderecho.com/mascara-de-subred-que-es/>