DIPLOMADO DE PROFUNDIZACION CISCO CCNP
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

LUIS ANTONIO VELASCO

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD
Escuela de Ciencias Básicas, Tecnología e Ingeniería.

2020

DIPLOMADO DE PROFUNDIZACION CISCO CCNP
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

LUIS ANTONIO VELASCO

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA UNAD
Escuela de Ciencias Básicas, Tecnología e Ingeniería.

2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Popayán, 22 de mayo de 2020

CONTENIDO

LISTA DE FIGURAS

GLOSARIO

IP Address. este término indica la dirección del protocolo de Internet asignada a un computador dentro de una red.

Hostname. se refiere al nombre que se le da un dispositivo de cómputo dentro de una red de comunicaciones a fin de identificarlo para la realización de las diferentes operaciones.

Network. es la denominación de un conjunto de computadoras interconectadas siguiendo una determinada disposición topología, a fin de intercambiar información entre ellas.

No shutdown. este comando habilita la interfaz de del equipo cisco, como por ejemplo un enrutador

Trunk. es una orden que permite conmutar el tráfico de un switch a otro dentro de una red de telecomunicaciones.

RESUMEN

En este informe correspondiente al Diplomado de profundización CISCO CCNP se describen los pasos seguidos para la simulación de dos escenarios; el primero en el que se utilizan en comandos de red para enrutar tráfico a través de diferentes dispositivos enrutadores; el segundo, que simula situaciones donde es necesaria la configuración BGP, del protocolo de pasarela frontera, con el fin de acceder a redes con direcciones IP privadas.

Para cada práctica, se suministra el código utilizado en cada uno de los cuatro enrutadores empleados, ilustrando la topología de la red y la información de las direcciones loopback.

Luego, el informe permite enfatizar en las habilidades adquiridas en el Diplomado para la adecuada instalación, configuración, administración, conmutación y enrutamiento para la resolución de problemas en redes LAN y WAN de pequeñas y medianas empresas, así como aquellas relativas a la configuración de enrutadores avanzados como IGRP, RIP, OSPF, y la utilización tanto el direccionamiento IPV4 e IPV6, haciendo especial énfasis en la seguridad, aspecto o de mucha relevancia en la actualidad dentro de las redes de comunicaciones electrónicas.

Palabras Clave

CISCO, CCNP, Conmutación, Enrutamiento, Redes, Electrónica.

ABSTRACT

In this report corresponding to the CISCO CCNP Deepening Diploma, the steps followed for the simulation of two scenarios are described; the first in which they are used in network commands to route traffic through different router devices; the second, which simulates situations where the BGP configuration of the border gateway protocol is necessary, in order to access networks with private IP addresses.

For each practice, the code used in each of the four routers used is provided, illustrating the network topology and loopback address information.

Then, the report emphasizes the skills acquired in the Diploma for the proper installation, configuration, administration, switching and routing for the resolution of problems in LAN and WAN networks of small and medium enterprises, as well as those related to the configuration of routers. advanced as IGRP, RIP, OSPF, and the use of both IPV4 and IPV6 addressing, with special emphasis on security, aspect or of great relevance today in electronic communication networks.

Keywords

CISCO, CCNP, Switching, Routing, Networks, Electronics

INTRODUCCION

Este Diplomado de profundización en enrutamiento y conmutación en redes cisco, está diseñado para certificar las destrezas o habilidades de los profesionales en telecomunicaciones para la planeación, implementación, verificación y resolución de problemas referentes a redes de área local o de área amplia pertenecientes a empresas, con el fin de soportar servicios o soluciones de video, voz, seguridad y comunicaciones inalámbricas.

En este orden de ideas, se han planteado actividades de profundización dirigidas al mejoramiento de las destrezas en enrutamiento IP en redes cisco, lo que configura en este informe el escenario uno, en el que se simulan situaciones que involucran cuatro enrutadores. Se practican aquí diferentes comandos para la manipulación de enrutadores.

De igual manera, se tienen actividades que hacen referencia al mejoramiento de las destrezas en conmutación IP con redes de conmutación cisco, de manera que sea posible que el profesional realice la implementación de este tipo de redes en su entorno de trabajo. Éste es el escenario número dos en este informe. Se tienen aquí diferentes situaciones de codificación para la conmutación BGP.

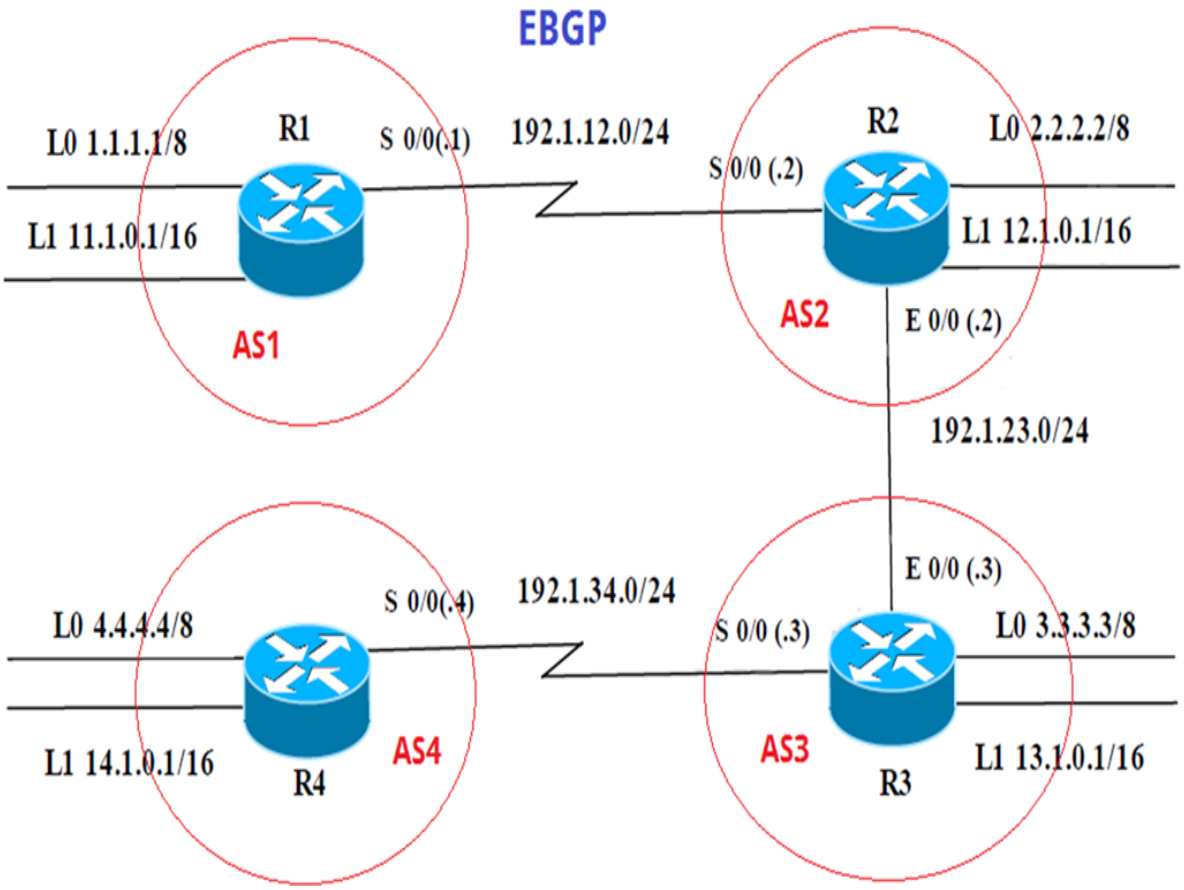
1. DESARROLLO

En esta sección se exponen los resultados obtenidos en cada uno de los escenarios realizados dentro de este Diplomado de profundización.

1.1. ESCENARIO 1

Este escenario se muestra en la figura 1.

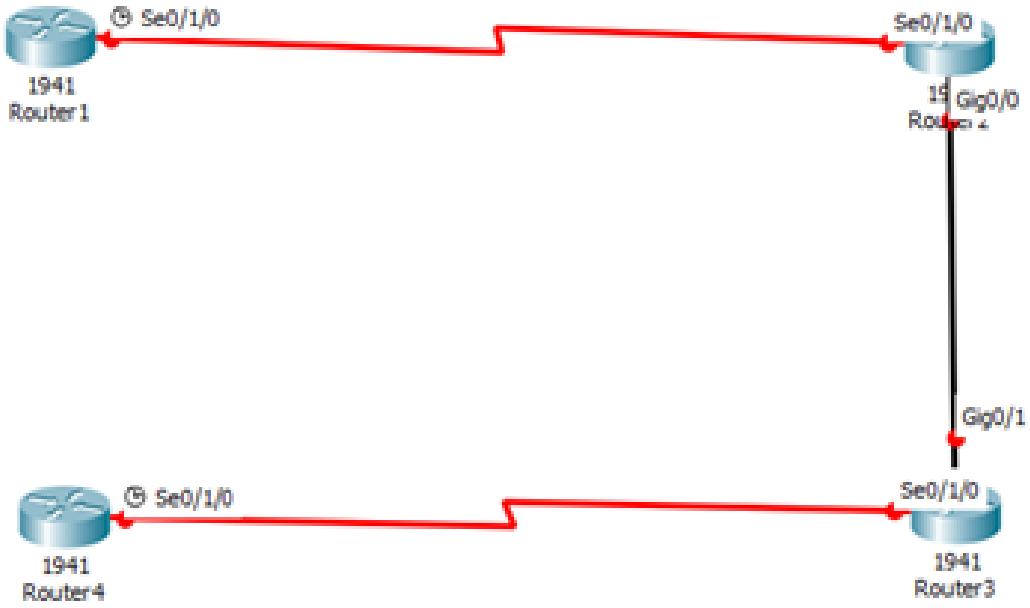
Figura 1. Escenario 1



Fuente. Propia del estudio

En la figura 2 se muestra la simulación del escenario 1.

Figura 2. Simulación del escenario 1¶



Fuente. Propia del estudio

Para que la simulación sea posible, es necesario asignar direcciones IP y máscaras de red a cada uno de los enrutadores involucrados en el escenario 1; la figura 3 muestra estos aspectos de configuración para el enrutador denominado R1.

Figura 3. Información de configuración loopback para R1

Interfaz	Dirección IP	Máscara
Loopback 0	1.1.1.1	255.0.0.0
Loopback 1	11.1.0.1	255.255.0.0
S 0/0	192.1.12.1	255.255.255.0

Fuente. Propia del estudio

De igual forma, la información de loopback para R2, R3 y R4, se muestran en la figura 4.

Figura 4. Información de configuración loopback para R2, R3 y R4

R2

Interfaz	Dirección IP	Máscara
Loopback 0	2.2.2.2	255.0.0.0
Loopback 1	12.1.0.1	255.255.0.0
S 0/0	192.1.12.2	255.255.255.0
E 0/0	192.1.23.2	255.255.255.0

R3

Interfaz	Dirección IP	Máscara
Loopback 0	3.3.3.3	255.0.0.0
Loopback 1	13.1.0.1	255.255.0.0
E 0/0	192.1.23.3	255.255.255.0
S 0/0	192.1.34.3	255.255.255.0

R4

Interfaz	Dirección IP	Máscara
Loopback 0	4.4.4.4	255.0.0.0
Loopback 1	14.1.0.1	255.255.0.0
S 0/0	192.1.34.4	255.255.255.0

Fuente. Propia del estudio

Con base en esta información, se procederá a la configuración de enrutamiento básico y de las direcciones de loopback. La evidencia para R1, se muestra en la figura 5.

Figura 5. Pantallazo de evidencia para R1

```
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
R1(config-if)#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 s
R1(config-if)#interface s0/1
R1(config-if)#interface s0/1/0
R1(config-if)#cl
R1(config-if)#clock ra
R1(config-if)#clock rate 64000
```

Fuente. Propia del estudio

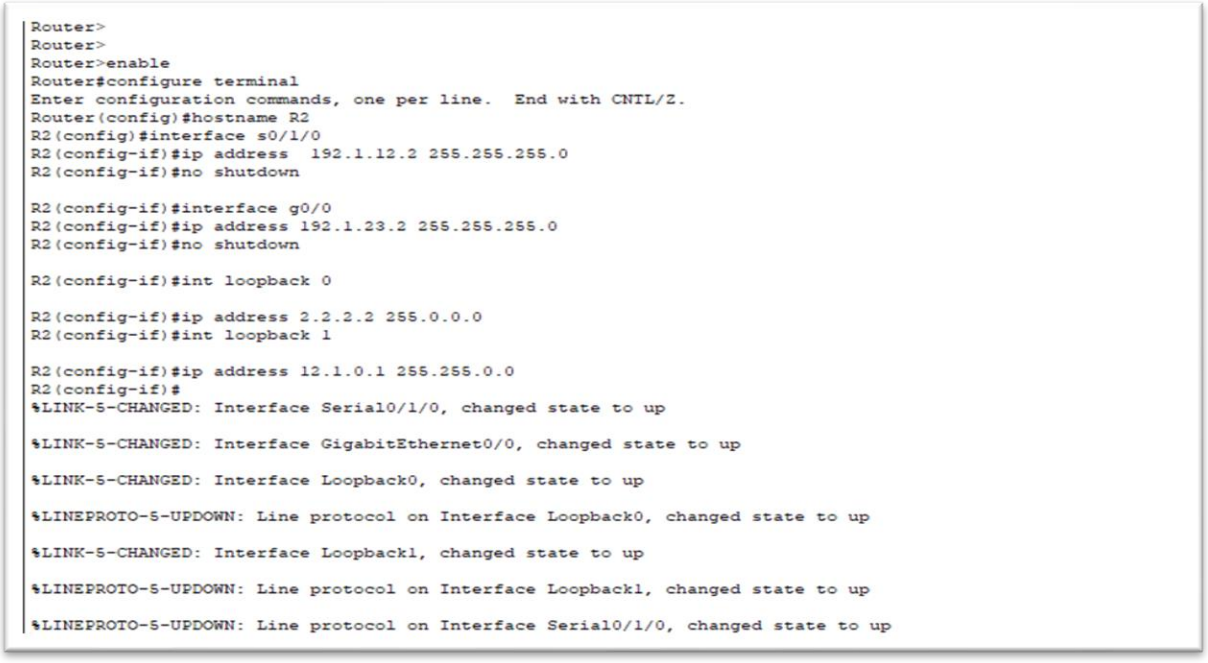
El código correspondiente a R1 es el siguiente:

R1

```
enable
configure terminal
hostname R1
interface s0/1/0
ip address 192.1.12.1 255.255.255.0
clock rate 64000
no shutdown
interface loopback 0
ip address 1.1.1.1 255.0.0.0
interface loopback 1
ip address 11.1.0.1 255.255.0.0
```

En la figura 6, se muestra la evidencia para R2.

Figura 6. Pantallazo de evidencia para R2



Fuente. Propia del estudio

El código correspondiente a R2 es el siguiente:

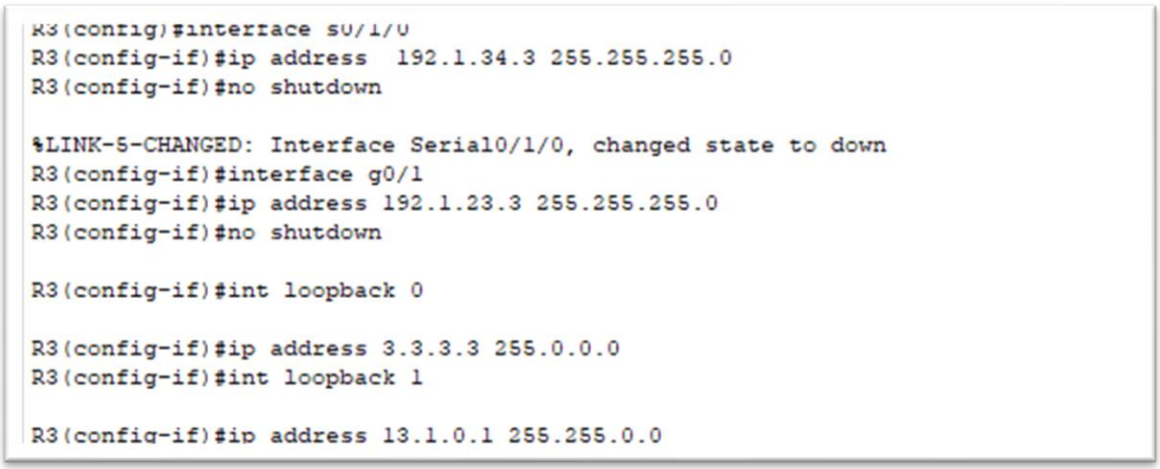
R2

```
enable
configure terminal
hostname R2
interface s0/1/0
ip address 192.1.12.2 255.255.255.0
no shutdown
interface g0/0
ip address 192.1.23.2 255.255.255.0
no shutdown
int loopback 0
ip address 2.2.2.2 255.0.0.0
int loopback 1
ip address 12.1.0.1 255.255.0.0
```

En la figura 7, se muestra la evidencia para R3.

Figura 7. Pantallazo de evidencia para R3

R3



Fuente. Propia del estudio

El código correspondiente a R3 es el siguiente:

R3

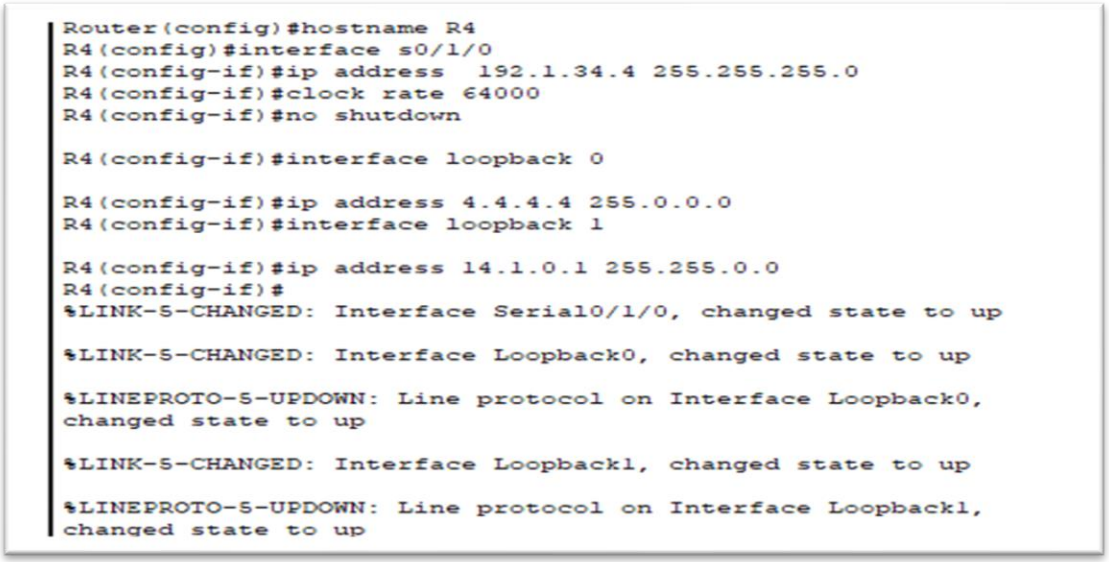
```
enable
configure terminal
hostname R3
```

interface s0/1/0
ip address 192.1.34.3 255.255.255.0
no shutdown
interface g0/1
ip address 192.1.23.3
255.255.255.0
no shutdown
int loopback 0
ip address 3.3.3.3 255.0.0.0
int loopback 1
ip address 13.1.0.1 255.255.0.0

En la figura 8, se muestra la evidencia para R4.

Figura 8. Pantallazo de evidencia para R4

R4



Fuente. Propia del estudio

El código correspondiente a R4 es el siguiente:

R4

enable
configure terminal
hostname R4
interface s0/1/0
ip address 192.1.34.4 255.255.255.0
clock rate 64000

no shutdown
interface loopback 0
ip address 4.4.4.4 255.0.0.0
interface loopback 1
ip address 14.1.0.1 255.255.0.0

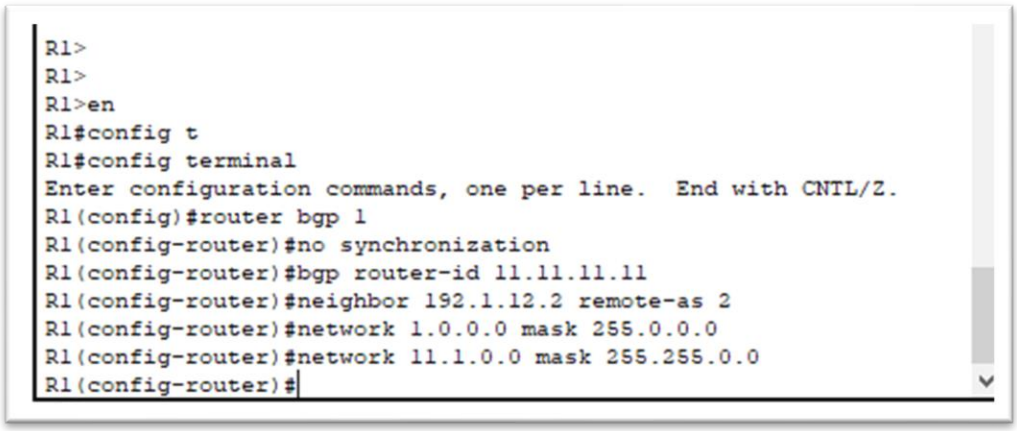
1.1.1. Paso a paso del desarrollo del escenario 1

En los siguientes apartados da el paso a paso de desarrollo del escenario 1, suministrando para cada uno evidencia de pantallazo del código utilizado para para el enrutamiento.

Paso 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 9. Pantallazo de evidencia para R1 paso 1

R1



Fuente. Propia del estudio

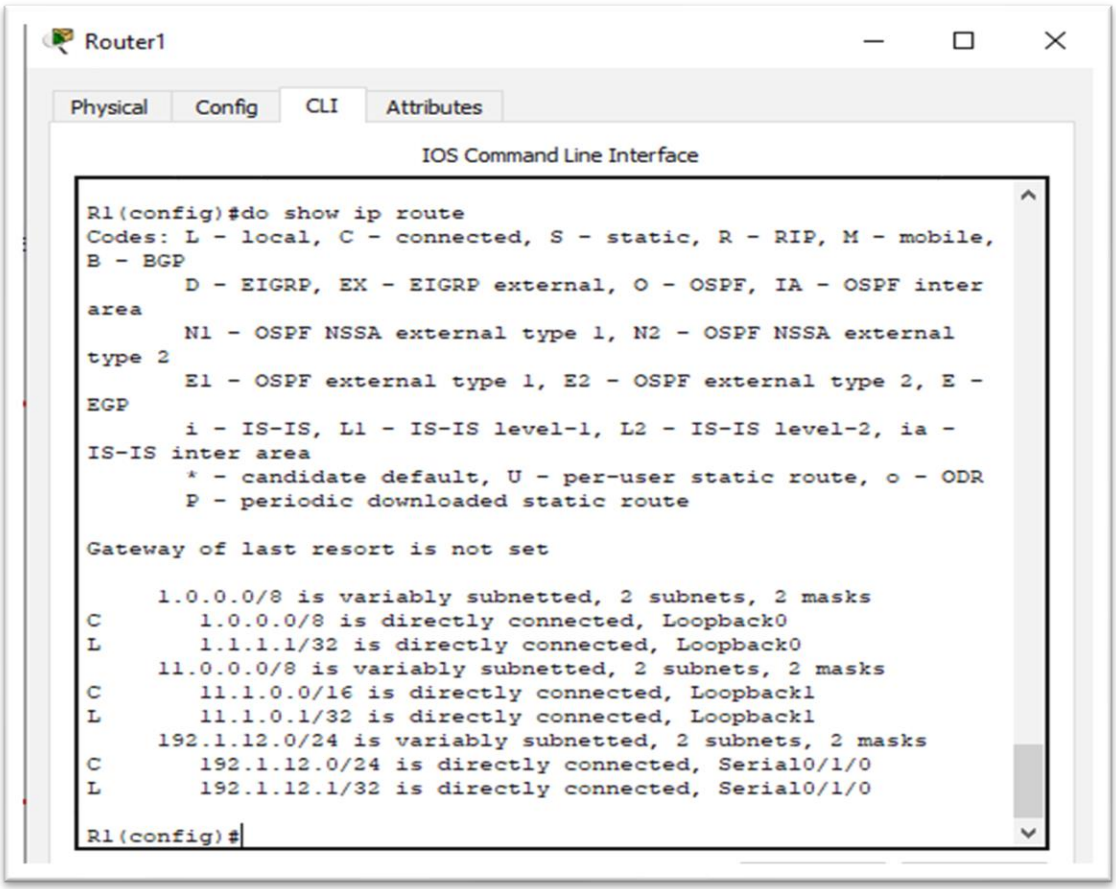
El código correspondiente a esta situación es:

R1

router bgp 1
no synchronization
bgp router-id 11.11.11.11
neighbor 192.1.12.2 remote-as 2
network 1.0.0.0 mask 255.0.0.0
network 11.1.0.0 mask 255.255.0.0

La interfaz de línea de comandos concomitante a esta situación se muestra en la figura 10.

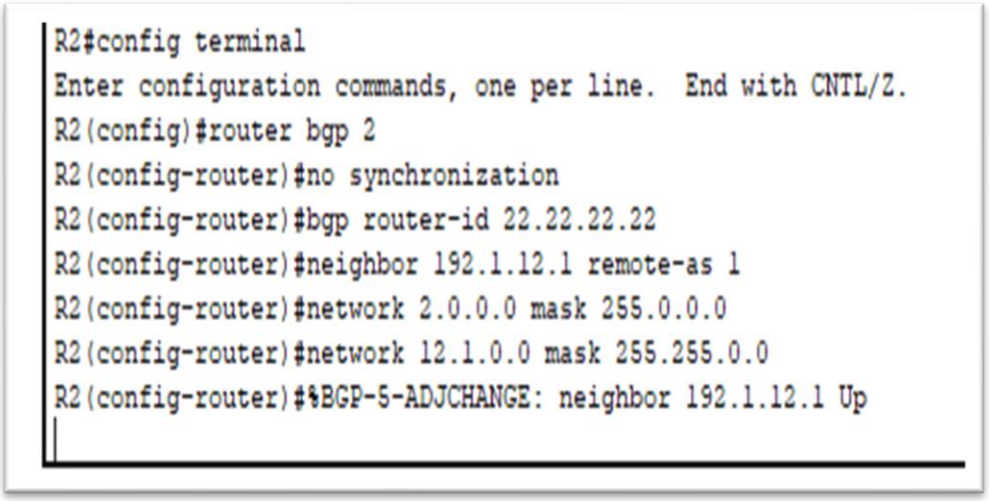
Figura 10. Interface de línea de comandos para R1 paso 1



Fuente. Propia del estudio

Figura 11. Pantallazo de evidencia para R2 paso 1

R2



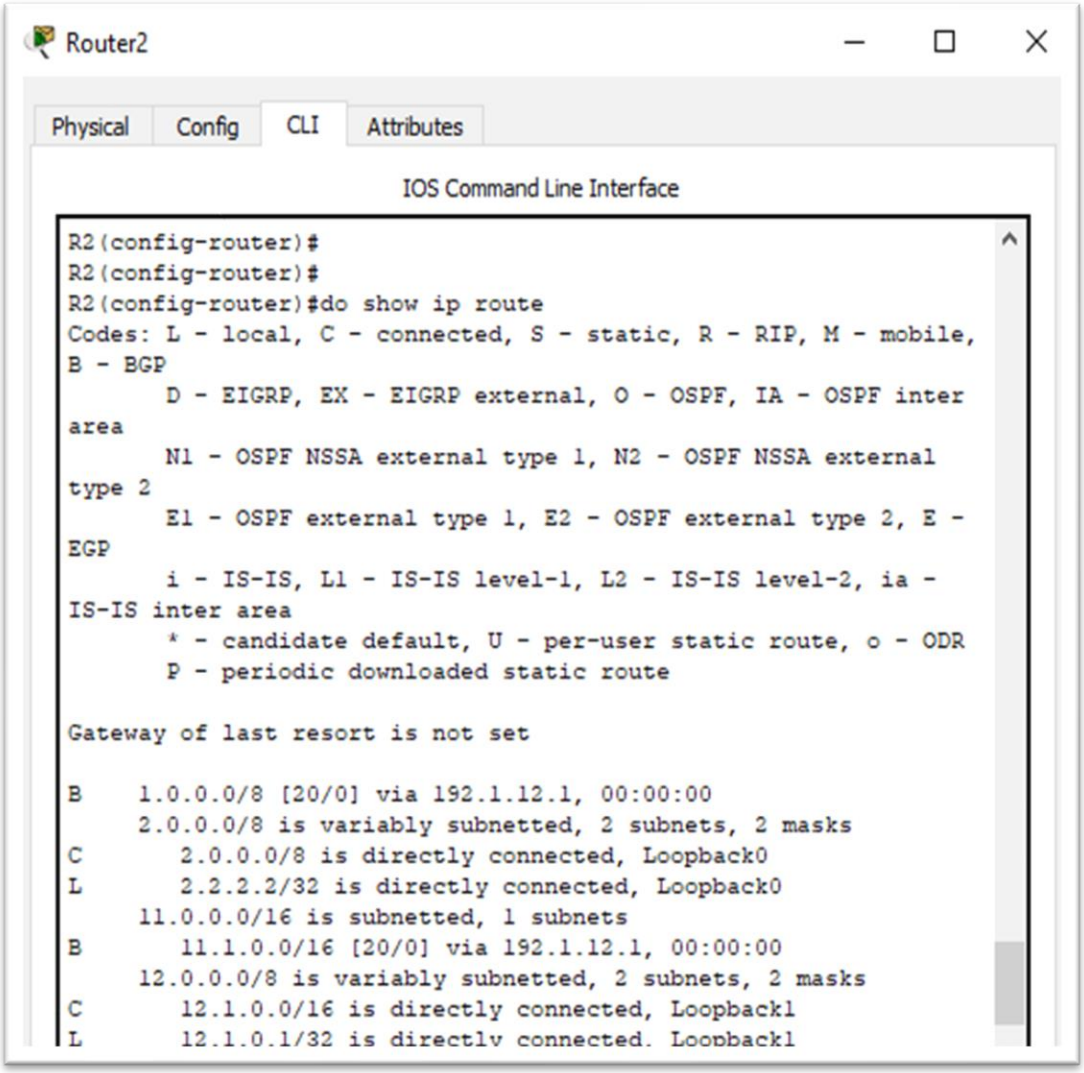
Fuente. Propia del estudio

El código correspondiente a esta situación es:

```
router bgp 2
no synchronization
bgp router-id 22.22.22.22
neighbor 192.1.12.1 remote-as 1
network 2.0.0.0 mask 255.0.0.0
network 12.1.0.0 mask 255.255.0.0
router bgp 2
neighbor 192.1.23.3 remote-as 3
```

La interfaz de línea de comandos concomitante a esta situación involucra en router 2, conforme aparece en el software de simulación utilizado, se muestra en la figura 12.

Figura 12. Interface de línea de comandos para R2 paso 1

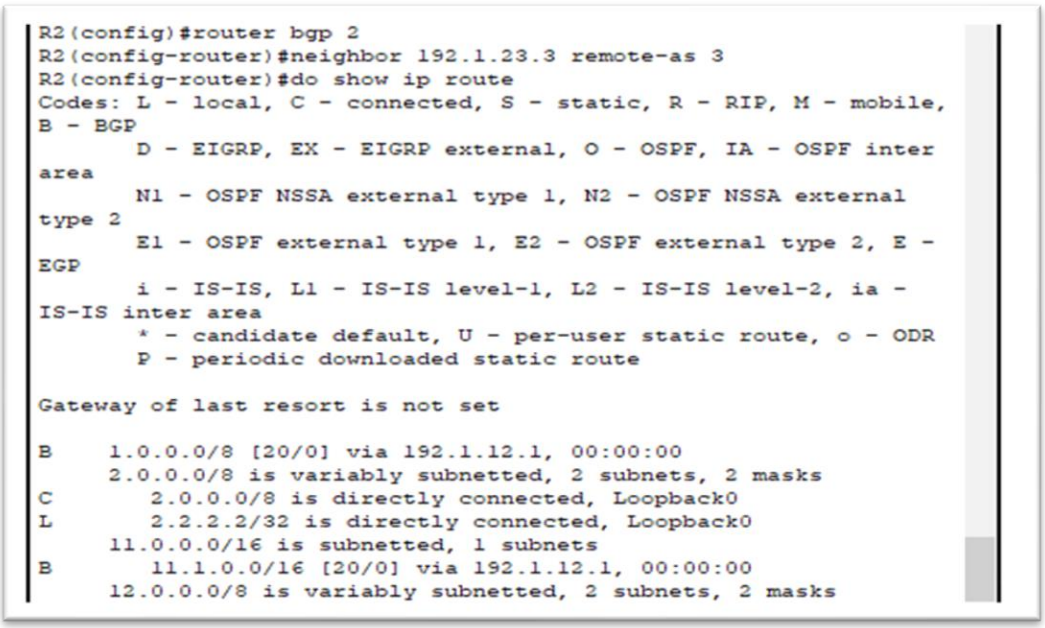


Fuente. Propia del estudio

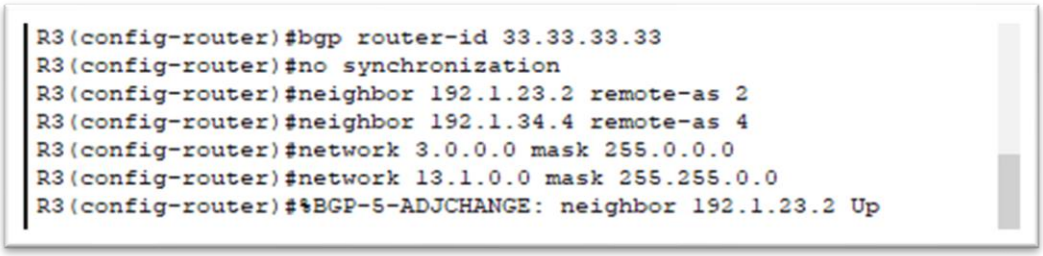
Paso 2. Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en **AS2** y R3 debería estar en **AS3**. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 44.44.44.44. Presente el paso a con los comandos utilizados y la salida del comando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

Las evidencias de configuración para este paso se muestran en la figura 13.

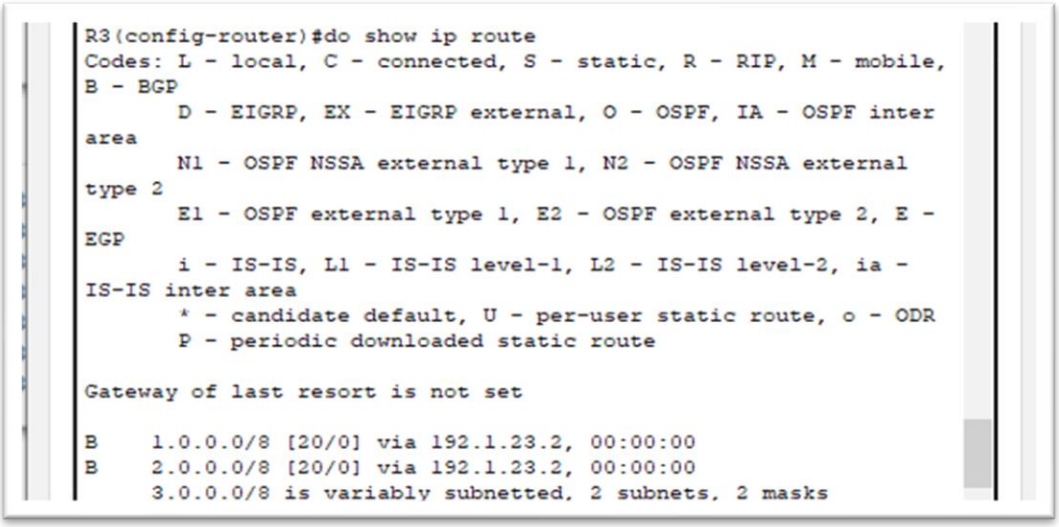
Figura 13. Evidencias de línea de comandos para el paso 2



```
R2(config)#router bgp 2
R2(config-router)#neighbor 192.1.23.3 remote-as 3
R2(config-router)#do 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
```



```
R3(config-router)#bgp router-id 33.33.33.33
R3(config-router)#no synchronization
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#neighbor 192.1.34.4 remote-as 4
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)#%BGP-5-ADJCHANGE: neighbor 192.1.23.2 Up
```



```
R3(config-router)#do 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 192.1.23.2, 00:00:00
B     2.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
      3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
```

Fuente. Propia del estudio

Paso 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.***

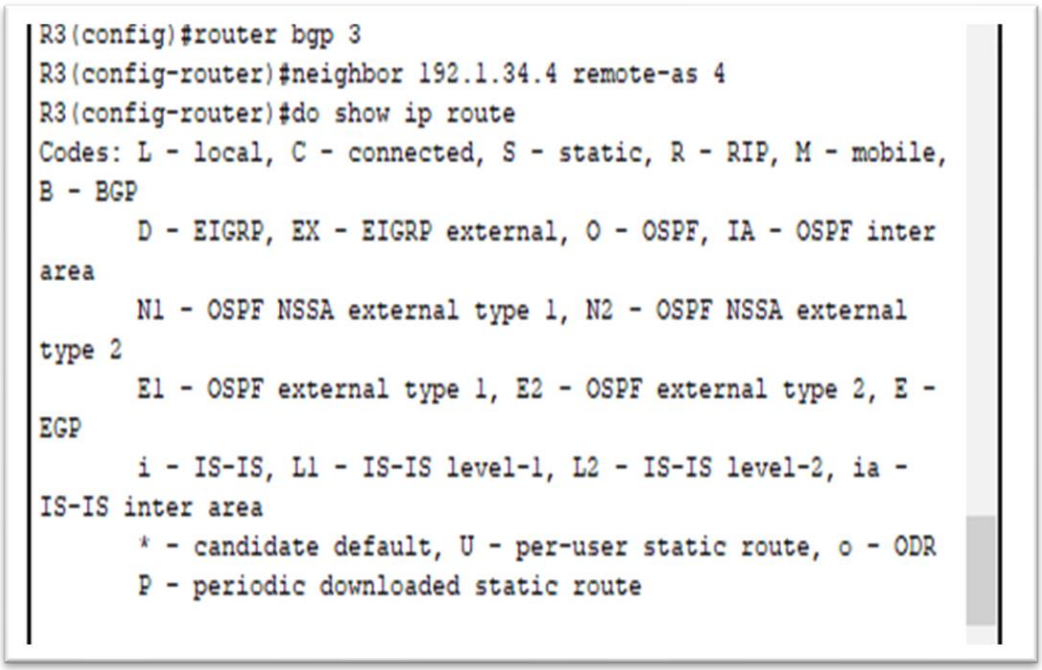
El código para esta situación del enrutador R3, es el siguiente:

```
R3

router bgp 3
bgp router-id 33.33.33.33
no synchronization
neighbor 192.1.23.2 remote-as 2
neighbor 192.1.34.4 remote-as 4
network 3.0.0.0 mask 255.0.0.0
network 13.1.0.0 mask 255.255.0.0
router bgp 3
neighbor 192.1.34.4 remote-as 4
```

La evidencia para este evento, que refiere al router R3, se evidencia en la figura 14. El código perteneciente a la configuración del router R4, de acuerdo al requerimiento de este paso tres, se consigna a continuación:

```
R4

router bgp 4
bgp router-id 44.44.44.44
no synchronization
neighbor 192.1.34.3 remote-as 3
network 4.0.0.0 mask 255.0.0.0
network 14.1.0.0 mask 255.255.0.0
```

Figura 14. Evidencias de línea de comandos para R3, paso 3



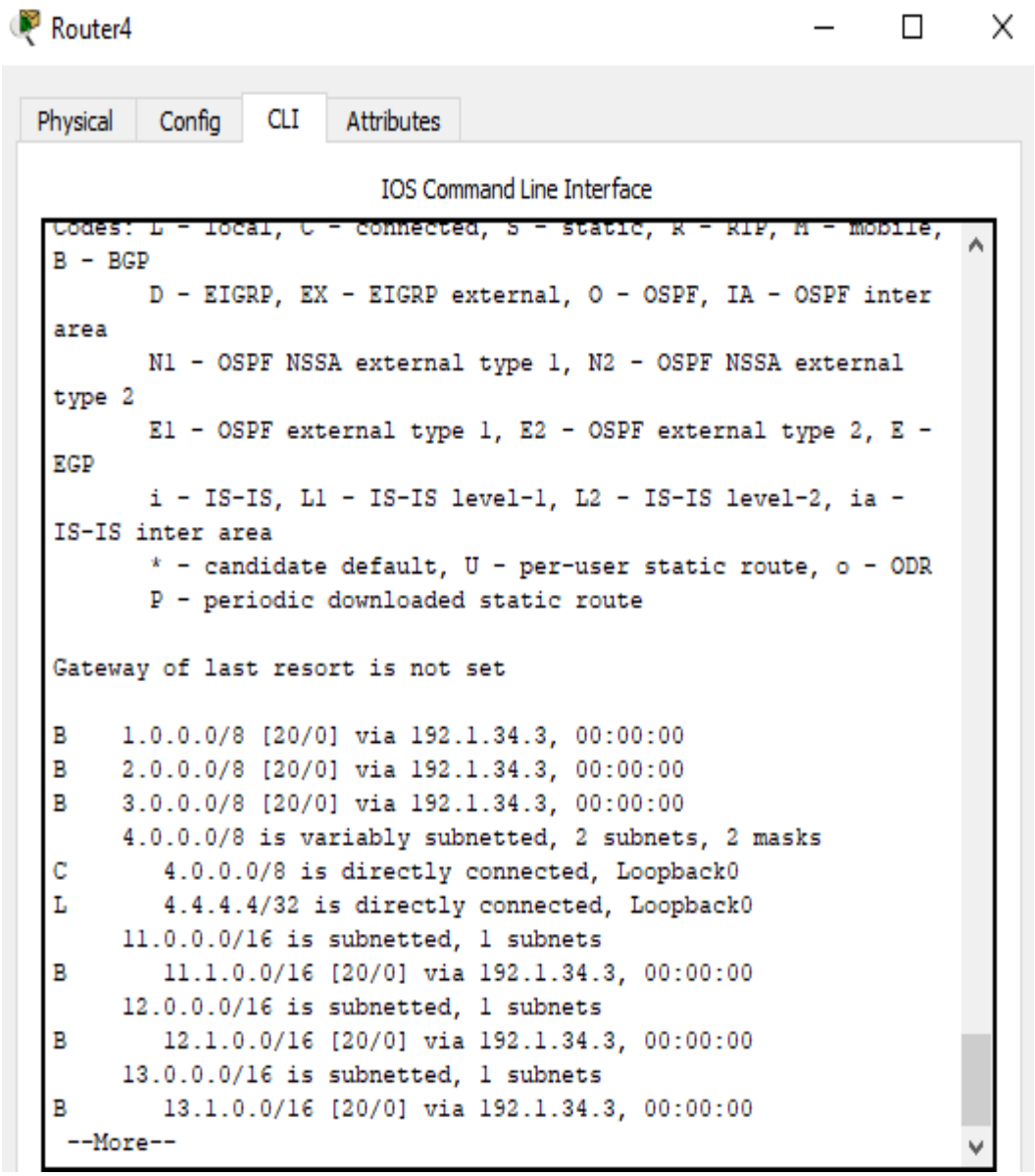
```
R3(config)#router bgp 3
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#do show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
       N1 - OSPF NSSA external type 1, N2 - 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
```

```
R4(config)#router bgp 4
R4(config-router)#bgp router-id 44.44.44.44
R4(config-router)#no synchronization
R4(config-router)#neighbor 192.1.34.3 remote-as 3
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)#%BGP-5-ADJCHANGE: neighbor 192.1.34.3 Up
```

Fuente. Propia del estudio

Finalmente, parece paso tres, se consigna la evidencia correspondiente al router R4, lo que refiere a la ventana de la línea de comandos IOS, como aparece en la figura 15.

Figura 15. Evidencias de línea de comandos para R4, paso 3

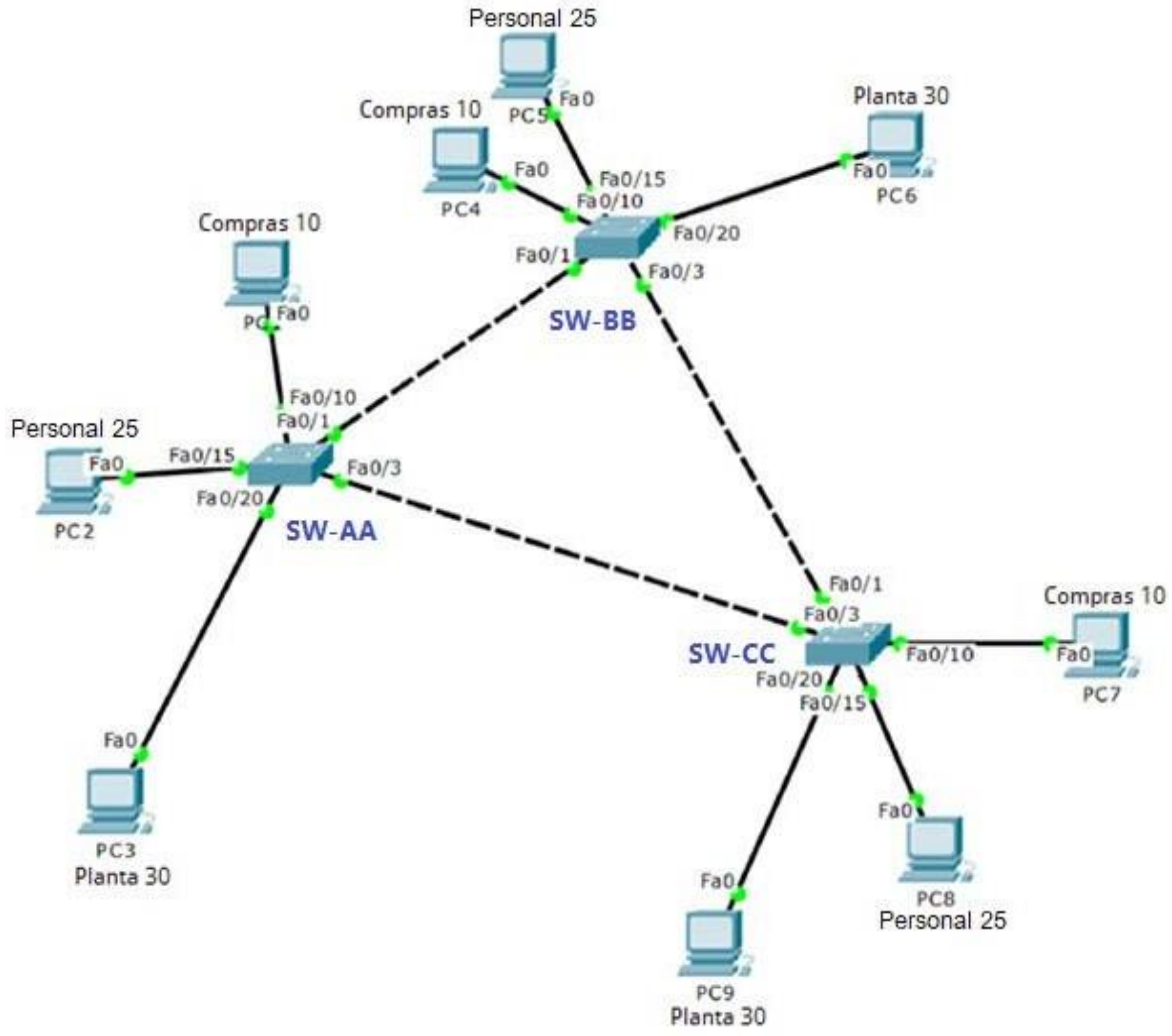


Fuente. Propia del estudio

1.2. Escenario 2¶

En esta sección se abordan las acciones requeridas por el segundo escenario, dentro de las actividades de profundización y en este Diplomado. Dentro de estas, se tienen las acciones de configuración de la comunicación de los diferentes switches utilizados. En la figura 16, se muestra el escenario dos planteado que se requiere simular.

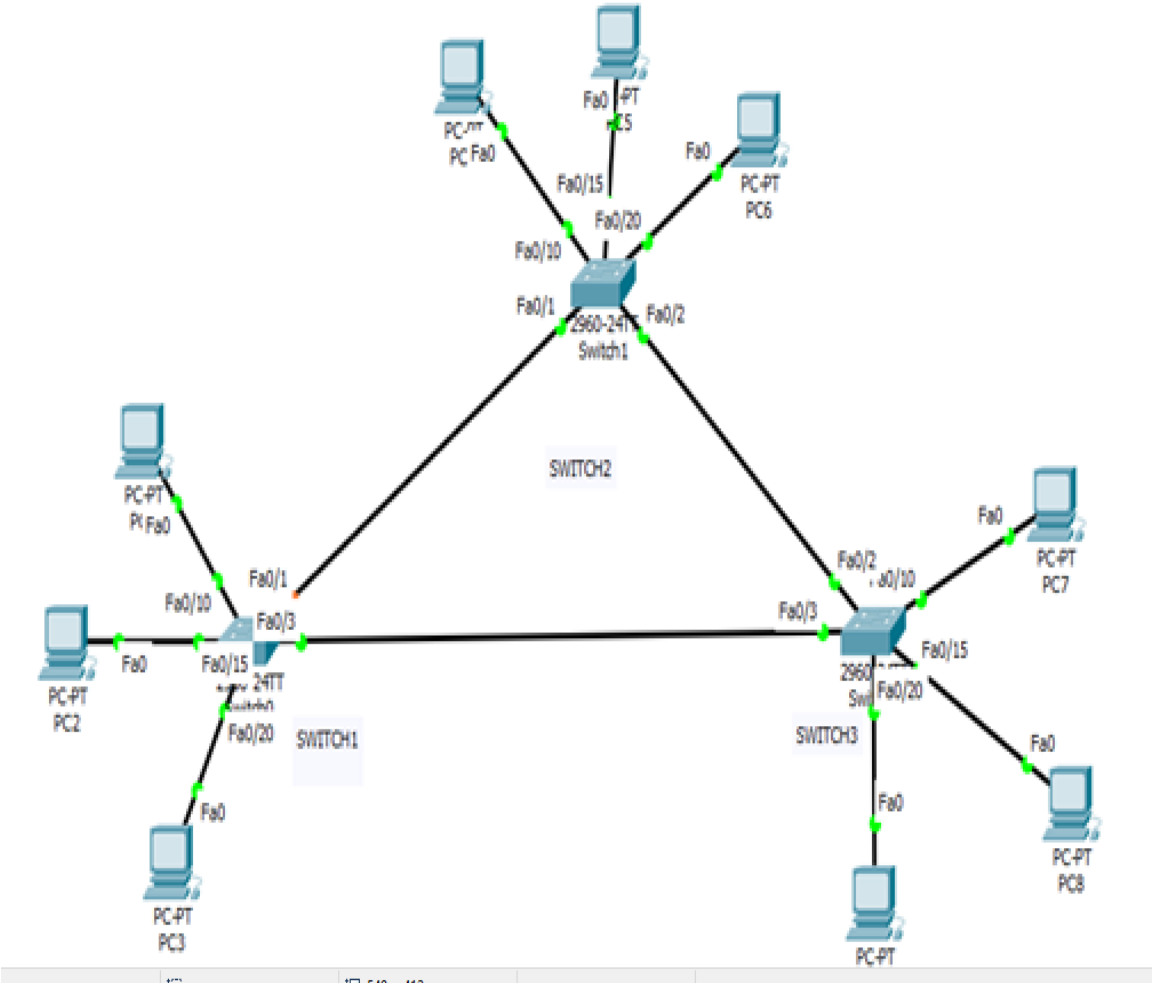
Figura 16. Escenario 2 a simular mediante Packet Tracer



Fuente. Propia del estudio

Este escenario se lleva a la topología de Packet Tracer, de la manera en que se ilustra en la figura 17.

Figura 17. Topología Packet Tracer para el Escenario 2



Fuente. Propia del estudio

Una vez que se detiene la topología de la red a simular en el software de cisco, se procede a la configuración de todos los switches para utilizar VTP, a fin que se pueda llevar a cabo la actualización de la red de área local virtual (VLAN). Esto os se realiza mediante una serie de pasos, que se describen en detalle, dando por su código y las evidencias pertinentes, en la siguiente sección.

1.2.1. Configuración VTP

Paso 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.

El código correspondiente a esta configuración se muestra a continuación:

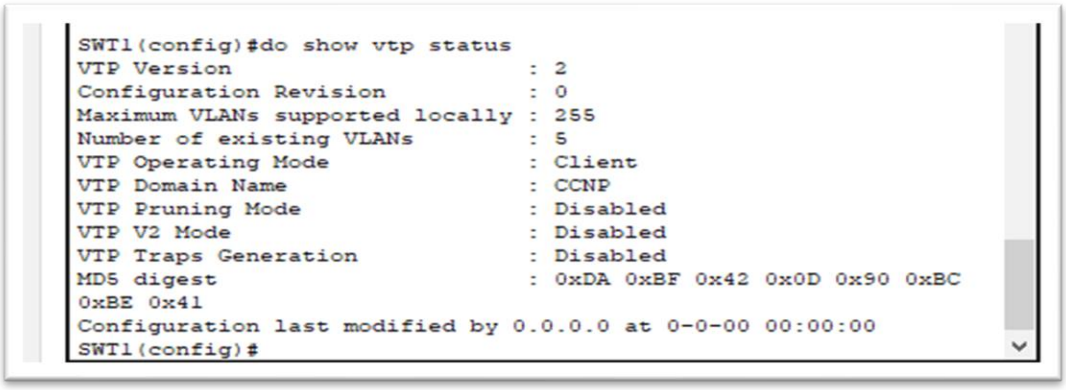
SW1	**SW2**	**SW3**
enable	enable	enable
configure terminal	configure terminal	configure terminal
hostname SWT1	hostname SWT2	hostname SWT3
vtp domain CCNP	vtp domain CCNP	vtp domain CCNP
vtp mode client	vtp mode server	vtp mode client
vtp pass cisco	vtp pass cisco	vtp pass cisco
vtp version 2	vtp version 2	vtp version 2
do show vtp status	do show vtp status	do show vtp status

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

Las evidencias de configuración mediante el comando que nos da la condición de los switches con respecto a VTP, se muestran en la figura 18, discriminando los pantallazos obtenidos para cada uno de los switches.

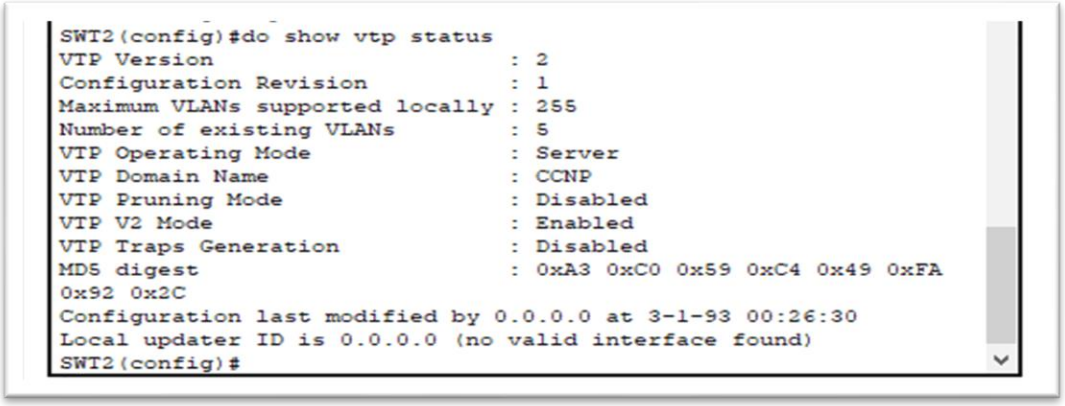
Figura 18. Evidencia de configuración de los switches

SWT1.



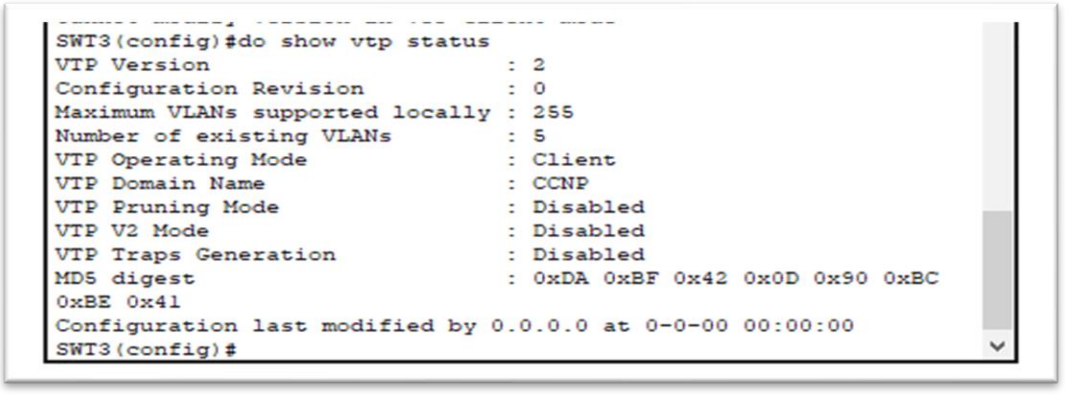
```
SWT1(config)#do show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
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
SWT1(config)#
```

SWT2



```
SWT2(config)#do show vtp status
VTP Version                     : 2
Configuration Revision          : 1
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                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xA3 0xC0 0x59 0xC4 0x49 0xFA
0x92 0x2C
Configuration last modified by 0.0.0.0 at 3-1-93 00:26:30
Local updater ID is 0.0.0.0 (no valid interface found)
SWT2(config)#
```

SWT3



```
SWT3(config)#do 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
SWT3(config)#
```

Fuente. Propia del estudio

1.2.2. Configuración DTP (Dynamic Trunking Protocol)

Paso 3. 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***.

La evidencia de la configuración de los conmutadores, se muestra en la figura 19.

Figura 19. Evidencia de configuración DTP de los switches

SWT1

```
SWT1(config)#int fa0/1
SWT1(config-if)#switchport mode trunk

SWT1(config-if)#switchport mode dynamic desirable

SWT1(config-if)#
%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

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```

SWT2

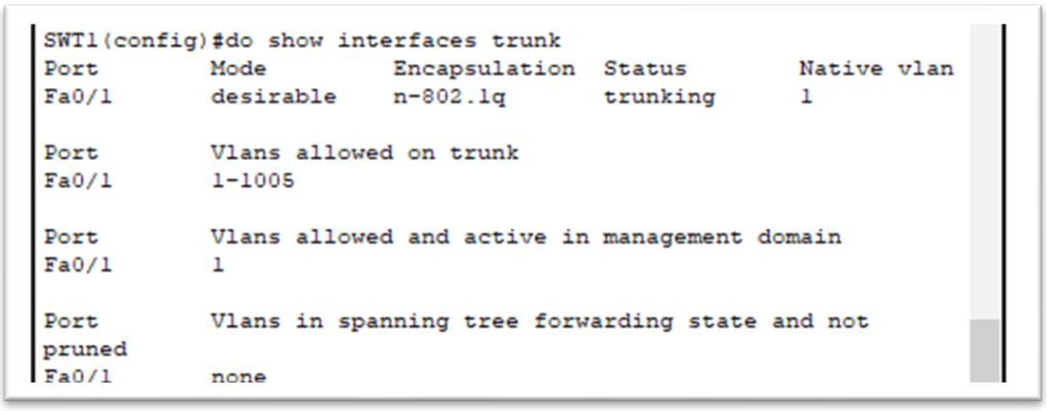
```
SWT2(config)#
SWT2(config)#int fa0/1
SWT2(config-if)#switchport mode trunk
```

Fuente. Propia del estudio

Paso 4. Verifique el enlace "trunk" entre SW-AA y SW-BB usando el comando ***show interfaces trunk***.

La evidencia de la verificación del enlace trunk, se muestra en la figura 20.

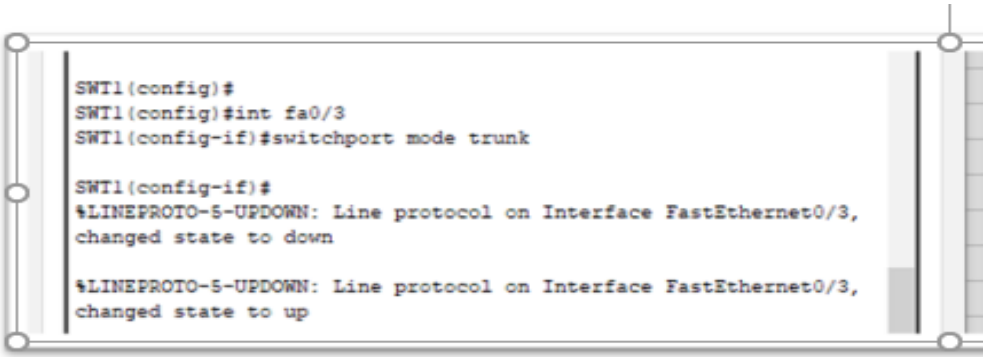
Figura 20. Evidencia de configuración trunk de los switches

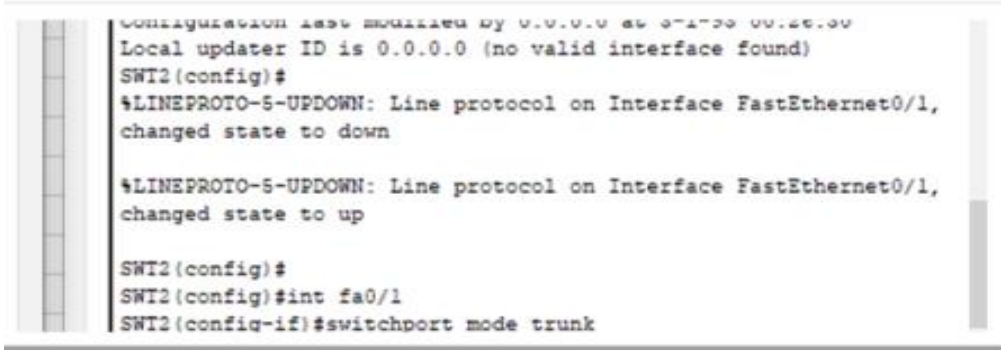


Fuente. Propia del estudio

Paso 5. 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

Figura 21. Evidencia de configuración trunk estática de los switches

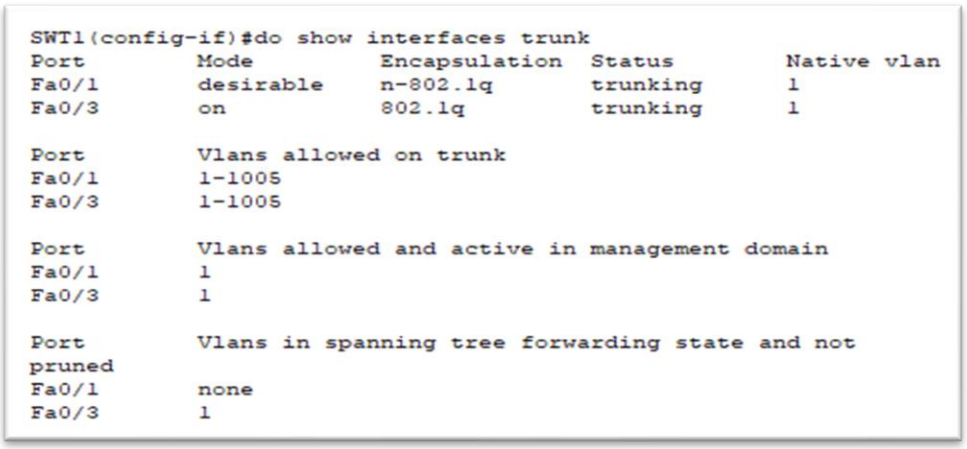




Fuente. Propia del estudio

Paso 6. Verifique el enlace "Trunk" el comando ***show interfaces Trunk*** en SW-AA.

Figura 22. Evidencia de la verificación trunk estática de los switches

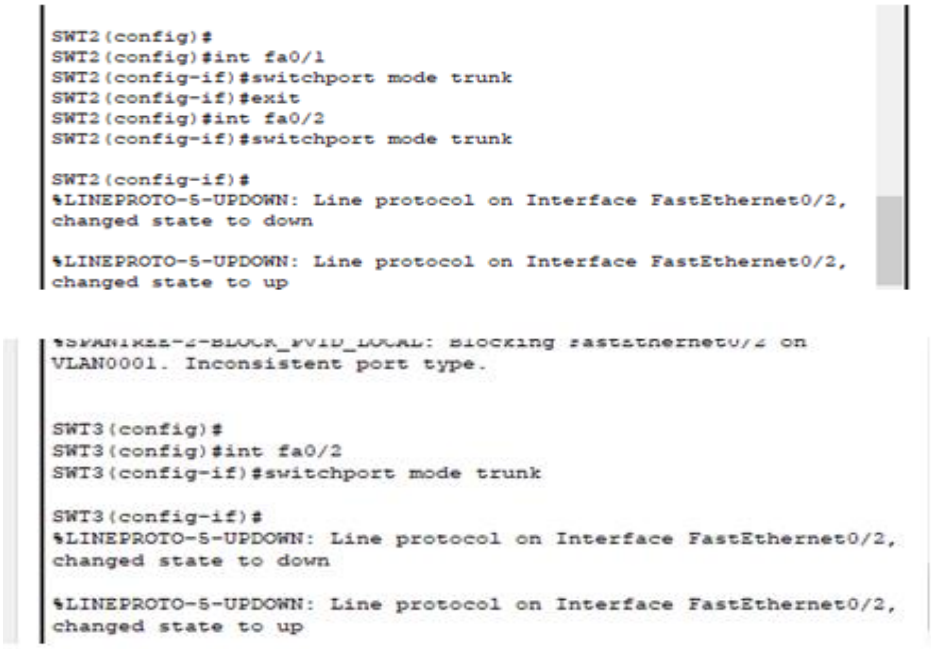


```
SWT1(config-if)#do show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       desirable    n-802.1q       trunking      1
Fa0/3       on           802.1q         trunking      1

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       none
Fa0/3       1
```

Fuente. Propia del estudio

Paso 7. Configure un enlace "Trunk" permanente entre SW-BB y SW-CC.

Figura 23. Evidencia de la verificación trunk permanente de los switches



```
SWT2(config)#
SWT2(config)#int fa0/1
SWT2(config-if)#switchport mode trunk
SWT2(config-if)#exit
SWT2(config)#int fa0/2
SWT2(config-if)#switchport mode trunk

SWT2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to up
```



```
VLAN0001. Inconsistent port type.


SWT3(config)#
SWT3(config)#int fa0/2
SWT3(config-if)#switchport mode trunk

SWT3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2,
changed state to up
```

Fuente. Propia del estudio

1.2.3. Agregar VLANs y asignar puertos

Paso 8. En SW-AA agregue la VLAN 10. En SW-BB agregue las VLANS Compras (10), Personal (25), Planta (30) y Admón. (99)

EI del código de configuración para agregar las VLAN, se muestra a continuación:

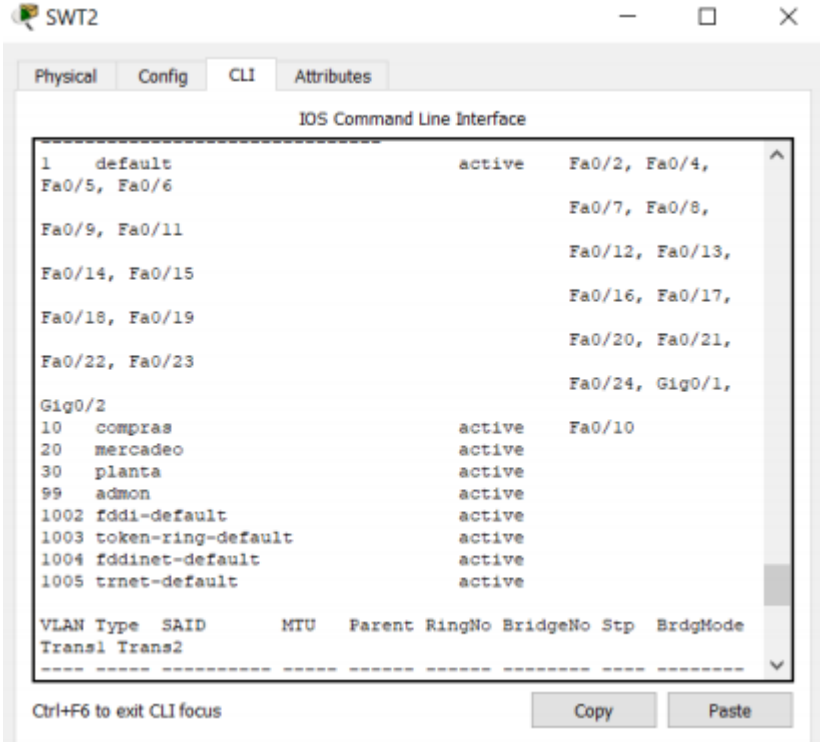
```
Vlan 10
name compras
```

```
Vlan 10
name compras
Vlan 20
name mercadeo
Vlan 99
name almon
```

Paso 9. Verifique que las VLANs han sido agregadas correctamente.

La evidencia que se han agregado las VLAN, se tiene en la figura 24

Figura 24. Evidencia de la verificación trunk estática de los switches



Fuente. Propia del estudio

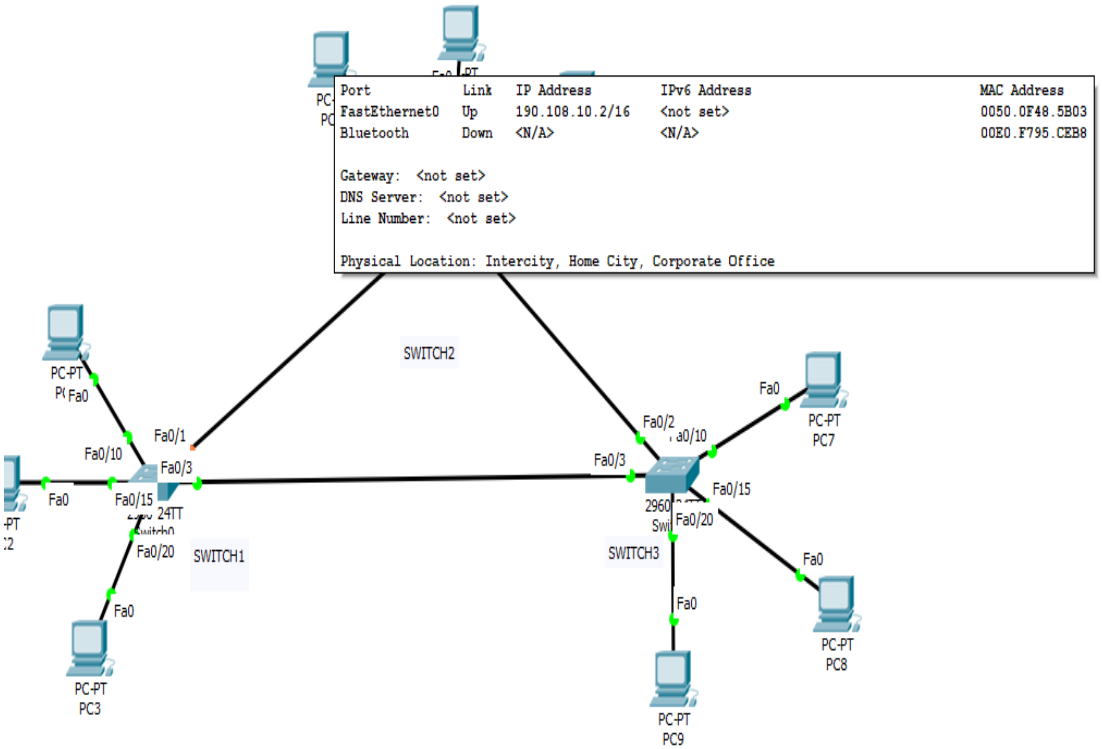
Paso 10. Asocie los puertos a las VLAN y configure las direcciones IP de acuerdo con la siguiente tabla.

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN y se sumen su 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

La asociación de puertos con las direcciones IP suministradas, se muestra en la figura 25.

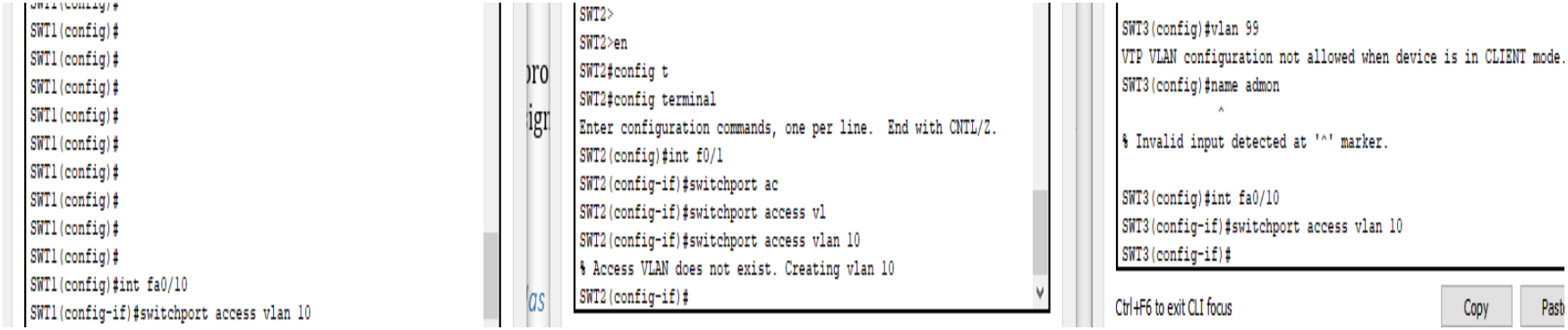
Figura 25. Evidencia de la asociación de los switches con las direcciones IP suministradas



Fuente. Propia del estudio

Paso 11. Configure el puerto F0/10 en modo de acceso para SW-AA, SW-BB y SW-CC y asígnelo a la VLAN 10.

Figura 26. Evidencia de configuración del puerto F0/10 en modo de acceso



Fuente. Propia del estudio

La codificación necesaria para esta acción, se muestra a continuación:

int f0/15	int f0/15	int f0/15
switchport mode access Vlan 20	switchport mode access Vlan 20	switchport mode access Vlan 20
int f0/20	int f0/20	int f0/20
switchport mode access Vlan 30	switchport mode access Vlan 30	switchport mode access Vlan 30

Paso 12. 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

La codificación necesaria para esta acción, se muestra a continuación:

```
int fa0/1                    int fa0/1
switchport mode trunk        switchport mode trunk
switchport mode dynamic
desirable
int fa0/3                    int fa0/3
switchport mode trunk        switchport mode trunk

                             switchport mode trunk      switchport mode trunk
```

1.2.4. Configuración de las direcciones IP en los Switches.

Paso 13. 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

La codificación necesaria, se muestra a continuación:

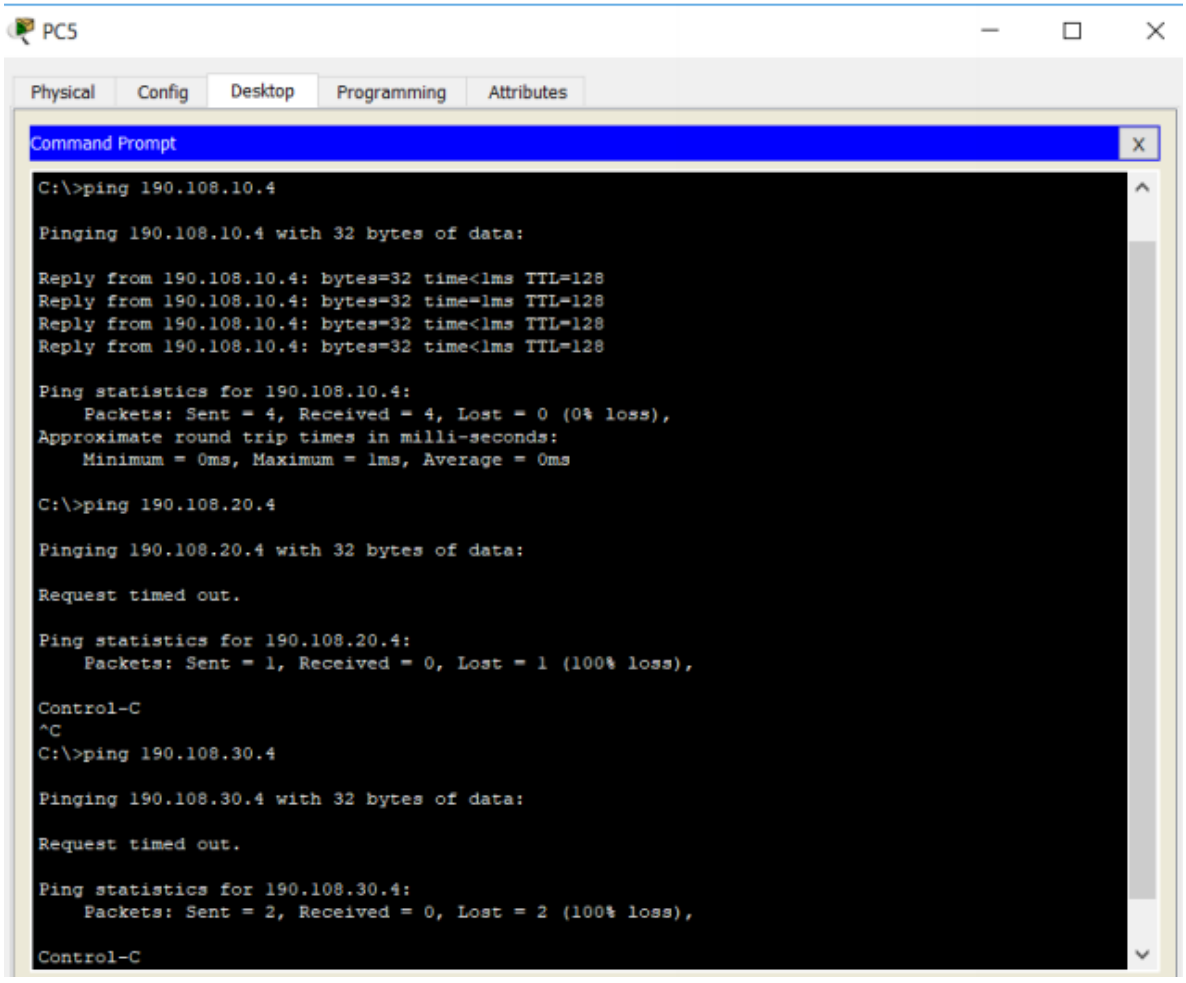
```
int Vlan 99                  int Vlan 99                  int Vlan 99
ip add 190.108.99.1          ip add 190.108.99.2          ip add 190.108.99.3
255.255.255.0                255.255.255.0                255.255.255.0
no shutdown                  no shutdown                  no shutdown
```

1.2.5. Verificar la conectividad Extremo a Extremo

Paso 14. Ejecute un Ping desde cada PC a los demás. Explique por qué el ping tuvo o no tuvo éxito.

En la figura 27, se muestra pantallazo de evidencia de la ejecución del ping para cada uno de los computadores.

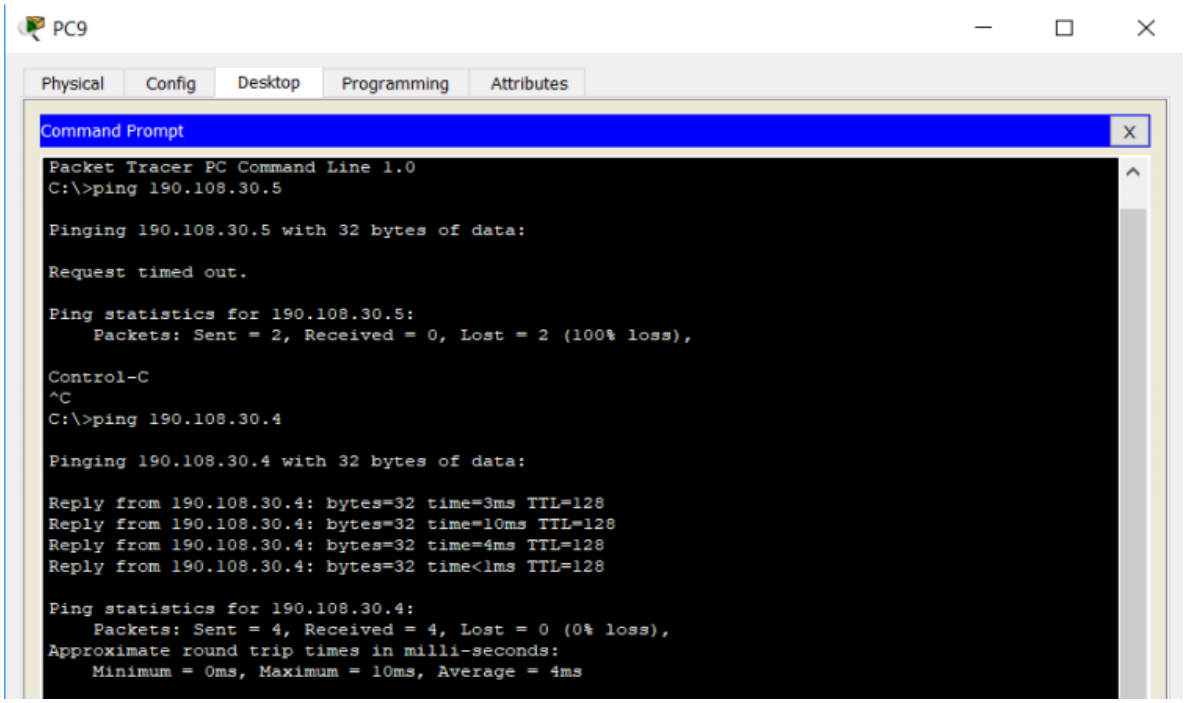
Figura 27. Evidencia de ejecución de ping a cada uno de los computadores



Fuente. Propia del estudio

De igual manera, en la figura 28, se muestra el resultado de la ejecución de ping para equipos que están en la misma LAN, con las estadísticas sobre el tráfico enviado y recibido, de lo que se deduce que ha sido exitoso.

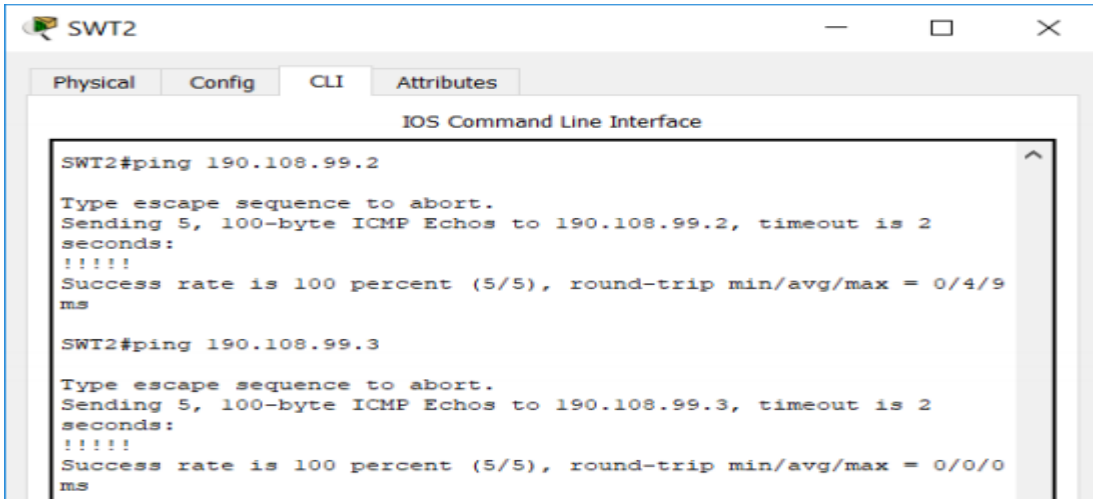
Figura 28. Evidencia de ping exitoso en PC de la misma LAN



Fuente. Propia del estudio

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

Figura 29. Evidencia de la ejecución de un ping entre los conmutadores

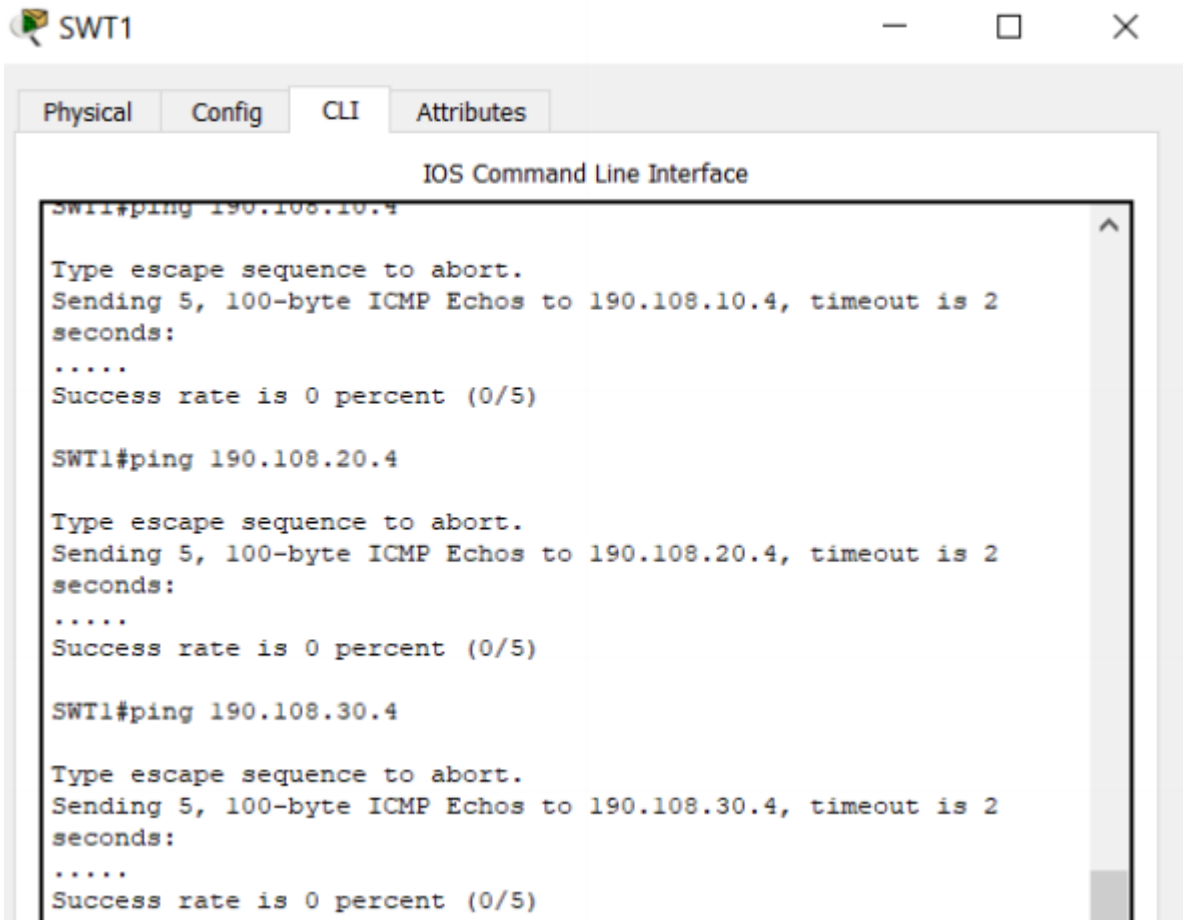


Fuente. Propia del estudio

Los pings sirven porque al estar en modo Trunk y en la misma Vlan hay conectividad.

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

Figura 30. Evidencia de la ejecución de un ping entre los conmutadores y los PCs



Fuente. Propia del estudio

El ping no tuvo éxito debido a que ningún switch tiene una ip a una vlan.

2. CONCLUSIONES

Pudimos aprender gracias al curso de diplomado de profundización en CCNP se adquirieron distintas habilidades de gestión de redes que van orientadas hacia el mundo de las telecomunicaciones, profesional y corporativo, además de ser necesarios para planificar, asegurar, mantener e implementar y solucionar conflictos de redes convergentes.

Protocolos como el EIGRP es un protocolo de transporte de datos en el que se puede depositar bastante confianza, se estudió que tiene la capacidad de estableces adyacencias, utiliza métricas compuestas y utiliza el algoritmo de actualización por difusión (DUAL).

Para el diplomado, durante todo el curso por medio de la herramienta Packet Tracer se pudo simular cada ejercicio propuesto en los entornos de las diferentes plataformas y variar los parámetros para comprender más a fondo las características de los protocolos, routers, switches, pcs.

Por medio del comando “redistribute” podemos realizar la redistribución de protocolos que nos permite conectar redes que tengan configurado un protocolo diferente, debido a que este proceso importa y exporta todas las rutas necesarias por donde viajaran nuestros paquetes.

Aprendimos a manejar y configurar rutas que solo puedan tener acceso cierto tipo de PCS, además de que los pings que enviábamos solo llegaban lógicamente a los equipos que estaban destinados a recibirlos, protegiendo la red de futuros intrusos.

REFERENCIAS BIBLIOGRAFICAS

Hucaby D. CCNA Wireless 640-722 Official Cert Guide [Internet]. Cisco Press. Indianapolis: Cisco Press; 2014. Available from: https://www.safaribooksonline.com/library/view/ccna-wireless-640-722/9780133445725/graphics/05fig01.jpg

Molenaar R. How to master CCNP Switch. New York: Cisco Press; 2015. 338 p.

Teare D, Vachone B, Graziani R. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide. Cisco Press. New York: Cisco Press; 2015. 768 p.

.