

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

**LAURA STEFANNY CALDERON NARVAEZ**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA ELECTRONICA  
NEIVA - HUILA  
2020**

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

**LAURA STEFANNY CALDERON NARVAEZ**

**Diplomado de opción de grado presentado para optar el título de  
INGENIERO ELECTRONICO**

**Director:  
GERARDO GRANADOS ACUÑA**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
INGENIERÍA ELECTRONICA  
DIPLOMADO CISCO CCNP  
NEIVA - HUILA  
2020**

NOTA DE ACEPTACIÓN:

---

---

---

---

---

---

---

---

---

Presidente del Jurado

---

Jurado

---

Jurado

Neiva, 15 de mayo de 2020

## **AGRADECIMIENTOS**

Quiero agradecer en primer lugar a Dios, por guiarme en el camino y fortalecerme espiritualmente para alcanzar cada una de mis metas y propósitos.

Los más sinceros y sentidos agradecimientos a las personas que me acompañaron en este proceso de aprendizaje y dedicación, agradezco a mi familia, que siempre me brindaron la confianza y apoyo incondicional.

Finalmente, un eterno agradecimiento a esta gran universidad, la cual me abre sus puertas, bajo una modalidad de aprendizaje autónomo, facilitando los tiempos y espacios para ser un profesional competitivo y ético.

## TABLA DE CONTENIDO

LISTA DE ILUSTRACIONES .....	6
LISTA DE TABLAS .....	9
GLOSARIO.....	10
RESUMEN.....	11
ABSTRACT .....	12
INTRODUCCIÓN.....	13
ESCENARIO 1 .....	14
ESCENARIO 2 .....	31
CONCLUSIONES.....	72
BIBLIOGRAFÍA.....	76

## LISTA DE ILUSTRACIONES

Figura 1 Topología en packet tracer (Escenario 1)	13
Figura 2 Escenario 1 Pack Tracer. (creado por: Autoría propia).	16
Figura 3 Configuración de una relación de vecino BGP en R1	16
Figura 4 Configuración de una relación de vecino BGP en R2	17
Figura 5 Tabla de enrutamiento de R1 con respecto a R2 (Escenario 1)	17
Figura 6 Tabla de enrutamiento de R2 con respecto a R1 (Escenario 1)	18
Figura 7 Configuración de una relación de vecino BGP en R2	18
Figura 8 Configuración de una relación de vecino BGP en R3	19
Figura 9 Tabla de enrutamiento de R2 con respecto a R3 (Escenario 1)	19
Figura 10 Tabla de enrutamiento de R3 con respecto a R2 (Escenario 1)	20
Figura 11 Configuración de una relación de vecino BGP en R3	20
Figura 12 Configuración de una relación de vecino BGP en R4	21
Figura 13 Tabla de enrutamiento de R3 con respecto a R4 (Escenario 1)	21
Figura 14 Tabla de enrutamiento de R4 con respecto a R3 (Escenario 1)	22
Figura 15 Topología en packet tracer (Escenario 2)	22
Figura 16 Verificación Vtp status en SWAA (Escenario 2)	23
Figura 17 Verificación Vtp status en SWBB (Escenario 2)	24
Figura 18 Verificación Vtp status en SWCC (Escenario 2)	24
Figura 19 Configuración de enlace troncal SWAA	25
Figura 20 Configuración de enlace troncal SWBB	25
Figura 21 Verificación interface troncal de SWBB a SWAA (Escenario 2)	26
Figura 22 Verificación interface troncal de SWBB a SWAA (Escenario 2)	27
Figura 23 configuración un enlace trunk SWAA	27
Figura 24 Verificación interface troncal de SWAA a SWCC (Escenario 2)	28
Figura 25 enlace trunk permanente entre SW-BB	28
Figura 26 enlace trunk permanente entre SW-CC	29
Figura 27 Configuración de VLAN en SWAA	29
Figura 28 Configuración de VLANS en SWBB	30
Figura 29 Verificación Vlans agregadas en SWAA (Escenario 2)	30
Figura 30 Verificación Vlans agregadas en SWBB (Escenario 2)	31
Figura 31 Verificación Vlans agregadas en SWCC (Escenario 2)	31
Figura 32 Configuración el puerto F0/10 en modo de acceso para SW-AA	32
Figura 33 Configuración el puerto F0/10 en modo de acceso para SW-BB	33
Figura 34 Configuración el puerto F0/10 en modo de acceso para SW-CC	33
Figura 35 Configuración de puertos en SWAA	33
Figura 36 Configuración de puertos en SWBB	34

Figura 37 Configuración de puertos en SWBB _____	34
Figura 38 Asignación de IP _____	35
Figura 39 Asignación de IP _____	35
Figura 40 Asignación de IP _____	36
Figura 41 Ping desde Pc1 a Pc4 y Pc 7 (Escenario 2) _____	36
Figura 42 Ping desde Pc2 a Pc5 y Pc 8 (Escenario 2) _____	37
Figura 43 Ping desde Pc3 a Pc6 y Pc 9 (Escenario 2) _____	38
Figura 44 Ping desde Pc1 a Pc2, Pc3, Pc5, Pc6 Pc8 y Pc 9 (Escenario 2) _____	39
Figura 45 Ping desde SWT1 a SWBB y SWCC (Escenario 2) _____	40
Figura 46 Ping desde SWT1 a SWBB y SWAA (Escenario 1) _____	40
Figura 47 Ping desde SWT2 a SWAA y SWCC (Escenario 2) _____	41
Figura 48 Ping desde SWAA a los Pc (Escenario 2) _____	42

## LISTA DE TABLAS

Table 1 Información para configuración de los Routers_____	14
Table 2 Comandos de configuración inicial de los routers_____	15
Table 3 Direccionamiento de los PCs (Escenario 2) _____	32
Table 4 Direccionamiento SVI (Escenario 2) _____	35



## GLOSARIO

**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

**CCNP:** Certificación en Routing y Switching, expedida por la compañía CISCO.

**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.

**Dirección IP:** Dirección de protocolo de Internet, la forma estándar de identificar un equipo que está conectado a Internet, de forma similar a como un número de teléfono identifica un aparato de teléfono en una red telefónica.

**EIGRP:** Protocolo de enrutamiento de puerta de enlace interior mejorado, el cual usa como parámetro la distancia y calidad del canal.

**EtherChannel:** Arreglo Lógico para la agrupación de varios enlaces físicos de forma que se suman sus velocidades obteniendo un enlace troncal de alta velocidad.

**INTERFAZ:** Es la conexión entre dos ordenadores o máquinas de cualquier tipo dando una comunicación entre distintos niveles.

**IPV4:** El Protocolo de Internet versión 4, en inglés: Internet Protocol version 4 (IPv4), es la cuarta versión del Internet Protocol (IP). Es uno de los protocolos centrales de los métodos estándares de interconexión de redes basados en Internet, y fue la primera versión implementada para la producción de ARPANET, en 1983.

**IPV6:** IPv6 es la versión 6 del Protocolo de Internet (IP por sus siglas en inglés, Internet Protocol), es el encargado de dirigir y encaminar los paquetes en la red, fue diseñado en los años 70 con el objetivo de interconectar redes.

**OSPF:** Camino más cortó abierto; protocolo de enrutamiento que proporciona la ruta más corta.

**VLAN:** Red Virtual de Área Local; arreglo lógico que distingue un conjunto de paquetes de otros independizándolos.

## RESUMEN

Finalizando el Diplomado de profundización CCNP (Cisco Certified Network Professional), Plantea como actividad final ejecutar la solución de la “Prueba de habilidades”, cuyo objetivo principal es demostrar las capacidades del estudiante, y verificar los conocimientos adquiridos mediante la solución de ejercicios donde tenga que ajustar la configuración básica de enrutamiento interno y/o externo, también el uso de los comandos básicos relacionados con enlaces, troncales y vlans.

El manejo de los módulos CCNP ROUTE, donde se relacionan los principios básicos de la red y los protocolos de enrutamiento IP versión 4 (IPv4) e IP versión 6 (IPv6), el Protocolo de enrutamiento de gateway interior mejorado (EIGRP), el protocolo Primer camino más corto (OSPF) y el protocolo de puesta de enlace de frontera (BGP).

El módulo CCNP SWITCH que permite apropiar la implementación, monitoreo y administración de la conmutación en una arquitectura de redes, la implementación de VLANs en redes corporativas, y la configuración y optimización para una alta disponibilidad y redundancia en los switches de capa dos y capa tres.

Palabras calves: CCNP, Conmutación, cisco, enrutamientos, redes, vlan. Router, switch

## **ABSTRACT**

Finishing the Diploma of deepening CCNP (Cisco Certified Network Professional), It raises as final activity to execute the solution of the "Test of skills", whose main objective is to demonstrate the abilities of the student, and verify the knowledge acquired through the solution of exercises where you have They adjust the basic internal and / or external routing settings, also the use of basic commands related to links, trunks and vlans.

The handling of the CCNP ROUTE modules, where the basic principles of the network and the routing protocols IP version 4 (IPv4) and IP version 6 (IPv6), the Enhanced Interior Gateway Routing Protocol (EIGRP), the protocol are related First Shortest Path (OSPF) and Border Link Putting Protocol (BGP).

The CCNP SWITCH module that enables the deployment, monitoring and management of switching in a network architecture, the implementation of VLANs in corporate networks, and the configuration and optimization for high availability and redundancy in layer two and layer three switches.

Key words: CCNP, Switching, Cisco, routing, networks, vlan. Router, switch

## INTRODUCCIÓN

La prueba de habilidades del Diplomado CCNP, es conocer el nivel de las capacidades y habilidades que aprendimos durante el desarrollo del curso, esta práctica pondrá a prueba al estudiante mediante el desarrollo de soluciones en problemas relacionados con redes. La actividad plantea dos escenarios los cuales se deben ajustar las configuraciones necesarias para lograr solventar la falla y dar solución exitosa al ejercicio propuesto.

En primera instancia contamos con un primer escenario donde se deberá configurar e interconectar cada uno de los dispositivos que hacen parte del ejercicio, siguiendo todos los lineamientos para el direccionamiento IP, protocolos de enrutamiento y otros aspectos que componen la topología de red.

Por otra parte, tenemos el segundo escenario en el cual se deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los protocolos establecidos para el direccionamiento IP, etherchannels, VLANs y demás aspectos que forman parte del escenario propuesto.

Finalmente, con el desarrollo de este proyecto se pretende emplear herramientas de simulación y laboratorios de acceso remoto con el fin de establecer y dar solución a dos escenarios, los cuales exigen un amplio manejo y conocimiento en CCNP ROUTE y CCNP SWITCH.

## Desarrollo del trabajo

### 1. Escenario 1

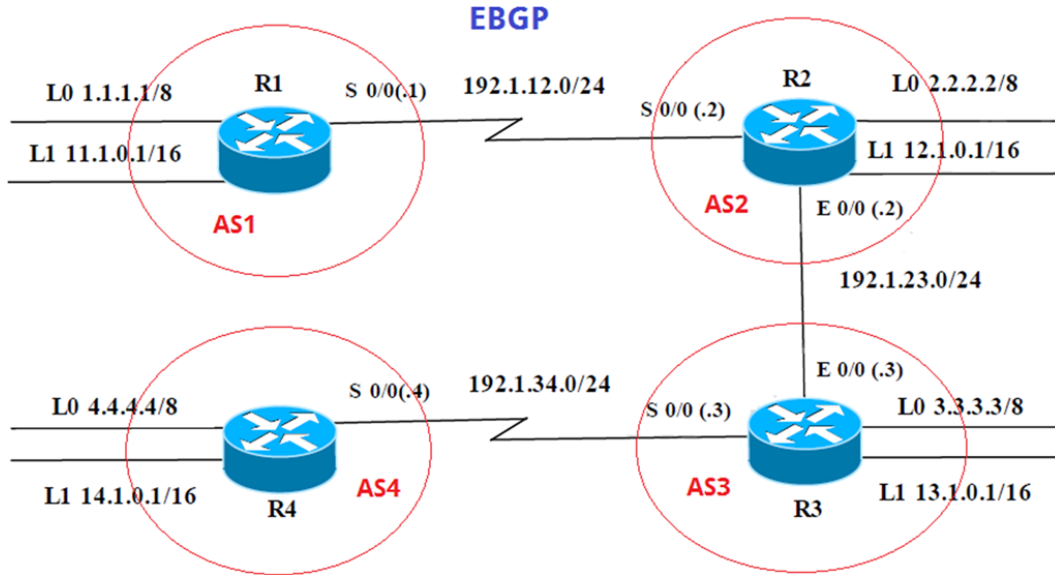


Figura 1 Topología en packet tracer (Escenario 1)

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

R1

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

R2

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

**R3**

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

**R4**

*Table 1 Información para configuración de los Routers*

Configuración básica inicial: Para este escenario debido a que no se asignan contraseñas para acceso por consola, enable y/o de acceso remoto, solo fue necesario la configuración del nombre de los routers, el banner de inicio, y la configuración de las interfaces

<b>R1</b>	<pre> configure terminal hostname R1 banner motd "Acceso restringido" interface serial 0/0/0 ip add 192.1.12.1 255.255.255.0 clock rate 64000 no shutdown description conecta con R2 exit interface Loopback0 ip address 1.1.1.1 255.0.0.0 interface Loopback1 R1(config-if)#ip address 11.1.0.1 255.255.0.0 copy running-config startup-config </pre>
<b>R2</b>	<pre> configure terminal hostname R2 banner motd "Acceso restringido" interface serial 0/0/0 ip address 192.1.12.2 255.255.255.0 no shutdown description conecta con R1 interface Loopback0 ip address 2.2.2.2 255.0.0.0 </pre>

	<pre> interface Loopback1 ip address 12.1.0.1 255.255.0.0 interface gigabitEthernet 0/0 ip address 192.1.23.2 255.255.255.0 no shutdown description conecta con R3 copy running-config startup-config </pre>
<b>R3</b>	<pre> configure terminal hostname R3 banner motd "Acceso restringido" interface serial 0/0/0 ip address 192.1.34.3 255.255.255.0 no shutdown interface ge0/0 ip address 192.1.23.3 255.255.255.0 no shutdown description conecta con R2 interface lo0 ip address 3.3.3.3 255.0.0.0 interface lo1 ip address 13.1.0.1 255.255.0.0 copy running-config startup-config </pre>
<b>R4</b>	<pre> configure terminal hostname R4 banner motd "Acceso restringido" interface s0/0/0 ip address 192.1.34.4 255.255.255.0 clock rate 64000 no shutdown description conecta con R3 exit interface lo0 ip address 4.4.4.4 255.0.0.0 interface lo1 ip address 14.1.0.1 255.255.0.0 copy running-config startup-config </pre>

*Table 2 Comandos de configuración inicial de los routers*

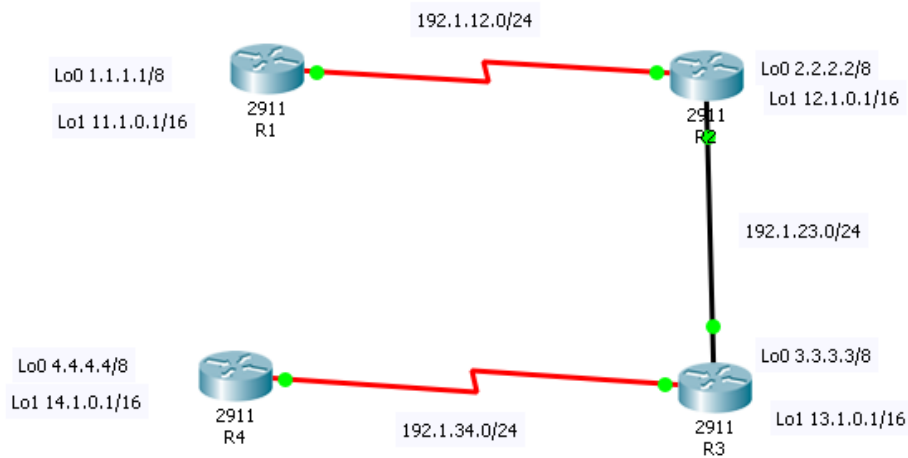


Figura 2 Escenario 1 Pack Tracer. (creado por: Autoría propia).

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**.

R1  
 router bgp 1  
 neighbor 192.1.12.2 remote-as 2  
 network 1.1.1.1 mask 255.0.0.0  
 network 11.1.0.1 mask 255.255.0.0  
 bgp router-id 22.22.22.22

```
R1#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router bgp 1
R1(config-router)#neighbor 192.1.12.2 remote-as 2
R1(config-router)#network 1.1.1.1 mask 255.0.0.0
R1(config-router)#network 11.1.0.1 mask 255.255.0.0
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.12.2 Up
%BGP-5-ADJCHANGE: neighbor 192.1.12.2 Up
|
```

Figura 3 Configuración de una relación de vecino BGP en R1



R2

```
router bgp 2
neighbor 192.1.12.1 remote-as 1
network 2.2.2.2 mask 255.0.0.0
network 12.1.0.1 mask 255.255.0.0
bgp router-id 33.33.33.33
```

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router bgp 2
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.12.1 Up
network 2.2.2.2 mask 255.0.0.0
R2(config-router)#network 12.1.0.1 mask 255.255.0.0
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.12.1 Up
```

Figura 4 Configuración de una relación de vecino BGP en R2

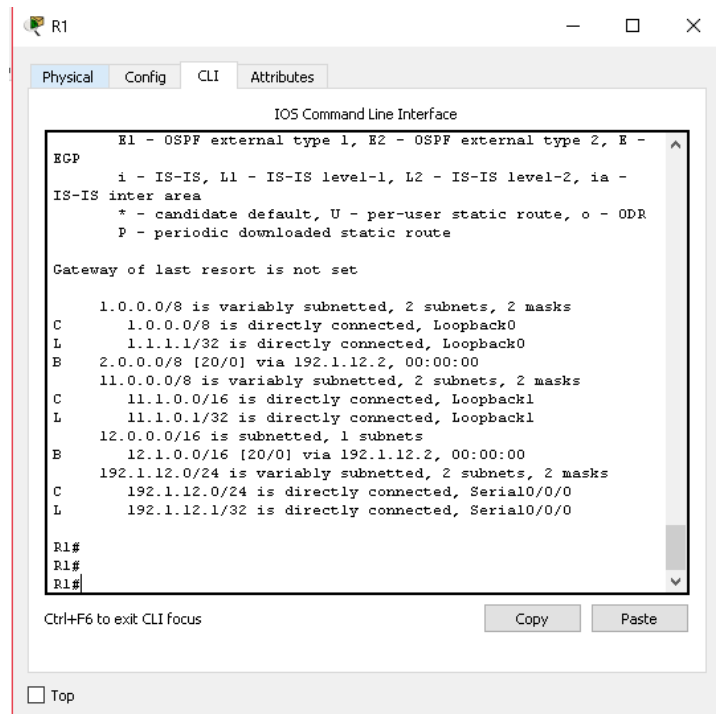


Figura 5 Tabla de enrutamiento de R1 con respecto a R2 (Escenario 1)

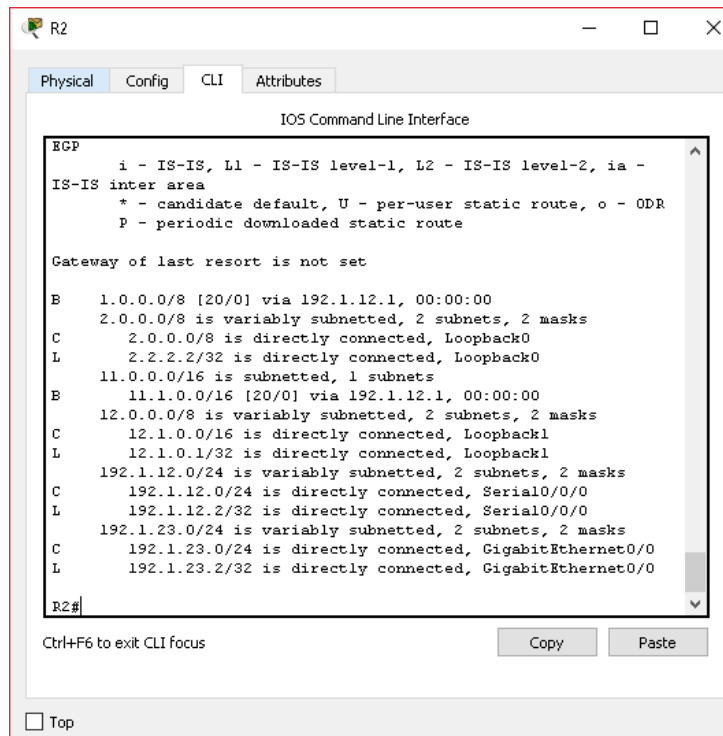


Figura 6 Tabla de enrutamiento de R2 con respecto a R1 (Escenario 1)

- 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)#neighbor 192.1.23.3 remote-as 3
```

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router bgp 2
R2(config-router)#neighbor 192.1.23.3 remote-as 3
R2(config-router)##BGP-5-ADJCHANGE: neighbor 192.1.23.3 Up
%BGP-5-ADJCHANGE: neighbor 192.1.23.3 Up
```

Figura 7 Configuración de una relación de vecino BGP en R2

```
R3(config)#router bgp 3
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#network 3.3.3.3 mask 255.0.0.0
```

```
R3(config-router)#network 13.1.0.1 mask 255.255.0.0
R3(config-router)#bgp router-id 44.44.44.44
```

```
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router bgp 3
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#*BGP-5-ADJCHANGE: neighbor 192.1.23.2 Up
network 3.3.3.3 mask 255.0.0.0
R3(config-router)#network 13.1.0.1 mask 255.255.0.0
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#*BGP-5-ADJCHANGE: neighbor 192.1.23.2 Up
```

Figura 8 Configuración de una relación de vecino BGP en R3

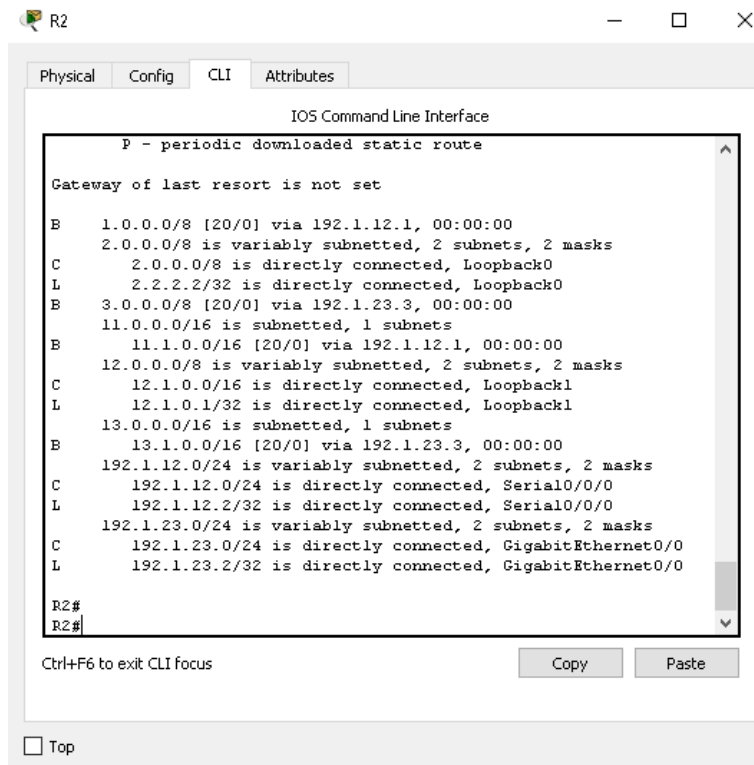


Figura 9 Tabla de enrutamiento de R2 con respecto a R3 (Escenario 1)

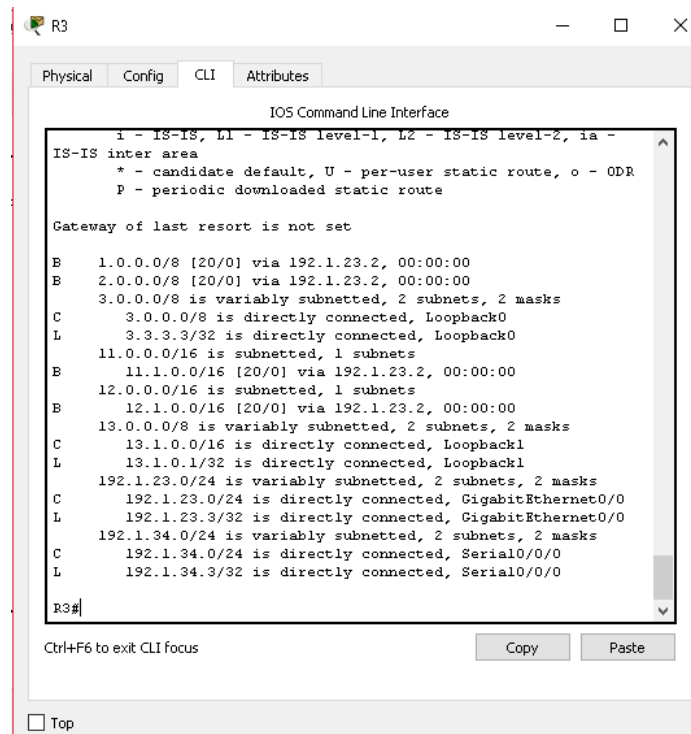


Figura 10 Tabla de enrutamiento de R3 con respecto a R2 (Escenario 1)

- 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:

```

R3(config)#router bgp 3
R3(config-router)# neighbor 192.1.34.4 remote-as 4
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router bgp 3
R3(config-router)# neighbor 192.1.34.4 remote-as 4
R3(config-router)#*BGP-5-ADJCHANGE: neighbor 192.1.34.4 Up
*BGP-5-ADJCHANGE: neighbor 192.1.34.4 Up

```

Figura 11 Configuración de una relación de vecino BGP en R3

R4:

```
router bgp 4
neighbor 192.1.34.3 remote-as 3
network 14.1.0.1 mask 255.255.0.0
network 4.4.4.4 mask 255.0.0.0
bgp router-id 66.66.66.66
```

```
R4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#
R4(config)#router bgp 4
R4(config-router)#neighbor 192.1.34.3 remote-as 3
R4(config-router)##%BGP-5-ADJCHANGE: neighbor 192.1.34.3 Up

R4(config-router)#network 14.1.0.1 mask 255.255.0.0
R4(config-router)#network 4.4.4.4 mask 255.0.0.0
R4(config-router)#bgp router-id 66.66.66.66
R4(config-router)##%BGP-5-ADJCHANGE: neighbor 192.1.34.3 Up
```

Figura 12 Configuración de una relación de vecino BGP en R4

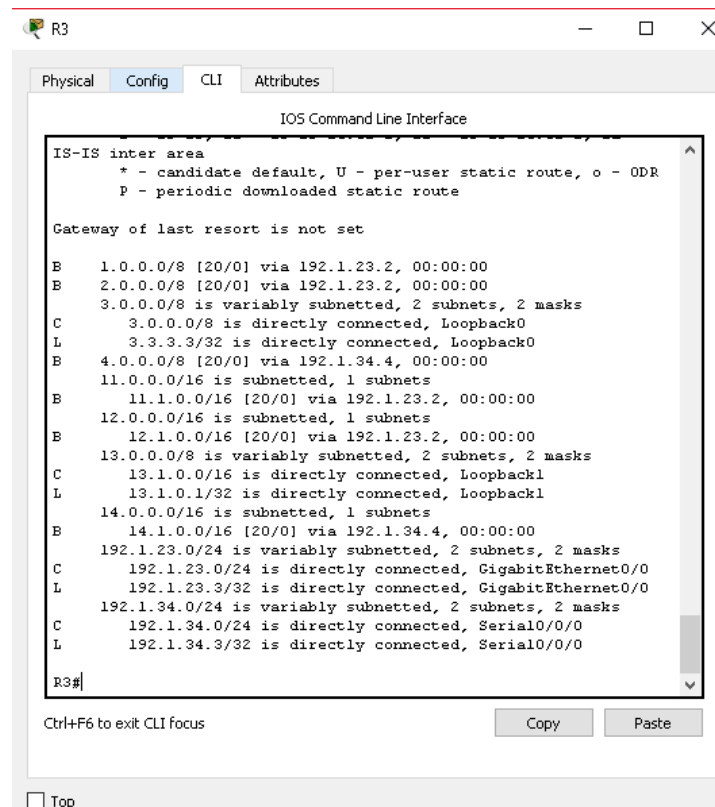


Figura 13 Tabla de enrutamiento de R3 con respecto a R4 (Escenario 1)

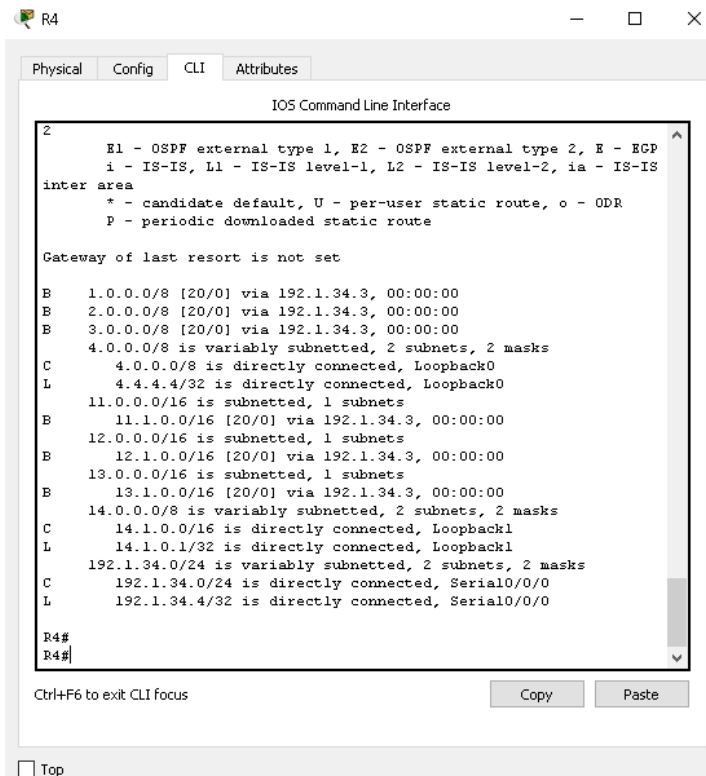


Figura 14 Tabla de enrutamiento de R4 con respecto a R3 (Escenario 1)

## 2. Escenario 2

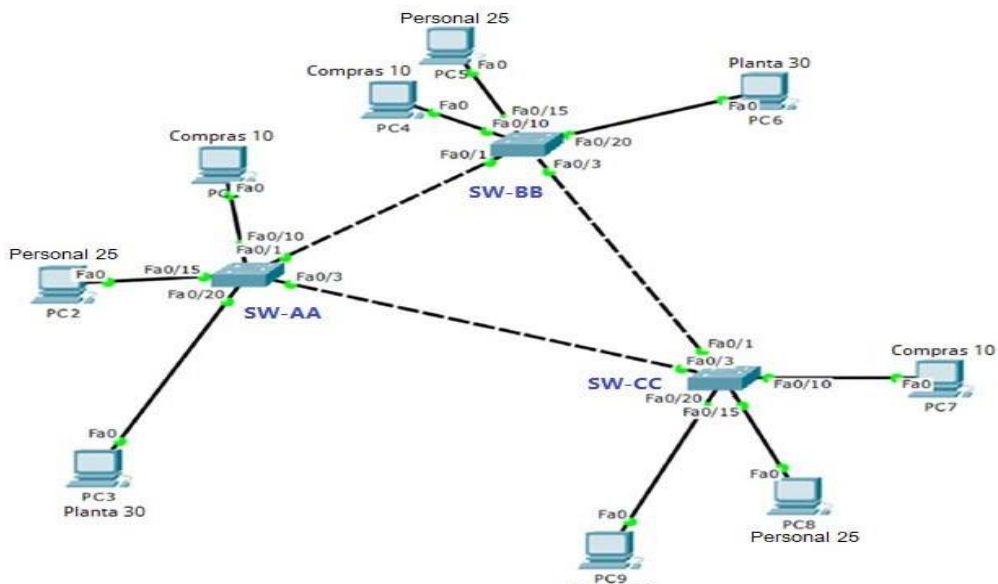


Figura 15 Topología en packet tracer (Escenario 2)

## 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.

SWBB:

```
vtp domain CCNP  
vtp version 2  
vtp mode server  
vtp password cisco
```

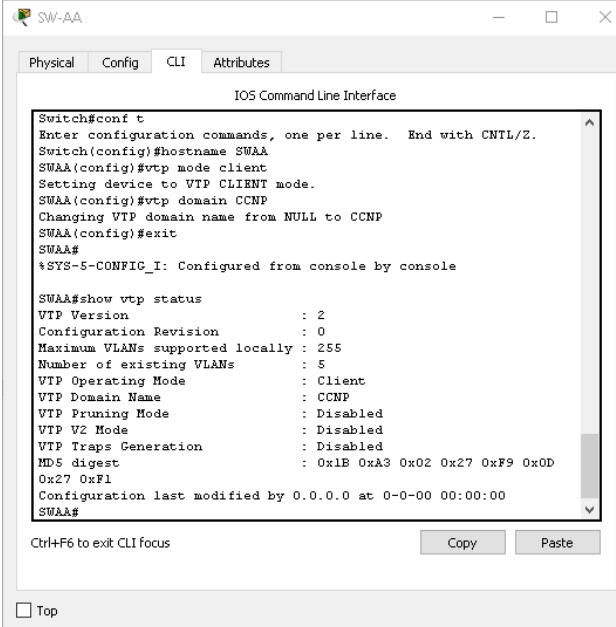
SWAA:

```
hostname SWAA  
vtp mode client  
vtp domain CCNP
```

SWCC:

```
hostname SWCC  
vtp mode client  
vtp domain CCNP
```

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



```
SW-AA  
Physical Config CLI Attributes  
IOS Command Line Interface  
Switch#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#hostname SWAA  
SWAA(config)#vtp mode client  
Setting device to VTP CLIENT mode.  
SWAA(config)#vtp domain CCNP  
Changing VTP domain name from NULL to CCNP  
SWAA(config)#exit  
SWAA#  
*SYS-5-CONFIG_I: Configured from console by console  
  
SWAA#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 : 0x1E 0xA3 0x02 0x27 0xF9 0x0D  
0x27 0xF1  
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00  
SWAA#
```

Figura 16 Verificación Vtp status en SWAA (Escenario 2)

SW-BB

Physical Config CLI Attributes

IOS Command Line Interface

```
Switch(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
Switch(config)#vtp version 2
Switch(config)#vtp mode server
Device mode already VTP SERVER.
Switch(config)#vtp password cisco
Setting device VLAN database password to cisco
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#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          : 0x9F 0x90 0x77 0xCE 0x81 0x8D
0xD9 0x02
Configuration last modified by 0.0.0.0 at 3-1-93 00:27:09
Local updater ID is 0.0.0.0 (no valid interface found)
Switch#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Figura 17 Verificación Vtp status en SWBB (Escenario 2)

SW-CC

Physical Config CLI Attributes

IOS Command Line Interface

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SWCC
SWCC(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWCC(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SWCC(config)#exit
SWCC#
%SYS-5-CONFIG_I: Configured from console by console

SWCC#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          : 0x1B 0xA3 0x02 0x27 0xF9 0x0D
0x27 0xF1
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SWCC#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Figura 18 Verificación Vtp status en SWCC (Escenario 2)



## B. Configurar DTP (Dynamic Trunking Protocol)

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.

```
SWAA
interface fastEthernet 0/1
switchport mode dynamic auto
```

```
-----
SWAA(config)#interface fastEthernet 0/1
SWAA(config-if)#switchport mode dynamic auto
SWAA(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
```

Figura 19 Configuración de enlace troncal SWAA

```
SWBB
interface fastEthernet 0/1
switchport mode dynamic desirable
```

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode dynamic desirable

Switch(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
```

Figura 20 Configuración de enlace troncal SWBB

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

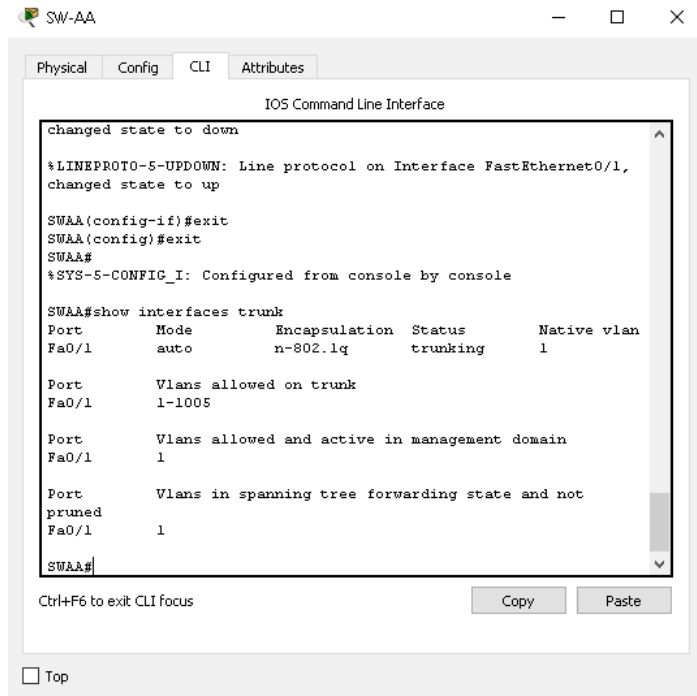


Figura 21 Verificación interface troncal de SWBB a SWAA (Escenario 2)

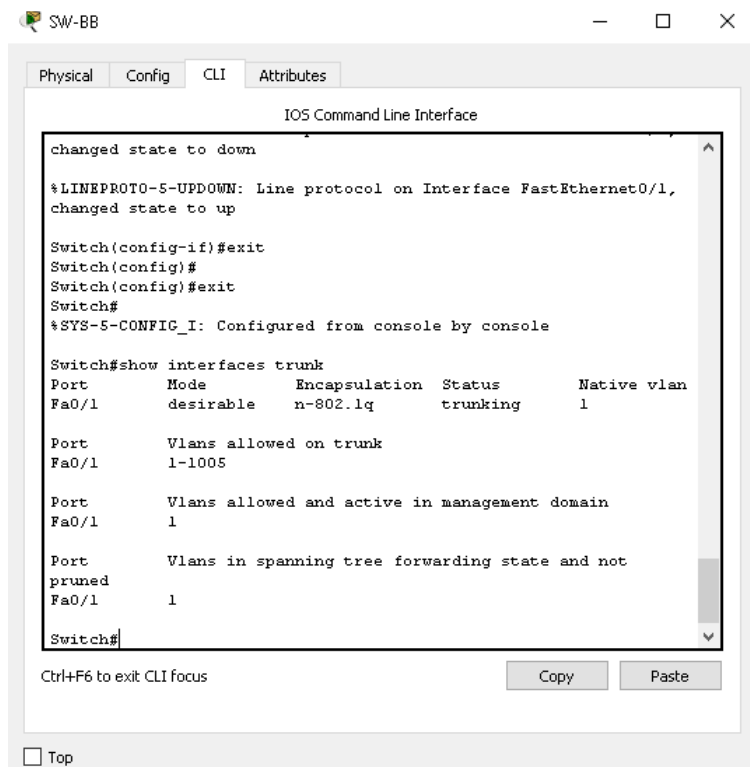


Figura 22 Verificación interface troncal de SWBB a SWAA (Escenario 2)

- 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

```

interface fastEthernet 0/3
switchport mode trunk

```

```

SWAA#
SWAA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SWAA(config)#interface fastEthernet 0/3
SWAA(config-if)#switchport mode trunk

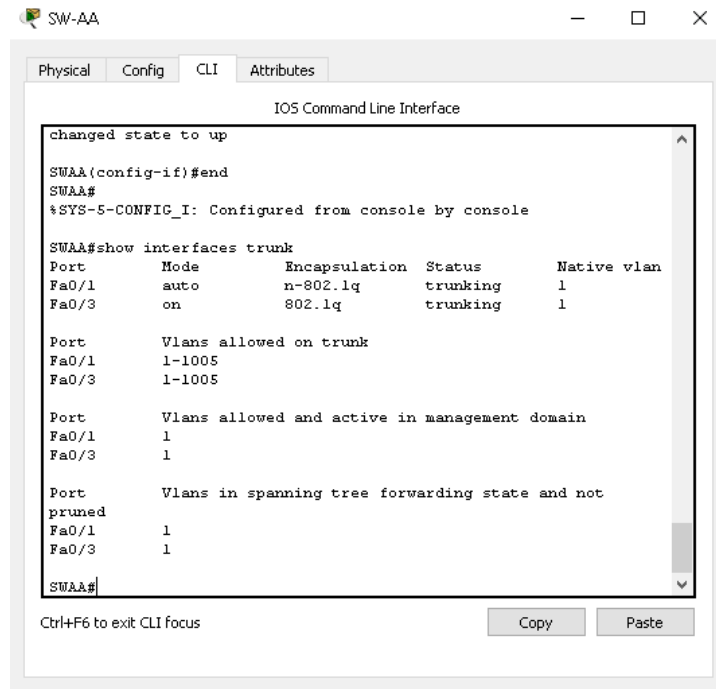
SWAA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to up
|

```

Figura 23 configuración un enlace trunk SWAA

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



```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
changed state to up
SWAA(config-if)#end
SWAA#
%SYS-5-CONFIG_I: Configured from console by console
SWAA#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     1
Fa0/3     1
SWAA#
```

Figura 24 Verificación interface troncal de SWAA a SWCC (Escenario 2)

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

SWBB:

```
interface fastEthernet 0/3
switchport mode trunk
```

```
Switch#CONF
Configuring from terminal, memory, or network [terminal]? T
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport mode trunk

Switch(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

Switch(config-if)#
```

Figura 25 enlace trunk permanente entre SW-BB

SWCC

```
interface fastEthernet 0/1
switchport mode trunk
```

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

SWCC(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

SWCC(config-if)#
```

Figura 26 enlace trunk permanente entre SW-CC

### C. Agregar VLANs y asignar puertos.

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

SWAA(config)#VLAN 10 VTP VLAN configuration not allowed when device is in CLIENT mode.

La Vlan 10 no puede ser agregada en el SWT1 debido a que se encuentra en modo cliente, se agrega a través de SWT2 que funciona en modo server.

```
SWAA(config)#VLAN 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
SWAA(config)#
SWAA(config)#
```

Figura 27 Configuración de VLAN en SWAA

```
vlan 10
name Compras
vlan 25
name Personal
vlan 30
name Planta
vlan 99
name Admon
```

```

SWBB#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
SWBB(config)#vlan 10
SWBB(config-vlan)#name Compras
SWBB(config-vlan)#vlan 25
SWBB(config-vlan)#name Personal
SWBB(config-vlan)#vlan 30
SWBB(config-vlan)#name Planta
SWBB(config-vlan)#vlan 99
SWBB(config-vlan)#name Admon
SWBB(config-vlan)#
SWBB(config-vlan)#

```

Figura 28 Configuración de VLANs en SWBB

9. Verifique que las VLANs han sido agregadas correctamente.

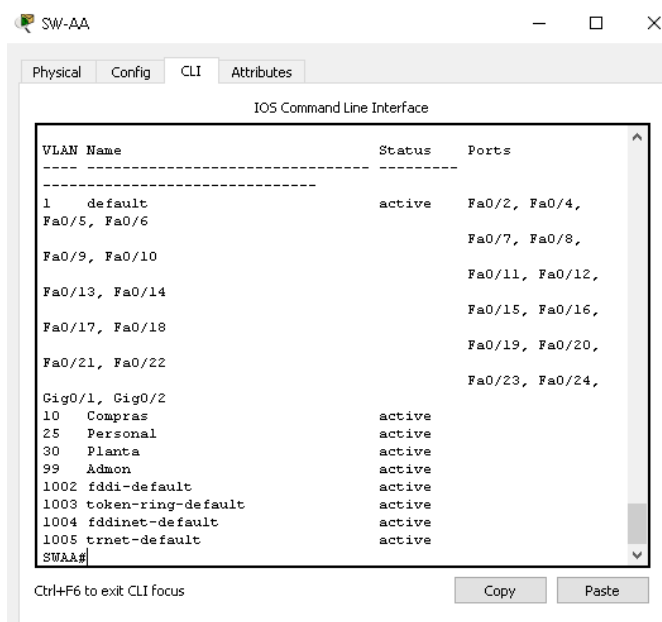


Figura 29 Verificación Vlan agregadas en SWAA (Escenario 2)

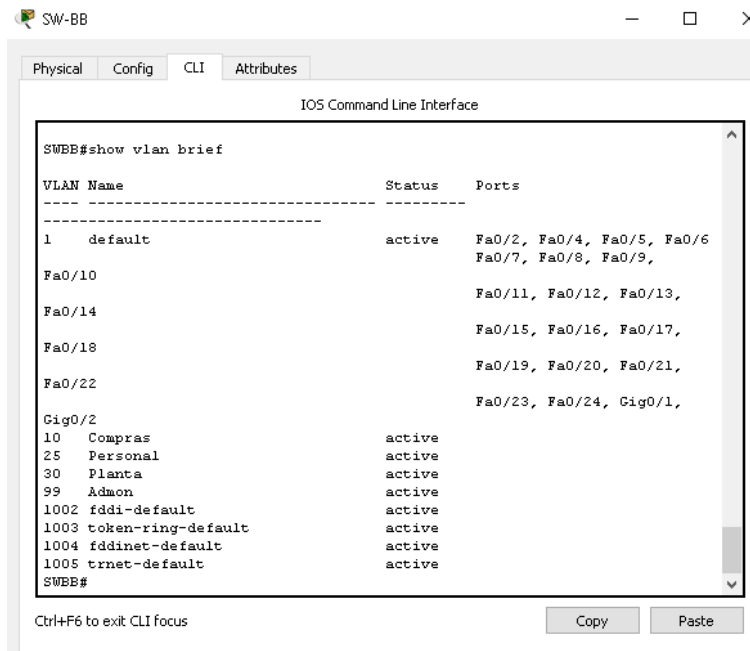


Figura 30 Verificación Vlans agregadas en SWBB (Escenario 2)

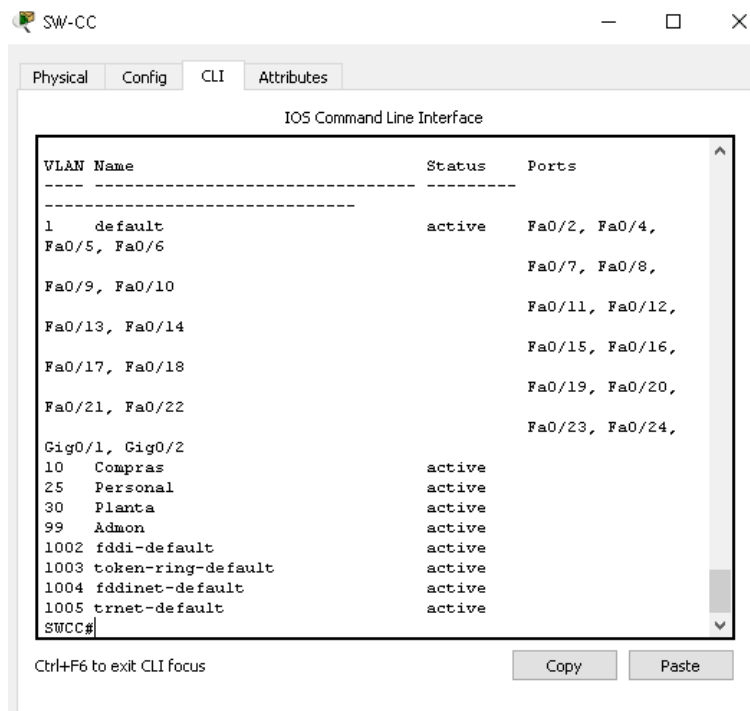


Figura 31 Verificación Vlans agregadas en SWCC (Escenario 2)

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 10	190.108.10.X / 24
F0/15	VLAN 25	190.108.20.X /24
F0/20	VLAN 30	190.108.30.X /24

*Table 3 Direccionamiento de los PCs (Escenario 2)*

Se asignan a cada uno de los PCs el direccionamiento correspondiente según la vlan a la que pertenecen.

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

SWAA

```
interface fastEthernet 0/10
switchport mode access
switchport access vlan 10
```

```
SWAA#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
SWAA(config)#interface fastEthernet 0/10
SWAA(config-if)#switchport mode access
SWAA(config-if)#switchport access vlan 10
```

*Figura 32 Configuración el puerto F0/10 en modo de acceso para SW-AA*

SWBB

```
interface fastEthernet 0/10
switchport mode access
switchport access vlan 10
```



```

SWBB#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
SWBB(config)#interface fastEthernet 0/10
SWBB(config-if)#switchport mode access
SWBB(config-if)#switchport access vlan 10
SWBB(config-if)#

```

Figura 33 Configuración el puerto F0/10 en modo de acceso para SW-BB

## SWCC

```

interface fastEthernet 0/10
switchport mode access
switchport access vlan 10

```

```

SWCC#CONF T
Enter configuration commands, one per line.  End with CNTL/Z.
SWCC(config)#interface fastEthernet 0/10
SWCC(config-if)#switchport mode access
SWCC(config-if)#switchport access vlan 10
SWCC(config-if)#

```

Figura 34 Configuración el puerto F0/10 en modo de acceso para SW-CC

- 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.

## SWAA:

```

interface fastEthernet 0/15
switchport mode access
switchport access vlan 25
interface fastEthernet 0/20
switchport mode access
switchport access vlan 30

```

```

SWAA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SWAA(config)#interface fastEthernet 0/15
SWAA(config-if)#switchport mode access
SWAA(config-if)#switchport access vlan 20
SWAA(config-if)#interface fastEthernet 0/20
SWAA(config-if)#switchport mode access
SWAA(config-if)#switchport access vlan 30
SWAA(config-if)#
SWAA(config-if)#

```

Figura 35 Configuración de puertos en SWAA

SWBB:

```
interface fastEthernet 0/15
switchport mode access
switchport access vlan 25
interface fastEthernet 0/20
switchport mode access
switchport access vlan 30
```

```
SWBB#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SWBB(config)#interface fastEthernet 0/15
SWBB(config-if)#switchport mode access
SWBB(config-if)#switchport access vlan 20
% Access VLAN does not exist. Creating vlan 20
SWBB(config-if)#interface fastEthernet 0/20
SWBB(config-if)#switchport mode access
SWBB(config-if)#switchport access vlan 30
SWBB(config-if)#
SWBB(config-if)#
```

Figura 36 Configuración de puertos en SWBB

SWCC:

```
interface fastEthernet 0/15
switchport mode access
switchport access vlan 25
interface fastEthernet 0/20
switchport mode access
switchport access vlan 30
```

```
SWCC#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SWCC(config)#interface fastEthernet 0/15
SWCC(config-if)#switchport mode access
SWCC(config-if)#switchport access vlan 20
SWCC(config-if)#interface fastEthernet 0/20
SWCC(config-if)#switchport mode access
SWCC(config-if)#switchport access vlan 30
SWCC(config-if)#
```

Figura 37 Configuración de puertos en SWBB

#### D. Configurar las direcciones IP en los Switches.

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

Table 4 Direcciónamiento SVI (Escenario 2)

SWAA:

```
interface vlan 99
ip address 190.108.99.1 255.255.255.0
```

```
SWAA(config)#interface vlan 99
SWAA(config-if)#ip address 190.108.99.1 255.255.255.0
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
```

Figura 38 Asignación de IP

SWBB:

```
interface VLAN 99
ip address 190.108.99.2 255.255.255.0
```

```
SWBB(config)#interface VLAN 99
SWBB(config-if)#ip address 190.108.99.2 255.255.255.0
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to
up
```

Figura 39 Asignación de IP

SWCC:

```
interface vlan 99
ip address 190.108.99.3 255.255.255.0
```

```

SWCC(config)#interface vlan 99
SWCC(config-if)#ip address 190.108.99.3 255.255.255.0
SWCC(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up

```

Figura 40 Asignación de IP

## E. Verificar la conectividad Extremo a Extremo

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

```

PC1
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 190.108.10.3 with 32 bytes of data:
Reply from 190.108.10.3: bytes=32 time<1ms TTL=128
Reply from 190.108.10.3: bytes=32 time<1ms TTL=128
Reply from 190.108.10.3: bytes=32 time<1ms TTL=128
Reply from 190.108.10.3: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 190.108.10.1

Pinging 190.108.10.1 with 32 bytes of data:
Reply from 190.108.10.1: bytes=32 time<1ms TTL=128
Reply from 190.108.10.1: bytes=32 time=1ms TTL=128
Reply from 190.108.10.1: bytes=32 time=7ms TTL=128
Reply from 190.108.10.1: bytes=32 time=1ms TTL=128

Ping statistics for 190.108.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 2ms

C:\>

```

Figura 41 Ping desde Pc1 a Pc4 y Pc 7 (Escenario 2)

Los pings fueron exitosos ya que los pc se encuentran en la misma vlan (10)

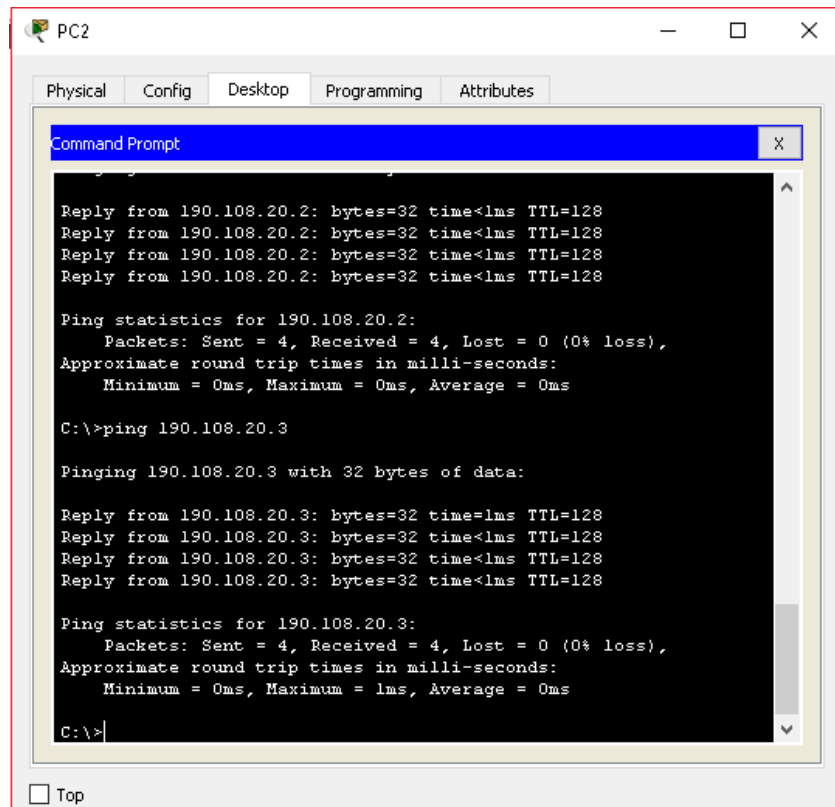


Figura 42 Ping desde Pc2 a Pc5 y Pc 8 (Escenario 2)

Fueron exitosos debido a que los pc se encuentran en la misma vlan (25)

PC3

```
Physical  Config  Desktop  Programming  Attributes
Command Prompt

Pinging 190.108.30.2 with 32 bytes of data:

Reply from 190.108.30.2: bytes=32 time=53ms TTL=128
Reply from 190.108.30.2: bytes=32 time<1ms TTL=128
Reply from 190.108.30.2: bytes=32 time<1ms TTL=128
Reply from 190.108.30.2: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 53ms, Average = 13ms

C:\>ping 190.108.30.3

Pinging 190.108.30.3 with 32 bytes of data:

Reply from 190.108.30.3: bytes=32 time=56ms TTL=128
Reply from 190.108.30.3: bytes=32 time<1ms TTL=128
Reply from 190.108.30.3: bytes=32 time<1ms TTL=128
Reply from 190.108.30.3: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 56ms, Average = 14ms

C:\>
```

Figura 43 Ping desde Pc3 a Pc6 y Pc 9 (Escenario 2)

Fueron exitosos debido a que los pc se encuentran en la misma vlan (30)

```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 190.108.10.3: bytes=32 time=1ms TTL=128
Reply from 190.108.10.3: bytes=32 time=2ms TTL=128

Ping statistics for 190.108.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 190.108.20.1

Pinging 190.108.20.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.20.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.20.2

Pinging 190.108.20.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.20.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.20.3

Pinging 190.108.20.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
```

Figura 44 Ping desde Pc1 a Pc2, Pc3, Pc5, Pc6 Pc8 y Pc 9 (Escenario 2)

Los pings desde el Pc 1 (vlan 10), hacia los Pc2, Pc3, Pc5, Pc6 Pc8 y Pc 9 no fueron exitosos debido a que los pc de destino se encuentran en otras vlans.

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

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

SWAA#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 = 0/0/0
ms

SWAA#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 = 0/0/0
ms

SWAA#
```

Figura 45 Ping desde SWT1 a SWBB y SWCC (Escenario 2)

```
SW-BB
Physical Config CLI Attributes
IOS Command Line Interface
SWBB(config-if)#exit
SWBB(config)#interface fastEthernet 0/15
SWBB(config-if)#switchport mode access
SWBB(config-if)#switchport access vlan 25
SWBB(config-if)#interface fastEthernet 0/20
SWBB(config-if)#switchport mode access
SWBB(config-if)#switchport access vlan 30
SWBB(config-if)#end
SWBB#
%SYS-5-CONFIG_I: Configured from console by console

SWBB#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 = 0/0/0 ms

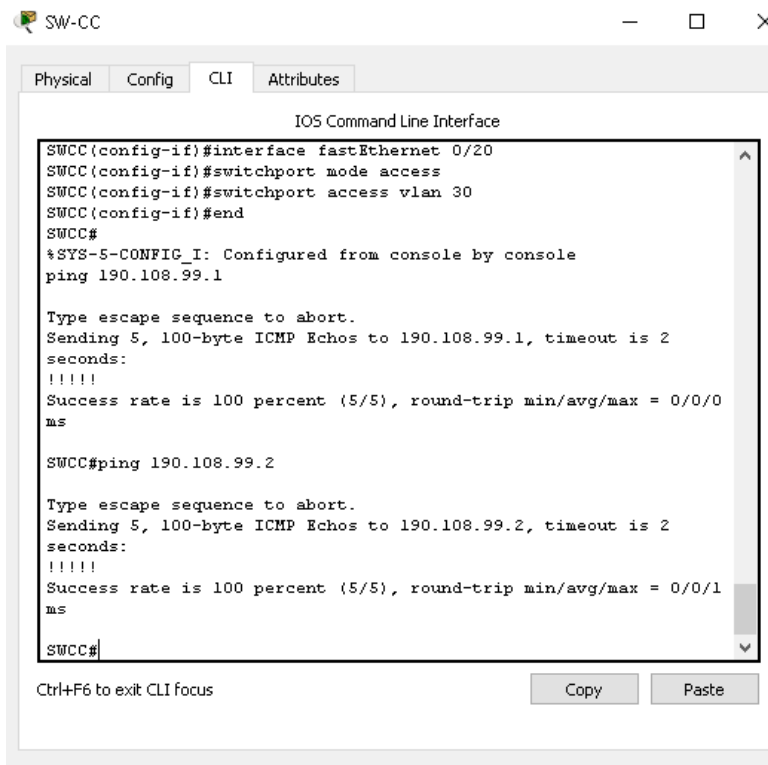
SWBB#ping 190.108.99.3

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 = 0/0/0 ms

SWBB#
```

Figura 46 Ping desde SWT1 a SWBB y SWAA (Escenario 1)





```
SW-CC
Physical Config CLI Attributes
IOS Command Line Interface
SWCC(config-if)#interface fastEthernet 0/20
SWCC(config-if)#switchport mode access
SWCC(config-if)#switchport access vlan 30
SWCC(config-if)#end
SWCC#
%SYS-5-CONFIG_I: Configured from console by console
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 = 0/0/0
ms

SWCC#ping 190.108.99.2

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

SWCC#
```

Ctrl+F6 to exit CLI focus      Copy      Paste

Figura 47 Ping desde SWT2 a SWAA y SWCC (Escenario 2)

El ping tuvo éxito debido a que los switches comparten la vlan 99 y cuentan con direccionamiento ip en esa interfaz virtual.

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

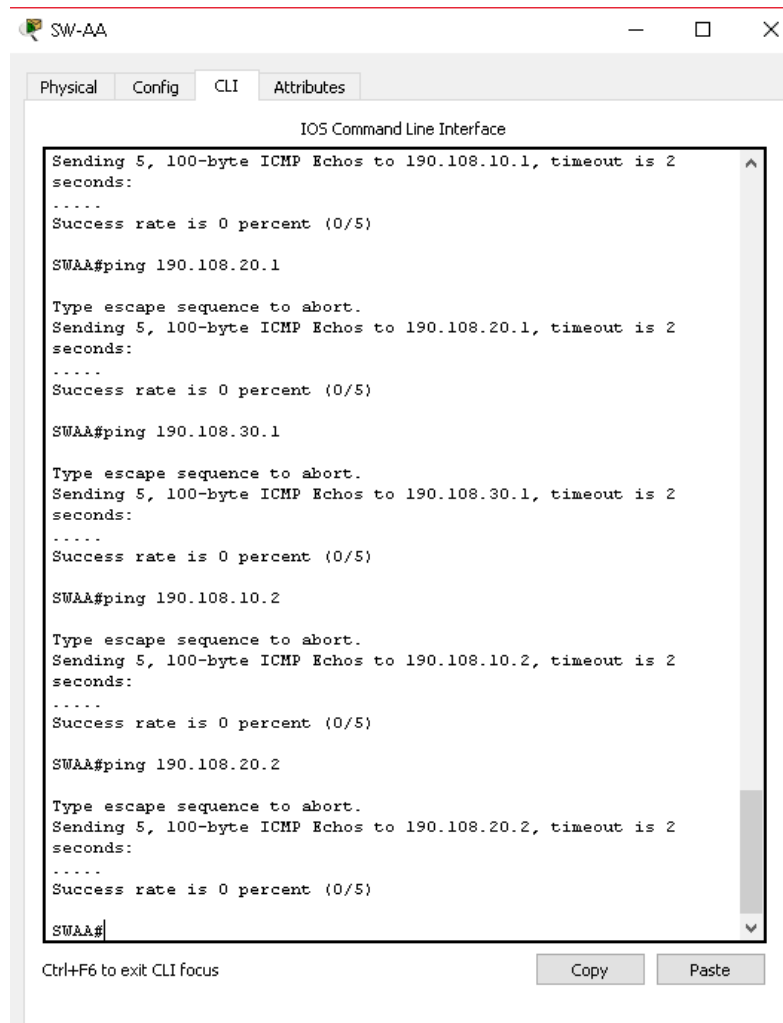


Figura 48 Ping desde SWAA a los Pc (Escenario 2)

los pings realizados desde los switch hacia cada uno de los Pc de la topología, no son exitosos debido a varias razones:

- No se crearon ni se configuraron en los switches interfaces virtuales con su respectivo direccionamiento para las vlan 10, vlan 25 y vlan 30.
- Las interfaces virtuales creadas en los switches están en la vlan 99 y los pc están en las vlan 10, 25 y 30 y en la topología no se implementaron dispositivos de capa 3 que permitan el enrutamiento entre las vlan.

## **CONCLUSIONES**

Se lograron identificar competencias y habilidades que fueron adquiridas a lo largo del diplomado para la comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Se logró implementar adecuadamente la ejecución de diferentes protocolos de enrutamiento, la integración de estos y la convergencia de la red, manifestada mediante la visualización de tablas de enrutamiento completas.

Se verificaron tablas de enrutamiento donde se verifican las rutas directamente conectadas y externas aprendidas mediante los protocolos OSPF, EIGRP y BGP.

El desarrollo de la actividad permitió planificar, implementar VLANs proporcionando segmentación y flexibilidad organizativa ayudando a implementar políticas de acceso y seguridad para grupos particulares de usuarios y limitar el dominio de difusión

## BIBLIOGRAFÍA

Donohue, D. (2017). CISCO Press (Ed). CCNP Quick Reference. Recuperado de <https://1drv.ms/b/s!AglGg5JUgUBthFt77ehzL5qp0OKD>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Switch Fundamentals Review. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Network Design Fundamentals. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Campus Network Architecture. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1InWR0hoMxgBNv1CJ>

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!AmIJYei-NT1InWR0hoMxgBNv1CJ>

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>

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

Macfarlane, J. (2014). Network Routing Basics: Understanding IP Routing in Cisco Systems. Recuperado

de <http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Path Control Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Enterprise Internet Connectivity. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing a Border Gateway Protocol (BGP). Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Routers and Routing Protocol Hardening. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx>

UNAD (2015). Switch CISCO - Procedimientos de instalación y configuración del IOS [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1IlyYRohwtwPUV64dg>