DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DORA LILIANA BONELO MANRIQUE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
SANTA FE DE BOGOTA D.C
2020

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

DORA LILIANA BONELO MANRIQUE

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
SANTA FE DE BOGOTA D.C
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

SANTA FE DE BOGOTA D.C, 22 de mayo de 2020

AGRADECIMIENTOS

En primera instancia agradezco a mis formadores, personas de gran sabiduría y a la universidad quienes se han esforzado por ayudarme a llegar hasta este punto enriqueciendo mi aprendizaje. A mi familia y a mi hijo, por su apoyo incondicional y acompañamiento permanente para hacer de este sueño una realidad.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Autentificación: mecanismos del sistema de información para poder identificar a los usuarios que acceden a sus recursos, y asegurar la integridad y autenticidad de los datos.

Bit: unidad básica de información en un ordenador. Sólo puede tener dos valores, 1 ó 0.

Red de Área Local (LAN o RAL): red física de interconexión a nivel local o departamental de varios ordenadores. Sólo permite conectar un número reducido de ordenadores

TCP/IP (Transport Control Protocol/Internet Protocol): Protocolo estándar desarrollado por la agencia de investigación de la defensa de USA como base para la red ARPANET (1983) y que es el utilizado por defecto en sistemas operativos abiertos y en la red Internet. Se utiliza para el intercambio de información entre ordenadores conectados a una red.

Dirección IP: 32 bits que identifican a un equipo en una red. Se representa en notación decimal punteada: cuatro bytes representados en decimal separados por puntos.

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

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

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

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

DHCP: Configuración Dinámica de protocolos para host; encargado de proveer de direccionamiento IP a dispositivos de forma automática.

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

RESUMEN

Para el desarrollo del Diplomado de profundización CISCO CCNP se ha identificado y utilizado la estrategia de aprendizaje fomentando el desarrollo de competencias mediante la elaboración de actividades en ambientes de simulación remota aprendimos los requisitos de red y los modelos de diseño para implementar servicios de enrutamiento avanzados en una red.

Implementando protocolos como EIGRP y OSPF, diversos mecanismos para controlar las actualizaciones de enrutamiento y el tráfico de red, implementando el protocolo BGP, monitorear y mantener la conmutación en la arquitectura de campus empresarial, implementar VLANs en redes, configurar y optimizar la alta disponibilidad y la redundancia en los switches para proporcionar redundancia de Capa 3. Implementar características de seguridad LAN y planificar y preparar la infraestructura de servicios avanzados en un campus empresarial.

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

ABSTRACT

For the development of the CISCO CCNP Depth Diploma, the learning strategy has been identified and used, promoting the development of competencies by preparing activities in remote simulation environments, learning the network requirements and design models to implement advanced routing services in a red

Implementing protocols such as EIGRP and OSPF, various mechanisms to control routing updates and network traffic, implementing the BGP protocol, monitoring and maintaining switching in the enterprise campus architecture, implementing VLANs in networks, configuring and optimizing high availability and redundancy in switches to provide Layer 3 redundancy. Implement LAN security features and plan and prepare advanced service infrastructure on a business campus.

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

INTRODUCCIÓN

En este trabajo se presenta una perspectiva de análisis y de aprendizaje de los conceptos adquiridos durante el curso para ser puestos en práctica durante el diplomado de profundización cisco, El módulo CCNP ROUTE aprendimos los requisitos de red y los modelos de diseño para implementar servicios de enrutamiento avanzados en una red, implementando protocolos como EIGRP y OSPF, diversos mecanismos para controlar las actualizaciones de enrutamiento y el tráfico de red, implementando el protocolo BGP para permitir que una red empresarial se conecte a un proveedor de servicio (ISP).

En el módulo CCNP SWITCH aprendimos a implementar, monitorear y mantener la conmutación en la arquitectura de campus empresarial, implementar VLANs en redes, configurar y optimizar la alta disponibilidad y la redundancia en los switches para proporcionar redundancia de Capa 3. Describir e implementar características de seguridad LAN y planificar y preparar la infraestructura de servicios avanzados en un campus empresarial.

El presente documento contiene el desarrollo de la Prueba de Habilidades desarrollo que logramos adquirir a lo largo del diplomado. Mediante los 2 escenarios propuestos se busca poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking, así como la configuración de áreas y sistemas autónomos respectivamente, el enrutamiento a través del protocolo BGP y el proceso de creación de adyacenticas en función del protocolo IPv4, del Router ID e interfaces Loopback. El segundo escenario se configurará una red basada en Switches capa 2 y PCs, se implementa protocolos como VLAN Trunking Protocol y Dynamic Trunking Protocol. Para los registros de los procesos de verificación de conectividad mediante el uso de comandos como ping, show ip route, show vtp status, show interfaces trunk, entre otros.

DESARROLLO

1. ESCENARIO 1

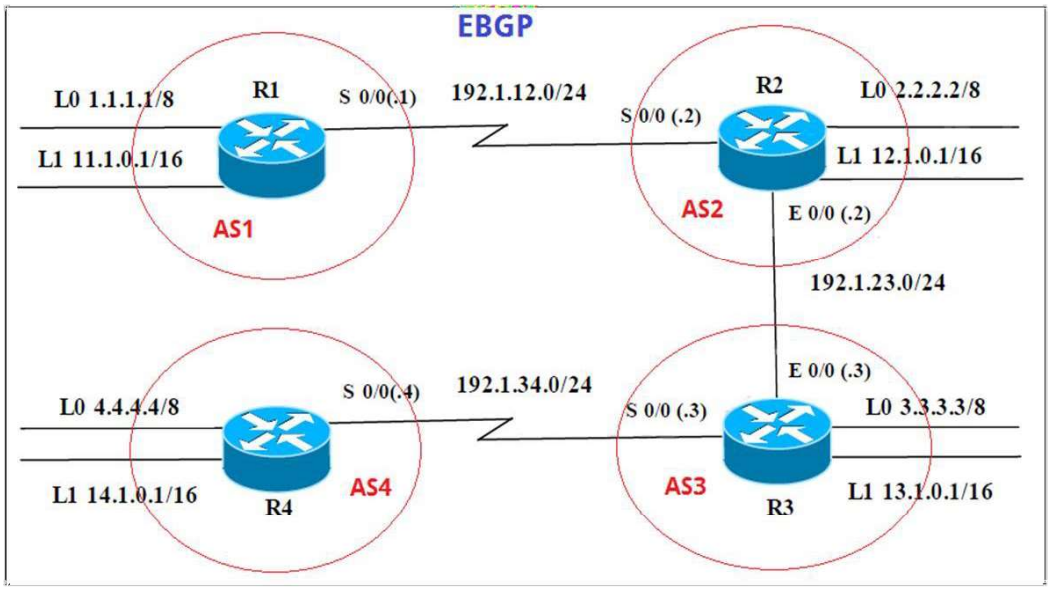


Figura 1. Escenario 1

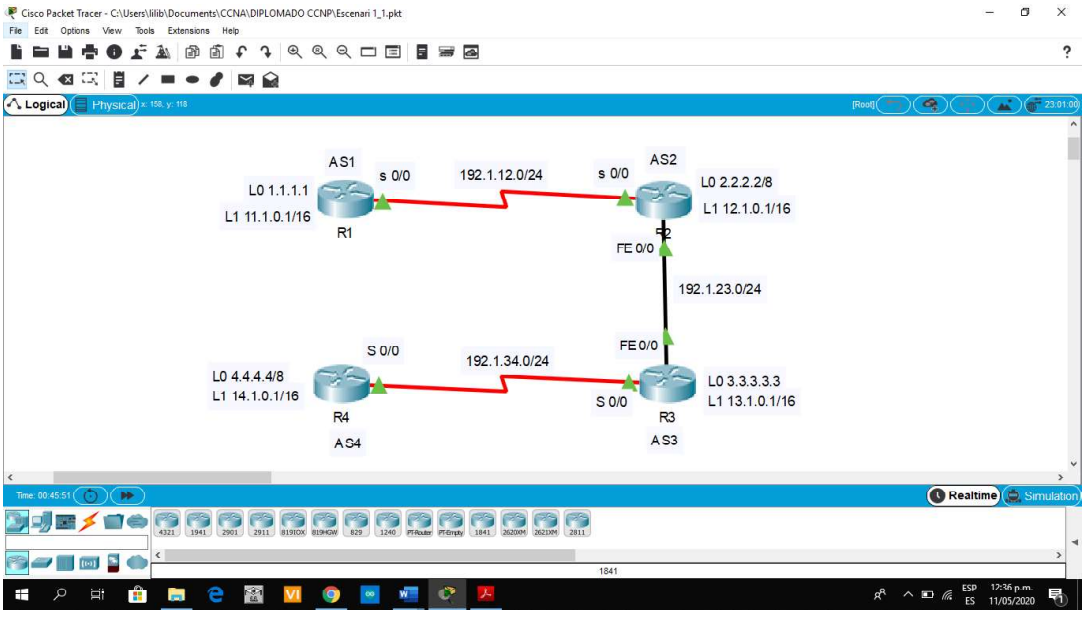


Figura 2. Simulación de escenario 1

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

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

Tabla 1. Interfaces loopback

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.

Se procede a configurar los enrutadores R1 Y R2.
Se asignan nombre y protocolos de comunicación mediante EIGRP que fueron asignados.

Se adjunta código y pantallazos con veracidad del código.

Configuración router 1.

Router>
Router>ena - **Ingreso a modo privilegiado**
Router#conf t - **Ingreso a modo de configuración**
Router(config)#hostname R1 - **asignamos un nombre al router**
R1(config)#^Z **para volver directamente a la petición de entrada de**

EXEC privilegiado en el nivel superior

R1#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#interface loopback 0 **- Configuracion de interfaz loopback**
R1(config-if) #ip address 1.1.1.1 255.0.0.0
R1(config-if) #interface loopback 1
R1(config-if) #
R1(config-if) #ip address 11.1.0.1 255.255.0.0
% 11.1.0.0 overlaps with Loopback1

R1(config)#interface loopback 1
R1(config-if) #ip address 11.1.0.1 255.255.0.0
R1(config-if) #interface Serial0/0/0
R1(config-if) #ip address 192.1.12.1 255.255.255.0
R1(config-if) #no shutdown
R1(config-if) #
R1(config-if) #exit

R1(config)#router bgp 1
R1(config-router) #bgp router-id 22.22.22.22
R1(config-router) #network 1.1.1.1 mask 255.0.0.0
R1(config-router) #network 11.1.0.0 mask 255.255.0.0
R1(config-router) #network 192.1.12.0 mask 255.255.255.0
R1(config-router) #neighbor 192.1.12.2 remote-as 2
R1(config-router) #

Ahora a el R1 le coloco el nombre de AS1.

R1(config)#hostname AS1 - **asignamos nombre AS1 al router**

Si le damos show ip route a AS, podemos validar que ya se configuro su tabla de enrutamiento las direcciones de loopback y las de red, lo cual indica que fueron aprendidas a través del protocolo BGP.

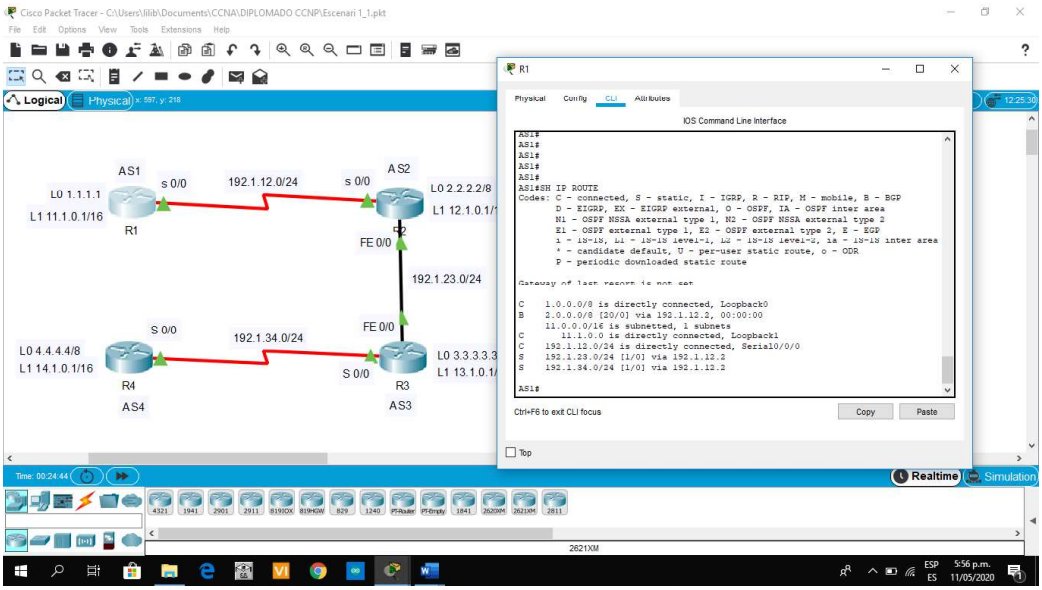


Figura 3. Aplicando código R1

Configuración router 2.

Router>ena
Router#conf t
Router(config)#hostname AS2
AS2(config)#^Z
AS2#
AS2#CONF T
AS2(config)#interface Loopback 0 - **configura la interfaz de loopback**
AS2(config-if) #ip address 2.2.2.2 255.0.0.0 - **asignación de IP.**
AS2(config-if) #interface loopback 1
AS2(config-if) #ip address 12.1.0.1 255.0.0.0
AS2(config-if) #interface serial 0/0/0 - **configura la interfaz**
AS2(config-if) #ip address 192.1.12.2 255.255.255.0
AS2(config-if) #no shutdown - **habilita una interfaz**.
AS2(config-if) #interface fastethernet 0/0
AS2(config-if) #ip address 192.1.23.2 255.255.255.0
AS2(config-if) #no shutdown **habilita una interfaz**.
AS2(config-if) #exit
AS2(config)#
AS2(config)#router bgp 2 - **Configuracion de bgp**
AS2(config-router) #bgp router-id 33.33.33.33 - **Configura el id del route**
AS2(config-router) #network 2.0.0.0 mask 255.0.0.0
AS2(config-router) #network 12.1.0.0 mask 255.255.0.0
AS2(config-router) #network 192.1.12.0 mask 255.255.255.0
AS2(config-router) #neighbor 192.1.12.1 remote-as 1
AS2(config-router) #%BGP-5-ADJCHANGE: neighbor 192.1.12.1 Up

AS2(config-router) #

Si le damos show ip route a AS2, podemos validar que ya se configuro su tabla de enrutamiento las direcciones de loopback y las de red, lo cual indica que fueron aprendidas a través del protocolo BGP.

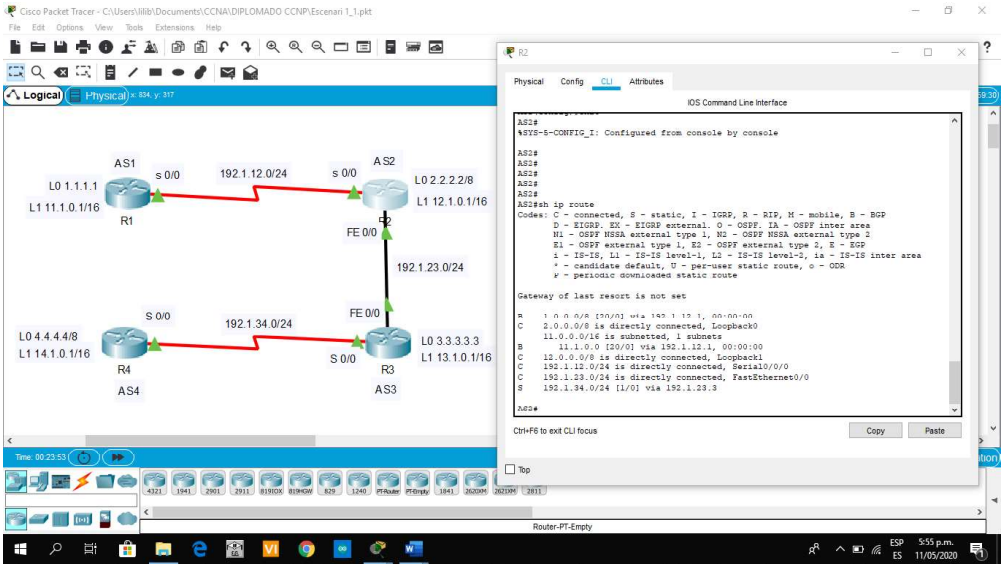


Figura 4. Aplicando código R2

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

Configuración router 2.

AS2(config)#
AS2(config)#route bgp 2
AS2(config-router) #network 192.1.23.0 mask 255.255.255.0
AS2(config-router) #neighbor 192.1.23.3 remote-as 3
AS2(config-router) #exit
AS2(config)#

Configuración router 3.

AS3(config)#
AS3(config)#interface loopback 0
AS3(config-if) #ip address 3.3.3.3 255.0.0.0
AS3(config-if) #interface loopback 1
AS3(config-if) #ip address 13.1.0.1 255.255.0.0

```
AS3(config-if) #interface fastethernet 0/0
AS3(config-if) #ip address 192.1.23.3 255.255.255.0
AS3(config-if) #no shutdown
AS3(config-if) #interface serial 0/0/0
AS3(config-if) #ip address 192.1.34.3 255.255.255.0
AS3(config-if) #no shutdown
AS3(config-if) #exit
AS3(config)#router bgp 3
AS3(config-router) #bgp router-id 44.44.44.44
AS3(config-router) #network 3.0.0.0 mask 255.0.0.0
AS3(config-router) #network 13.1.0.0 mask 255.255.0.0
AS3(config-router) #network 192.1.23.0 mask 255.255.255.0
AS3(config-router) #neighbor 192.1.23.2 remo
AS3(config-router) #neighbor 192.1.23.2 remote-as 2
AS3(config-router) #%BGP-5-ADJCHANGE: neighbor 192.1.23.2 Up
```

Si le damos **Show ip route** al AS2**,** se puede validar que se actualizo la tabla de enrutamiento y ya se visualiza las direcciones de loopback configuradas en R3, a través del protocolo BGP el route 2 ya aprendió 4 rutas.

En el route 3 se puede validar en la tabla de enrutamiento las redes que conoce y las configuradas en sus interfaces loopback y la red que lo comunica con los routes R3 y R4 y las interfaces loopback que se configuraron en los routes 1 y 2 ya que con el protocolo BGP dichas redes se anuncian en cada uno de los routers.

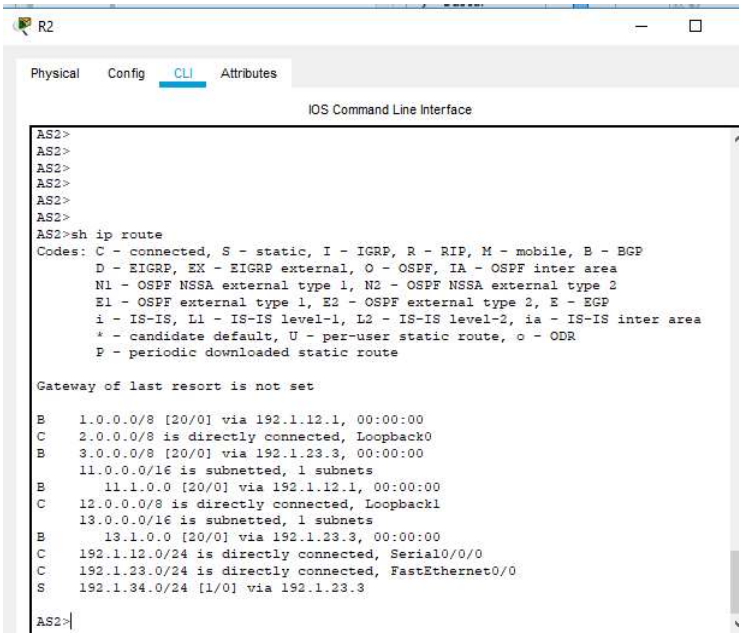


Figura 5. Aplicando código R2

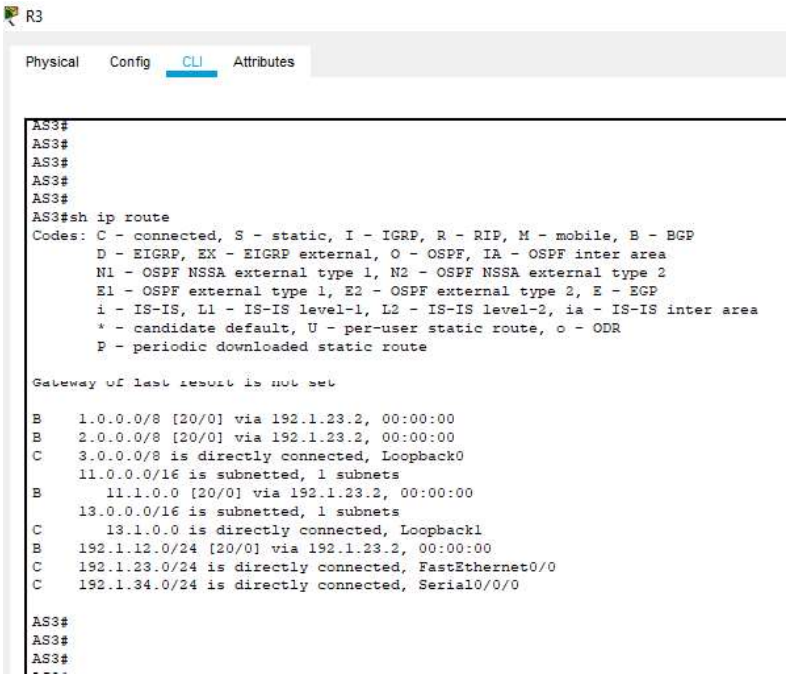


Figura 6. Aplicando código R3

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.

Configuración router 3.

AS3>ena
AS3#conf t
AS3(config)#router bgp 3
AS3(config-router) #network 192.1.34.0 mask 255.255.255.0
AS3(config-router) #neighbor 192.1.34.4 remote-as 4
AS3(config-router) #
AS3(config-router) #exit
AS3(config)#

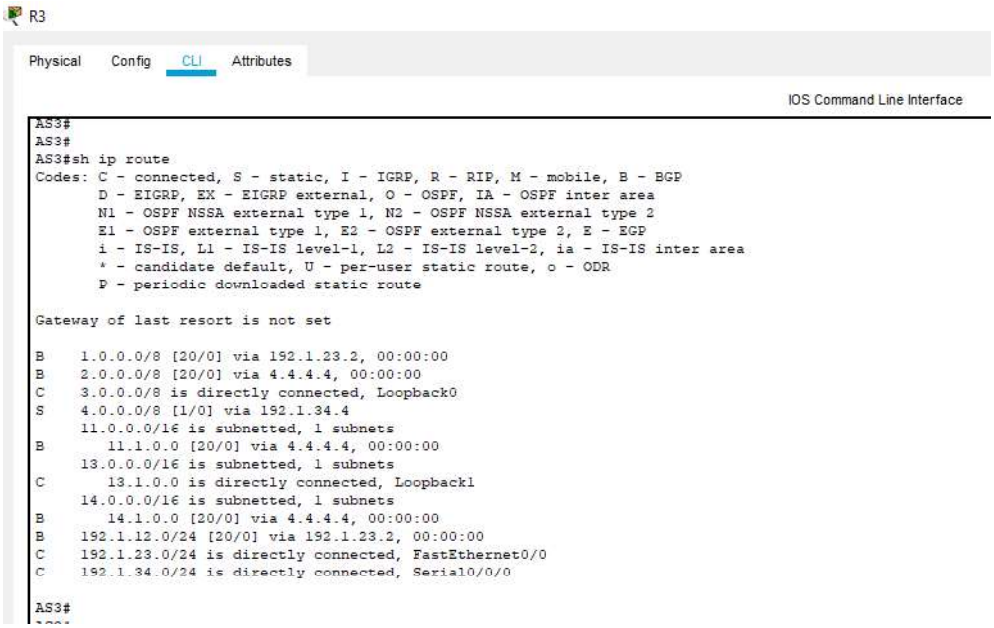


Figura 7. Aplicando código R3

Configuración router 4.

AS4(config)#route bgp 4
AS4(config-router) #neighbor 192.1.34.3 remote-as 3
AS4(config-router) #neighbor 192.1.34.3 remote-as 3
AS4(config-router) #neighbor 192.1.23.3 remote-as 3
AS4(config-router) #neighbor 192.1.23.3 remote-as 2
AS4(config-router) #neighbor 192.1.12.3 remote-as 2
AS4(config-router) #neighbor 192.1.12.3 remote-as 1
AS4(config-router) #network 3.3.3.3 mask 255.0.0.0
AS4(config-router) #network 13.1.0.1 mask 255.255.0.0
AS4(config-router) #network 12.1.0.1 mask 255.255.0.0
AS4(config-router) #network 2.2.2.2 mask 255.0.0.0
AS4(config-router) #network 11.1.0.1 mask 255.255.0.0
AS4(config-router) #network 4.4.4.4 mask 255.0.0.0
AS4(config-router) #network 14.1.0.1 mask 255.255.0.0

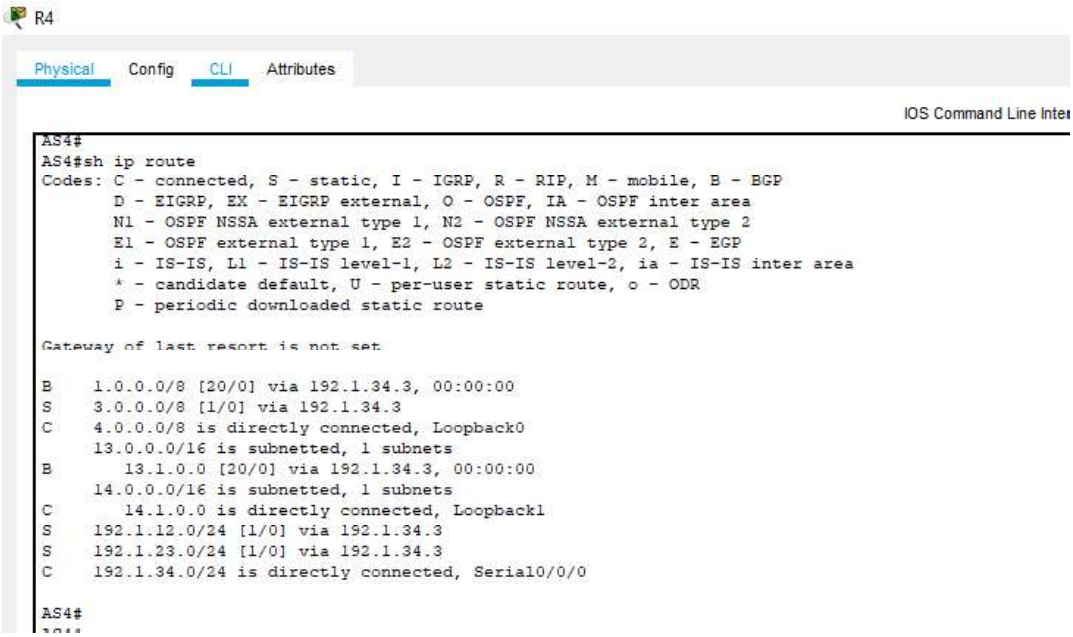


Figura 8. Aplicando código R4

2. ESCENARIO 2

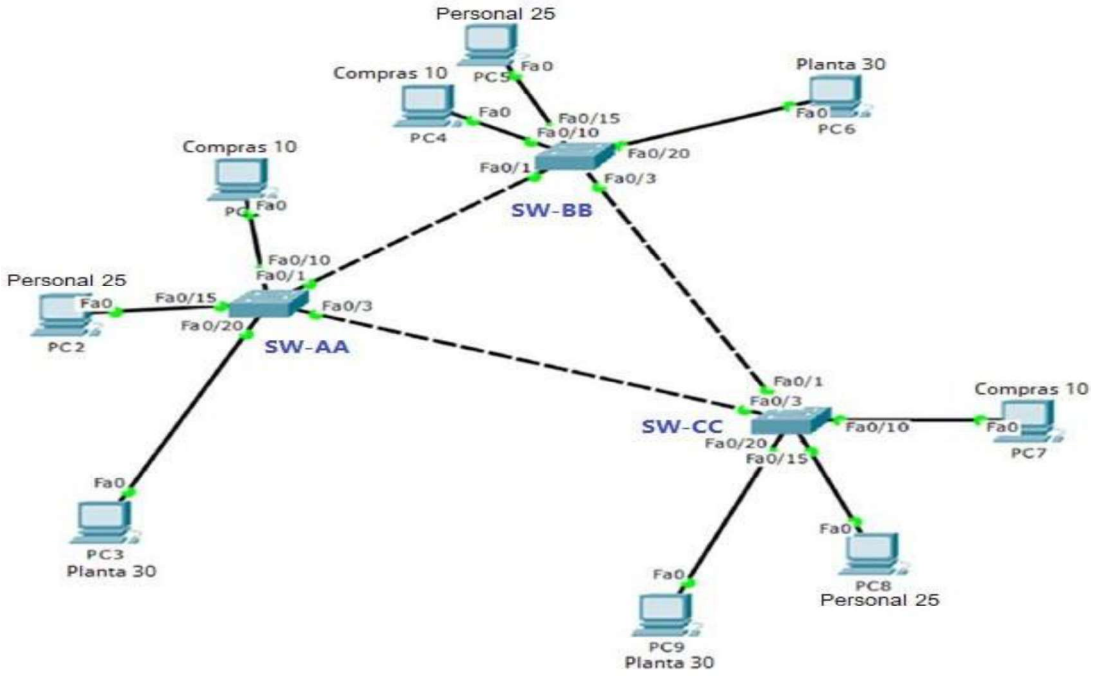


Figura 8. Escenario 2

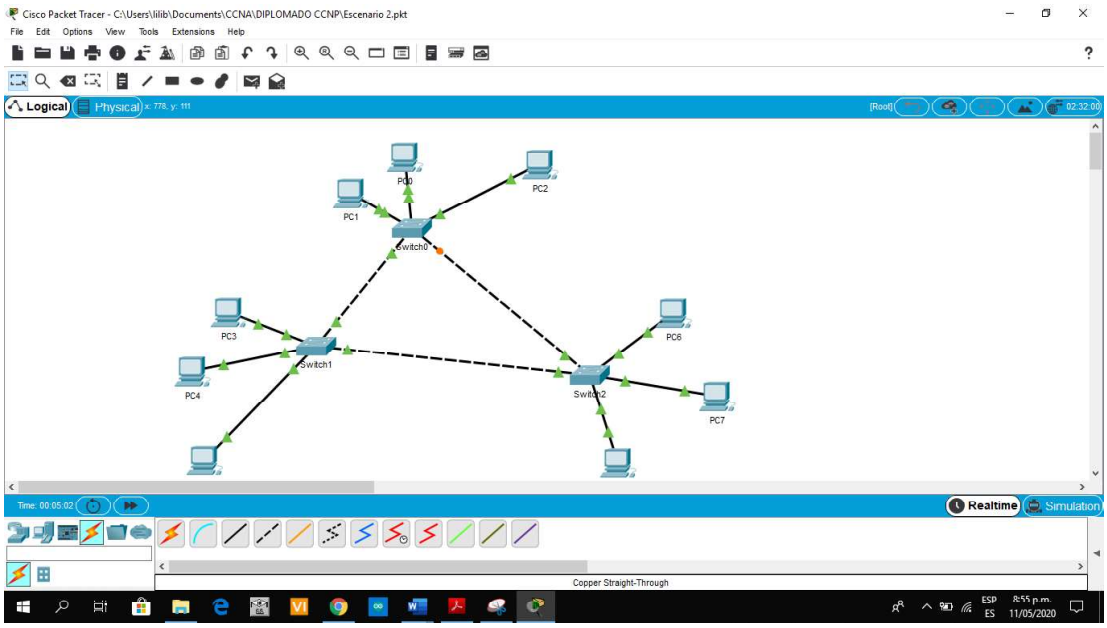


Figura 9. Simulación del escenario 2

A. Configurar VTP

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

```
Switch>ena
Switch#conf t
Switch(config)#
Switch(config)#hostname SW-AA
SW-AA(config)#
SW-AA(config)#^Z

SW-AA(config)#
SW-AA(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-AA(config)#vtp version 2
SW-AA(config)#vtp mode client
SW-AA(config)#vtp password cisco
SW-AA(config)#

Switch#
```

```
Switch#conf t
Switch(config)#hostname SW-CC
SW-CC(config)#
SW-CC(config)#^Z

SW-CC#CONF T
SW-CC(config)#vtp domain CCNP
Domain name already set to CCNP.
SW-CC(config)#vtp version 2
VTP mode already in V2.
SW-CC(config)#vtp mode client
Setting device to VTP CLIENT mode.
SW-CC(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-CC(config)#

Switch>ena
Switch#conf t
Switch(config)#hostname SW-BB

SW-BB#
SW-BB#CONF T
SW-BB(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-BB(config)#vtp version 2
SW-BB(config)#vtp mode server
Device mode already VTP SERVER.
SW-BB(config)#vtp password cisco
Setting device VLAN database password to cisco
SW-BB(config)#
```

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

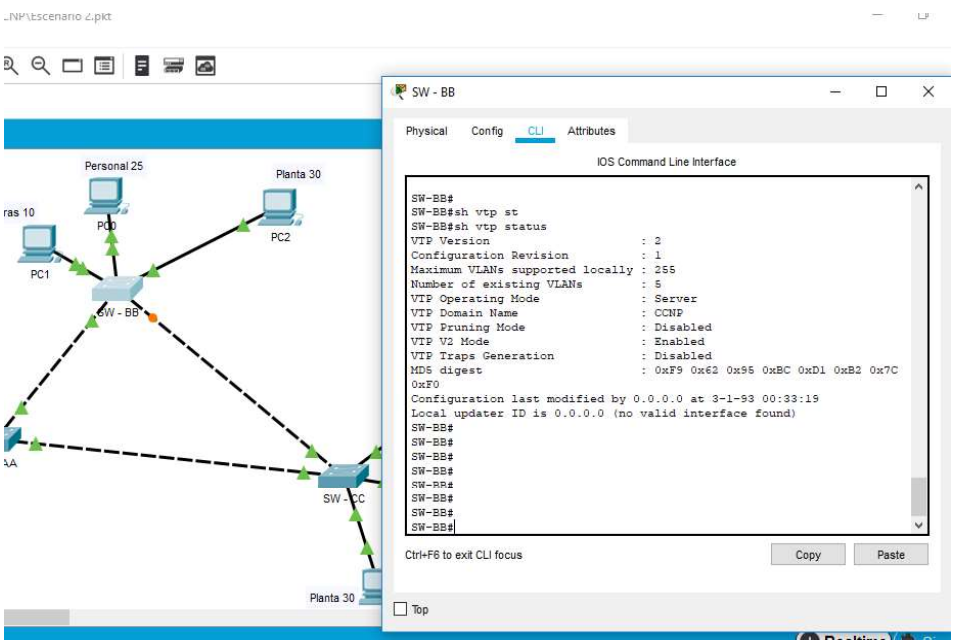


Figura 10. Configuración código SWBB

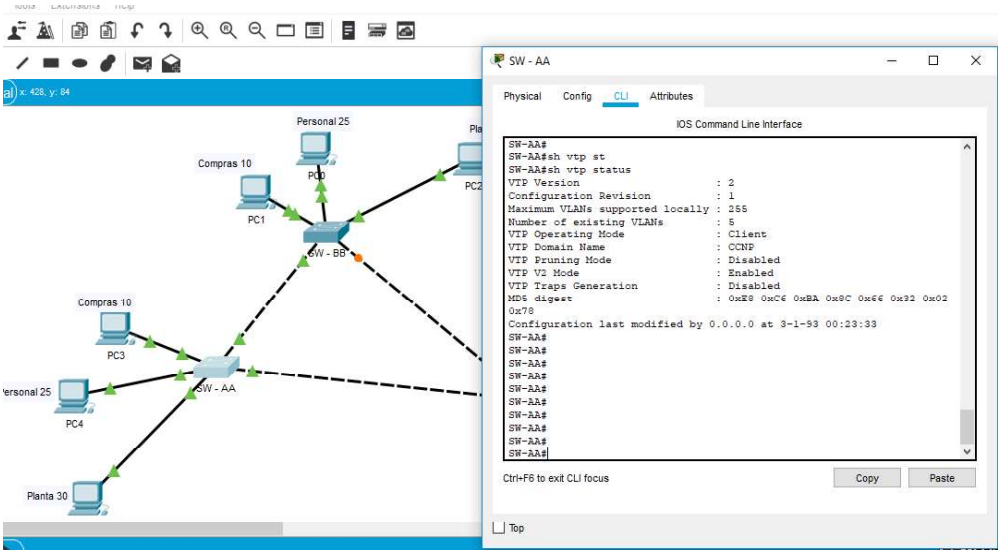


Figura 11. Configuración código SWAA

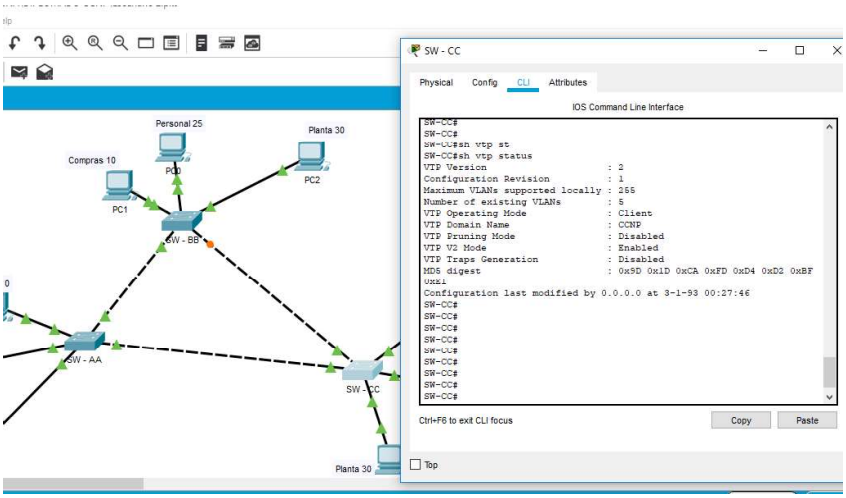


Figura 12. Configuración código SWCC

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.

   SW-AA#
   SW-AA#conf t
   SW-AA(config)#interface fastEthernet 0/1
   SW-AA(config-if) #switchport mode dynamic desirable

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

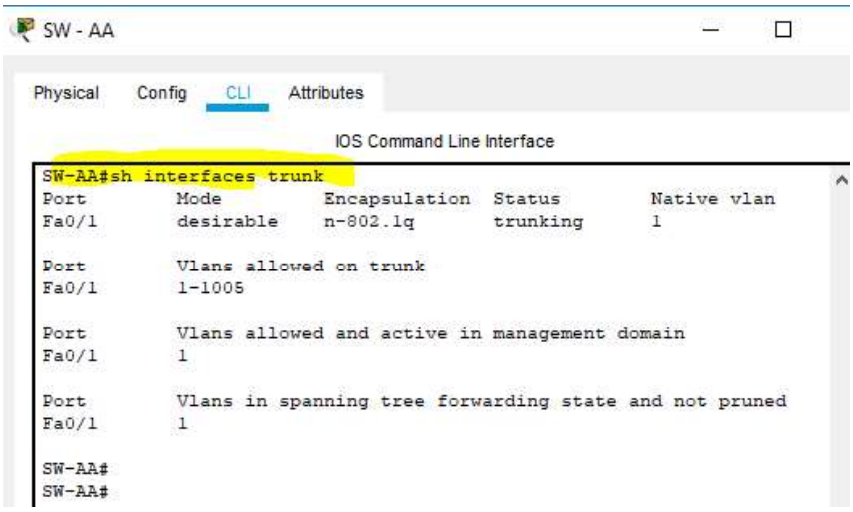


Figura 13. Aplicando código SWAA

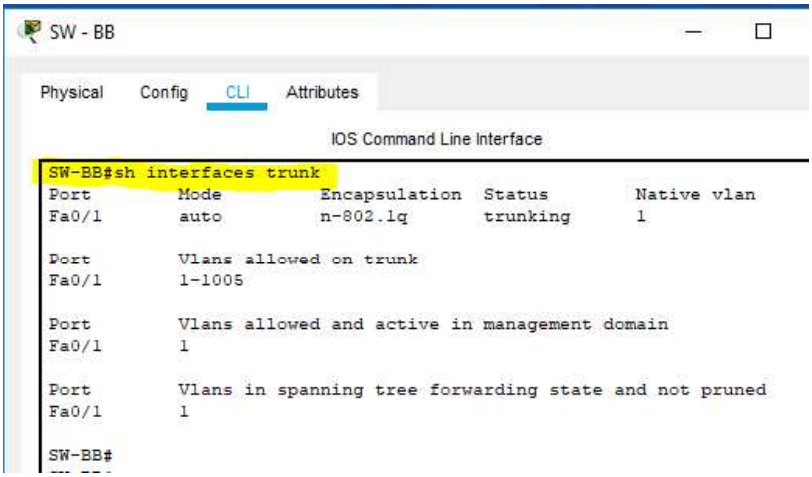


Figura 14. Aplicando código SWBB

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

   SW-AA(config)#interface fas
   SW-AA(config)#interface fastEthernet 0/3
   SW-AA(config-if) #switchport mode trunk - **Habilito el modo trunk en la int.**

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

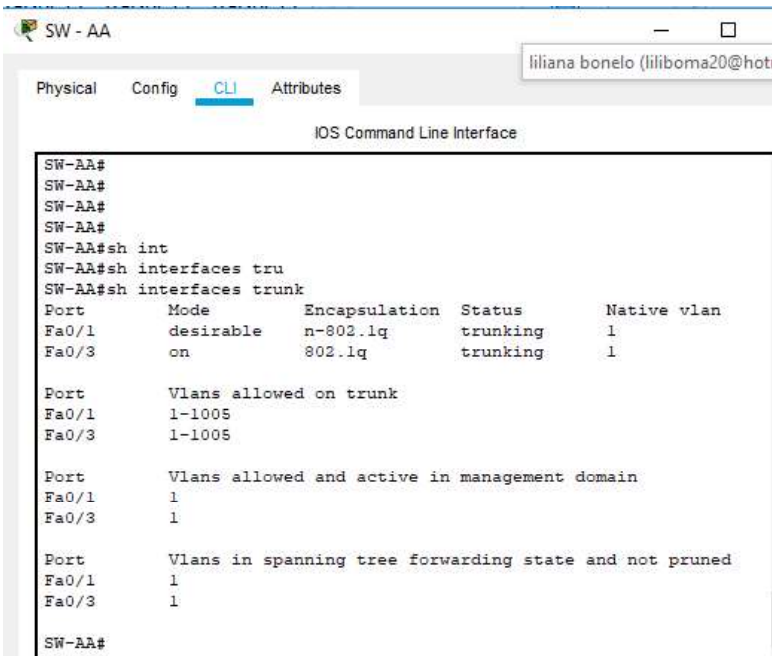


Figura 15. Aplicando código Trunk

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

SW-CC#conf t
SW-CC(config)#interface fastEthernet 0/1
SW-CC(config-if) #switchport mode trunk

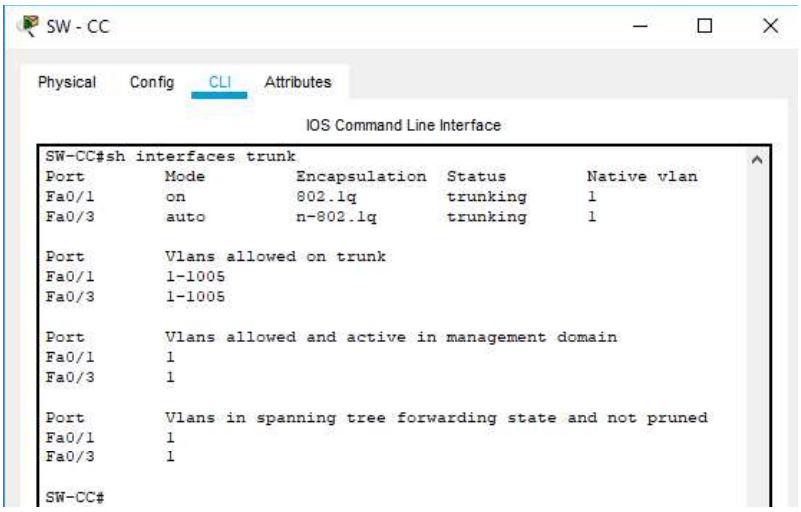


Figura 16. Aplicando código Trunk

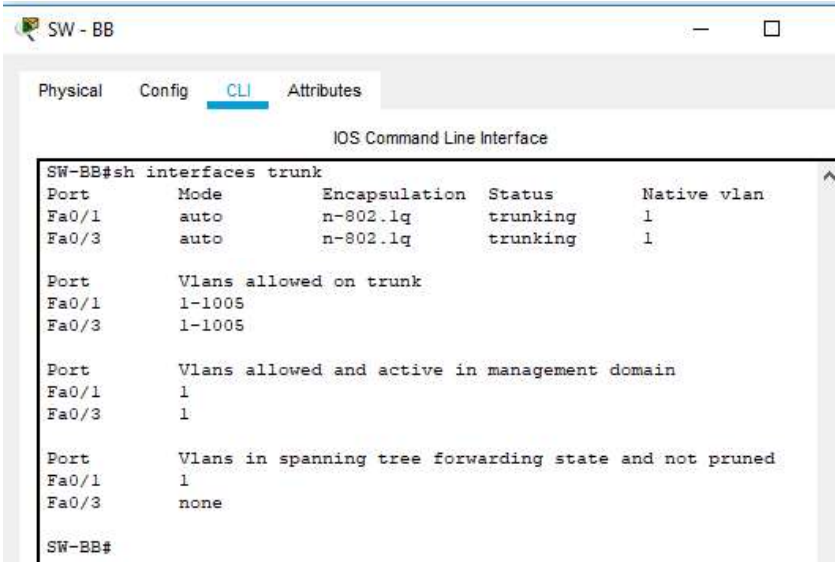


Figura 17. Aplicando código Trunk

B. 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)

```
SW-BB#conf t
SW-BB(config)#vlan 10                    - creo la vlan 10
SW-BB(config-vlan)#name Compras          - asigno el nombre
SW-BB(config-vlan)#vlan 25                creo la vlan 25
SW-BB(config-vlan)#name Personal         asigno el nombre
SW-BB(config-vlan)#vlan 30                creo la vlan 30
SW-BB(config-vlan)#name Planta           asigno el nombre
SW-BB(config-vlan)#vlan 99                creo la vlan 99
SW-BB(config-vlan)#name Admon             asigno el nombre
SW-BB(config-vlan)#exit
SW-BB(config)#
```

9. Verifique que las VLANs han sido agregadas correctamente.

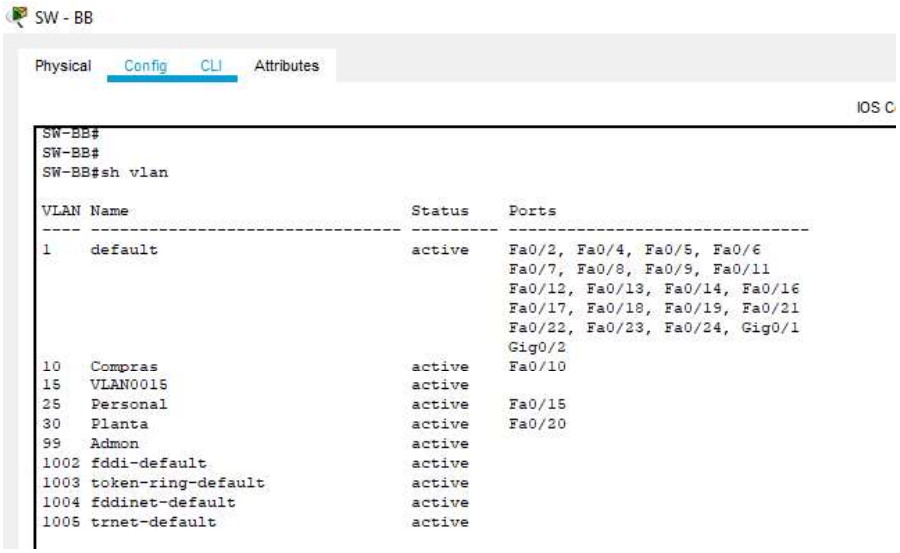


Figura 18. Configuración VLANs SWBB

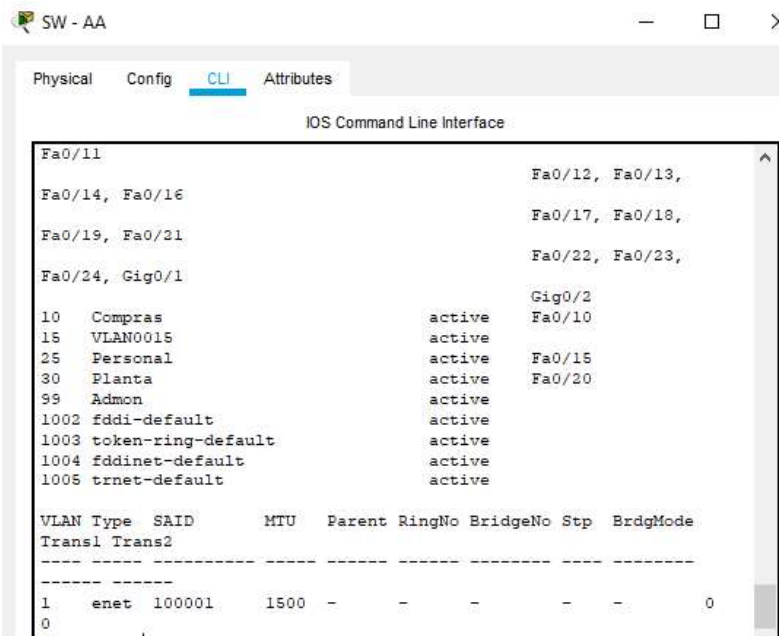


Figura 19. Configuración VLANs SWAA

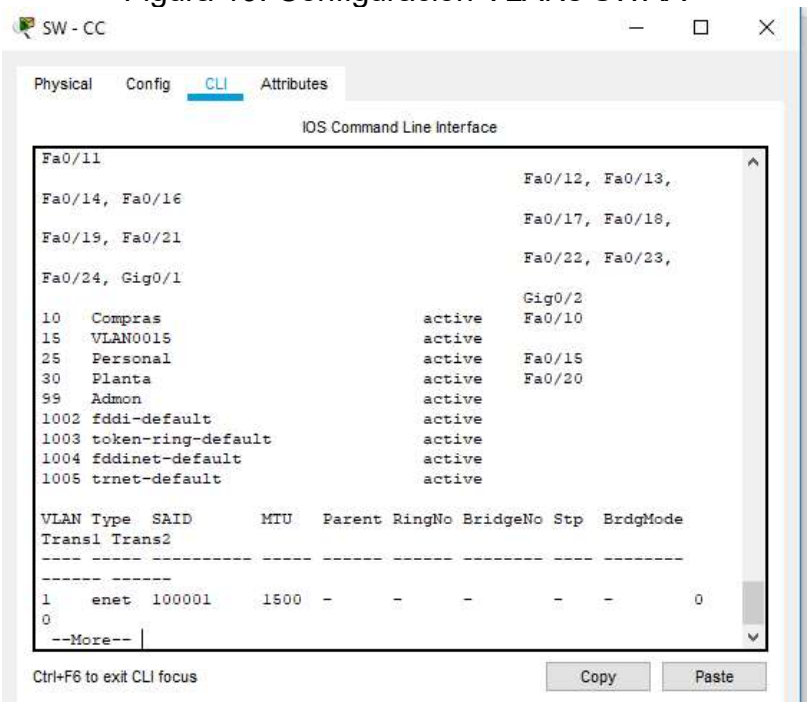


Figura 20. Configuración VLANs SWCC

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

Tabla 2. Configuración direcciones VLANs / IP

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

```
SW-AA(config)#int
SW-AA(config)#interface fastEthernet 0/10    - ingreso al puerto
SW-AA(config-if) #switchport mode access     - configuro el modo de acceso
SW-AA(config-if) #switchport access vlan 10  - asigno la vlan
SW-AA(config-if) #exit
SW-AA(config)#interface fastEthernet 0/15
SW-AA(config-if) #switchport mode access
SW-AA(config-if) #switchport access vlan 25
SW-AA(config-if) #exit
SW-AA(config)#interface fastEthernet 0/20
SW-AA(config-if) #switchport mode access
SW-AA(config-if) #switchport access vlan 30
SW-AA(config-if) #

SW-BB(config)#interface fastEthernet 0/10
SW-BB(config-if) #switchport mode access
SW-BB(config-if) #switchport access vlan 10
SW-BB(config-if) #exit
SW-BB(config)#interface fastEthernet 0/15
SW-BB(config-if) #switchport mode access
SW-BB(config-if) #switchport access vlan 25
SW-BB(config-if) #exit
SW-BB(config)#interface fastEthernet 0/20
SW-BB(config-if) #switchport mode access
SW-BB(config-if) #switchport access vlan 30
SW-BB(config-if) #end
SW-BB#

SW-CC(config)#int
```

```
SW-CC(config)#interface fastEthernet 0/10
SW-CC(config-if) #switchport mode access
SW-CC(config-if) #switchport access vlan 10
SW-CC(config-if) #exit
SW-CC(config)#interface fastEthernet 0/15
SW-CC(config-if) #switchport mode access
SW-CC(config-if) #switchport access vlan 25
SW-CC(config-if) #exit
SW-CC(config)#interface fastEthernet 0/20
SW-CC(config-if) #switchport mode access
SW-CC(config-if) #switchport access vlan 30
SW-CC(config-if) # exit
SW-CC(config)#
```

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.

SWICTH	PC	Interfaz	VLAN	IP ADDRESS	MASK
SW_BB	PC1	F0/10	10	190.108.10.1	255.255.255.0
	PC2	F0/15	25	190.108.20.2	255.255.255.0
	PC3	F0/20	30	190.108.30.3	255.255.255.0
SW-AA	PC4	F0/10	10	190.108.10.4	255.255.255.0
	PC5	F0/15	25	190.108.20.5	255.255.255.0
	PC6	F0/20	30	190.108.30.6	255.255.255.0
SW-CC	PC7	F0/10	10	190.108.10.7	255.255.255.0
	PC8	F0/15	25	190.108.20.8	255.255.255.0
	PC9	F0/20	30	190.108.30.9	255.255.255.0

Tabla 3. Configuración direcciones IP

C. 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

Tabla 4. Configuración direcciones IP VLAN 99

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

SW-BB#conf t
SW-BB(config)#interface vlan 99 - **ingreso a la vlan 99**
SW-BB(config-if) #ip address 190.108.99.2 255.255.255.0 - **configuramos ip**
SW-BB(config-if) #exit

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

D. 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.

RTA/

Los pings realizados a PCs que perteneces a la misma Vlan, si tuvieron éxito. los pings realizados entre los PCs pertenecientes a diferentes Vlans no tuvo éxito, ya que se encuentran en diferentes Vlans y pertenecen a un segmento de red diferente. Por tanto, para lograr establecer comunicación entre estos PCs, sería necesario incluir en la topología de la red un enrutador o un Switch de capa 3 (Switch Multicapa), para lograr comunicar el tráfico ICMP entre las diferentes redes propuestas en la tabla de enrutamiento para estos dispositivos.

						PING	
SWICTH	PC	Interfaz	VLAN	IP ADDRESS	MASK	Exitoso	No exitoso
SW_BB	PC1	F0/10	10	190.108.10.1	255.255.255.0	PC4/PC7	PC2 /PC3/PC5/PC6/PC8/PC9
	PC2	F0/15	25	190.108.20.2	255.255.255.0	PC5/PC8	PC1/PC3/PC4/PC6/PC7/PC9
	PC3	F0/20	30	190.108.30.3	255.255.255.0	PC6/PC9	PC1/PC2/PC4/PC5/PC7/PC8
SW-AA	PC4	F0/10	10	190.108.10.4	255.255.255.0	PC1/PC7	PC2/PC3/PC5/PC6/PC8/PC9
	PC5	F0/15	25	190.108.20.5	255.255.255.0	PC2/PC8	PC1/PC3/PC4/PC6/PC7/PC9
	PC6	F0/20	30	190.108.30.6	255.255.255.0	PC3/PC9	PC1/PC2/PC4/PC5/PC7/PC8
SW-CC	PC7	F0/10	10	190.108.10.7	255.255.255.0	PC1/PC4	PC2/PC3/PC5/PC6/PC8/PC9
	PC8	F0/15	25	190.108.20.8	255.255.255.0	PC1/PC5	PC1/PC3/PC4/PC6/PC7/PC9
	PC9	F0/20	30	190.108.30.9	255.255.255.0	PC3/PC6	PC1/PC2/PC4/PC5/PC7/PC8

Tabla 5. Ejecución de Pings

PC1 ping Éxito con la PC4 Y PC7

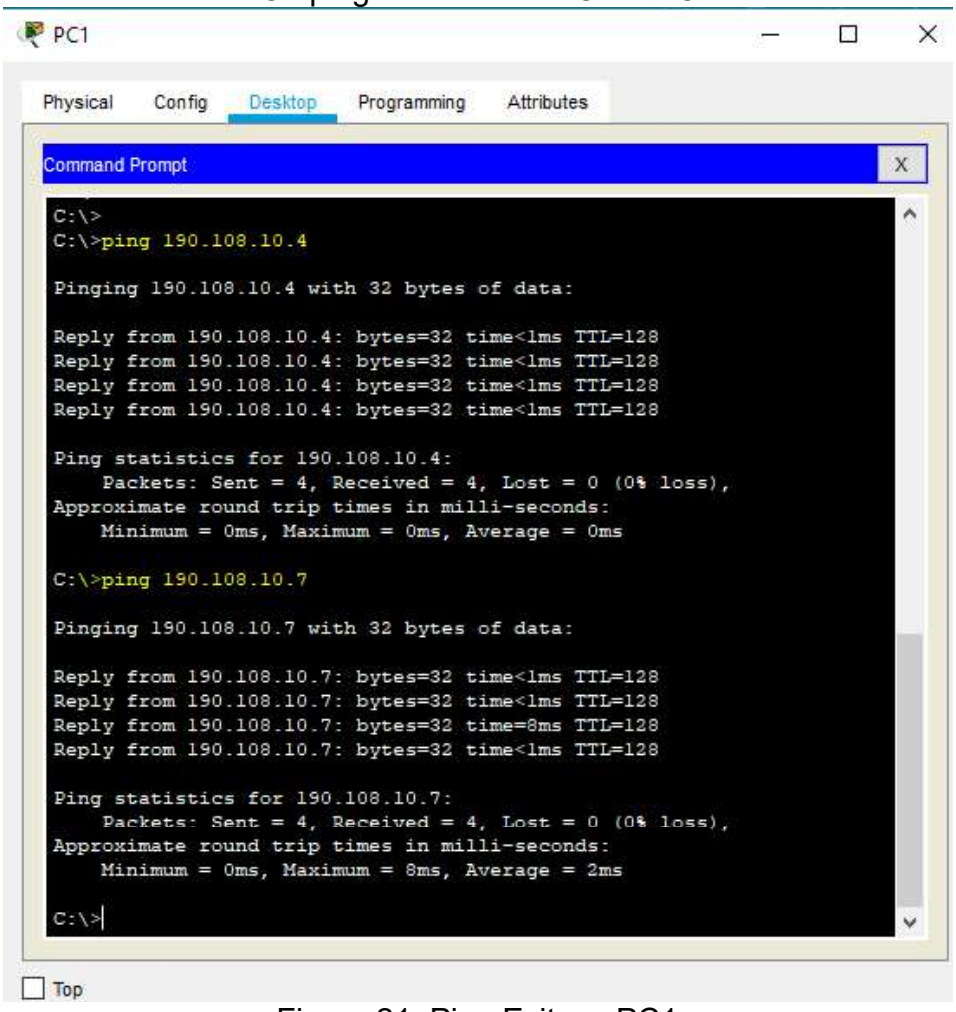


Figura 21. Ping Exitoso PC1

PC2 Ping Exitoso con la PC 5 Y PC8

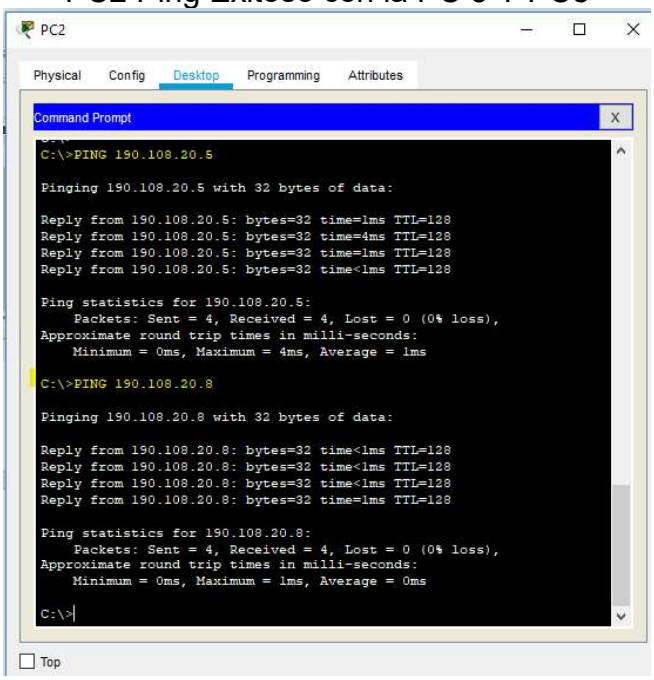


Figura 22. Ping Exitoso PC2

PC3 Ping Exitoso con la PC6 Y PC9

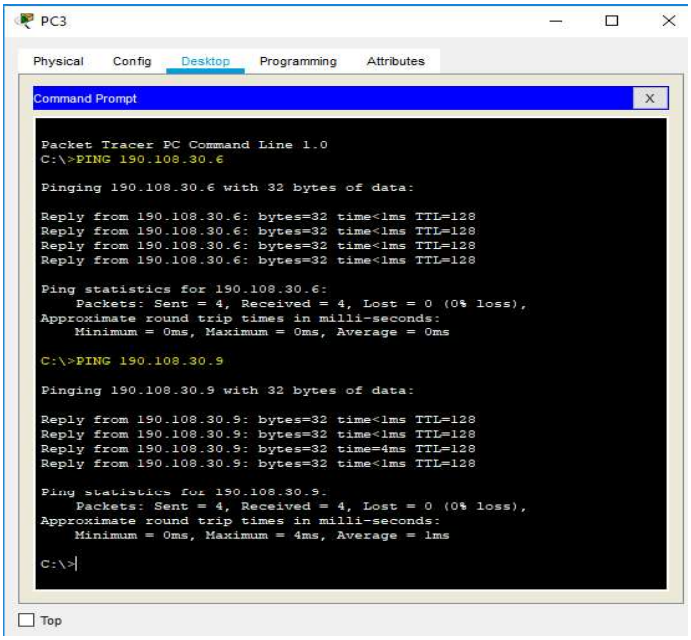


Figura 23. Ping Exitoso PC3

PC1 Ping NO exitoso con la PC5 y PC9

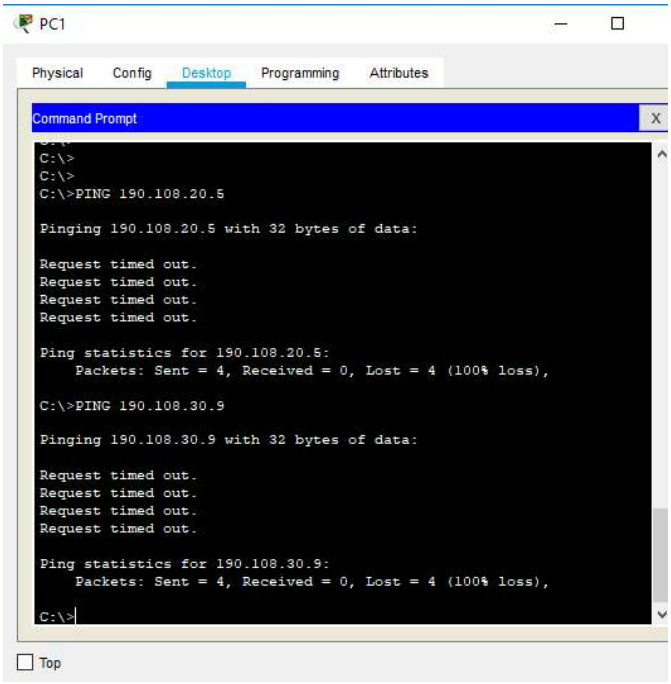
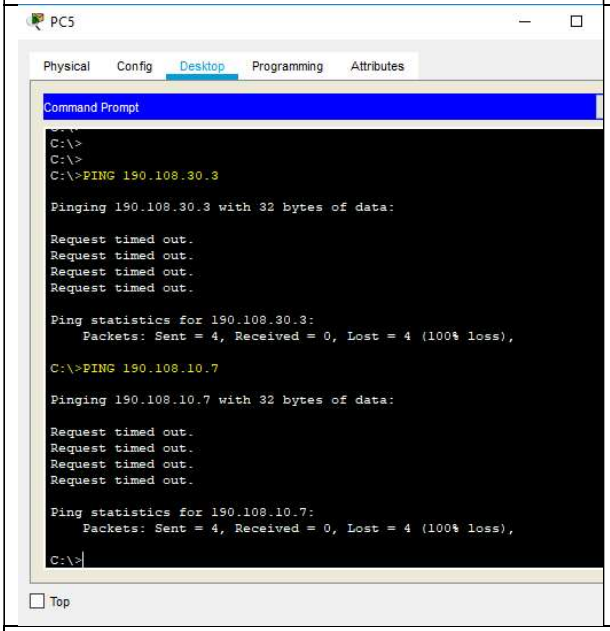


Figura 24. Ping NO Exitoso PC1

PC5 Ping NO exitoso con la PC3 y PC7



PC9 Ping NO exitoso con la PC2 y PC4

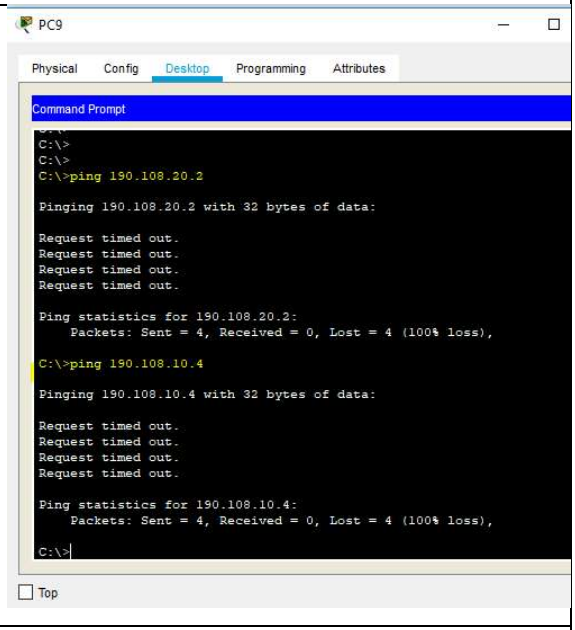


Figura 25. Ping NO Exitoso PC5 / PC9

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

Se realiza ping a las direcciones IP de las VLAN 99 de los switches y todas dieron exitosas, dado que las interfaces físicas que en rutan los datos enviados a través del protocolo ICMP entre los tres Switches están configuradas en modo troncal, y comparten el mismo tipo de encapsulamiento, así como se encuentran en un modo compatible, para establecer el permiso a las VLANs creadas, además, se debe determinar la VLAN nativa para las interfaces.

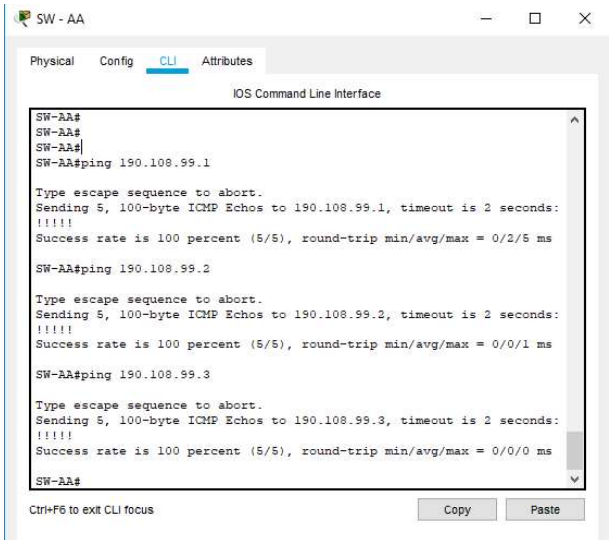


Figura 26. SW Ping exitoso SWAA

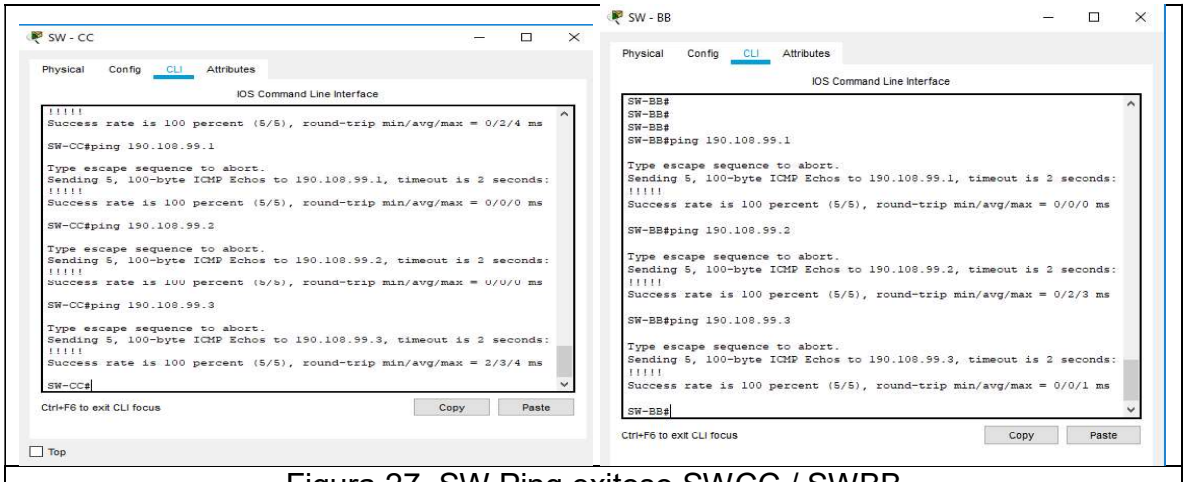
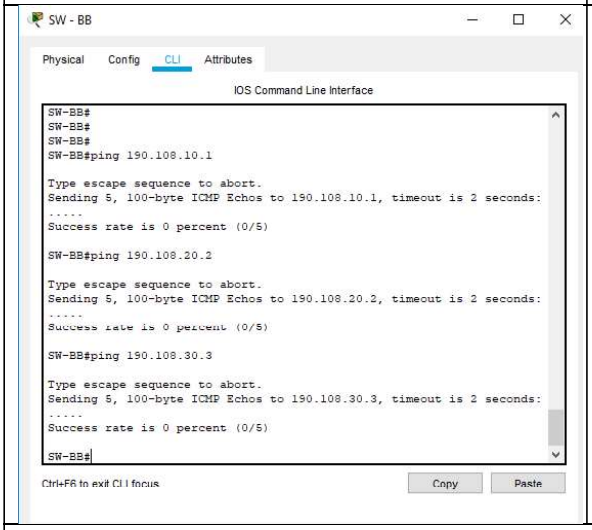


Figura 27. SW Ping exitoso SWCC / SWBB

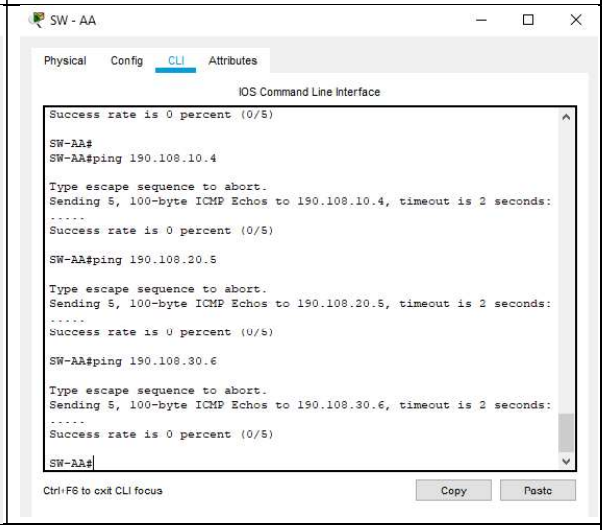
16. Ejecute un Ping desde cada Switch a cada PC. Explique por qué el ping tuvo o no tuvo éxito.

    Los pings realizados entre los Switches y los PCs no tuvieron éxito. Ya que las VLANs habilitadas en cada uno de los Switches a través del protocolo VTP en las interfaces se configuraron en modo de acceso y aun no se configura un enrutamiento IP en las VLANs creadas 10 Compras, 25 Mercadeo y 30 Planta. Para solucionar esto, es necesario configurar una dirección IP y una máscara de subred en cada una de las interfaces VLAN de los Switches, la cual pertenezca al mismo segmento de red al cual pertenece el PC que se conecta a cada VLAN. Además, se debe determinar la VLAN nativa para dichas interfaces.

SWBB



SW AA



SW CC

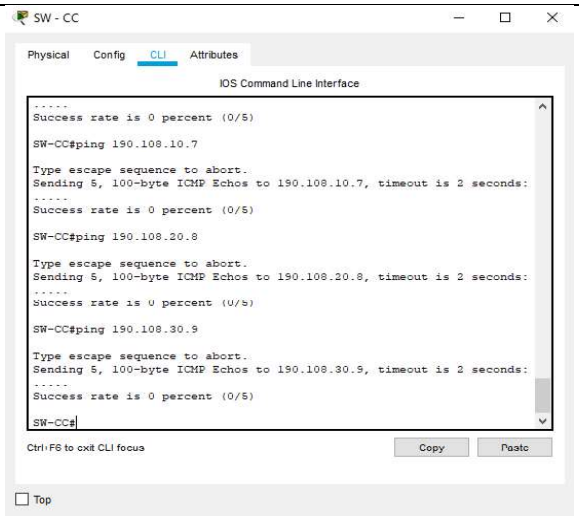


Figura 28. SW Ping exitoso SWBB / SWAA / SWCC

CONCLUSIONES

Con el desarrollo de los dos escenarios se implementa lo aprendido a lo largo del curso Diplomado de profundización Cisco CCNP. Se detalla los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

Aprendimos a implementar y configurar una red que este soportada por VLANs con el uso de los protocolos VTP y STP, donde se pueda diseñar y configuración para su uso en múltiples dispositivos, configurar troncales y vlan usando el protocolo VTP, los EtherChannel Link en red de switch, entro otros usos.

Con la verificación final de la conectividad en el último escenario propuesto, analizamos las posibles causas de los fallos en la búsqueda de paquetes mediante los pings realizados entre los dispositivos, identificando las configuraciones faltantes en dichos dispositivos y las soluciones más factibles para estos errores de conectividad.

BIOGRAFIA

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-NT1IlnWR0hoMxgBNv1CJ

Froom, R., Frahim, E. (2015). CISCO Press (Ed). v. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

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

Wallace, K. (2015). CISCO Press (Ed). CCNP Routing and Switching ROUTE 300-101 Official Cert Guide. Recuperado de https://1drv.ms/b/s!AgIGg5JUgUBthFx8WOxiq6LPJppl