DIPLOMADO DE PROFUNDIZACION
PRUEBA DE HABILIDADES PRACTICAS CISCO

BEATRIZ TORRES NUÑEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
ELECTRÓNICA
GUAJIRA
2020

DIPLOMADO DE PROFUNDIZACION
PRUEBA DE HABILIDADES PRACTICAS CISCO

BEATRIZ TORRES NUÑEZ

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
ELECTRÓNICA
GUAJIRA
2020

NOTA DE ACEPTACIÓN

Presidente del Jurado

Jurado

Jurado

Riohacha, 22 de mayo de 2020

AGRADECIMIENTOS

Quiero agradecer en primer lugar a DIOS padre por darme la fuerza y la confianza para creer en mi sueño guiarme en este sendero de la vida y fortalecerme espiritualmente, permitiendo alcanzar cada una de mis metas y designios en mi formación profesional.

Los más sinceros y sentidos agradecimientos a mi tutor Gerardo Granados Acuña, por su incansable orientación, compromiso y disposicion incondicional, siempre estuvo atento ofreciendo todo su conocimiento, durante este proceso de formación en CCNP.

A las personas que me acompañaron en este proceso de aprendizaje y dedicación, como siempre a mi familia, que siempre me brindaron la confianza y apoyo absoluto en pro de alcanzar esta meta, A mis compañeros de grupos, por entretejer ideas constructivas que me ayudaron a fortalecer mis conocimientos los cuales fueron muy importantes en este proceso.

Finalmente, un eterno agradecimiento la Universidad a lo largo de mi viaje y por eso estoy agradecido por los recursos y el apoyo que siempre me ha ofrecido la cual me abre sus puertas, para ser un profesional competitivo y ético.

¡Muchas gracias por todo!...

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ROUTER: También conocido como enrutador, se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática. se trata de un producto de hardware que permite interconectar computadoras que funcionan en el marco de una 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.

PROTOCOLO EIGRP: Es una versión mejorada de IGRP. La tecnología de vector distancia que se usa en IGRP también se emplea en EIGRP. Además, la información de la distancia subyacente no presenta cambios. Utilizado en redes TCP/IP y de Interconexión de Sistemas Abierto (OSI) como un protocolo de enrutamiento del tipo vector distancia avanzado, de propiedad de Cisco, donde sus características se basan en algoritmos vector distancia y de estado de enlace.

SWITCH: Son dispositivos digitales lógicos de interconexión de equipos que operan en la capa de enlace de datos del modelo OSI. Interconectar dos o más host de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada ésta.

CCNP: Capacita a los estudiantes para instalar, configurar y operar redes locales y de área amplia, y para brindar servicios de acceso por marcación a organizaciones que tienen redes desde 100 hasta 500 nodos con protocolos y tecnologías tales como TCP/IP, OSPF, EIGRP, BGP, ISDN, Frame Relay, STP y VTP.

RESUMEN

Este proyecto tiene como objetivo demostrar la gestión de los módulos CCNP ROUTE, donde los principios básicos de los protocolos de enrutamiento de red e IP versión 4 (IPv4) e IP versión 6 (IPv6) están relacionados, el Gateway Routing Protocol Internal Enhanced (EIGRP), el primer camino más corto Protocolo (OSPF) y Protocolo de colocación de enlaces fronterizos (BGP). El módulo SWITCH CCNP que permite la implementación, monitoreo y administración adecuados de la conmutación en una red empresarial, implementando VLAN en redes corporativas y configurando y optimizando para alta disponibilidad y redundancia en la capa Interruptores 2 y Capa 3. Se explora la conectividad empresarial hacia Internet y se analiza la administración de las actualizaciones de enrutamiento y las rutas que toma el tráfico en la red. El siguiente trabajo lo llevará paso a paso a través de dos configuraciones en el plotter de paquetes que corresponde a la prueba de habilidades prácticas del diploma CISCO CCNP, que cubren en gran medida los conocimientos adquiridos y permiten reforzar lo que se aplica durante el programa. como electrónica y telecomunicaciones. formado en gran parte por el código aplicado a la configuración.

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

ABSTRACT

This project aims to demonstrate the management of CCNP ROUTE modules, where the basic principles of network routing protocols and IP version 4 (IPv4) and IP version 6 (IPv6) are related, the Gateway Routing Protocol Internal Enhanced (EIGRP), the First Shortest Path Protocol (OSPF) and Border Link Placement Protocol (BGP). SWITCH CCNP module that enables the proper implementation, monitoring, and management of switching in an enterprise network, implementing VLANs in enterprise networks, and configuring and optimizing for high availability and redundancy at Layer 2 and Layer 3. Business connectivity is explored towards Internet and the management of routing updates and routes taken by network traffic is discussed. The following work will take you step-by-step through two configurations on the package plotter corresponding to the CISCO CCNP Diploma practical skills test, which largely cover the knowledge acquired and allow you to reinforce what is applied during the program. such as electronics and telecommunications. formed largely by the code applied to the configuration.

KeyWords: CISCO, CCNP, Switching, Routing, Networks, Electronics.

INTRODUCCIÓN

El Diplomado Cisco CCNP (Cisco Certified Networking Proffesional / Profesional en Redes certificado por Cisco) permite desarrollar la capacidad de planificar, implementar, verificar y solucionar problemas de redes empresariales locales y de área amplia y trabajar en colaboración con especialistas en soluciones avanzadas de seguridad, voz, redes inalámbricas y video.El módulo CCNP SWITCH, permite apropiar las temáticas relacionadas con la implementación, monitoreo y administración de la conmutación en una arquitectura de red empresarial, la implementación de VLANs en redes corporativas, y la configuración y optimización para una alta disponibilidad y redundancia en los switches de capa 2 y capa 3. También se describirán e implementarán las características de seguridad en redes LAN y WAN.

Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos. La importancia de establecer niveles de seguridad básicos, mediante la definición de criterios y políticas de seguridad aplicadas a diversos escenarios de red.

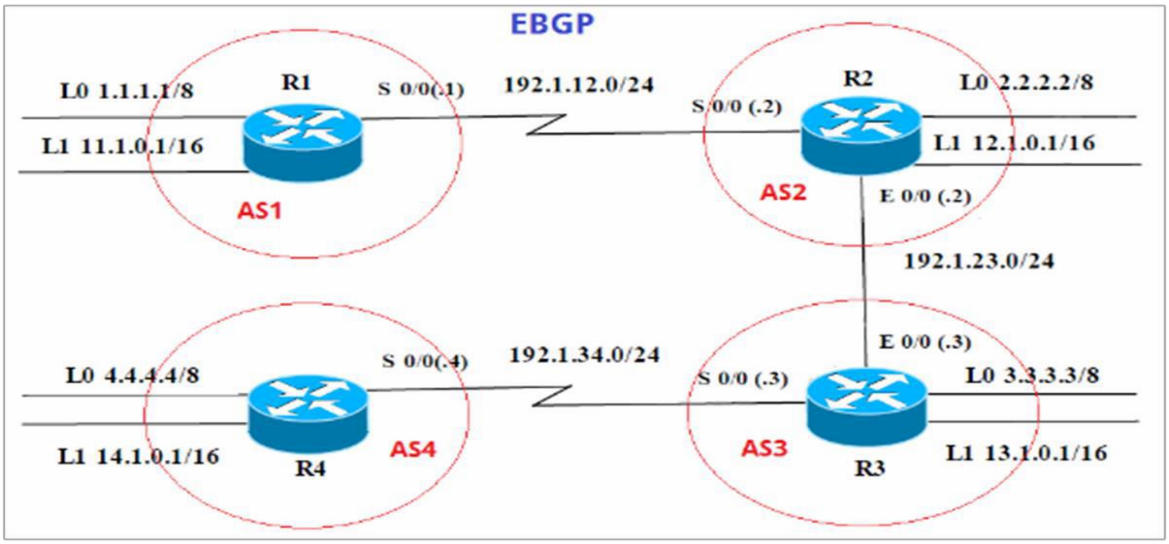
En el siguiente trabajo se realizará el paso a paso de dos configuraciones en packet tracer los cuales corresponde a la prueba de habilidades practicas del diplomado cisco CCNP, Aplicando los conocimientos para dar solución a dos escenarios: o de los dos propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros. Con el desarrollo de este proyecto se emplean herramientas de simulación y laboratorios los cuales exigen un amplio manejo y conocimiento en CCNP ROUTE y CCNP SWITCH.

DESARROLLO

DESARROLLO DE LA ACTIVIDAD

1. Escenario 1.

Figura 1. Escenario 1



1.1 Información para configuración de los Routers.

Tabla 1. Información configuración R1

	Interfaz	Dirección IP	Máscara
R1	Loopback 0	1.1.1.1	255.0.0.0
	Loopback 1	11.1.0.1	255.255.0.0
	S 0/0	192.1.12.1	255.255.255.0

Tabla 2. Información configuración R2

	Interfaz	Dirección IP	Máscara
R2	Loopback 0	2.2.2.2	255.0.0.0
	Loopback 1	12.1.0.1	255.255.0.0
	S 0/0	192.1.12.2	255.255.255.0
	E 0/0	192.1.23.2	255.255.255.0

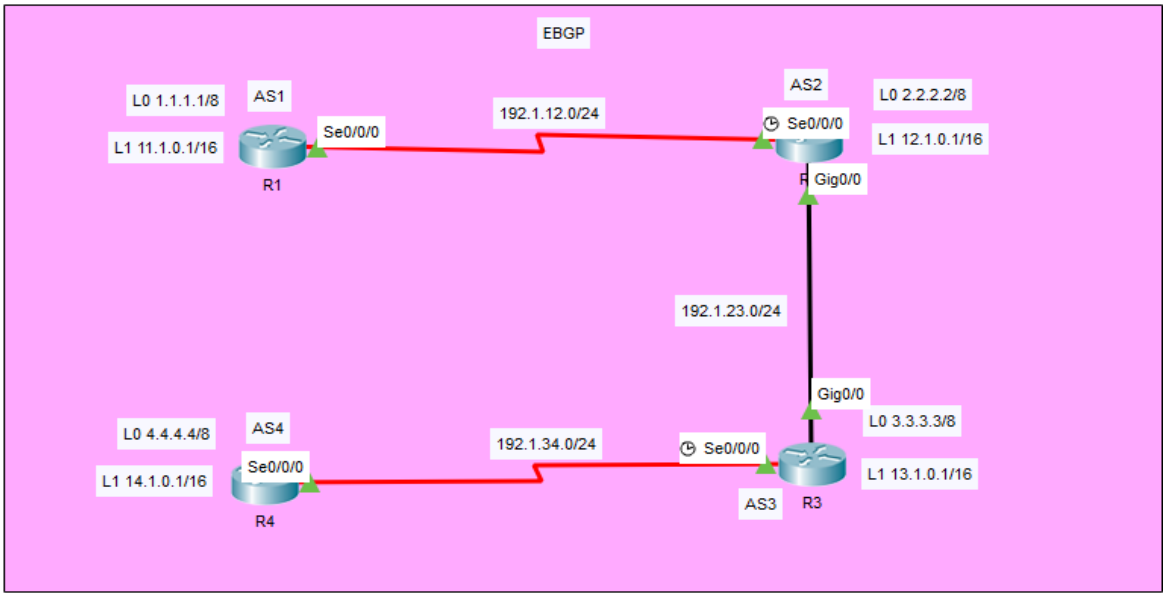
Tabla 3. Información configuración R3

	Interfaz	Dirección IP	Máscara
R3	Loopback 0	3.3.3.3	255.0.0.0
	Loopback 1	13.1.0.1	255.255.0.0
	E 0/0	192.1.23.3	255.255.255.0
	S 0/0	192.1.34.3	255.255.255.0

Tabla 4. Información configuración R4

	Interfaz	Dirección IP	Máscara
R4	Loopback 0	4.4.4.4	255.0.0.0
	Loopback 1	14.1.0.1	255.255.0.0
	S 0/0	192.1.34.4	255.255.255.0

Figura 2. Escenario 1 desarrollado

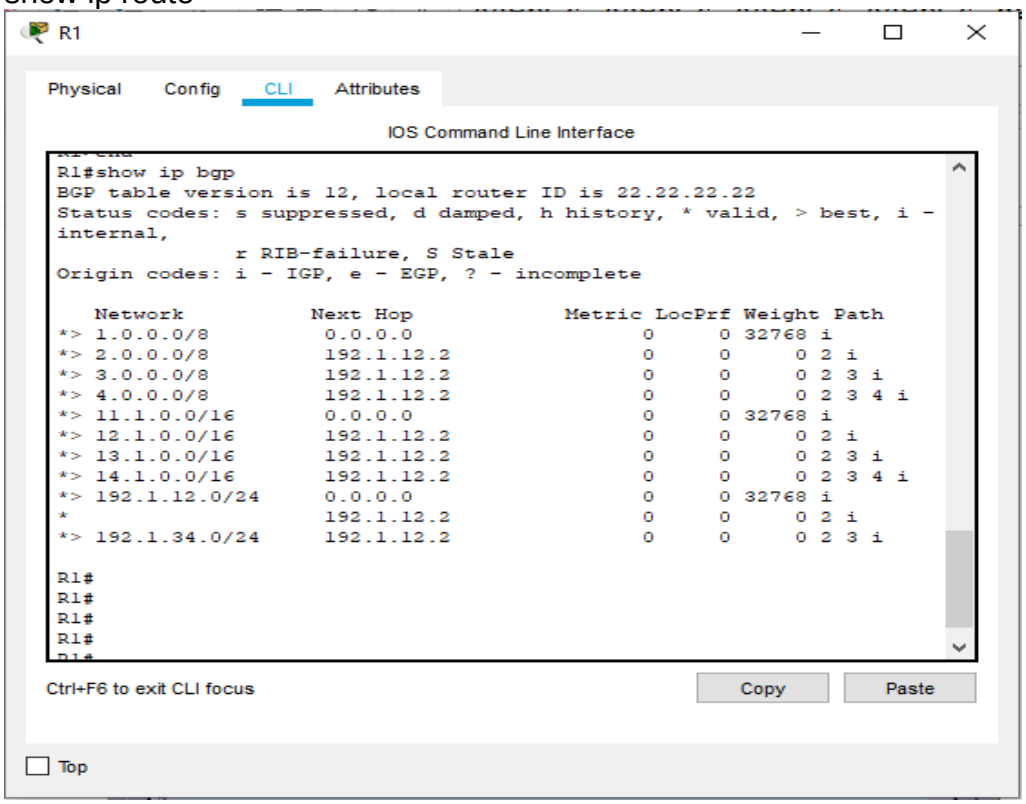


1.2 Configure una relación de vecino BGP entre R1 y R2. R1 debe estar en AS1 y R2 debe estar en AS2. Anuncie las direcciones de Loopback en BGP. Codifique los ID para los routers BGP como 22.22.22.22 para R1 y como 33.33.33.33 para R2. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

Desarrollo

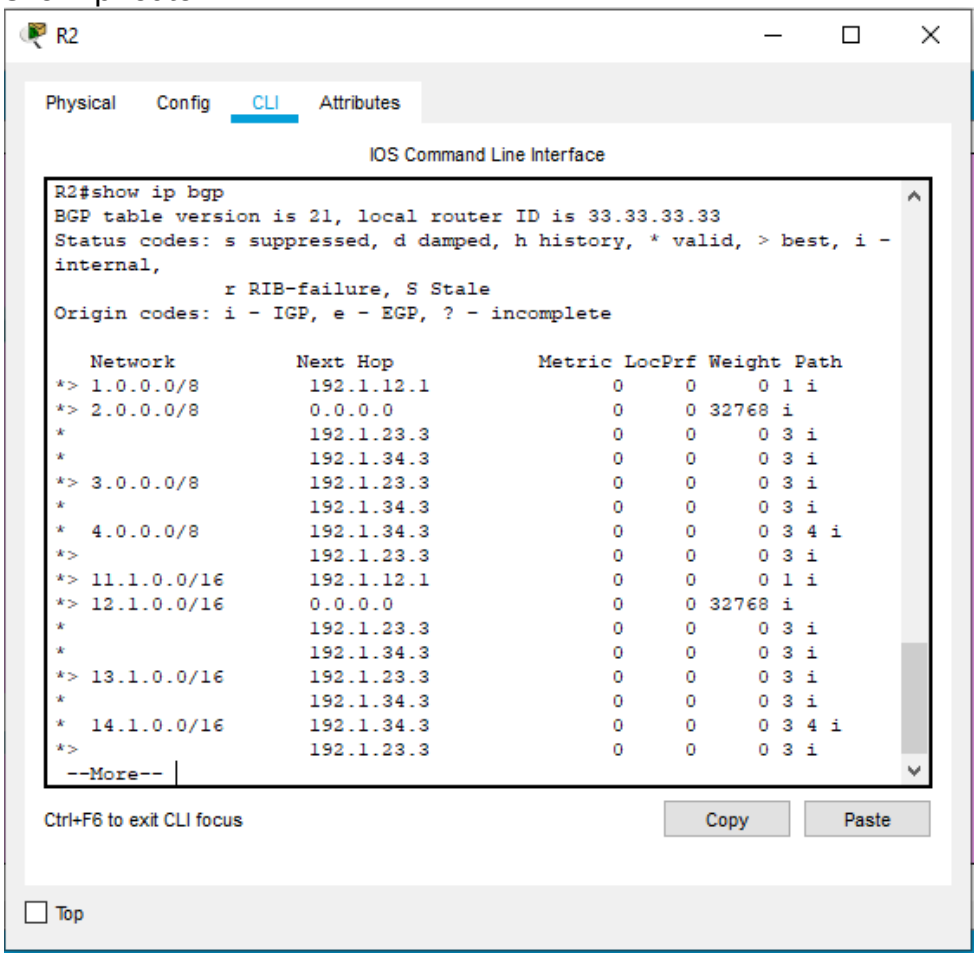
R1#enable
R1#configure term
Enter configuration commands, one per line. End with CNTL/Z.
R1 (config)#router bgp 1
R1(config-router)#exit
R1(config)#no router bgp 1
R1(config)#router bgp 1
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#neighbor 192.1.12.2 remote-as 2
R1(config-router)#network 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)#exit
R1(config)#exit
R1#

Figura 3. Presentación paso con los comandos utilizados y la salida del comando show ip route



```
R2>enable
R2#config term
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router bgp 2
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#neighbor 192.1.34.3 remote-as 3
R2(config-router)#neighbor 192.1.23.3 remote-as 3
R2(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.12.1 Up
R2(config-router)#network 1.1.1.0
R2(config-router)#network 11.1.0.0
R2(config-router)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
```

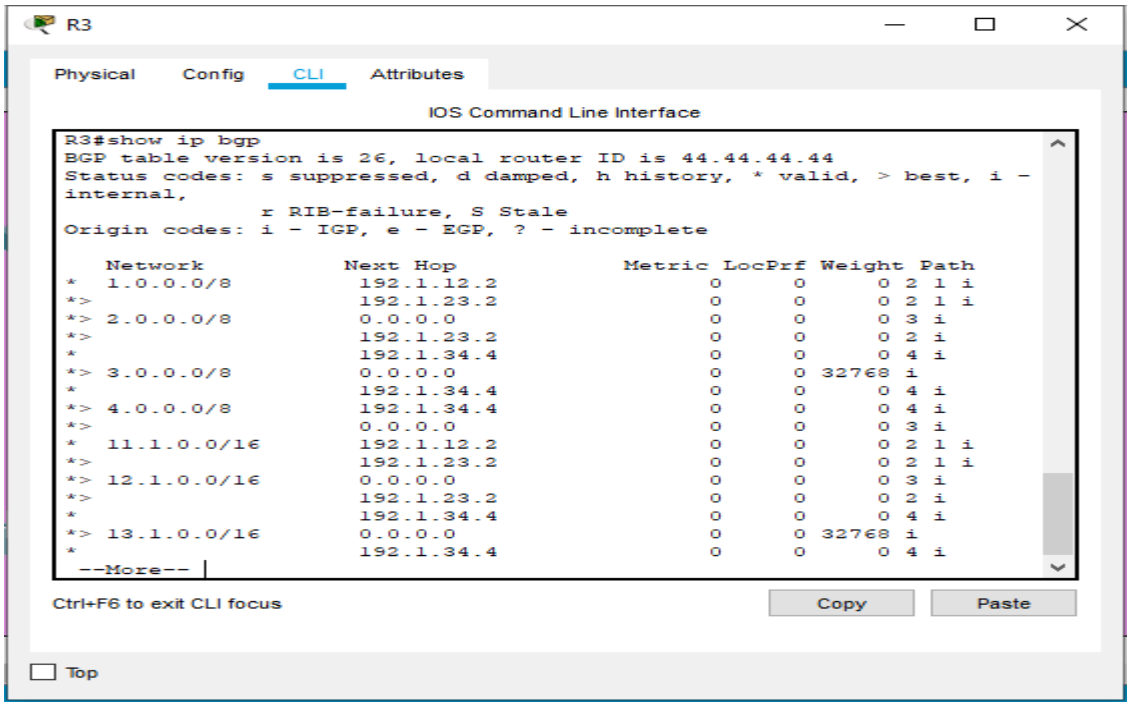
Figura 4. Presentación paso con los comandos utilizados y la salida del comando show ip route 2



1.3 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.

```
R3>enable
R3#config term
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#neighbor 192.1.12.2 remote-as 2
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3#%BGP-5-ADJCHANGE: neighbor 192.1.23.2 Up
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#network 4.4.4.4 mask 255.0.0.0
R3(config-router)#network 14.1.0.1 mask 255.255.0.0
R3(config-router)#network 2.2.2.2 mask 255.0.0.0
R3(config-router)#network 12.1.0.1 mask 255.255.0.0
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)#exit
```

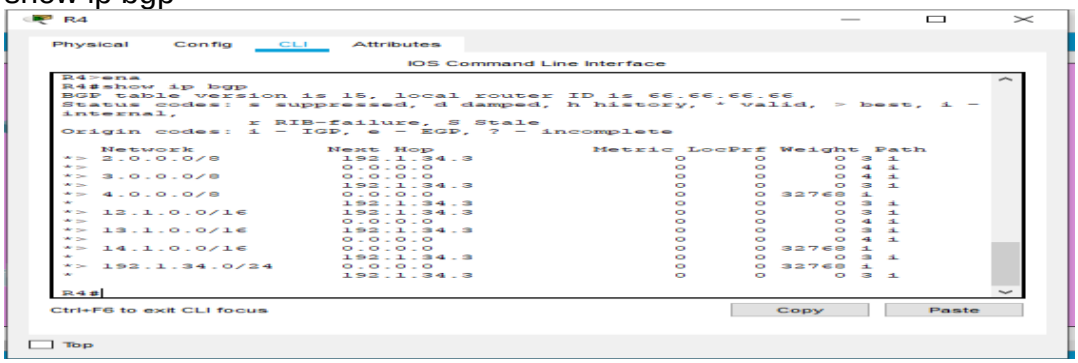
Figura 5. Presentación paso con los comandos utilizados y la salida del comando show ip route 3



1.4 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
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.

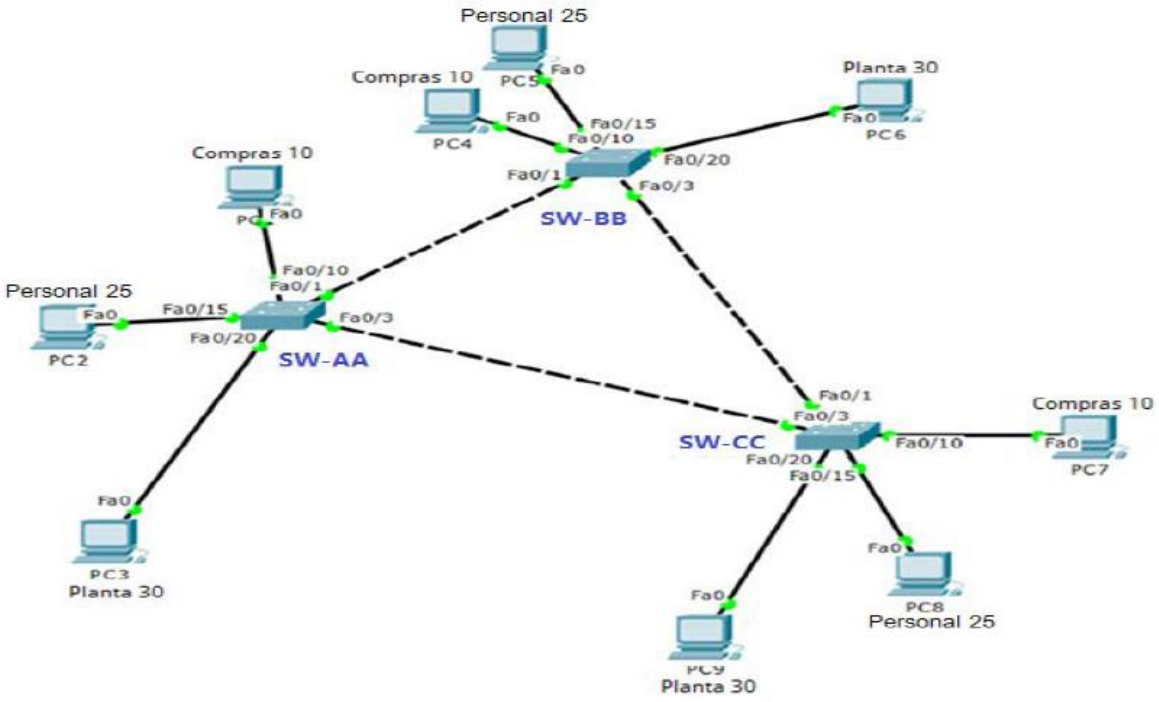
```
R4>enable
R4#config term
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#router bgp 4
R4(config-router)#bgp router-id 66.66.66.66

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)#neighbor 192.1.23.3 remote-as 3
R4(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.23.3 Up
R4(config-router)#neighbor 192.1.23.2 remote-as 2
R4(config-router)#neighbor 192.1.12.2 remote-as 2
R4(config-router)#neighbor 192.1.12.1 remote-as 1
R4(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.34.3 Up
R4(config-router)#network 3.3.3.3 mask 255.0.0.0
R4(config-router)#network 13.1.0.1 mask 255.255.0.0
R4(config-router)#network 12.1.0.1 mask 255.255.0.0
R4(config-router)#network 2.2.2.2 mask 255.0.0.0
R4(config-router)#network 11.1.0.1 mask 255.255.0.0
R4(config-router)#network 4.4.4.4 mask 255.0.0.0
R4(config-router)#network 14.1.0.1 mask 255.255.0.0
R4(config-router)#exit
R4(config)#exit
```

Figura 6. Presentación paso con los comandos utilizados y la salida del comando show ip bgp



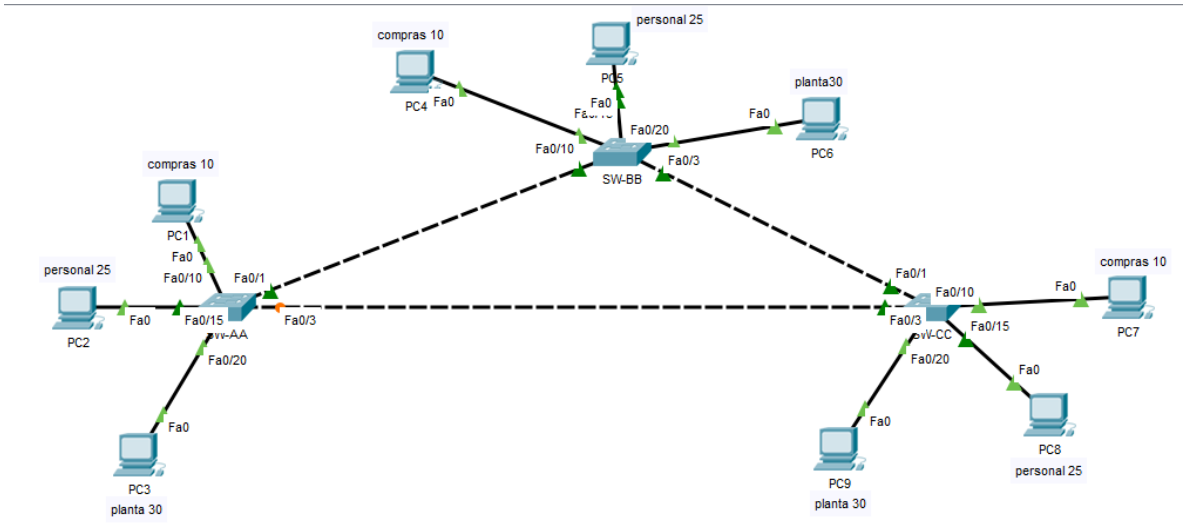
Escenario 2.

Figura 7. Topologia red escenario 2



Desarrollo

Figura 8. Simulacion Escenario 2



2. Configurar VTP

2.1.1. 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.

Desarrollo

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

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-CC
SW-CC(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-CC(config)#vtp version 2
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>enable Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW-BB
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)#

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

Figura 9. Verificación de las configuraciones mediante el comando show vtp status

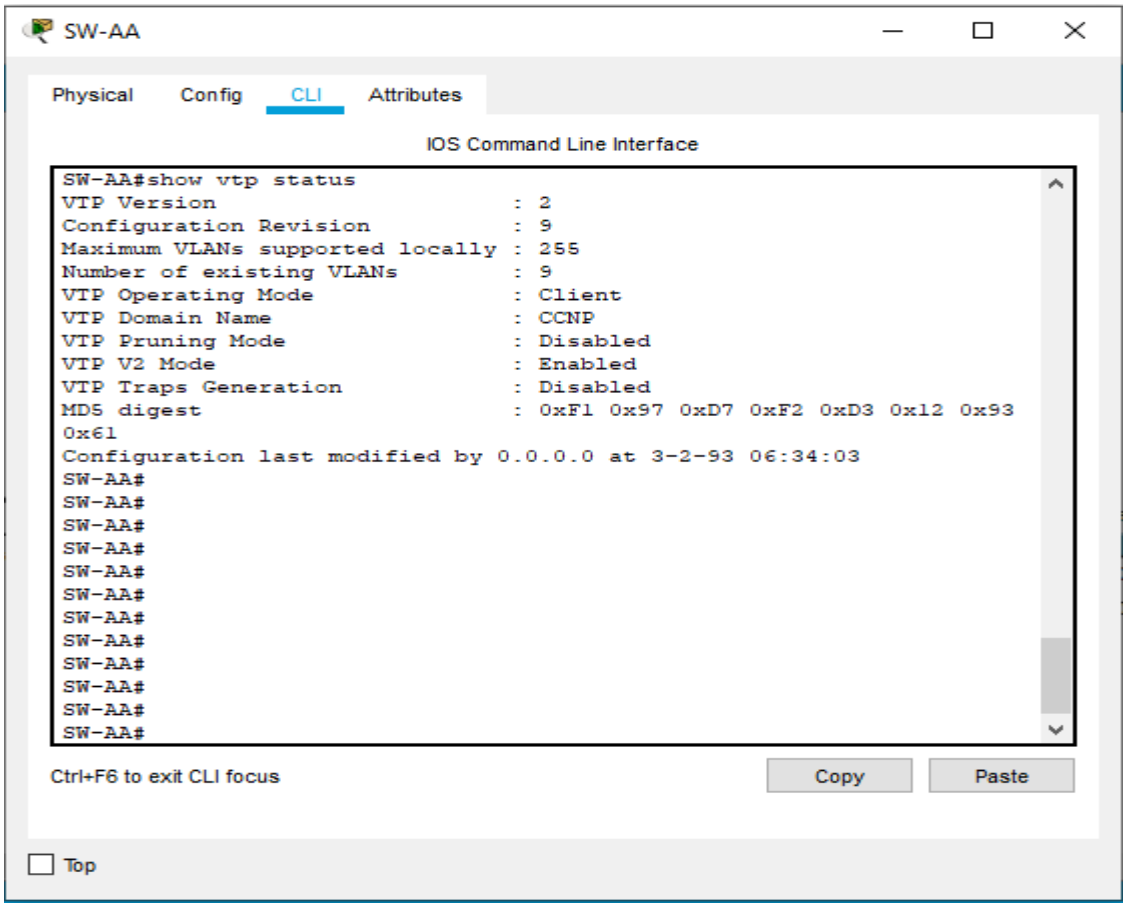


Figura 10. Verificación de las configuraciones mediante el comando show vtp status 2

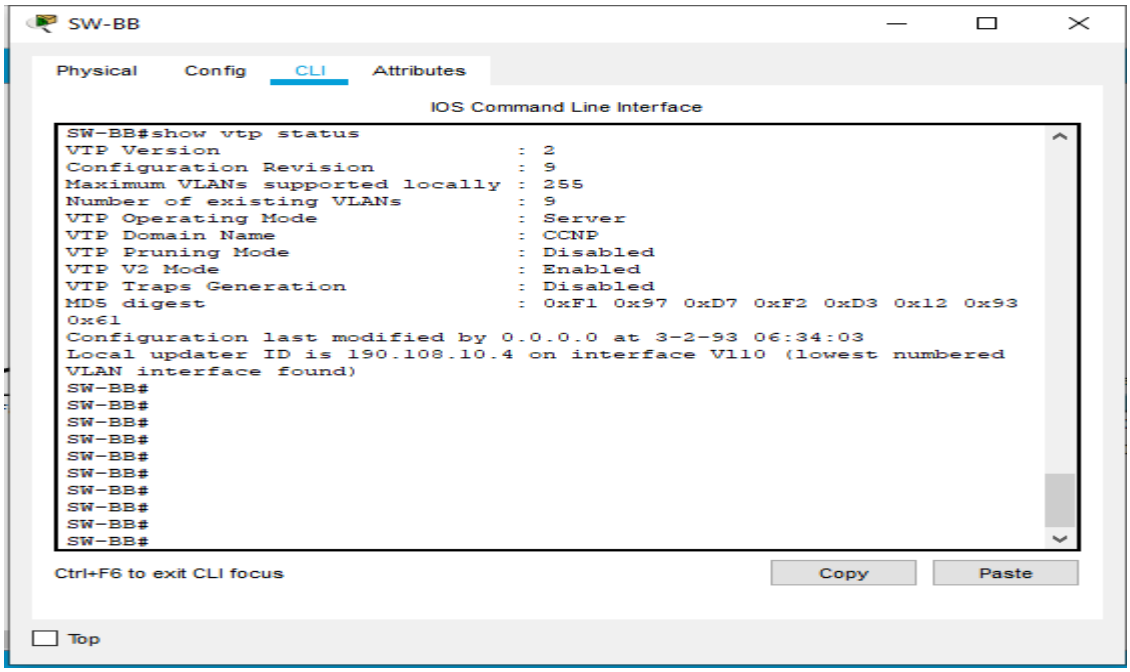
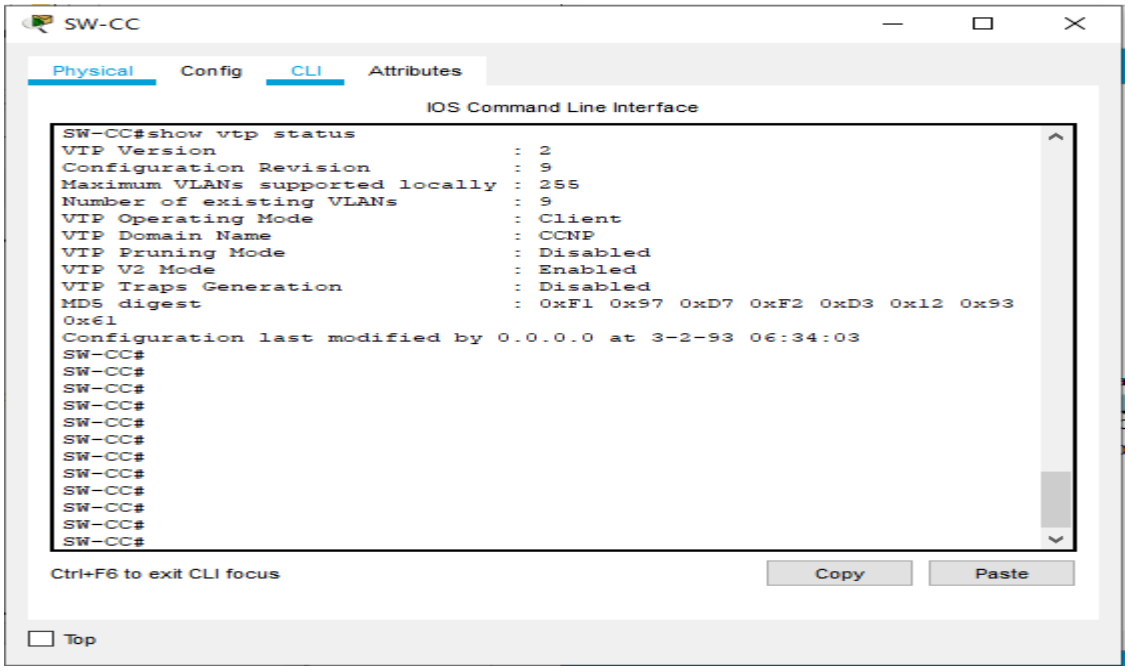


Figura 11. Verificación de las configuraciones mediante el comando show vtp status 3



2.2. Configurar DTP (Dynamic Trunking Protocol)

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

```
SW-AA>enable
SW-AA#conf term
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface fa
SW-AA(config)#interface fastEthernet 0/1
SW-AA(config-if)#switchport mode dynamic desirable
SW-AA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

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

Figura 12. Verificación del estado del enlace trunk en SW-AA

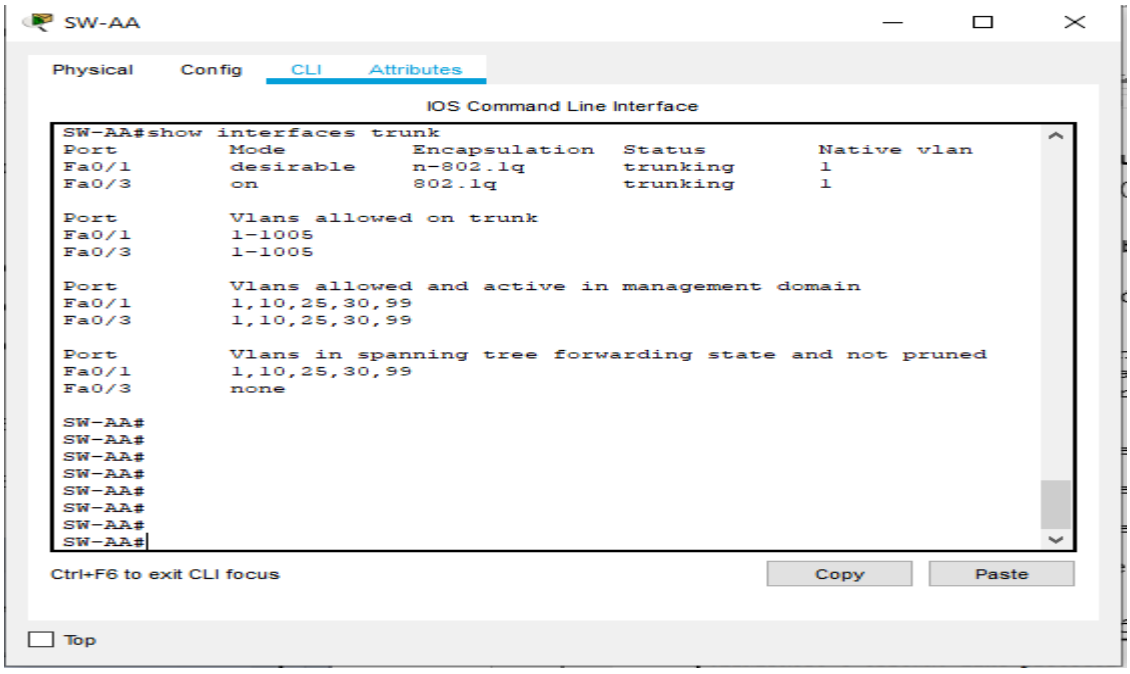
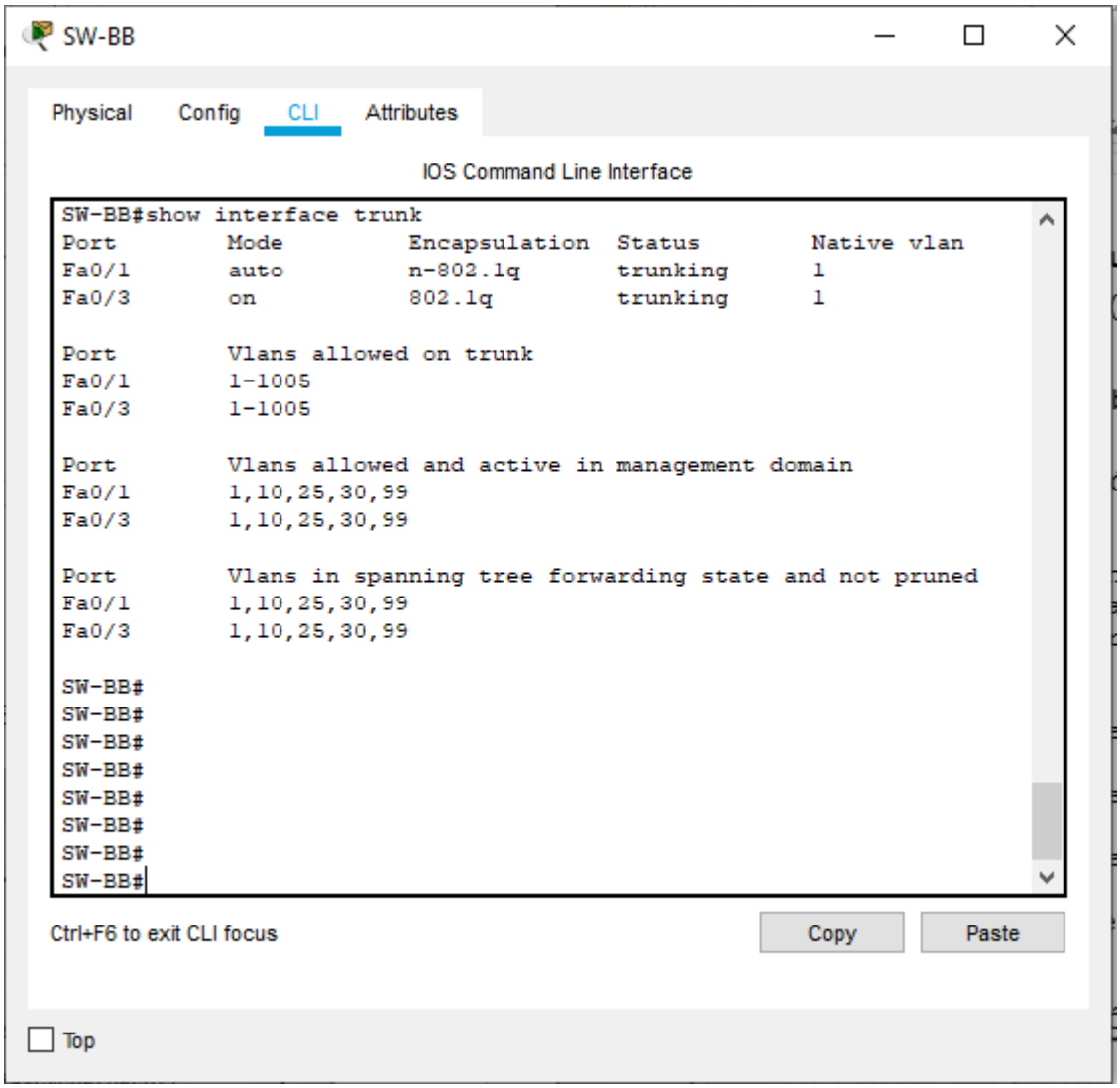


Figura 13. Verificación del estado del enlace trunk en SW-BB



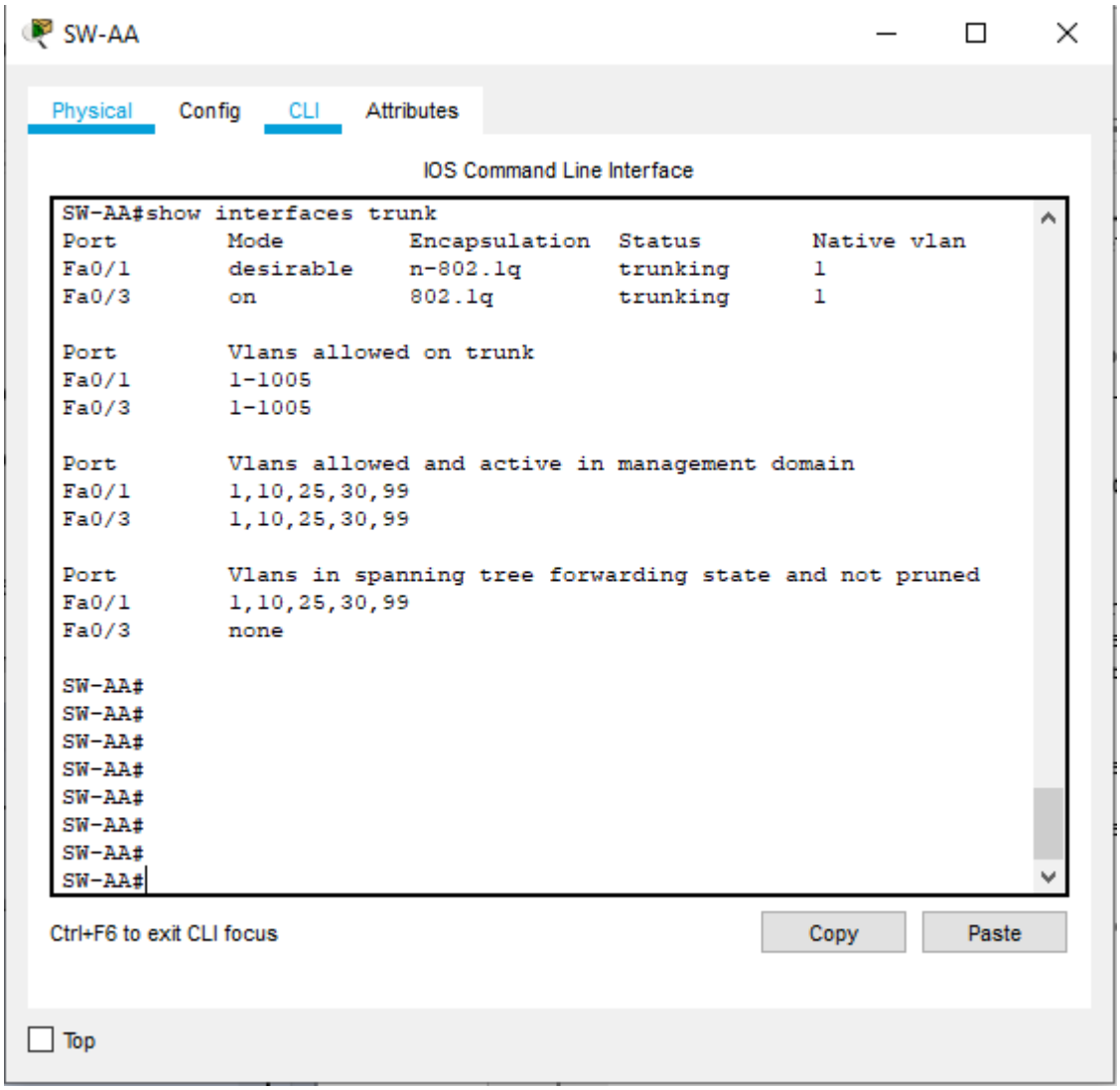
2.2.3. Entre SW-AA y SW-BB configure un enlace "trunk" estático utilizando el comando switchport mode trunk en la interfaz F0/3 de SW-AA

SW-AA>enable
SW-AA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface fa
SW-AA(config)#interface fastEthernet 0/3
SW-AA(config-if)#switchport mode trunk

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

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

Figura 14. Verificación del estado del enlace trunk en SW-AA



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

SW-BB>enable
SW-BB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#interface fa
SW-BB(config)#interface fastEthernet 0/3
SW-BB(config-if)#switchport mode trunk
SW-BB(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
SW-BB(config-if)#exit SWT2(config)#

SW-CC>enable
%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
SW-CC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#interface fa
SW-CC(config)#interface fastEthernet 0/1
SW-CC(config-if)#switchport mode trunk
SW-CC(config-if)#exit
SW-CC(config)#end
SW-CC#

2.3. Agregar VLANs y asignar puertos.

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

En SW-AA

SW-AA>enable
SW-AA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
SW-AA(config)#

En SW-BB

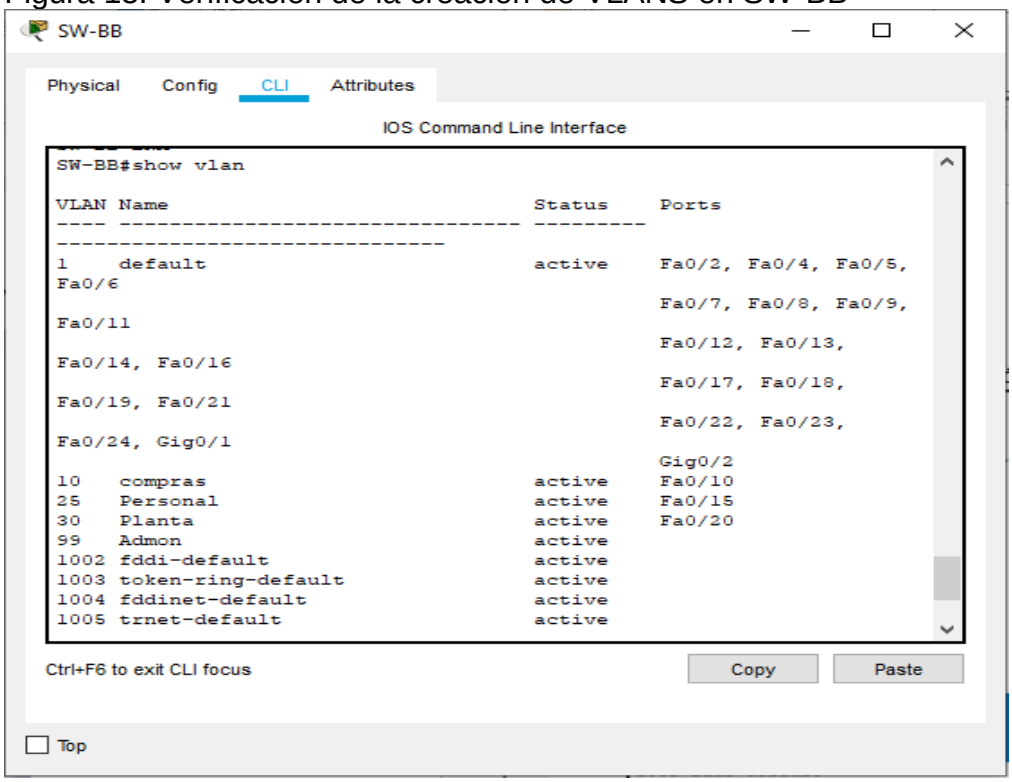
```
SW-BB>enable
SW-BB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#vlan 10
SW-BB(config-vlan)#name compras
SW-BB(config-vlan)#vlan 25
SW-BB(config-vlan)#name Personal
SW-BB(config-vlan)#vlan 30
SW-BB(config-vlan)#name Planta
SW-BB(config-vlan)#vlan 99
SW-BB(config-vlan)#name Admon
SW-BB(config-vlan)#exit
SW-BB(config)#
```

2.3.2. Verifique que las VLANs han sido agregadas correctamente.

En SW-AA: No se pude crear la vlan 10 ya que en el switch AA tiene un vtp en modo cliente, lo que no permite crear la Vlan.

En SW-BB:

Figura 15. Verificación de la creación de VLANS en SW-BB



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

Tabla 5. VLAN y configure las direcciones IP

Interfaz	VLAN	Direcciones IP de los PCs
F0/10	VLAN 10	190.108.10.X / 24
F0/15	VLAN 25	190.108.20.X /24
F0/20	VLAN 30	190.108.30.X /24

X = número de cada PC particular

En SW-AA.

```
SW-AA>enable
SW-AA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface vlan 10
SW-AA(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
SW-AA(config-if)#ip address 190.108.10.1 255.255.255.0
SW-AA(config-if)#exit
SW-AA(config)#interface vlan 25
SW-AA(config-if)#
%LINK-5-CHANGED: Interface Vlan25, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan25, changed state to up
SW-AA(config-if)#ip address 190.108.20.2 255.255.255.0
SW-AA(config-if)#exit
SW-AA(config)#interface vlan 30
SW-AA(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up
SW-AA(config-if)#ip address 190.108.30.3 255.255.255.0 SWT1(config-if)#exit
```

En SW-BB.

```
SW-BB>enable
SW-BB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#interface vlan 10
SW-BB(config-if)#ip address 190.108.10.4 255.255.255.0
```

SW-BB(config-if)#exit
SW-BB(config)#interface vlan 25
SW-BB(config-if)#ip address 190.108.20.5 255.255.255.0
SW-BB(config-if)#exit
SW-BB(config)#interface vlan 30
SW-BB(config-if)#ip address 190.108.30.6 255.255.255.0
SW-BB(config-if)#exit

En SW-CC

SW-CC>enable
SW-CC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#interface vlan 10
SW-CC(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
SW-CC(config-if)#ip address 190.108.10.7 255.255.255.0
SW-CC(config-if)#exit
SW-CC(config)#interface vlan 25
SW-CC(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up

SW-CC(config-if)#ip address 190.108.20.8 255.255.255.0
SW-CC(config-if)#exit
SW-CC(config)#interface vlan 30
SW-CC(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up
SW-CC(config-if)#ip address 190.108.30.9 255.255.255.0
SW-CC(config-if)#exit

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

En SW-AA.

SW-AA>enable

```
SW-AA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface fa
SW-AA(config)#interface fastEthernet 0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#exit
SW-AA(config)#exit
SW-AA#
%SYS-5-CONFIG_I: Configured from console by console
```

En SW-BB.

```
SW-BB(config)#interface fa
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)#
SW-BB#
```

En SW-CC.

```
SW-CC>enable
SW-CC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z..
SW-CC(config)#interface fa
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)#exit
SW-CC#
%SYS-5-CONFIG_I: Configured from console by console
SWCC#
```

2.3.5. Repita el procedimiento para los puertos F0/15 y F0/20 en SW-AA, SW-BB y SW-CC. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

En SW-AA.

```
SW-AA>enable
SW-AA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface fa
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 fa
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)#exit
SW-AA(config)#exit
SW-AA#
%SYS-5-CONFIG_I: Configured from console by console
```

En SW-BB

```
SW-BB>enable
SW-BB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#interface fa
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)#no shut
SW-BB(config-if)#exit
SW-BB(config)#interface fa
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#
%SYS-5-CONFIG_I: Configured from console by console
```

En SW-CC

```
SW-CC>enable
```

```
SW-CC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#interface fa
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 fa
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)#exit
SW-CC#
%SYS-5-CONFIG_I: Configured from console by console
```

2.4. Configurar las direcciones IP en los Switches.

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

Tabla 6. Configurar las direcciones IP en los switches

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

En SW-AA

```
SW-AA>enable
SW-AA#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface vlan99
SW-AA(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
SW-AA(config-if)#exit
SW-AA(config)#
```

En SW-BB
SW-BB>enable
SW-BB#configure terminal
Enter configuration commands, one per line. End with CNTL/Z. SW-BB(config)#interface vlan 99
SW-BB(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
SW-BB(config-if)#exit

En SW-CC.

SW-CC>enable
SW-CC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#interface vlan 99
SW-CC(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0
SW-CC(config-if)#exit
SW-CC(config)#end
SW-CC#
%SYS-5-CONFIG_I: Configured from console by console
SW-CC#

2.5. Verificar la conectividad Extremo a Extremo

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

ping desde la pc1 a la pc7

C:\>ping 190.108.10.5

Pinging 190.108.10.5 with 32 bytes of data:

Reply from 190.108.10.5: bytes=32 time=8ms TTL=128
Reply from 190.108.10.5: bytes=32 time=8ms TTL=128
Reply from 190.108.10.5: bytes=32 time=8ms TTL=128
Reply from 190.108.10.5: bytes=32 time=8ms TTL=128

Ping statistics for 190.108.10.5:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 8ms, Maximum = 8ms, Average = 8ms

ping desde la pc2 a la pc5 y pc8

Packet Tracer PC Command Line 1.0
C:\>ping 190.108.20.6

Pinging 190.108.20.6 with 32 bytes of data:

Reply from 190.108.20.6: bytes=32 time=57ms TTL=128
Reply from 190.108.20.6: bytes=32 time=3ms TTL=128
Reply from 190.108.20.6: bytes=32 time=12ms TTL=128
Reply from 190.108.20.6: bytes=32 time=12ms TTL=128

Ping statistics for 190.108.20.6:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 57ms, Average = 21ms

C:\>ping 190.108.20.9

Pinging 190.108.20.9 with 32 bytes of data:

Reply from 190.108.20.9: bytes=32 time=31ms TTL=128
Reply from 190.108.20.9: bytes=32 time=15ms TTL=128
Reply from 190.108.20.9: bytes=32 time=18ms TTL=128
Reply from 190.108.20.9: bytes=32 time=15ms TTL=128

Ping statistics for 190.108.20.9:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 15ms, Maximum = 31ms, Average = 19ms

RESPUESTA: El ping entre PCs es exitoso porque están dentro de la misma vlan. En caso de tratar de hacer ping entre una vlans diferentes no es posible.

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

ping desde SW-AA a SW-BB

SW-AA#ping 190.108.99.2

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

ping desde SW-AA a SW-CC

SW-AA#ping 190.108.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/2/6 ms

SW-AA#

RESPUESTA: Al ejecutar un ping de cada ping a los demás es correcto, porque la vlan 99 está asignada, por tanto, al realizar ping entre switchs, usando las direcciones ip asignadas en su respectiva sección es satisfactorio.

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

ping desde SW-CC a los pc1, pc2 y pc3

SW-CC#ping 190.108.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 5/16/38 ms

SW-CC#ping 190.108.20.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 3/6/11 ms

SW-CC#ping 190.108.30.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 5/10/13 ms

RESPUESTA: Al realizar un ping entre un switch y los demás pc tiene éxito, debido a que los PCs están comunicado por las troncales de las vlans que hacen parte de las interfaces FastEthernet y estas fueron compartidas entre los switches, por esta razón se puede efectuar un ping entre ellos.

CONCLUSIONES

Es muy importante el uso del comandos como el show ip interface brief, para la revisión de la configuración de las interfaces en dispositivos como los switch, la configuración de la interfaz Vlan del switch mediante la secuencia de comandos, Configure Terminal/ interface vlan1 / ip address [Dirección IP]/ así mismo, el comando ip default Gateway [Dirección IP] para la configuración del Gateway en el switch y corregir así las falencias que tuviese la red para lograr la conexión y obtener el rendimiento de la misma, que se traduce en una experiencia muy provechosa para la evaluación de estos casos eventuales en la vida real.

En la comunicación entre redes es muy importante la configuración de red proporcionada a través de una dirección IP, la correspondiente mascara de subred y el Gateway o puerta de enlace predeterminada, esta ultima la más importante para la comunicación entre redes. Estos tres parámetros son fundamentales a la hora de determinar causas de fallas en la red, para lo cual se debe seguir una metodología de detección, que permita encontrar y corregir el problema, así se recomienda, revisar la documentación de la red y la aplicación de pruebas de conexión para ir descartando dispositivos y bloques de la red, al detectar el problema se determinara la solución pertinente.

La implementación de VLAN en una red permite la optimización del tráfico de red, al separar a los usuarios en grupos con lo cual se puede tener una mejor administración. Al configurar una VLAN en un switch es importante tener en cuenta que éstas comparten el ancho de banda, por ello se requieren medidas de seguridad adicionales como la asignación de un número de VLAN nativo único a los puertos de enlace troncal, limitar las VLAN a transportar sobre los enlaces troncales, desactivar el protocolo de enlace troncal VTP, de lo contrario deben configurarse su dominio de gestión, contraseña y eliminación.

El uso de simuladores de red para el desarrollo de las actividades prácticas contribuye con el proceso de configuración de dispositivos de interconexión de redes Cisco de manera simulada lo que puede proporcionarle seguridad y práctica cuando lo realice en equipos reales, brinda un entorno de práctica donde se pueden agregar o eliminar cuantos dispositivos se requiera, tanto alámbricos como inalámbricos, puede probar diferentes tipos de medios de transmisión dentro de una misma red, observar el comportamiento de los paquetes origen y destino dentro de la red.

BIBLIOGRAFIA

Amberg, E. (2014). CCNA 1 Powertraining: ICND1/CCENT (100-101). Heidleberg: MITP. Recuperado de http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=979032&lang=es&site=ehost-live

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-NT1IlnWR0hoMxgBNv1CJ

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

Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de http://www.birminghamcharter.com/ourpages/auto/2012/3/22/41980164/CCNA%20Electronic%20Book%206th%20edition.pdf

Lucas, M. (2009). Cisco Routers for the Desperate: Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=440032&lang=es&site=ehost-live

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

Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.pdf

Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de http://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxilary%20materials/Cisco-ICND2.pdf

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. 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). EIGRP 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). Manipulating Routing Updates. 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). OSPF Implementation. 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