DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

HEIDY JOHANNA GARCIA WILCHES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ
2020

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

HEIDY JOHANNA GARCIA WILCHES

Diplomado de opción de grado presentado para optar el titulo
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
BOGOTÁ
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, 22 de Mayo de 2020

DEDICATORIA

En primer lugar agradezco a Dios por permitirme estar culminando mi carrera, la que con tanto esfuerzo, esmero y sacrificio finalizo como Ingeniera en Telecomunicaciones, seguido por mi esposo Jeisson quien siempre estuvo apoyándome aun cuando pensaba en rendirme, a mi hija Sharon Sofia por su paciencia y sacrificar tardes de juego o momentos familiares para permitirme mi espacio y dedicarme de lleno a la universidad también dedico este gran logro a mi bebe Thiago por llegar a nuestro hogar y culminar conmigo en esta fase de mi carrera.

A los tutores, quienes, sin importar la hora, en muchas ocasiones trasnocharon conmigo para permitirme adquirir sus valiosos conocimientos por medio de tutorías vía Skype, y a la Universidad UNAD por permitir la reunión de medios y estrategias para la adquisición de estos conocimientos.

A todos mil gracias.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

CCNP:(Cisco Certified Network Professional / Profesional en Redes certificado por Cisco), es una certificación de nivel intermedio entregada por la compañía Cisco Systems a las personas que hayan rendido satisfactoriamente el curso y el examen correspondiente, consta de dos módulos CCNP ROUTE y CCNP SWITCH.

IPv4: Una dirección IP con base en el IPv4. Esas direcciones consisten en 32 bits (0 al 31) particionados en cuatro grupos de ocho bits cada uno (llamados octetos) y organizados en cinco clases (A a la E) con base en los valores de bits 0 al 3.

Networking: también llamada red de ordenadores, red de comunicaciones de datos o red informática conjunto de equipos informáticos y software reconectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

.

ROUTE: O también llamado enrutador Dispositivo hardware o software de interconexión de redes de computadores que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red. El router toma decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirige los paquetes hacia el segmento y el puerto de salida adecuados.

SWITCH: Dispositivo de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconection). Un switch interconecta dos o más segmentos de red, pasando datos de un segmento a otro, de acuerdo con la dirección de destino de los datagramas en la red. Un switch en el centro de una red en estrella. Los switches se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs.

RESUMEN

El siguiente trabajo corresponde al trabajo final del diplomado de CISCO llamado CCNP el cual está Dirigido a: Técnicos, Tecnólogos y Profesionales de las áreas de electrónica, telecomunicaciones y sistemas. Este diplomado se divide en dos módulos CCNP ROUTE y CCNP SWITCH en donde el estudiante demuestra conocimientos adquiridos en la administración y buen manejo de los equipos de red, para ello se presentan dos escenarios los cuales se deben desarrollar las configuraciones correspondientes aplicando los conceptos adquiridos como lo son protocolos de enrutamiento EIGRP, OSPF, BGP, redistribución de rutas, conmutación en una arquitectura de red empresarial, la implementación de VLANs en redes corporativas, como la detección y solución de problemas.

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

ABSTRACT

The following text belongs to the final delivery for Cisco course called CCNP, which is oriented to: Technicians, technologist, and professionals for Electronics, telecommunications and systems fields. This course is divided in two modules CCNP ROUTE and CCNP SWITCH, the student will evidence knowledge about management and networking. for these two scenarios will be shown and all the configurations learnt must be applied related to the routing protocols as EIGPR, OSPF, BGP, routing distribution, switching in a enterprise architecture, VLANs implementation in corporative networks, detection and problem solving

Keywords: CISCO, CCNP, Routing, Switching, Networking, Electronics

INTRODUCCIÓN

El Diplomado Cisco CCNP (Cisco Certified Networking Proffesional tiene como gran objetivo que el estudiante adquiera conocimientos de nivel medio en el cual se centra en planificar, implementar y monitorear redes de tipo LAN Y WAN implementando los principios básicos de enrutamiento IP versión 4 (IPv4) e IP versión 6 (IPv6) EIGRP, OSPF, BGP.

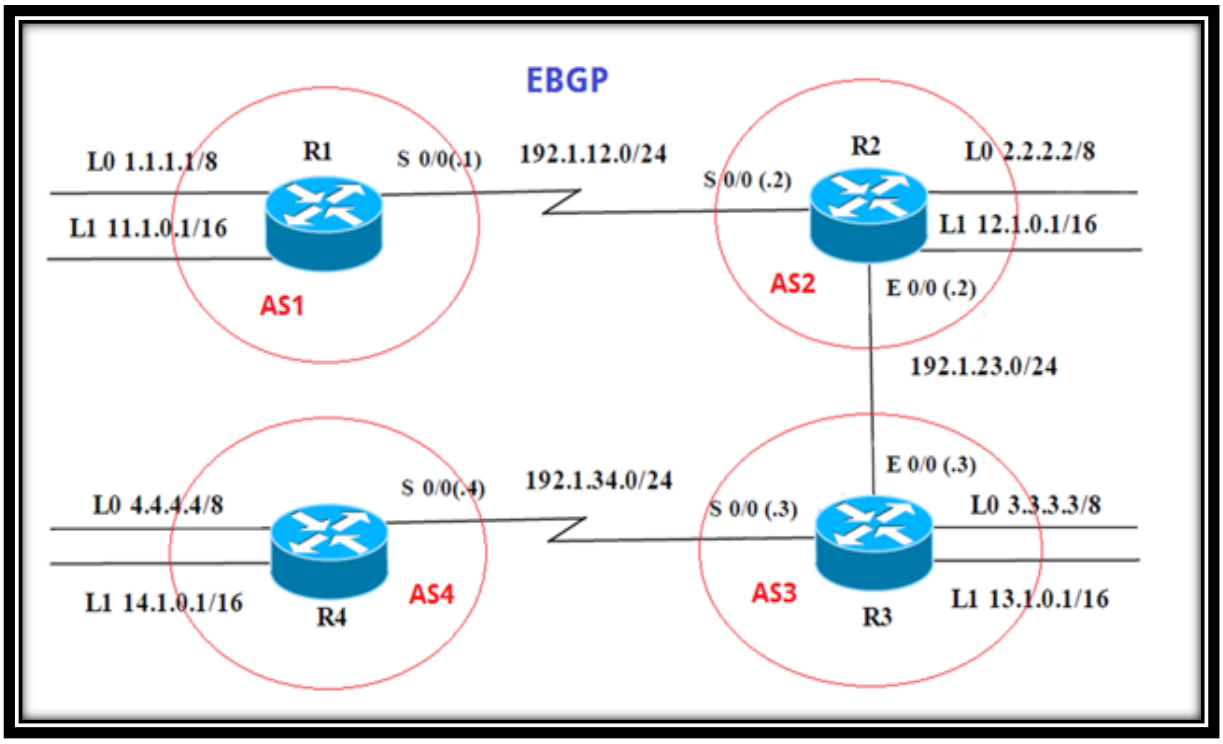
Encontramos en la presente prueba de habilidades dos escenarios, en el primer escenario se realizara la configuración de Routers con sus correspondientes protocolos de enrutamiento, configuración de interfaces, asignación de ip según tabla asignada, Configuración de relaciones EBGP, establecimientos de las relaciones de vecinos, cconfiguración de interfaz loopback y validar por medio del comando Show ip route esta configuración.

Luego podemos aplicar en el escenario #2 conceptos correspondientes a configuración de Switch, en donde se realizaran configuración de VTP creando un switch como servidor y los otros como clientes, luego se realizara una configuración de enlace troncal ("trunk") entre SWT1 y SWT2, se evidencia el resultado de estas configuraciones por medio del paso a paso de la configuración y comprobación de cada uno de los dispositivos en la verificación de conectividad de cada escenario se realizado mediante los comandos ping, traceroute, show ip route, entre otros.

DESARROLLO DE LOS DOS ESCENARIOS

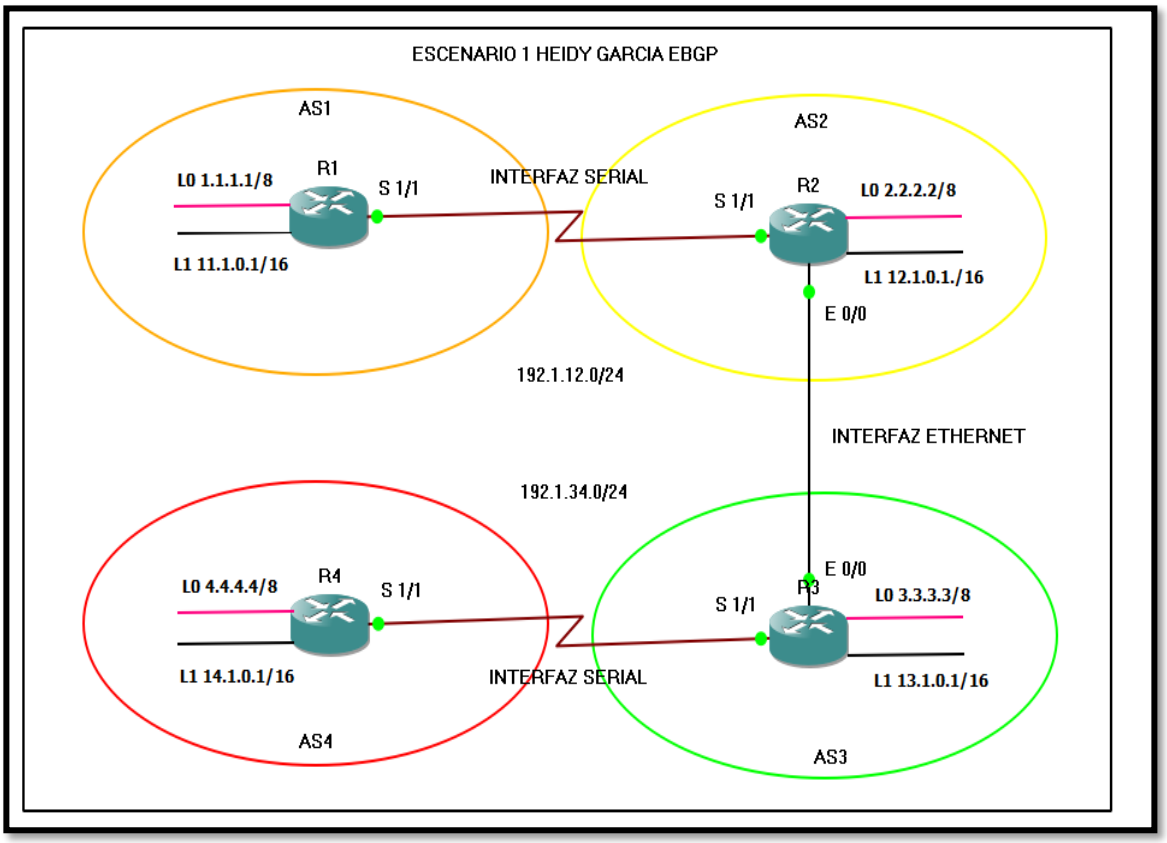
1. ESCENARIO 1

Figura 1. Topología de red primer escenario



En la siguiente imagen se evidencia simulación del escenario 1 en software GNS3:

Figura 2. Simulación de escenario



Información para configuración de los Routers:

Tabla 1 Direccionamiento IP R1

Interfaz	Dirección IP	Mascara
Loopback 0	1.1.1.1	8
Loopback 1	11.1.0.1	16
Serial 1/1	192.1.12.1	24

Tabla 2 Direccionamiento IP R2

Interfaz	Dirección IP	Mascara
Loopback 0	2.2.2.2	8
Loopback 1	12.1.0.1	16
Serial 1/1	192.1.12.2	24
Ethernet 0/0	192.1.23.2	24

Tabla 3 Direccionamiento IP R3

Interfaz	Dirección IP	Mascara
Loopback 0	3.3.3.3	8
Loopback 1	13.1.0.1	16
Serial 1/1	192.1.23.3	24
Ethernet 0/0	192.1.34.3	24

Tabla 4 Direccionamiento IP R4

Interfaz	Dirección IP	Mascara
Loopback 0	4.4.4.4	8
Loopback 1	14.1.0.1	16
Serial 1/1	192.1.34.4	24

Implementación:

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.***

En primer lugar, procedemos a realizar la configuración básica de los Routers:

Tabla 5 Configuración básica Router R1

Código de Configuración Aplicado - R1	**Descripción**
Router>	
Router>enable	Se ingresa a modo privilegiado
Router#configure terminal	Se Ingresa a modo de configuración
Router(config)#hostname R1	Se Asigna nombre al Router
R1(config)#no ip domain-lookup	Desactivar la resolución DNS en el router
R1(config)#line console 0	Ingresa a parámetros de consola
	evita que los mensajes inesperados que aparecen en pantalla, nos

R1(config-line)#logging synchronous	desplacen los comandos que estamos escribiendo en el momento
R1(config-line)#exec-timeout 0 0	Desconexión por inactividad en una sesión de acceso. Si se configura un tiempo 0, se entiende como que no hay límite de tiempo
R1(config-line)#exit R1(config)#	Salir del modo de configuración

De igual manera se procede a configurar los otros Router:

Código de Configuración Aplicado – R2

```
Router>
Router>enable
Router#configure terminal
Router(config)#hostname R2
 R2(config)#no ip domain-lookup
 R2(config)#line console 0
R2(config-line)#logging synchronous
R2(config-line)#exec-timeout 0 0
R2(config-line)#exit
R2(config)#
```

Código de Configuración Aplicado – R3

```
Router>
Router>enable
Router#configure terminal
Router(config)#hostname R3
R3(config)#no ip domain-lookup
 R3(config)#line console 0
R3(config-line)#logging synchronous
R3(config-line)#exec-timeout 0 0
 R3(config-line)#exit
 R3(config)#
```

Código de Configuración Aplicado – R4

```
Router>
```

Router>enable
Router#configure terminal
Router(config)#hostname R3
R4(config)#no ip domain-lookup
R4(config)#line console 0
R4(config-line)#logging synchronous
R4(config-line)#exec-timeout 0 0
R4(config-line)#exit
R4(config)#

Luego, procedemos a realizar configuración en cada Rourter, asignando el direccionamiento IP correspondiente según tablas suministradas anteriormente, la relación de vecinos y el loockback:

Tabla 6 Configuración IP Router R1

Código de Configuración Aplicado - R1	**Descripción**
R1> R1>enable	Se ingresa a modo privilegiado
R1#configure terminal	Se Ingresa a modo de configuración
R1(config)#interface serial 1/1	Permite Configurar interfaz serial
R1(config-if)#description R1 to R2	Descripción de interfaz
R1(config-if)#clock rate 64000	Sincronismo conexión seria DCE
R1(config-if)#bandwidth 64	Establece el valor de ancho de banda
R1(config-if)#ip address 192.1.12.1 255.255.255.0	Asignación IPV4
R1(config-if)#no shutdown R1(config-if)#exit	Activa la interfaz Salir del modo de configuración

Tabla 7 Configuración Loopback Router R1

Código de Configuración Aplicado - R1	**Descripción**
R1> R1>enable	Se ingresa a modo privilegiado
R1#configure terminal	Se Ingresa a modo de configuración
R1(config)#interface loopback 0	Configuración del interfaz loopback 0

R1(config-if)#ip address 1.1.1.1 255.0.0.0	Asignación IPV4
R1(config-if)#exit	Salir del modo de configuración
R1(config)#interface loopback1	Configuración del interfaz loopback 1
R1(config-if)#ip address 11.1.0.1 255.255.0.0	Asignación IPV4
R1(config-if)#exit	Salir del modo de configuración

De igual manera se procede a configurar los otros Routers:

Configuración Router R2

```
R2>
R2>enable
R2#configure terminal
R2(config)#interface serial 1/1
R2(config-if)#description R2 to R1
R2(config-if)#bandwidth 64
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit

R2>
R2>enable
R2#configure terminal
R2(config)# interface fastEthernet 0/0
R2(config-if)#description R2 to R3
R2(config-if)#bandwidth 64
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit

R2>
R2>enable
R2#configure terminal
R2(config)#interface loopback 0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#exit
R2(config)#interface loopback 1
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#exit
```

Configuración Router R3

```
R3>
R3>enable
R3#configure terminal
R3(config)#interface serial 1/1
R3(config-if)#description R3 to R4
R3(config-if)#clock rate 64000
R3(config-if)#bandwidth 64
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3>

R3>enable
R3#configure terminal
R3(config)# interface fastEthernet 0/0
R3(config-if)#description R3 to R2
R3(config-if)#bandwidth 64
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit

R3>
R3>enable
R3#configure terminal
R3(config)#interface loopback 0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#exit
R3(config)#interface loopback 1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#exit
```

Configuración Router R4

```
R4>
R4>enable
R4#configure terminal
R4(config)#interface serial 1/1
R4(config-if)#description R4 to R3
R4(config-if)#clock rate 64000
R4(config-if)#bandwidth 64
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
```

R4>
R4>enable
R4#configure terminal
R4(config)#interface loopback 0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#exit
R4(config)#interface loopback 1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#exit

Ahora, procedemos a configurar la relación BGP:

Tabla 8 Configuración BGP Router R1

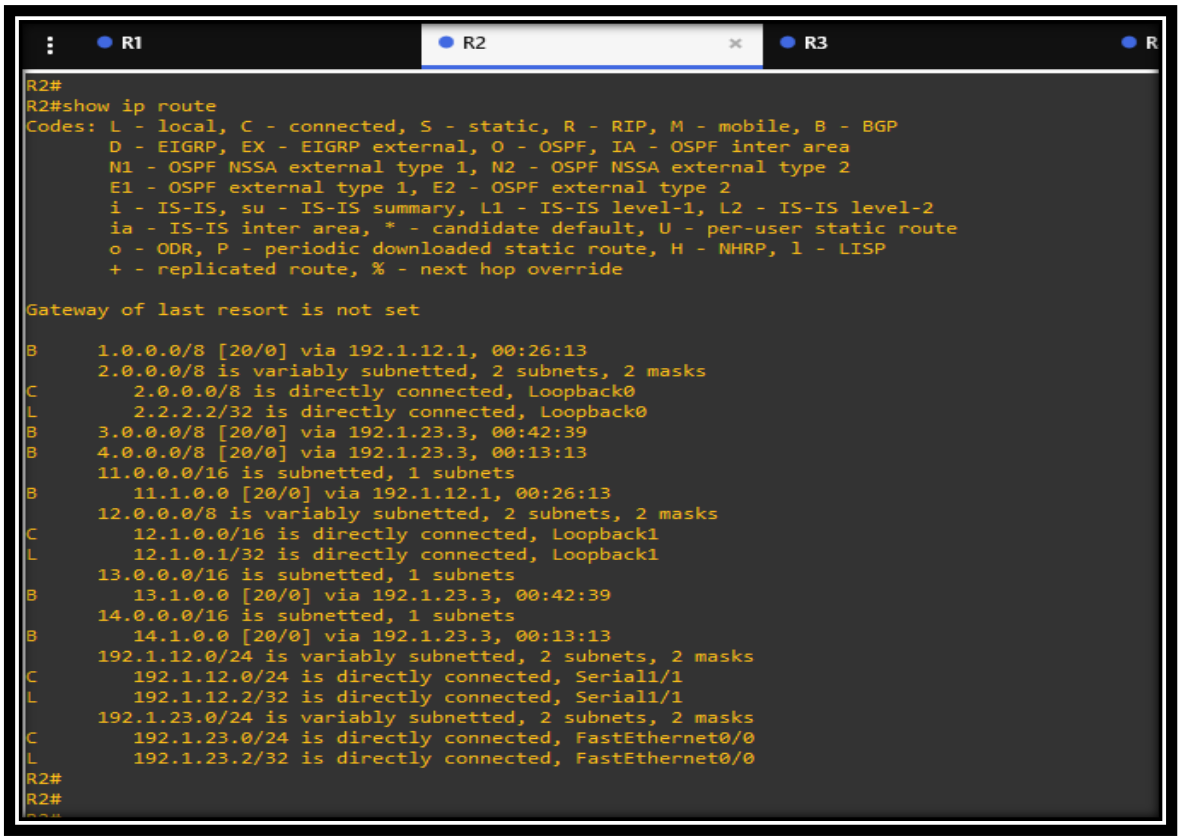
Código de Configuración Aplicado - R1	**Descripción**
R1> R1>enable	Ingresa a modo privilegiado
R1#configure terminal	Ingresa a modo de configuración
R1(config)#router bgp 1	Configurar el protocolo BGP
R1(config-router)#no synchronization	Ignora la sincronización
R1(config-router)#bgp router-id 22.22.22.22	Asigna ID al router
R1(config-router)#neighbor 192.1.12.2 remote-as 2	Detección de redes
R1(config-router)#network 1.0.0.0 mask 255.0.0.0	Anunciar red
R1(config-router)#network 11.1.0.0 mask 255.255.0.0	Anunciar red
R1(config-router)#exit	Salir del modo de configuración

Configuración BGP Router R2 Y R1
R2>
R2>enable
R2#configure terminal
R2(config)#router bgp 2
R2(config-router)#no synchronization

R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#network 2.0.0.0 mask 255.0.0.0
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
R2(config-router)#exit

Figura 3. Show ip Router 1

Figura 4. Show ip Router 2



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 BGP Router R2 y R3

R2>
R2>enable
R2#configure terminal
R2(config)#router bgp 2
R2(config-router)#no synchronization
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#neighbor 192.1.23.3 remote-as 3
R2(config-router)#network 2.0.0.0 mask 255.0.0.0
R2(config-router)#network 12.1.0.0 mask 255.255.0.0

R2(config-router)#exit

Configuración BGP Router R3 Y R2

R3>
R3>enable
R3#configure terminal
R3(config)#router bgp 3
R3(config-router)#no synchronization
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#network 3.0.0.0 mask 255.0.0.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3(config-router)#exit

Figura 5. Show ip Router 2

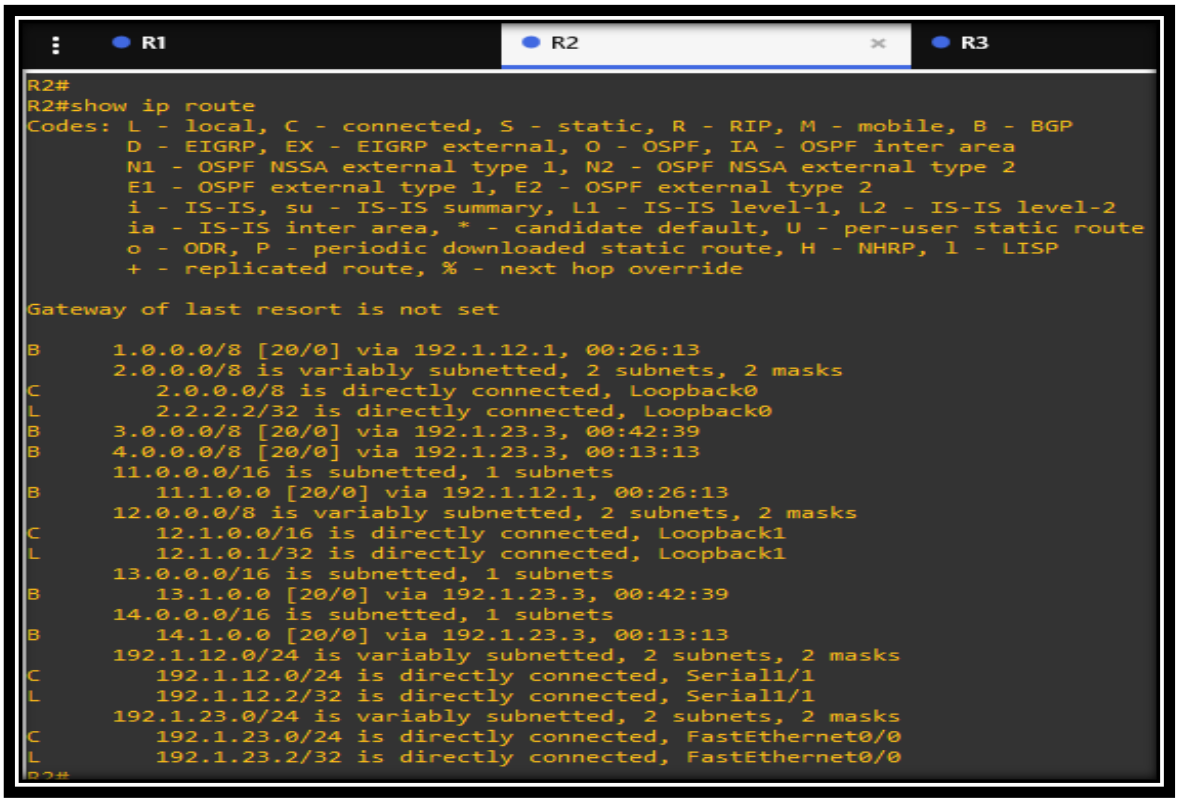


Figura 6. Show ip Router 3

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 BGP Router R3 Y R4

R3>

R3>enable

R3#configure terminal

R3(config)#router bgp 3

R3(config-router)#no synchronization

R3(config-router)#bgp router-id 44.44.44.44

R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#network 3.0.0.0 mask 255.0.0.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3(config-router)#exit

Configuración BGP Router R4 Y R3

R4>
R4>enable
R4#configure terminal
R4(config)#router bgp 4
R4(config-router)#no synchronization
R4(config-router)#bgp router-id 66.66.66.66
R4(config-router)#neighbor 192.1.34.3 remote-as 3
R4(config-router)#network 4.0.0.0 mask 255.0.0.0
R4(config-router)#network 14.1.0.0 mask 255.255.0.0
R4(config-router)#exit

Por último se deben crear las rutas estáticas para alcanzar la loopback del otro router.

Configuración ruta estatica Router R3

R3>
R3>enable
R3#configure terminal
R3(config)#ip route 4.0.0.0 255.0.0.0 192.1.34.4

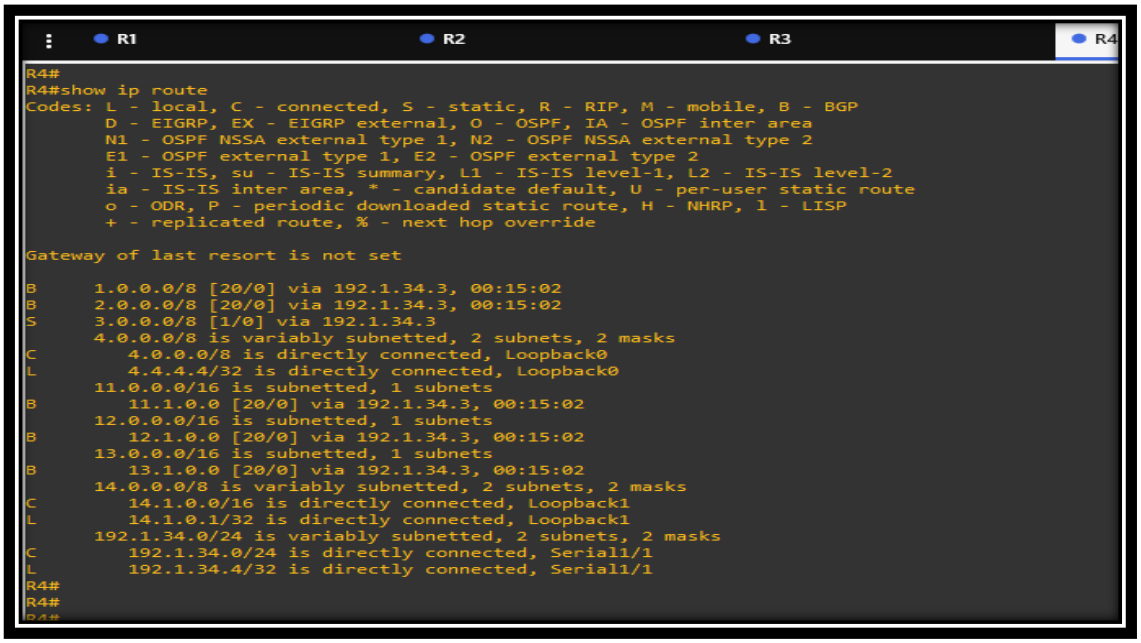
Configuración ruta estatica Router R4

R4>
R4>enable
R4#configure terminal
R4(config)#ip route 3.0.0.0 255.0.0.0 192.1.34.3

Validación con comando ***show ip route:***

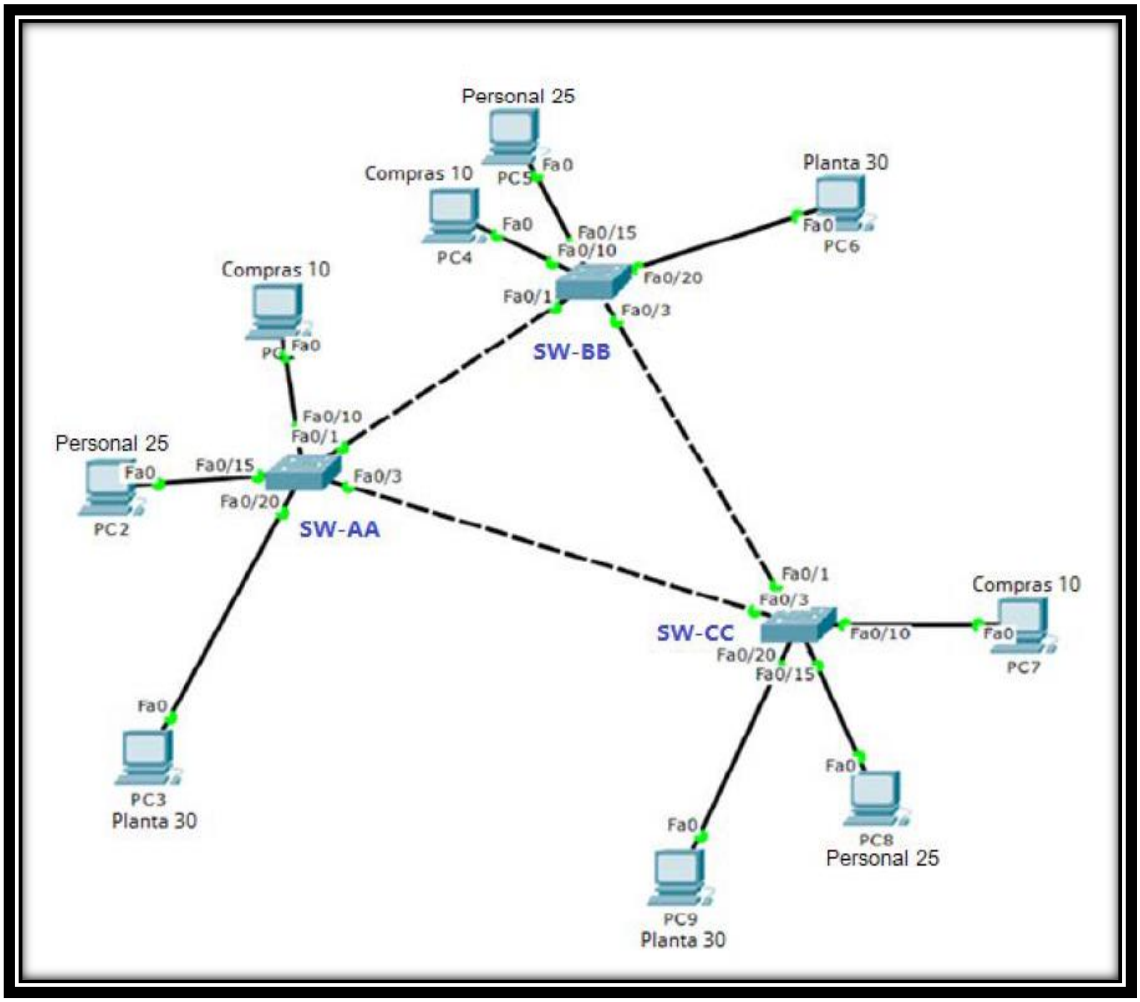
Figura 7. Show ip Router 3

Figura 8. Show ip Router 4



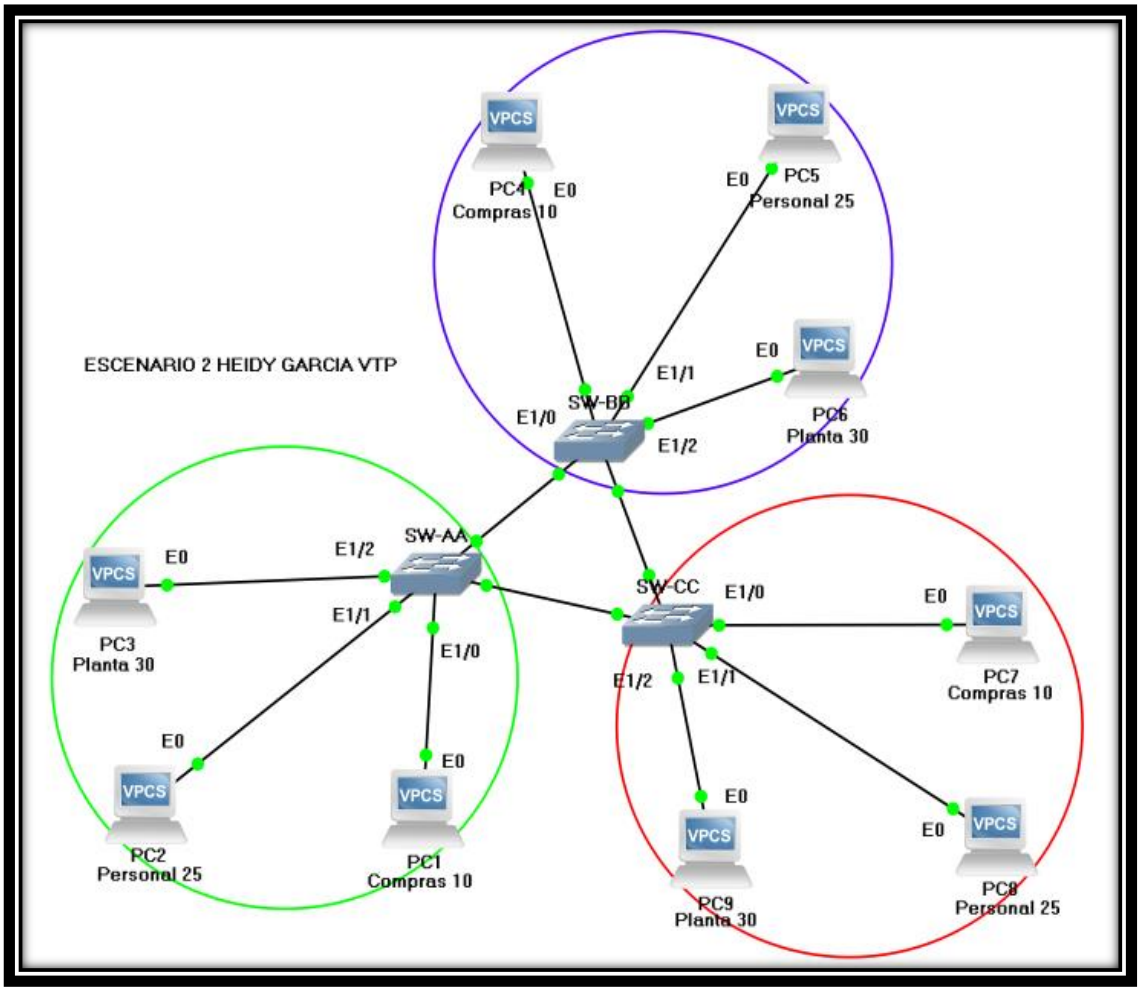
2. ESCENARIO 2

Figura 9. Topología de red escenario 2.



En la siguiente imagen se evidencia simulación del escenario 1 en software GNS3:

Figura 10. Simulación del escenario 2



Implementación:

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.

Tabla 9 Configuración SW-AA

Código de Configuración Aplicado – SW-AA	**Descripción**
Switch> Switch>enable	Se ingresa a modo privilegiado
Switch#configure terminal	Se Ingresa a modo de configuración
Switch(config)#hostname SW-AA	Se Asigna nombre al Switch
SW-AA(config)#no ip domain-lookup	Desactivar la resolución DNS en el Switch
SW-AA(config)#line console 0	Ingresa a parámetros de consola
SW-AA(config-line)#logging synchronous	evita que los mensajes inesperados que aparecen en pantalla, nos desplacen los comandos que estamos escribiendo en el momento
SW-AA(config-line)#exec-timeout 0 0	Desconexión por inactividad en una sesión de acceso. Si se configura un tiempo 0, se entiende como que no hay límite de tiempo
SW-AA(config-line)#exit	Salir del modo de configuración
SW-AA(config)# vtp mode client	Configuración VTP modo cliente
SW-AA(config)#vtp domain CCNP	Configuración dominio VTP
SW-AA(config)#vtp password cisco	Contraseña de VTP cisco
SW-AA(config)#exit	Salir del modo de configuración

De igual manera se procede a configurar los otros Switch:

Configuración SW-BB

Switch>
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-BB
SW-BB(config)#no ip domain-lookup
SW-BB(config)#line console 0

SW-BB(config-line)#logging synchronous
SW-BB(config-line)#exec-timeout 0 0
SW-BB(config-line)#exit
SW-BB(config)# vtp mode server
SW-BB(config)#vtp domain CCNP
SW-BB(config)#vtp password cisco
SW-BB(config)#exit

Configuración SW-CC

Switch>
Switch>enable
Switch#configure terminal
Switch(config)#hostname SW-CC
SW-CC(config)#no ip domain-lookup
SW-CC(config)#line console 0
SW-CC(config-line)#logging synchronous
SW-CC(config-line)#exec-timeout 0 0
SW-CC(config-line)#exit
SW-CC(config)# vtp mode client
SW-CC(config)#vtp domain CCNP
SW-CC(config)#vtp password cisco
SW-CC(config)#exit

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

Figura 11. Show VTP Status SW-AA

Figura 12. Show VTP Status SW-BB

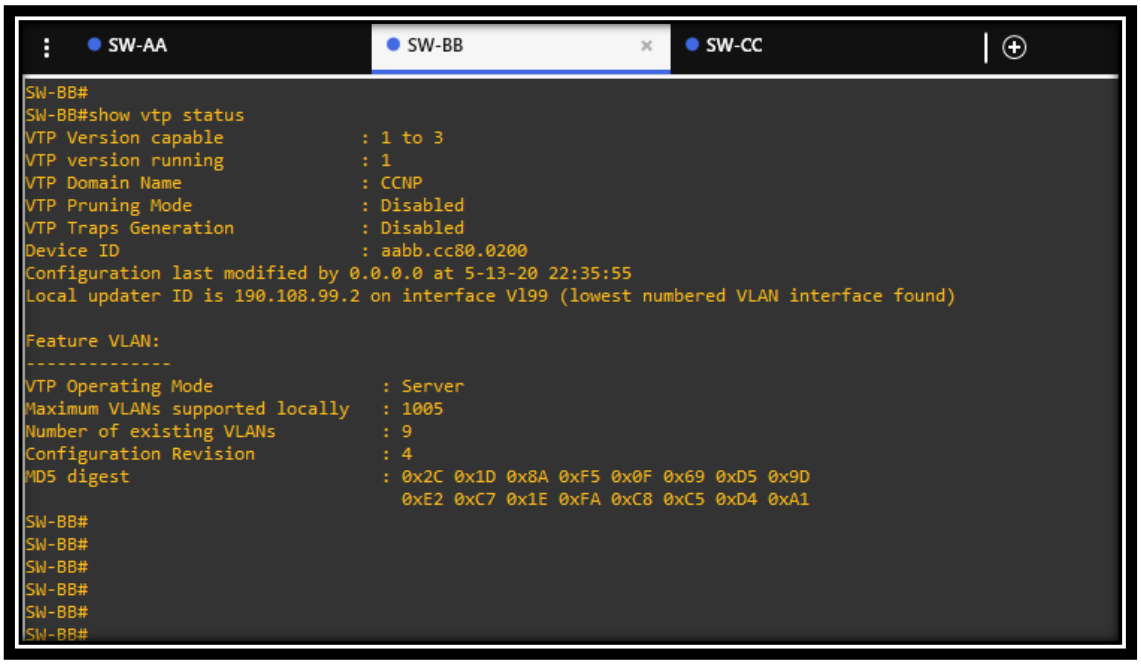
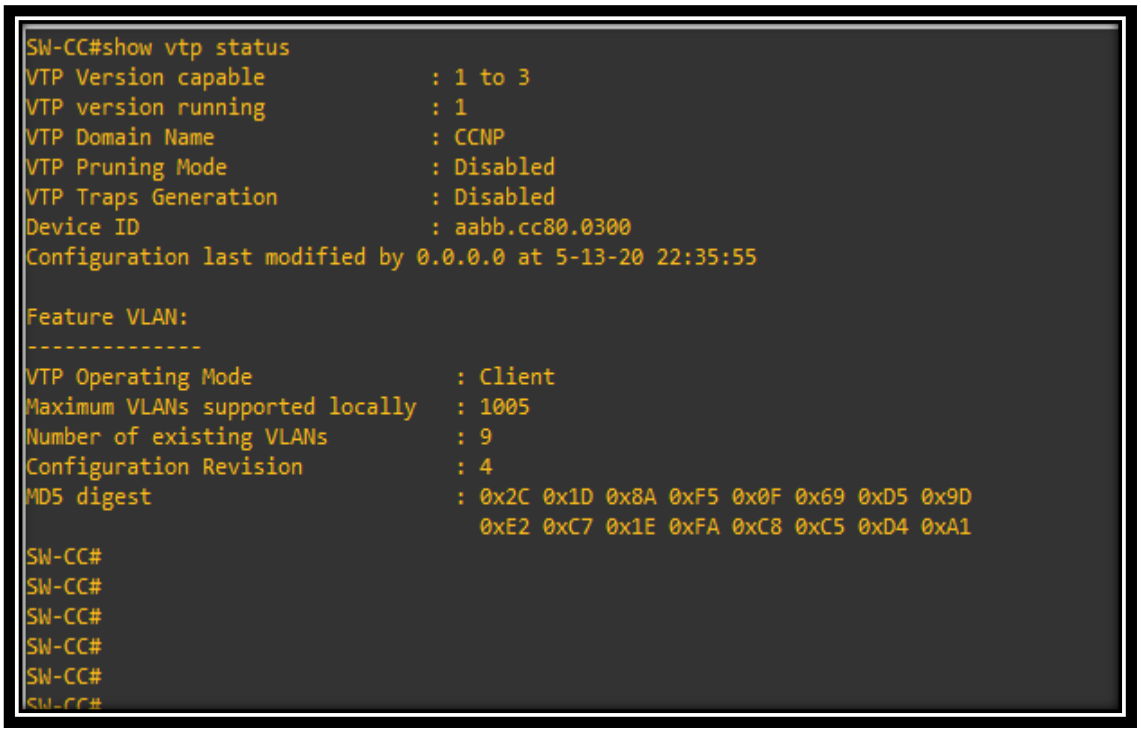


Figura 13. Show VTP Status SW-CC



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***.

Tabla 10 Configuración DTP SW-AA

Código de Configuración Aplicado – SW-AA	**Descripción**
SW-AA>enable	Se ingresa a modo privilegiado
SW-AA#configure terminal	Se Ingresa a modo de configuración
SW-AA(config)#interface ethernet 0/0	Se Configura interfaz ethernet
SW-AA(config-if)#switchport mode trunk	Modo trunk del Puerto
SW-AA(config-if)#switchport mode Dynamic desirable	Ingresa a parámetros de Modo de operación troncal
SW-AA(config)#exit	Salir del modo de configuración

Configuración DTP SW-BB

SW-BB>enable
SW-BB#configure terminal
SW-BB(config)#interface ethernet 0/0
SW-BB(config-if)#switchport mode trunk
SW-BB(config-if)#exit

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

Figura 14. Show Interface Trunck SW-AA

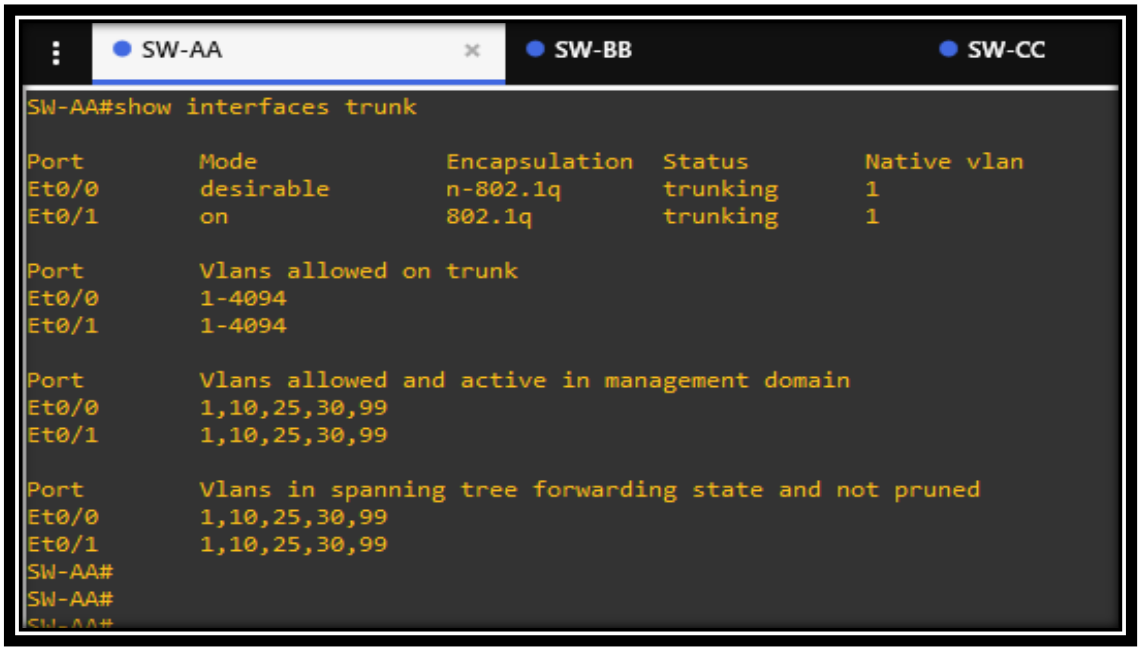
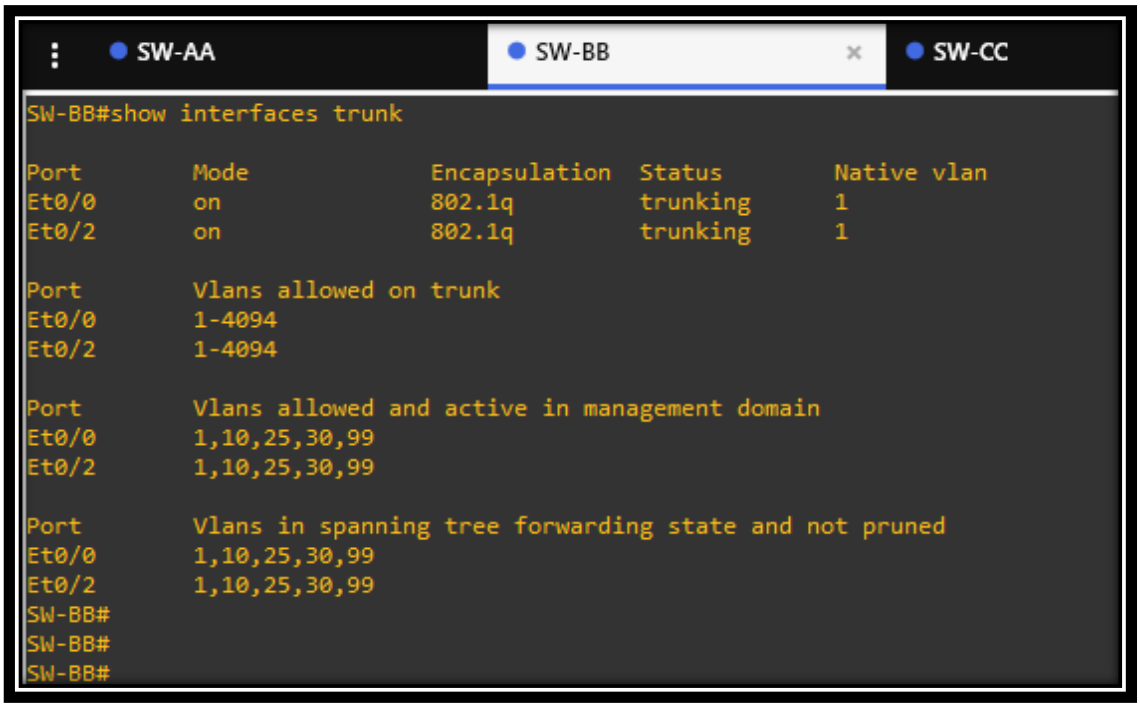


Figura 15. Show Interface Trunck SW-BB



5. Entre SW-AA y SW-BB configure un enlace "trunk" estático utilizando el comando ***switchport mode trunk*** en la interfaz F0/1 de SW-AA

Tabla 11 Configuración Trunck SW-AA y SW-BB

Código de Configuración Aplicado – SW-AA	**Descripción**
SW-AA>enable	Se ingresa a modo privilegiado
SW-AA#configure terminal	Se Ingresa a modo de configuración
SW-AA(config)#interface ethernet 0/1	Se Configura interfaz ethernet
SW-AA(config-if)switchport trunk encapsulation dot1q	Encapsulación de enlace 802.1q
SW-AA(config-if)#switchport mode trunk	Puerto modo trunk
SW-CC(config-if) switchport trunk allowed vlan all	Permite acceso a todas las vlan
SW-AA(config)#exit	Salir del modo de configuración

Configuración TRUNK SW-CC

SW-CC>enable
SW-CC#configure terminal
SW-CC(config)#interface ethernet 0/1
SW-CC(config-if)switchport trunk encapsulation dot1q
SW-CC(config-if)#switchport mode trunk
SW-CC(config-if) switchport trunk allowed vlan all
SW-CC(config-if)#exit

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

Figura 16. Show Interface Trunck SW-AA

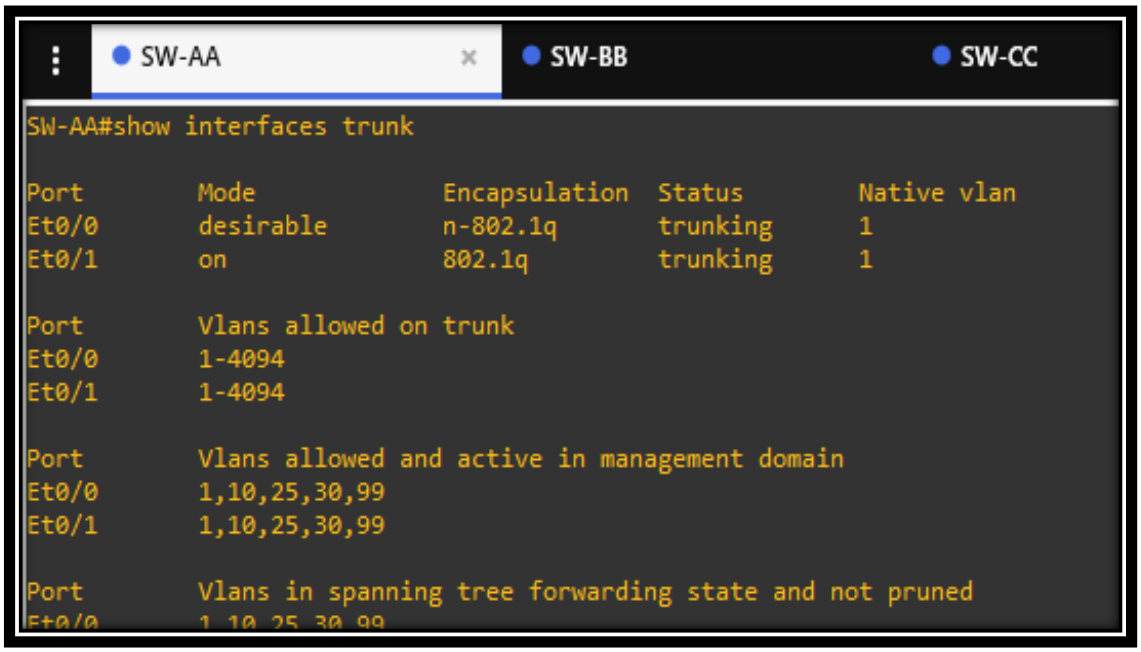
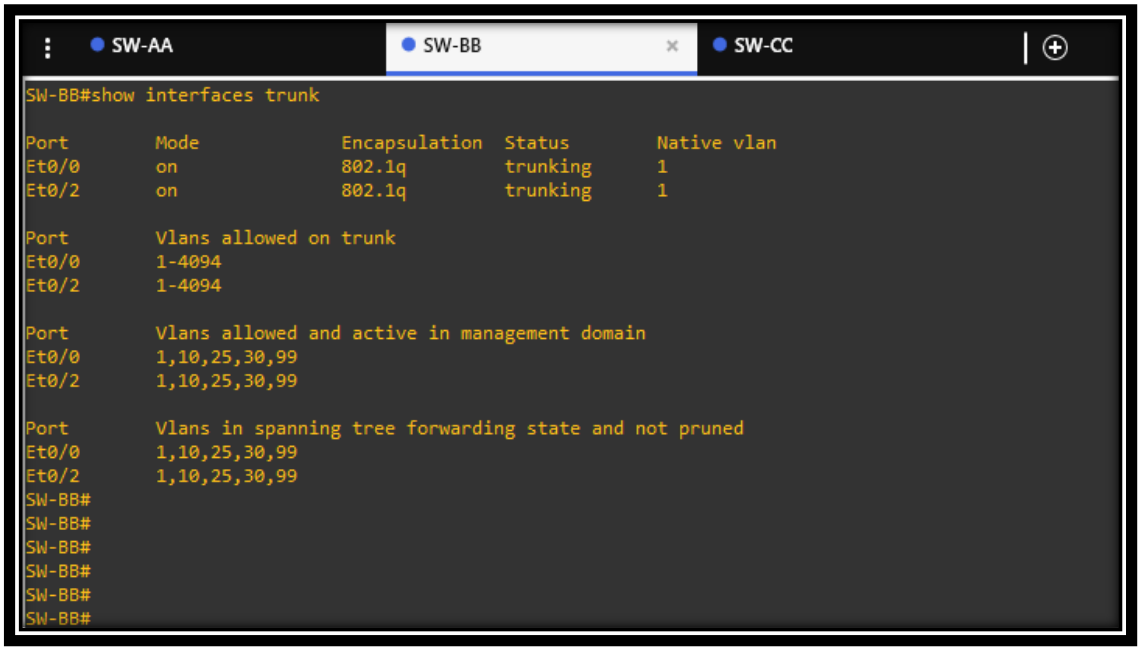


Figura 17. Show Interface Trunck SW-BB



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

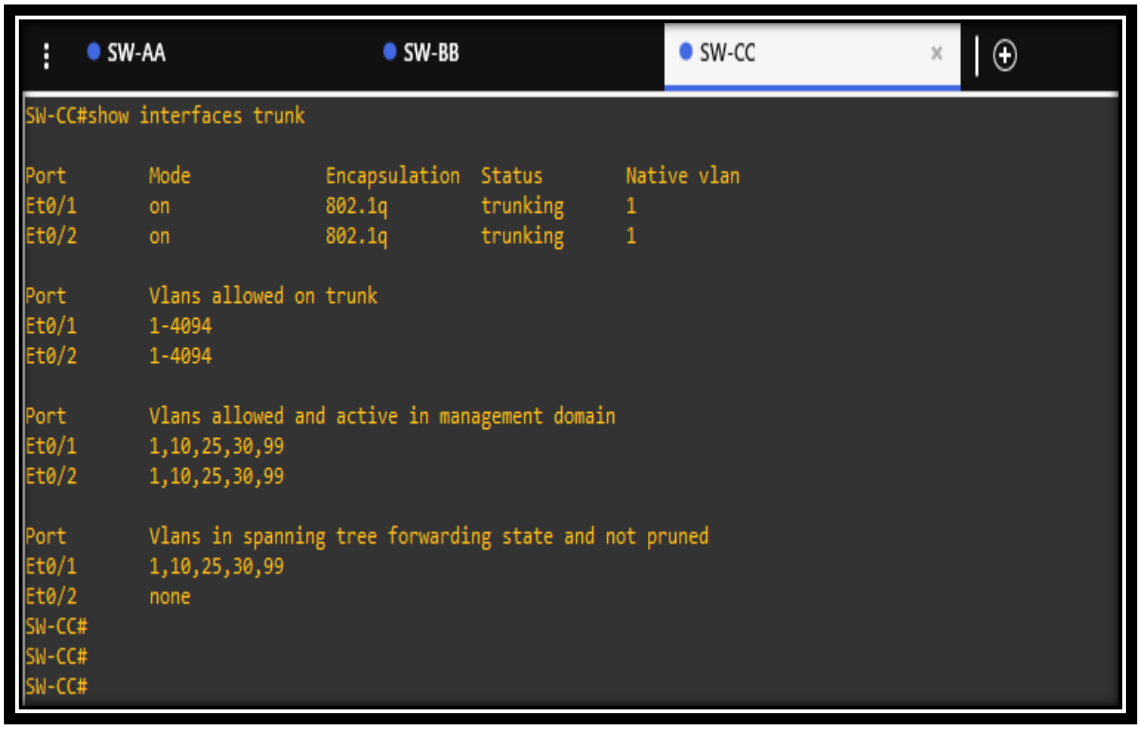
Configuración TRUNK SW-BB

SW-BB>enable
SW-BB#configure terminal
SW-BB(config)#interface ethernet 0/2
SW-BB(config-if)switchport trunk encapsulation dot1q
SW-BB(config-if)#switchport mode trunk
SW-CC(config-if) switchport trunk allowed vlan all
SW-BB(config-if)#exit

Configuración TRUNK SW-CC

SW-CC>enable
SW-CC#configure terminal
SW-CC(config)#interface ethernet 0/2
SW-CC(config-if)switchport trunk encapsulation dot1q
SW-CC(config-if)#switchport mode trunk
SW-CC(config-if) switchport trunk allowed vlan all
SW-CC(config-if)#exit

Figura 18. Show Interface Trunck 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)

Configuración VLAN SW-AA

SW-AA>enable
SW-AA#configure terminal
SW-AA(config-vlan)#vlan 10
SW-AA(config-vlan)#name Compras
SW-AA(config)#exit

Configuración VLAN SW-BB

SW-BB>enable
SW-BB#configure terminal
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

9. Verifique que las VLANs han sido agregadas correctamente

Figura 19. Show Vlan SW-AA

Figura 20. Show Vlan SW-BB

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

Tabla 12 Direccionamiento IP VLAN

Interfaz	VLAN	Direcciones IP de los PCs
Ethernet 1/0	VLAN 10	190.108.10.X/24
Ethernet 1/1	VLAN 25	190.108.20.X/24
Ethernet 1/2	VLAN 30	190.108.30.X/24

11. Configure el puerto ethernet 1/0 en modo de acceso para SW-AA, SW-BB y SW-CC y asígnelo a la VLAN 10.

Configuración VLAN 10 SW-AA

SW-AA>enable
SW-AA#configure terminal
SW-AA(config)#interface ethernet 1/0
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#exit

Configuración VLAN 10 SW-BB

```
SW-BB>enable
SW-BB#configure terminal
SW-BB(config)#interface ethernet 1/0
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport  access vlan 10
SW-BB(config-if)#exit
```

Configuración VLAN 10 SW-CC

```
SW-CC>enable
SW-CC#configure terminal
SW-CC(config)#interface ethernet 1/0
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport  Access vlan 10
SW-CC(config-if)#exit
```

12. Repita el procedimiento para los puertos ethernet 1/1 y ethernet 1/2 en SW-AA, SW-BB y SW-CC. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de

Configuración VLAN 25 y VLAN 30 SW-AA

```
SW-AA>enable
SW-AA#configure terminal
SW-AA(config)#interface ethernet 1/1
SW-AA(config-if)#switchport mode Access vlan 25
SW-AA(config-if)#switchport  access
SW-AA(config-if)#exit
SW-AA#configure terminal
SW-AA(config)#interface ethernet 1/2
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport  access vlan 30
SW-AA(config-if)#exit
```

Configuración VLAN 25 y VLAN 30 SW-BB

```
SW-BB>enable
SW-BB#configure terminal
SW-BB(config)#interface ethernet 1/1
SW-BB(config-if)#switchport mode Access vlan 25
SW-BB(config-if)#switchport  access
```

SW-BB(config-if)#exit
SW-BB#configure terminal
SW-BB(config)#interface ethernet 1/2
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30
SW-BB(config-if)#exit

Configuración VLAN 25 y VLAN 30 SW-CC

SW-CC>enable
SW-CC#configure terminal
SW-CC(config)#interface ethernet 1/1
SW-CC(config-if)#switchport mode Access vlan 25
SW-CC(config-if)#switchport access
SW-CC(config-if)#exit
SW-CC#configure terminal
SW-CC(config)#interface ethernet 1/2
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30
SW-CC(config-if)#exit

Tabla 13 Direccionamiento IP HOST

PC	Interfaz	Direccion IP	Mascara
PC3	VLAN 30	190.108.30.1	255.255.255.0
PC2	VLAN 25	190.108.20.1	255.255.255.0
PC1	VLAN 10	190.108.10.1	255.255.255.0
PC4	VLAN 10	190.108.10.2	255.255.255.0
PC5	VLAN 25	190.108.20.2	255.255.255.0
PC6	VLAN 30	190.108.30.2	255.255.255.0
PC7	VLAN 10	190.108.10.3	255.255.255.0
PC8	VLAN 25	190.108.20.3	255.255.255.0
PC9	VLAN 30	190.108.30.3	255.255.255.0

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.

Tabla 14 Direccionamiento IP VLAN99

Switch	Interfaz	Direccion IP	Mascara
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

Configuración SVI SW-AA

SW-AA>enable
SW-AA#configure terminal
SW-AA(config)#interface vlan 99
SW-AA(config)#ip address 190.108.99.1 255 255 255.0
SW-AA(config)#no shutdown
SW-AA(config)#exit

Configuración SVI SW-BB

SW-BB>enable
SW-BB#configure terminal
SW-BB(config)#interface vlan 99
SW-BB(config)#ip address 190.108.99.2 255 255 255.0
SW-BB(config)#no shutdown
SW-BB(config)#exit

Configuración SVI SW-BB

SW-CC>enable
SW-CC#configure terminal
SW-CC(config)#interface vlan 99
SW-CC(config)#ip address 190.108.99.203 255 255 255.0
SW-CC(config)#no shutdown
SW-CC(config)#exit

E. **Verificar la conexión extrema a extremo**

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

Tabla 15 Resultado Ping Host

Origen	Destino	Comando	Resultado
PC1	PC2	Ping 190.108.20.1	No accesible
PC1	PC3	Ping 190.108.10.1	No accesible
PC1	PC4	Ping 190.108.10.2	Accesible
PC1	PC5	Ping 190.108.20.2	No accesible
PC1	PC6	Ping 190.108.30.2	No Accesible
PC1	PC7	Ping 190.108.10.3	Accesible
PC1	PC8	Ping 190.108.20.3	No accesible
PC1	PC9	Ping 190.108.30.3	No Accesible
Conclusión:Al validar con la ejecución del ping desde cada uno de los PC entre sí, se observa que únicamente son accesibles los miembros de la misma Vlan (10, 25, 30), ya que no se planteó para este escenario configuración de enrutamiento entre vlans.			

Figura 21. Ping PC1 to (PC4 and PC7)

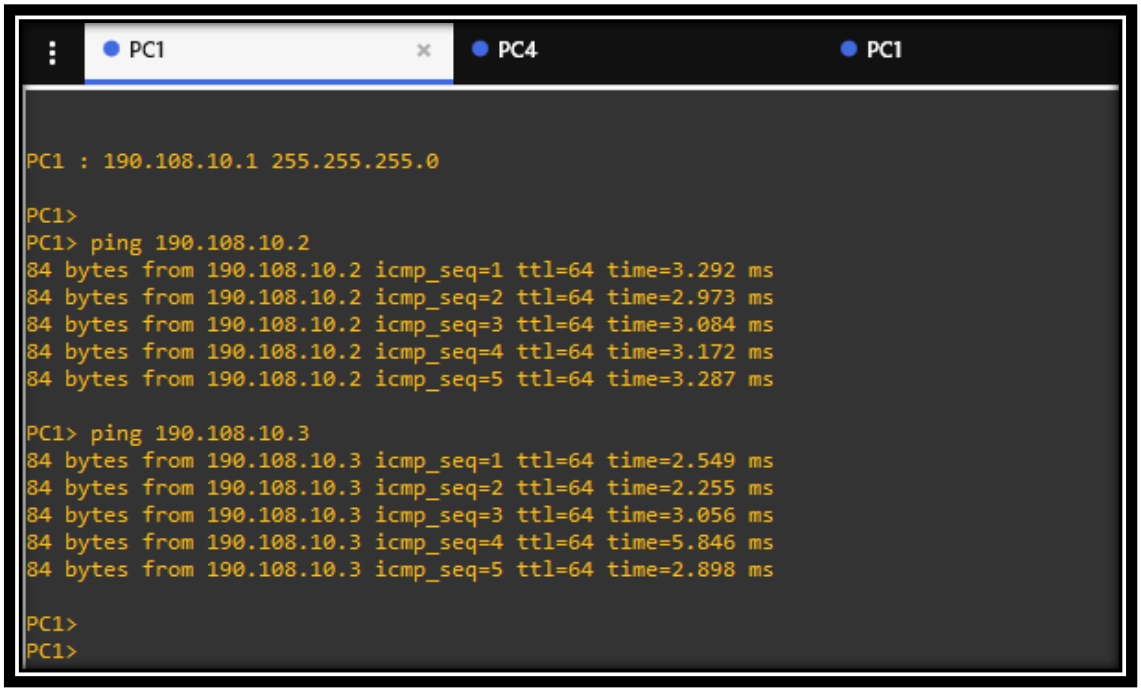
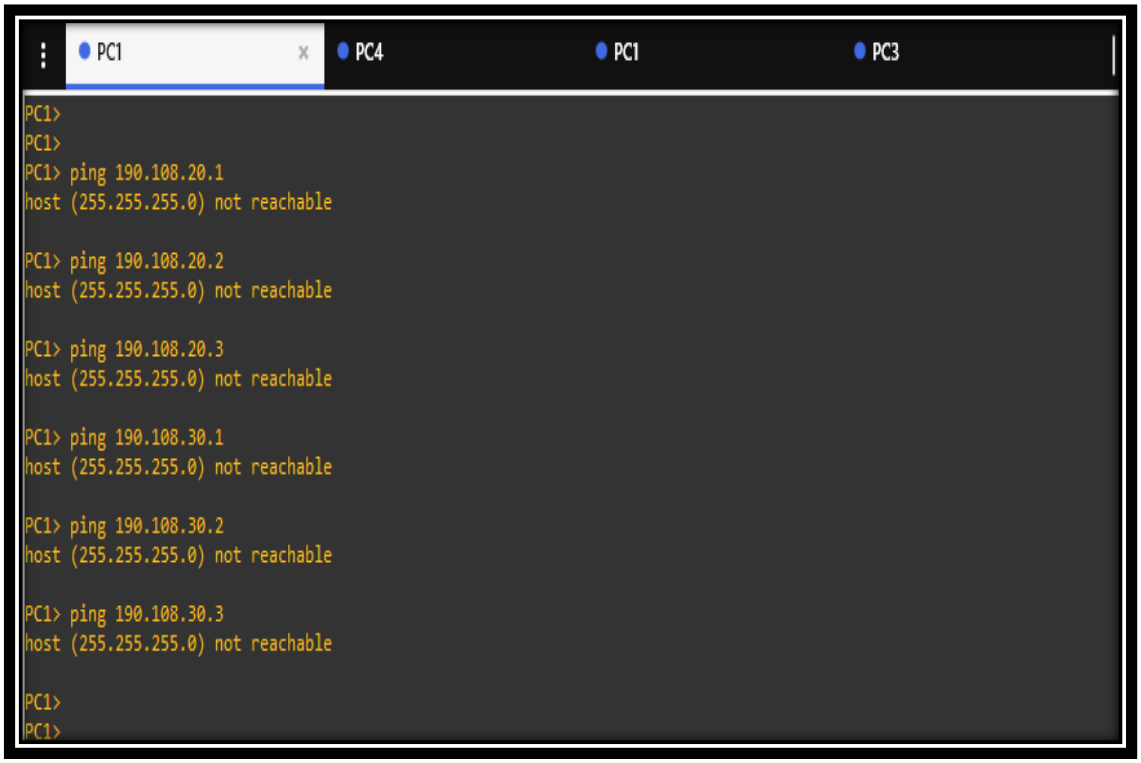


Figura 22. Ping PC1 to (PC2,PC5,PC6,PC8, and PC9)



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

Tabla 16 Resultado Ping SWITCH

Origen	Destino	Comando	Resultado
SW-AA	SW-BB	Ping 190.108.99.2	Accesible
SW-AA	SW-CC	Ping 190.108.99.3	Accesible
SW-BB	SW-AA	Ping 190.108.99.1	Accesible
SW-BB	SW-CC	Ping 190.108.99.3	Accesible
SW-CC	SW-AA	Ping 190.108.99.1	Accesible
SW-CC	SW-BB	Ping 190.108.99.2	Accesible
Conclusión:Se evidencia que al ejecutar ping desde cada uno de los switches entre sí, al ser miembros de la misma Vlan 99 todos son accesibles			

Figura 23. Ping SW-AA to SW-BB

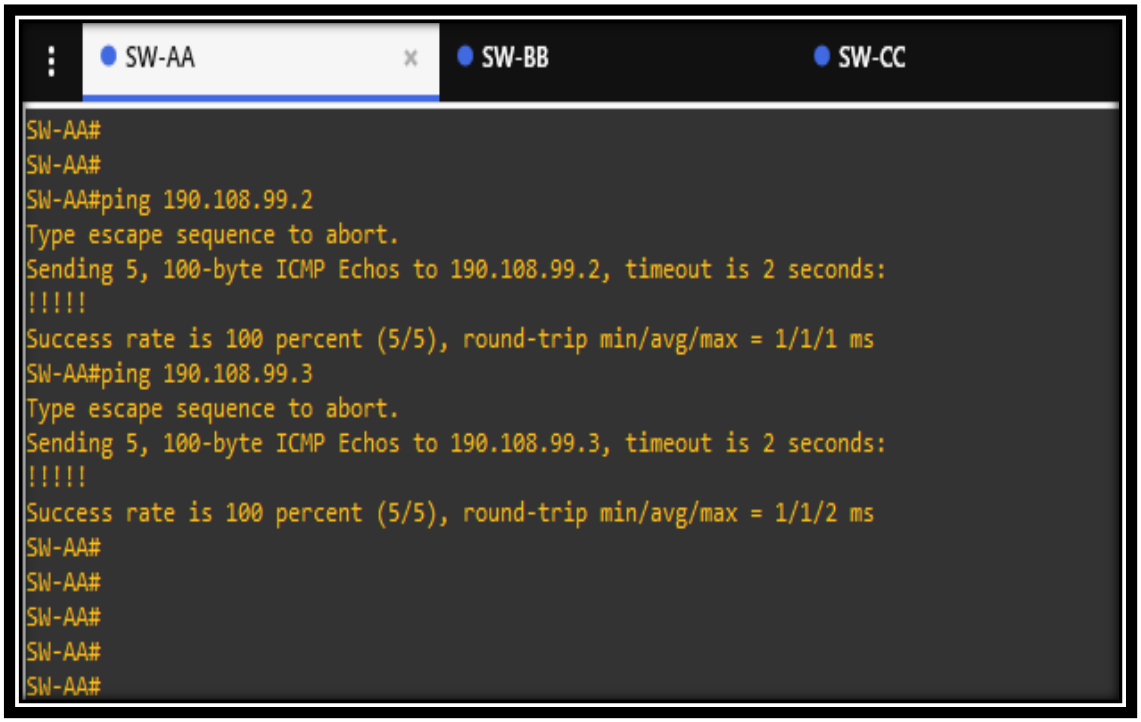


Figura 24. Ping SW-BB to SW-AA

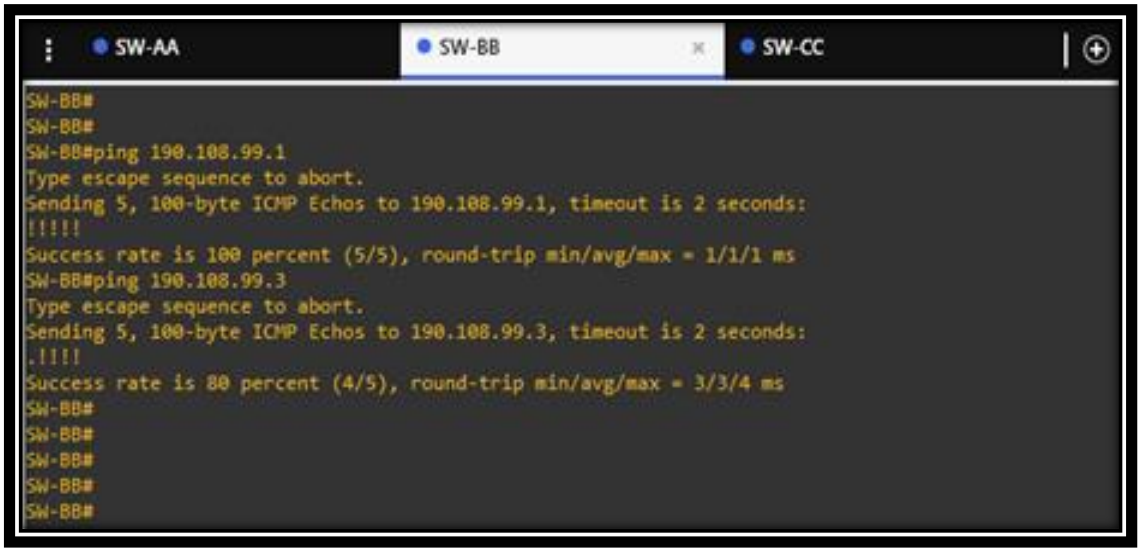
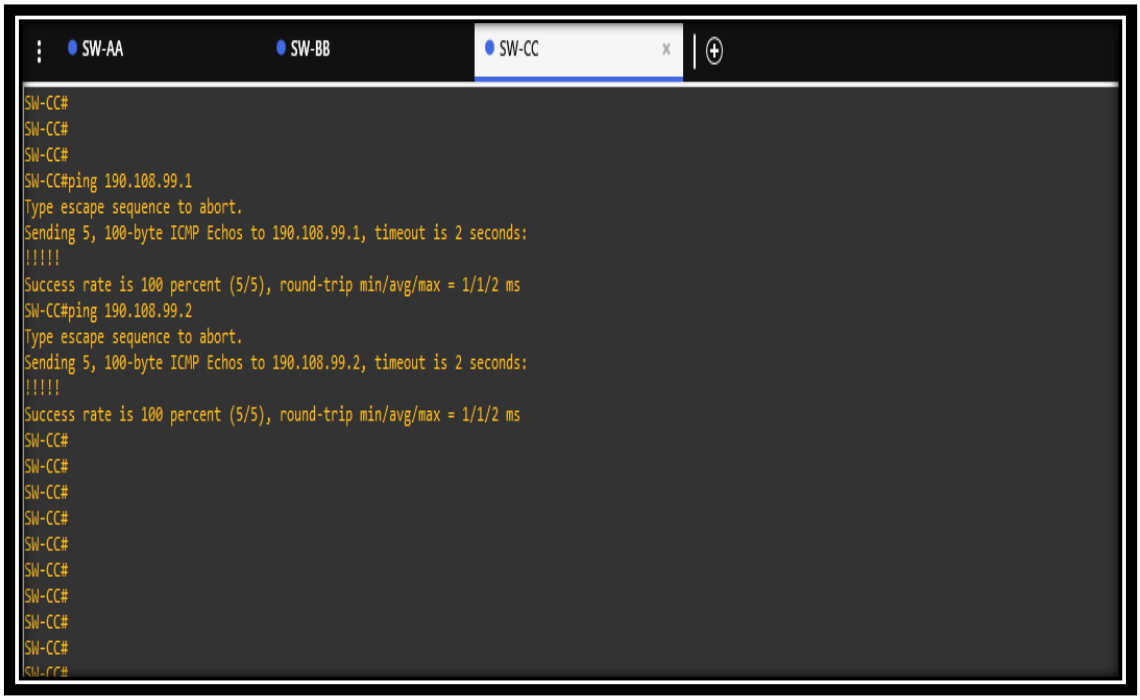


Figura 25. Ping SW-CC to SW-AA



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

Tabla 17 Resultado Ping entre SWITCH-AA y Host

Origen	Destino	Comando	Resultado
SW-AA	PC1	Ping 190.108.10.1	No accesible
SW-AA	PC2	Ping 190.108.20.1	No accesible
SW-AA	PC3	Ping 190.108.30.1	No accesible
SW-AA	PC4	Ping 190.108.10.2	No accesible
SW-AA	PC5	Ping 190.108.20.2	No accesible
SW-AA	PC6	Ping 190.108.30.2	No accesible
SW-AA	PC7	Ping 190.108.10.3	No accesible
SW-AA	PC8	Ping 190.108.20.3	No accesible
SW-AA	PC9	Ping 190.108.30.3	No accesible
Conclusion:Se evidencia que al ejecutar ping desde cada uno de los Switches hacia los PC no se evidencia que sean accesibles ya que no son miembros de la misma			

vlan (10, 25, 30), debido a que no se planteó para este escenario configuración de enrutamiento entre vlans.

Figura 26. Ping SW-AA to PC1

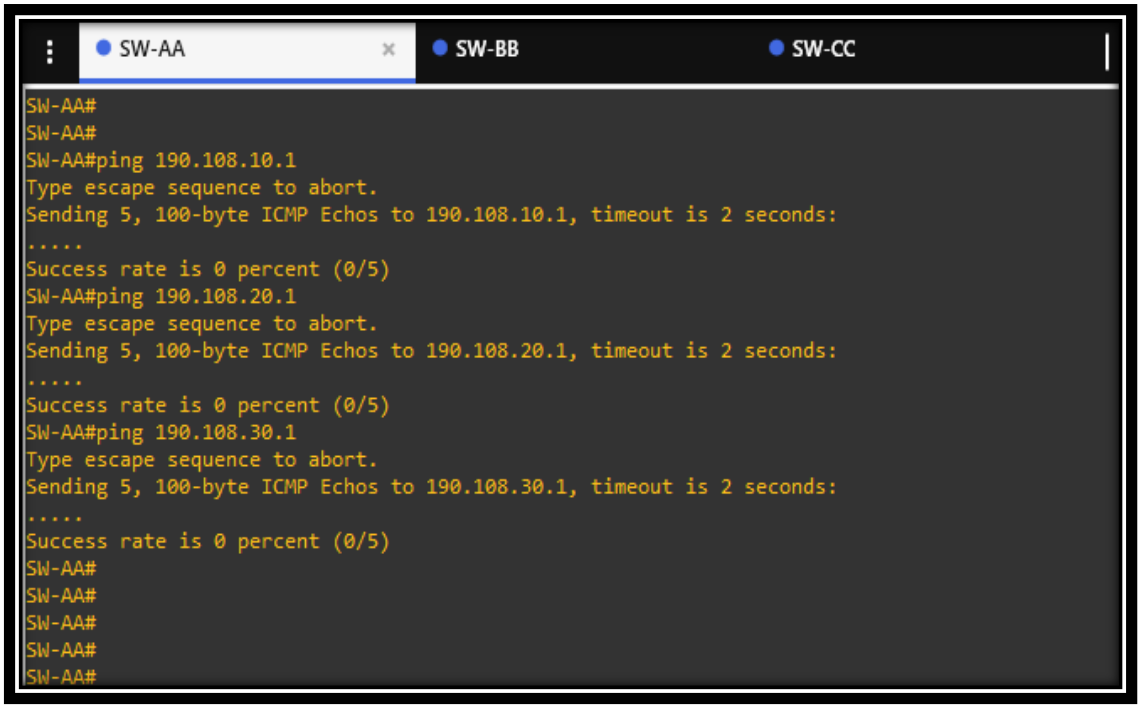


Tabla 18 Resultado Ping entre SWITCH-BB y Host

Origen	Destino	Comando	Resultado
SW-BB	PC1	Ping 190.108.10.1	No accesible
SW-BB	PC2	Ping 190.108.20.1	No accesible
SW-BB	PC3	Ping 190.108.30.1	No accesible
SW-BB	PC4	Ping 190.108.10.2	No accesible
SW-BB	PC5	Ping 190.108.20.2	No accesible
SW-BB	PC6	Ping 190.108.30.2	No accesible
SW-BB	PC7	Ping 190.108.10.3	No accesible
SW-BB	PC8	Ping 190.108.20.3	No accesible
SW-BB	PC9	Ping 190.108.30.3	No accesible

Conclusion:Se evidencia que al ejecutar ping desde cada uno de los Switches hacia los PC no se evidencia que sean accesibles ya que no son miembros de la misma vlan (10, 25, 30), debido a que no se planteó para este escenario configuración de enrutamiento entre vlans.

Tabla 19 Resultado Ping entre SWITCH-CC y Host

Origen	Destino	Comando	Resultado
SW-CC	PC1	Ping 190.108.10.1	No accesible
SW-CC	PC2	Ping 190.108.20.1	No accesible
SW-CC	PC3	Ping 190.108.30.1	No accesible
SW-CC	PC4	Ping 190.108.10.2	No accesible
SW-CC	PC5	Ping 190.108.20.2	No accesible
SW-CC	PC6	Ping 190.108.30.2	No accesible
SW-CC	PC7	Ping 190.108.10.3	No accesible
SW-CC	PC8	Ping 190.108.20.3	No accesible
SW-CC	PC9	Ping 190.108.30.3	No accesible
Conclusiones: evidencia que al ejecutar ping desde cada uno de los Switches hacia los PC no se evidencia que sean accesibles ya que no son miembros de la misma vlan (10, 25, 30), debido a que no se planteó para este escenario configuración de enrutamiento entre vlans.			

CONCLUSIONES

Se establecieron los niveles de seguridad básicos a través de la definición de criterios y políticas de seguridad aplicados en dos escenarios de red, bajo el uso de estrategias hardware y software, protegiendo la integridad de la información frente a cualquier tipo de ataque que se pueda presentar; en especial en soluciones de red que involucren el uso de aplicaciones cliente-servidor.

Los conocimientos necesarios para el diseño de redes escalables se fortalecieron mediante el uso del modelo jerárquico de tres niveles, la optimización en el rendimiento de la red e incorporación adecuada de tecnologías y protocolos de conmutación mejorados tales como: VLAN, protocolo de enlace troncal de VLAN (VTP), protocolo rápido de árbol de expansión (Rapid Spanning Tree Protocol - RSTP), Protocolo de árbol de expansión por VLAN (Spanning Tree per VLAN - PVSTP) y encapsulamiento por 802.1q.

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

BIBLIOGRAFÍA

Donohue, D. (2017). CISCO Press (Ed). CCNP Quick Reference. Recuperado de https://1drv.ms/b/s!AgIGg5JUgUBthFt77ehzL5qp0OKD

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). Campus Network Security. 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). First Hop Redundancy Protocols. 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). First Hop Redundancy Protocols. 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). High Availability. 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). 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). Network Design Fundamentals. 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). Network Management. 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

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-NT1IlnWR0hoMxgBNv1CJ

Hucaby, D. (2015). CISCO Press (Ed). CCNP Routing and Switching SWITCH 300-115 Official Cert Guide. Recuperado de https://1drv.ms/b/s!AgIGg5JUgUBthF16RWCSsCZnfDo2

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). 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). 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