DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRACTICAS CCNP

MILLER ORLANDO LINARES CASTELLANOS

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

MILLER ORLANDO LNARES CASTELLANOS

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

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

BOGOTA D.C, 22 de mayo de 2020

AGRADECIMIENTOS

En primer lugar, mis agradecimientos van dirigidos a Dios, por permitirme atravesar los obstáculos que se me han presentado para estar victorioso culminando mis estudios y convertirme en Ingeniero, seguidos a mi madre y a mi esposa, por su apoyo, comprensión y fortaleza en todo este proceso.

A mi hija Evelyn, por ser mi motor, y la que me llena de energía para no desfallecer,

A mi papá por su amor, su apoyo, sus consejos, y su humildad, por compartir conmigo los aciertos y fracasos, por que se que desde el cielo esta muy orgulloso de que hoy su hijo culmine su carrera.

A y mis familiares por su apoyo en todo este proceso.

CONTENIDO

Contenido

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

GLOSARIO

CCNP:(Cisco Certified Network Professional) es el nivel intermedio de certificación de la compañía. Para obtener esta certificación, se han de superar varios exámenes, clasificados según la empresa en 3 módulos. Esta certificación, es la intermedia de las certificaciones generales de Cisco, no está tan valorada como el CCIE, pero sí, mucho más que el CCNA.

GNS3: Es un simulador gráfico de red,el cual permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos. Lo diferencia del packet tracer, que este software no cuenta con imágenes incluidas , en este caso se deben descargar las imágenes desde la página oficial de cisco, este software tiene varias ventajas dentro de ellas encontramos que hace la simulación real entre nuestro pc y una máquina virtual que tenga configurada, otra ventaja es que se puedan simular redes gama alta.GNS3 está estrechamente vinculada con: Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarios e imágenes IOS de Cisco Systems.

Networking: Es una red de computadoras, 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

Protocolos de red: Conjunto de normas standard que especifican el método para enviar y recibir datos entre varios ordenadores. Es una convención que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales.

VLAN: Es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local.

RESUMEN

El desarrollo del presente trabajo corresponde a la evaluación denominada “Prueba de habilidades prácticas”, el cual forma parte de las actividades evaluativas del Diplomado de Profundización de la academia CISCO llamado CCNP Dirigido a: Técnicos, Tecnólogos y Profesionales de las áreas de electrónica, telecomunicaciones y sistemas.
El propósito de este es identificar el nivel de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado poniendo a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Se refuerza el manejo de plataformas en este caso GSN3 para la solución de escenarios que incluyen temas avanzados en el diseño, configuración, Conmutación, Enrutamiento y operación de redes LAN y WAN.

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

ABSTRACT

The development of this text belongs to the evaluation called “Practical skills test", which is part of the evaluative activities of the Deepening Diploma of the CISCO academy called CCNP oriented to: Technicians, Technologists and Professionals in the areas of electronics, telecommunications and systems fields.
The purpose of this is to identify the level of development of competencies and skills that were acquired throughout the course, testing the levels of understanding and solution of problems related to various aspects of Networking.

The handling of platforms is reinforced in this case GSN3 for the solution of scenarios that includes advanced topics in the design, configuration, Switching, Routing and operation of LAN and WAN networks.

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

INTRODUCCIÓN

En este documento se encuentra el desarrollo de la Prueba de Habilidades Practicas, certificación CCNP (Cisco Certified Network Professional) el cual permite aumentar la capacidad de planificar, implementar, verificar y solucionar problemas relacionados con diversos aspectos de Networking,en redes LAN y WAN.

Para cumplir con los propósitos mencionados, se desarrollan 2 escenarios, En el módulo ROUTE se abordarán conceptos principales como protocolos de enrutamiento EIGRP, OSPF, BGP, redistribución de rutas, Dynamic Multi VPN, VRF Lite y protocolos en IPv6, 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. En el módulo SWITCH se abordarán conceptos principales como operaciones y puertos de swtiches, VLANs y troncales (VLAN Trunking Protocol y Dynamic Trunking Protocol) y configuración de usuarios .

se realiza evidencia de todas las configuraciones anteriormente mencionadas demostrando el paso a paso de cada una y el proceso de verificación de conectividad por medio de comandos ping, show ip route, show vtp status, show interfaces trunk, entre otros.

DESARROLLO

1. ESCENARIO 1

Figura 1. Escenario 1

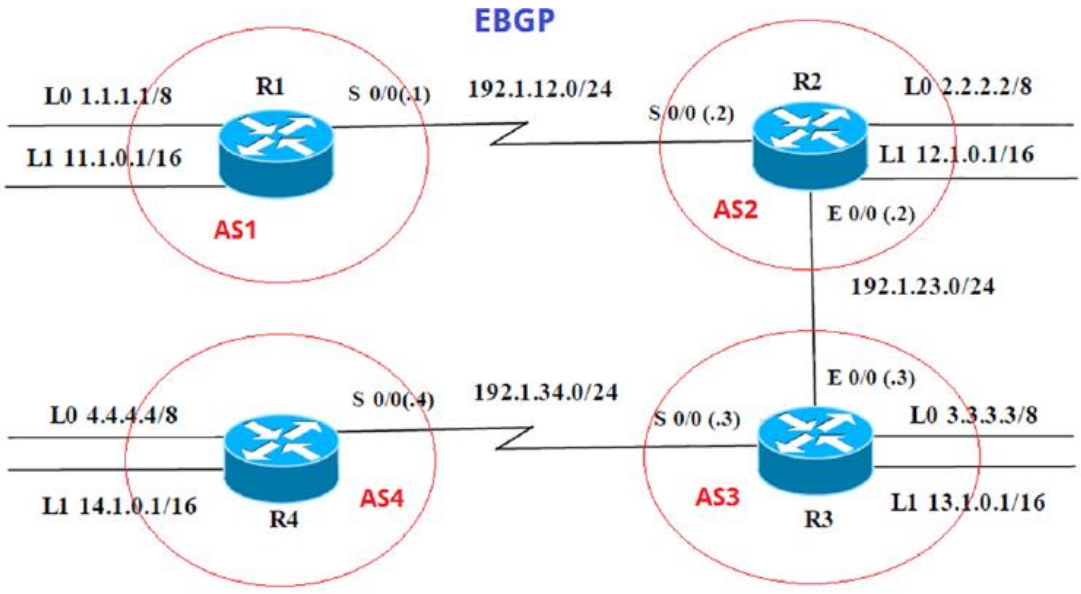
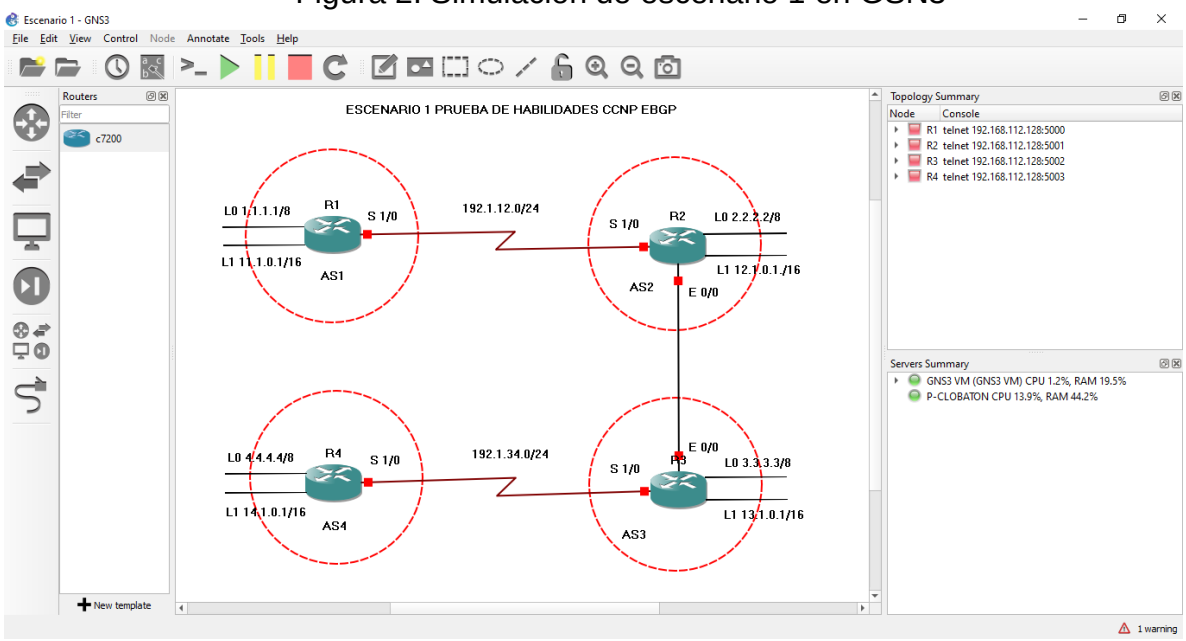


Figura 2. Simulación de escenario 1 en GSN3



1.1. Configuración Inicial Routers

Aplique las configuraciones iniciales y los protocolos de enrutamiento para los routers R1, R2, R3, R4 y R5 según el diagrama. No asigne passwords en los routers. Configurar las interfaces con las direcciones que se muestran en la topología de red.

Se procede a configurar cada uno de los enrutadores. 1, 2, 3, 4,
Se asignan nombre y protocolos de comunicación mediante EBGP que fueron asignados.

Se adjunta código y pantallazos con veracidad del código.

Router R1

```
Router>
Router>enable                          Ingresa a modo privilegiado
Router#configure terminal              Ingresa a modo de configuración
Router(config)#hostname R1             Asigna nombre al Router
R1(config)#no ip domain-lookup         Desactiva la traducción DNS
R1(config)#line console 0              Ingresa a parámetros de consola
R1(config-line)#logging synchronous    Evita el mensaje no solicitado
R1(config-line)#exec-timeout 0 0       Sin límite de tiempo en inactividad
R1(config-line)#exit                   Salir del modo de configuración
R1(config)#
```

Router R2

```
Router>
Router>enable                          Ingresa a modo privilegiado
Router#configure terminal              Ingresa a modo de configuración
Router(config)#hostname R2             Asigna nombre al Router
R2(config)#no ip domain-lookup         Desactiva la traducción DNS
R2(config)#line console 0              Ingresa a parámetros de consola
R2(config-line)#logging synchronous    Evita el mensaje no solicitado
R2(config-line)#exec-timeout 0 0       Sin límite de tiempo en inactividad
R2(config-line)#exit                   Salir del modo de configuración
R2(config)#
```

Router R3

```
Router>
Router>enable                          Ingresa a modo privilegiado
Router#configure terminal              Ingresa a modo de configuración
Router(config)#hostname R3             Asigna nombre al Router
R3(config)#no ip domain-lookup         Desactiva la traducción DNS
R3(config)#line console 0              Ingresa a parámetros de consola
R3(config-line)#logging synchronous    Evita el mensaje no solicitado
R3(config-line)#exec-timeout 0 0       Sin límite de tiempo en inactividad
R3(config-line)#exit                   Salir del modo de configuración
R3(config)#
```

Router R4

```
Router>
Router>enable                          Ingresa a modo privilegiado
Router#configure terminal              Ingresa a modo de configuración
Router(config)#hostname R4             Asigna nombre al Router
R4(config)#no ip domain-lookup         Desactiva la traducción DNS
R4(config)#line console 0              Ingresa a parámetros de consola
R4(config-line)#logging synchronous    Evita el mensaje no solicitado
R4(config-line)#exec-timeout 0 0       Sin límite de tiempo en inactividad
R4(config-line)#exit                   Salir del modo de configuración
R4(config)#
```

1.2. Direccionamiento IP

Agregar el direccionamiento IP a los Routers basados en las siguientes tablas:

Tabla 1 Direccionamiento IP R1

Interfaz	Dirección IP	Mascara
Loopback 0	1.1.1.1	8
Loopback 1	11.1.0.1	16
Serial 1/0	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 1/0	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 1/0	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 1/0	192.1.34.4	24

Router R1

```
R1>
R1>enable                                   Ingresa a modo privilegiado
R1#configure terminal                       Ingresa a modo de configuración
R1(config)#interface serial 1/0             Configure interfaz serial
R1(config-if)#description R1 to R2          Breve descripción de la interfaz
R1(config-if)#clock rate 64000              Sincronismo conexión seria DCE
R1(config-if)#bandwidth 64                  Indica la velocidad de la interfaz
R1(config-if)#ip address 192.1.12.1 255.255.255.0   Asignación IPV4
R1(config-if)#no shutdown                   Activa la interfaz
R1(config-if)#exit                          Salir del modo de configuración

R1>
R1>enable                                   Ingresa a modo privilegiado
R1#configure terminal                       Ingresa a modo de configuración
R1(config)#interface loopback 0             Configure 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 loopback 1             Configure 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
```

Router R2

```
R2>
R2>enable                                   Ingresa a modo privilegiado
R2#configure terminal                       Ingresa a modo de configuración
R2(config)#interface serial 1/0             Configure interfaz serial
R2(config-if)#description R2 to R1          Breve descripción de la interfaz
R2(config-if)#bandwidth 64                  Indica la velocidad de la interfaz
R2(config-if)#ip address 192.1.12.2 255.255.255.0    Asignación IPV4
```

R2(config-if)#no shutdown Activa la interfaz
R2(config-if)#exit Salir del modo de configuración

R2>
R2>enable Ingresa a modo privilegiado
R2#configure terminal Ingresa a modo de configuración
R2(config)# interface fastEthernet 0/0 Configure interfaz fastEthernet
R2(config-if)#description R2 to R3 Breve descripción de la interfaz
R2(config-if)#bandwidth 64 Indica la velocidad de la interfaz
R2(config-if)#ip address 192.1.23.2 255.255.255.0 Asignación IPV4
R2(config-if)#no shutdown Activa la interfaz
R2(config-if)#exit Salir del modo de configuración

R2>
R2>enable Ingresa a modo privilegiado
R2#configure terminal Ingresa a modo de configuración
R2(config)#interface loopback 0 Configure interfaz loopback 0
R2(config-if)#ip address 2.2.2.2 255.0.0.0 Asignación IPV4
R2(config-if)#exit Salir del modo de configuración
R2(config)#interface loopback 1 Configure interfaz loopback 1
R2(config-if)#ip address 12.1.0.1 255.255.0.0 Asignación IPV4
R2(config-if)#exit Salir del modo de configuración

Router R3

R3>
R3>enable Ingresa a modo privilegiado
R3#configure terminal Ingresa a modo de configuración
R3(config)#interface serial 1/0 Configure interfaz serial
R3(config-if)#description R3 to R4 Breve descripción de la interfaz
R3(config-if)#clock rate 64000 Sincronismo conexión seria DCE
R3(config-if)#bandwidth 64 Indica la velocidad de la interfaz
R3(config-if)#ip address 192.1.34.3 255.255.255.0 Asignación IPV4
R3(config-if)#no shutdown Activa la interfaz
R3(config-if)#exit Salir del modo de configuración
R3>
R3>enable Ingresa a modo privilegiado
R3#configure terminal Ingresa a modo de configuración
R3(config)# interface fastEthernet 0/0 Configure interfaz fastEthernet
R3(config-if)#description R3 to R2 Breve descripción de la interfaz
R3(config-if)#bandwidth 64 Indica la velocidad de la interfaz
R3(config-if)#ip address 192.1.23.3 255.255.255.0 Asignación IPV4
R3(config-if)#no shutdown Activa la interfaz
R3(config-if)#exit Salir del modo de configuración

R3>
R3>enable Ingresa a modo privilegiado
R3#configure terminal Ingresa a modo de configuración
R3(config)#interface loopback 0 Configure interfaz loopback 0
R3(config-if)#ip address 3.3.3.3 255.0.0.0 Asignación IPV4
R3(config-if)#exit Salir del modo de configuración
R3(config)#interface loopback 1 Configure interfaz loopback 1
R3(config-if)#ip address 13.1.0.1 255.255.0.0 Asignación IPV4
R3(config-if)#exit Salir del modo de configuración

Router R4

R4>
R4>enable Ingresa a modo privilegiado
R4#configure terminal Ingresa a modo de configuración
R4(config)#interface serial 1/0 Configure interfaz serial
R4(config-if)#description R4 to R3 Breve descripción de la interfaz
R4(config-if)#clock rate 64000 Sincronismo conexión seria DCE
R4(config-if)#bandwidth 64 Indica la velocidad de la interfaz
R4(config-if)#ip address 192.1.34.4 255.255.255.0 Asignación IPV4
R4(config-if)#no shutdown Activa la interfaz
R4(config-if)#exit Salir del modo de configuración

R4>
R4>enable Ingresa a modo privilegiado
R4#configure terminal Ingresa a modo de configuración
R4(config)#interface loopback 0 Configure interfaz loopback 0
R4(config-if)#ip address 4.4.4.4 255.0.0.0 Asignación IPV4
R4(config-if)#exit Salir del modo de configuración
R4(config)#interface loopback 1 Configure interfaz loopback 1
R4(config-if)#ip address 14.1.0.1 255.255.0.0 Asignación IPV4
R4(config-if)#exit Salir del modo de configuración

1.3. Configuración de relaciones EBGP

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.

Router R1

R1>
R1>enable Ingresa a modo privilegiado
R1#configure terminal Ingresa a modo de configuración
R1(config)#router bgp 1 Configurar el protocol 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

Router R2

R2>
R2>enable Ingresa a modo privilegiado
R2#configure terminal Ingresa a modo de configuración
R2(config)#router bgp 2 Configurar el protocol BGP
R2(config-router)#no synchronization Ignora la sincronización
R2(config-router)#bgp router-id 33.33.33.33 Asigna ID al router
R2(config-router)#neighbor 192.1.12.1 remote-as 1 Detección de redes
R2(config-router)#network 2.0.0.0 mask 255.0.0.0 Anunciar red
R2(config-router)#network 12.1.0.0 mask 255.255.0.0 Anunciar red
R2(config-router)#exit Salir del modo de configuración

Figura 1. Show ip Router 1

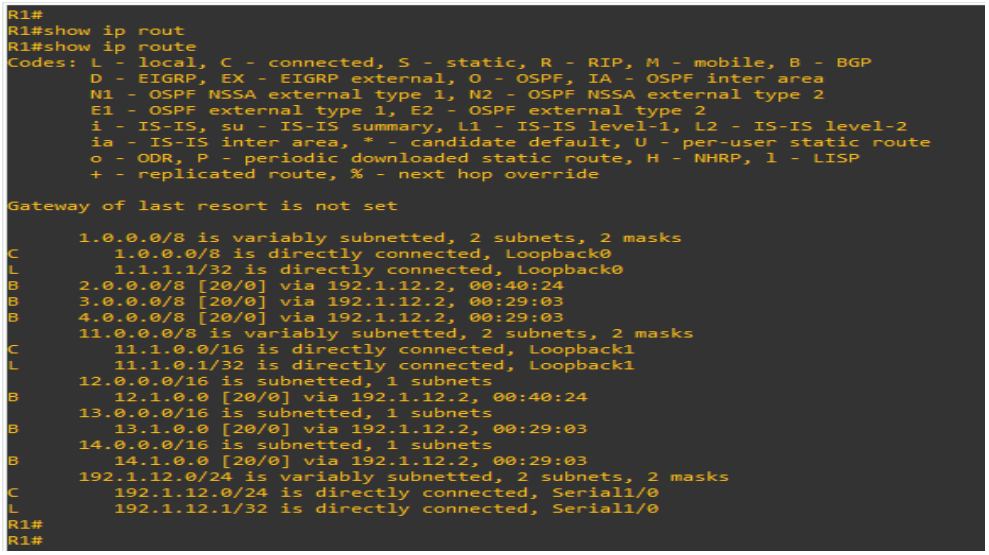
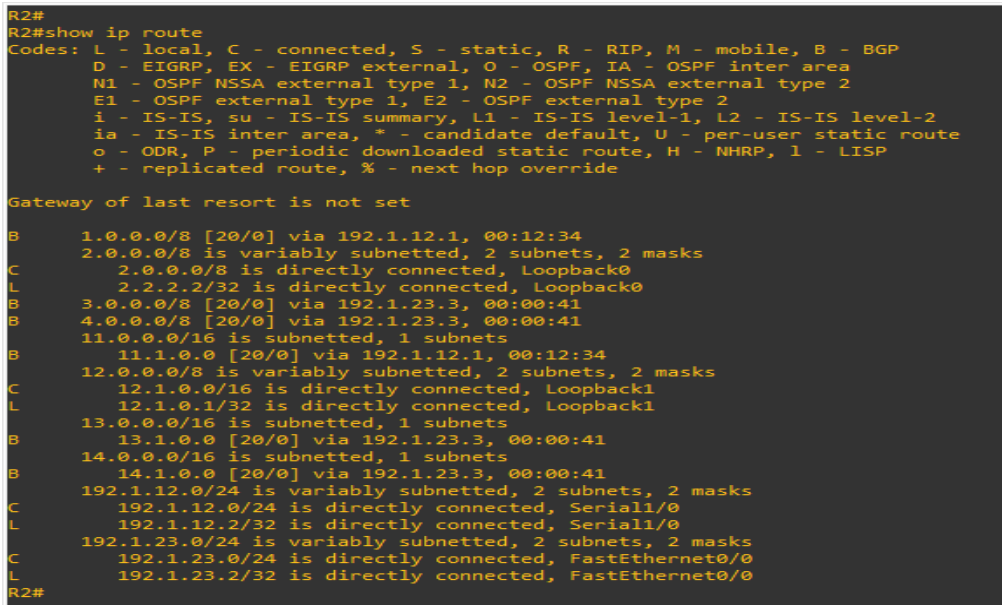


Figura 4. Show ip Router 2



```
R2#
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B      1.0.0.0/8 [20/0] via 192.1.12.1, 00:12:34
       2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C         2.0.0.0/8 is directly connected, Loopback0
L         2.2.2.2/32 is directly connected, Loopback0
B      3.0.0.0/8 [20/0] via 192.1.23.3, 00:00:41
B      4.0.0.0/8 [20/0] via 192.1.23.3, 00:00:41
       11.0.0.0/16 is subnetted, 1 subnets
B         11.1.0.0 [20/0] via 192.1.12.1, 00:12:34
       12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C         12.1.0.0/16 is directly connected, Loopback1
L         12.1.0.1/32 is directly connected, Loopback1
       13.0.0.0/16 is subnetted, 1 subnets
B         13.1.0.0 [20/0] via 192.1.23.3, 00:00:41
       14.0.0.0/16 is subnetted, 1 subnets
B         14.1.0.0 [20/0] via 192.1.23.3, 00:00:41
       192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.1.12.0/24 is directly connected, Serial1/0
L         192.1.12.2/32 is directly connected, Serial1/0
       192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.1.23.0/24 is directly connected, FastEthernet0/0
L         192.1.23.2/32 is directly connected, FastEthernet0/0
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.

Router R2

R2>
R2>enable Ingresa a modo privilegiado
R2#configure terminal Ingresa a modo de configuración
R2(config)#router bgp 2 Configurar el protocol BGP
R2(config-router)#no synchronization Ignora la sincronización
R2(config-router)#bgp router-id 33.33.33.33 Asigna ID al router
R2(config-router)#neighbor 192.1.23.3 remote-as 3 Detección de redes
R2(config-router)#network 2.0.0.0 mask 255.0.0.0 Anunciar red
R2(config-router)#network 12.1.0.0 mask 255.255.0.0 Anunciar red
R2(config-router)#exit Salir del modo de configuración

Router R3

R3>
R3>enable Ingresa a modo privilegiado
R3#configure terminal Ingresa a modo de configuración
R3(config)#router bgp 3 Configurar el protocol BGP
R3(config-router)#no synchronization Ignora la sincronización
R3(config-router)#bgp router-id 44.44.44.44 Asigna ID al router
R3(config-router)#neighbor 192.1.23.2 remote-as 2 Detección de redes
R3(config-router)#network 3.0.0.0 mask 255.0.0.0 Anunciar red
R3(config-router)#network 13.1.0.0 mask 255.255.0.0 Anunciar red
R3(config-router)#exit Salir del modo de configuración

Figura 5. Show ip Router 2

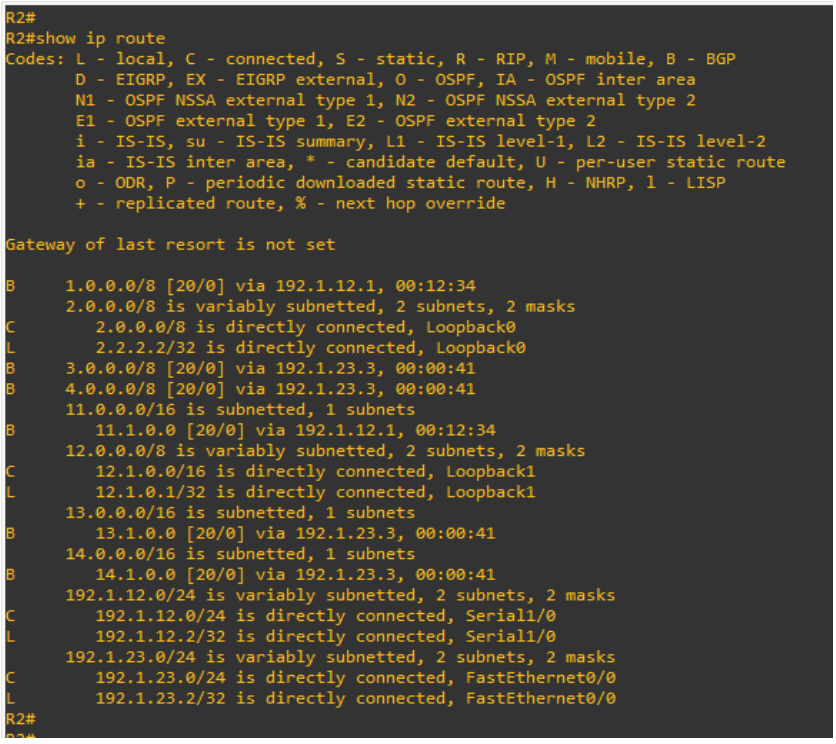
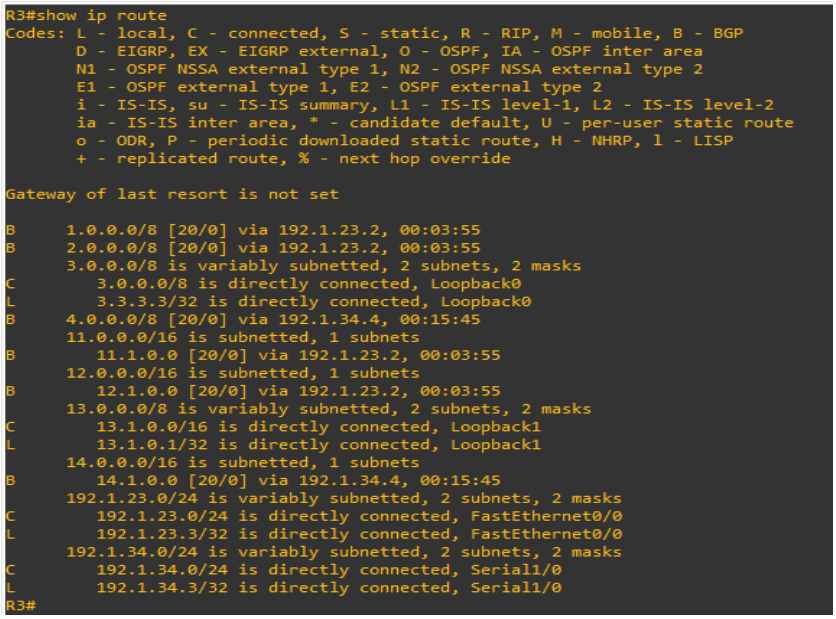


Figura 6. Show ip Router 3



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.

Router R3

R3>
R3>enable Ingresa a modo privilegiado
R3#configure terminal Ingresa a modo de configuración
R3(config)#router bgp 3 Configurar el protocol BGP
R3(config-router)#no synchronization Ignora la sincronización
R3(config-router)#bgp router-id 44.44.44.44 Asigna ID al router
R3(config-router)#neighbor 192.1.34.4 remote-as 4 Detección de redes
R3(config-router)#network 3.0.0.0 mask 255.0.0.0 Anunciar red
R3(config-router)#network 13.1.0.0 mask 255.255.0.0 Anunciar red
R3(config-router)#exit Salir del modo de configuración

Router R4

```
R4>
R4>enable                                   Ingresa a modo privilegiado
R4#configure terminal                       Ingresa a modo de configuración
R4(config)#router bgp 4                     Configurar el protocol BGP
R4(config-router)#no synchronization        Ignora la sincronización
R4(config-router)#bgp router-id 66.66.66.66 Asigna ID al router
R4(config-router)#neighbor 192.1.34.3 remote-as 3 Detección de redes
R4(config-router)#network 4.0.0.0 mask 255.0.0.0  Anunciar red
R4(config-router)#network 14.1.0.0 mask 255.255.0.0  Anunciar red
R4(config-router)#exit                      Salir del modo de configuración
```

Cree rutas estáticas para alcanzar la Loopback 0 del otro router.

Router R3

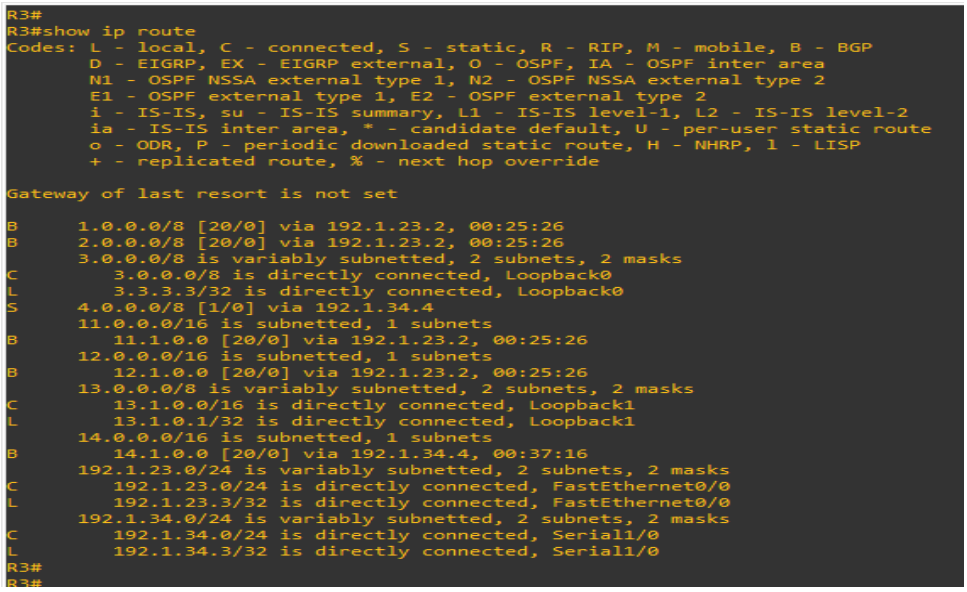
```
R3>
R3>enable                                   Ingresa a modo privilegiado
R3#configure terminal                       Ingresa a modo de configuración
R3(config)#ip route 4.0.0.0 255.0.0.0 192.1.34.4   Declarar red destino
```

Router R4

```
R4>
R4>enable                                   Ingresa a modo privilegiado
R4#configure terminal                       Ingresa a modo de configuración
R4(config)#ip route 3.0.0.0 255.0.0.0 192.1.34.3  Declarar red destino
```

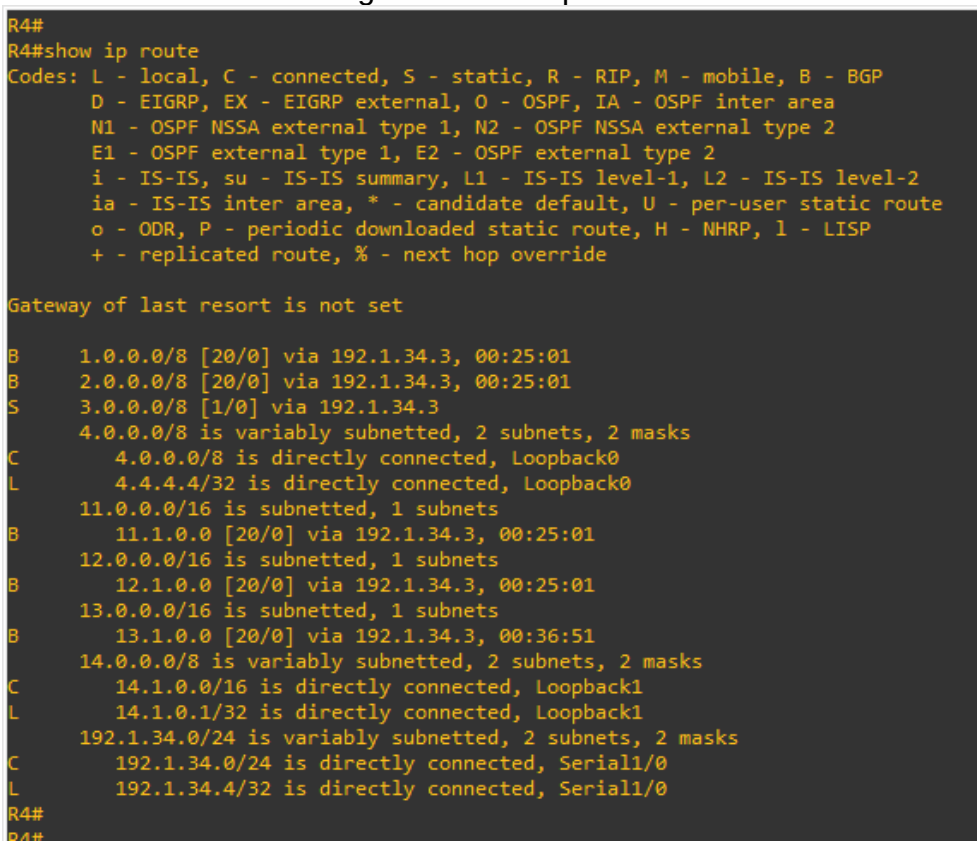
1.4. Revisión tablas de enrutamiento comando show ip route

Figura 7. Show ip Router 3



```
R3#
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B      1.0.0.0/8 [20/0] via 192.1.23.2, 00:25:26
B      2.0.0.0/8 [20/0] via 192.1.23.2, 00:25:26
       3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C         3.0.0.0/8 is directly connected, Loopback0
L         3.3.3.3/32 is directly connected, Loopback0
S      4.0.0.0/8 [1/0] via 192.1.34.4
       11.0.0.0/16 is subnetted, 1 subnets
B         11.1.0.0 [20/0] via 192.1.23.2, 00:25:26
       12.0.0.0/16 is subnetted, 1 subnets
B         12.1.0.0 [20/0] via 192.1.23.2, 00:25:26
       13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C         13.1.0.0/16 is directly connected, Loopback1
L         13.1.0.1/32 is directly connected, Loopback1
       14.0.0.0/16 is subnetted, 1 subnets
B         14.1.0.0 [20/0] via 192.1.34.4, 00:37:16
       192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.1.23.0/24 is directly connected, FastEthernet0/0
L         192.1.23.3/32 is directly connected, FastEthernet0/0
       192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.1.34.0/24 is directly connected, Serial1/0
L         192.1.34.3/32 is directly connected, Serial1/0
R3#
R3#
```

Figura 8. Show ip Router 4



```
R4#
R4#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

B      1.0.0.0/8 [20/0] via 192.1.34.3, 00:25:01
B      2.0.0.0/8 [20/0] via 192.1.34.3, 00:25:01
S      3.0.0.0/8 [1/0] via 192.1.34.3
       4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C         4.0.0.0/8 is directly connected, Loopback0
L         4.4.4.4/32 is directly connected, Loopback0
       11.0.0.0/16 is subnetted, 1 subnets
B         11.1.0.0 [20/0] via 192.1.34.3, 00:25:01
       12.0.0.0/16 is subnetted, 1 subnets
B         12.1.0.0 [20/0] via 192.1.34.3, 00:25:01
       13.0.0.0/16 is subnetted, 1 subnets
B         13.1.0.0 [20/0] via 192.1.34.3, 00:36:51
       14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C         14.1.0.0/16 is directly connected, Loopback1
L         14.1.0.1/32 is directly connected, Loopback1
       192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C         192.1.34.0/24 is directly connected, Serial1/0
L         192.1.34.4/32 is directly connected, Serial1/0
R4#
R4#
```

Guardar cambios en los Router

2. ESCENARIO 2

Figura 9. Escenario 2

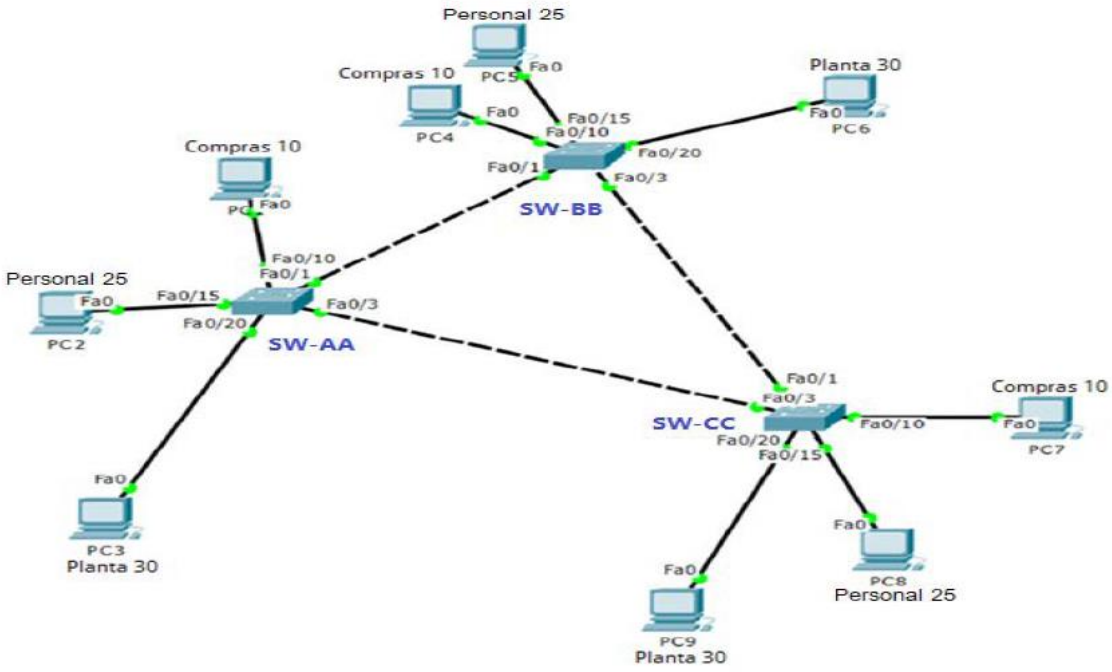
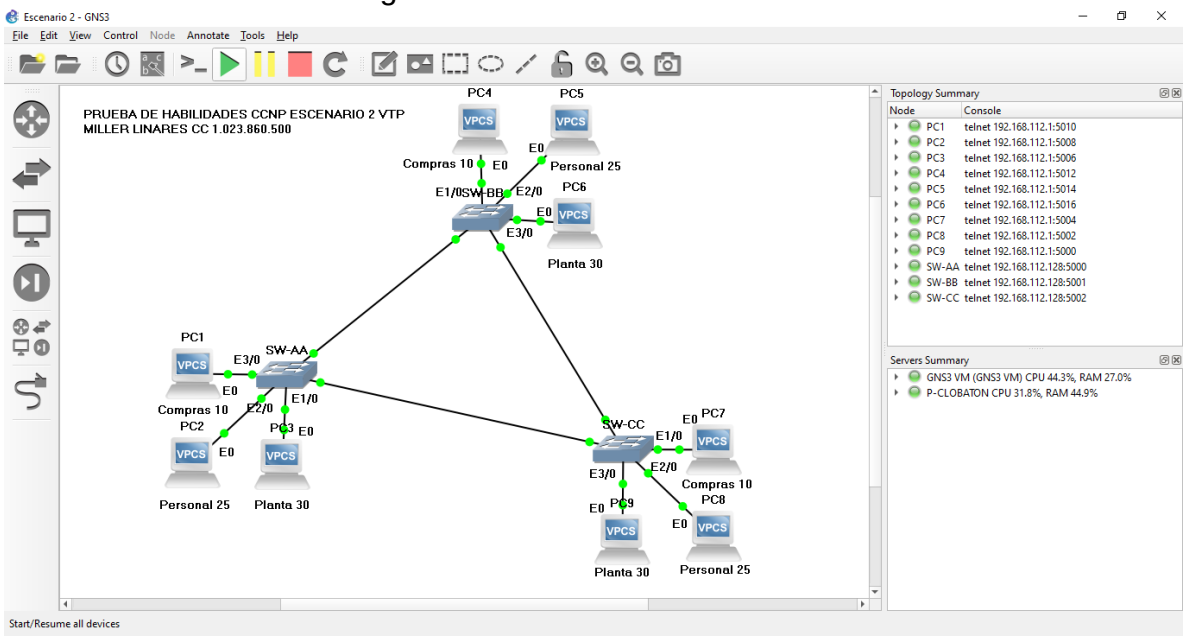


Figura 10. Simulación del escenario 2



1.5. Configuración VTP

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.

SW-AA

```
Switch>
Switch>enable                                   Ingresa a modo privilegiado
Switch#configure terminal                       Ingresa a modo de configuración
Switch(config)#hostname SW-AA                   Asigna nombre al switch
SW-AA(config)#no ip domain-lookup       Desactiva la traducción DNS
SW-AA(config)#line console 0            Ingresa a parámetros de consola
SW-AA(config-line)#logging synchronous Evita el mensaje no solicitado
SW-AA(config-line)#exec-timeout 0 0  Sin límite de tiempo inactividad
SW-AA(config-line)#exit                 Salir del modo de configuración
SW-AA(config)#
```

SW-BB

```
Switch>
Switch>enable                                   Ingresa a modo privilegiado
Switch#configure terminal                       Ingresa a modo de configuración
Switch(config)#hostname SW-BB                   Asigna nombre al switch
SW-BB(config)#no ip domain-lookup       Desactiva la traducción DNS
SW-BB(config)#line console 0            Ingresa a parámetros de consola
SW-BB(config-line)#logging synchronous  Evita el mensaje no solicitado
SW-BB(config-line)#exec-timeout 0 0     Sin límite de tiempo inactividad
SW-BB(config-line)#exit                 Salir del modo de configuración
SW-BB(config)#
```

SW-CC

```
Switch>
Switch>enable                                   Ingresa a modo privilegiado
Switch#configure terminal                       Ingresa a modo de configuración
Switch(config)#hostname SW-CC                   Asigna nombre al switch
SW-CC(config)#no ip domain-lookup       Desactiva la traducción DNS
SW-CC(config)#line console 0            Ingresa a parámetros de consola
SW-CC(config-line)#logging synchronous Evita el mensaje no solicitado
SW-CC(config-line)#exec-timeout 0 0 Sin límite de tiempo inactividad
SW-CC(config-line)#exit                 Salir del modo de configuración
```

SW-CC(config)#

SW-AA

SW-AA>enable	Ingresa a modo privilegiado
SW-AA#configure terminal	Ingresa a 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

SW-BB

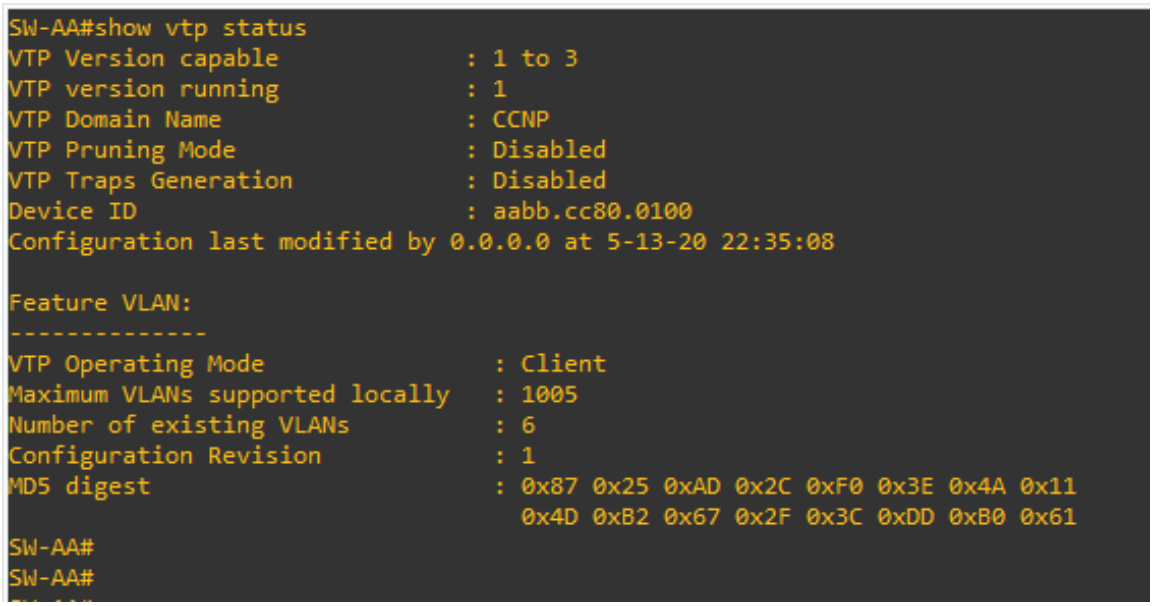
SW-BB>enable	Ingresa a modo privilegiado
SW-BB#configure terminal	Ingresa a modo de configuración
SW-BB(config)#vtp mode server	Configuración VTP modo cliente
SW-BB(config)#vtp domain CCNP	Configuración dominio VTP
SW-BB(config)#vtp password cisco	Contraseña de VTP cisco
SW-BB(config)#exit	Salir del modo de configuración

SW-CC

SW-CC>enable	Ingresa a modo privilegiado
SW-CC#configure terminal	Ingresa a modo de configuración
SW-CC(config)#vtp mode client	Configuración VTP modo cliente
SW-CC(config)#vtp domain CCNP	Configuración dominio VTP
SW-CC(config)#vtp password cisco	Contraseña de VTP cisco
SW-CC(config)#exit	Salir del modo de configuración

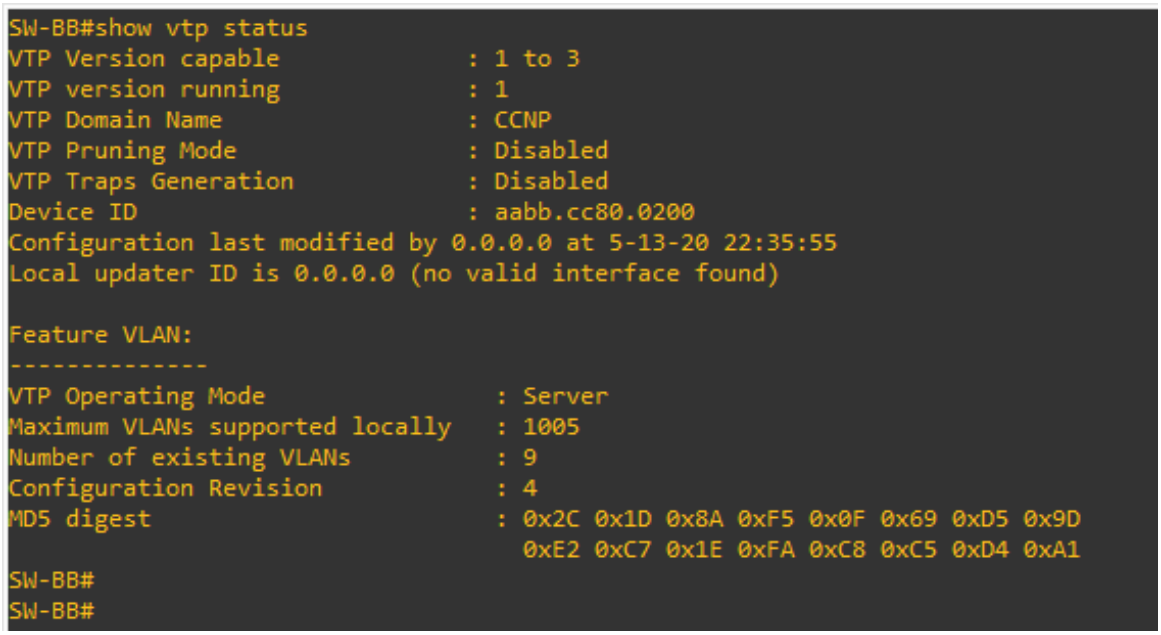
1.6. Verifique las configuraciones mediante el comando show vtp status.

Figura 11. Show VTP Status SW-AA



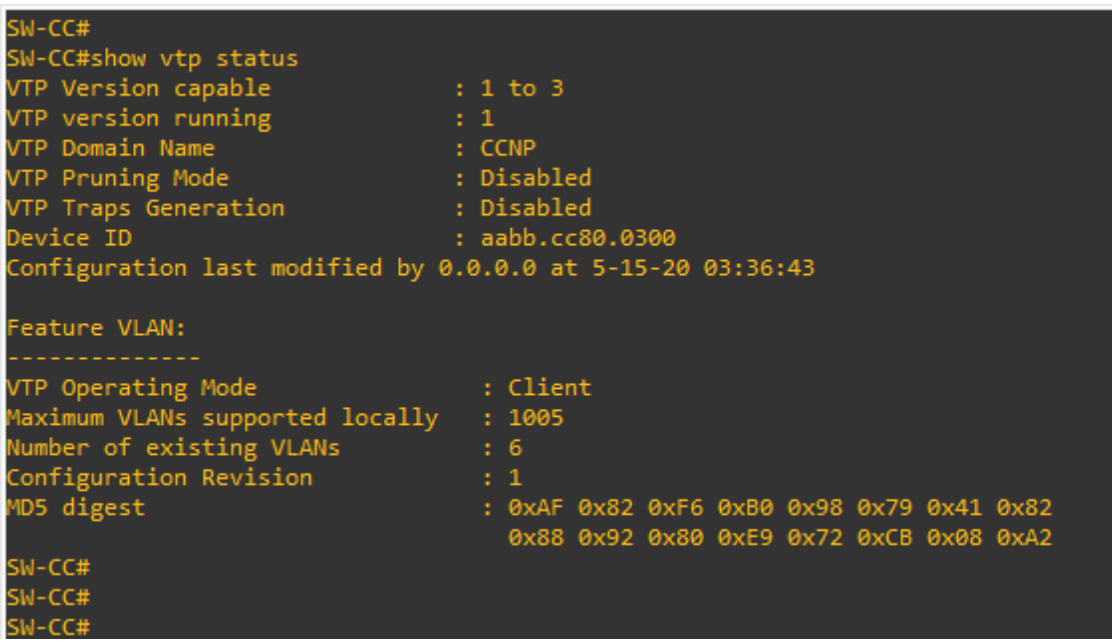
```
SW-AA#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0100
Configuration last modified by 0.0.0.0 at 5-13-20 22:35:08

Feature VLAN:
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 6
Configuration Revision            : 1
MD5 digest                        : 0x87 0x25 0xAD 0x2C 0xF0 0x3E 0x4A 0x11
                                    0x4D 0xB2 0x67 0x2F 0x3C 0xDD 0xB0 0x61

SW-AA#
SW-AA#
```

Figura 12. Show VTP Status SW-BB



```
SW-BB#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0200
Configuration last modified by 0.0.0.0 at 5-13-20 22:35:55
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 9
Configuration Revision            : 4
MD5 digest                        : 0x2C 0x1D 0x8A 0xF5 0x0F 0x69 0xD5 0x9D
                                    0xE2 0xC7 0x1E 0xFA 0xC8 0xC5 0xD4 0xA1

SW-BB#
SW-BB#
```

Figura 13. Show VTP Status SW-CC



1.7. Configurar DTP (Dynamic Trunking Protocol)

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>enable	Ingresa a modo privilegiado
SW-AA#configure terminal	Ingresa a modo de configuración
SW-AA(config)#interface ethernet 0/0	Configure interfaz ethernet
SW-AA(config-if)#switchport mode trunk	Puerto modo trunk
SW-AA(config-if)#switchport mode Dynamic desirable	Modo de operación troncal
SW-AA(config-if)#exit	Salir del modo de configuración

SW-BB

SW-BB>enable	Ingresa a modo privilegiado
SW-BB#configure terminal	Ingresa a modo de configuración
SW-BB(config)#interface ethernet 0/0	Configure interfaz ethernet
SW-BB(config-if)#switchport mode trunk	Puerto modo trunk
SW-BB(config-if)#exit	Salir del modo de configuración

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

Figura 14. Show Interface Trunck SW-AA

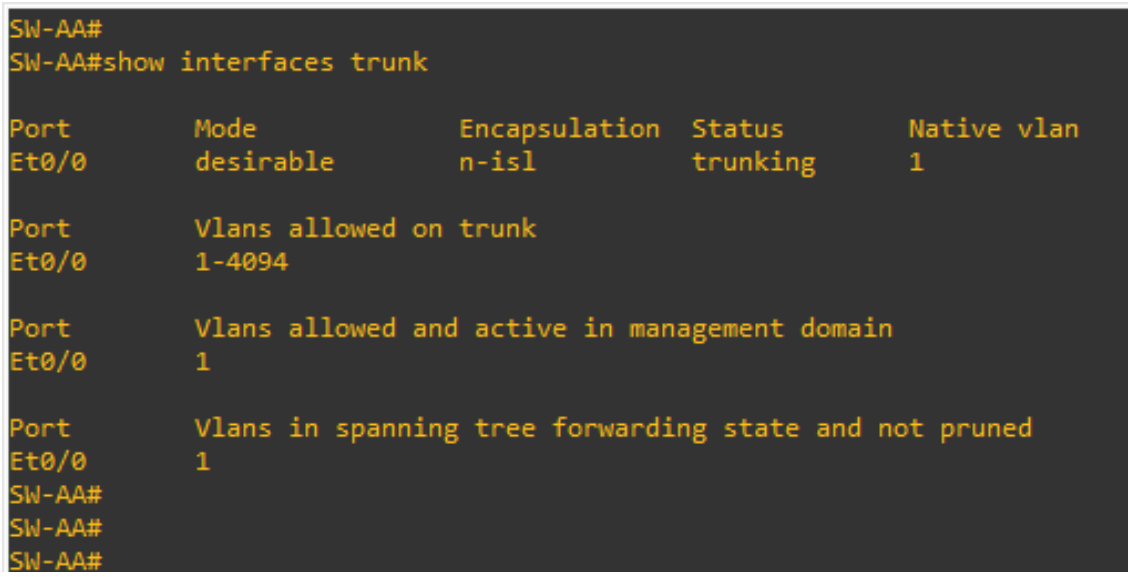
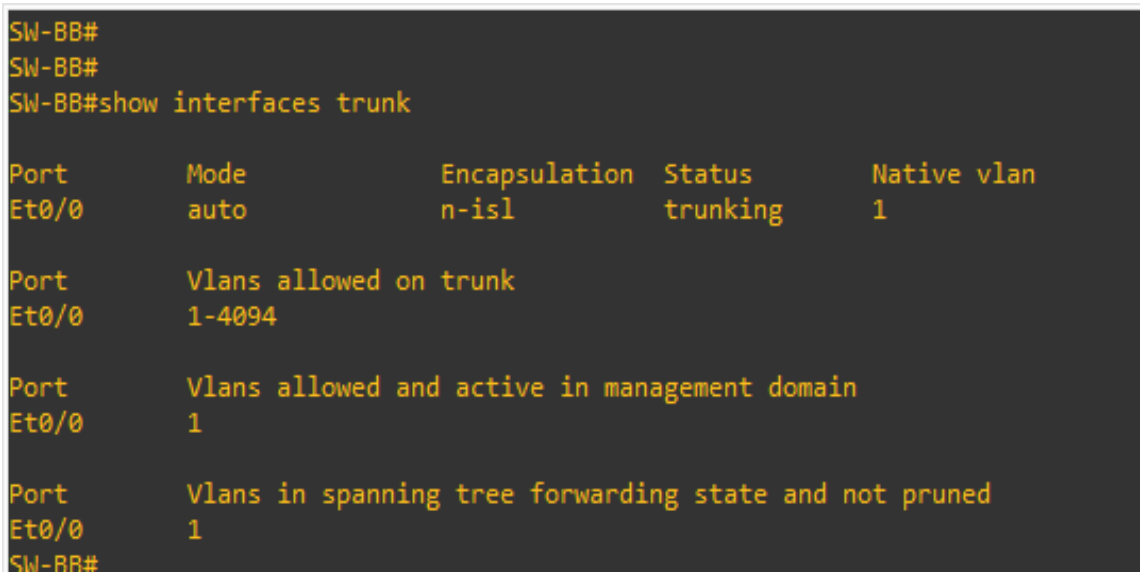


Figura 15. Show Interface Trunck SW-BB



Entre SW-AA y SW-CC configure un enlace "trunk" estático utilizando el comando ***switchport mode trunk*** en la interfaz ethernet 0/1 de SW-AA

SW-AA

SW-AA>enable Ingresa a modo privilegiado
SW-AA#configure terminal Ingresa a modo de configuración
SW-AA(config)#interface ethernet 0/1 Configure 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-if)#exit Salir del modo de configuración

SW-CC

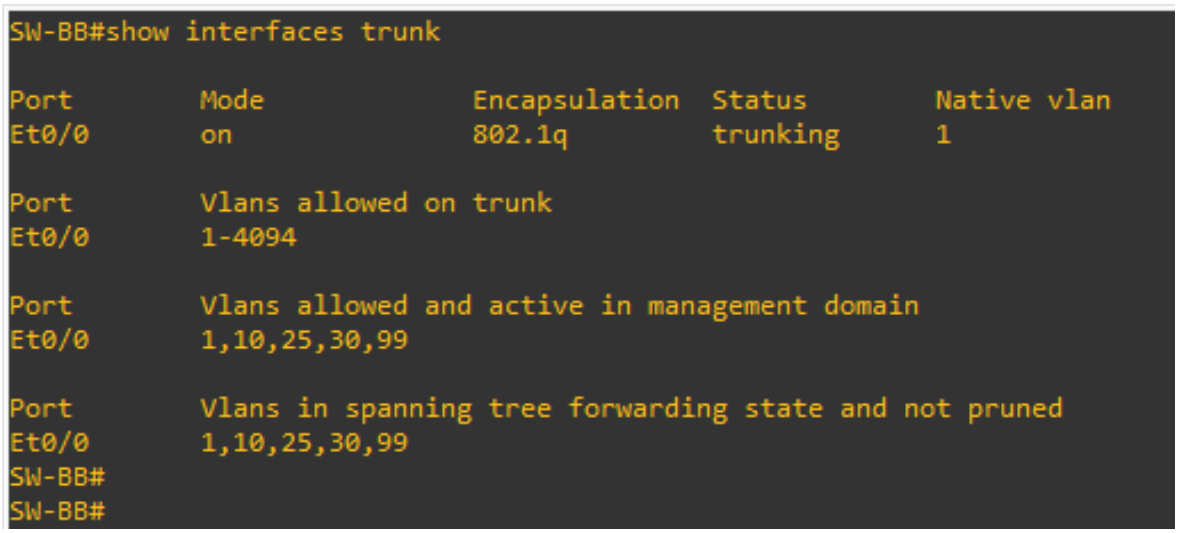
SW-CC>enable Ingresa a modo privilegiado
SW-CC#configure terminal Ingresa a modo de configuración
SW-CC(config)#interface ethernet 0/1 Configure interfaz ethernet
SW-CC(config-if)switchport trunk encapsulation dot1q Encapsulación de enlace 802.1q
SW-CC(config-if)#switchport mode trunk Puerto modo trunk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

Verifique el enlace "trunk" el comando ***show interface***

Figura 17. Show Interface Trunck SW-AA

```
SW-AA#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       desirable        802.1q         trunking      1
Et0/1       auto             n-802.1q       trunking      1

Port        Vlans allowed on trunk
Et0/0       1-4094
Et0/1       1-4094

Port        Vlans allowed and active in management domain
Et0/0       1,10,25,30,99
Et0/1       1,10,25,30,99

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       1,10,25,30,99
Et0/1       1,10,25,30,99
SW-AA#
```

Figura 18. Show Interface Trunck SW-BB



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

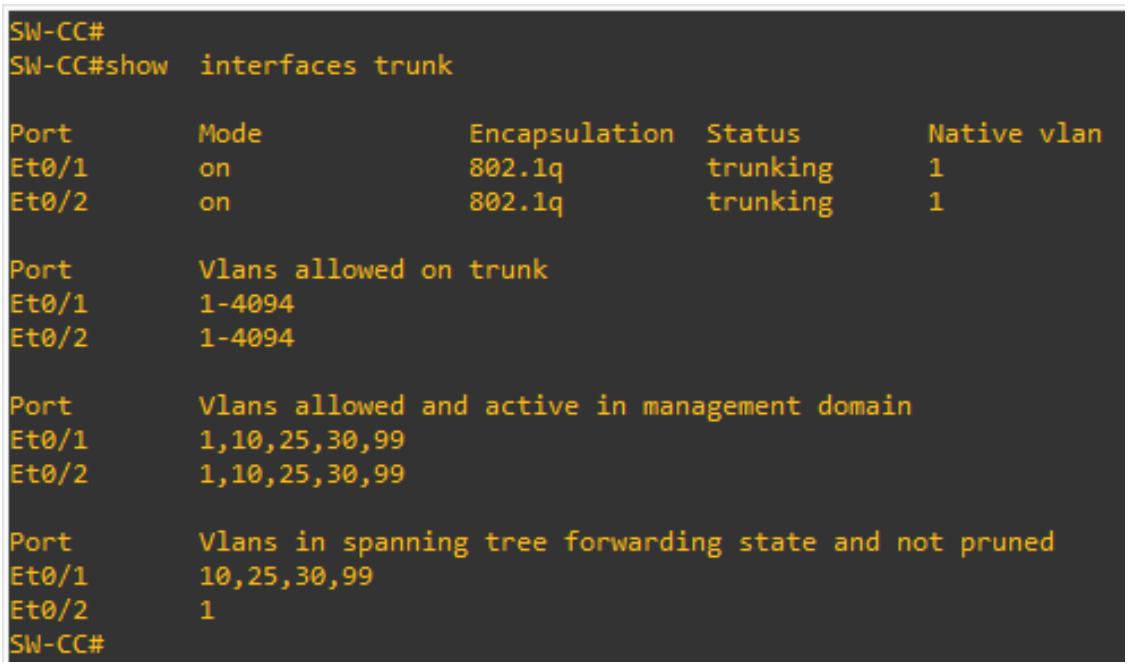
SW-BB

SW-BB>enable Ingresa a modo privilegiado
SW-BB#configure terminal Ingresa a modo de configuración
SW-BB(config)#interface ethernet 0/2 Configure interfaz ethernet
SW-BB(config-if)switchport trunk encapsulation dot1q Encapsulación de enlace 802.1q
SW-BB(config-if)#switchport mode trunk Puerto modo trunk
SW-CC(config-if) switchport trunk allowed vlan all Permite acceso a todas las vlan
SW-BB(config-if)#exit Salir del modo de configuración

SW-CC

SW-CC>enable Ingresa a modo privilegiado
SW-CC#configure terminal Ingresa a modo de configuración
SW-CC(config)#interface ethernet 0/2 Configure interfaz ethernet
SW-CC(config-if)switchport trunk encapsulation dot1q Encapsulación de enlace 802.1q
SW-CC(config-if)#switchport mode trunk Puerto modo trunk
SW-CC(config-if) switchport trunk allowed vlan all Permite acceso a todas las vlan
SW-CC(config-if)#exit Salir del modo de configuración

Figura 19. Show Interface Trunck SW-CC



```
SW-CC#
SW-CC#show  interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/1       on               802.1q         trunking      1
Et0/2       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/1       1-4094
Et0/2       1-4094

Port        Vlans allowed and active in management domain
Et0/1       1,10,25,30,99
Et0/2       1,10,25,30,99

Port        Vlans in spanning tree forwarding state and not pruned
Et0/1       10,25,30,99
Et0/2       1
SW-CC#
```

1.8. Agregar VLANS y asignar puertos

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

SW-AA

SW-AA>enable	Ingresa a modo privilegiado
SW-AA#configure terminal	Ingresa a modo de configuración
SW-AA(config-vlan)#vlan 10	Agregar VLAN 10
SW-AA(config-vlan)#name Compras	Agregar nombre a la VLAN
SW-AA(config)#exit	Salir del modo de configuración

SW-BB

SW-BB>enable	Ingresa a modo privilegiado
SW-BB#configure terminal	Ingresa a modo de configuración
SW-BB(config)#vlan 10	Agregar VLAN 10
SW-BB(config-vlan)#name Compras	Agregar nombre a la VLAN
SW-BB(config-vlan)#vlan 25	Agregar VLAN 25
SW-BB(config-vlan)#name Personal	Agregar nombre a la VLAN
SW-BB(config-vlan)#vlan 30	Agregar VLAN 30

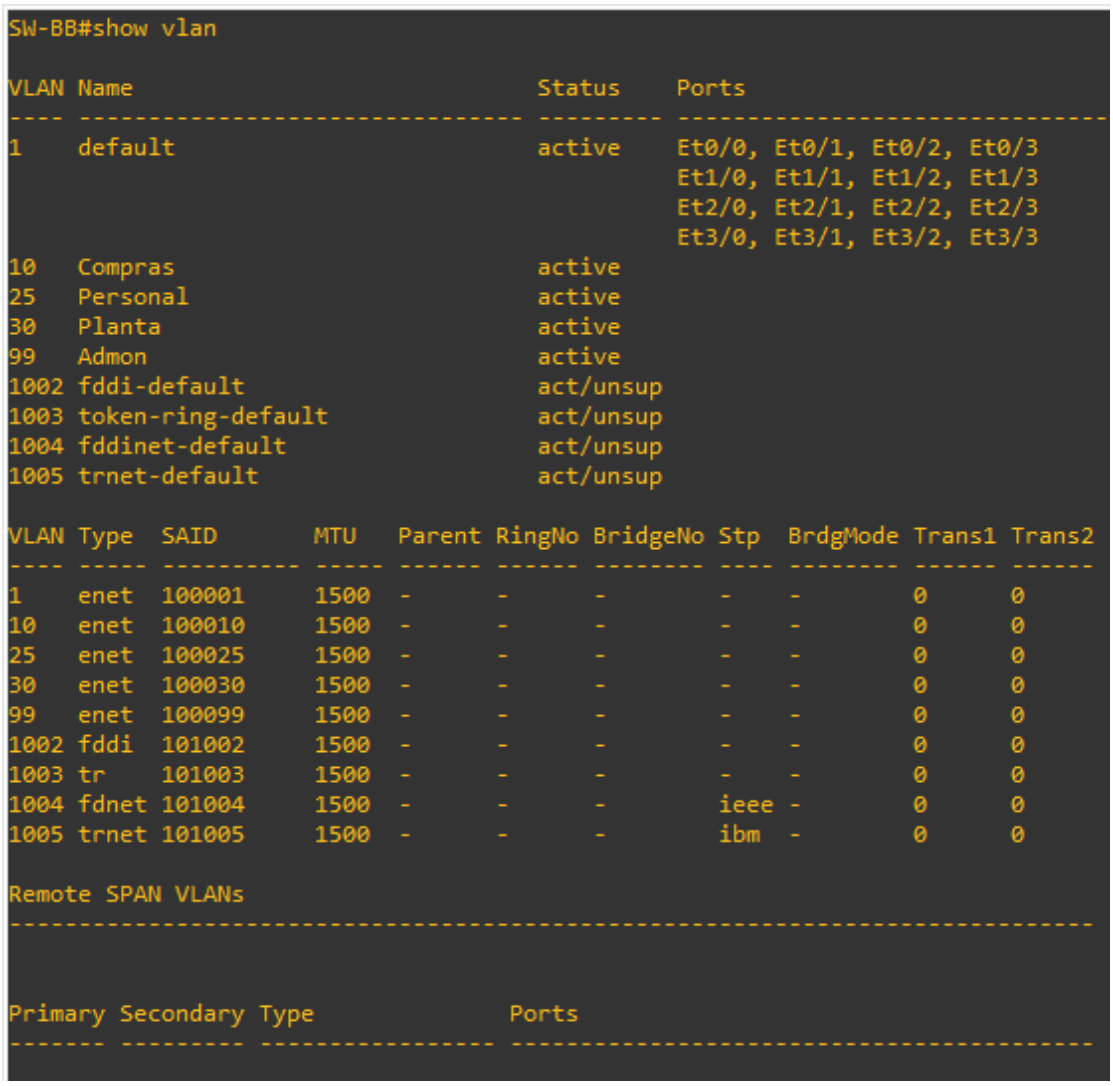
SW-BB(config-vlan)#name Planta	Agregar nombre a la VLAN
SW-BB(config-vlan)#vlan 99	Agregar VLAN 99
SW-BB(config-vlan)#name Admon	Agregar nombre a la VLAN
SW-BB(config-vlan)#exit	Salir del modo de configuración

Verifique que las VLANs han sido agregadas correctamente usando el comando show vlans

Figura 20. Show Vlan SW-AA

```
SW-AA#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et0/0, Et0/1, Et0/2, Et0/3
                                                 Et1/0, Et1/1, Et1/2, Et1/3
                                                 Et2/0, Et2/1, Et2/2, Et2/3
                                                 Et3/0, Et3/1, Et3/2, Et3/3
10   Compras                           active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Figura 21. Show Vlan SW-BB



```
SW-BB#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et0/0, Et0/1, Et0/2, Et0/3
                                                 Et1/0, Et1/1, Et1/2, Et1/3
                                                 Et2/0, Et2/1, Et2/2, Et2/3
                                                 Et3/0, Et3/1, Et3/2, Et3/3
10   Compras                           active
25   Personal                          active
30   Planta                            active
99   Admon                             active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
25   enet  100025     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
99   enet  100099     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

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

Tabla 5 Direccionamiento IP VLAN

Interfaz	VLAN	Direcciones IP de los PCs
Ethernet 1/0	VLAN 10	190.108.10.X/24
Ethernet 2/0	VLAN 25	190.108.20.X/24
Ethernet 3/0	VLAN 30	190.108.30.X/24

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

SW-AA

SW-AA>enable Ingresa a modo privilegiado
SW-AA#configure terminal Ingresa a modo de configuración
SW-AA(config)#interface ethernet 1/0 Configure interfaz ethernet
SW-AA(config-if)#switchport mode access Puerto en modo acceso
SW-AA(config-if)#switchport access vlan 10 Puerto en modo acceso
SW-AA(config-if)#exit Salir del modo de configuración

SW-BB

SW-BB>enable Ingresa a modo privilegiado
SW-BB#configure terminal Ingresa a modo de configuración
SW-BB(config)#interface ethernet 1/0 Configure interfaz ethernet
SW-BB(config-if)#switchport mode access Puerto en modo acceso
SW-BB(config-if)#switchport access vlan 10 Puerto en modo acceso
SW-BB(config-if)#exit Salir del modo de configuración

SW-CC

SW-CC>enable Ingresa a modo privilegiado
SW-CC#configure terminal Ingresa a modo de configuración
SW-CC(config)#interface ethernet 1/0 Configure interfaz ethernet
SW-CC(config-if)#switchport mode access Puerto en modo acceso
SW-CC(config-if)#switchport Access vlan 10 Puerto en modo acceso
SW-CC(config-if)#exit Salir del modo de configuración

Repita el procedimiento para los puertos ethernet 2/0 y ethernet 3/0 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.

SW-AA

SW-AA>enable Ingresa a modo privilegiado
SW-AA#configure terminal Ingresa a modo de configuración
SW-AA(config)#interface ethernet 2/0 Configure interfaz ethernet
SW-AA(config-if)#switchport mode Access vlan 25 Puerto en modo acceso
SW-AA(config-if)#switchport access Puerto en modo acceso

SW-AA(config-if)#exit Salir del modo de configuración

SW-BB

SW-BB>enable Ingresa a modo privilegiado
SW-BB#configure terminal Ingresa a modo de configuración
SW-BB(config)#interface ethernet 2/0 Configure interfaz ethernet
SW-BB(config-if)#switchport mode Access vlan 25 Puerto en modo acceso
SW-BB(config-if)#switchport access Puerto en modo acceso
SW-BB(config-if)#exit Salir del modo de configuración

SW-CC

SW-CC>enable Ingresa a modo privilegiado
SW-CC#configure terminal Ingresa a modo de configuración
SW-CC(config)#interface ethernet 2/0 Configure interfaz ethernet
SW-CC(config-if)#switchport mode Access vlan 25 Puerto en modo acceso
SW-CC(config-if)#switchport access Puerto en modo acceso
SW-CC(config-if)#exit Salir del modo de configuración

SW-AA

SW-AA>enable Ingresa a modo privilegiado
SW-AA#configure terminal Ingresa a modo de configuración
SW-AA(config)#interface ethernet 3/0 Configure interfaz ethernet
SW-AA(config-if)#switchport mode access Puerto en modo acceso
SW-AA(config-if)#switchport access vlan 30 Puerto en modo acceso
SW-AA(config-if)#exit Salir del modo de configuración

SW-BB

SW-BB>enable Ingresa a modo privilegiado
SW-BB#configure terminal Ingresa a modo de configuración
SW-BB(config)#interface ethernet 3/0 Configure interfaz ethernet
SW-BB(config-if)#switchport mode access vlan 30 Puerto en modo acceso
SW-BB(config-if)#switchport access Puerto en modo acceso
SW-BB(config-if)#exit Salir del modo de configuración

SW-CC

SW-CC>enable Ingresa a modo privilegiado
SW-CC#configure terminal Ingresa a modo de configuración
SW-CC(config)#interface ethernet 3/0 Configure interfaz ethernet
SW-CC(config-if)#switchport mode access Puerto en modo acceso

SW-CC(config-if)#switchport access vlan 30 Puerto en modo acceso
SW-CC(config-if)#exit Salir del modo de configuración

Tabla 6 Direccionamiento IP HOST

PC	Interfaz	Direccion IP	Mascara
PC3	VLAN 10	190.108.10.201	255.255.255.0
PC2	VLAN 25	190.108.20.201	255.255.255.0
PC1	VLAN 30	190.108.30.201	255.255.255.0
PC4	VLAN 10	190.108.10.202	255.255.255.0
PC5	VLAN 25	190.108.20.202	255.255.255.0
PC6	VLAN 30	190.108.30.202	255.255.255.0
PC7	VLAN 10	190.108.10.203	255.255.255.0
PC8	VLAN 25	190.108.20.203	255.255.255.0
PC9	VLAN 30	190.108.30.203	255.255.255.0

1.9. Configurar las direcciones IP en los Switches

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 7 Direccionamiento IP VLAN99

Switch	Interfaz	Direccion IP	Mascara
SW-AA	VLAN 99	190.108.99.201	255.255.255.0
SW-BB	VLAN 99	190.108.99.202	255.255.255.0
SW-CC	VLAN 99	190.108.99.203	255.255.255.0

SW-AA

SW-AA>enable Ingresa a modo privilegiado
SW-AA#configure terminal Ingresa a modo de configuración
SW-AA(config)#interface vlan 99 Configure interfaz SVI
SW-AA(config)#ip address 190.108.99.201 255 255 255.0 Asignacion IPV4
SW-AA(config)#no shutdown Activamos la interfaz
SW-AA(config)#exit Salir del modo de configuración

SW-BB

SW-BB>enable Ingresa a modo privilegiado
SW-BB#configure terminal Ingresa a modo de configuración
SW-BB(config)#interface vlan 99 Configure interfaz SVI
SW-BB(config)#ip address 190.108.99.202 255 255 255.0 Asignacion IPV4
SW-BB(config)#no shutdown Activamos la interfaz
SW-BB(config)#exit Salir del modo de configuración

SW-CC

SW-CC>enable Ingresa a modo privilegiado
SW-CC#configure terminal Ingresa a modo de configuración
SW-CC(config)#interface vlan 99 Configure interfaz SVI
SW-CC(config)#ip address 190.108.99.203 255 255 255.0 Asignacion IPV4
SW-CC(config)#no shutdown Activamos la interfaz
SW-CC(config)#exit Salir del modo de configuración

1.10. Verificar la conexión extremo a extremo

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

Tabla 8 Resultado Ping Host

Origen	Destino	Comando	Resultado
PC1	PC2	Ping 190.108.20.201	No accesible
PC1	PC3	Ping 190.108.10.201	No accesible
PC1	PC4	Ping 190.108.10.202	No accesible
PC1	PC5	Ping 190.108.20.202	No accesible
PC1	PC6	Ping 190.108.30.202	Accesible
PC1	PC7	Ping 190.108.10.203	No accesible
PC1	PC8	Ping 190.108.20.203	No accesible
PC1	PC9	Ping 190.108.30.203	Accesible
Conclusión: Se evidencia que, al ejecutar ping desde cada uno de los PC entre sí, 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 22. Ping PC1 to (PC6 and PC9)

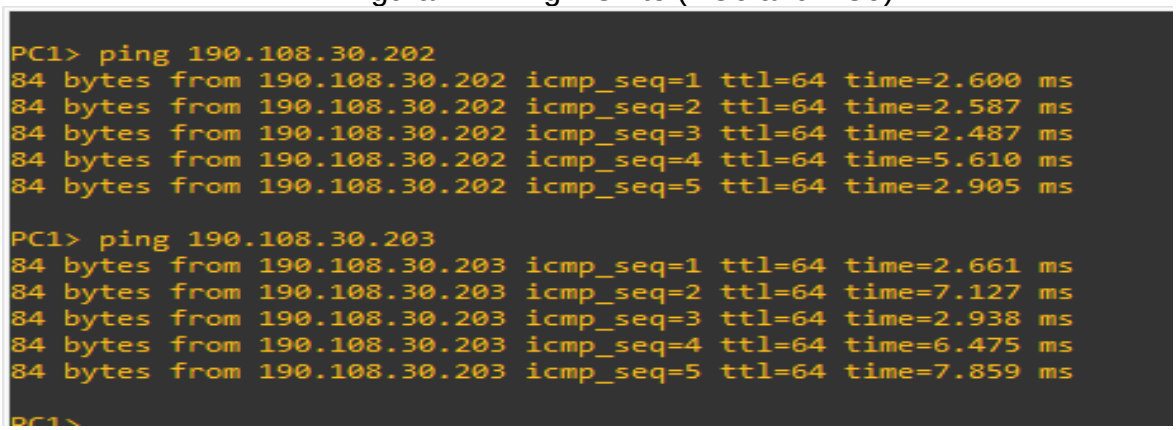
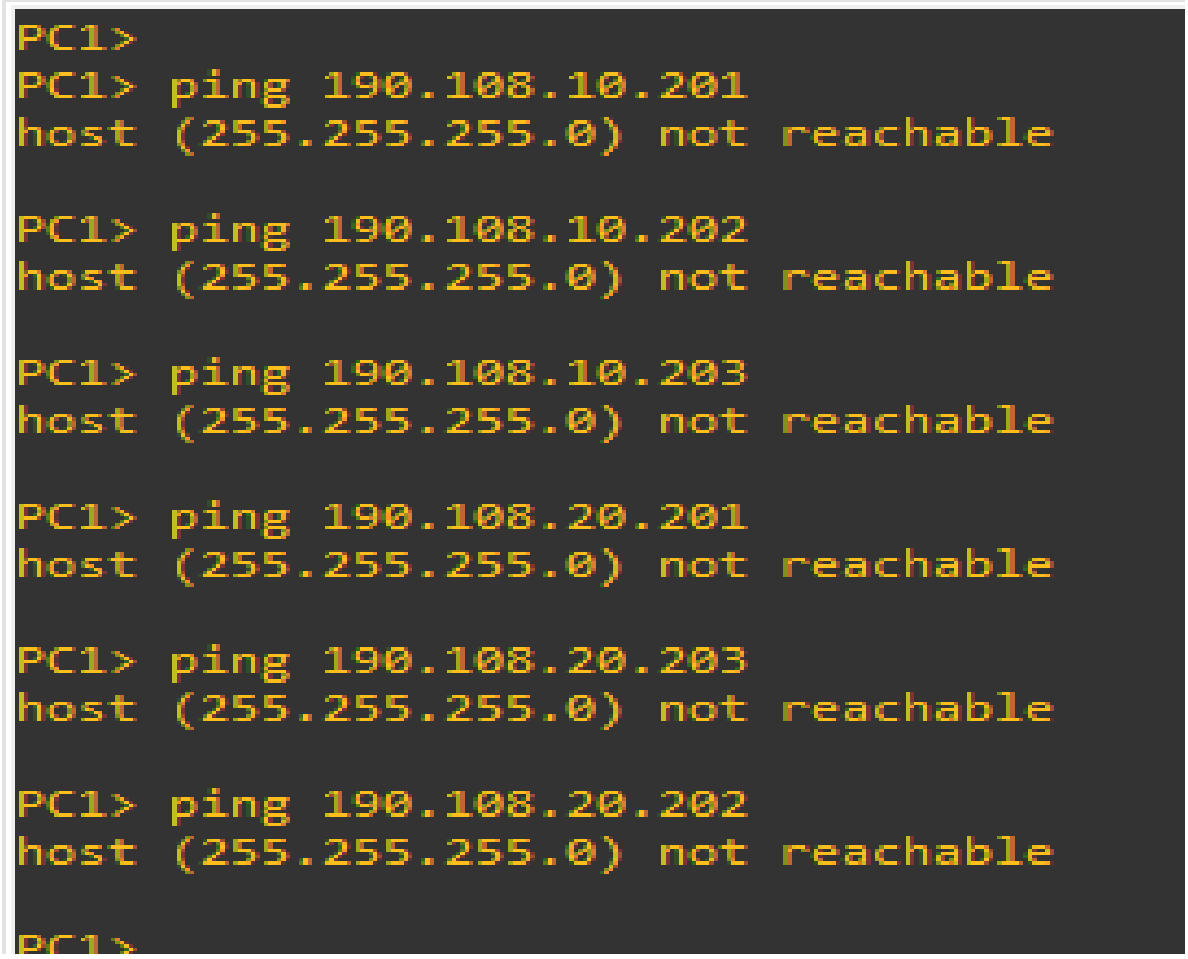


Figura 23. Ping PC1 to (PC2-PC3-PC4-PC5-PC7-PC8)



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

Tabla 9 Resultado Ping SWITCH

Origen	Destino	Comando	Resultado
SW-AA	SW-BB	Ping 190.108.99.202	Accesible
SW-AA	SW-CC	Ping 190.108.99.203	Accesible
SW-BB	SW-AA	Ping 190.108.99.201	Accesible
SW-BB	SW-CC	Ping 190.108.99.203	Accesible
SW-CC	SW-AA	Ping 190.108.99.201	Accesible
SW-CC	SW-BB	Ping 190.108.99.202	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

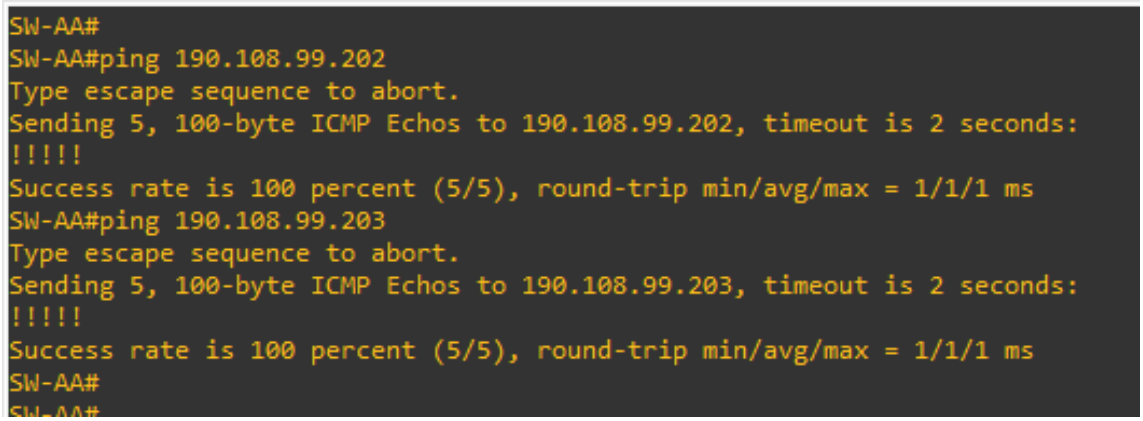


Figura 24. Ping SW-BB to SW-AA

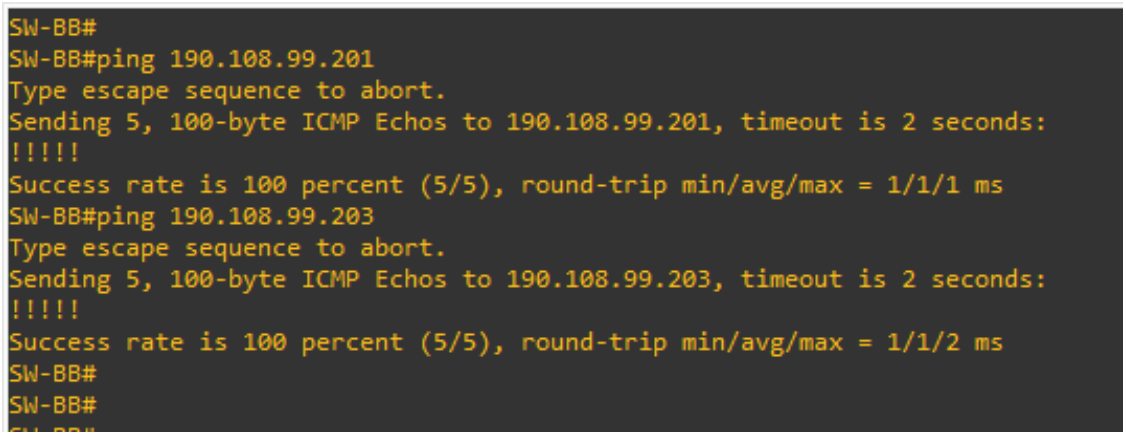
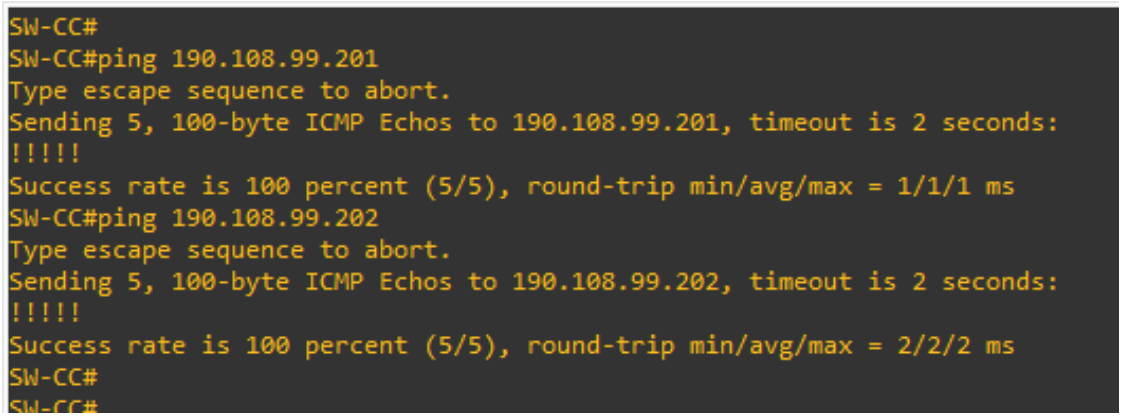


Figura 25. Ping SW-CC to SW-AA



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

Tabla 10 Resultado Ping entre SWITCH-AA y Host

Origen	Destino	Comando	Resultado
SW-AA	PC1	Ping 190.108.30.201	No accesible
SW-AA	PC2	Ping 190.108.20.201	No accesible
SW-AA	PC3	Ping 190.108.10.201	No accesible
SW-AA	PC4	Ping 190.108.10.202	No accesible
SW-AA	PC5	Ping 190.108.20.202	No accesible
SW-AA	PC6	Ping 190.108.30.202	No accesible
SW-AA	PC7	Ping 190.108.10.203	No accesible
SW-AA	PC8	Ping 190.108.20.203	No accesible
SW-AA	PC9	Ping 190.108.30.203	No accesible
Conclusión: 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 11 Resultado Ping entre SWITCH-BB y Host

Origen	Destino	Comando	Resultado
SW-BB	PC1	Ping 190.108.30.201	No accesible
SW-BB	PC2	Ping 190.108.20.201	No accesible
SW-BB	PC3	Ping 190.108.10.201	No accesible
SW-BB	PC4	Ping 190.108.10.202	No accesible
SW-BB	PC5	Ping 190.108.20.202	No accesible
SW-BB	PC6	Ping 190.108.30.202	No accesible
SW-BB	PC7	Ping 190.108.10.203	No accesible
SW-BB	PC8	Ping 190.108.20.203	No accesible
SW-BB	PC9	Ping 190.108.30.203	No accesible
Conclusión: 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 planteo para este escenario configuración de enrutamiento entre vlans.			

Tabla 12 Resultado Ping entre SWITCH-CC y Host

Origen	Destino	Comando	Resultado
SW-CC	PC1	Ping 190.108.30.201	No accesible
SW-CC	PC2	Ping 190.108.20.201	No accesible
SW-CC	PC3	Ping 190.108.10.201	No accesible
SW-CC	PC4	Ping 190.108.10.202	No accesible
SW-CC	PC5	Ping 190.108.20.202	No accesible
SW-CC	PC6	Ping 190.108.30.202	No accesible
SW-CC	PC7	Ping 190.108.10.203	No accesible
SW-CC	PC8	Ping 190.108.20.203	No accesible
SW-CC	PC9	Ping 190.108.30.203	No accesible

CONCLUSIONES

Para el desarrollo de los escenarios se utilizó el software de simulación GNS3 el cual permite realizar simulaciones de alta gama y permite la ejecución de comandos que en packet tracer no se lograron realizar pues no fueron soportados por el software y la realización en cada uno de los procesos en la configuración de dispositivos de Networking en base a los lineamientos sugeridos para cada caso.

Con el desarrollo de este trabajo se afianzaron conocimientos necesarios para el diseño de redes escalables los cuales se pusieron en practica en dos escenarios de red, como lo son 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).

Al culminar toda la actividad de este diplomado se pudo observar tanto el Routing como el Switching permiten aumentar la velocidad de acceso a la información y con esta acción administrar de manera eficiente y verificar lo que sucede donde está funcionando, todo esto gracias a la implementación de protocolos de enrutamiento como lo son OSPF y EIGRP.

BIBLIOGRAFIA

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

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!AmIJYeiNT1IlnMfy2rhPZHwEoWx

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!AmIJYeiNT1IlnMfy2rhPZHwEoWx

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!AmIJYeiNT1IlnMfy2rhPZHwEoWx

UNAD (2015). Introducción a la configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

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

Systems.Recuperadode 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 300101 Official Cert Guide. Recuperado de https://1drv.ms/b/s!AgIGg5JUgUBthFx8WOxiq6LPJppl

UNAD (2015). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm