# DIPLOMADO DE PROFUNDIZACION CISCO
# PRUEBA DE HABILIDADES PRÁCTICAS CCNP

**FRANK DIAZ GALINDO**

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI INGENIERÍA ELECTRÓNICA BOGOTA

2020

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

**FRANK DIAZ GALINDO**

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

DIRECTOR:

MSc. EFRAIN ALEJANDRO PEREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI INGENIERÍA ELECTRÓNICA BOGOTA

2020

NOTA DE ACEPTACIÓN:

Presidente del Jurado

Jurado

Jurado

Bogotá, 20 de mayo de 2020

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

# GLOSARIO

**BGP**: En telecomunicaciones, el protocolo de puerta de enlace de frontera o BGP (del inglés Border Gateway Protocol) es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Por ejemplo, los proveedores de servicio registrados en Internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.

**SISTEMA AUTONOMO**: Un Sistema Autónomo (en inglés, Autonomous System: AS) se define como “un grupo de redes IP que poseen una política de rutas propia e independiente”. Esta definición hace referencia a la característica fundamental de un Sistema Autónomo: realiza su propia gestión del tráfico que fluye entre él y los restantes Sistemas Autónomos que forman Internet. Un número de AS o ASN se asigna a cada AS, el que lo identifica de manera única a sus redes dentro de Internet.

**VLAN**: Son las siglas de LAN virtual, es una red de área local que agrupa un conjunto de equipos de manera lógica y no física. Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física.

**VTP**: Son las siglas de VLAN Trunking Protocol, un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite centralizar y simplificar la administración en un dominio de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos. El protocolo VTP nace como una herramienta de administración para redes de cierto tamaño, donde la gestión manual se vuelve inabordable.

**DTP**: Dynamic Trunking Protocol es un protocolo propietario creado por Cisco Systems que opera entre switches Cisco, el cual automatiza la configuración de trunking (etiquetado de tramas de diferentes VLAN's con ISL o 802.1Q) en enlaces Ethernet. Dicho protocolo puede establecer los puertos ethernet en cinco modos diferentes de trabajo: AUTO, ON, OFF, DESIRABLE y NON-NEGOTIATE.

## RESUMEN

La revolución de las nuevas tecnologías a nivel mundial está cambiando considerablemente la forma de las economías llevándolas a ser más competitivas, más exigentes y con niveles muy altos de optimización de infraestructura y de las comunicaciones, es por ello por lo que las TIs juegan un papel muy importante en el crecimiento y desarrollo de los diferentes sectores económicos del mundo.

El desarrollo de las actividades para el Diplomado de profundización de Cisco CCNP permite lograr entender a profundidad los diferentes temas por medio de la teoría y la práctica, logrando obtener habilidades y destrezas en redes a nivel LAN/WAN por medio de diferentes escenarios propuestos en cada actividad y llevándolos a la realidad por medio de los programas como GNS3, Packet Tracert, entre otros.



**Palabras clave:** BGP, SISTEMA AUTONOMO, VLAN, VTP, DTP.

ABSTRACT

The revolution of new technologies worldwide is changing considerably the way of economies leading them to make them more competitive, more demanding and with very high levels of infrastructure and communications optimization, which is why ITs play a role very important in the growth and development of the different economic sectors of the world.

The development of activities for the Cisco CCNP Certificate of deepening allows us to understand in depth the different topics through theory and practice, obtaining skills and abilities in LAN / WAN networks through different scenarios proposed in each activity and bringing them to reality through programs such as GNS3, Packet Tracert, among others.

**Keywords:** BGP, AUTONOMOUS SYSTEM, VLAN, VTP, DTP.

# INTRODUCCIÓN

Es muy importante comprender que las redes actuales deben admitir una amplia variedad de aplicaciones y servicios, como así también funcionar con diferentes tipos de infraestructuras físicas. El término arquitectura de red, en este contexto, se refiere a las tecnologías que admiten la infraestructura y a los servicios y protocolos programados que pueden trasladar los mensajes en toda esa infraestructura. Debido a que Internet evoluciona, al igual que las redes en general, toma fuerza la existencia de cuatro características básicas que la arquitectura subyacente necesita para cumplir con las expectativas de los usuarios: tolerancia a fallas, escalabilidad, calidad del servicio y seguridad, las cuales son vitales en la administración, gestión de seguridad e implementación de redes conmutadas enrutadas, cada vez más robustas.

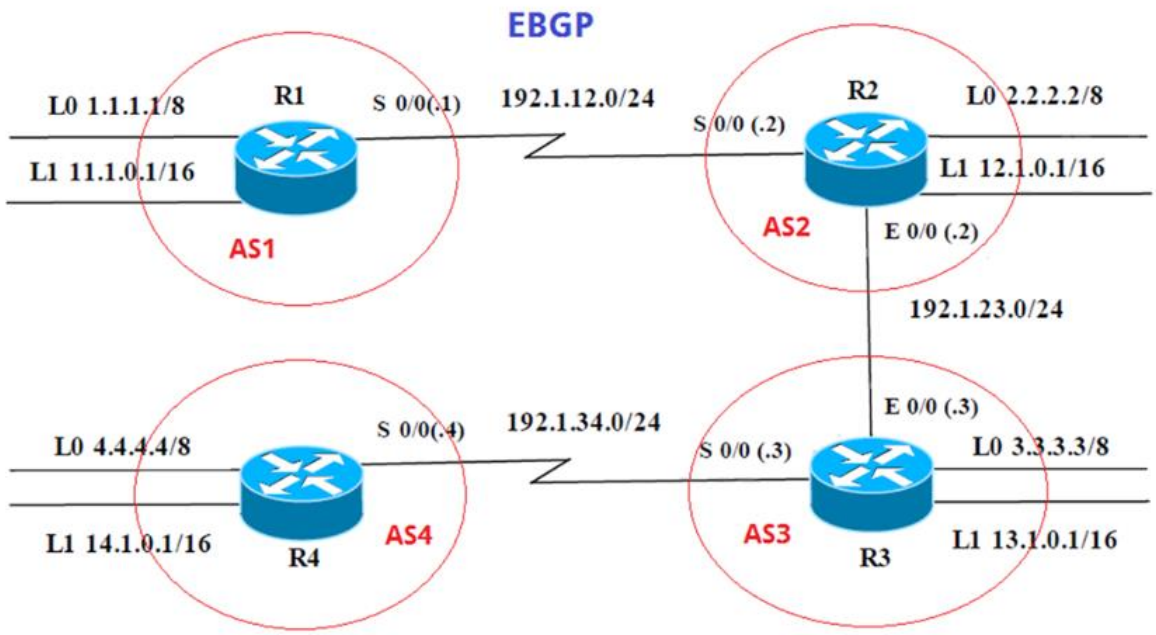
El mundo de hoy, tal como lo conocemos, se mantiene en un intercambio constante de información en medios digitales, las redes de cómputo hacen posible esta tarea, cada día aumenta de forma exponencial, ya que se agregan nuevos dispositivos, tales como celulares, televisores, lavadoras y todo lo que comprende el Iota o internet de las cosas, nuevas granjas de servidores más pc's entre otros. Entendiendo dichos requerimientos, surge una necesidad en el ámbito de las tecnologías de la información y es el de ingenieros que puedan realizar las implementaciones que contribuyan a la integración del mundo cibernético.

El siguiente trabajo escrito, en el cual se desarrollan las habilidades prácticas del diplomado CCNP, plasma el conocimiento adquirido, se puede apreciar, como todas y cada una de las actividades están enfocadas a la solución de problemas de la vida cotidiana de las empresas, las cuales dependen en gran medida de las tecnologías de la información.

Para ello, tenemos dos escenarios, en el primero hacemos uso del enrutamiento dinámico BGP para el segundo caso usaremos VTP y DTP.

# 1. ESCENARIO UNO

*Figura 1.Ilustración escenario uno*




DESARROLLO DE LAS ACTIVIDADES ESCENARIO UNO

Para el desarrollo de este escenario, configuraremos BGP para comunicar sistemas autónomos y a través de esto, los routers conocerán las redes remotas y como alcanzarlas.

## 1.1. Configuración del escenario propuesto

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***.

A continuación, el script requerido:

```
R1#configure terminal
R1(config)#interface Loopback 0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#interface Loopback 1
```

```
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#interface serial 3/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#router bgp 1
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#network 1.0.0.0 mask 255.0.0.0
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router)#network 192.1.12.0 mask 255.255.255.0
R1(config-router)#neighbor 192.1.12.2 remote-as 2

R2#configure terminal
R2(config)#interface Loopback 0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#interface Loopback 1
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#interface serial 3/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#interface GigabitEthernet 0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router bgp 2
R2(config-router)#bgp router-id 33.33.33.33
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)#network 192.1.12.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.12.1 remote-as 1
```

A continuación, se puede evidenciar en resultado obtenido del comando ***show ip route***, que tanto el router R1 como el router R2 contienen en su tabla de enrutamiento las direcciones de Loopback y las direcciones de las redes a las cuales se encuentran conectados de forma directa, además, de las redes configuradas en las interfaces Loopback de su respectivo router vecino. Estas últimas se pueden identificar mediante el código ***B*** que las precede, lo cual indica que ambas fueron aprendidas a través del protocolo BGP. Así también, se puede ver en la tabla de enrutamiento que cada router reconoce como vía para alcanzar estas rutas, la red 192.1.12.0/24 conectada a través de la interfaz serial 3/0, ya que este es el enlace que comunica físicamente ambos dispositivos.

*Figura 2. Verificación de rutas en R1*

```
R1#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

      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.0.0.0/8 is directly connected, Loopback0
L        1.1.1.1/32 is directly connected, Loopback0
B     2.0.0.0/8 [20/0] via 192.1.12.2, 00:00:00
      11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        11.1.0.0/16 is directly connected, Loopback1
L        11.1.0.1/32 is directly connected, Loopback1
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.12.2, 00:00:00
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial3/0
L        192.1.12.1/32 is directly connected, Serial3/0
R1#
```

*Figura 3. Verificación de rutas en 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

      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
      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
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial3/0
L        192.1.12.2/32 is directly connected, Serial3/0
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, GigabitEthernet0/0
L        192.1.23.2/32 is directly connected, GigabitEthernet0/0
R2#
```

### 1.2. Configuración de relación de vecino BGP entre R2 y R3

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 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***.

**Script requerido:**

```
R2#configure terminal
R2(config)#router bgp 2
R2(config-router)#network 192.1.23.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.23.3 remote-as 3

R3#configure terminal
R3(config)#interface Loopback 0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#interface Loopback 1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#interface GigabitEthernet 0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#interface serial 3/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
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)#network 192.1.23.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.23.2 remote-as 2
```

A continuación, se puede evidenciar en el resultado que se obtiene del comando ***show ip route***, que el router R2 ha actualizado su tabla de enrutamiento y ahora contiene también las direcciones de Loopback configuradas en el router R3, por tanto, este dispositivo ha aprendido hasta este momento 4 rutas a través del protocolo BGP las cuales identifica con el código ***B***. De otro lado, el router R3 contiene en su tabla de enrutamiento las redes que reconoce conectadas directamente, es decir, las configuradas en sus interfaces Loopback y las redes que lo comunican con los routers R3 y R4 mediante las interfaces GigabitEthernet 0/0 y serial 3/0 respectivamente. Además, este router (R3) ha actualizado su tabla de

enrutamiento con las direcciones de red correspondientes a las interfaces Loopback que se configuraron en R2 y R1, rutas que aprendió mediante el protocolo BGP gracias a su relación de adyacencia con R2 y a que dichas redes se anunciaron en cada uno de los routers, así también, R3 contiene la dirección de red que conecta los routers R1 y R2 la cual aprendió mediante el protocolo BGP como lo evidencia el código ***B*** que la precede. Por último, se identifica que R3 alcanza todas estas redes a través de la interfaz GigabitEthernet 0/0 que lo conecta con R2 (192.1.23.0/24)

*Figura 4. Verificación de rutas en R2*

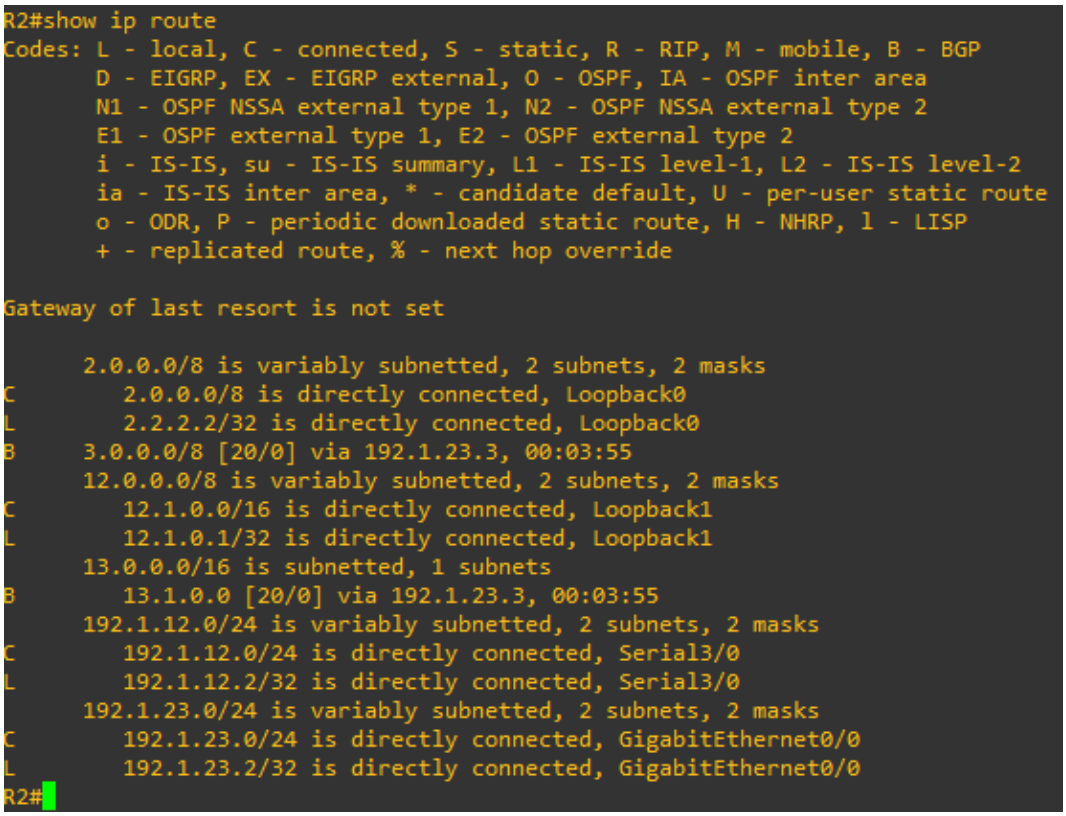
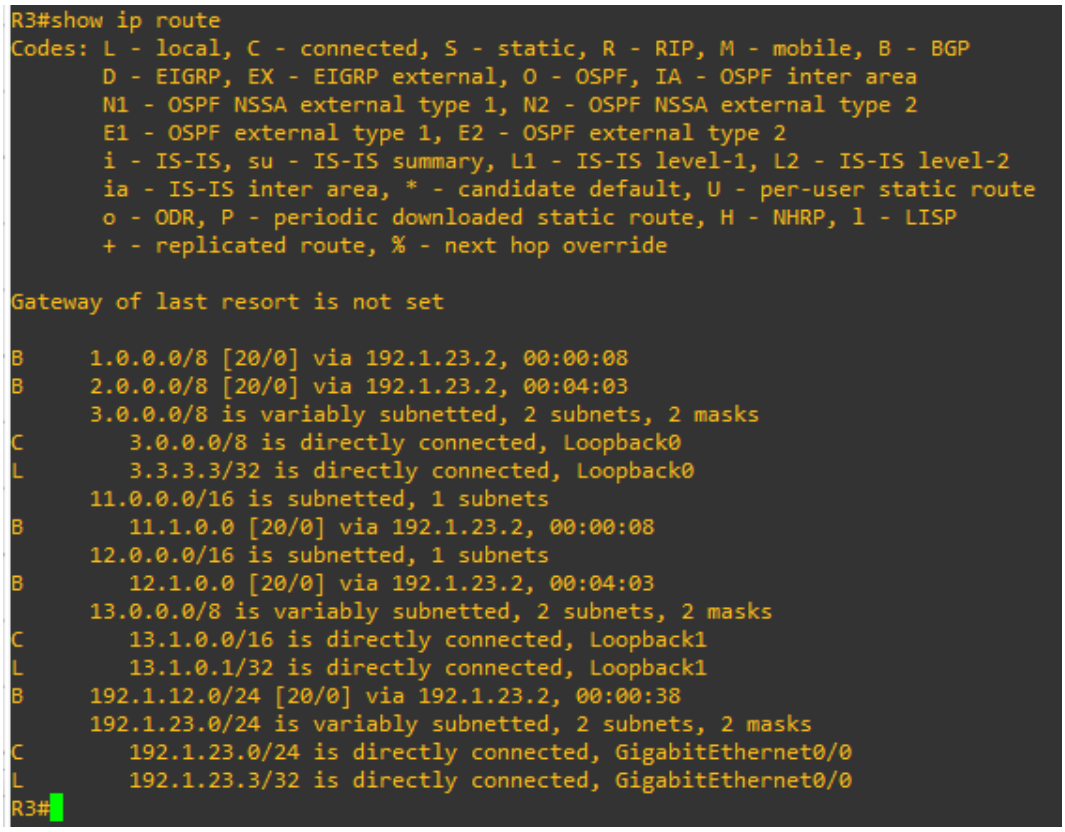


*Figura 5. Verificación de rutas en R3*




### 1.3. Configuración de relación de vecino BGP entre R3 y R4

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***.

**Script requerido**

R3#configure terminal
R3(config)#router bgp 3
R3(config-router)#network 192.1.34.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.34.4 remote-as 4

```
R4#configure terminal
R4(config)#interface Loopback 0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#interface Loopback 1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#interface serial 3/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#router bgp 4
R4(config-router)#bgp router-id 66.66.66.66
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)#network 192.1.34.0 mask 255.255.255.0
R4(config-router)#neighbor 192.1.34.3 remote-as 3
```

Para establecer las relaciones de adyacencia mediante las direcciones de Loopback, el router vecino necesita informar sobre el uso de esta interfaz en lugar de una interfaz física y, por tanto, se requiere una configuración adicional para establecer los vecinos:

**Script requerido**

```
R3#configure terminal
R3(config)#ip route 4.0.0.0 255.0.0.0 192.1.34.4
R3(config)#router bgp 3
R3(config-router)#no neighbor 192.1.34.4
R3(config-router)#no network 3.0.0.0 mask 255.0.0.0
R3(config-router)#neighbor 4.4.4.4 remote-as 4
R3(config-router)#neighbor 4.4.4.4 update-source loopback 0
R3(config-router)# neighbor 4.4.4.4 ebgp-multihop
```

```
R4#configure terminal
R4(config)#ip route 3.0.0.0 255.0.0.0 192.1.34.3
R4(config)#router bgp 4
R4(config-router)#no neighbor 192.1.34.3
R4(config-router)#no network 4.0.0.0 mask 255.0.0.0
R4(config-router)#neighbor 3.3.3.3 remote-as 3
R4(config-router)#neighbor 3.3.3.3 update-source loopback 0
R4(config-router)# neighbor 3.3.3.3 ebgp-multihop
```

A continuación, se puede evidenciar en el resultado que se obtiene del comando ***show iproute***, que el router R3 ha actualizado su tabla de enrutamiento y la

dirección de red que conecta este dispositivo con R4 ha cambiado y ahora corresponde a la dirección de Loopback 0, la cual aparece como una dirección estática dado que así se estableció en el paso anterior, sin embargo, pese a que se usa la dirección lógica Loopback 0 para establecer la adyacencia, la vía de conexión física sigue siendo la red 192.1.4.0/24 correspondiente a la interfaz serial 3/0. Así también, se puede identificar que la dirección de red de la interfaz Loopback 1 se siegue aprendiendo mediante el protocolo BGP, pero ahora se alcanza mediante la interfaz Loopback 0 de R4 (4.4.4.4). Los demás vecinos no se alteraron, por tanto, las demás entradas de la tabla de enrutamiento permanecen iguales. De otro lado, en la tabla de enrutamiento del router R4 se puede evidenciar que la dirección mediante la cual este se comunica con sus vecinos BGP ha cambiado y ahora corresponde a la dirección de la interfaz Loopback 0 de R3. Se muestra, además, en el resultado del comando ***show ip route,*** la ruta estática que se creó hacia R3.

*Figura 6. Verificación de rutas en R3*

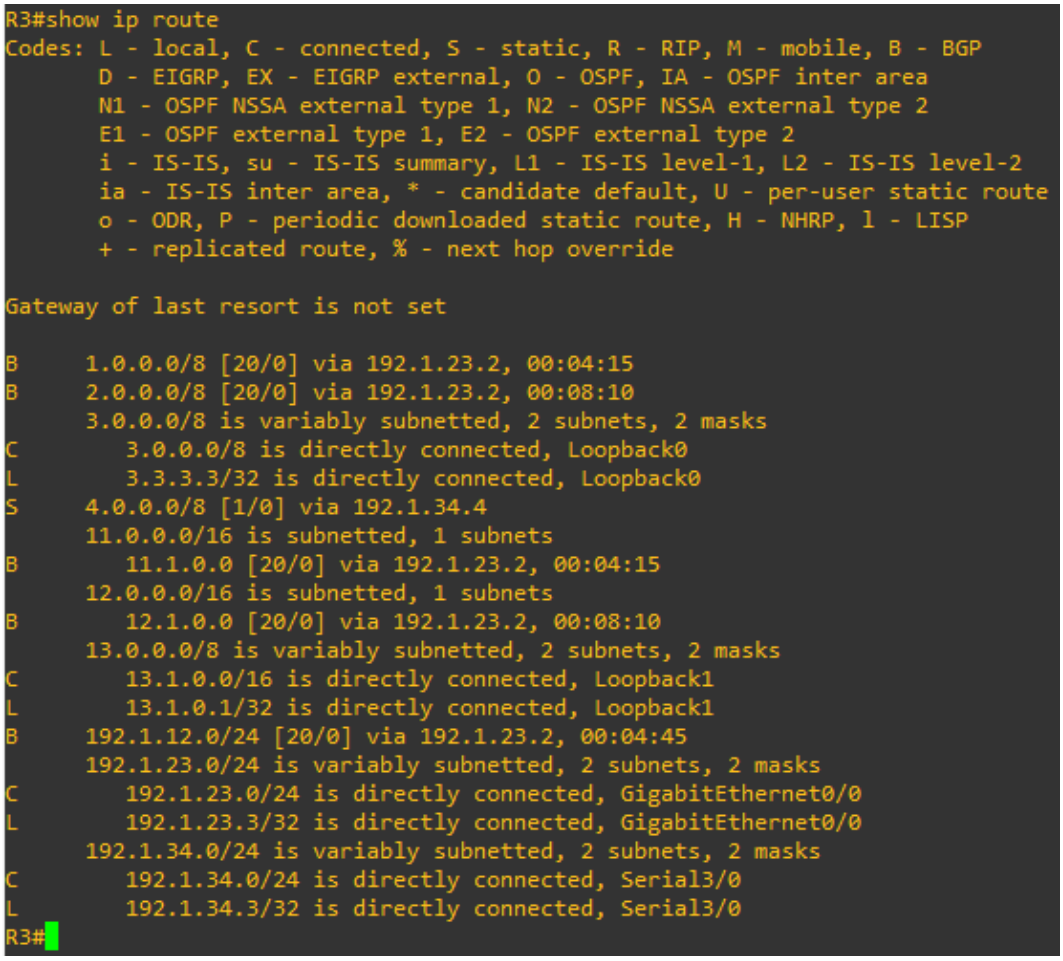
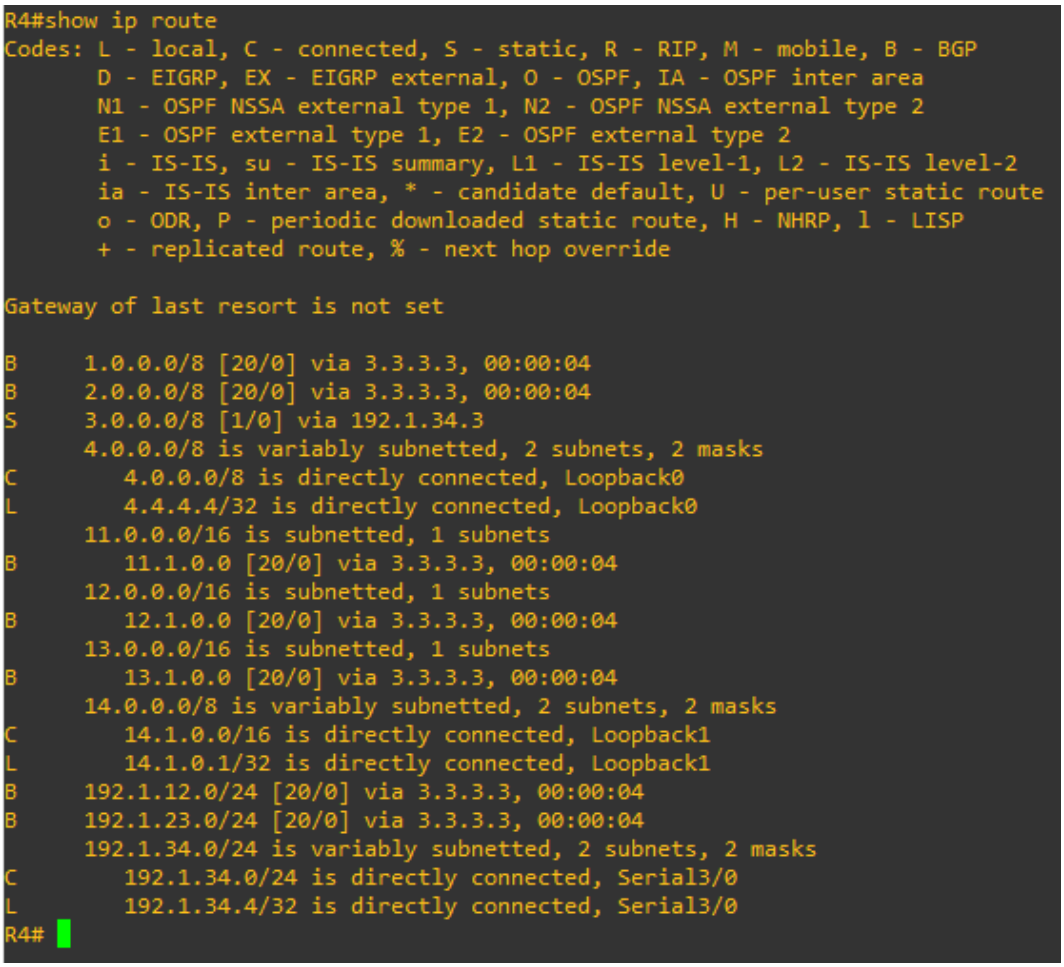


*Figura 7. Verificación de rutas en R4*



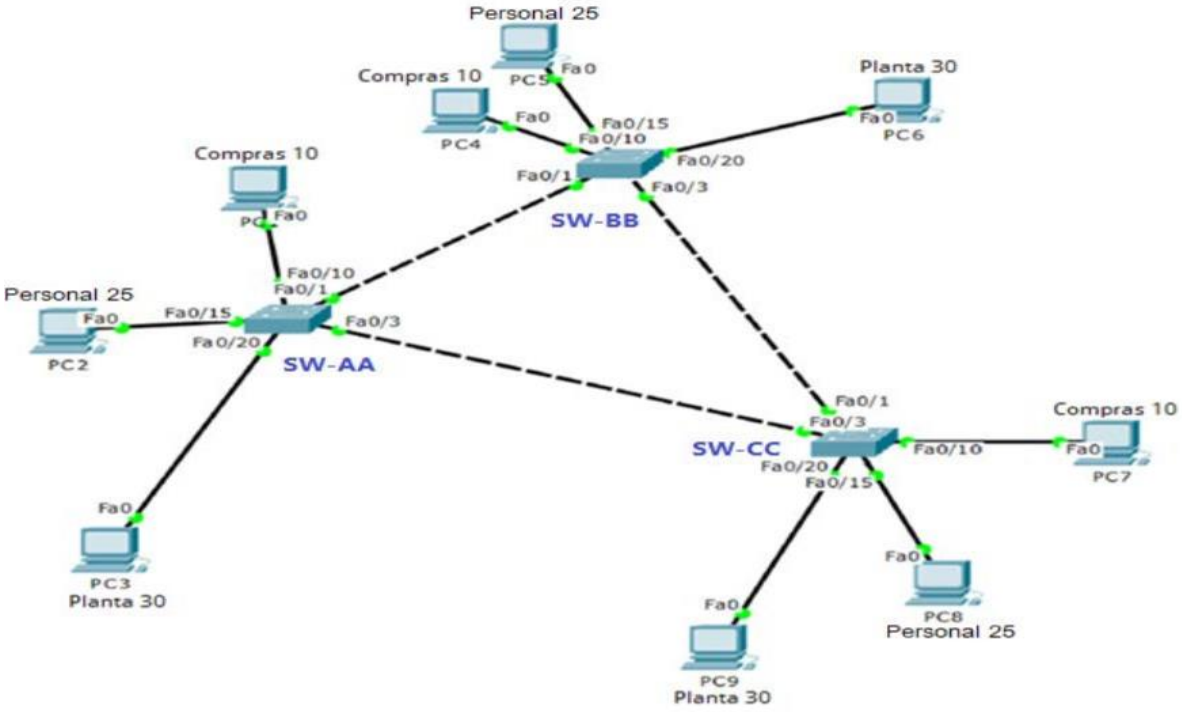
```
R4#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       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 3.3.3.3, 00:00:04
B     2.0.0.0/8 [20/0] via 3.3.3.3, 00:00:04
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 3.3.3.3, 00:00:04
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 3.3.3.3, 00:00:04
      13.0.0.0/16 is subnetted, 1 subnets
B        13.1.0.0 [20/0] via 3.3.3.3, 00:00:04
      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
B     192.1.12.0/24 [20/0] via 3.3.3.3, 00:00:04
B     192.1.23.0/24 [20/0] via 3.3.3.3, 00:00:04
      192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.34.0/24 is directly connected, Serial3/0
L        192.1.34.4/32 is directly connected, Serial3/0
R4#
```

## 2. ESCENARIO DOS

*Figura 8. Topología de red*




### 2.1. **Configurar 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.

**Script requerido**

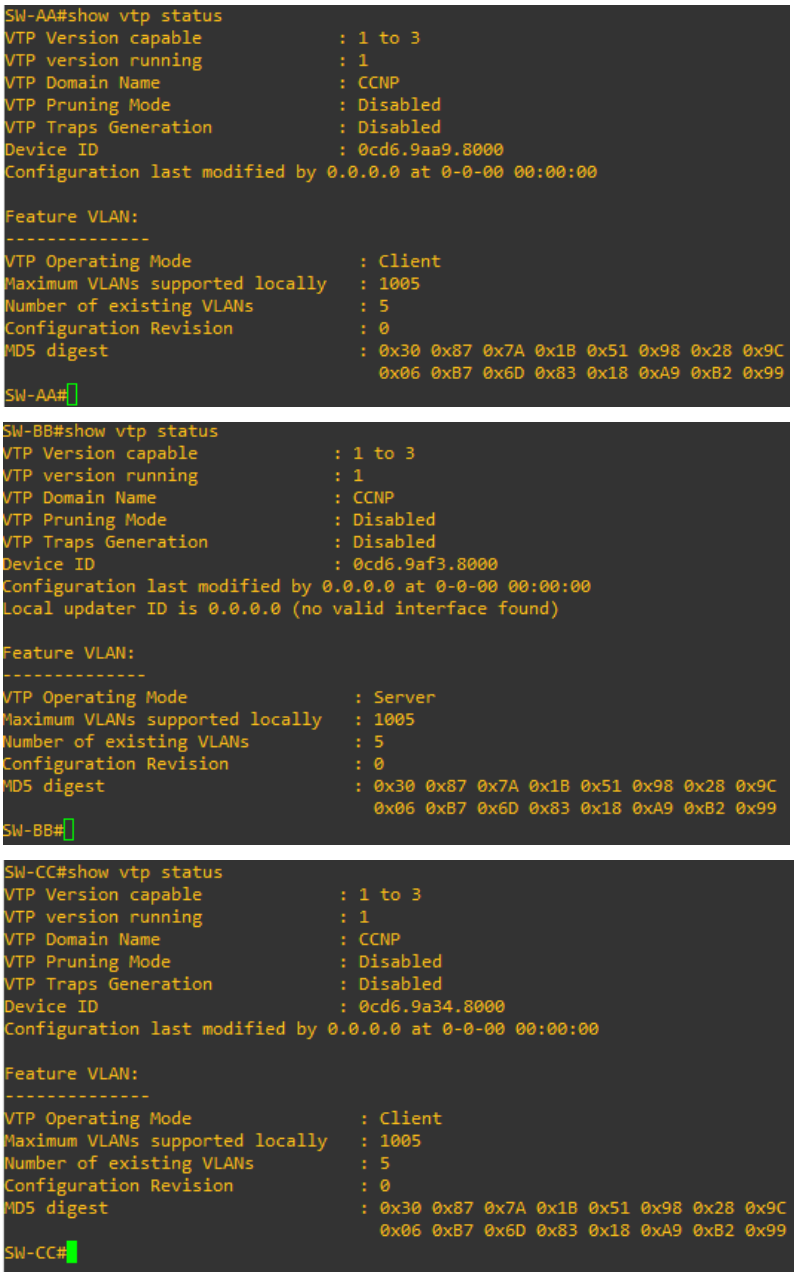
```
SW-AA# configure terminal
SW-AA(config)# vtp mode client
SW-AA(config)# vtp domain CCNP
SW-AA(config)# vtp password cisco

SW-BB# configure terminal
SW-BB(config)# vtp mode server
SW-BB(config)# vtp domain CCNP
SW-BB(config)# vtp password cisco
```

```
SW-CC# configure terminal
SW-CC(config)# vtp mode client
SW-CC(config)# vtp domain CCNP
SW-CC(config)# vtp password cisco
```

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

*Figura 9. Verificación de estado de VTP*



## 2.2. **Configurar DTP (Dynamic Trunking Protocol)**

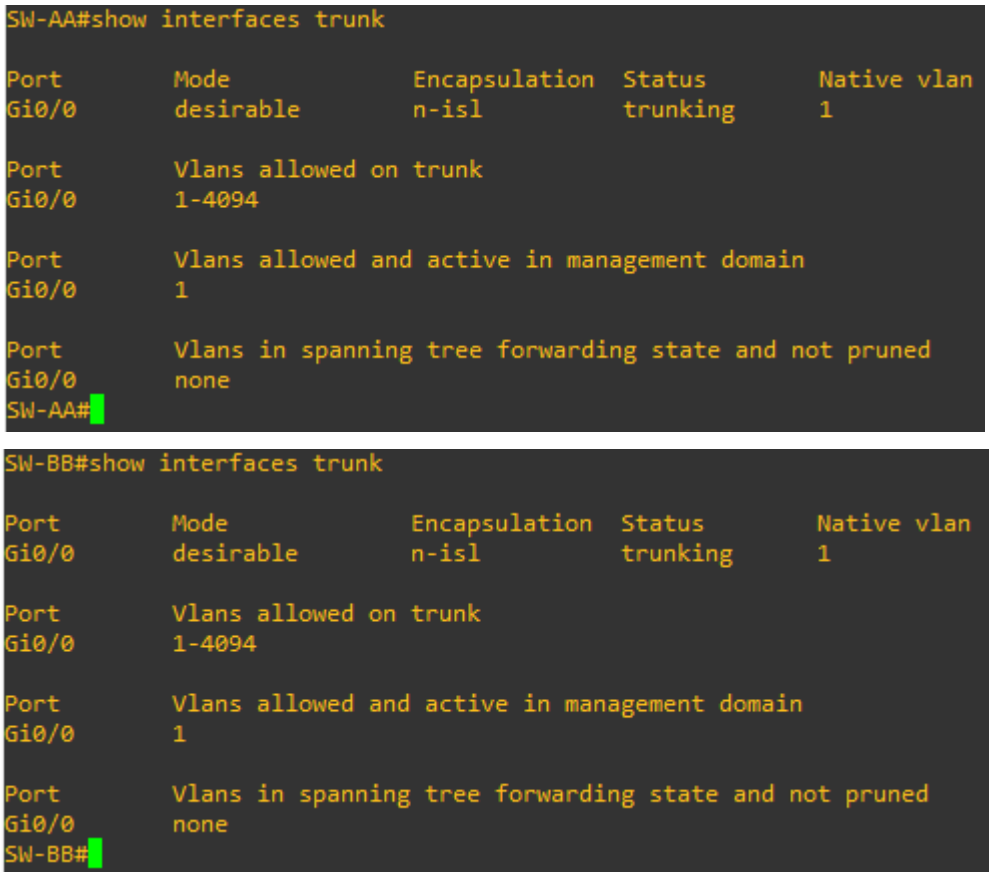
Configure un enlace troncal ("trunk") dinámico entre SW-AA y SW-BB. Debido a que el modo por defecto es dynamic auto, solo un lado del enlace debe configurarse como dynamic desirable.

SW-AA# configure terminal
SW-AA(config)# interface GigabitEthernet 0/0
SW-AA(config)# switchport mode dynamic desirable

SW-BB# configure terminal
SW-BB(config)# interface GigabitEthernet 0/0
SW-BB(config)# switchport mode dynamic desirable

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

*Figura 10. Verificación de enlace trunk*



## 2.3. **Configuración de enlace troncal entre SW-AA y SW-BB.**

Entre SW-AA y SW-BB configure un enlace "trunk" estático utilizando el comando switchport mode trunk en la interfaz F0/3 de SW-AA. Cabe anotar que teniendo en cuenta que la simulación se realiza en GNS3, se utliliza una numeración de puertos diferente pero el resultado es el mismo:

```
SW-AA#configure terminal
SW-AA(config)#interface GigabitEthernet 0/1
SW-AA(config-if)#switchport mode trunk
SW-AA(config-if)#switchport trunk encapsulation dot1q
SW-AA(config-if)#switchport mode trunk
```

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

*Figura 11. Verificación de enlace "trunk" en SW-AA*

```
SW-AA#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi0/0       desirable        n-isl          trunking      1
Gi0/1       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Gi0/0       1-4094
Gi0/1       1-4094

Port        Vlans allowed and active in management domain
Gi0/0       1
Gi0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/0       1
Gi0/1       1
SW-AA#
```

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

```
SW-BB#configure terminal
SW-BB(config)#interface GigabitEthernet 0/2
SW-BB(config-if)#switchport mode trunk
SW-BB(config-if)#switchport trunk encapsulation dot1q
SW-BB(config-if)#switchport mode trunk
SW-CC#configure terminal
SW-CC(config)#interface GigabitEthernet 0/2
SW-CC(config-if)#switchport mode trunk
```

```
SW-CC(config-if)#switchport trunk encapsulation dot1q
SW-CC(config-if)#switchport mode trunk
```

### 2.4. **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-BB#conf ter
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
```

Verifique que las VLANs han sido agregadas correctamente.

*Figura 12. Verificación de VLANs han sido agregadas*

```
SW-BB#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/1, Gi0/3, Gi1/0, Gi1/1
                                                Gi1/2, Gi1/3, Gi2/0, Gi2/1
                                                Gi2/2, Gi2/3, Gi3/0, Gi3/1
                                                Gi3/2, Gi3/3
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
SW-BB#
```

### 2.5. **Asociación de puertos.**

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

*Tabla 1: asociación de puertos*

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

**Script requerido**

```
SW-AA#configure terminal
SW-AA(config)# interface GigabitEthernet 0/3
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config)# interface GigabitEthernet 1/0
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config)# interface GigabitEthernet 1/1
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30

SW-BB#configure terminal
SW-BB(config)# interface GigabitEthernet 0/3
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
SW-BB(config)# interface GigabitEthernet 1/0
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config)# interface GigabitEthernet 1/1
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30

SW-CC#configure terminal
SW-CC(config)# interface GigabitEthernet 0/3
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config)# interface GigabitEthernet 1/0
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config)# interface GigabitEthernet 1/1
SW-CC(config-if)#switchport mode access
```

SW-CC(config-if)#switchport access vlan 30

### 2.6. Configuración de puertos en acceso a VLAN 10.

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

**Script en PC's de GNS3**

PC1> ip 190.108.10.1/24
PC4> ip 190.108.10.2/24
PC7> ip 190.108.10.3/24

### 2.7. Configuración de puertos en acceso.

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

**Script en PC's de GNS3**

PC2> ip 190.108.20.1/24
PC3> ip 190.108.30.1/24
PC5> ip 190.108.20.2/24
PC6> ip 190.108.30.2/24
PC8> ip 190.108.20.3/24
PC9> ip 190.108.30.3/24

### 2.8. 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 2: Configuración interface vlan SVI*

| Equipo | Interfaz | Dirección IP | Máscara |
|---|---|---|---|
| SW-AA | VLAN 99 | 190.108.99.1 | 255.255.255.0 |
| SW-BB | VLAN 99 | 190.108.99.2 | 255.255.255.0 |
| SW-CC | VLAN 99 | 190.108.99.3 | 255.255.255.0 |

## 2.9. Verificar la conectividad Extremo a Extremo.

*Figura 13. Prueba de conectividad entre PC1 y PC2 – PC9*

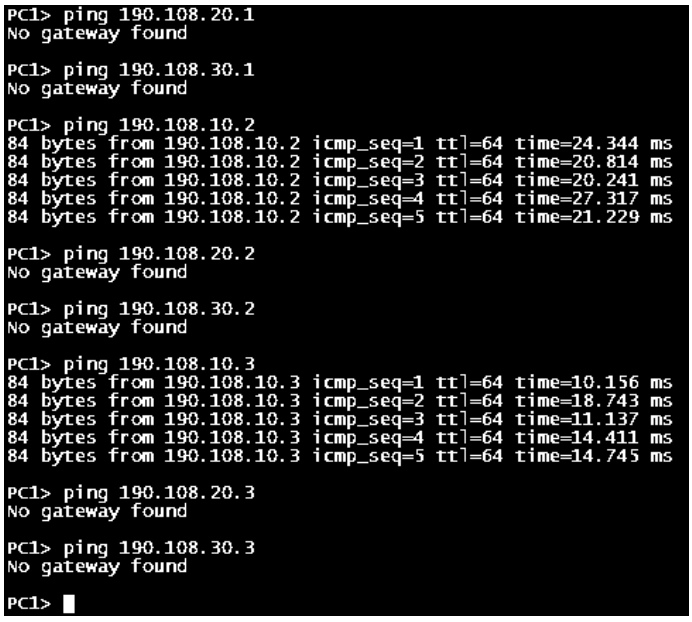



*Figura 14. Prueba de conectividad entre PC2 y PC1, PC3 – PC9*

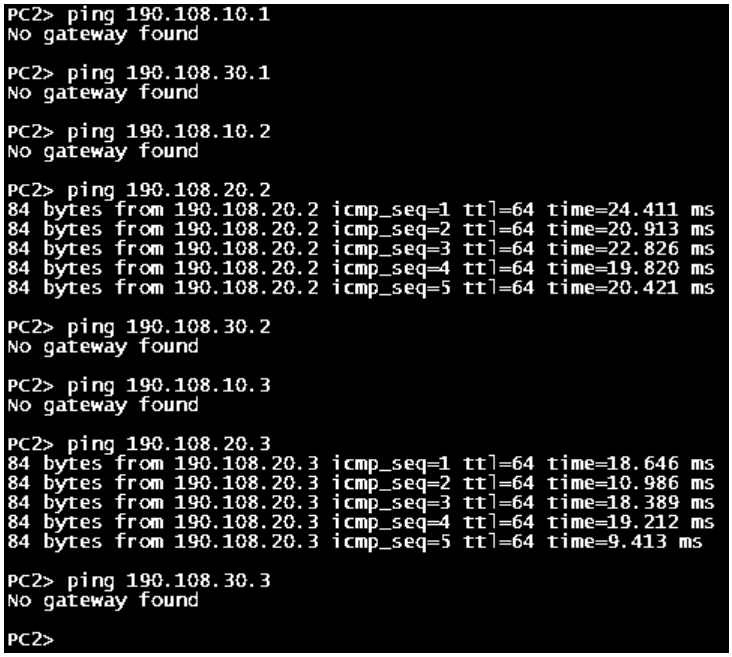


*Figura 15. Prueba de conectividad entre PC3 y PC1, PC2, PC4 – PC9*

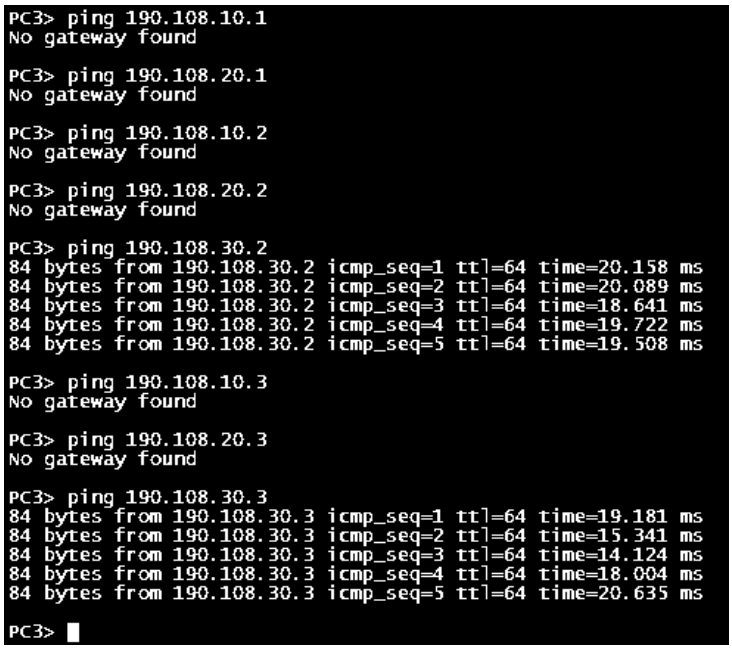



*Figura 16. Prueba de conectividad entre PC4 y PC1-PC3, PC5 – PC9*

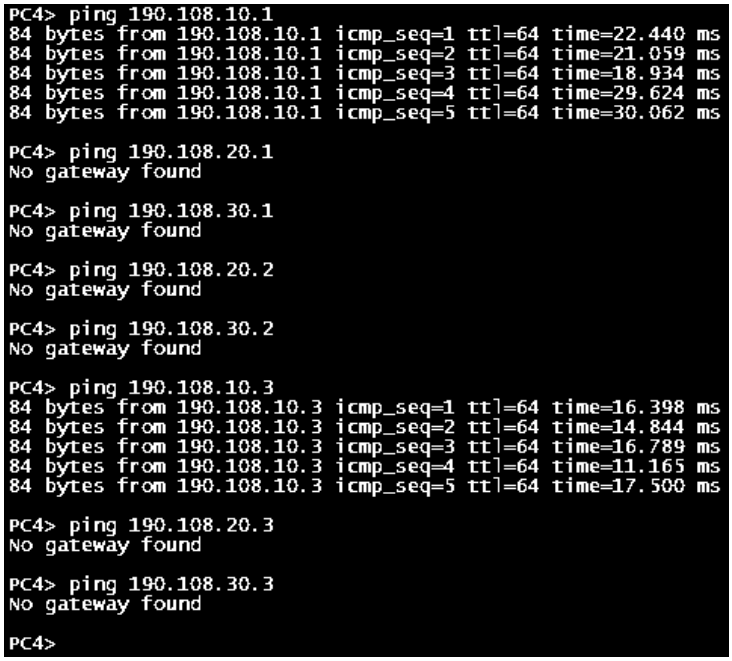


*Figura 17. Prueba de conectividad entre PC5 y PC1-PC4, PC6 – PC9*

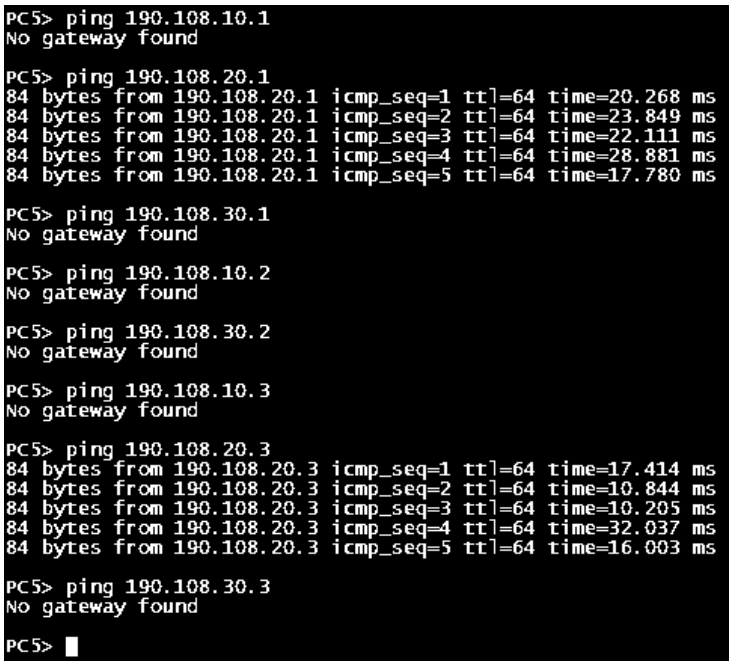



*Figura 18. Prueba de conectividad entre PC6 y PC1-PC5, PC7 – PC9*

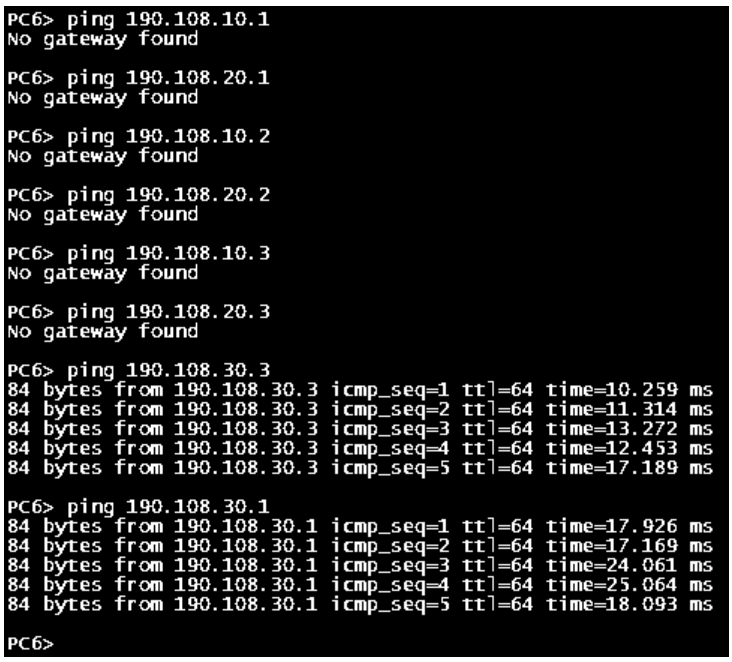


*Figura 19. Prueba de conectividad entre PC7 y PC1-PC6, PC8, PC9*

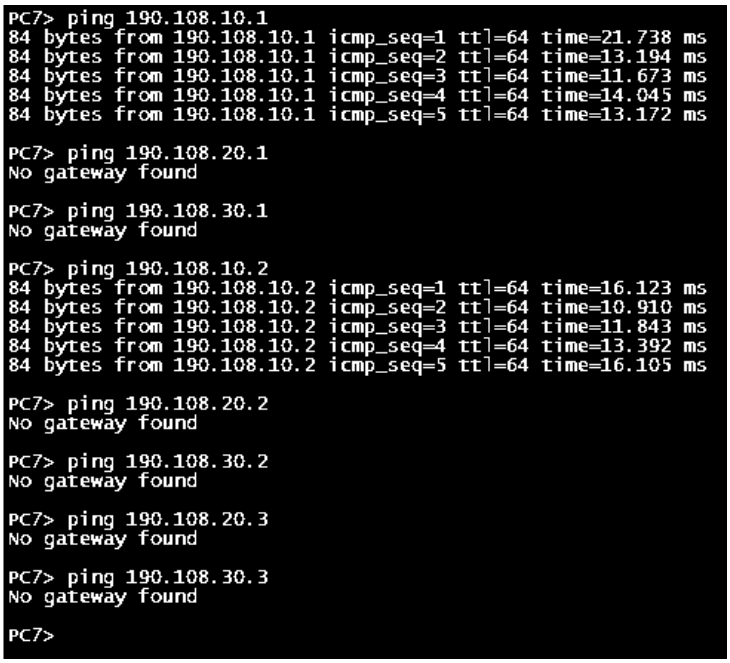



*Figura 20. Prueba de conectividad entre PC8 y PC1-PC7, PC9*

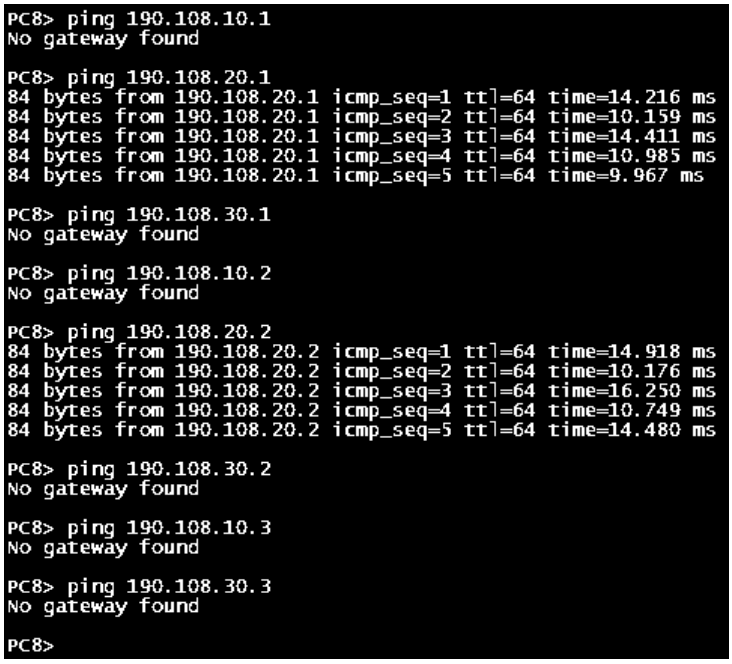
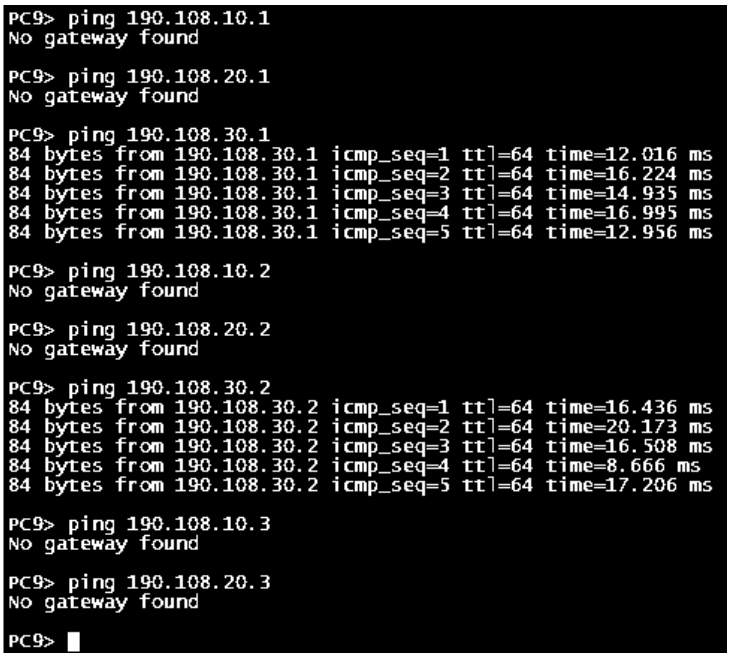


*Figura 21. Prueba de conectividad entre PC9 y PC1-PC8*




De acuerdo a lo que se pudo observar en las imágenes, podemos observar que los pings exitosos se dieron entre los nodos que se encontraban dentro de una misma red, los que no, se encontraban en redes diferentes, por eso el output era ***"No gateway found"***

### 2.10. **Prueba de conectividad entre switches.**

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

*Figura 22. Prueba de conectividad entre SW-AA y SW-BB, SW-CC.*

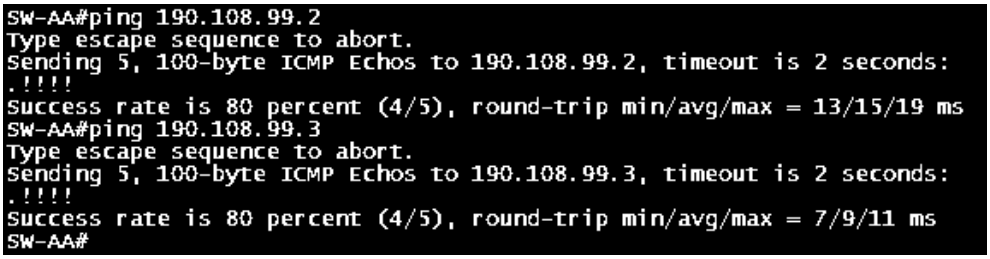


*Figura 23. Prueba de conectividad entre SW-BB y SW-AA, SW-CC.*

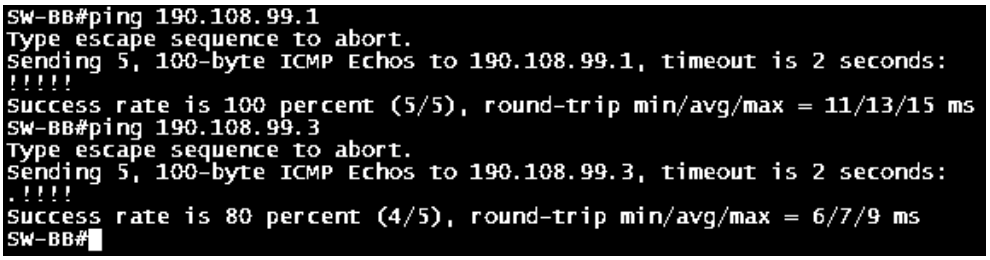
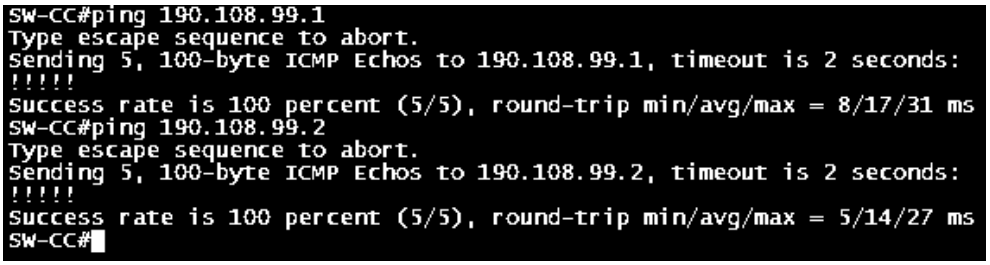



*Figura 24. Prueba de conectividad entre SW-CC y SW-AA, SW-BB.*




Las pruebas fueron exitosas, dado que cada switch tiene un SVI sobre la vlan 99 cuyo nombre es Admon.

## 2.11. **Prueba de conectividad entre switches y PS's.**

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

*Figura 25. Verificación de conectividad entre SW-AA y PC1-PC9.*

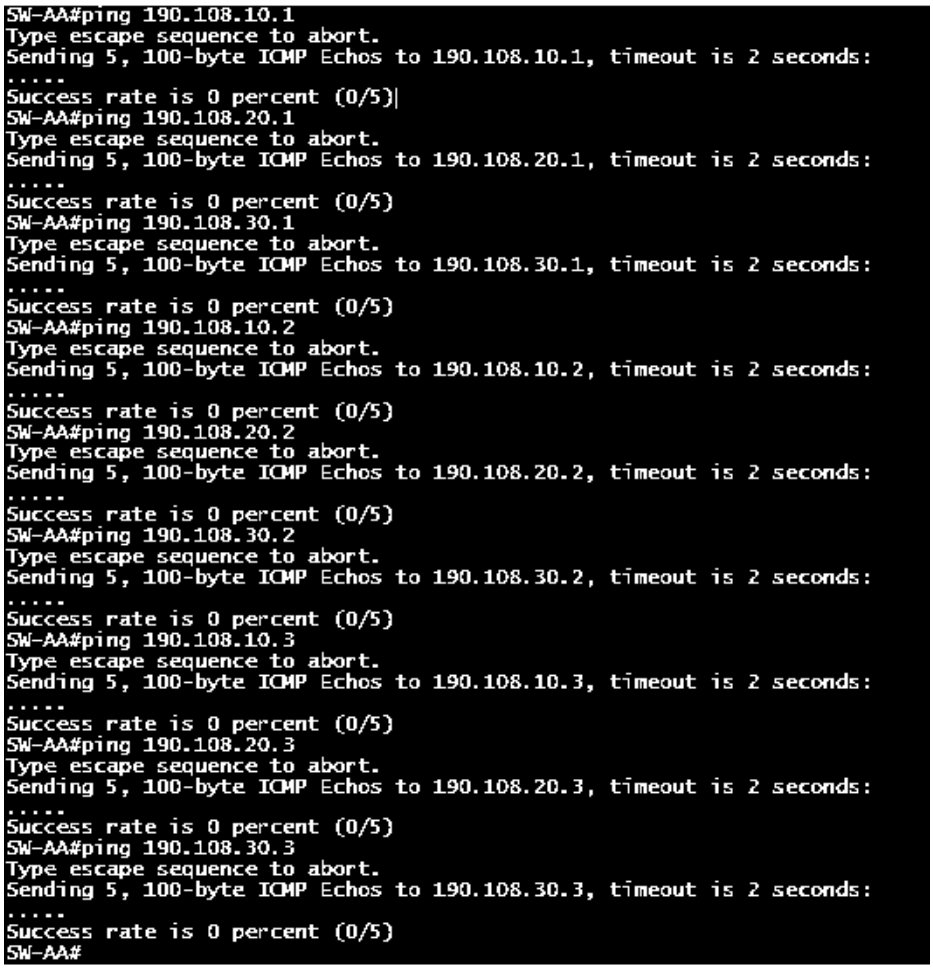


*Figura 26. Verificación de conectividad entre SW-BB y PC1-PC9.*

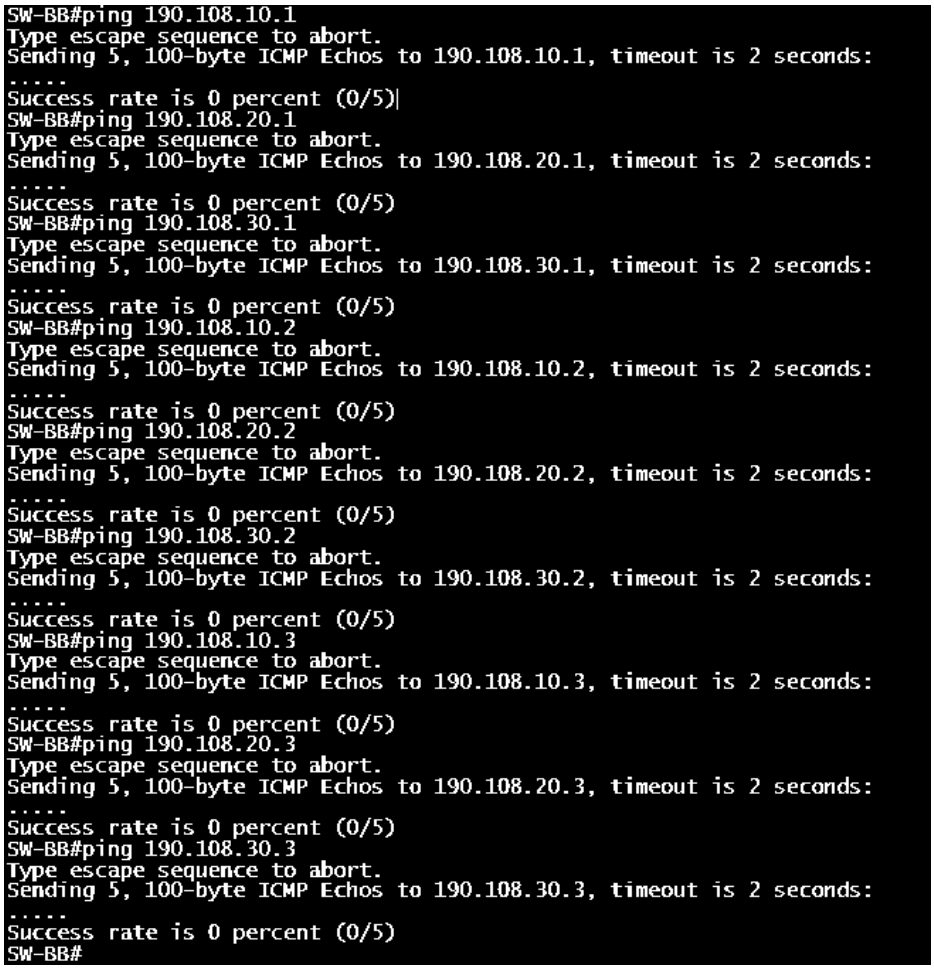
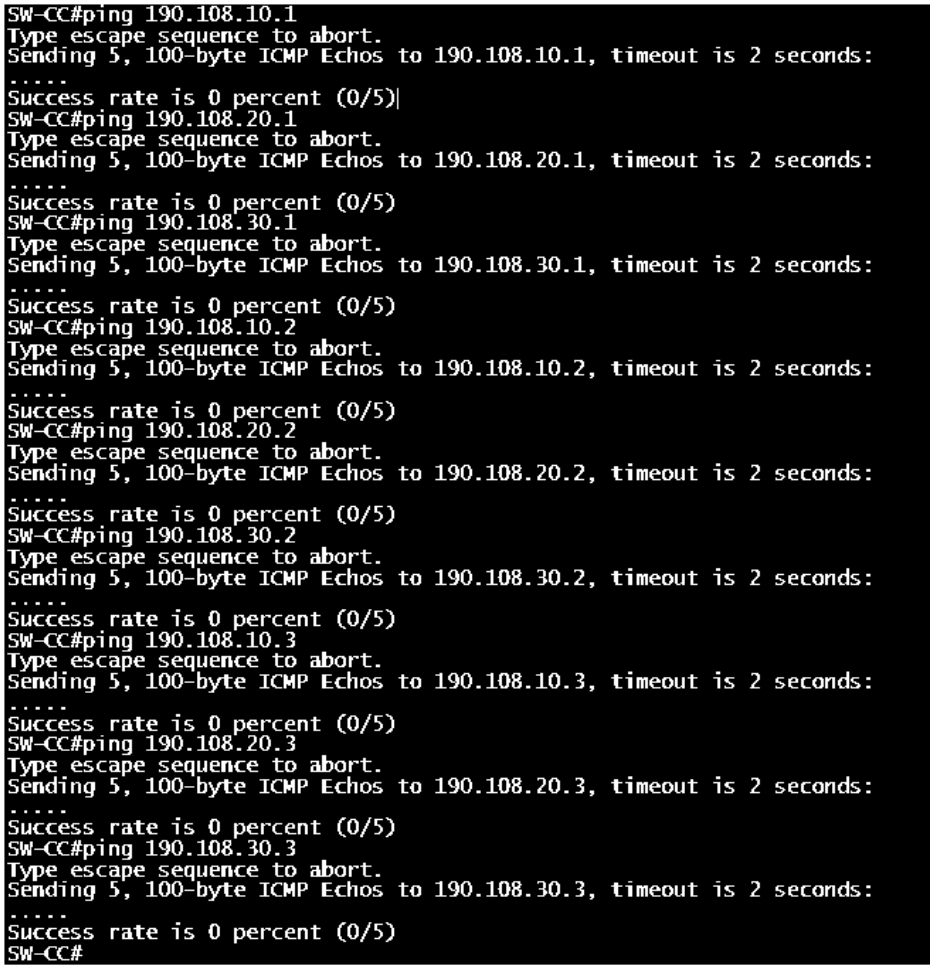


*Figura 27. Verificación de conectividad entre SW-CC y PC1-PC9.*




Los ping no fueron exitosos, debido a que ninguno de los switches tiene configurada una interface vlan sobre la vlan correspondiente a cada switch, para solucionar esto, se debe configurar una ip en cada switch para cada vlan y si se desea además comunicación entre diferentes redes, se debe habilitar el routing entre vlans en alguno de los switches.

# CONCLUSIONES

El uso de protocolos de enrutamiento dinámico nos permite el aprendizaje rápido de la topología de red por la cual estemos pasando y la cantidad de saltos posibles para alcanzar un destino.

Como elemento de seguridad el uso de Vlan nos permite la segmentación adecuada de una red limitando el acceso a los recursos que sean absolutamente necesarios y logrando una división basada en departamentos, servicios o localidades.

Se debe poseer especial cuidado al momento de implementar un esquema de red usando el protocolo VTP ya que al ser el aprendizaje de Vlan dinámico, la introducción de un nuevo Switch con un número de revisión más alto puede afectar el funcionamiento y generar indisponibilidad.

En un ambiente empresarial de alta envergadura donde la disponibilidad de los servicios posee una alta demanda se hace necesaria la implementación de soluciones redundantes donde soluciones como HSRP para los Router y Etherchannel aparecen como alternativas eficientes para dar solución a esta necesidad.

# BIBLIOGRAFIA


Configuración DHCP en Router (s.f), 27 de Mayo de 2018, recuperado de https://apuntesdecisco.blogspot.com/2008/07/configuracin-de-dhcp-en- lrouter.html

Froom, R., Frahim, E. (2015). CISCO Press (Ed). InterVLAN Routing. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115.

Froom, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115.

Gerometta Oscar, (2015), 28 de Junio, Que es una SVI, recuperado de http://librosnetworking.blogspot.com/2015/06/que-es-una-svi.html

HSRP Versión 2 (s.f), 27 Mayo de 2018, recuperado de https://www.cisco.com/c/en/us/td/docs/ios-ml/ios/ipapp_fhrp/configuration/xe3s/fhp-xe-3s-book/fhp-hsrp-v2.html

Morales, J. M. Introduccción al CLI en routers y switches cisco. Recuperado de: https://pics.unlugarenelmundo.es/hechoencasa/CLI%20en%20Routers%20y%20Switches%20Cisco.pdf