DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

VICTOR HUGO PERDOMO MORENO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRÓNICA
BOGOTÁ D.C.
2020

DIPLOMADO DE PROFUNDIZACIÓN CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

VICTOR HUGO PERDOMO MORENO

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

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
INGENIERÍA ELECTRÓNICA
BOGOTÁ D.C.
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá D.C., 22 de mayo de 2020

AGRADECIMIENTOS

Solo puedo decir gracias, primero a Dios por darme la voluntad de trabajar cada día para ser una mejor persona, capaz de generar conciencia y siempre con la voluntad de aportar los conocimientos adquiridos al crecimiento de la sociedad.

En segundo lugar a mi familia, por tanto apoyo incondicional, por no dejarme caer cuando llegue a pensar en abandonar en medio de altas cargas laborales y dificultades para acceder a la plataforma, debido a los diferentes sitios en los que me encontraba desempeñando mi cargo como militar, porque siempre me brindaron las fuerzas para continuar hasta ver cumplido mi sueño.

Finalmente a la Universidad Abierta y a Distancia, que brinda esta oportunidad a personas que como yo no podemos asistir de manera presencial y nos permite crecer a nivel educativo, preparándonos para desarrollar nuestra profesiones en un ambiente laboral competitivo.

A todos los compañeros con quienes trabajamos para cumplir una a una las actividades de cada curso, siempre encaminados a la misma meta.

A todos, gracias.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

BGP: es un protocolo de gateway exterior (EGP), usado para realizar el ruteo entre dominios en las redes TCP/IP.

CCNP: Cisco Certified Network Professional.

Conectividad: capacidad de establecer una conexión: una comunicación, un vínculo. El concepto suele aludir a la disponibilidad que tiene de un dispositivo para ser conectado a otro o a una red.

Dynamic Trunking Protocol: se utiliza para negociar la formación de un enlace troncal entre dos dispositivos Cisco. DTP provoca un aumento del tráfico y está habilitado de forma predeterminada, pero puede deshabilitarse.

GNS3: Es un simulador gráfico de red lanzado en 2008, que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos, permitiendo la combinación de dispositivos tanto reales como virtuales.

IP: La IP se traduce por Internet Protocol, protocolo de Internet en español, y se trata de un protocolo utilizado para la comunicación de datos a través de una red de paquetes combinados.

Loopback: interfaz de red virtual, Las direcciones de loopback pueden ser redefinidas en los dispositivos, incluso con direcciones IP públicas, una práctica común en los routers. y son usualmente utilizadas para probar la capacidad de la tarjeta interna si se están enviando datos BGP.

Networking: es la integración de dos sistemas de redes completas. Una red consiste en dos o más computadoras unidas que comparten recursos como archivos, CD-Roms o impresoras, y que son capaces de realizar comunicaciones electrónicas. Las redes están unidas por cable, líneas de teléfono, ondas de radio, satélite, etc.

Trunk: es una configuración de canal para puertos de switch que estén en una red Ethernet, que posibilita que se pueda pasar varias VLAN por un único link, o sea, un link de troncal es un canal que puede ser switch-switch o switch-router, por donde se pasan informaciones originadas y con destino a más de una VLAN.

VLAN: acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red 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.

RESUMEN

El Diplomado de CCNP de Cisco es una valiosa herramienta a utilizar como futuro ingeniero, en el cual se involucran una serie de capacidades que sobre todo resaltan la capacidad de análisis de una situación para presentar una solución viable en aspectos de enrutamiento y conmutación; para esto, hay dos escenarios los cuales se van a simular en el Software GNS3, en donde el primero se trabajará con cuatro routers, estableciendo una configuración de vecino BGP, a la cual se ira sumando los demás, hasta establecer una conectividad total; en el segundo escenario se utilizaran tres switch's y nueve PC's, realizando configuración VTP y DTP, asignando VLANs y direcciones IP de acuerdo a lo indicado, para finalmente poder hacer una verificación del enrutamiento extremo a extremo con la que se analizaran las características de la red, logrando de esta manera construir conocimiento por medio de la práctica, la experiencia y el análisis del funcionamiento de una red.

Palabras Claves: CCNP, CISCO, BGP, GNS3, Conmutación, Enrutamiento, VTP, DTP, VLANs, Conectividad, red.

ABSTRACT

The Cisco CCNP Course is a valuable tool to use as a future engineer, whereby involves a series of capabilities that above all emphasize the ability to analyze a situation to present a viable solution in routing and switching aspects; For this, there are two scenarios whereby will be pretend in the GNS3 Software, where the first one works with four routers, establishing a BGP neighbor configuration, to which the others will be added, until establishing full connectivity; In the second scenario, three switches and nine PCs will be used, VTP and DTP configuration, assigning VLANs and IP addresses as indicated, to finally be able to do a verification of the extreme routing with which the characteristics of the network will be analyzed, achieving this way to build knowledge through the practice, experience and analysis of the operation of a network**.**

Keywords: CCNP, CISCO, BGP, GNS3, routing, switching, VTP, DTP, VLAN, Connectivity, Network.

INTRODUCCIÓN

El Presente documento unifica de manera resumida el objetivo del Diplomado CCNP, mediante la capacidad de comprensión y análisis de una situación para poder presentar soluciones que incluyan diversos aspectos de Networking, circunstancia que se establece como el fin principal del mismo.

Dentro de este desarrollo se encuentra principalmente un escenario que conlleva a la aplicación de conocimientos adquiridos en el módulo de routing, en el cual se presenta la configuración de las características básicas de la conectividad entre routers, para pasar a configurar una relación de vecino BGP entre los diferentes routers, que se irán probando una a una hasta establecer la comunicación total.

Asimismo, como segundo escenario se aplicarán conceptos relacionados con switching, inicialmente se utilizaran las configuraciones básicas a cada uno de los switch's para usar VTP en las actualizaciones de VLAN y dominio CCNP.

Posteriormente, se realizará una configuración DTP (Dynamic Trunking Protocol), con lo cual se busca generar el canal de conectividad entre los diferentes switch's, utilizando diferentes modos de conexión como dynamic auto, trunk y dynamic desirable.

Esta red de switch's, contiene una serie de PC's, los cuales representan algunas áreas comunes entre sí, a estos, así como a los switch's se les agregan VLANs y se asignaran puertos, para finalmente hacer una verificación de la conectividad extremo a extremo, sobre la cual en la configuración se pueden evidenciar las causas de existir o no conectividad.

DESARROLLO

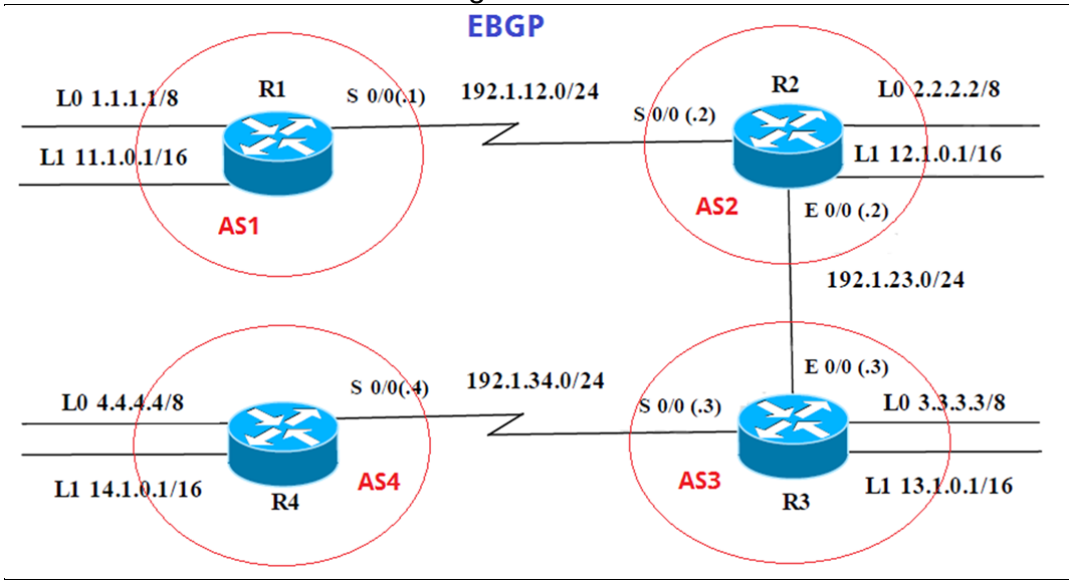
La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNP, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para esta actividad, el estudiante debe realizar las tareas asignadas en cada uno de los dos (2) escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

Teniendo en cuenta que la Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: Packet Tracer , GNS3 o SMARTLAB.

ESCENARIO 1

Figura 1. Escenario 1



Información para configuración de los Routers

R1

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

Tabla No. 1 Información configuración R1

R2

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

Tabla No. 2 Información configuración R2

R3

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

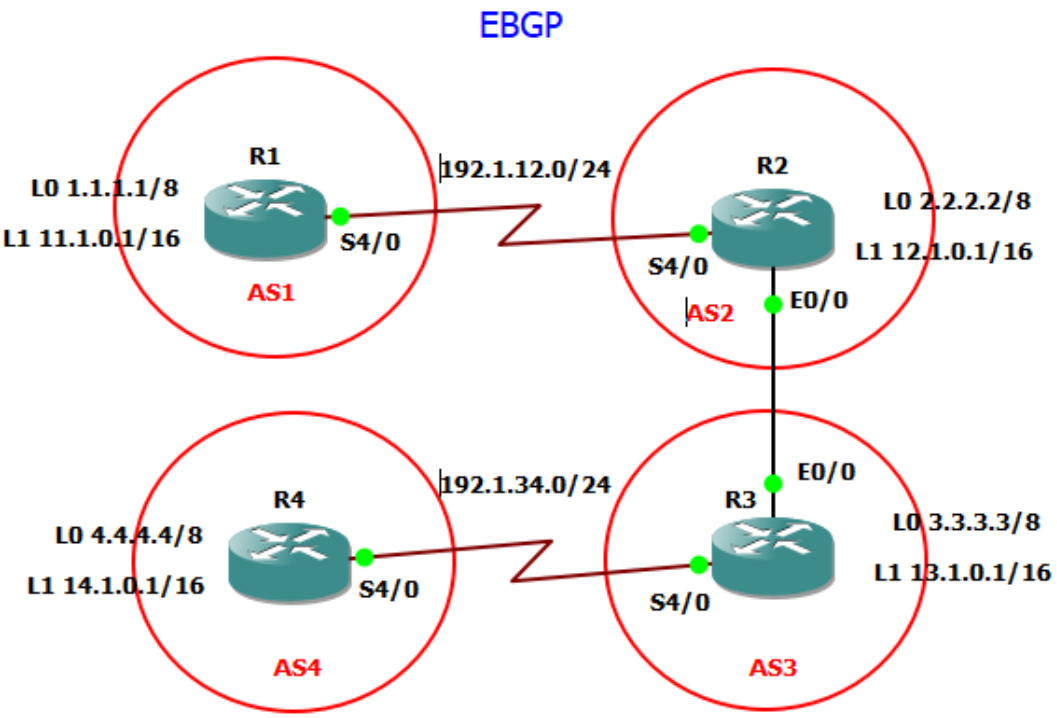
Tabla No. 3 Información configuración R3

R4

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

Tabla No. 4 Información configuración R4

Figura 2. Simulación Escenario 1 en GNS3



https://www.dropbox.com/s/clm4o93syapyhyb/Escenario_1_Victor_Perdomo.rar?dl=0

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

   R1#configure terminal
   R1(config)#interface Loopback0

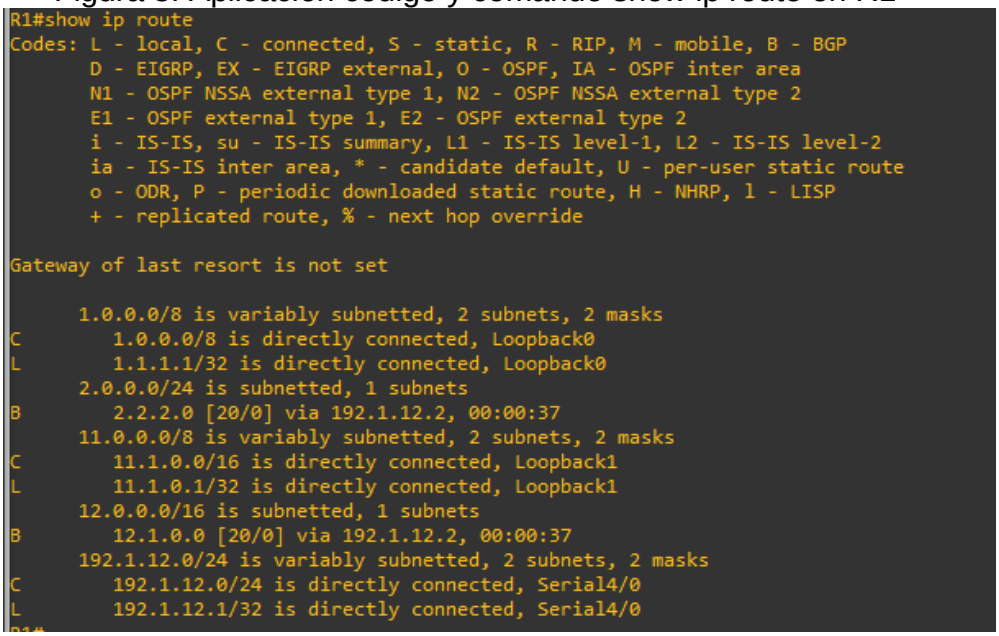
```
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#exit
R1(config)#interface Loopback1
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#exit
R1(config)#interface serial 4/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
R1(config-if)#exit

R2#configure terminal
R2(config)#interface Loopback0
R2(config-if)#ip address 2.2.2.2 255.255.255.0
R2(config-if)#exit
R2(config)#interface Loopback1
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#exit
R2(config)#interface serial 4/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface FastEthernet 0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
```

Se configura la relación de vecino BGP entre R1 y R2:

```
R1(config)#router bgp 1
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#neighbor 192.1.12.2 remote-as 2
R1(config-router)#network 1.1.1.0 mask 255.255.255.0
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router)#exit

R2(config)#router bgp 2
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#neighbor 192.1.23.3 remote-as 3
R2(config-router)#network 2.2.2.0 mask 255.255.255.0
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
R2(config-router)# exit
```

Comprobamos la configuración con el comando show ip route en R1:

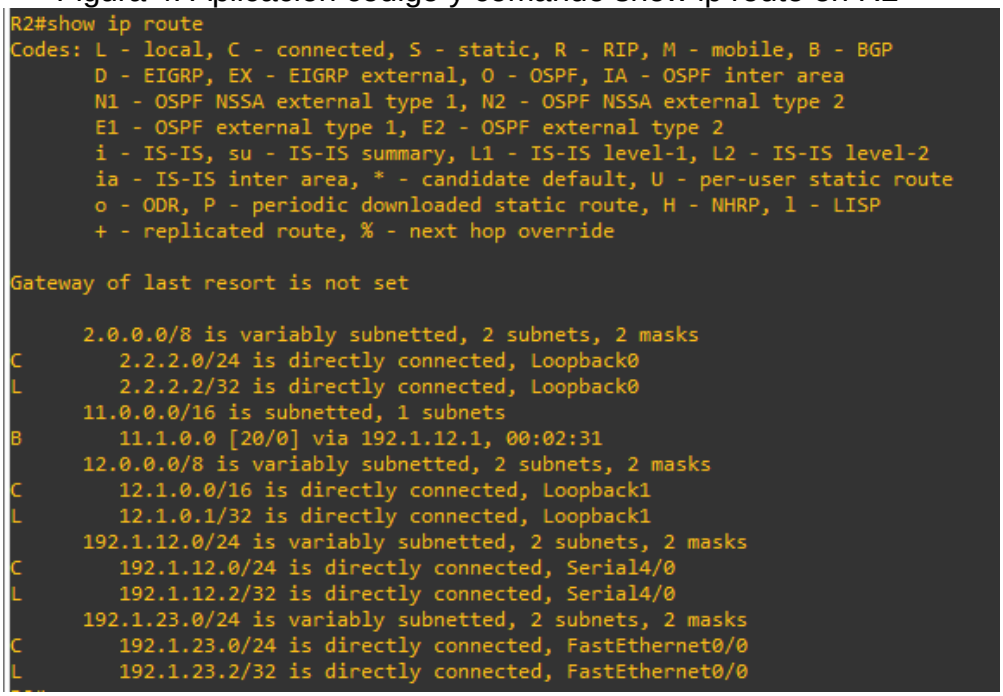
Figura 3. Aplicación código y comando show ip route en R1



```
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
      2.0.0.0/24 is subnetted, 1 subnets
B        2.2.2.0 [20/0] via 192.1.12.2, 00:00:37
      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, 00:00:37
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial4/0
L        192.1.12.1/32 is directly connected, Serial4/0
```

Comprobamos la configuración con el comando show ip route en R2:

Figura 4. Aplicación código y comando show ip route 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        2.2.2.0/24 is directly connected, Loopback0
L        2.2.2.2/32 is directly connected, Loopback0
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.12.1, 00:02:31
      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, Serial4/0
L        192.1.12.2/32 is directly connected, Serial4/0
      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
```

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.

   Se realiza la configuración del Router R3:

```
R3#configure terminal
R3(config)#interface Loopback0
R3(config-if)#ip address 3.3.3.3 255.255.255.0
R3(config-if)#exit
R3(config)#interface Loopback1
R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#exit
R3(config)#interface serial 4/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#clock rate 128000
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface FastEthernet 0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
```

   Se configura la relación faltante de vecino BGP entre R2 y R3:

```
R3(config)#router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#neighbor 192.1.34.4 remote-as 4
R3(config-router)#network 3.3.3.0 mask 255.255.255.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3(config-router)# exit
```

   Comprobamos la configuración con el comando show ip route en R2:

Figura 5. Aplicación código y comando show ip route 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        2.2.2.0/24 is directly connected, Loopback0
L        2.2.2.2/32 is directly connected, Loopback0
      3.0.0.0/24 is subnetted, 1 subnets
B        3.3.3.0 [20/0] via 192.1.23.3, 00:01:47
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.12.1, 00:23:57
      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, 00:01:47
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial4/0
L        192.1.12.2/32 is directly connected, Serial4/0
      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
```

Comprobamos la configuración con el comando show ip route en R3:

Figura 6. Aplicación código y comando show ip route en 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

      2.0.0.0/24 is subnetted, 1 subnets
B        2.2.2.0 [20/0] via 192.1.23.2, 00:00:43
      3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        3.3.3.0/24 is directly connected, Loopback0
L        3.3.3.3/32 is directly connected, Loopback0
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.23.2, 00:00:43
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.23.2, 00:00:43
      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
      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
R3#
```

Al realizar la configuración de vecino en R3, esta se enlaza con la realizada en el paso anterior en R2 y encuentra una ruta de comunicación.

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.

   Se realiza la configuración del Router R4:

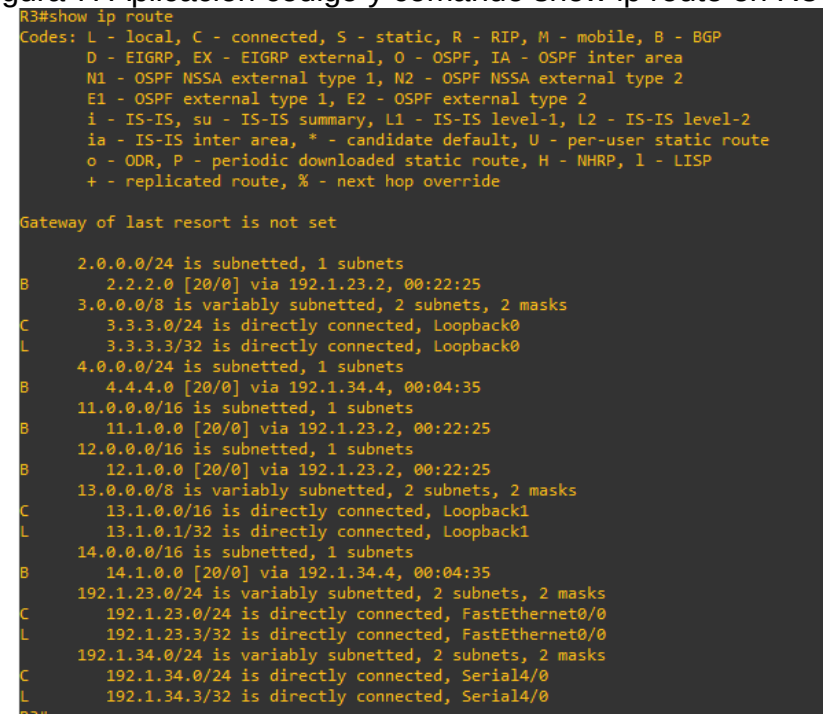
```
R4#configure terminal
R4(config)#interface Loopback0
R4(config-if)#ip address 4.4.4.4 255.255.255.0
R4(config-if)#exit
R4(config)#interface Loopback0
R4(config-if)#ip address 4.4.4.4 255.255.255.0
R4(config-if)#exit
R4(config)#interface Loopback1
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#exit
R4(config)#interface serial 4/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#
```

   Se configura la relación faltante de vecino BGP entre R3 y R4:

```
R4(config)#router bgp 4
R4(config-router)#bgp router-id 66.66.66.66
R4(config-router)#neighbor 192.1.34.3 remote-as 3
R4(config-router)#network 4.4.4.0 mask 255.255.255.0
R4(config-router)#network 14.1.0.0 mask 255.255.0.0
R4(config-router)#exit
```

   Comprobamos la configuración con el comando show ip route en R3:

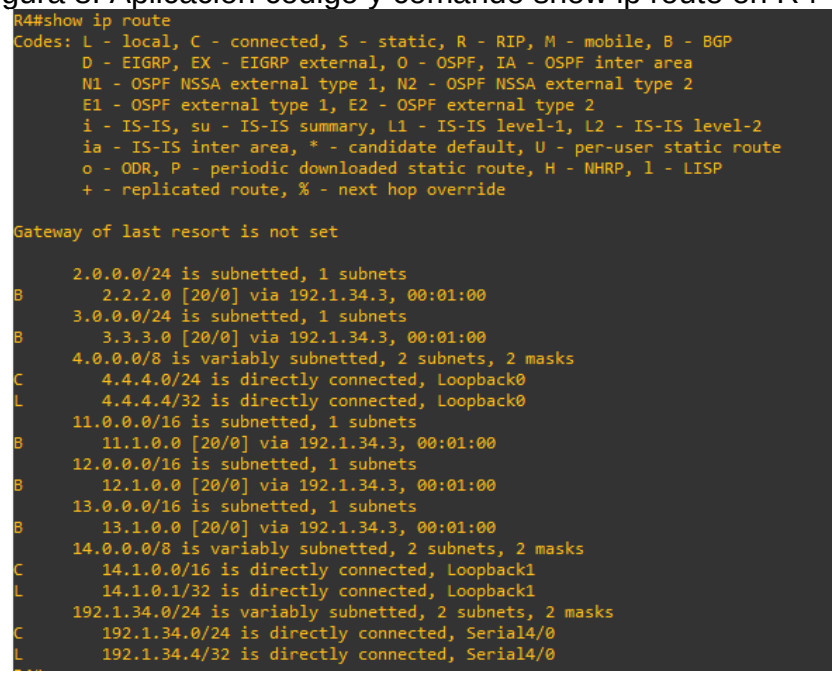
Figura 7. Aplicación código y comando show ip route en R3



```
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

      2.0.0.0/24 is subnetted, 1 subnets
B        2.2.2.0 [20/0] via 192.1.23.2, 00:22:25
      3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        3.3.3.0/24 is directly connected, Loopback0
L        3.3.3.3/32 is directly connected, Loopback0
      4.0.0.0/24 is subnetted, 1 subnets
B        4.4.4.0 [20/0] via 192.1.34.4, 00:04:35
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.23.2, 00:22:25
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.23.2, 00:22:25
      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, 00:04:35
      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, Serial4/0
L        192.1.34.3/32 is directly connected, Serial4/0
```

Comprobamos la configuración con el comando show ip route en R4:

Figura 8. Aplicación código y comando show ip route 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

      2.0.0.0/24 is subnetted, 1 subnets
B        2.2.2.0 [20/0] via 192.1.34.3, 00:01:00
      3.0.0.0/24 is subnetted, 1 subnets
B        3.3.3.0 [20/0] via 192.1.34.3, 00:01:00
      4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        4.4.4.0/24 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, 00:01:00
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.34.3, 00:01:00
      13.0.0.0/16 is subnetted, 1 subnets
B        13.1.0.0 [20/0] via 192.1.34.3, 00:01:00
      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, Serial4/0
L        192.1.34.4/32 is directly connected, Serial4/0
```

Al realizar la configuración de vecino en R4, esta se enlaza con la realizada en el paso anterior en R3 y encuentra una ruta de comunicación.

ESCENARIO 2

Figura 9. Escenario 2

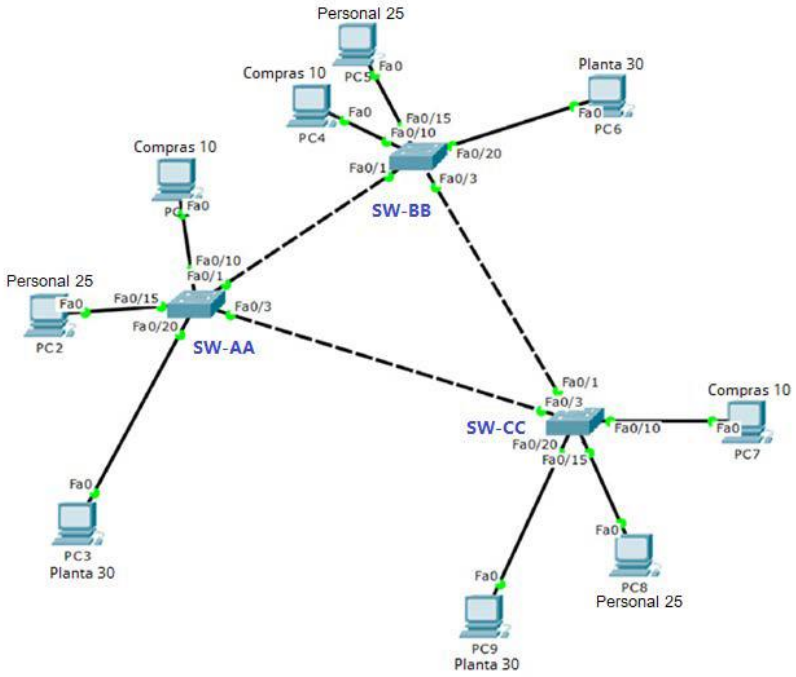
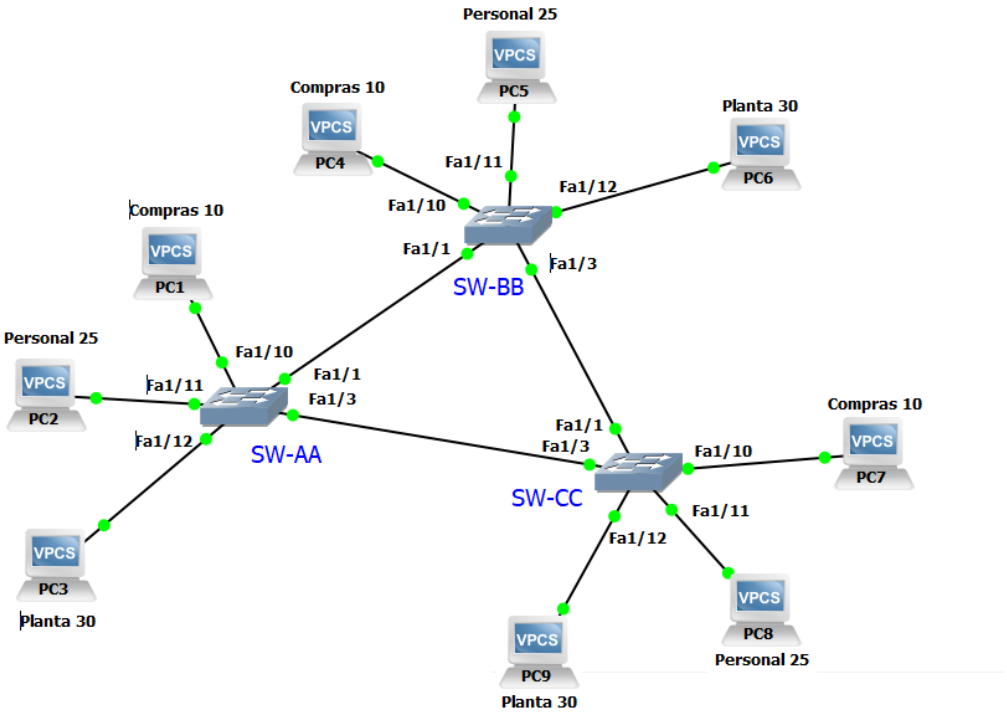


Figura 10. Simulación Escenario 2 en GNS3



https://www.dropbox.com/s/2xj9d8t39sz8mvd/Escenario_2_Victor_Perdomo.rar?dl=0

A. Configurar VTP

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

   Se configura el Switch SW-AA:

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

   Se configura el Switch SW-BB:

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

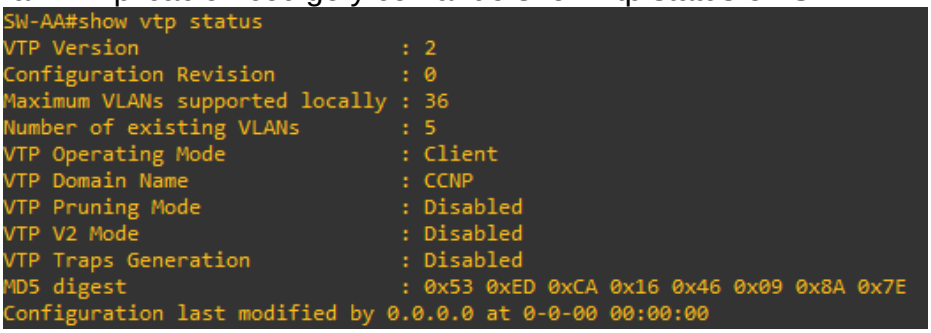
   Se configura el Switch SW-CC:

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

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

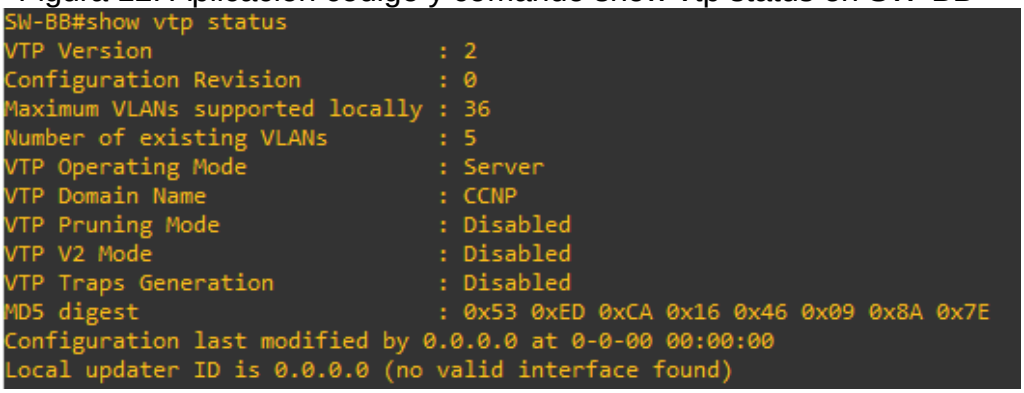
   Se verifica la configuración de SW-AA con el comando show vtp status:

   Figura 11. Aplicación código y comando show vtp status en SW-AA



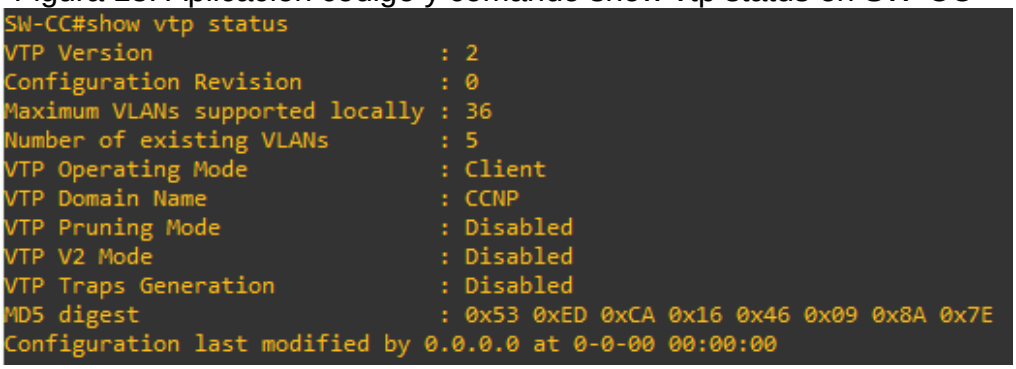
Se verifica la configuración de SW-BB con el comando show vtp status:

Figura 12. Aplicación código y comando show vtp status en SW-BB



Se verifica la configuración de SW-CC con el comando show vtp status:

Figura 13. Aplicación código y comando show vtp status en SW-CC



B. Configurar DTP (Dynamic Trunking Protocol)

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

Se configura el enlace en SW-AA:

SW-AA#configure terminal
SW-AA(config)#interface Fa1/1
SW-AA(config-if)#switchport trunk encapsulation dot1q
SW-AA(config-if)#end

Se configura el enlace en SW-BB como dynamic desirable:

```
SW-BB#configure terminal
SW-BB(config)#interface Fa1/1
SW-BB(config-if)#switchport trunk encapsulation dot1q
SW-BB(config-if)#switchport mode desirable
SW-BB(config-if)#end
```

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

Figura 14. Aplicación código y comando show interfaces trunk en SW-AA

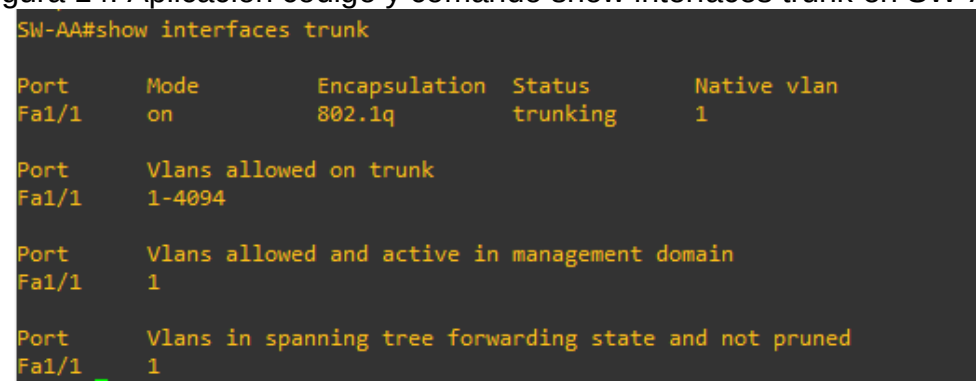
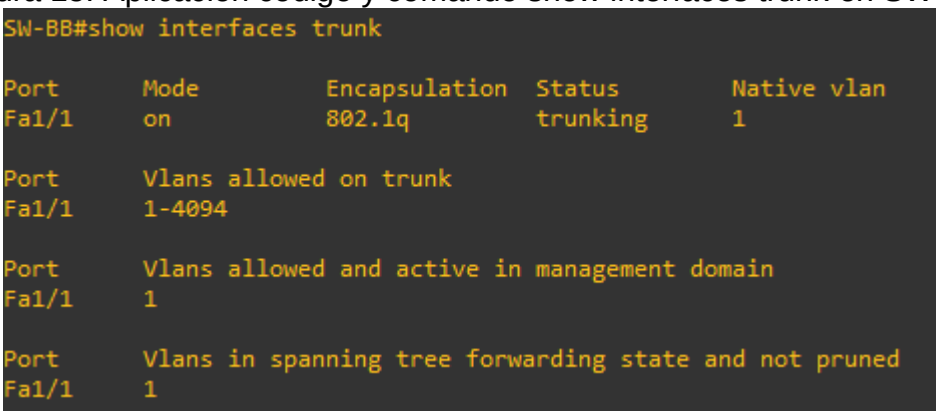


Figura 15. Aplicación código y comando show interfaces trunk en SW-BB

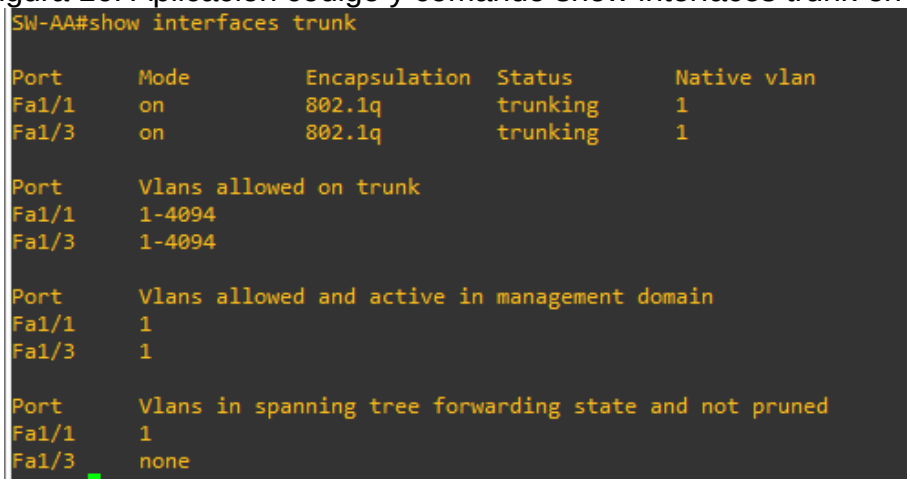


5. Entre SW-AA y SW-BB configure un enlace "trunk" estático utilizando el comando switchport mode trunk en la interfaz F0/3 de SW-AA.

```
SW-AA#configure terminal
SW-AA(config)#interface Fa1/3
SW-AA(config-if)#switchport trunk encapsulation dot1q
SW-AA(config-if)#switchport mode trunk
SW-AA(config-if)#end
```

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

Figura 16. Aplicación código y comando show interfaces trunk en SW-AA



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

SW-BB#configure terminal
SW-BB(config)#interface Fa1/3
SW-BB(config-if)#switchport trunk encapsulation dot1q
SW-BB(config-if)#switchport mode trunk
SW-BB(config-if)#end

SW-CC#configure terminal
SW-CC(config)#interface Fa1/1
SW-CC(config-if)#switchport trunk encapsulation dot1q
SW-CC(config-if)#switchport mode trunk
SW-CC(config-if)#end

Figura 17. Aplicación código y comando show interfaces trunk en SW-BB

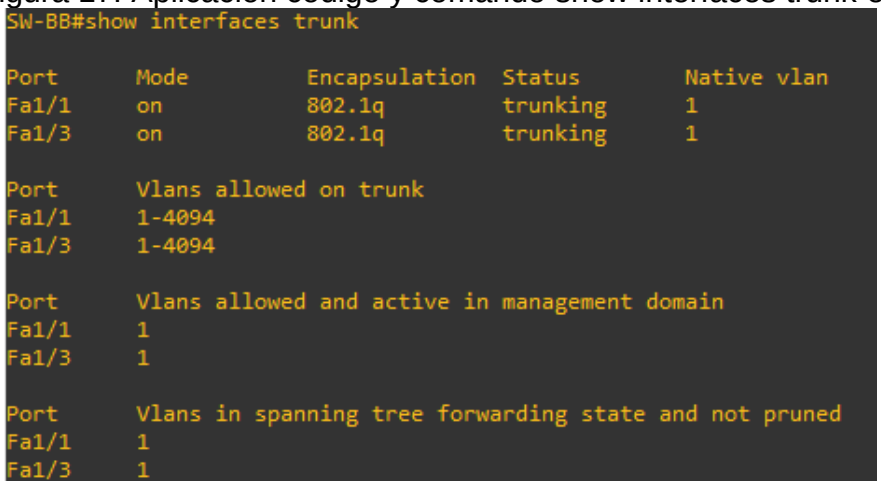


Figura 18. Aplicación código y comando show interfaces trunk en SW-CC

```
SW-CC#show interfaces trunk

Port      Mode         Encapsulation  Status        Native vlan
Fa1/1     on           802.1q         trunking      1
Fa1/3     on           802.1q         trunking      1

Port      Vlans allowed on trunk
Fa1/1     1-4094
Fa1/3     1-4094

Port      Vlans allowed and active in management domain
Fa1/1     1
Fa1/3     1

Port      Vlans in spanning tree forwarding state and not pruned
Fa1/1     none
Fa1/3     none
SW-CC#
```

C. Agregar VLANs y asignar puertos.

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

   SW-AA#configure terminal
   SW-AA(config)#vlan 10
   SW-AA(config)#end

   SW-BB#configure terminal
   SW-BB(config)#vlan 10
   SW-BB(config-vlan)#name Compras
   SW-BB(config-vlan)#vlan 25
   SW-BB(config-vlan)#name Personal
   SW-BB(config-vlan)#vlan 30
   SW-BB(config-vlan)#name Planta
   SW-BB(config-vlan)#vlan 99
   SW-BB(config-vlan)#name Admon
   SW-BB(config-vlan)#end

9. Verifique que las VLANs han sido agregadas correctamente.

   Se utiliza el Comando show vlan-switch brief:

Figura 19. Aplicación código y comando show vlan-switch brief en SW-AA

```
SW-AA#show vlan-switch brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/0, Fa1/2, Fa1/4, Fa1/5
                                                Fa1/6, Fa1/7, Fa1/8, Fa1/9
                                                Fa1/10, Fa1/11, Fa1/12, Fa1/13
                                                Fa1/14, Fa1/15
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
```

Figura 20. Aplicación código y comando show vlan-switch brief en SW-BB

```
SW-BB#show vlan-switch brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/0, Fa1/2, Fa1/4, Fa1/5
                                                Fa1/6, Fa1/7, Fa1/8, Fa1/9
                                                Fa1/10, Fa1/11, Fa1/12, Fa1/13
                                                Fa1/14, Fa1/15
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
```

Figura 21. Aplicación código y comando show vlan-switch brief en SW-CC

```
SW-CC#show vlan-switch brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/0, Fa1/2, Fa1/4, Fa1/5
                                                Fa1/6, Fa1/7, Fa1/8, Fa1/9
                                                Fa1/10, Fa1/11, Fa1/12, Fa1/13
                                                Fa1/14, Fa1/15
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
```

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

    X = número de cada PC particular

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

Tabla No. 5 Configuración puertos VLAN y Direcciones IP

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

```
SW-AA#configure terminal
SW-AA(config)#interface Fa1/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#exit

SW-BB#configure terminal
SW-BB(config)#interface Fa1/10
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#exit

SW-CC#configure terminal
SW-CC(config)#interface Fa1/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#exit
```

12. Repita el procedimiento para los puertos 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.

```
SW-AA(config)#interface Fa1/11
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#exit
SW-AA(config)#interface Fa1/12
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
SW-AA(config-if)#exit
```

```
SW-BB(config)#interface Fa1/11
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#exit
SW-BB(config)#interface Fa1/12
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30
SW-BB(config-if)#exit

SW-CC(config)#interface Fa1/11
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#exit
SW-CC(config)#interface Fa1/12
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30
SW-CC(config-if)#exit


PC1> ip 190.108.30.1 24
PC2> ip 190.108.20.2 24
PC3> ip 190.108.10.3 24
PC4> ip 190.108.10.4 24
PC5> ip 190.108.20.5 24
PC6> ip 190.108.30.6 24
PC7> ip 190.108.10.7 24
PC8> ip 190.108.20.8 24
PC9> ip 190.108.30.9 24
```

D. Configurar las direcciones IP en los Switches.

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

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

Tabla No. 6 Configuración Direcciones IP de los switch

```
SW-AA#configure terminal
SW-AA(config)#interface vlan 99
```

```
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
SW-AA(config-if)#end

SW-BB#configure terminal
SW-BB(config)#interface vlan 99
SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
SW-BB(config-if)#end

SW-CC#configure terminal
SW-CC(config)#interface vlan 99
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0
SW-CC(config-if)#end
```

E. Verificar la conectividad Extremo a Extremo

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

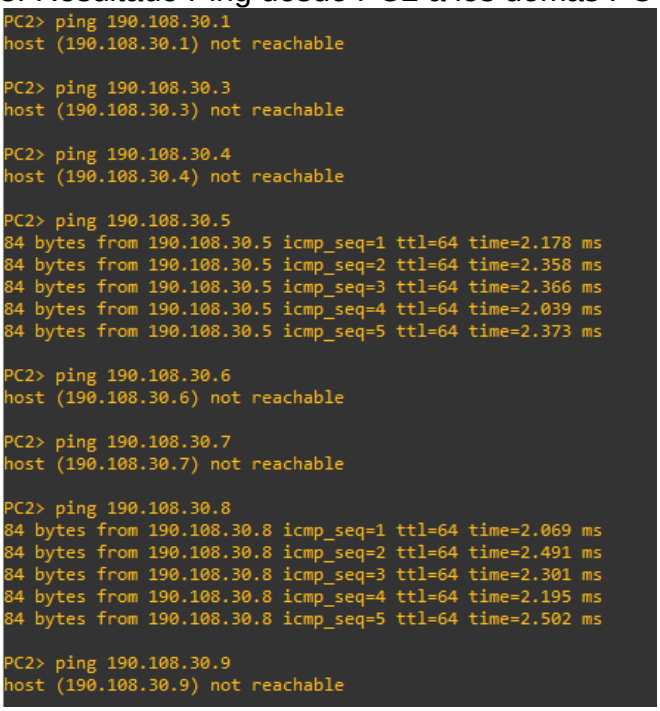
Se hace ping desde PC1

Figura 22. Resultado Ping desde PC1 a los demás PC´s

```
PC1> ping 190.108.30.2
host (190.108.30.2) not reachable

PC1> ping 190.108.30.3
host (190.108.30.3) not reachable

PC1> ping 190.108.30.4
84 bytes from 190.108.30.4 icmp_seq=1 ttl=64 time=2.620 ms
84 bytes from 190.108.30.4 icmp_seq=2 ttl=64 time=2.051 ms
84 bytes from 190.108.30.4 icmp_seq=3 ttl=64 time=2.397 ms
84 bytes from 190.108.30.4 icmp_seq=4 ttl=64 time=2.361 ms
84 bytes from 190.108.30.4 icmp_seq=5 ttl=64 time=2.157 ms

PC1> ping 190.108.30.5
host (190.108.30.5) not reachable

PC1> ping 190.108.30.6
host (190.108.30.6) not reachable

PC1> ping 190.108.30.7
84 bytes from 190.108.30.7 icmp_seq=1 ttl=64 time=3.649 ms
84 bytes from 190.108.30.7 icmp_seq=2 ttl=64 time=1.960 ms
84 bytes from 190.108.30.7 icmp_seq=3 ttl=64 time=1.938 ms
84 bytes from 190.108.30.7 icmp_seq=4 ttl=64 time=1.958 ms
84 bytes from 190.108.30.7 icmp_seq=5 ttl=64 time=1.956 ms

PC1> ping 190.108.30.8
host (190.108.30.8) not reachable

PC1> ping 190.108.30.9
host (190.108.30.9) not reachable
```

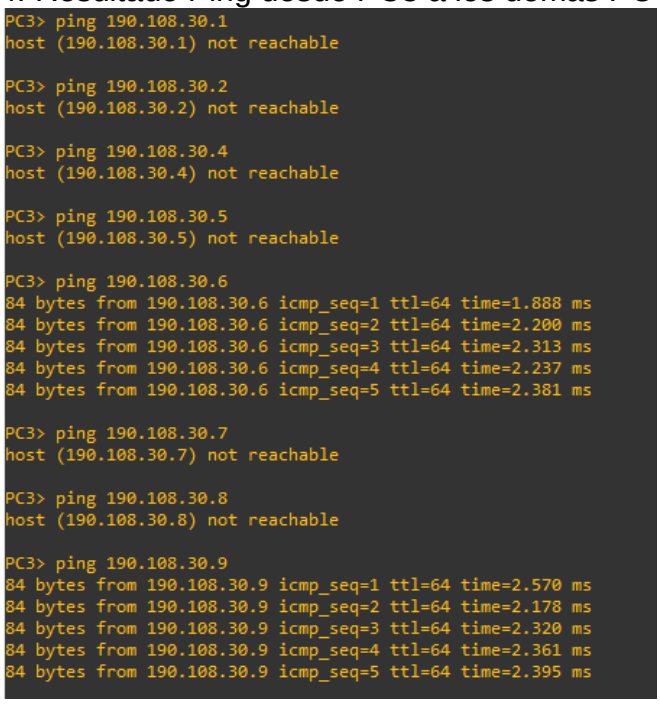
Se hace ping desde PC2

Figura 23. Resultado Ping desde PC2 a los demás PC´s



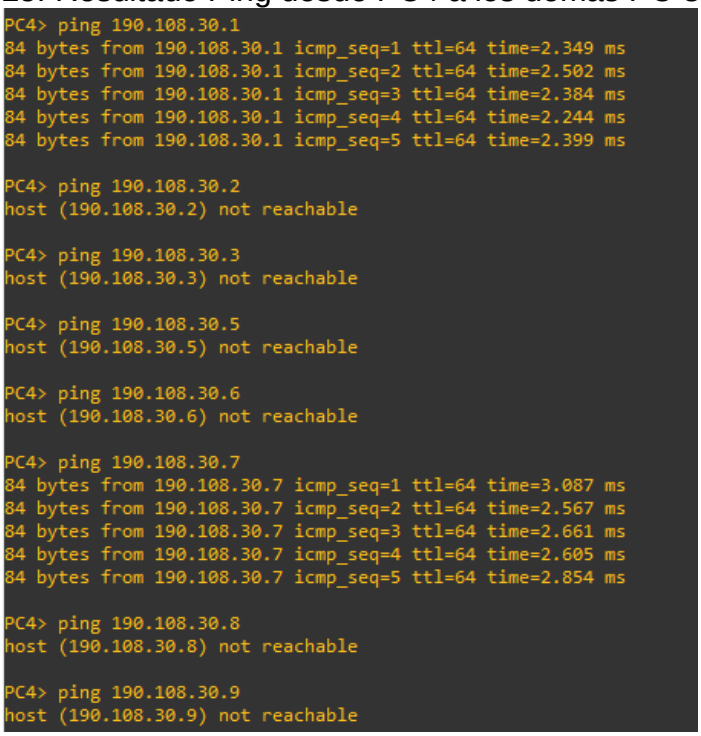
Se hace ping desde PC3

Figura 24. Resultado Ping desde PC3 a los demás PC´s



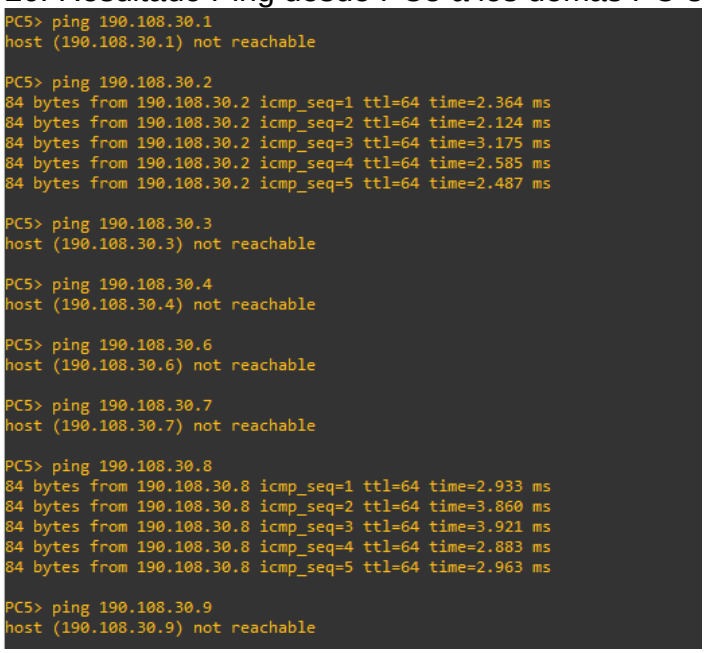
Se hace ping desde PC4

Figura 25. Resultado Ping desde PC4 a los demás PC´s



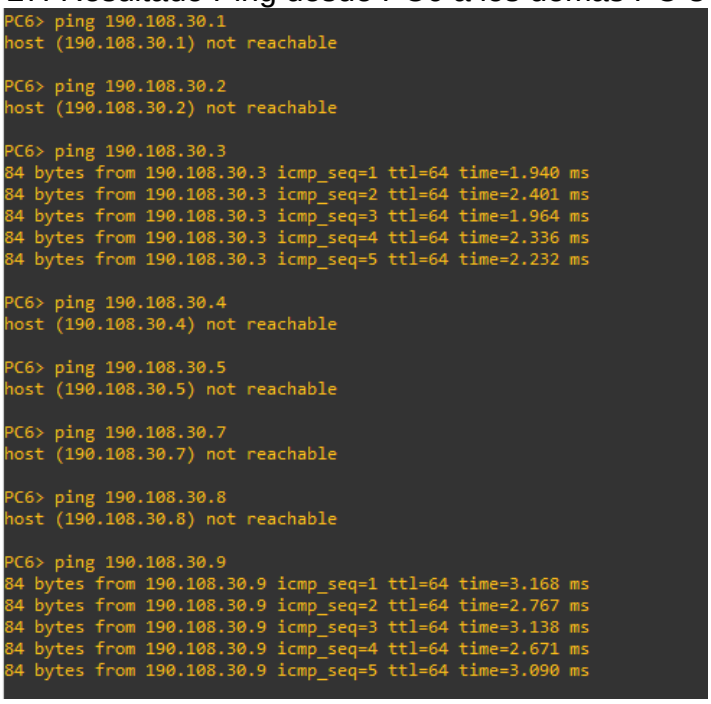
Se hace ping desde PC5

Figura 26. Resultado Ping desde PC5 a los demás PC´s



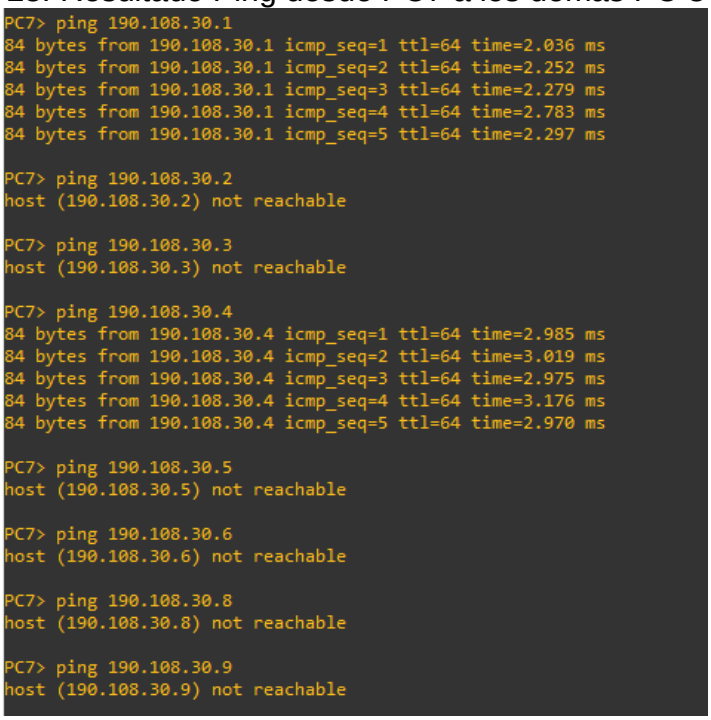
Se hace ping desde PC6

Figura 27. Resultado Ping desde PC6 a los demás PC´s



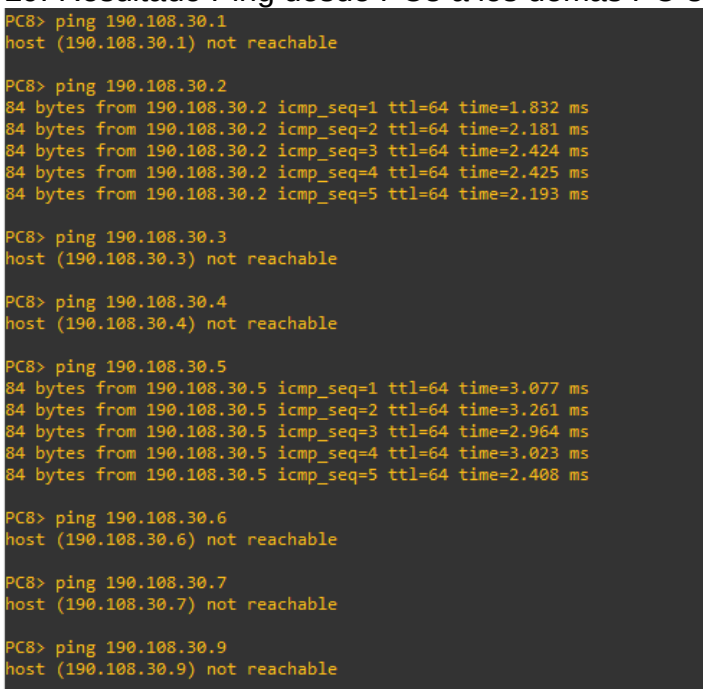
Se hace ping desde PC7

Figura 28. Resultado Ping desde PC7 a los demás PC´s



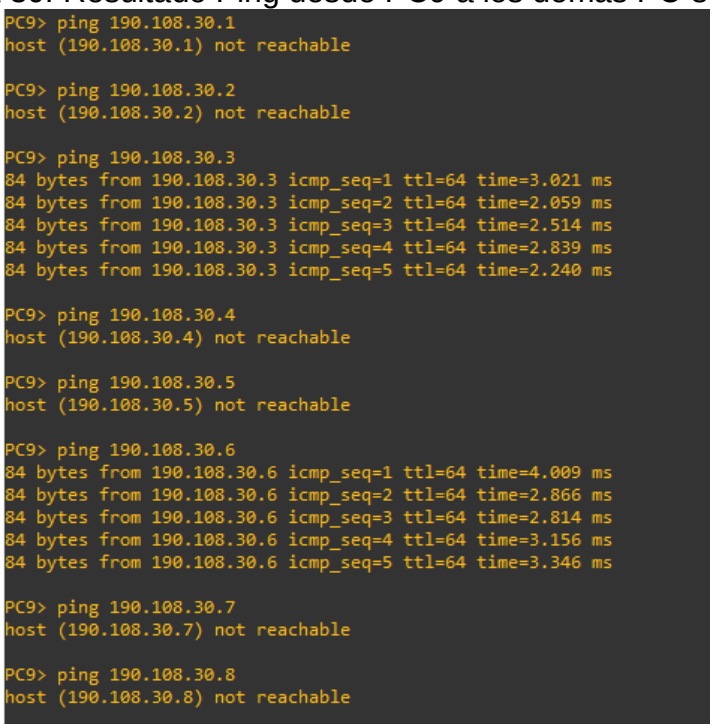
Se hace ping desde PC8

Figura 29. Resultado Ping desde PC8 a los demás PC´s



Se hace ping desde PC9

Figura 30. Resultado Ping desde PC9 a los demás PC´s



Los Ping que fueron satisfactorios estuvieron relacionados en tres grupos debido a que compartían la misma VLAN, esto debido a que tienen el mismo direccionamiento IP, así:

Grupo de la VLAN 10, PC1, PC4 y PC7
Grupo de la VLAN 25, PC2, PC5 y PC8
Grupo de la VLAN 30, PC3, PC6 y PC9

Para las demás relaciones no fue satisfactorio porque no tienen una comunicación entre sí que cuente con privilegios de VLAN adyacencias y/o de dispersión que permita conmutar las interfaces troncales entre estas.

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

Figura 31. Resultado Ping desde SW-AA a SW-BB y SW-CC

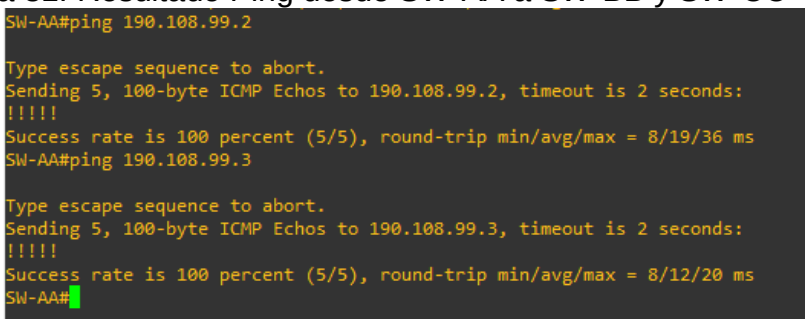


Figura 32. Resultado Ping desde SW-BB a SW-AA y SW-CC

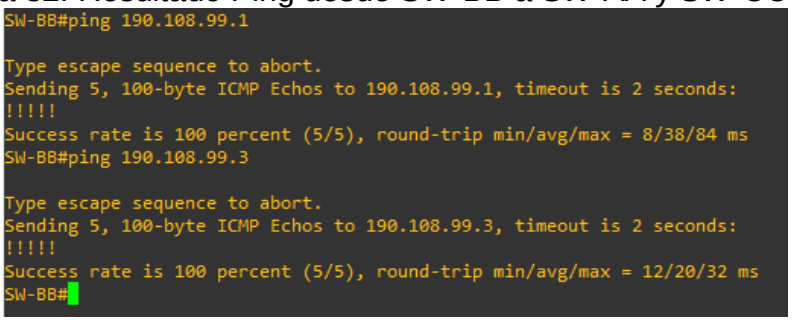
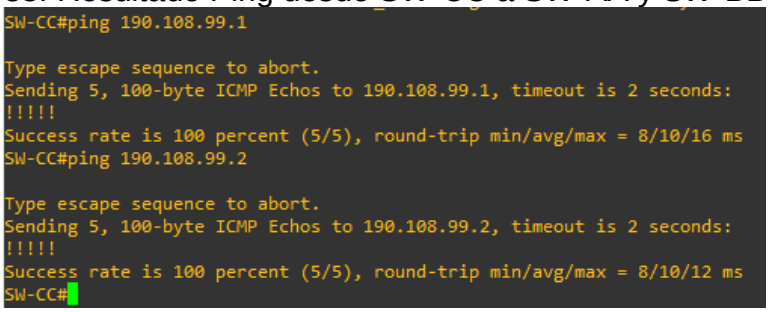


Figura 33. Resultado Ping desde SW-CC a SW-AA y SW-BB



Todos los ping realizados desde y hacia los diferentes switch's fueron satisfactorios, esto debido a que tienen la misma VLAN de gestión, están en el mismo segmento de la red y se configuraron con el mismo direccionamiento IP.

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

Figura 34. Resultado Ping desde SW-AA a todos los PC´s

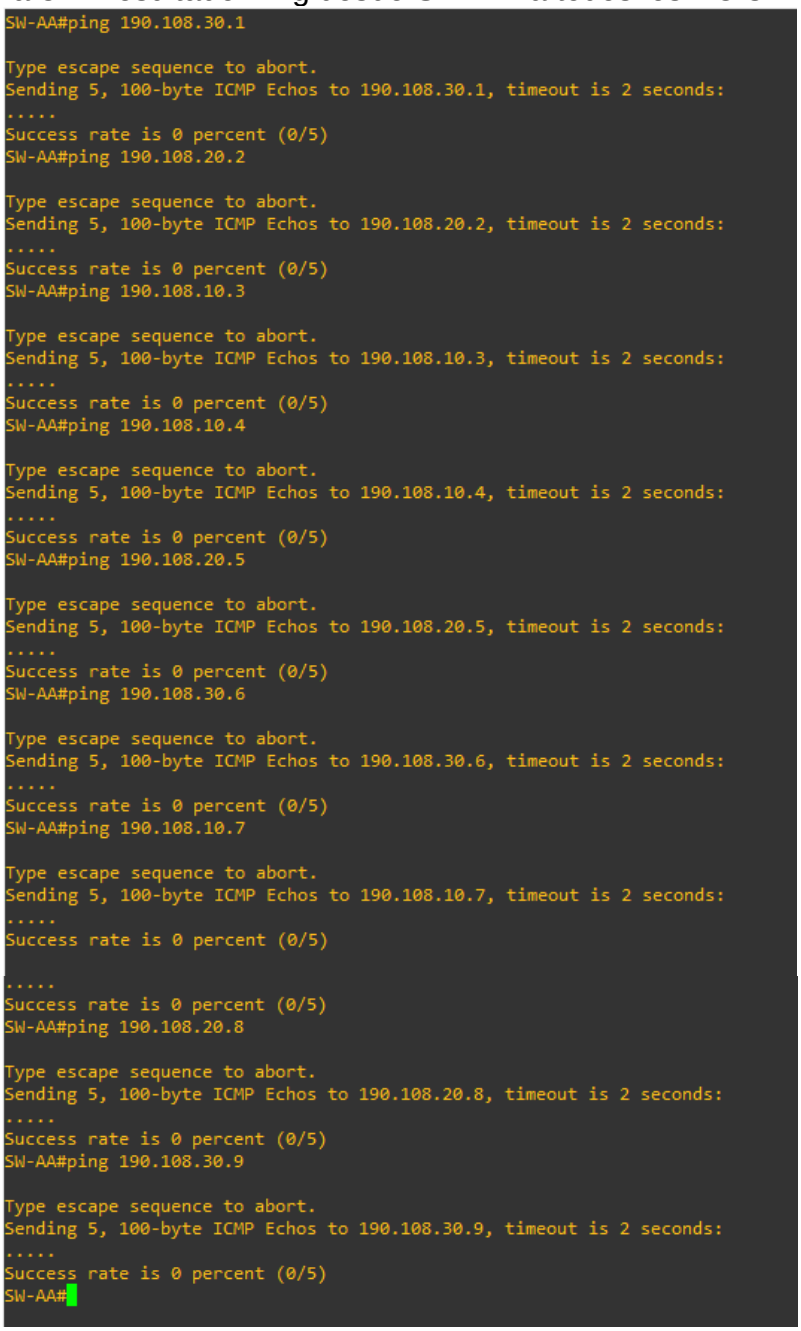


Figura 35. Resultado Ping desde SW-BB a todos los PC´s

```
SW-BB#ping 190.108.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#ping 190.108.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#ping 190.108.10.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#ping 190.108.10.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#ping 190.108.20.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.5, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#ping 190.108.30.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#ping 190.108.10.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.7, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.20.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#ping 190.108.30.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.9, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-BB#
```

Figura 36. Resultado Ping desde SW-CC a todos los PC´s

```
SW-CC#ping 190.108.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-CC#ping 190.108.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-CC#ping 190.108.10.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-CC#ping 190.108.10.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-CC#ping 190.108.20.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.5, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-CC#ping 190.108.30.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-CC#ping 190.108.10.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.7, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-CC#ping 190.108.20.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-CC#ping 190.108.20.9

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.9, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
SW-CC#
```

Todos los ping realizados desde los switch’s a cada uno de los PC’s, no fueron satisfactorios, esto debido a que no se realizó ninguna configuración de direccionamiento IP en la VLAN, además la conexión de puerto a cada PC es modo acceso con la VLAN de gestión (VLAN 99), por lo que no tiene una puerta de enlace hacia los PC’s.

CONCLUSIONES

Se realizó un análisis de cada uno de los escenarios, buscando presentar una solución a los mismos, aplicando los conocimientos adquiridos tanto en el módulo CCNP ROUTE, como en el módulo CCNP SWITCH, los cuales son aplicables a redes empresariales y otros tipos de soluciones los que además se involucren tanto aspectos avanzados como redes inalámbricas, voz, seguridad, entre otros.

Al configurar un protocolo BGP se genera un intercambio de datos alineados entre sus componentes, aun cuando estos sean autónomos mediante enrutamientos IPV4, intercambiando información entre los routers de acuerdo al alcance de la misma red.

Al configurar DTP, el enlace troncal por defecto es modo dynamic auto, por lo tanto, al realizar esta configuración, solamente hace falta configurar uno de los lados como dynamic desirable para establecer el enlace troncal.

Para lograr la configuración de las PC's terminales de los switch's, hace falta configurar una comunicación entre sí que cuente con privilegios de VLAN adyacencias y/o de dispersión que permita conmutar las interfaces troncales entre estas, sin embargo, estos grupos de VLAN nos permiten decidir los accesos por los cuales queremos que exista comunicación entre diferentes grupos de trabajo preestablecidos, de igual manera, al no realizarse ninguna configuración de direccionamiento IP en la VLAN, además que la conexión de puerto a cada PC es modo acceso con la VLAN de gestión (VLAN 99), no se tendrá una puerta de enlace hacia los PC's.

El realizar las simulaciones se permite entender el funcionamiento de los routers y switch's, así como sus capacidades y limitaciones para realizar el planeamiento de la solución de un problema.

BIBLIOGRAFÍA

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

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

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). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

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

Macfarlane, J. (2014). Network Routing Basics: Understanding IP Routing in Cisco Systems. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=158227&lang=es&site=ehost-live

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing a Border Gateway Protocol (BGP). Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx.

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

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