DIPLOMADO DE PROFUNDICACION CISCO PRUEBA DE HABILIDADES PRACTICAS CCNP

KEVIN HARRISON HERNANDEZ CANO

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA – UNAD
ESCULA DE CIENCIAS BÁSICAS, TECNOLOGIA E INGENIERÍA – ECBTI
INGENIRIA EN TELECOMUNICACIONES
BOGOTÁ DC
2020

DIPLOMADO DE PROFUNDICACION CISCO PRUEBA DE HABILIDADES PRACTICAS CCNP

KEVIN HARRISON HERNANDEZ CANO

Diplomado de opción de grado para optar el título de
INGENIERO EN TELECOMUNICACIONES

DIRECTOR:
Mcs. GERARDO GRANADOS ACUÑA

UNIVERSIDAD NACIONAL ABIERTA Y ADISTANCIA – UNAD
ESCULA DE CIENCIAS BÁSICAS, TECNOLOGIA E INGENIERÍA – ECBTI
INGENIRIA EN TELECOMUNICACIONES
BOGOTÁ DC
2020

NOTA DE ACEPTACION

_____
_____
_____
_____
_____
_____
_____

_____
Firma del presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá 22 de mayo de 2020

AGRADECIMIENTOS

Gracias a la Universidad Nacional Abierta y Distancia UNAD que me permitió realizar este documento en conjunto a los tutores que brindaron ese conocimiento con el cual se pudo lograr el desarrollo de este. A provecho la oportunidad para también darle gracias a mi familia que siempre estuvieron ahí apoyándome en todo, en especial a mi hija. Ya que ella me demostró que la superación profesional y personal existe, que siempre hay un motor de vida que lo anima a uno a querer seguir saliendo a delante, a nunca retroceder y siempre seguir un lineamiento que me forme como persona y siempre siendo un buen profesional.

CONTENIDO

.

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

RED LAN: Red de Área Local, es una red de diferentes computadores conectados entre sí, bien sea en un área pequeña, como un edificio o una habitación, lo que permite a los usuarios enviar, compartir y recibir archivos.

RED WAN: Red de Área Amplia, es una red de computadoras que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física. Muchas WAN son construidas por organizaciones o empresas para su uso privado, otras son instaladas por los proveedores de Internet (ISP) para proveer conexión a sus clientes.

DIRECCION IP: Es un número que identifica de forma única a una interfaz en red de cualquier dispositivo conectado a ella que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

MASCARA DE RED: Es una combinación de bits que sirve para delimitar el ámbito de una red de ordenadores.1 Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host.

SWITCH: O conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).

ROUTER: Es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

PROTOLOCO 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 domino 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.

IP LOOPBACK: Esta dirección se suele utilizar cuando una transmisión de datos tiene como destino el propio host. También se suele usar en tareas de diagnóstico de conectividad y validez del protocolo de comunicación.

PUERTO 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.

RESUMEN

Se realiza la implementación de dos topologias de redres, escenarios 1 y 2, donde en el primero nos solicitan realizan la implementación de 4 router configurando una relación de vecino BGP entre R1 y R2. Así mismo una relación de vecino BGP entre R2 y R3. Terminando con la última relación BGP entre R3 y R4 Abordaremos sobre el protocolo BGP y EBGP, donde veremos qué tipos de configuraciones se realizaron para poder dar solución, que pruebas nos muestran los resultados obtenidos y garantizar que por medio de lo realizado se cumplió a satisfacción con el escenario número 1, dentro del diplomado Cisco Certificaicon CCNP.

Para el escenario número 2, se nos plantea realiza la configuración de dos protocolos de comunicación, el primero es el protocolo VTP el cual consiste en 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. Para ellos se nos plantean diferentes interrogantes donde nos piden realizar la configuración y enrutamiento para mostrar los resultados obtenidos. El segundo protocolo para implementar es el Dynamic Trunk Protocol el cual consiste en la forma de establecer los puertos ethernet en cinco modos diferentes de trabajo: AUTO, ON, OFF, DESIRABLE y NON-NEGOTIATE. Donde se debe configurar sobre los 3 SW, para posteriormente realizar pruebas de conectividad y conmutación sobre los equipos de cómputo que comparten diferentes VLAN, garantizando este por medio del protocolo ICMP. Para dar solución al escenario 2, se nos solito realizar diferentes pruebas, tanto en equipos de cómputo como en switch con el fin de garantizar la solución de este.

Palabras Clave: Redes, Cisco, CCNP, Configuración, conmutación y enrutamiento.

ABSTRACT

The implementation of two network topologies is carried out, scenarios 1 and 2, where in the first one they ask us to carry out the implementation of 4 routers configuring a BGP neighbor relationship between R1 and R2. Likewise a BGP neighbor relationship between R2 and R3. Ending with the last BGP relationship between R3 and R4 We will discuss the BGP and EBGP protocol, where we will see what types of configurations were carried out in order to provide a solution, which tests show us the results obtained and guarantee that through what was carried out it was fulfilled to satisfaction with scenario number 1, within the Cisco Certificaicon CCNP diploma.

For scenario number 2, we are presented with the configuration of two communication protocols, the first is the VTP protocol which consists of centralizing and simplifying the administration in a domain of VLANs, being able to create, delete and rename them, thus reducing the need to configure the same VLAN on all nodes.

For them, different questions are asked where they ask us to configure and route to show the results obtained. The second protocol to implement is the Dynamic Trunk Protocol which consists of the way to establish the ethernet ports in five different working modes: AUTO, ON, OFF, DESIRABLE and NON-NEGOTIATE. Where it must be configured on the 3 SWs, to subsequently perform connectivity and switching tests on the computer equipment that shares different VLANs, guaranteeing this through the ICMP protocol. In order to solve scenario 2, we were asked to carry out different tests, both on computer equipment and on a switch, in order to guarantee its solution.

Key Words: Networks, Cisco, CCNP, Configuration, switching and routing.

INTRODUCCION

En este documento presentamos la última actividad individual como método de evaluación final para culminar el diplomado en certificación CCNP. El cual pretende identificar el grado de aprendizaje obtenido durante este diplomado. Se nos propone realizar la configuración de 2 escenarios propuestos en la prueba de habilidades el cual busca poner a prueba los conocimientos y niveles de solución a problemas sobre soluciones de red.

Abordaremos protocolos de enrutamiento como lo es el BGP y OSPF, para el primer escenario, donde por medio de la configuración que le damos a los routers resolvemos a los interrogantes planteados. En la segunda interrogante se nos pide realizar una configuración sobre los switches, con el fin de establecer comunicación y respuestas exitosas a ICMP con varios equipos conectados entre diferentes redes.

A continuación, mostramos el paso a paso y una descripción detallada de como por medio de lo aprendido durante el curso damos solución a cada paso y cada interrogante planteado en esta métrica evaluativa. Además, como por medio de diferentes comandos mostramos y justificamos cada respuesta.

DESARROLLO

1. Escenario 1:

Figura 1. Escenario 1

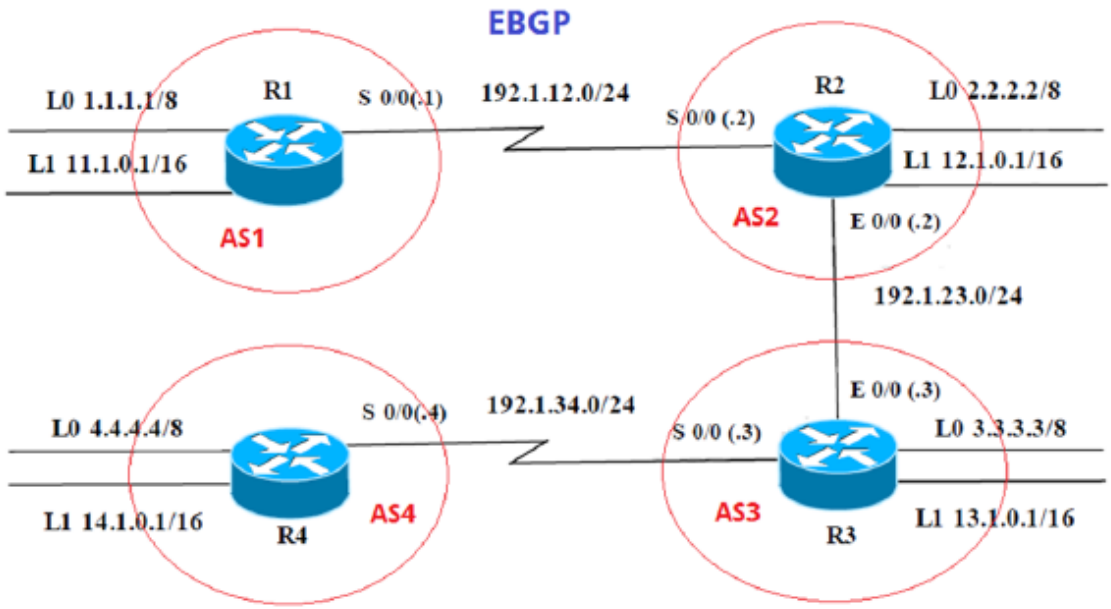
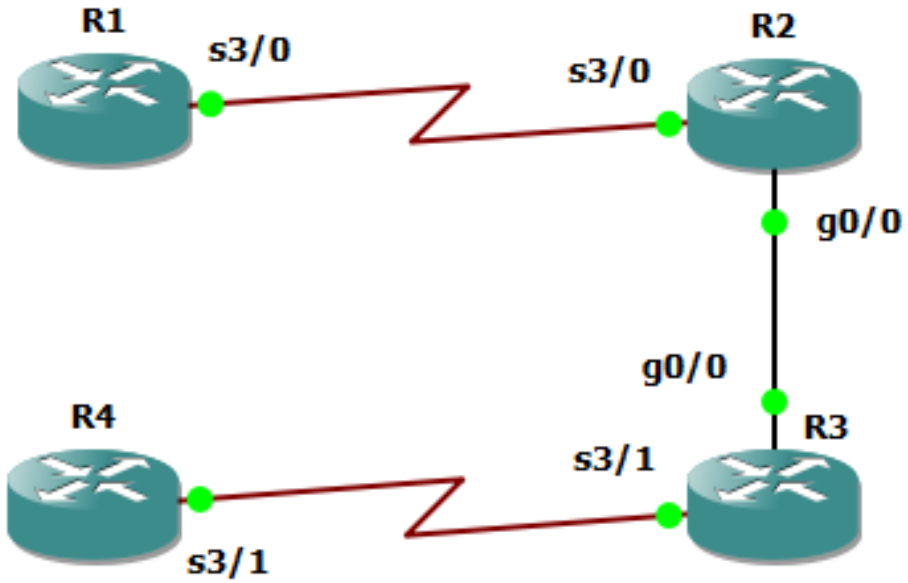


Figura 2. Simulación de escenario 1



Información para configuración de los Routers :

Tabla 1. Interfaces loopback para crear R1

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 2. Interfaces loopback para crear R2

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 3. Loopback para crear R3

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 4. Loopback para crear R4

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

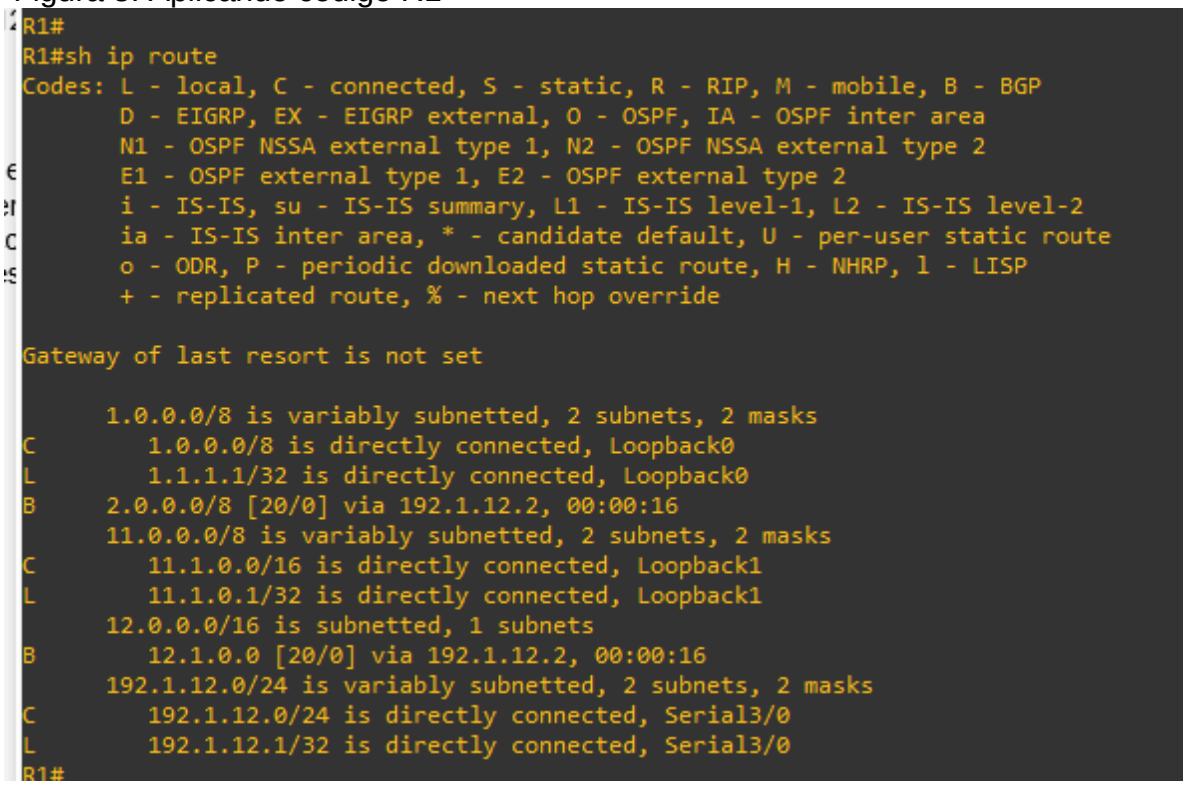
1. **Configure una relación de vecino BGP entre R1 y R2. R1 debe estar en AS1 y R2 debe estar en AS2. Anuncie las direcciones de Loopback en BGP. Codifique los ID para los routers BGP como 22.22.22.22 para R1**

y como 33.33.33.33 para R2. Presente el paso a con los comandos utilizados y la salida del comando show ip route.

```
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 GigaEthernet 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
```

Figura 3. Aplicando código R1

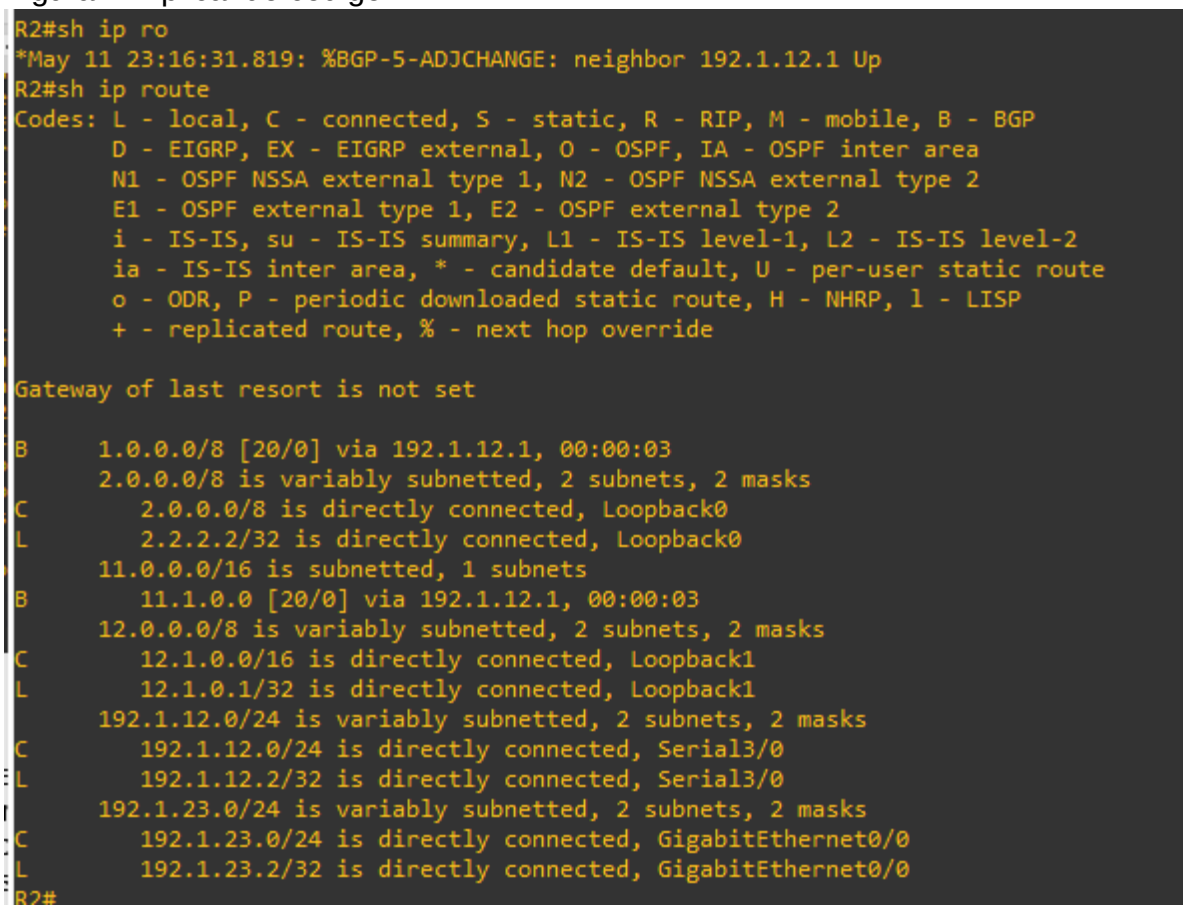


```
R1#
R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       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, 00:00:16
      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, 00:00:16
      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 4. Aplicando código R2



```
R2#sh ip ro
*May 11 23:16:31.819: %BGP-5-ADJCHANGE: neighbor 192.1.12.1 Up
R2#sh 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, 00:00:03
      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
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.12.1, 00:00:03
      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#
```

Podemos observar que al ejecutar el comando ***sh ip route,*** en R1 tanto en R2 contienen en su tabla de enrutamiento las direcciones de loopback y las de las redes a las cuales se encuentran conectados de forma directa, además de sus redes configuradas en las interfaces loopback de su vecino, las que acabamos de mencionar se identifican por el código **B** que las precede, lo cual informa que ambas redes fueron aprendidas por el protocolo BGP. Podemos ver que en la tabla de enrutamiento cada router reconoce la vía para alcanzar estas rutas. Podemos observar también que la interface gigabiteethernet 0/0 es la que conecta físicamente a los routers.

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.**

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 gigabiteethernet 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 3/1
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
```

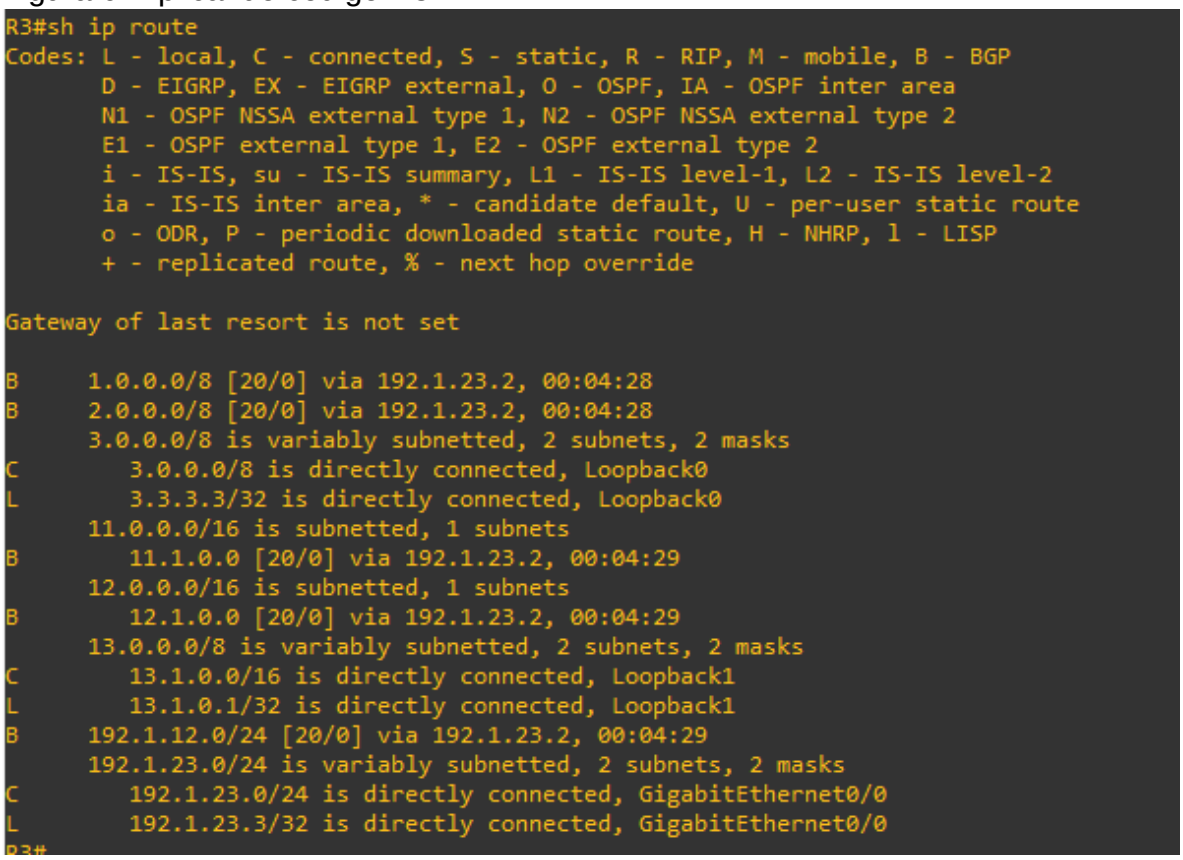
Figura 5. Aplicando código R2

```
R2#SH 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, 00:46:11
      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, 00:13:40
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.12.1, 00:46:11
      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, 00:13:40
      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
```

Figura 6. Aplicando código R3



```
R3#sh 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, 00:04:28
B     2.0.0.0/8 [20/0] via 192.1.23.2, 00:04:28
      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
      11.0.0.0/16 is subnetted, 1 subnets
B        11.1.0.0 [20/0] via 192.1.23.2, 00:04:29
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.23.2, 00:04:29
      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
B     192.1.12.0/24 [20/0] via 192.1.23.2, 00:04:29
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, GigabitEthernet0/0
L        192.1.23.3/32 is directly connected, GigabitEthernet0/0
R3#
```

Al correr el comando ***sh ip route*** observamos que la tabla de enrutamiento se ha actualizado y ahora tiene las rutas loopback configuradas en **R3**. Se puede observar que el **R2** aprendido 4 rutas de BGP, que se pueden evidenciar con el código ***B.*** Podemos ver que el **R3** contiene dentro de su tabla de enrutamiento las redes que el reconoce que están conectadas directamente, es decir la interfaces loopbacks y las redes que conectan los routers **R3** y **R4** por medio de las int Gigabiteethernet 0/0 y serial 3/1. Adicional a esto **R3** ya ha aprendido las rutas configuradas sobre R1 y R2, gracias a la configuración del protocolo BGP, el cual por medio de su configuración reconoce la relación de adyacencia en **R2**, y que dichas redes se anunciaron en cada uno de los routers. En **R3** están las direcciones de red que conecta los **R1** y **R2** como se puede observar en su tabla de enrutamiento la cual aprendio mediante el protocolo BGP. **R3** alcanza todas estas redes gracias a su configuración en gigabiteethernet 0/0 que lo conecta con R2 (192.1.23.0/24).

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.

```
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 3/1
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
```

forma de establecer la relación de adyacencias mediante las direcciones de loopback es que el router vecino necesita informar sobre una interface virtual en lugar de una interface física. Debido a esto se requiere otro tipo de configuración para establecer los vecinos:

```
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(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)# 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

Figura 7. Aplicando código R3

R3:

```
R3#sh 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, 00:51:45
B     2.0.0.0/8 [20/0] via 192.1.23.2, 00:51:55
      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, 00:51:45
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 192.1.23.2, 00:51:55
      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 4.4.4.4, 00:02:46
B     192.1.12.0/24 [20/0] via 192.1.23.2, 00:51:55
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, GigabitEthernet0/0
L        192.1.23.3/32 is directly connected, GigabitEthernet0/0
      192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.34.0/24 is directly connected, Serial3/1
L        192.1.34.3/32 is directly connected, Serial3/1
```

R4:

Figura 8. Aplicando código R4

```
R4#sh 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, 00:06:56
B     2.0.0.0/8 [20/0] via 3.3.3.3, 00:06:56
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, 00:06:56
      12.0.0.0/16 is subnetted, 1 subnets
B        12.1.0.0 [20/0] via 3.3.3.3, 00:06:56
      13.0.0.0/16 is subnetted, 1 subnets
B        13.1.0.0 [20/0] via 3.3.3.3, 00:06:56
      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, 00:06:56
B     192.1.23.0/24 [20/0] via 3.3.3.3, 00:06:56
      192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.34.0/24 is directly connected, Serial3/1
L        192.1.34.4/32 is directly connected, Serial3/1
```

Al ejecutar el comando ***sh ip route*** nos muestra que el router R3 ha actualizado su tabla de enrutamiento y la dirección de red que conecta hacia R4, que ahora corresponde a la dirección de loopback 0, la cual aparece de forma estática, ya que el paso anterior nos indican dejarla de esa manera. Para establecer la adyacencia se utiliza la dirección lógica de la loopback 0. Ya que la vía de conexión física sigue siendo la red 192.1.4.0/24 correspondiente a la serial 1/0. De esa manera se puede identificar que la dirección de red de la interface loopback 1 se siegue aprendiendo mediante el protocolo BGP, pero partir de este momento se alcanza mediante la interface loopback 0 de R4 (4.4.4.4). En la tabla de enrutamiento del router R4 se puede evidenciar que la dirección por la cual este se comunica con sus vecinos BGP ha cambiado y ahora es la dirección de la interface Loopback 0 en R3.

2. **Escenario 2:**

Figura 9. Escenario 2

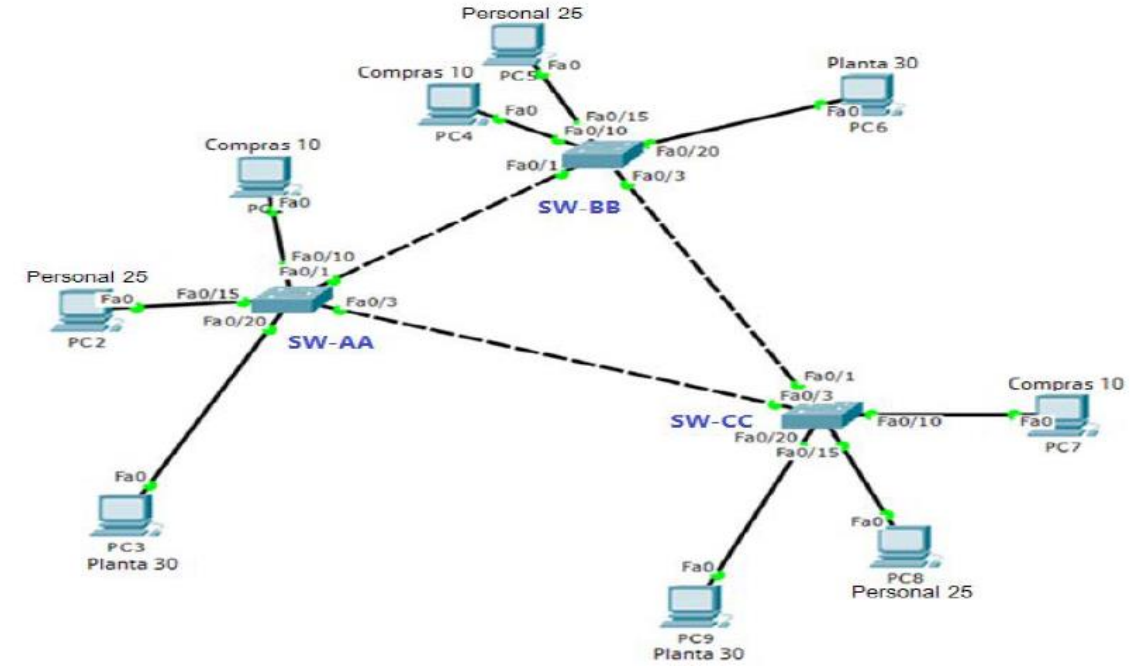
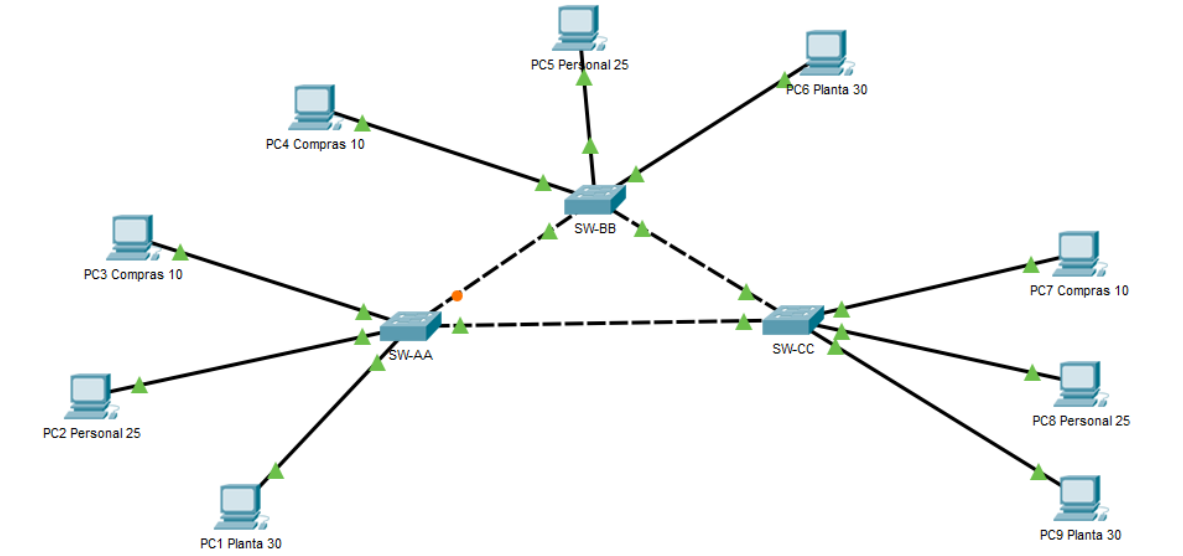


Figura 10. Simulación del escenario 2



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:

SW-AA #configure terminal
SW-AA (config)#vtp mode client
Changing VTP domain name from NULL to CCNP
SW-AA (config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-AA (config)#vtp password cisco
Setting device VLAN database password to cisco

SW-BB#configure terminal
SW-BB (config)#vtp mode server
Device mode already VTP SERVER.
SW-BB (config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-BB (config)#vtp password cisco
Setting device VLAN database password to cisco

SW-CC#configure terminal
SW-CC (config)#vtp mode client
Changing VTP domain name from NULL to CCNP
SW-CC (config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SW-CC (config)#vtp password cisco
Setting device VLAN database password to cisco

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

SW-AA:

Figura 11. Se aplica código SW-AA

```
SW-AA#sh vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE
0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SW-AA#
```

Figura 12. Se aplica código SW-BB

```
SW-BB#sh vtp st
SW-BB#sh vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE
0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
SW-BB#
```

Figura 13. Se aplica código SW-CC

```
SW-CC#sh vtp st
SW-CC#sh vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xDA 0xBF 0x42 0x0D 0x90 0xBC 0xBE
0x41
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
SW-CC#
```

B. Configurar DTP (Dynamic Trunking Protocol)

4. 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-BB#configure terminal
SW-BB (config)#interface fastEthernet 0/1
SW-BB (config-if)#switchport mode dynamic desirable

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

Figura 14. Se aplica código SW-AA

```
SW-AA#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       none
```

Figura 15. Se aplica código SW-BB

```
SW-BB#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       desirable    n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       none
```

6. Entre SW-AA y SW-CC 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 fastEthernet 0/3
SW-AA (config-if)#switchport mode trunk

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

Figura 16. Se aplica código SW-CC

```
SW-AA#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       auto         n-802.1q       trunking      1
Fa0/3       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/3       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1
Fa0/3       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       none
Fa0/3       none
```

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

SW-CC#configure terminal
SW-CC (config)#interface fastEthernet 0/1
SW-CC (config-if)#switchport mode trunk

SW-CC:
Figura 17. Se aplica código SW-AA

```
SW-CC#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/3       auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/3       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1
Fa0/3       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
Fa0/3       1
```

SW-BB:

Figura 18. Se aplica código SW-BB

```
SW-BB#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       desirable    n-802.1q       trunking      1
Fa0/3       auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/3       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1
Fa0/3       1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1
Fa0/3       1
```

C. Agregar VLANs y asignar puertos.

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

SW-AA#conf t
SW-AA(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.

Figura 19. Configuración Vlan SW-AA

```
SW-AA(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
SW-AA(config)#
```

SW-BB#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#vlan 10
SW-BB(config-vlan)#name compras
SW-BB(config-vlan)#vlan 25
SW-BB(config-vlan)#name Personal
SW-BB(config-vlan)#vlan 30
SW-BB(config-vlan)#name Planta
SW-BB(config-vlan)#vlan 99
SW-BB(config-vlan)#name Admon

10. Verifique que las VLANs han sido agregadas correctamente:

SS-BB:

Figura 20. Se aplica código SW-BB

```
SW-BB#sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/4, Fa0/5,
Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9,
Fa0/10
                                                 Fa0/11, Fa0/12,
Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16,
Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20,
Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24,
Gig0/1, Gig0/2
10   compras                           active
25   Personal                          active
30   Planta                            active
99   Admon                             active
```

SW-AA:

Figura 21. Se aplica código SW-AA

```
SW-AA#sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/4, Fa0/5,
Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9,
Fa0/10
                                                 Fa0/11, Fa0/12,
Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16,
Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20,
Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24,
Gig0/1, Gig0/2
10   compras                           active
25   Personal                          active
30   Planta                            active
99   Admon                             active
```

SW-CC:

Figura 22. Se aplica código SW-CC

```
SW-CC#sh vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/4, Fa0/5,
Fa0/6
                                                 Fa0/7, Fa0/8, Fa0/9,
Fa0/10
                                                 Fa0/11, Fa0/12,
Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16,
Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20,
Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24,
Gig0/1, Gig0/2
10   compras                           active
25   Personal                          active
30   Planta                            active
99   Admon                             active
```

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

Tabla 5. Configuración direcciones IP

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

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

13. 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#configure terminal
SW-AA(config)#interface fastEthernet 0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config)#interface fastEthernet 0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config)#interface fastEthernet 0/20
SW-AA(config-if)#switchport mode access

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

SW-BB#configure terminal
SW-BB(config)#interface fastEthernet 0/10
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
SW-BB(config)#interface fastEthernet 0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config)#interface fastEthernet 0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30

SW-CC#configure terminal
SW-CC(config)#interface fastEthernet 0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config)#interface fastEthernet 0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config)#interface fastEthernet 0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30

Se evidencia un pequeño error dentro de la topología, donde se ve el PC1 como PC3, se corrige y se acomodan de la siguiente manera.

PC1: ip address 190.108.10.2 255.255.255.0
PC2: ip address 190.108.20.3 255.255.255.0
PC3: ip address 190.108.30.4 255.255.255.0
PC4: ip address 190.108.10.5 255.255.255.0
PC5: ip address 190.108.20.6 255.255.255.0
PC6: ip address 190.108.30.7 255.255.255.0
PC7: ip address 190.108.10.8 255.255.255.0
PC8: ip address 190.108.20.9 255.255.255.0
PC9: ip address 190.108.30.10 255.255.255.0

D. Configurar las direcciones IP en los Switches:

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

Tabla 6. Configurar las direcciones IP en los switch

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

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

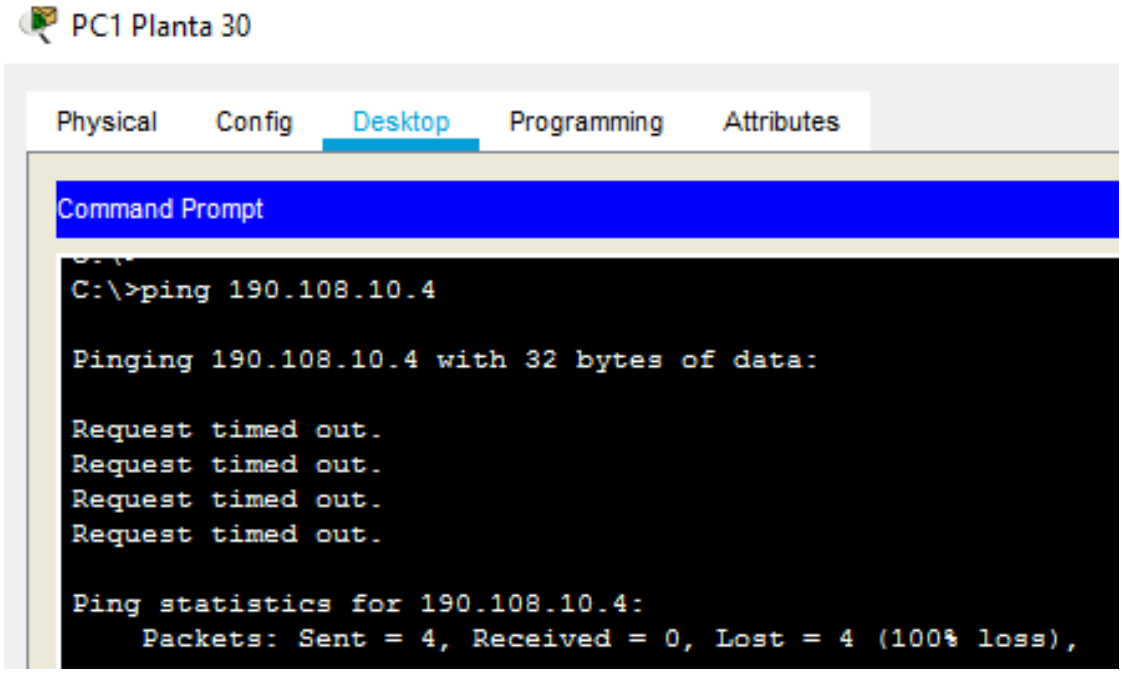
SW-CC#configure terminal
SW-CC(config)#interface vlan 99
SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0

E. Verificar la conectividad Extremo a Extremo

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

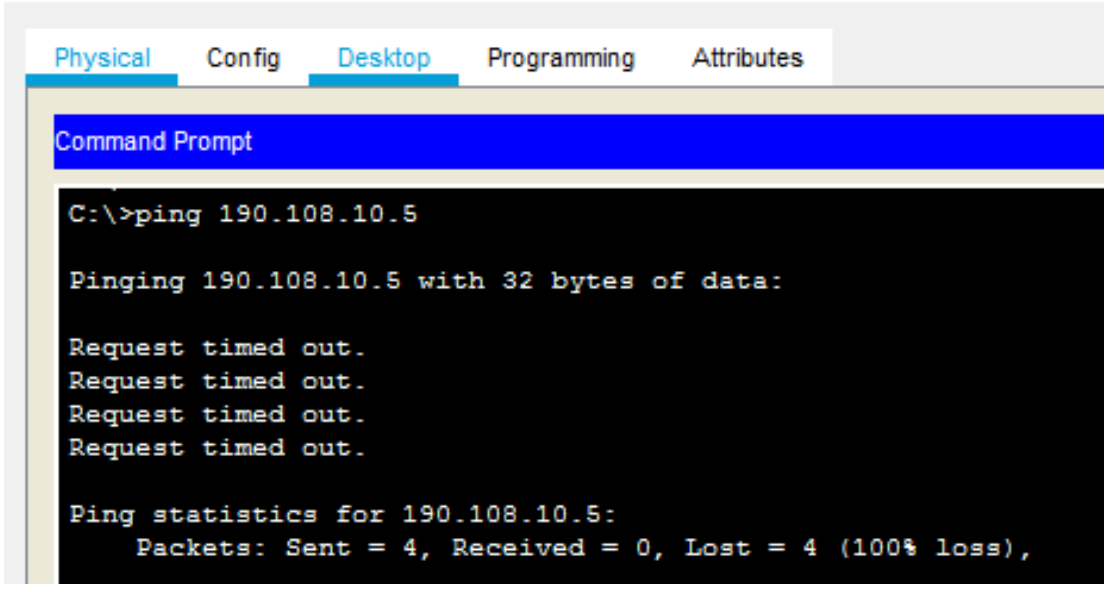
PC1 A PC3:

Figura 23. Pruebas entre PCs



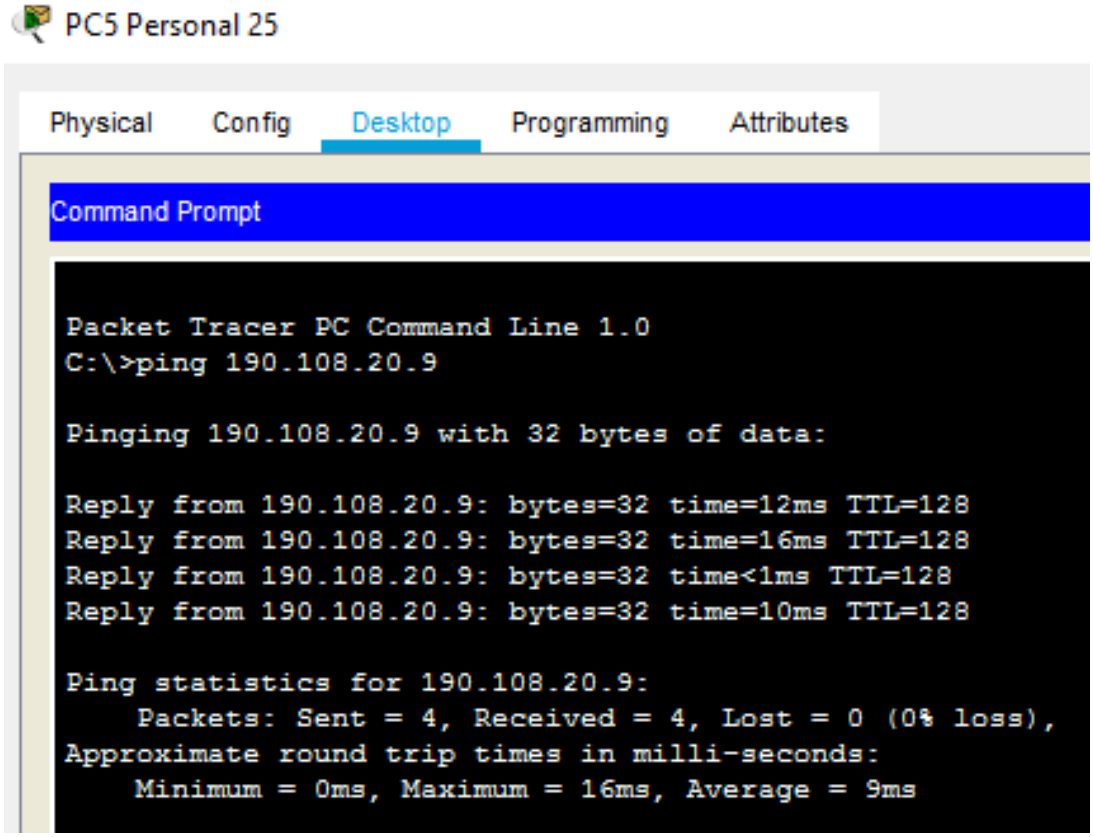
PC1 A PC4

Figura 24. Pruebas entre PCs



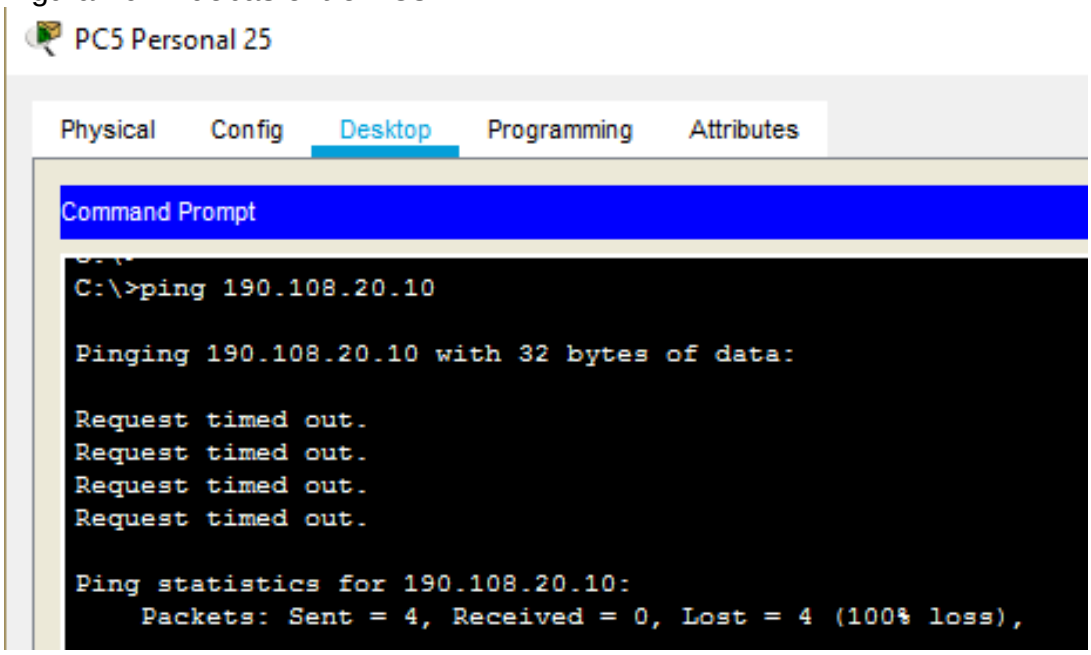
PC5 A PC8:

Figura 25. Pruebas entre PCs



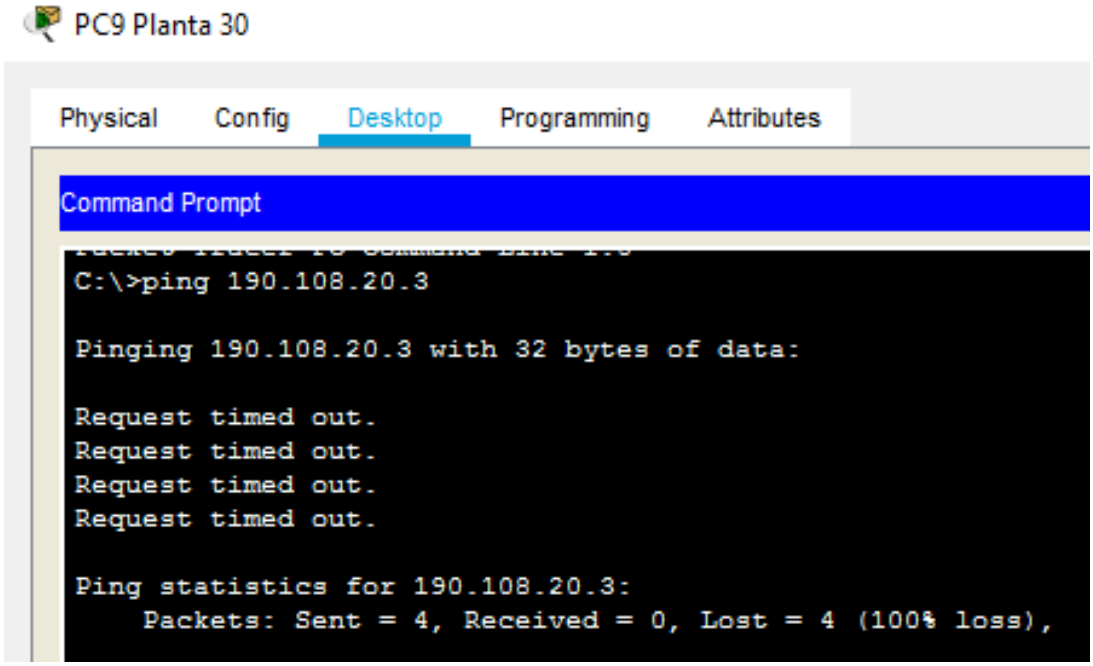
PC5 A PC9:

Figura 26. Pruebas entre PCs



PC9 A PC2:

Figura 27. Pruebas entre PCs



El Ping que fue exitoso sobre los equipos, fue el perteneciente al de las mismas vlans asignado y por otro lado el no éxito del ping fue el de equipos de diferentes vlans. También podemos ver que se genera un error entre diferentes vlans ya que no todas comparten el mismo segmento de red. Para que de todas las formas fuera exitoso los pings sobre diferentes vilas y segmentos, sería necesario realizarle a la topología la inclusión de un equipo Switch-multicapa con el fin de realizar un enrutamiento intrínseco entre las diferentes vlans.

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

Figura 28. Pruebas ICMP entre SW-AA a SW-BB y SW-CC

```
SW-AA#ping 190.108.99.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/7/12 ms

SW-AA#ping 190.108.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/4 ms
```

Ping de SW-BB a SW-AA y SW-CC:

Figura 29. Pruebas ICMP entre SW-BB a SW-AA y SW-CC

```
SW-BB#ping 190.108.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/11 ms

SW-BB#ping 190.108.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/10 ms
```

Ping de SW-CC a SW-AA y SW-BB:

Figura 30. Pruebas ICMP entre SW-CC a SW-AA y SW-BB

```
SW-CC#ping 190.108.99.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

SW-CC#ping 190.108.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

Los pings realizados entre los SWs, todos fueron exitosos, ya que en el paso 12 y 13, se nos solicitó realizar la configuración de los switches en modo troncal. Y cuando hicimos el comando ***sh int trunk*** evidenciamos que todos están en modo compatible y además todos comparten el mismo encapsulamiento.

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

Ping desde SS-AA hacia PC1, PC2 y PC3:

Figura 31. Pruebas ICMP desde SS-AA hacia PC1, PC2 y PC3

```
SW-AA#ping 190.108.10.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.20.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.30.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.4, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Ping desde SS-BB hacia PC4, PC5 y PC6:

Figura 32. Pruebas ICMP desde SS-BB hacia PC4, PC5 y PC6

```
SW-BB#ping 190.108.10.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.5, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.20.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-BB#ping 190.108.30.7

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.7, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Ping desde SS-BB hacia PC7, PC8 y PC9:

Figura 33. Pruebas ICMP desde SS-BB hacia PC7, PC8 y PC9

```
SW-CC#ping 190.108.10.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.8, 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#ping 190.108.30.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Viendo los resultados obtenidos, podemos analizar que el ping no es exitoso entre los SW y PCs. Se realizaron las configuraciones en las VLAN en cada uno de los Switches atraves del protocolo de comunicaciones VTP, y también se configuro cada una de las interfaces que conectan a los SWs con los PCs en modo de acceso, teniendo en cuanta cada VLAN a la cual pertenecen. El resultado que no sea exitoso, radica en que hace falta la creación y configuración de los direccionamientos de red de cada Vlan (compras (10), Personal (25) y Planta (30)). Para mitigar este problema se requerirá la creación del lo mencionado anterior mente, teniendo en cuenta el direccionamiento asignado a cada PC para que se conecte a cada VLAN correspondiente, adicional también tener en cuenta la VLAN nativa.

CONCLUSIONES

- Al realizar el desarrollo de los escenarios propuestos para esta evaluación final, evidenciamos que se logró con lo establecido por la prueba de habilidades, ya que demostramos los conocimientos necesarios para el abordaje de los escenarios, mostrando el procedimiento y el paso a paso de cada uno de los ítems y la utilización correcta de los diferentes simuladores que se vieron durante todo el abordaje del curso, GNS3, Packet Tracer, y Smartlab de Cisco. Abordando los diferentes protocolos de enrutamiento se evidencia que dentro de cada configuración realizada en cada equipo se logró a satisfacción, ya que pusimos demostrar que por medio dela práctica adquirida durante el curso se lograron los escenarios a satisfacción.

- Al hacer la verificación final en la conectividad de Extremo a Extremo en el último escenario establecidos demuestra los conocimientos obtenidos tras el cumplimiento del curso sobre estas temáticas propuestas, al tener que analizar las posibles causas de los fallos en la búsqueda de paquetes mediante las pruebas ICMP realizados entre los dispositivos, identificando las configuraciones faltantes en dichos dispositivos y las soluciones más factibles para estos errores de conectividad.

- Mostramos que en el segundo escenario hay forma de poder enviar y recibir paquetes con la necesidad de configurar Vlans entre Switches, esto con el fin de que las pruebas a nivel de ICMP sean exitosas.

- Una vez completada las configuraciones sobre los 2 escenarios para cada dispositivo demostramos que los conocimientos adquiridos en el transcurso del curso fueron los necesarios para poder establecer métricas sobre cada escenario.

BIBLIOGRAFIA

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

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

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

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

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

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