DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CARLOS ALBERTO CHAPARRO FUYA

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

CARLOS ALBERTO CHAPARRO FUYA

Diplomado de opción de grado presentado para
optar el título de INGENIERO DE
TELECOMUNICACIONES

DIRECTOR:
ING. JUAN CARLOS VESGA G

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Tunja, 22 de mayo de 2020

AGRADECIMIENTOS

Doy gracias a Dios por darme la fuerza, la paciencia y la sabiduría para no solo empezar sino poder terminar este gran logro en mi vida, es un gran paso en mi vida personal y el comienzo de una vida profesional donde nos permitirá brindar ayuda a la sociedad para el continuo crecimiento de la misma.

Agradezco a mi familia en los cuales siempre conté con su apoyo, y en momentos de debilidad me ayudaron para poder cumplir el gran sueño de convertirme en un profesional

A si mismo agradezco a la universidad el cual me brindo las herramientas de trabajo que me permitieron cumplir mis logros, gracias a todo el grupo de trabajo de la escuela de ciencias básicas, tecnología e ingeniería – ECBTI por el acompañamiento en cada una de las actividades a lo largo de mi paso por la universidad, que aunque siempre hubieron momentos de dificultad ustedes siempre estuvieron ahí para ser ese gran apoyo que uno siempre requiere para no dejar de lados sus metas y logros.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

Protocolo BGP (Border Gateway Protocol): es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos.

Show ip route: es un comando de cisco que muestra la tabla completa de rutas IP, en si es un resumen de la tabla de enrutamiento o información de ruta para direcciones IP específicas, máscaras de red o protocolos.

Protocolo VTP: (Vlan Trunking Protocol) es un protocolo de mensajes de nivel 2 usado para configurar y administrar Vlans en equipos cisco.

Protocolo DTP (Dynamic Trunking Protocol): Es un protocolo creado por cisco system que opera entre switches.

Dynamic auto: es el modo por defecto de los switches Catalyst 2960 de cisco, el Puerto aguardara pasivamente la indicación del otro extremo del enlace para pasar a modo troncal.

Dynamic desirable: es el modo por defecto de los switches Catalyst 2950 de cisco, en este modo el Puerto activamente intenta convertir el enlace en un enlace troncal.

RESUMEN

El protocolo de puerta de enlace de frontera (BGP) es un protocolo el cual permite el intercambio de información de encaminamiento entre sistemas autónomos (AS) dicho intercambio de información de encaminamiento se hace entre Reuters externos que sean compatibles con el protocolo BGP
BGP es el sistema que utilizan los grandes nodos de internet para poder tener comunicación entre si y transferir una gran cantidad de información entre dos puntos de la red y su misión es poder encontrar la ruta más eficiente entre los nodos para poder brindar una correcta circulación de la información a través de internet.
VTP es un protocolo de mensajes de nivel 2 el cual se usa para administrar y realizar configuraciones VLANs en equipos cisco, el cual sirve para centralizar en un solo Switch la administración de todas las vlans de la red
Una de las grandes ventajas de este protocolo es que reduce la complejidad de la administración y el análisis del tráfico de redes en las que se han definidos las VLANs
Para configurar VLANs utilizando VTP se debe seleccionar uno de los switches como servidor VTP (también llamado Primary Domain Controller). Los switches Catalyst están configurados por defecto como servidores VTP. En el Switch servidor de VTP se crearán todas las VLANs. El resto de los switches serán clientes. En los switches cliente no hay que definir o crear las VLANs. Sólo habrá que asignar los puertos a las Vlans

Cisco CCNP permite que los usuarios puedan certificarse en un nivel intermedio superando una serie de exámenes en el cual se reflejan los conocimientos adquiridos durante el curso.

Palabras Clave: Cisco, CCNP, Conmutación, protocolo VTP, protocolo BGP, Enrutamiento, conectividad, Redes, Electrónica.

ABSTRACT

The Border Gateway Protocol (BGP) is a protocol which allows the exchange of routing information between autonomous systems (AS). This exchange of routing information is done between external Reuters that are compatible with the BGP protocol.
BGP is the system used by large internet nodes to be able to communicate with each other and transfer a large amount of information between two points on the network and its mission is to be able to find the most efficient route between the nodes in order to provide a correct circulation of information through the internet.
VTP is a level 2 message protocol which is used to manage and make VLAN configurations on Cisco equipment, which serves to centralize the administration of all vlans on the network on a single switch
One of the great advantages of this protocol is that it reduces the complexity of managing and analyzing traffic on networks in which VLANs have been defined.
To configure VLANs using VTP, one of the switches must be selected as the VTP server (also called Primary Domain Controller). Catalyst switches are configured by default as VTP servers. All VLANs will be created on the VTP server switch. The rest of the switches will be clients. VLANs do not have to be defined or created on client switches. Only the ports will have to be assigned to the VLANs

Cisco CCNP allows users to become certified at an intermediate level by passing a series of exams that require the knowledge acquired during the course.

Keywords: CISCO, CCNP, Switching, commutation, VTP protocol, BGP protocol, routing, networking, Electronics.

INTRODUCION

Con el desarrollo del presente informe lo que se pretende es dar conocer los conceptos básicos de los protocolos BGP y VTP y basándonos en ellos poder realizar las respectivas configuraciones y así dar solución a los dos escenarios expuestos en la guía de actividades el cual es un requisito para poder finalizar con éxito el diplomado de profundización cisco CCNP. Con el fin de poder realizar dicha solución de cada uno de los escenarios nos apoyamos en el software Packet tracer en el cual haremos las configuraciones y simulaciones y estas quedaran plasmadas por medio de pantallazos con su paso a paso del desarrollo, con la solución de estos ejercicios nos permite practicar las diferentes configuraciones de los protocolos estudiados y así tener una clara idea para llevar a cabo a la vida real.

En el escenario 1 encontraremos una red conformada por 4 router en el cual se realiza las configuraciones del protocolo BGP, asignando sus respectivas direcciones IP para poder obtener una relación de vecino BGP entre R1 y R2 de igual forma entre R2 y R3 teniendo en cuenta cada sistema Autónomo (AS).

En el escenario 2 encontramos una red el cual está conformada por 3 switches cada uno con 3 equipos donde se configura el protocolo VTP, inicialmente se configura el Switch SW-BB como el servidor y los Switches SW-AA y SW-CC se configuran como clientes, de igual forma se configura el protocolo DTP (dynamic Trunking Protocol), se asignan las diferentes direcciones IP dadas, de esta manera se podrá tener conexión entre cada equipo y esto es verificado por medio de Ping desde cada PC hacia los switches.

1. ESCENARIO 1

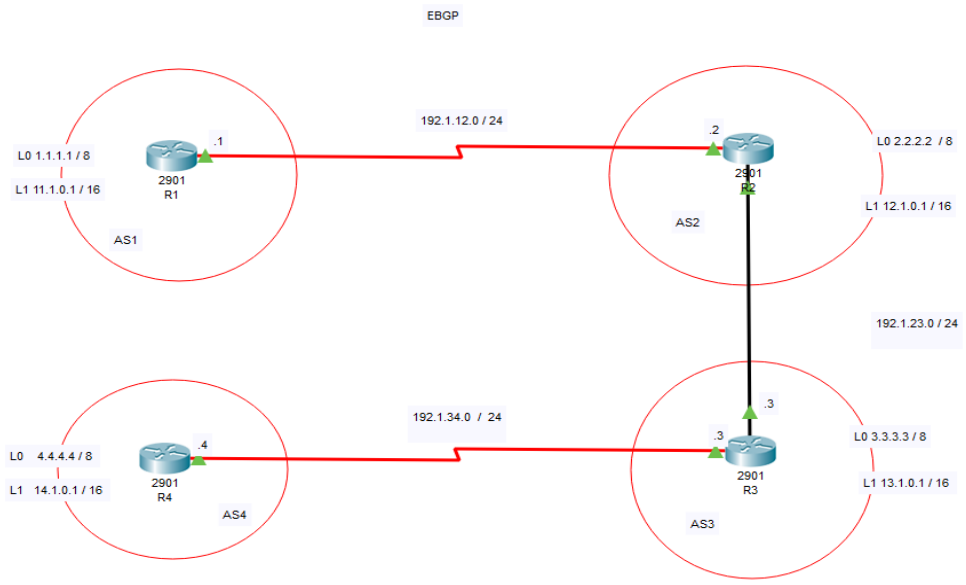

Figura 1 escenario 1

En la anterior imagen se describe nuestro primer escenario el cual consta de una pequeña red conformada por 4 routers conectados entre si, para la elaboracion de este escenario hacemos uso del software Packet tracer, en cada router se dan a conocer sus respetivas direcciones IP para sus configuraciones.

R1		
INTERFAZ	**DIRECCION IP**	**MASCARA**
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 1. Configuraciones IP R1

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#interface serial0/0/0
R1(config-if)#ip address 192.1.12.1 255.
^
% Invalid input detected at '^' marker.
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit
R1(config)#interface loopback0

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#exit
R1(config)#interface loopback 1

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#exit
R1(config)#router bgp 1
R1(config-router)#network 192.1.12.0 mask 255.255.255.0
R1(config-router)#network 1.1.1.1 mask 255.0.0.0
R1(config-router)#network 11.1.0.1 mask 255.255.0.0
R1(config-router)#neighbor 192.1.12.2 remote-as 2
R1(config-router)#
```

R2		
INTERFAZ	**DIRECCION IP**	**MASCARA**
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 2. Configuración direcciones IP R2

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#interface serial 0/0/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shut

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R2(config-if)#exit
R2(config)#interf
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface g0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shut

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

R2(config-if)#exit
R2(config)#interface loopback 0

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#exit
R2(config)#interface loopback 1

R2(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#exit
R2(config)#router bgp
% Incomplete command.
R2(config)#router bgp 2
R2(config-router)#network 192.1.12.0 mask 255.255.255.0
R2(config-router)#network 192.1.23.0 mask 255.255.255.0
R2(config-router)#network 2.2.2.2 mask 255.0.0.0
R2(config-router)#network 12.1.0.1 mas 255.255.0.0
R2(config-router)#neighbor 192.1.12.1 remote-as1
^
% Invalid input detected at '^' marker.
R2(config-router)#neighbor 192.1.12.1 remote-as 1
R2(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.12.1 Up

R2(config-router)#neighbor 192.1.23.3 remote-as 3
R2(config-router)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#
```

R3		
INTERFAZ	**DIRECCION IP**	**MASCARA**
Loopback 0	**3.3.3.3**	**255.0.0.0**
Loopback 1	**13.1.0.1**	**255.255.0.0**
S 0/0	**192.1.23.3**	**255.255.255.0**
E 0/0	**192.1.34.3**	**255.255.255.0**

Tabla 3 .Configuraciones direcciones IP R3

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#interface serial 0/0/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R3(config-if)#
R3(config-if)#exit
R3(config)#interface g0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R3(config-if)#exit
R3(config)#interface loopback 0

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#exit
R3(config)#inteface loopback 1
^
% Invalid input detected at '^' marker.
R3(config)#interface loopback 1

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

R3(config-if)#ip address 13.1.0.1 255.255.0.0
R3(config-if)#exit
```

R3(config)#router bgp 3
R3(config-router)# network 192.1.23.0 mask 255.255.255.0
R3(config-router)#network 192.1.34.0 mask 255.255.255.0
R3(config-router)#network 3.3.3.3 mask 255.0.0.0
R3(config-router)#network 13.1.0.1 mask 255.255.0.0
R3(config-router)#neighbor 192.1.23.2 remote-as 2
R3(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.23.2 Up

R3(config-router)#neighbor 192.1.34.4 remote-as 4

R3(config-router)#

R4		
INTERFAZ	**DIRECCION IP**	**MASCARA**
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 4. Configuraciones direcciones IP R4

Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R4
R4(config)#interface serial 0/0/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shut

R4(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

R4(config-if)#exit
R4(config)#inter
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
face loopback 0

R4(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#exit
R4(config)#interface loopback 1

R4(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

R4(config-if)#ip address 14.1.0.1 255.255.0.0

```
R4(config-if)#exit
R4(config)#router bgp 4
R4(config-router)#network 192.1.34.0 mask 255.255.255.0
R4(config-router)#network 4.4.4.4 mask 255.0.0.0
R4(config-router)#network 14.1.0.1 mask 255.255.0.0
R4(config-router)#neighbor 192.1.34.3 remote-as 3
R4(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.34.3 Up
```

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.

Comando show ip route

```
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, E - EGP
       i - IS-IS, 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

Gateway of last resort is not set

     1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       1.0.0.0/8 is directly connected, Loopback0
L       1.1.1.1/32 is directly connected, Loopback0
B    2.0.0.0/8 [20/0] via 192.1.12.2, 00:00:00
B    3.0.0.0/8 [20/0] via 192.1.12.2, 00:00:00
B    4.0.0.0/8 [20/0] via 192.1.12.2, 00:00:00
     11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       11.1.0.0/16 is directly connected, Loopback1
L       11.1.0.1/32 is directly connected, Loopback1
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0/16 [20/0] via 192.1.12.2, 00:00:00
     13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0/16 [20/0] via 192.1.12.2, 00:00:00
     14.0.0.0/16 is subnetted, 1 subnets
B       14.1.0.0/16 [20/0] via 192.1.12.2, 00:00:00
     192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.12.0/24 is directly connected, Serial0/0/0
L       192.1.12.1/32 is directly connected, Serial0/0/0
B    192.1.23.0/24 [20/0] via 192.1.12.2, 00:00:00
B    192.1.34.0/24 [20/0] via 192.1.12.2, 00:00:00

R1>
```

Figura 2 comando show ip R1

```
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, E - EGP
       i - IS-IS, 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

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:00:00
     2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       2.0.0.0/8 is directly connected, Loopback0
L       2.2.2.2/32 is directly connected, Loopback0
B    3.0.0.0/8 [20/0] via 192.1.23.3, 00:00:00
B    4.0.0.0/8 [20/0] via 192.1.23.3, 00:00:00
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0/16 [20/0] via 192.1.12.1, 00:00:00
     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       13.1.0.0/16 [20/0] via 192.1.23.3, 00:00:00
     14.0.0.0/16 is subnetted, 1 subnets
B       14.1.0.0/16 [20/0] via 192.1.23.3, 00:00:00
     192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.12.0/24 is directly connected, Serial0/0/0
L       192.1.12.2/32 is directly connected, Serial0/0/0
     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
B    192.1.34.0/24 [20/0] via 192.1.23.3, 00:00:00
```

Figura 3 comando show ip R2.

En las figuras 2 y 3 evidenciamos la ejecución del comando show IP route en el router 1 y router 2. Donde se muestran las configuraciones del protocolo BGP.

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.

```
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, E - EGP
       i - IS-IS, 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

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
B    2.0.0.0/8 [20/0] via 192.1.23.2, 00:00:00
     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
B    4.0.0.0/8 [20/0] via 192.1.34.4, 00:00:00
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0/16 [20/0] via 192.1.23.2, 00:00:00
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0/16 [20/0] via 192.1.23.2, 00:00:00
     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       14.1.0.0/16 [20/0] via 192.1.34.4, 00:00:00
B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:00:00
     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, Serial0/0/0
L       192.1.34.3/32 is directly connected, Serial0/0/0
```

Figura 4. Comando show ip R3

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.

IOS Command Line Interface

```
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, E - EGP
       i - IS-IS, 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

Gateway of last resort is not set

B    1.0.0.0/8 [20/0] via 192.1.34.3, 00:00:00
B    2.0.0.0/8 [20/0] via 192.1.34.3, 00:00:00
B    3.0.0.0/8 [20/0] via 192.1.34.3, 00:00:00
     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       11.1.0.0/16 [20/0] via 192.1.34.3, 00:00:00
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0/16 [20/0] via 192.1.34.3, 00:00:00
     13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0/16 [20/0] via 192.1.34.3, 00:00:00
     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
B    192.1.12.0/24 [20/0] via 192.1.34.3, 00:00:00
B    192.1.23.0/24 [20/0] via 192.1.34.3, 00:00:00
     192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.1.34.0/24 is directly connected, Serial0/0/0
L       192.1.34.4/32 is directly connected, Serial0/0/0

R4>
```

Figura5. Comando show ip R4

Configuración de las id de cada router

R1

```
R1>en
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#bgp router-id
              ^
% Invalid input detected at '^' marker.

R1(config)#router bgp 1
R1(config-router)#bgp router-id 22.22.22.22
R1(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.12.2 Up
%BGP-5-ADJCHANGE: neighbor 192.1.12.2 Up
```

R2

```
R2>en
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router bgp 2
R2(config-router)#bgp router-id 33.33.33.33
R2(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.23.3 Up
%BGP-5-ADJCHANGE: neighbor 192.1.12.1 Up
%BGP-5-ADJCHANGE: neighbor 192.1.23.3 Up

%BGP-3-NOTIFICATION: sent to neighbor 192.1.12.1 4/0 (hold time expired) 0 bytes
%BGP-5-ADJCHANGE: neighbor 192.1.12.1 Up
```

R3

```
R3>en
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.34.4 Up
%BGP-5-ADJCHANGE: neighbor 192.1.23.2 Up
%BGP-5-ADJCHANGE: neighbor 192.1.34.4 Up
```

R4

```
R4#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#route bgp 4
R4(config-router)#bgp router-id 66.66.66.66
R4(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.34.3 Up
```

Figura 6. Configuración Id R1, R2, R3, R4

En la figura 6 se evidencia la asignación de las Id dadas para cada uno de los routers

EVIDENCIA DE PING ENTRE CADA ROUTER

Realizamos ping entre las interfaces 192.1.34.3 y 192.1.34.4 del router 3 as3 donde se evidencia es exitoso de igual forma realizamos ping a la Loopback 1 del router 4 14.1.0.1

```
R1>ping 192.1.34.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.34.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/24 ms

R1>ping 192.1.34.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.34.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/19 ms

R1>ping 14.1.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 14.1.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/4/16 ms

R1>
```

Figura 7. Realización ping R1

En la siguiente imagen (imagen8) se realiza ping entre los router 1 y router 3 donde es satisfactorio, se evidencia la comunicación entre los router R3 sistema autónomo (AS 3) y R1 Sistema Autónomo (AS1) a las interfaces 192.1.12.1, 192.1.12.2 y a la interfaz Loopback 0 del router R1

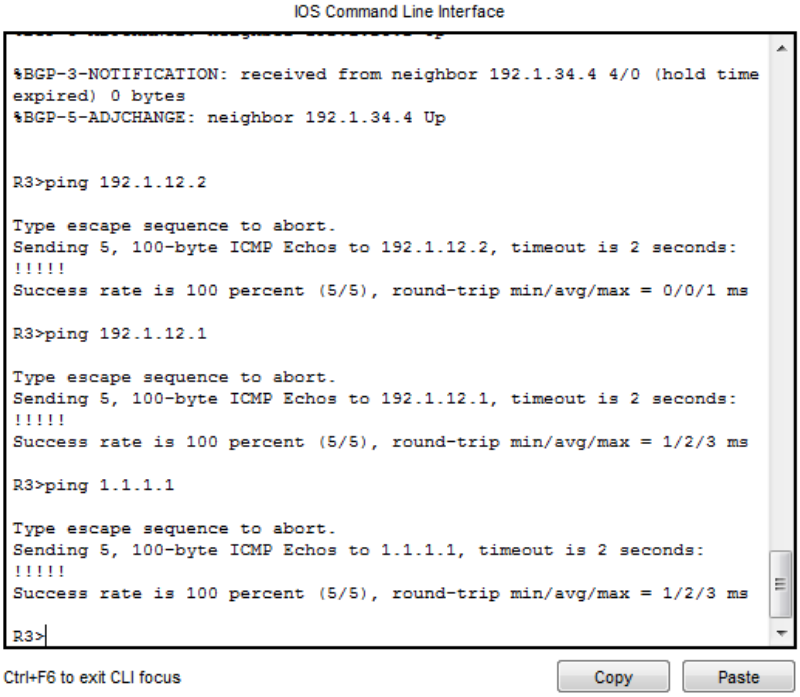

Figura 8. Realización ping R3

Figura 2. Simulación de escenario 1

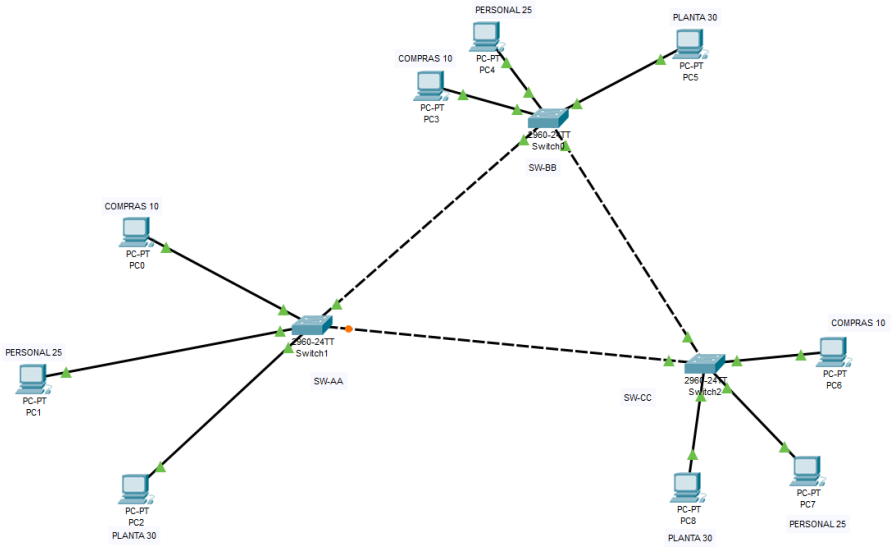

Figura 9. Escenario 2.

En la figura 9 el cual corresponde al escenario 2, es una red que consta de 3 switches y 9 computadores en donde se pretende configurar el protocolo VTP así como el protocolo DTP (Dynamic Trunking Protocol) se realizó las diferentes configuraciones, se asignaron las vlan según corresponden

A. Configurar VTP 1.

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-BB>en
SW-BB#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#vtp mode server
Device mode already VTP SERVER.
SW-BB(config)#vtp domain CCNP
Domain name already set to CCNP.
SW-BB(config)#vtp password cisco
Password already set to cisco
SW-BB(config)#exit
SW-BB#
%SYS-5-CONFIG_I: Configured from console by console
```

```
SW-AA>en
SW-AA#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#vtp mode client
Device mode already VTP CLIENT.
SW-AA(config)#vtp domain CCNP
Domain name already set to CCNP.
SW-AA(config)#vtp password cisco
Password already set to cisco
SW-AA(config)#exit
SW-AA#
%SYS-5-CONFIG_I: Configured from console by console

SW-CC>en
SW-CC#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#vtp mode client
Device mode already VTP CLIENT.
SW-CC(config)#vtp domain CCNP
Domain name already set to CCNP.
SW-CC(config)#vtp password cisco
Password already set to cisco
SW-CC(config)#exit
SW-CC#
%SYS-5-CONFIG_I: Configured from console by console
```

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

```
SW-BB>en
SW-BB#config t
Enter configuration commands, one per line.  End with CNTL/Z.
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-BB(config)#exit
SW-BB#
%SYS-5-CONFIG_I: Configured from console by console

SW-BB#show 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 10. Configuración vtp Switch 0

```
% Invalid input detected at '^' marker.

SW-AA(config)#vtp mode client
Setting device to VTP CLIENT mode.
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-AA(config)#
SW-AA(config)#exit
SW-AA#
%SYS-5-CONFIG_I: Configured from console by console

SW-AA#show 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 11. Configuración vtp Switch 1.

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-CC
SW-CC(config)#vtp mode client
Setting device to VTP CLIENT mode.
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
SW-CC(config)#exit
SW-CC#
%SYS-5-CONFIG_I: Configured from console by console

SW-CC#show 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#
```

Figura 12. Configuración vtp Switch 2

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.

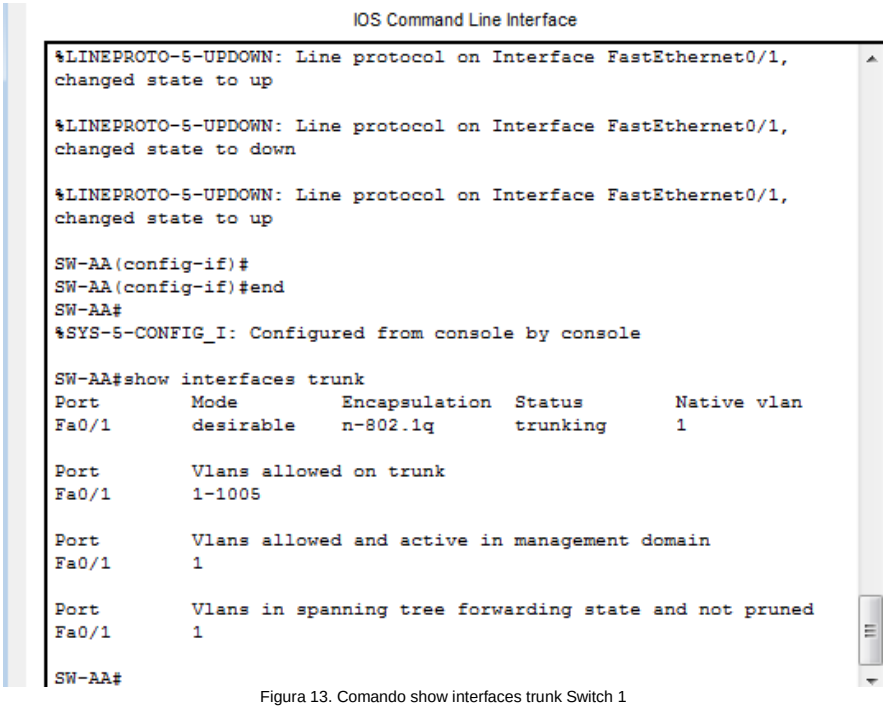

Figura 13. Comando show interfaces trunk Switch 1

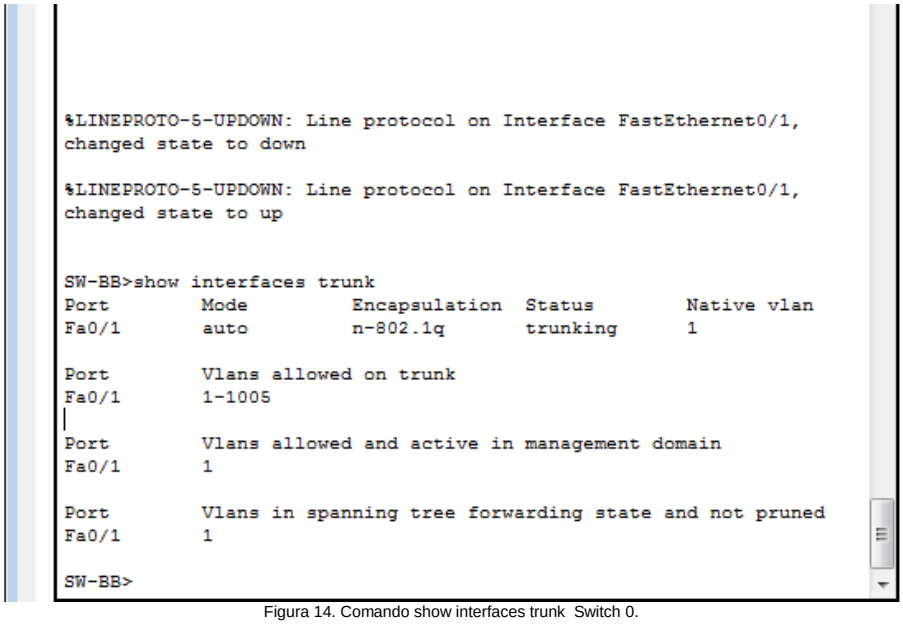

Figura 14. Comando show interfaces trunk Switch 0.

SW-AA#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface f0/3
SW-AA(config-if)#switchport mode trunk

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

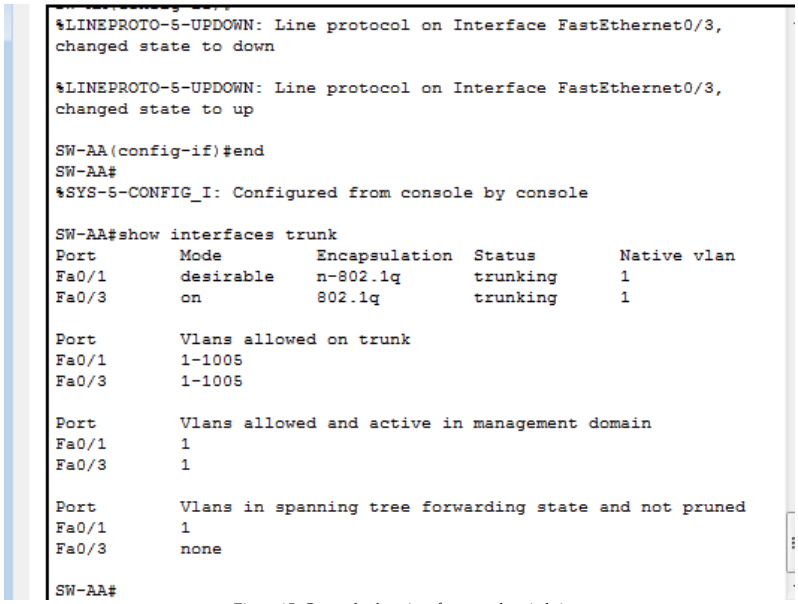

Figura 15. Comando show interfaces trunk switch 1

SW-CC>en
SW-CC#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#interface f0/1
SW-CC(config-if)#switchport mode trunk

SW-BB>en
SW-BB#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#interface f0/3
SW-BB(config-if)#switchport mode trunk

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 Admón. (99)

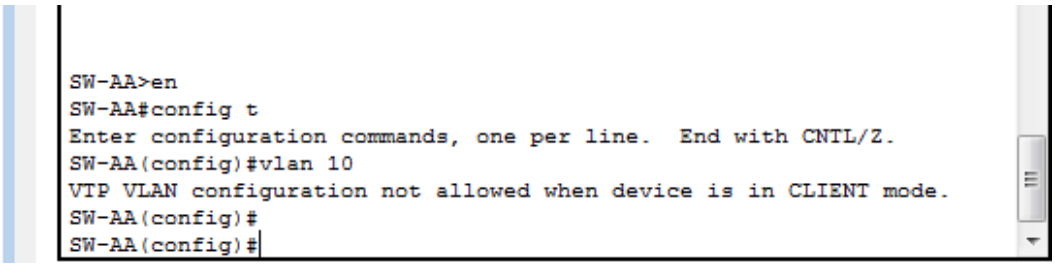

Figura 16. Asignación puerto y vlan Switch 1

SW-BB>en
SW-BB#config 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
SW-BB(config-vlan)#end
SW-BB#
%SYS-5-CONFIG_I: Configured from console by console

SW-BB#

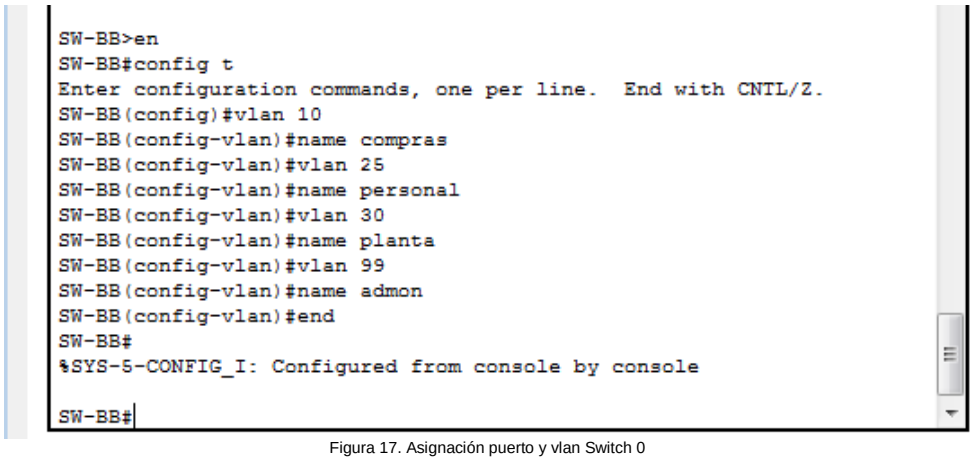

Figura 17. Asignación puerto y vlan Switch 0

10. Verifique que las VLANs han sido agregadas correctamente

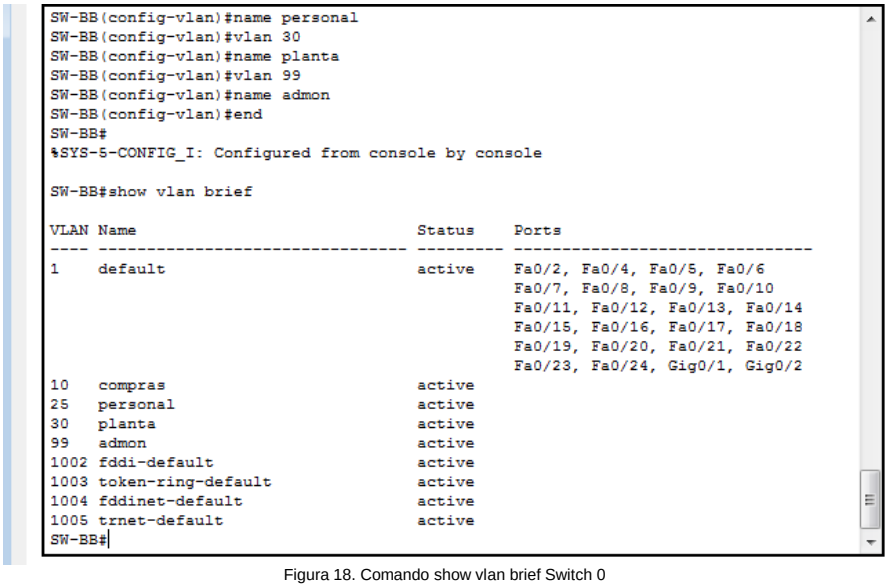

Figura 18. Comando show vlan brief Switch 0

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

Interfaz	Vlan	Direcciones IP de los pcs
F0/10	Vlan 10	190.108.10.X / 24
F0/15	Vlan 25	190.108.10.X / 24
F0/20	Vlan 30	190.108.10.X / 24

X=número de cada pc particular

Tabla 5. Configuraciones puerto y vlan

12. 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>en
SW-AA#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface f0/10
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 10
SW-AA(config)#interface f0/15
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#exit
SW-AA(config)#interface f0/20
SW-AA(config-if)#
SW-AA(config-if)#switchport mode access
SW-AA(config-if)#switchport access vlan 30
SW-AA(config-if)#no shut
SW-AA(config-if)#exit
SW-AA(config)#
```

```
SW-BB>en
SW-BB#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW-BB(config)#interface f0/10
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 10
SW-BB(config-if)#no shut
SW-BB(config-if)#interface f0/15
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 25
SW-BB(config-if)#exit
SW-BB(config)#interface f0/20
SW-BB(config-if)#switchport mode access
SW-BB(config-if)#switchport access vlan 30
SW-BB(config-if)#no shut
SW-BB(config-if)#exit
SW-BB(config)#
```

```
SW-CC>en
SW-CC#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#interface f0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config)#interface f0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
SW-CC(config-if)#exit
```

```
SW-CC(config)#interface f0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30
SW-CC(config-if)#no shut
SW-CC(config-if)#
```

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

INTERFAZ	VLAN	DIRECCION IP PCs
SW-AA F0/10	VLAN 10	190.108.10.1
SW-AA F0/15	VLAN 25	190.108.10.2
SW-AA F0/20	VLAN 30	190.108.10.3
SW-BB F0/10	VLAN 10	190.108.10.4
SW-BB F0/15	VLAN 25	190.108.10.5
SW-BB F0/20	VLAN 30	190.108.10.6
SW-CC F0/10	VLAN 10	190.108.10.7
SW-CC F0/15	VLAN 25	190.108.10.8
SW-CC F0/20	VLAN 30	190.108.10.9

Tabla 6. Configuraciones puertos vlan pcs

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.

EQUIPO	INTERFAZ	DIRECCION IP	MASCARA
SW-AA	VLAN 99	190.108.99.1	255.255.255.0
SW-BB	VLAN 99	190.108.99.2	255.255.255.0
SW-CC	VLAN 99	190.108.99.3	255.255.255.0

Tabla 7. Configuraciones direcciones IP switches

```
SW-AA>en
SW-AA#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW-AA(config)#interface vlan 99
SW-AA(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0
SW-AA(config-if)#no shut
SW-AA(config-if)#


SW-BB>en
SW-BB#config t
Enter configuration commands, one per line. End with CNTL/Z.
```

```
SW-BB(config)#interface vlan 99
SW-BB(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

SW-BB(config-if)#ip address 190.108.99.2 255.255.255.0
SW-BB(config-if)#no shut
SW-BB(config-if)#


SW-CC>en
SW-CC#config t
Enter configuration commands, one per line. End with CNTL/Z.
SW-CC(config)#interface vlan 99
SW-CC(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

SW-CC(config-if)#ip address 190.108.99.3 255.255.255.0
SW-CC(config-if)#no shut
SW-CC(config-if)#
```

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

Se realiza Ping desde la pc compras de SW-AA a la pc compras de SW-BB y SW-CC el cual es exitosa la comunicación entre ellos.

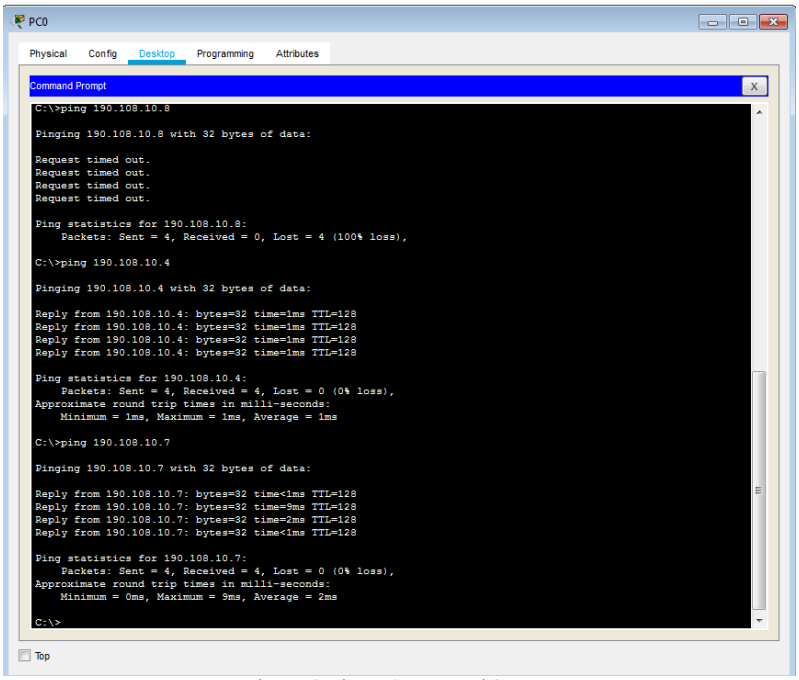

Figura 19. Ping Pc0 – personal SW_AA

Ping desde la pc personal de SW-AA a las Pc personal de SW-BB y SW-CC el cual es exitoso y se evidencia la comunicación entre ellos

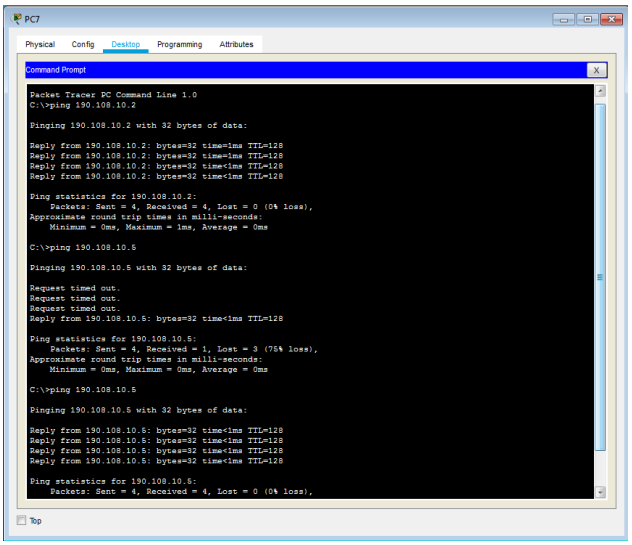

Figura 20. Ping Pc0 – planta SW_AA

ping desde la pc planta SW_AA a las pc planta de SW-BB y SW-CC

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

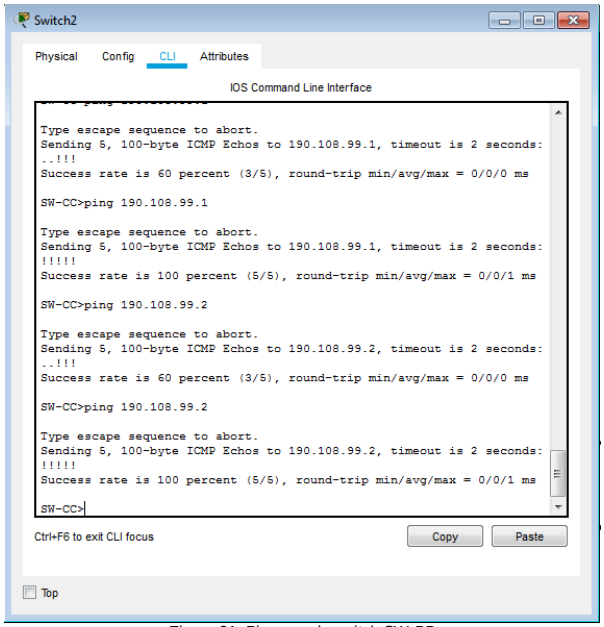

Figura 21. Ping a cada switch SW-BB

Ping desde el switch SW-BB a los demas switchs de la red

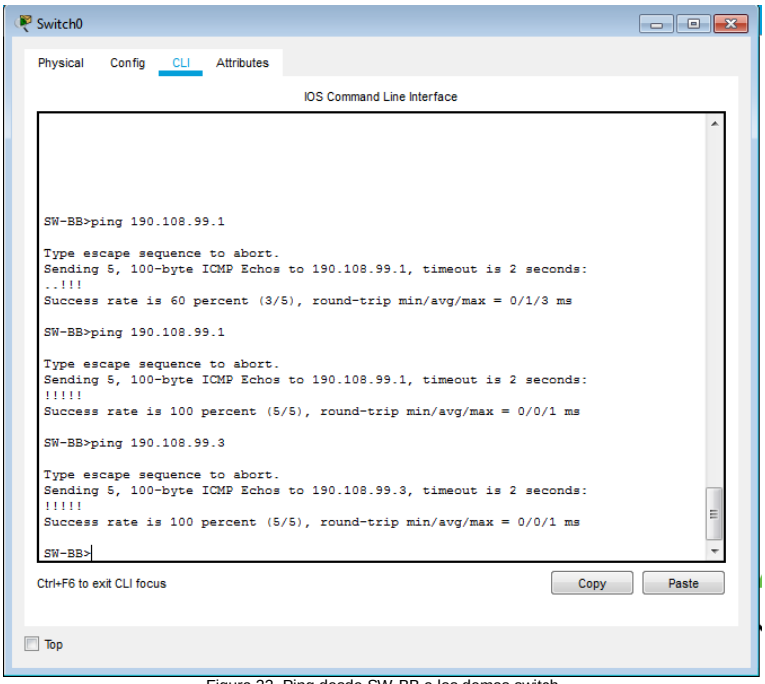

Figura 22. Ping desde SW-BB a los demas switch

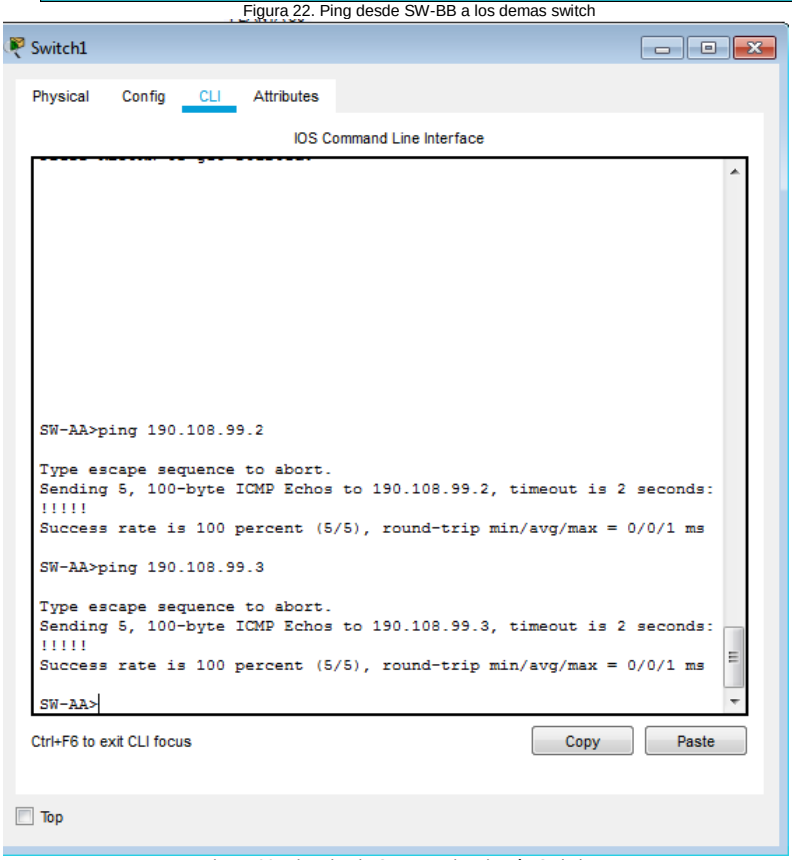

Figura 23. Ping desde SW-AA a los demás Switch

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

Se hace ping desde el Switch SW-CC a las pcs conectadas al Switch SW-AA y estos no han sido exitosos puesto que las direcciones IP de cada equipo de cómputo no han sido configuradas dentro de la misma vlan

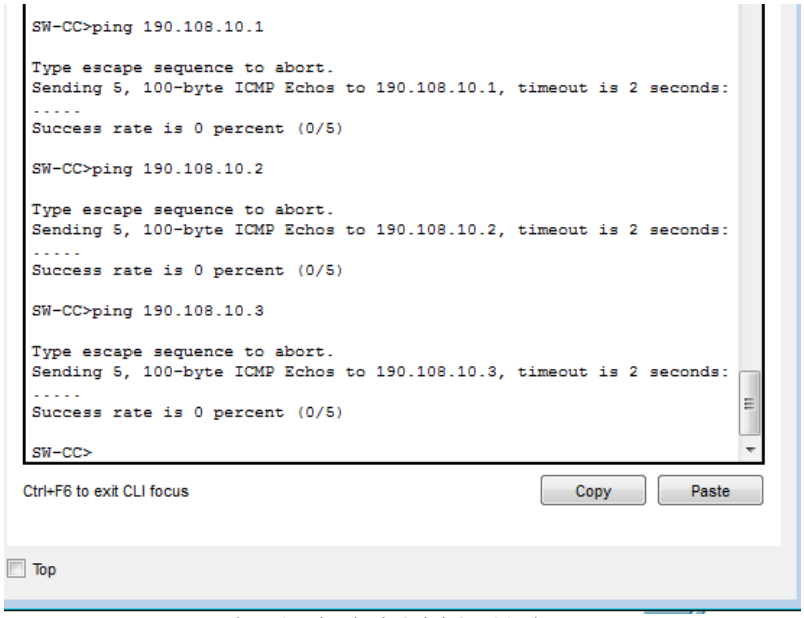

Figura 24. Ping desde Switch SW-CC a las pc

CONCLUSIONES

Con el desarrollo de cada una de las actividades se ha podido adquirir un sin número de conocimientos y habilidades el cual nos permiten poder poner en práctica en nuestra vida profesional como futuros ingenieros de telecomunicaciones de igual forma nos apoyamos de software como Packet tracer (en mi caso) que permite poder llevar a cabo dicha solución y práctica.

Es de suma importancia tener los conocimientos básicos sobre el enrutamiento así como saber los diferentes comandos que permiten realizar las configuraciones adecuadas para poder realizar una comunicación entre router y/o switches ya que este tipo de configuraciones hacen que las comunicaciones entre empresas, sedes, gobiernos quizá sea posible y así poder estar al tanto de todo los movimientos en general de las entidades y compañías.

Sin duda alguna la realidad de las telecomunicaciones es otra y muy diferente a lo que nos ofrecen las simulaciones virtuales y software como (Packet tracer, gns3… etc.) sin embargo estos software nos acercan un poco más a lo que se debe realizar en la vida de un ingeniero de telecomunicaciones y su vida laboral y gracias a estos simuladores se permite tener una idea clara sobre nuestra vida laboral como realidad.

BIBLIOGRÁFIA

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

Froom, R., Frahim, E. (2015). CISCO Press (Ed). InterVLAN Routing. 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