

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES
PRÁCTICAS CCNP

JAIVER ALEXIS ARIAS CADENA

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

DIPLOMADO DE PROFUNDIZACION CISCO PRUEBA DE HABILIDADES
PRÁCTICAS CCNP

JAIVER ALEXIS ARIAS CADENA

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

DIRECTOR: MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

Villavicencio, 22 de mayo de 2020

AGRADECIMIENTOS

De manera muy especial doy gracias a DIOS por haberme permitido alcanzar un logro más en mi vida.

Apreciados tutores, compañeros de grupo y público en general tengo el gusto de expresar mis más sinceros agradecimientos, como medio de gratitud por esta meta conseguida.

A mis padres, quienes me apoyaron en todo lo indispensable, a mi esposa que tuvo la suficiente paciencia para apoyarme en esos tiempos difíciles que todo parecía complicarse.

Agradezco a la Universidad Nacional Abierta y A Distancia, que con sus docentes y con ayuda de todas esas valiosas herramientas tecnológicas y pedagógicas, lograron maximizar mi potencial académico, competencias y de aprendizaje autónomo y lograr mi titulación en la carrera de Ingeniería Electrónica.

CONTENIDO

AGRADECIMIENTOS.....	4
CONTENIDO.....	5
LISTA DE TABLAS.....	6
LISTA DE FIGURAS.....	7
GLOSARIO.....	8
RESUMEN.....	9
ABSTRACT.....	10
INTRODUCCION.....	11
DESARROLLO.....	12
1. Escenario 1.....	12
2. Escenario 2.....	21
CONCLUSIONES.....	34
BIBLIOGRAFIAS.....	35

LISTA DE TABLAS

Tabla 1. Configuración direcciones IP.....	26
Tabla 2. Direcciones IP en los Switches.....	27

LISTA DE FIGURAS

Figura 1. Escenario 1.....	12
Figura 2. Esquema de la topología en packet tracer.....	13
Figura 3. Escenario 2, simulación del escenario 2.....	21
Figura 4. Ping de PC1 a PC2.....	28
Figura 5. Ping de PC1 a PC3.....	28
Figura 6. Ping de PC1 a PC4.....	28
Figura 7. Ping de PC1 a PC7.....	29
Figura 8. Ping de PC2 a PC5.....	29
Figura 9. Ping de PC2 a PC3.....	29
Figura 10. Ping de PC2 a PC8.....	29
Figura 11. Ping de PC3 a PC6.....	30
Figura 12. Ping de PC3 a PC5.....	30
Figura 13. Ping de PC3 a PC6.....	30
Figura 14. Ping de PC3 a PC9.....	30

GLOSARIO

Configuración

Es darle forma a algo (organizar elementos que constituyan algo dándoles formas y características en particular).

Enrutamiento

Es el camino por el cual se envían datos en una red (la ruta más adecuada).

Interfaz

Es un conjunto de dispositivos que se utilizan para conectar dos sistemas entre sí (componentes o programas de cualquier tipo) comunicación en niveles distintos con intercambio de información).

Protocolo

Conjunto de reglas o normas que facilitan que varias entidades de un sistema de comunicación se entre Llassen o comuniquen entre sí, transmitiendo la información adecuada en (cualquier tipo de variación de una magnitud física).

Router

Es un instrumento que lleva el tráfico a la red, producto del hardware que permite interconectar los computadores.

Switch

Este dispositivo analógico interconecta operadores y redes en el nivel de enlace de datos o capa 2 del modelo OSI u Open Systems Interconnection.

RESUMEN

En el presente trabajo tiene como propósito realizar el estudio y análisis de dos escenarios a partir de los conocimientos adquiridos durante el desarrollo del presente diplomado en CCNP, lo cual nos permite ahondar sobre los diferentes protocolos enrutamiento y su responsabilidad en establecer reglas que permitan la conmutación de información sobre una red.

En el escenario uno, se compone de un arreglo de cuatro routers conectados en cascada mediante interfaces seriales y Ethernet respectivamente, los cuales se interconectan mediante el protocolo BGP para anunciar el estado de la topología de la red en cuanto a las redes asociadas.

En el escenario dos, se compone del montaje de una red local mediante un arreglo de 3 switch de capa 2, que se interconectan mediante el protocolo VTP en el modelo cliente-servidor para poner en conocimiento las VLAN configuradas en el servidor a los equipos clientes. De tal manera que se limitan los dominios de broadcast para las interfaces que poseen las VLAN configuradas por cada switch.

En este orden de ideas se podría decir que el diplomado en profundización CISCO ayuda a conocer más afondo esta temática, como funciona y a apropiarnos de acciones tales como la posibilidad aprender de forma práctica como los administradores de red y problemáticas similares que puedan perjudican enormemente a la red sean resueltas con nuestra experiencia.

En este trabajo se pudo realizar de manera práctica en la electrónica como administrar una red (conocimiento del diseño de red hasta la capacidad de esta en conectarse) permitiendo mayor competitividad en las empresas ya sean medianas o pequeñas en un mundo globalizado y cambiante.

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

ABSTRACT

The purpose of this work is to carry out the study and analysis of two scenarios based on the knowledge acquired during the development of this diploma course in CCNP, which allows us to delve into the different routing protocols and their responsibility in establishing rules that allow switching of information about a network.

In scenario one, it consists of an array of four routers cascaded via serial and Ethernet interfaces respectively, which are interconnected using the BGP protocol to announce the status of the network topology for associated networks.

In scenario two, it consists of mounting a local network using an arrangement of 3 layer 2 switches, which are interconnected using the VTP protocol in the client-server model to inform the VLANs configured on the server to the client computers. . In such a way that the broadcast domains are limited for the interfaces that have the VLANs configured by each switch.

In this order of ideas, it could be said that the CISCO in-depth course helps to learn more about this topic, how it works and to take ownership of actions such as the possibility of learning in a practical way as network administrators and similar problems that can greatly harm the network are resolved with our experience.

In this work, it was possible to carry out in a practical way in electronics how to manage a network (knowledge of network design until its capacity to connect) allowing greater competitiveness in companies, whether medium or small, in a globalized and changing world.

Keywords: CISCO, CCNP, Routing, Swicthing, Networking, Electronics

INTRODUCCIÓN

El presente trabajo tiene como propósito el desarrollo de dos escenarios que se complementan mediante la aplicación de los protocolos de enrutamiento como el BGP en una red de equipos capa 3, y el protocolo VTP para la configuración y administración de la VLAN en una red switch capa 2.

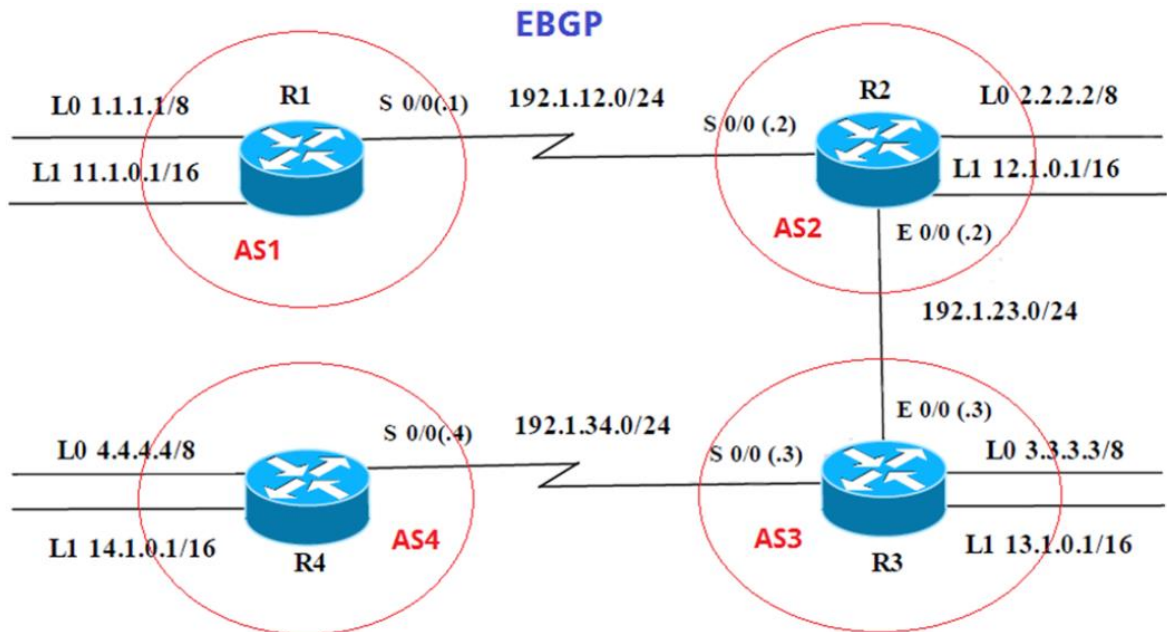
El primer escenario que se presenta se constituye de un arreglo de 4 routers que mediante una conexión específica de interconexión, comparten la información de enrutamiento a través del protocolo BGP a nivel de capa 3 con el fin de anunciar las redes virtuales Loopback y física a través de la interfaces seriales; en el segundo escenario, presenta un arreglo de 3 switch de capa 2 para red local que aprovechando el protocolo VTP que mediante la centralización en un solo switch para la administración de las VLAN se propaga dicha información a los otros equipos de capa 2 que operan como clientes. Finalmente, mediante los diferentes comandos se pudo verificar la conectividad de las terminales pertenecientes a mismo segmento de red.

Por lo que el desarrollo de estos dos escenarios, permiten acercarnos al panorama de un mundo globalizado y cambiante que genera nuevos conocimientos se hace necesario reconocer la importancia de la programación como facilitador de eventos en la vida de toda la sociedad, en este orden de ideas el desarrollo de este trabajo permite asimilar los diferentes conceptos de modelos de capas y aplicarlos de forma práctica en relación a los contenidos del diplomado.

DESARROLLO

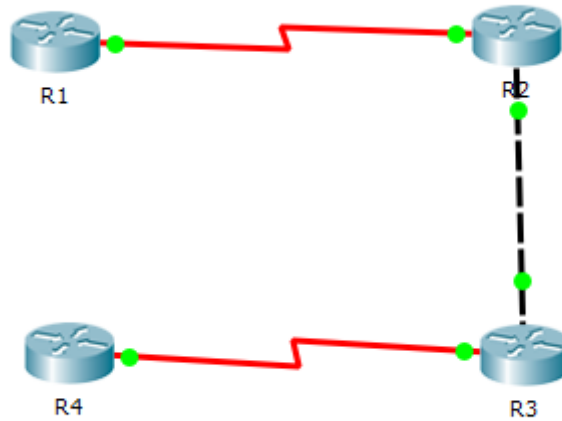
1. ESCENARIO 1.

Figura 1. Escenario 1



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*.

Figura 2. Esquema de la topología en Packet Tracer



Configuración ROUTER R1.

```
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 serial0/0/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown
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
```

Configuración ROUTER R2.

```
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 s0/0/0
```

```

R2(config-if)#ip add 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#interface g0/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#no shutdown
R2(config)#router bgp 2
R2(config-router)#bgp router
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 12.1.12.0 mask 255.255.255.0
R2(config-router)#neighbor 192.1.12.1 remote-as 1

```

A continuación se puede observar la ejecución comando show ip route, tanto el ROUTER R1 como al ROUTER R2 lo cuales presentan en la tabla de enrutamiento las direcciones de Loopback, las direcciones de las redes conectadas de forma directa, y las redes Loopback del ROUTER vecino, las cuales se puede identificar mediante la letra Bindicando que fueron aprendidas a través del protocolo BGP.

Respuesta del comando show ip route desde el ROUTER 1.

```

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 externaltype 1, E2 - OSPF externaltype 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
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
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

```

Respuesta del comando show ip route desde el ROUTER 2.

```
R2#showip 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 externaltype 1, E2 - OSPF externaltype 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  
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  
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
```

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*.

Configuración ROUTER R2.

```
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  
R2(config-router)#neighbor 192.1.23.3 remote-as 3
```

Configuración ROUTER R3.

```
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)#inter g0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#
R3(config-if)#interface s0/0/0
R3(config-if)#ip add 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config)#router bgp 3
R3(config-router)#bgp route
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
R3(config-router)#neighbor 192.1.23.2 remote-as 2

```

A continuación, se observa la ejecución del comando show ip route, en el ROUTER R2 se ha actualizado su tabla de enrutamiento y contiene las direcciones de Loopback del ROUTER R3, porque este equipo ha aprendido hasta este momento 4 rutas a través del protocolo BGP las cuales se especifica mediante el prefijo B. Por otra parte, el ROUTER R3 contiene en su tabla de enrutamiento las redes conectadas directamente, las cuales fueron configuradas en sus interfaces Loopback y las redes que lo comunican con los ROUTER R2 y R4 mediante las interfaces fastEthernet 0/0 y serial 0/0/0 respectivamente.

Respuesta del comando show ip route desde el ROUTER 2.

```

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
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
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

Respuesta del comando show ip route desde el ROUTER 3.

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 externaltype 1, E2 - OSPF externaltype 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
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
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

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*.

Configuración ROUTER R3.

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

Configuración ROUTER R4.

```
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 add 14.1.0.1 255.255.0.0
R4(config-if)#interface s0/0/0
R4(config-if)#ip add 192.1.34.4 255.255.255.0
R4(config-if)#clock rate 64000
R4(config-if)#no shutdown
R4(config)#router bgp 4
R4(config-router)#bgp router-id 66.66.66.66
R4(config-router)#network 4.0.0.0 mask 255.0.0.0
R4(config-router)#network 14.1.0.0 mask 255.255.0.0
R4(config-router)#network 192.1.34.0 mask 255.255.255.0
R4(config-router)#neighbor 192.1.34.3 remote-as 3
```

Para constituir las relaciones de adyacencia mediante las direcciones de Loopback, el ROUTER vecino necesita informar la interfaz asociado que implica una configuración adicional para los vecinos.

Configuración ROUTER R3.

```
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
```

Configuración ROUTER R4.

```
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 4
```

A continuación, se presenta el resultado del comando show ip route, en el ROUTER R3 ha actualizado su tabla de enrutamiento y la dirección de red que conecta este equipo con R4 ha cambiado y ahora corresponde a la dirección de Loopback 0, la cual aparece como una dirección estática tal como se estableció anteriormente. Igualmente, se puede identificar que la dirección de red de la interfaz Loopback 1 se sigue aprendiendo mediante el protocolo BGP, pero ahora se alcanza mediante la interfaz Loopback 0 de R4. La tabla de enrutamiento del ROUTER R4 se puede evidenciar que la dirección mediante la cual este se comunica con sus vecinos BGP ha cambiado y ahora corresponde a la dirección de la interfaz Loopback 0 de R3. El resultado del comando show ip route, la ruta estática que se creó hacia R3.

Respuesta del comando show ip route desde el ROUTER 3.

```
R3#showip 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 externaltype 1, E2 - OSPF externaltype 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
S 4.0.0.0/8 [1/0] via 192.1.34.4
11.0.0.0/16 is subnetted, 1 subnets
B 11.1.0.0/16 [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
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

Respuesta del comando show ip route desde el ROUTER 4.

R4#showip route

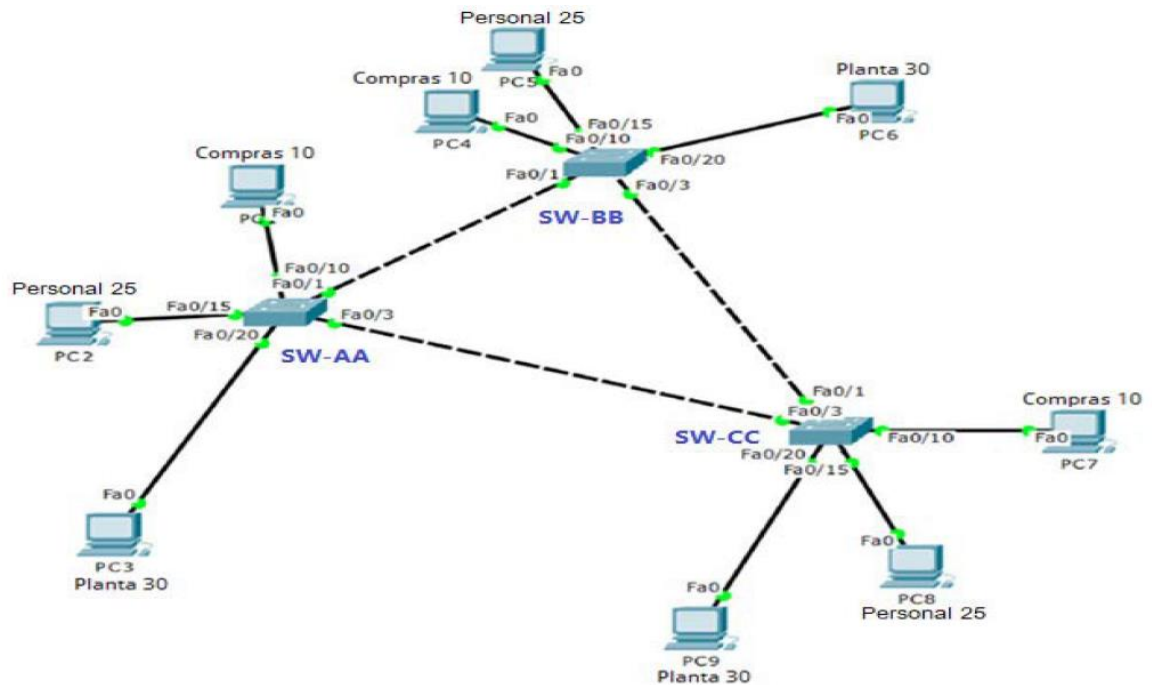
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF externaltype 1, E2 - OSPF externaltype 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS 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

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
14.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 14.1.0.0/16 is directly connected, Loopback1
L 14.1.0.1/32 is directly connected, Loopback1
192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.1.34.0/24 is directly connected, Serial0/0/0
L 192.1.34.4/32 is directly connected, Serial0/0/0

2. ESCENARIO 2.

Figura 3. 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(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-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(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
```

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

Respuesta del comando *show vtp status* en el SWITCH SW-AA.

```
SW-AA#showvtp 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
```

Respuesta del comando *show vtp status* en el SWITCH SW-BB.

```
SW-BB#showvtp 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)
```

Respuesta del comando *show vtp status* en el SWITCH SW-CC.

```
SW-CC#showvtp 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

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 *dynamicdesirable*.

```
SW-BB(config)#interfacefastEthernet 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*.

```
SW-BB#show interfaces 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 1
```

6. Entre SW-AA y SW-BB configure un enlace "trunk" estático utilizando el comando *switchportmodetrunken* la interfaz F0/3 de SW-AA.

```
SW-AA(config)#inter fastEthernet 0/3  
SW-AA(config-if)#switchport mode trunk
```

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

```
SW-AA#show interfaces 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 1
Fa0/3 1
```

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

```
SW-CC(config)#interface fa0/1
SW-CC(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 Admon (99).

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

```
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)#
```

10. Verifique que las VLANs han sido agregadas correctamente.

```
SW-BB#showvlan 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
25Personal active
30 Planta active
99 Admon active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active

SW-AA#showvlan 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
25Personal active
30 Planta active
99 Admon active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active

SW-CC#showvlan 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
25Personal active
30 Planta active
99 Admon active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active

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	190.108.20.X / 24
F0/20	VLAN 30	190.108.30.X / 24

X = número de cada PC particular

Tabla 1. Configuración direcciones IP

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(config)#interface fa 0/10
SW-AA(config-if)#switchport mode acces
SW-AA(config-if)#switchport access vlan 10
SW-AA(config-if)#interface fa 0/15
SW-AA(config-if)#switchport mode acces
SW-AA(config-if)#switchport access vlan 25
SW-AA(config-if)#interface fa 0/20
SW-AA(config-if)#switchport mode acces
SW-AA(config-if)#switchport access vlan 30
```

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

```
SW-CC(config)#interface fa 0/10
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 10
SW-CC(config-if)#interface fa 0/15
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 25
```

```

SW-CC(config-if)#interface fa 0/20
SW-CC(config-if)#switchport mode access
SW-CC(config-if)#switchport access vlan 30

```

```

IP PC1: 190.108.10.1 Mascara 255.255.255.0
IP PC2: 190.108.20.2 Mascara 255.255.255.0
IP PC3: 190.108.30.3 Mascara 255.255.255.0
IP PC4: 190.108.10.4 Mascara 255.255.255.0
IP PC5: 190.108.20.5 Mascara 255.255.255.0
IP PC6: 190.108.30.6 Mascara 255.255.255.0
IP PC7: 190.108.10.7 Mascara 255.255.255.0
IP PC8: 190.108.20.8 Mascara 255.255.255.0
IP PC9: 190.108.30.9 Mascara 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.

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

Tabla 2. Direcciones IP en los Switches

```

SW-AA(config)#interfacevlan 99
SW-AA(config-if)#ip address 190.108.99.1 255.255.255.0

```

```

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

```

```

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.

Al realizar ping entre los PCs pertenecientes a la misma Vlan se realizo con éxito, pero al realizar el ping entre los PCs de diferente Vlan no tuvo éxito. Esto se debe a que los PCs pertenecen a diferentes segmentos de red o Vlan diferentes. Por

tanto, para lograr establecer comunicación entre estos PCs de diferente Vlan, se hace necesario incluir un equipo de capa 3, que proporcione la funcionalidad de enrutamiento entre VLANs.

Figura 4. Ping de PC1 a PC2

```
C:\>ping 190.108.20.2

Pinging 190.108.20.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.20.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 5. Ping de PC1 a PC3

```
C:\>ping 190.108.30.3

Pinging 190.108.30.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 6. Ping de PC1 a PC4

```
C:\>ping 190.108.10.4

Pinging 190.108.10.4 with 32 bytes of data:

Reply from 190.108.10.4: bytes=32 time=45ms TTL=128
Reply from 190.108.10.4: bytes=32 time=10ms TTL=128
Reply from 190.108.10.4: bytes=32 time=16ms TTL=128
Reply from 190.108.10.4: bytes=32 time=15ms TTL=128

Ping statistics for 190.108.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 45ms, Average = 21ms
```

Figura 7. Ping de PC1 a PC7

```
C:\>ping 190.108.10.7

Pinging 190.108.10.7 with 32 bytes of data:

Reply from 190.108.10.7: bytes=32 time=14ms TTL=128
Reply from 190.108.10.7: bytes=32 time<1ms TTL=128
Reply from 190.108.10.7: bytes=32 time=1ms TTL=128
Reply from 190.108.10.7: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.10.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 14ms, Average = 3ms
```

Figura 8. Ping de PC2 a PC5

```
C:\>ping 190.108.20.5

Pinging 190.108.20.5 with 32 bytes of data:

Reply from 190.108.20.5: bytes=32 time=29ms TTL=128
Reply from 190.108.20.5: bytes=32 time<1ms TTL=128
Reply from 190.108.20.5: bytes=32 time=4ms TTL=128
Reply from 190.108.20.5: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.20.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 29ms, Average = 8ms
```

Figura 9. Ping de PC2 a PC3

```
C:\>ping 190.108.30.3

Pinging 190.108.30.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.30.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 10. Ping de PC2 a PC8

```
C:\>ping 190.108.20.8

Pinging 190.108.20.8 with 32 bytes of data:

Reply from 190.108.20.8: bytes=32 time=25ms TTL=128
Reply from 190.108.20.8: bytes=32 time=11ms TTL=128
Reply from 190.108.20.8: bytes=32 time=10ms TTL=128
Reply from 190.108.20.8: bytes=32 time=13ms TTL=128

Ping statistics for 190.108.20.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 25ms, Average = 14ms
```

Figura 11. Ping de PC3 a PC6

```
C:\>ping 190.108.30.6

Pinging 190.108.30.6 with 32 bytes of data:

Reply from 190.108.30.6: bytes=32 time=13ms TTL=128
Reply from 190.108.30.6: bytes=32 time<1ms TTL=128
Reply from 190.108.30.6: bytes=32 time<1ms TTL=128
Reply from 190.108.30.6: bytes=32 time=15ms TTL=128

Ping statistics for 190.108.30.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 15ms, Average = 7ms
```

Figura 12 Ping de PC3 a PC5

```
C:\>ping 190.108.20.5

Pinging 190.108.20.5 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 190.108.20.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 13 Ping de PC3 a PC6

```
C:\>ping 190.108.30.6

Pinging 190.108.30.6 with 32 bytes of data:

Reply from 190.108.30.6: bytes=32 time=26ms TTL=128
Reply from 190.108.30.6: bytes=32 time=1ms TTL=128
Reply from 190.108.30.6: bytes=32 time<1ms TTL=128
Reply from 190.108.30.6: bytes=32 time=5ms TTL=128

Ping statistics for 190.108.30.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 26ms, Average = 8ms
```

Figura 14 Ping de PC3 a PC9

```
C:\>ping 190.108.30.9

Pinging 190.108.30.9 with 32 bytes of data:

Reply from 190.108.30.9: bytes=32 time=34ms TTL=128
Reply from 190.108.30.9: bytes=32 time=17ms TTL=128
Reply from 190.108.30.9: bytes=32 time<1ms TTL=128
Reply from 190.108.30.9: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.30.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 34ms, Average = 12ms
```

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

Al realizar el ping entre los Switch resulta exitoso, debido a que las interfaces físicas que se encargan de enrutar los datos entre los tres Switches están configurados en modo troncal, lo cual se verifico mediante comando show interfaces trunk. Por lo que es necesario implementar en las interfaces que interconectan Switches el comando switchport trunk allowed vlan except "vlan id", para dar permiso a las VLANs creadas en esta situación.

```
Ping SW-AA a SW-BB  
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 = 0/4/18 ms
```

```
Ping SW-BB a SW-CC  
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 = 0/4/20 ms
```

```
Ping SW-CC a SW-AA  
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 = 0/4/12 ms
```

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

Al realizar el ping entre los Switches y los PCs se observa que no tuvo éxito. Debido a que las VLANs configuradas en SW-BB, y que se replican a los Switches cliente empleando el protocolo VTP, y las interfaces que interconectan de los switches a los PCs en modo de acceso según la VLAN a la cual se encuentra asociada, e igualmente no se configura un enrutamiento IP en las VLANs para las diferentes áreas. Lo cual se hace necesario configurar una dirección IP a cada una de las interfaces VLAN de los Switches, que pertenezca al mismo segmento de red que corresponde el PC.

Ping del Switch SW-AA a los PCs.
SW-AA#ping 190.108.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW-AA#ping 190.108.20.2

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

SW-AA#ping 190.108.30.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

Ping del Switch SW-BB a los PCs.

SW-BB#ping 190.108.10.4

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

SW-BB#ping 190.108.20.5

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

SW-BB#ping 190.108.30.6

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

Ping del Switch SW-CC a los PCs.

```
SW-CC#ping 190.108.10.7
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 190.108.10.7, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

```
SW-CC#ping 190.108.20.8
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 190.108.20.8, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

```
SW-CC#ping 190.108.30.9
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 190.108.30.9, timeout is 2 seconds:

.....

Successrateis 0 percent (0/5)

CONCLUSIONES

La configuración de red es muy importante a la hora de realizar cualquier tipo de programación por medio de la práctica en la implementación y configuración de una red por medio de VLAN y los protocolos VTP y STP, se logró fortalecer los conocimientos adquiridos en este tipo de programación.

Se realizaron de manera practica la configuración de protocolos de enrutamiento para el escenario uno logrando tener conectividad entre cada uno de los equipos activos del escenario uno, se realizaron pruebas de ping obteniendo respuesta y pusimos en prueba comando show en don nos muestran las diferentes configuraciones realizadas.

Conseguimos información detallada a nivel de Direcciones ip para poder ejecutarla implementación del protocolo BGP y verificar la correcta configuración de este protocolo corroborando a través de comandos show.

BIBLIOGRAFÍAS

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

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

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

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Path Control Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101.

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing a Border Gateway Protocol (BGP) Solution for ISP Connectivity. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101.

Tomado de Características de BGP www.eduangi.org/node372.html
Tomado de Definición de configuración - Qué es, Significado y Concepto definicion.de/configuración

Tomado de Qué es una dirección IP, para qué sirve y cómo funciona www.hostgator.mx/blog/que-es-una-direccion-ip

Tomado de La importancia de la programación en la actualidad... www.madridiario.es/470766/importancia-programacion-actualidad