DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

NIDIA XIMENA ESPINOSA LADINO

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

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

NIDIA XIMENA ESPINOSA LADINO

Diplomado de opción de grado presentado para optar el título de INGENIERA ELECTRONICA

DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA

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

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

BOGOTA D.C, 22 de mayo de 2020

AGRADECIMIENTOS

Agradezco a Dios por ser mi principal guía dándome discernimiento y sabiduría para comprender la importancia de los saberes disciplinares que me permiten enriquecer mi profesión como Ingeniera Electrónica; a mi madre Nidia Rocio Ladino por su apoyo emocional en el logro de cada objetivo trazado durante mi vida y mi carrera profesional y especialmente a mi hija Valerie Sofia Mendez motivo inspirador de mi vida que nunca me deja desfallecer ante los obstáculos presentados.

A todos mis profesores de la escuela de Ingeniería de la Universidad Nacional Abierta y a Distancia UNAD que fueron guía en el transcurrir del desarrollo de mi carrera transmitiendo sus conocimientos que me permiten hoy consolidarlos en el desarrollo de este trabajo.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ISO: Organización internacional para estandarización (ISO, International Organization for Standardization). Una organización internacional que desarrolla y promueve estándares de operación entre redes en todo el mundo.

VPN: (Virtual Private Network/Red Privada Virtual). Una conexión IP entre dos sitios sobre una red pública IP que tiene su tráfico de carga útil codificada de manera que sólo los nodos fuente y destino pueden descifrar los paquetes de tráfico. Una VPN permite a una red públicamente accesible sera usada para transmisiones de datos altamente confidenciales, dinámicas y seguras.

WAN: Una red que interconecta recursos de computadoras que están geográficamente ampliamente separadas (usualmente a más de 100 km). Esto incluye pueblos, ciudades, estados y condados. Un WAN cubre generalmente un área mayor que 5 millas (8 km) y puede considerarse que consiste en una colección de LAN.

DIRECCIÓN IPv4: Una dirección IP con base en el IPv4. Esas direcciones consisten en 32 bits (0 al 31) particionados en cuatro grupos de ocho bits cada uno (llamados octetos) y organizados en cinco clases (A a la E) con base en los valores de bits 0 al 3.

DIRECCIÓN IPV6: Una dirección IP con base en IPv6. Una dirección IPv6 consiste en 128 bits y tiene 4000 millones X 4000 millones de veces el tamaño del espacio de dirección IPv4 (2128 vs. 232). A diferencia de las direcciones IPv4, las direcciones IPv6 usan dos puntos como delimitador (en vez de una notación “punto”), y ellas son escritas como ocho enteros de 16 bits expresados en forma hexadecimal.

RESUMEN

La prueba de habilidades del diplomado de profundización Cisco CCNP es el producto de la preparación del estudiante para configurar, administrar y solucionar problemas presentados en redes LAN y WAN a través de las temáticas establecidas en los protocolos RIPv2 y OSPF, configuración de DHCP, NAT y ACL. Mediante el desarrollo de la prueba se plantea la conmutación y enrutamiento de dos escenarios que ponen en práctica los conocimientos adquiridos en el transcurso del diplomado y así identificar las habilidades que se lograron en el proceso de formación profesional. Estos problemas que se trazan permiten mostrar el resumen de las actividades ejecutadas en la totalidad del curso a través del paso a paso realizado para ciertas configuraciones y la verificación de conectividad usando comandos básicos como show ip route.

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

ABSTRACT

The Cisco CCNP Diploma of Depth Skills Test is the product of the student's preparation to configure, manage and modify specific problems in LAN and WAN networks through the topics established in the RIPv2 and OSPF protocols, DHCP configuration, NAT and ACL Through the development of the test, the commutation and routing of two situations are proposed, which put into practice the knowledge acquired during the diploma and thus identify the skills achieved in the professional training process. These traced problems allow showing the summary of the activities executed in the entire course through the step by step carried out for certain settings and the connectivity verification using basic commands such as show ip route.

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

INTRODUCCIÓN

El diplomado de profundización Cisco CCNP es una herramienta que ayuda al enriquecimiento de conocimientos en networking y permite el desarrollo de habilidades y nociones obtenidas en el transcurso de la carrera profesional, así mismo prepara al estudiante para configurar, administrar y solucionar problemas presentados en redes a través del desarrollo de dos escenarios propuestos. El siguiente documento desarrolla la prueba de habilidades prácticas que hace parte de una serie de actividades propuestas para el curso.

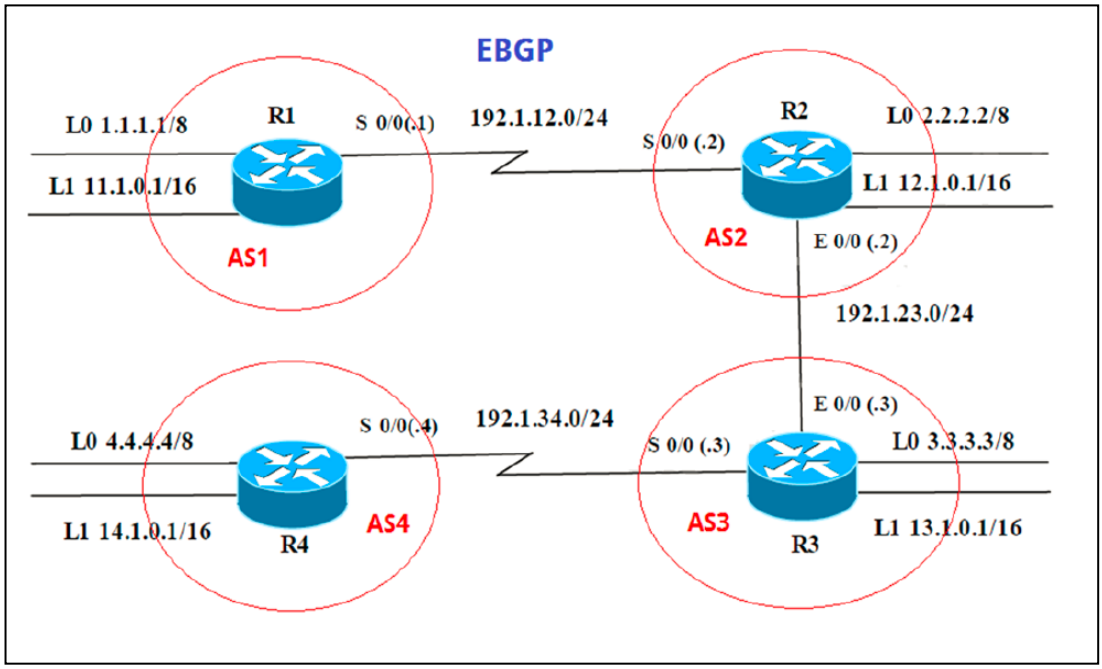
Para el desarrollo de dicha prueba se tocan diferentes temas tales como el enrutamiento a través del protocolo BGP, configuraciones relacionas a IPV4, EBGP e interfaces Loopback; para luego finalizar con una sencilla red compuesta por switches y computadoras donde se realiza la configuración del enrutamiento, VLANs, protocolo de enlace y protocolo dinámico de enlace.

Finalmente, en este documento se encontrara la descripción y desarrollo de cada uno de los puntos establecidos para la aplicación de las prueba de habilidades practicas con su respectivo análisis, explicación y la verificación de conectividad usando comandos básicos.

DESAROLLO

1. ESCENARIO 1

Figura 1. Escenario 1



Información para configuración de los Routers

Tabla 1. Loopback para crear 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. Loopback para crear 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

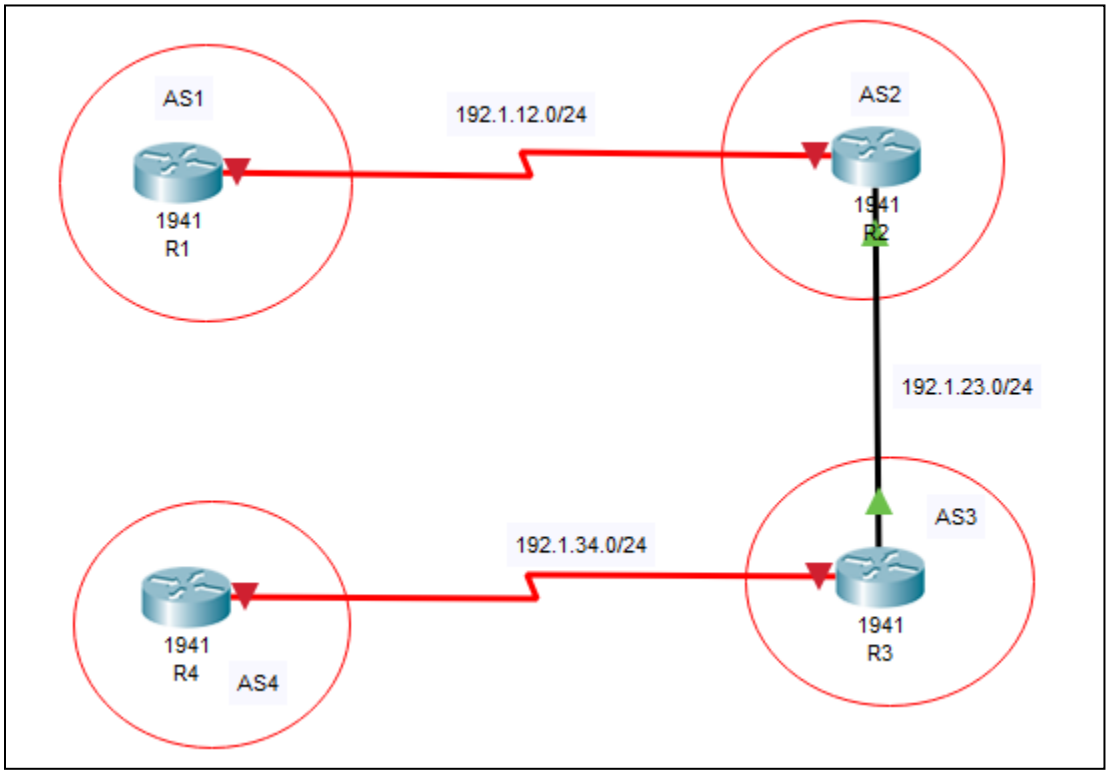
Tabla 3. Loopback para crear R3

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	192.1.34.3	255.255.255.0

Tabla 4. Loopback para crear 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

Figura 2. Simulación 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.

   Configuración en R1

   ```
   Router#configure terminal
   Router(config)#hostname 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 serial 1/0
   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
   ```

   Configuración en R2

   ```
   Router#configure terminal
   Router(config)#hostname R2
   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 1/0
   R2(config-if)#ip address 192.1.12.2 255.255.255.0
   R2(config-if)#no shutdown
   R2(config-if)#interface fastEthernet 0/0
   R2(config-if)#ip address 192.1.23.2 255.255.255.0
   ```

```
R2(config-if)#no shutdown
R2(config-if)#exit
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
```

Al ejecutar el comando *show ip route* en R1 y R2 se obtiene la tabla de enrutamiento con el direccionamiento Loopback y las direcciones de la interfaces de conexión directa. Según esta tabla se visualiza el enrutamiento Loopback de su router vecino mediante el código B aprendidas a través del protocolo BGP.

Figura 3. Comando show ip route en R1

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

Figura 4. Comando show ip route en R2

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

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 en R2

   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

   Configuración en R3

   Router#configure terminal
   Router(config)#hostname 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)#interface fastEthernet 0/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#interface serial 1/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router bgp 3
R3(config-router)#bgp router-id 44.44.44.44
R3(config-router)#network 3.0.0.0 mask 255.0.0.0
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3(config-router)#network 192.1.23.0 mask 255.255.255.0
R3(config-router)#neighbor 192.1.23.2 remote-as 2
```

Al ejecutar nuevamente el comando show ip route en R2 se evidencia la actualización de la tabla de enrutamiento ya que este equipo ha aprendido 4 rutas mediante el protocolo BGP identificando como nuevas las direcciones Loopback de R3. Para el equipo R3 su tabla de enrutamiento reconoce las direcciones conectadas directamente en las interfaces y se visualiza las direcciones correspondientes a las Loopback configuradas en R2 y R1.

Figura 5. Comando show ip route en R2

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

Figura 6. Comando show ip route en R3

```
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, 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
```

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 en R3

   ```
   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
   ```

   Configuración en R4

   ```
   Router#configure terminal
   Router(config)#hostname R4
   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 1/0
   R4(config-if)#ip address 192.1.34.4 255.255.255.0
   R4(config-if)#no shutdown
   R4(config-if)#exit
   R4(config)#router bgp 4
   R4(config-router)#bgp router-id 66.66.66.66
   R4(config-router)#network 4.0.0.0 mask 255.0.0.0
   R4(config-router)#network 14.1.0.0 mask 255.255.0.0
   R4(config-router)#network 192.1.34.0 mask 255.255.255.0
   R4(config-router)#neighbor 192.1.34.3 remote-as 3
   ```

El router vecino necesita informar el uso de las direcciones loopback para ello se debe realizar una configuración adicional sobre R3 y R4.

Configuración en R3

```
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
```

Configuración en 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
R4(config-router)#neighbor 3.3.3.3 update-source loopback 0
R4(config-router)# neighbor 3.3.3.3 ebgp-multihop
```

Al ejecutar el comando show ip route en R3 se ve la actualización de la tabla de enrutamiento cambiando la dirección que se conecta con R4 correspondiente a la Loopback 0, a pesar de haber realizado este cambio aun se visualiza que la conexión física se encuentra bajo direccionamiento 192.1.4.0/24. En la tabla de enrutamiento de R4 se evidencia que el direccionamiento de BGP con el que se comunica con sus vecinos ha cambiado correspondiente al Loopback 0 en R3.

Figura 7. Comando show ip route en R3

```
R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, 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
```

Figura 8. Comando show ip route en R4

```
R4#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, 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 9. Escenario 2

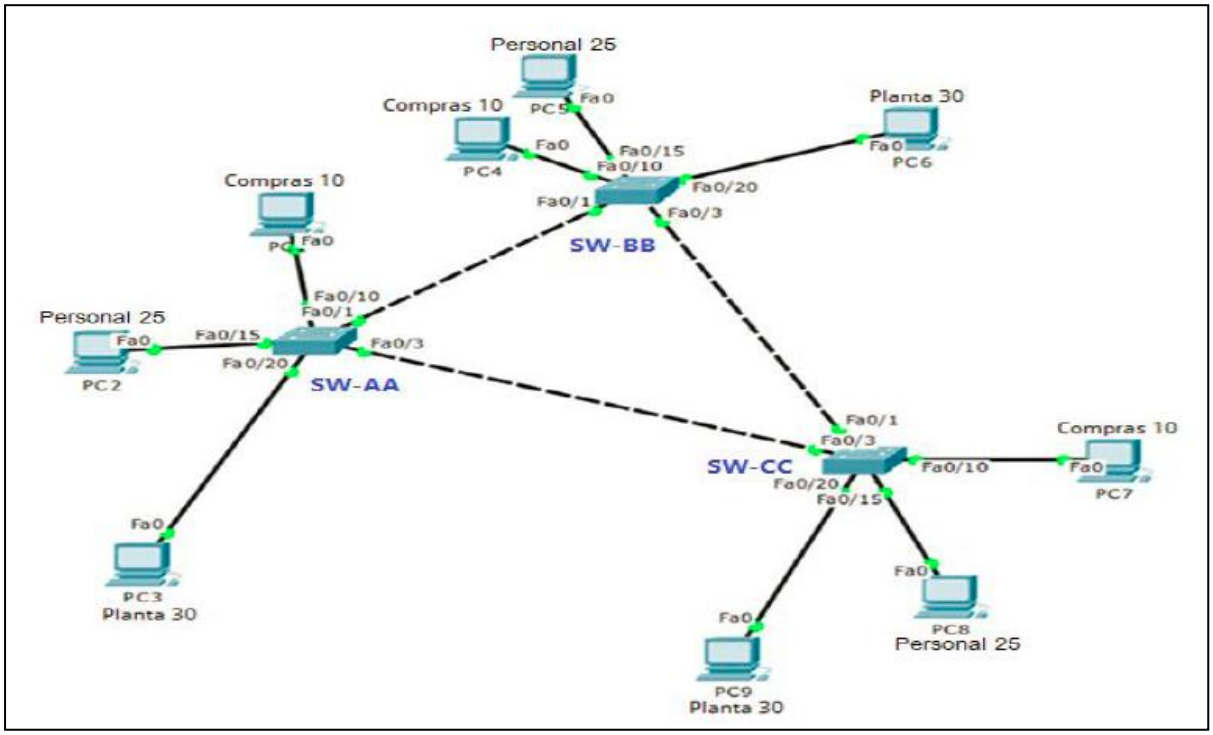
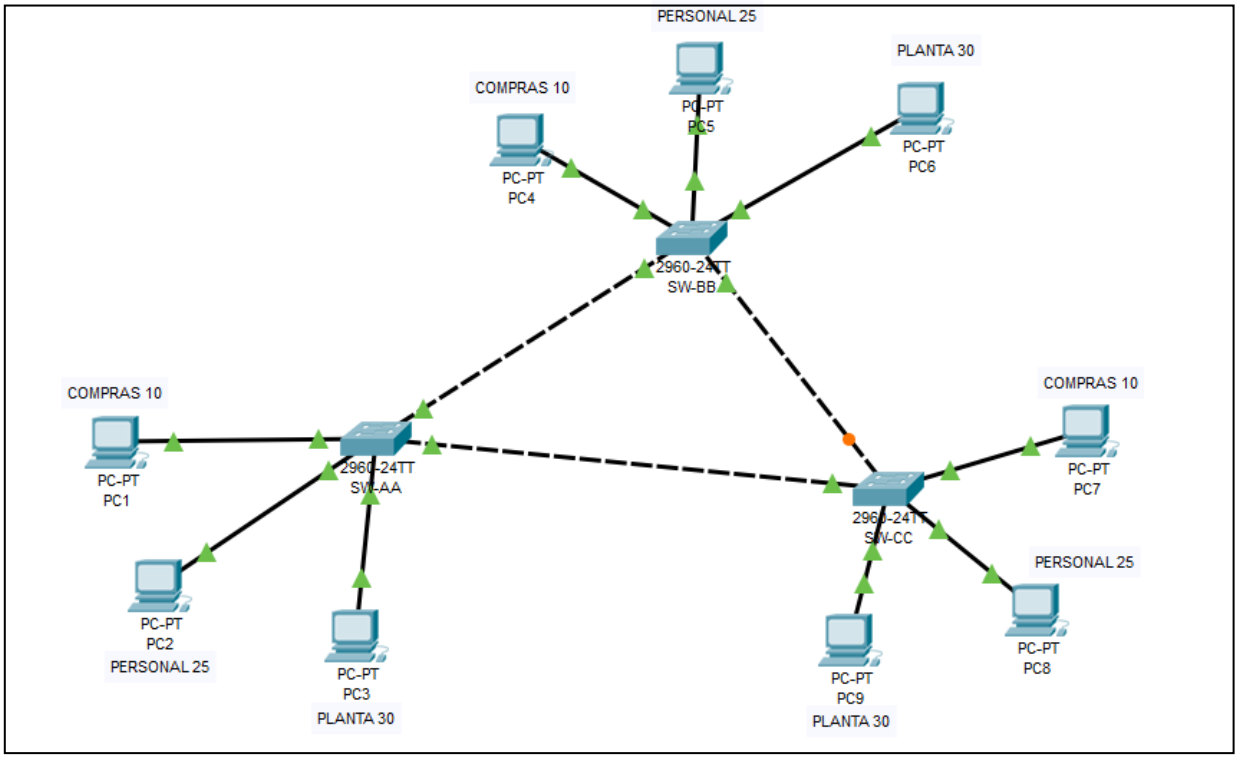


Figura 10. Simulación escenario 2



Configurar VTP

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

Se procede a realizar configuración sobre SW-AA y SW-CC como clientes con dominio VPT y se asigna contraseña

SW-AA#configure terminal
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-CC#configure terminal
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

En SW-BB se realiza configuración de servidor se asigna dominio y contraseña

SW-BB#configure terminal
SW-BB(config)#vtp mode server
Setting device to VTP SERVER mode.
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

Verifique las configuraciones mediante el comando show vtp status.

Figura 11. Configuración SW-AA

```
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
```

Figura 12. Configuración SW-BB

```
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)
```

Figura 13. Configuración SW-CC

```
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
```

Configurar DTP (Dynamic Trunking Protocol)

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

Configuración de enlace troncal dinámico en SW-BB

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

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

Figura 14. Enlace trunk en SW-AA

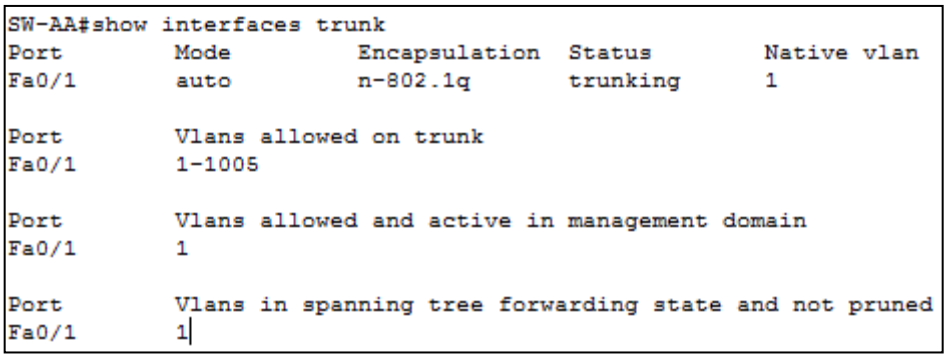
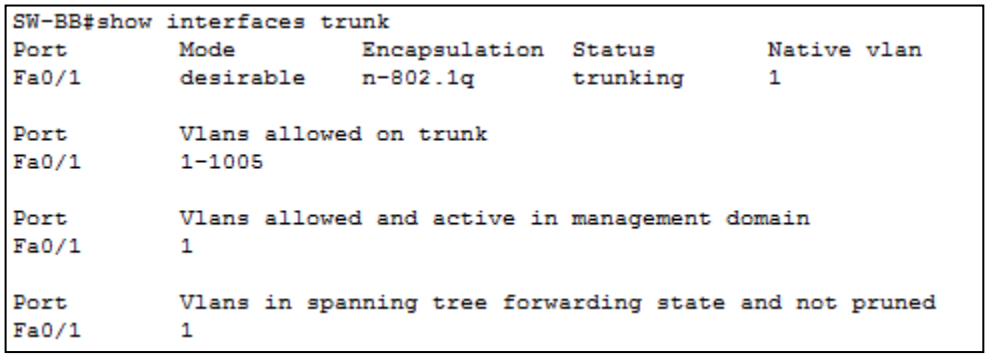


Figura 15. . Enlace trunk en SW-BB



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

SW-AA#configure terminal
SW-AA(config)#interface fastEthernet 0/3
SW-AA(config-if)#switchport mode trunk

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

Figura 16. Enlace trunk en SW-BB

```
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       none
```

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

Se realiza configuración del enlace trunk permanente sobre SW-CC

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

Figura 17. Enlace trunk en SW-BB

```
SW-BB#show interfaces 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       none
```

Figura 18. Enlace trunk en SW-CC

```
SW-CC#show interfaces 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       none
Fa0/3       1
```

Agregar VLANs y asignar puertos.

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

Configuración VLAN 10 en SS-AA

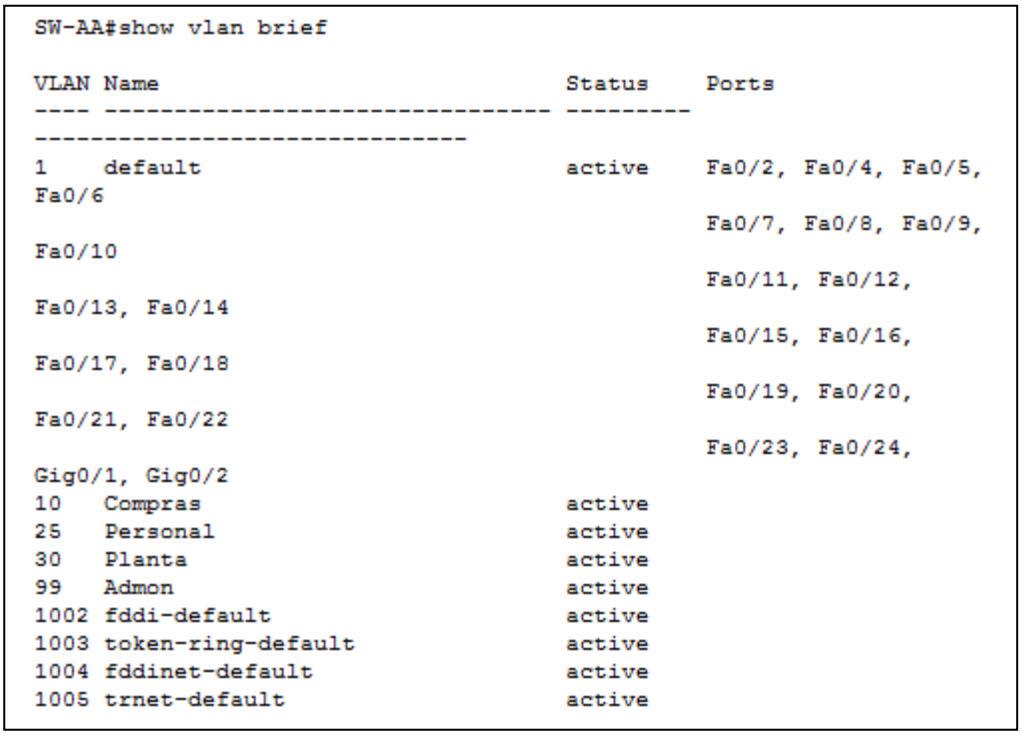
SW-AA#configure terminal
SW-AA(config)#vlan 10

Configuración de VLANS en SW-BB

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

Verifique que las VLANs han sido agregadas correctamente.

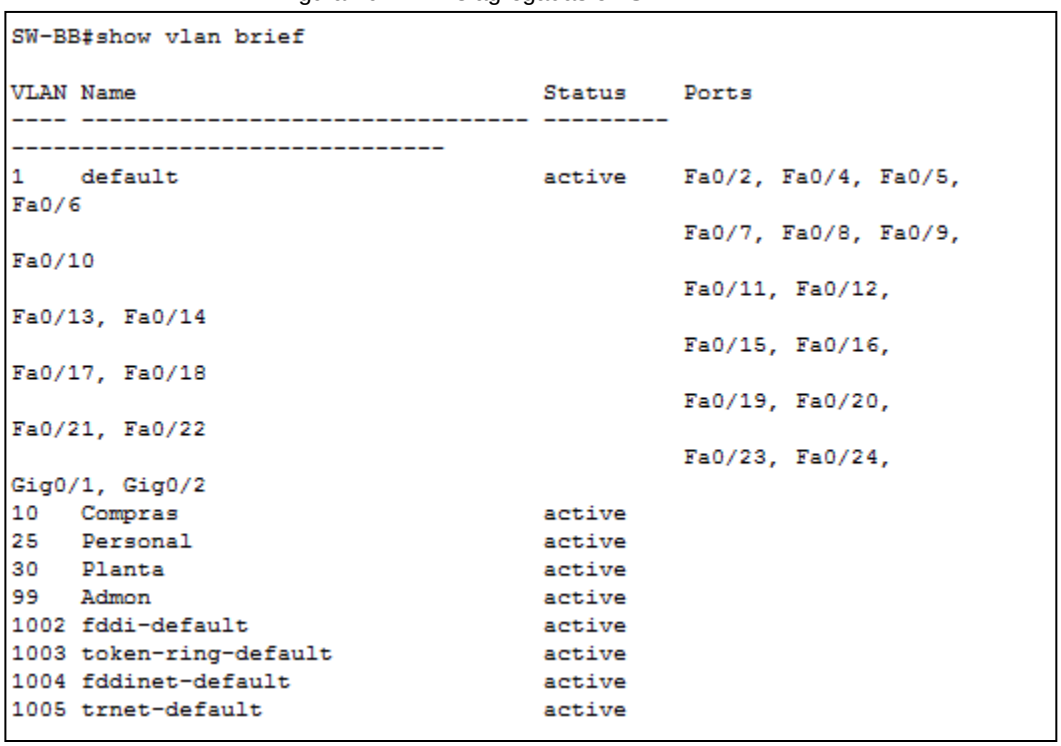
Figura 19. VLANs agregadas en SW-AA



```
SW-AA#show 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
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Figura 20. VLANs agregadas en SW-BB



```
SW-BB#show 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
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Figura 21. VLANs agregadas en SW-CC

```
SW-CC#show 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
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

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

Tabla 5. Direccionamiento 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

X = número de cada PC particular

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

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.

Configuración en SW-AA

```
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
```

Configuración en SW-BB

```
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
```

Configuración en SW-CC

```
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
```

Direccionamiento de los computadores

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

Configurar las direcciones IP en los Switches.

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

Tabla 6. Direccionamiento Switches

Equipo	Interfaz	Dirección 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

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-BB(config)#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

Verificar la conectividad Extremo a Extremo

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 de diferente VLANs no se obtiene éxito, pero el ping realizado en PCs con la misma VLAN si lo tuvieron, esto se debe a que los equipos pertenecientes a diferente VLANs hacen parte de un segmento de red diferente.

Figura 22. Ping desde PC1

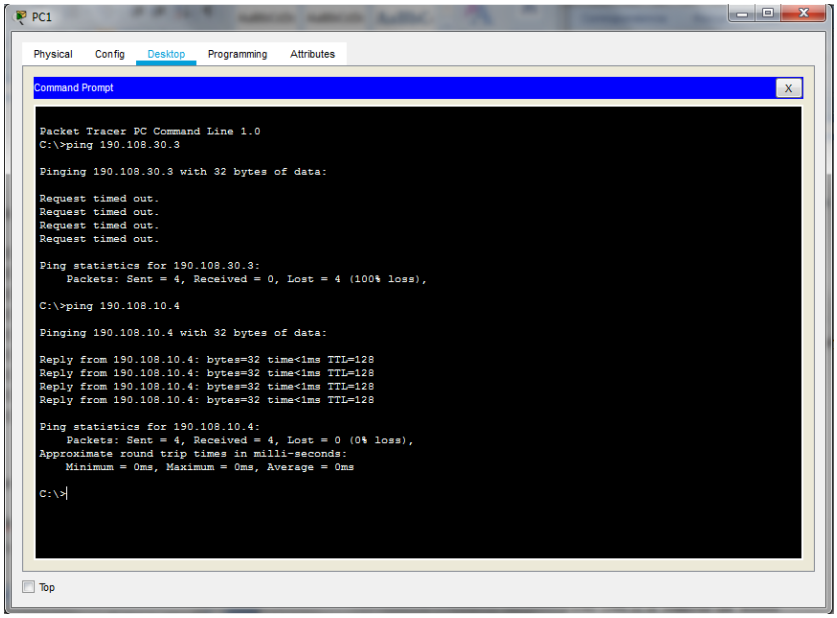


Figura 23. Ping desde PC5

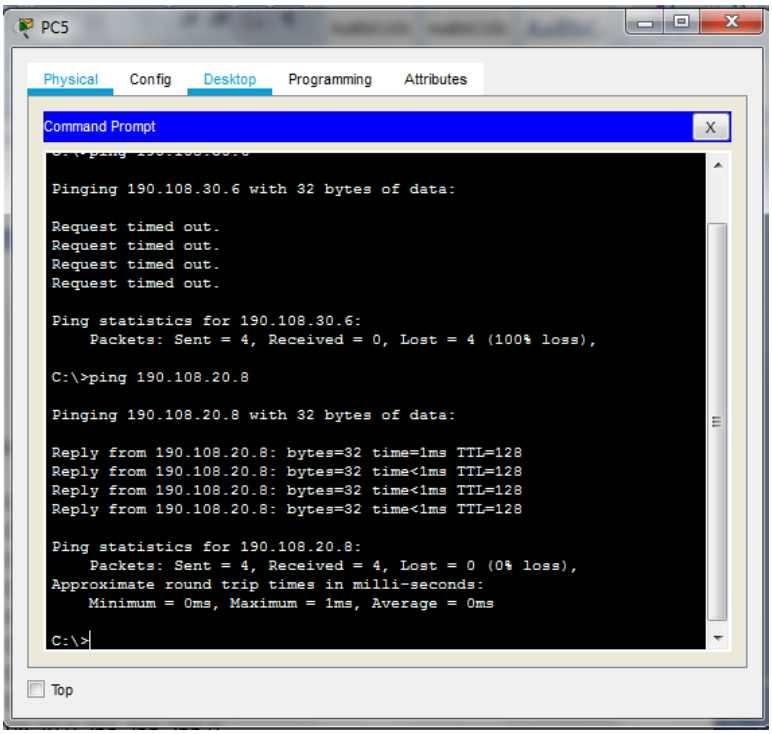
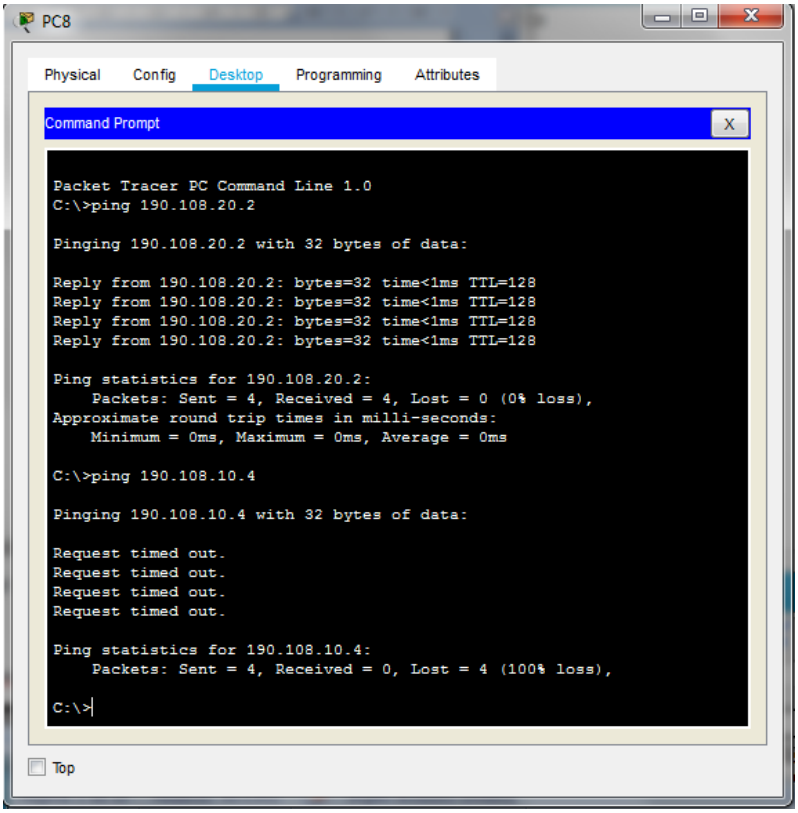


Figura 24. Ping desde PC8



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

Todos los ping realizado entre los switch son exitosos, ya que las interface físicas están enrutadadas mediante el protocolo ICMP y se encuentran configurados en modo troncal compartiendo el mismo encapsulamiento.

Figura 25. Ping de SW-AA a SW-BB y SW-CC

```
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 = 0/2/8 ms

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 = 0/0/1 ms
```

Figura 26. Ping de SW-BB a SW-AA y 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 = 0/0/1 ms

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 = 0/0/1 ms
```

Figura 27. Ping de SW-CC a SW-BB y SW-CC

```
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 = 0/0/0 ms
```

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

Al realizar ping entre los Switches y los PCs no se tiene éxito ya que no se configuro un enrutamiento ip en las VLANs que se crearon aunque estas se tengas habilitadas en cada uno de los switches.

Figura 28. Ping de SW-AA a PC1, PC2 y PC3

```
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)
```

Figura 29. Ping de SW-BB a PC4, PC5 y PC6

```
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)
```

Figura 30. Ping de SW-CC a PC7, PC8 y PC9

```
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:
.....
Success rate is 0 percent (0/5)
```

CONCLUSIONES

El proceso de identificación del enrutador BGP corresponde con el mismo para EIGRP y OSPF. Cuando falta un comando de id de enrutador, los enrutadores utilizan las direcciones de bucle de retorno más altas para sus ID de enrutador. Por otro lado, BGP habilita un protocolo basado en políticas (que opera bajo variables) en lugar de algoritmos complejos presentes en otros protocolos. En este caso, BGP elige una ruta desde un dispositivo con la ID de BGP más baja, como resultado de encontrar otras características iguales.

El protocolo VTP permite la gestión de redes a través de diferentes medios tales como, el servidor que permite crear y configurar parámetros específicos, el cliente encargado de la transmisión y recepción

El protocolo de enlace VLAN es el medio para garantizar la coherencia y la gestión adecuada de las VLAN que coexisten en la misma red; esto mediante la resolución de problemas relacionados con la duplicidad, los flujos en la configuración y los problemas de seguridad.

BIBLIOGRAFIA

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

Gallo, M. A. H., Gallo, W. M. M. A., & Hancock, W. M. (2002). Glosario. Comunicación entre computadoras y tecnología de redes. Thomson. Recuperado de: http://go.galegroup.com/ps/i.do?id=GALE%7CCX4059900177&v=2.1&u=unad&it=r&p=GVRL&sw=w&asid=ebb3f06c3e49cace676a520de3807353

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