

DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP

MIGUEL ZULETA PEREZ

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

**DIPLOMADO DE PROFUNDIZACION CISCO
PRUEBA DE HABILIDADES PRÁCTICAS CCNP**

MIGUEL ZULETA PEREZ

Diplomado de opción de grado presentado para optar el
título de INGENIERÍA DETELECOMUNICACIONES

**DIRECTOR:
MSc. GERARDO GRANADOS ACUÑA**

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

NOTA DE ACEPTACIÓN

Firma del Presidente del Jurado

Firma del Jurado

Firma del Jurado

MEDELLÍN 22 de mayo de 2020

CONTENIDO

CONTENIDO	4
LISTA DE TABLAS	5
LISTA DE FIGURAS	6
GLOSARIO.....	7
RESUMEN	8
ABSTRACT	8
INTRODUCCIÓN	9
DESARROLLO	10
1. Escenario 1	10
2. Escenario 2	20
CONCLUSIONES	33
BIBLIOGRAFÍA.....	34

LISTA DE TABLAS

Tabla 1. Direccionamiento PC----- 26

Tabla 2. Direccionamiento SW----- 27

LISTA DE FIGURAS

Figura 1. Escenario 1	10
Figura 2. Simulación de escenario 1	11
Figura 3. Salida del comando show ip route	13
Figura 4. Salida del comando show ip route	13
Figura 5. Salida del comando show ip route	15
Figura 6. Salida del comando show ip route	15
Figura 7. Salida del comando show ip route	17
Figura 8. Salida del comando show ip route	18
Figura 9. Salida del comando show ip route	19
Figura 10. Escenario 2	20
Figura 11. Simulación del escenario 2	21
Figura 12. show vtp status	22
Figura 13. show vtp status	22
Figura 14. show vtp status	22
Figura 15. interfaces trunk	23
Figura 16. interfaces trunk	23
Figura 17. interfaces trunk	24
Figura 18. show vlan br	25
Figura 19. show vlan br	25
Figura 20. Prueba de Ping PC1(VLan 10) a PC 10(VLan 10) y PC 23(VLan 30)	28
Figura 21. Prueba de Ping PC2(VLan 25) a PC 13(VLan 30) y PC 22(VLan 25)	29
Figura 22. Prueba de Ping PC3(VLan 30) a PC 10(VLan 10) y PC 23(VLan 30)	29
Figura 23. Prueba de Ping Origen SW SW-AA a SW-BB y SW-CC	30
Figura 24. Prueba de Ping Origen SW SW-BB a SW-AA y SW-CC	30
Figura 25. Prueba de Ping Origen SW SW-CC a SW-AA y SW-BB	31
Figura 26. Prueba de Ping Origen SW SW-AA a PC1, PC2 y PC3	31
Figura 27. Prueba de Ping Origen SW SW-BB a PC10, PC12 y PC13	32
Figura 28. Prueba de Ping Origen SW SW-CC a PC20, PC22 y PC23	32

GLOSARIO

BGP: El Border Gateway Protocol (BGP) es el sistema que utilizan los grandes nodos de Internet para comunicarse entre ellos y transferir una gran cantidad de información entre dos puntos de la Red. Su misión es encontrar el camino más eficiente entre los nodos para propiciar una correcta circulación de la información en Internet.

PACKET TRACER: Es la herramienta de aprendizaje y simulación de redes interactiva para los instructores y alumnos de Cisco. Esta herramienta les permite a los usuarios crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales. Packet Tracer se enfoca en apoyar mejor los protocolos de redes que se enseñan en las certificaciones Cisco.

PING: Es una utilidad de diagnóstico en redes de computadoras que comprueba el estado de la comunicación del anfitrión local con uno o varios equipos remotos de una red que ejecuten IP. Se vale del envío de paquetes ICMP de solicitud y de respuesta.

ROUTER: Un rúter, enrutador, o encaminador, es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

TRACEROUTE: Es una utilidad de diagnóstico en redes de computadoras que comprueba el estado de la comunicación del anfitrión local con uno o varios equipos remotos de una red que ejecuten IP. Se vale del envío de paquetes ICMP de solicitud y de respuesta.

VLAN: Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el dominio de difusión y ayudan en la administración de la red, separando segmentos lógicos de una red de área local.

RESUMEN

Se realizó los 2 ejercicios donde fue demostrado el conocimiento adquirido en administración de redes, específicamente en CCNP de la empresa CISCO que se especializa en Redes de comunicaciones. Estos se desarrollaron el aplicativo Packet Tracer. En el primer escenario se configura 4 routers con enrutamiento dinámico BGP, que se establece con las IP configuradas en las interfaces físicas, cada router anuncia a su vecino las IP loopback que tiene configuradas. Entre el los router R3 y R4 se modificó el enrutamiento para establecer BGP con una de las interfaces Loopback, lo que requirió modificar una de las configuraciones a enrutamiento estático. En este punto no logramos terminar dado que Packet Tracer no reconoce 2 comandos necesarios para subir esta configuración. En el segundo escenario se configuro 3 SW, uno en modo servidor y dos más modo cliente, los tres están conectados entre sí, esto permite tener una alta conmutación. En el SW Servidor configura las Vlans y se replica en los SW cliente. Se asigna un direccionamiento diferente a cada Vlan por lo que solo entre las mismas vlan tienen conectividad. El circuito está diseñado que en caso de fallar algún Switch por la Electrónica o alguna desconexión física, halla una conmutación por otro SW.

Palabras Clave: CISCO, CCNP, CONMUTACIÓN, ENRUTAMIENTO, REDES, ELECTRÓNICA.

ABSTRACT

The 2 exercises were carried out where the knowledge acquired in networking was demonstrated, specifically in CCNP of the CISCO company that specializes in Communication Networks. These were developed the Packet Tracer application. In the first scenario, 4 routers are configured with dynamic BGP routing, which is established with the IPs configured on the physical interfaces, each router announces its configured IP loopback to its neighbor. Between routers R3 and R4, routing was modified to establish BGP with one of the Loopback interfaces, which required modifying one of the configurations to static routing. At this point we were unable to finish since Packet Tracer does not recognize the 2 commands necessary to upload this configuration. In the second scenario, 3 SW were configured, one in server mode and two more in client mode, all three are connected to each other, this allows high switching. In the Server SW, configure the Vlans and replicate in the client SW. A different addressing is assigned to each Vlan so that only between the same vlan do they have connectivity. The circuit is designed so that in the event of a failure by the Electronics or a physical disconnection, it finds a switch for another SW.

Keywords: CISCO, CCNP, ROUTING, SWICHTING, NETWORKING, ELECTRONICS

INTRODUCCIÓN

En este documento se encuentra el desarrollo de la PRUEBA DE HABILIDADES CCNP, con la cual se evalúa la parte final del diplomado, con el objetivo de desarrollar y demostrar las habilidades técnicas sobre el conocimiento de Networking en cisco, se propuso desarrollar 2 escenarios donde se trabajarán temas como Enrutamiento, BGP, EBGP, VLAN, VTP, Conectividad, Conmutación, Troubleshooting, Rutas Estáticas, entre otros.

En el primer escenario se trabajó con enrutamiento dinámico EBGP y enrutamiento Estático, se realizan pruebas de conectividad, verificando la tabla de enrutamiento identificando que cargue correctamente las tablas en cada router. En este caso encontraremos con la función del router que se desempeña en la capa 3 del modelo OSI, donde interconecta con distintos segmentos IP con distintas máscaras de subred.

En el segundo Escenario se trabajó principalmente la capa 2 del modelo OSI, donde todo el tema de conectividad se verá ligado principalmente al transporte de VLANS entre los distintos SW, y como prueba final la configuración de algunos PC conectados a cada una de las VLAN, y según la conexión a una VLAN se asignó un direccionamiento IP. Fueron usados comandos como show interfaces trunk, show vtp status, show ip route y ping, para verificar la correcta operatividad.

1. ESCENARIO 1

Figura 1. Escenario 1

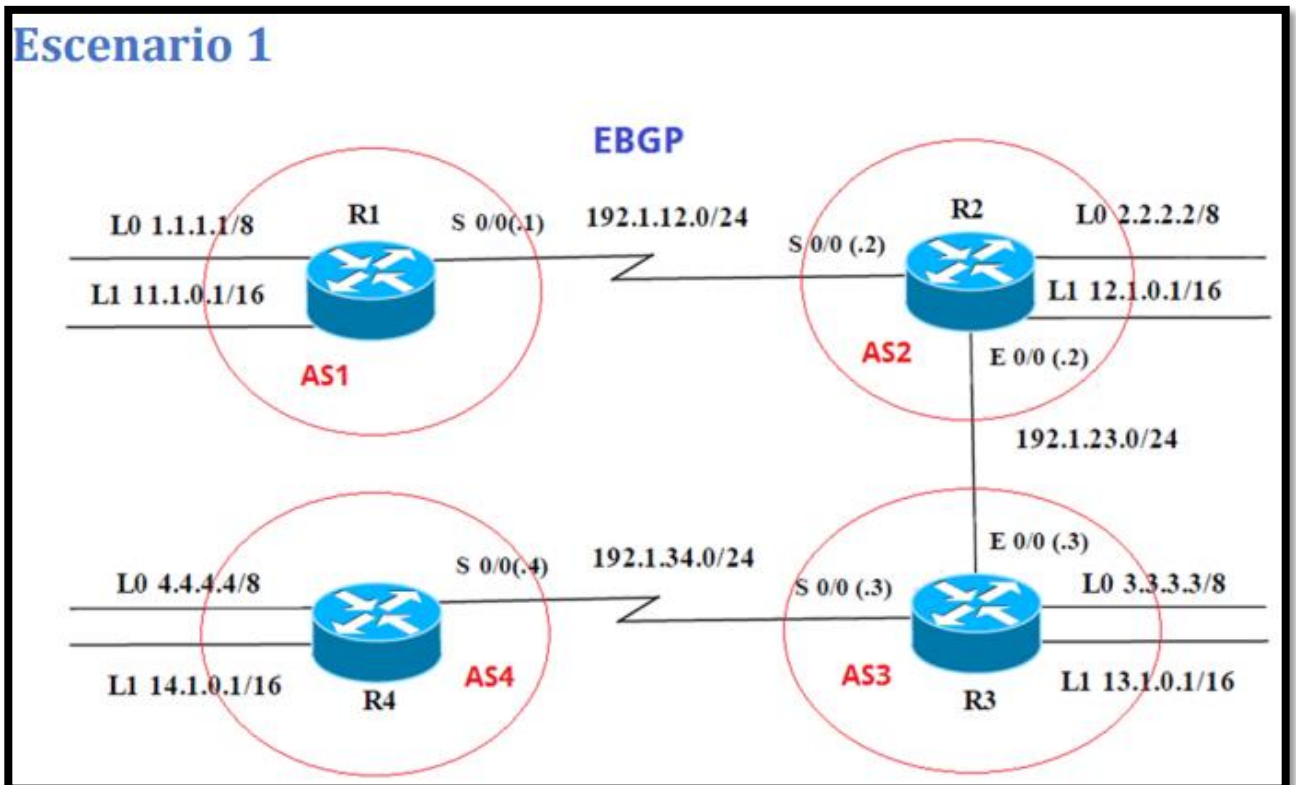
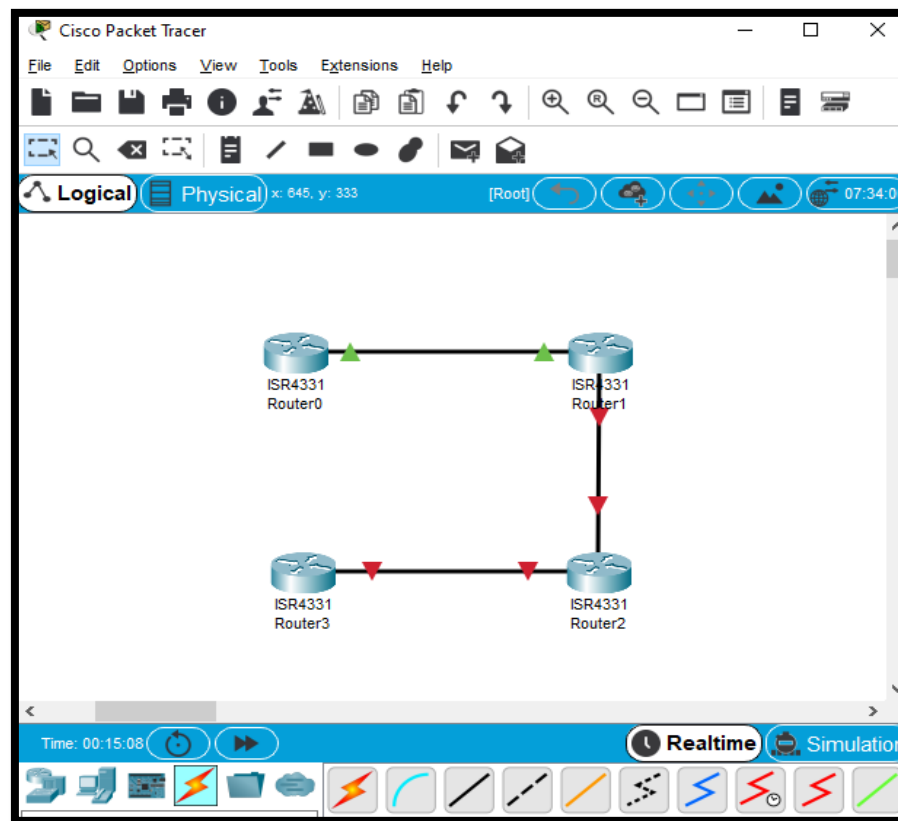


Figura 2. Simulación de escenario 1



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**.

Se procede a configurar cada uno de los enrutadores. 1 y 2,
Se asignan nombre y protocolos de comunicación mediante enrutamiento BGP según los datos que fueron asignados.

Se adjunta código y pantallazos con veracidad del código.

Router R1

```
Router>  
Router>en
```

Ingreso a modo privilegiado

```

Router#conf t                               Ingreso a modo de configuración
Router(config)#hostname R1                  Asigno nombre al router
R1(config)# router bgp 1
R1(config-router)# bgp router-id 22.22.22.22 Identifico el router
R1(config-router)#network 1.0.0.0 mask 255.0.0.0 Anunciar red
R1(config-router)#network 11.1.0.0 mask 255.255.0.0
R1(config-router)#neighbor 192.1.12.2 remote-as 2 Vecindad
R1(config-router)#exit
R1(config)#int lo 0                          Configuro interfaz L0
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#
R1(config-if)#int lo 1                       Configuro interfaz L1
R1(config-if)#ip add 11.1.0.1 255.255.0.0
R1(config)#int GigabitEthernet0/0/0         Configuro interfaz Gi0/0/0
R1(config-if)#ip add 192.1.12.1 255.255.255.0
R1(config-if)#des R1

```

Router R2

```

Router>
Router>en                                   Ingreso a modo privilegiado
Router#conf t                               Ingreso a modo de configuración
Router(config)#hostname R2                  Asigno nombre al router
R2(config)# router bgp 2
R2(config-router)# bgp router-id 33.33.33.33 Identifico el router
R2(config-router)#network 2.0.0.0 mask 255.0.0.0 Anunciar red
R2(config-router)#network 12.1.0.0 mask 255.255.0.0
R2(config-router)#neighbor 192.1.12.1 remote-as 1 Vecindad
R2(config-router)#exit
R2(config)#int lo 0                          Configuro interfaz L0
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#
R2(config-if)#int lo 1                       Configuro interfaz L1
R2(config-if)#ip add 12.1.0.1 255.255.0.0
R2(config)#int GigabitEthernet0/0/0         Configuro interfaz Gi0/0/0
R2(config-if)#ip add 192.1.12.2 255.255.255.0
R2(config-if)#des R2

```

Figura 3. -Salida del comando show ip route

```

R1#sho 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, GigabitEthernet0/0/0
L       192.1.12.1/32 is directly connected, GigabitEthernet0/0/0

R1#

```

Ctrl+F6 to exit CLI focus

Copy Paste

Figura 4. -Salida del comando show ip route

```

R2#show ip rout
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, GigabitEthernet0/0/0
L       192.1.12.2/32 is directly connected, GigabitEthernet0/0/0

R2#

```

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**.

Router R2

```
R2r>
R2>en Ingreso a modo privilegiado
R2(config)# router bgp 2
R2(config-router)# neighbor 192.1.23.3 remote-as 3 Vecindad
R2(config-router)#exit
R2(config)#int GigabitEthernet0/0/1 Configuro interfaz Gi0/0/1
R2(config-if)#ip add 192.1.23.2 255.255.255.0
R2(config-if)#des R2
```

Router R3

```
Router>en Ingreso a modo privilegiado
Router#conf t Ingreso a modo de configuración
Router(config)#hostname R3 Asigno nombre al router
R3(config)# router bgp 3
R3(config-router)# bgp router-id 44.44.44.44 Identifico el Router
R3(config-router)#network 3.0.0.0 mask 255.0.0.0 Anunciar red
R3(config-router)#network 13.1.0.0 mask 255.255.0.0
R3(config-router)#neighbor 192.1.23.2 remote-as 2 Vecindad
R3(config-router)#exit
R3(config)#int lo 0 Configuro interfaz L0
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#
R3(config-if)#int lo 1 Configuro interfaz L1
R3(config-if)#ip add 13.1.0.1 255.255.0.0
R3(config)#int GigabitEthernet0/0/1 Configuro interfaz Gi0/0/1
R3(config-if)#ip add 192.1.23.3 255.255.255.0
R3(config-if)#des R3
```

Figura 5. -Salida del comando show ip route

```
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, GigabitEthernet0/0/0
L 192.1.12.2/32 is directly connected, GigabitEthernet0/0/0
  192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.1.23.0/24 is directly connected, GigabitEthernet0/0/1
L 192.1.23.2/32 is directly connected, GigabitEthernet0/0/1

R2#
```

Figura 6. -Salida del comando show ip route

```
R3#show ip ro
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
  192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.1.23.0/24 is directly connected, GigabitEthernet0/0/1
L 192.1.23.3/32 is directly connected, GigabitEthernet0/0/1

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**.

Router R3

```
R3>
R3>en                               Ingreso a modo privilegiado
R3#conf t                            Ingreso a modo de configuración
R3(config)# router bgp 4
R3(config-router)# neighbor 192.1.34.4 remote-as 3  Vecindad
R3(config-router)#exit
R3(config)#int GigabitEthernet0/0/0           Configuro interfaz Gi0/0/0
R3(config-if)#ip add 192.1.34.3 255.255.255.0
R3(config-if)#des R3
```

Router R4

```
Router>
Router>en                               Ingreso a modo privilegiado
Router#conf t                            Ingreso a modo de configuración
Router(config)#hostname R4              Asigno nombre al router
R4(config)# router bgp 4
R4(config-router)# bgp router-id 66.66.66.66  Identifico el router
R4(config-router)#network 4.0.0.0 mask 255.0.0.0  Anunciar red
R4(config-router)#network 14.1.0.0 mask 255.255.0.0
R4(config-router)#neighbor 192.1.34.3 remote-as 3  Vecindad
R4(config-router)#exit
R4(config)#int lo 0                       Configuro interfaz L0
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#
R4(config-if)#int lo 1                     Configuro interfaz L1
R4(config-if)#ip add 14.1.0.1 255.255.0.0
R4(config)#int GigabitEthernet0/0/0       Configuro interfaz Gi0/0/0
R4(config-if)#ip add 192.1.34.4 255.255.255.0
R4(config-if)#des R4
```


Figura 7. -Salida del comando show ip route

```
R4#show ip ro
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
     192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.1.34.0/24 is directly connected, GigabitEthernet0/0/0
L    192.1.34.4/32 is directly connected, GigabitEthernet0/0/0

R4#
```

4. 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**.

Para esta configuración se presentaron problemas con el IOS de Cisco, y aun que al parecer se establece el BGP, realmente no opera como debería. El router no tomo algunos comandos necesarios.

Router R4

```
R4(config)# router bgp 4
R4(config-router)#no network 4.0.0.0 mask 255.0.0.0 No anunciar red
R4(config-router)#neighbor 3.3.3.3 remote-as 3 Vecindad
```

Los siguientes 2 comandos no los toma el router, necesarios para operar correctamente.

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

```
R4(config-router)#no neighbor 192.1.34.3 remote-as 3 Borra vecino.
R4(config-router)#exit
```

```
R4(config)# ip route 3.0.0.0 255.0.0.0 192.1.34.3 Ruta estática
```

Router R3

```
R3(config)# router bgp 3  
R3(config-router)#no network 3.0.0.0 mask 255.0.0.0 No anunciar red  
R3(config-router)#neighbor 4.4.4.4 remote-as 4 Vecindad
```

Los siguientes 2 comandos no los toma el router, necesarios para operar correctamente.

```
R3(config-router)#neighbor 4.4.4.4 update-source loopback 0  
R3(config-router)#neighbor 4.4.4.4 ebgp-multihop
```

```
R4(config-router)#no neighbor 192.1.34.4 remote-as 4 Borra vecino  
R4(config-router)#exit  
R4(config)# ip route 4.0.0.0 255.0.0.0 192.1.34.4 Ruta estática
```

Figura 8. -Salida del comando show ip route

```
R3#show ip ro  
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  
192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks  
C 192.1.23.0/24 is directly connected, GigabitEthernet0/0/1  
L 192.1.23.3/32 is directly connected, GigabitEthernet0/0/1  
192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks  
C 192.1.34.0/24 is directly connected, GigabitEthernet0/0/0  
L 192.1.34.3/32 is directly connected, GigabitEthernet0/0/0  
|  
R3#
```

Figura 9. -Salida del comando show ip route

```
R4#show ip ro
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
L    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, GigabitEthernet0/0/0
L    192.1.34.4/32 is directly connected, GigabitEthernet0/0/0

R4#
```

2. ESCENARIO 2

Figura 10. Escenario 2

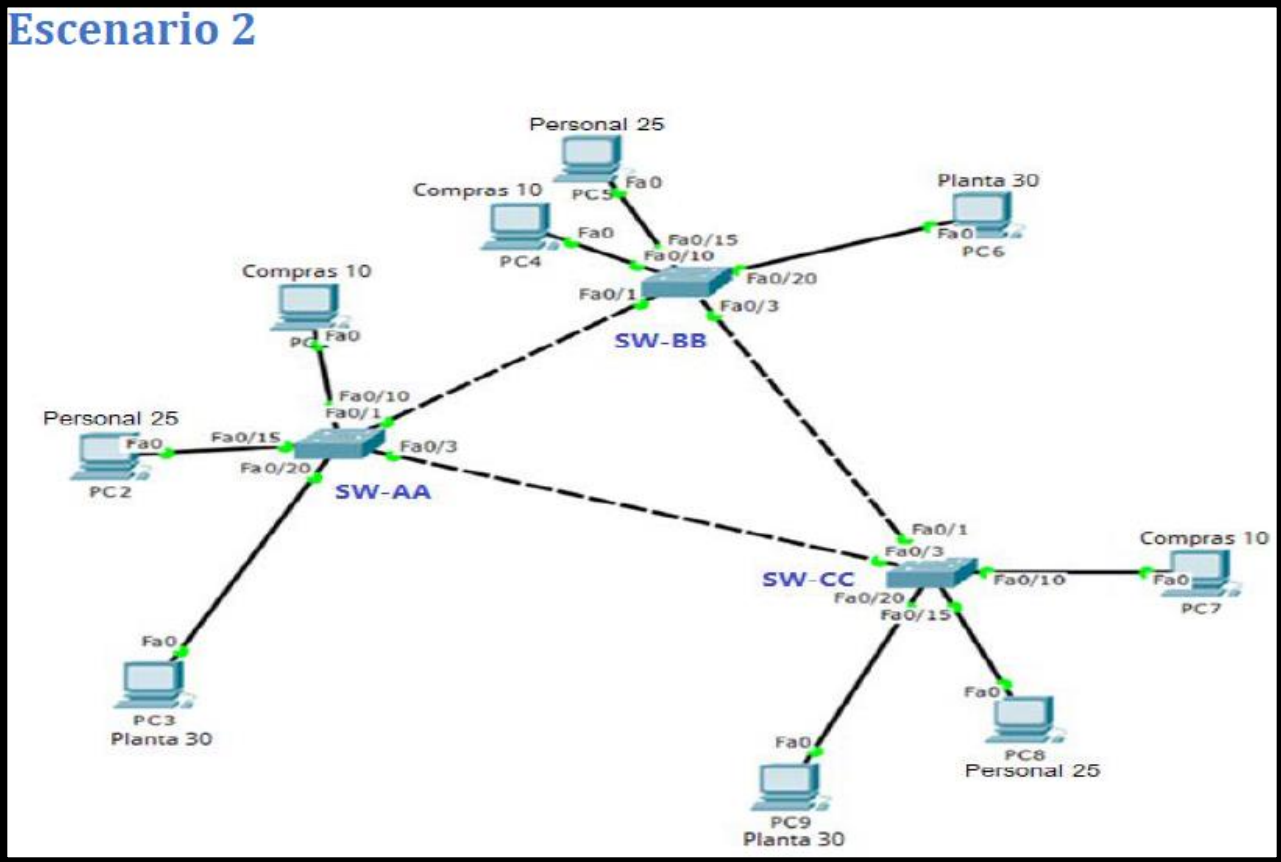
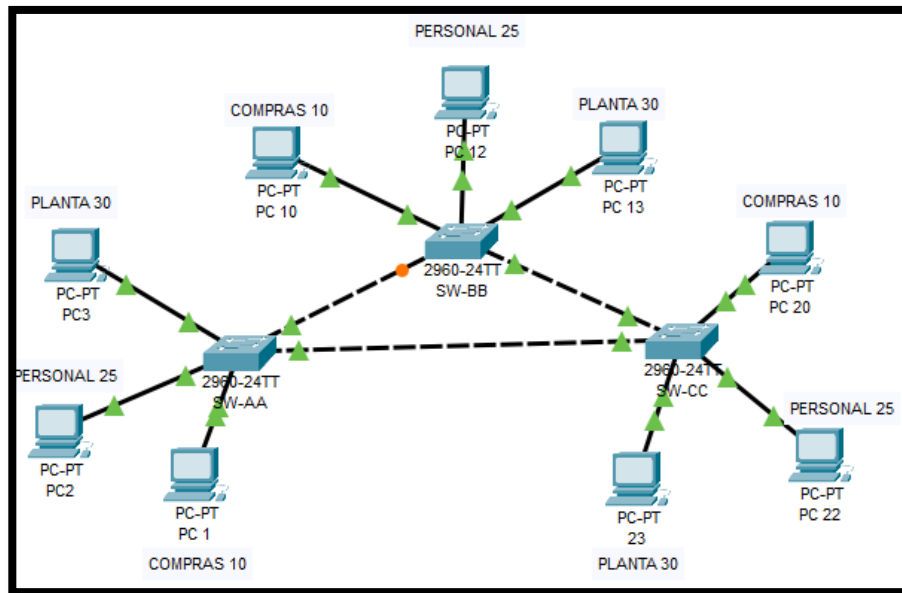


Figura 11. Simulación del escenario 2



A. Configurar VTP

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

```
SW1#configure terminal
SW1(config)#vtp mode client      VTP modo cliente
SW1(config)#vtp domain CCNP     Aignar dominio CCNP
SW1(config)#vtp password cisco  Asignación password
```

```
SW2#configure terminal
SW2(config)#vtp mode server     VTP modo server
SW2(config)#vtp domain CCNP     Aignar dominio CCNP
SW2(config)#vtp password cisco  Asignación password
```

```
SW3#configure terminal
SW3(config)#vtp mode client     VTP modo cliente
SW3(config)#vtp domain CCNP     Aignar dominio CCNP
SW3(config)#vtp password cisco  Asignación password
```

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

Figura 12. show vtp status.

```
SW1#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
SW1#
```

Figura13. show vtp status.

```
SW2#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
```

Figura14. show vtp status.

```
SW3#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
SW3#
```

B. Configurar DTP (Dynamic Trunking Protocol)

3. Todos 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.

```
SW2(config)#interface fastEthernet 0/1          Configuración F0/1
SW2(config-if)#switchport mode dynamic desirable Troncal dinámico
```

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

Figura 15. interfaces trunk.

```
SW1#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     auto      n-802.1q       trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005

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

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

SW1#
```

Figura 16. interfaces trunk.

```
SW2#runk
Translating "runk"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer
address

SW2#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     none

SW2#
```

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

Al parecer existe un error, ya que ente el SW-AA y SW-BB la conexión este en F0/1 y en el punto anterior ya se realizó una configuración troncal entre estos 2 puertos, mirando la practica completa deduzco que esta configuración debe realizarse entre SW-AA y SW-CC

```
SW1(config)#interface fastEthernet 0/3    Configuración F0/1
SW1(config-if)#switchport mode trunk    modo troncal
```

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

Figura 17. interfaces trunk.

```
SW1# 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
```

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

```
SW3(config)#interface fastEthernet 0/1    Configuración F0/1
SW3(config-if)#switchport mode trunk    modo troncal
```

C. Agregar VLANs y asignar puertos.

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

Al intentar configurar el SW-AA nos anuncia un error, ya que este SW esta como cliente y no como el servidor.

```
SW1(config)#vlan 10    Configuración vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
SW1(config)
```


Al configurar el SW-BB se crean las Vlan en los demás SW, esto ya que este SW-BB esta como servidor y los demás como cliente.

SW2(config)#vlan 10	<i>Configuración vlan 10</i>
SW2(config-vlan)#name Compras	<i>Descripción vlan 10</i>
SW2(config-vlan)#vlan 25	<i>Configuración vlan 25</i>
SW2(config-vlan)#name Personal	<i>Descripción vlan 25</i>
SW2(config-vlan)#vlan 30	<i>Configuración vlan 30</i>
SW2(config-vlan)#name Planta	<i>Descripción vlan 30</i>
SW2(config-vlan)#vlan 99	<i>Configuración vlan 99</i>
SW2(config-vlan)#name Admon	<i>Descripción vlan 99</i>
SW2(config-vlan)#exit	<i>Salida</i>

9. Verifique que las VLANs han sido agregadas correctamente.

Figura18. show vlan br.

```
SW2#show vlan br
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
SW2#
```

Figura19. show vlan br.

```
SW1#show vlan br
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
SW1#
```

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

Tabla 1. Direccionamiento PC.

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

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

12. Repita el procedimiento para los puertos F0/15 y F0/20 en SW-AA, SW-BB y SW-CC. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

```
SW1(config)#interface fastEthernet 0/10           Configuración Interface
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config)#interface fastEthernet 0/15           Configuración Interface
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 25
SW1(config)#interface fastEthernet 0/20           Configuración Interface
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 30
```

```
SW2(config)#interface fastEthernet 0/10           Configuración Interface
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 10
SW2(config)#interface fastEthernet 0/15           Configuración Interface
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 25
SW2(config)#interface fastEthernet 0/20           Configuración Interface
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 30
```

SW3(config)#interface fastEthernet 0/10	<i>Configuración Interface</i>
SW3(config-if)#switchport mode access	
SW3(config-if)#switchport access vlan 10	
SW3(config)#interface fastEthernet 0/15	<i>Configuración Interface</i>
SW3(config-if)#switchport mode access	
SW3(config-if)#switchport access vlan 25	
SW3(config)#interface fastEthernet 0/20	<i>Configuración Interface</i>
SW3(config-if)#switchport mode access	
SW3(config-if)#switchport access vlan 30	

Asignación IP PC

PC1: 190.108.10.1/24
 PC2: 190.108.20.1/24
 PC3: 190.108.30.1/24

PC10: 190.108.10.2/24
 PC12: 190.108.20.2/24
 PC13: 190.108.30.2/24

PC20: 190.108.10.3/24
 PC22: 190.108.20.3/24
 PC23: 190.108.30.3/24

D. Configurar las direcciones IP en los Switches.

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

Tabla 2. Direccionamiento SW.

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

SW1(config)#interface vlan 99	<i>Configuración vlan 99</i>
SW1(config-if)#ip address 190.108.99.1 255.255.255.0	<i>Configuración IP</i>
SW2(config)#interface vlan 99	<i>Configuración vlan 99</i>
SW2(config-if)#ip address 190.108.99.2 255.255.255.0	<i>Configuración IP</i>
SW3(config)#interface vlan 99	<i>Configuración vlan 99</i>
SW3(config-if)#ip address 190.108.99.3 255.255.255.0	<i>Configuración IP</i>

E. Verificar la conectividad Extremo a Extremo

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

Previo a realizar las pruebas sabemos técnicamente que cuando un equipo está en diferente Vlan y tienen configurada una IP en distintos segmentos de red, no tendrán conectividad, Ping, traza...

Solo en caso de que existiera un enrutador con las configuraciones necesarias para que a través de este exista conectividad entre Vlans y Segmentos de red.

Teniendo en cuenta lo mencionado anteriormente solo realizaré 2 pruebas, una con un PC que tenga respuesta y otro con el que no tenga respuesta.

Figura 20. Prueba de Ping PC1(VLan 10) a PC 10 (VLan 10) y PC 23 (VLan 30)

```

PC1
Physical  Config  Desktop  Programming  Attributes
Command Prompt
C:\>ping 190.108.10.2

Pinging 190.108.10.2 with 32 bytes of data:

Reply from 190.108.10.2: bytes=32 time=1ms TTL=128
Reply from 190.108.10.2: bytes=32 time=1ms TTL=128
Reply from 190.108.10.2: bytes=32 time<1ms TTL=128
Reply from 190.108.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

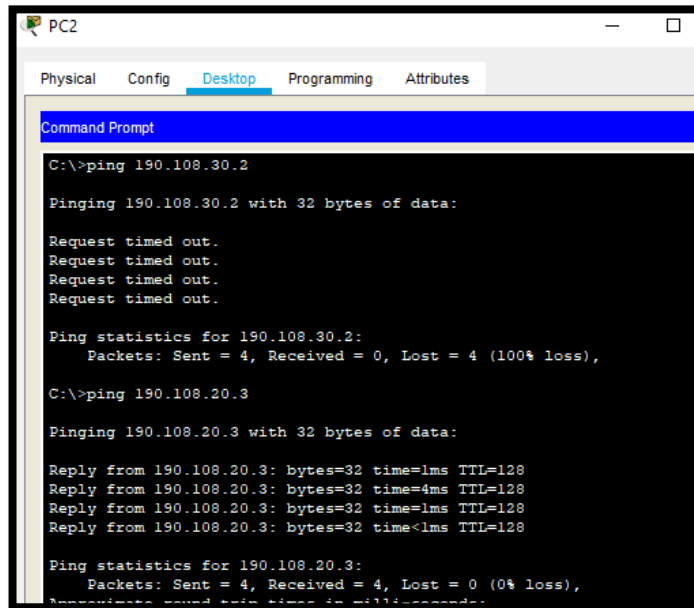
C:\>ping 190.108.30.3

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 21. Prueba de Ping PC2 (Vlan 25) a PC 13 (Vlan 30) y PC 22 (Vlan 25)



```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 190.108.30.2

Pinging 190.108.30.2 with 32 bytes of data:

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

Ping statistics for 190.108.30.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Requested Reply times: 0 milliseconds

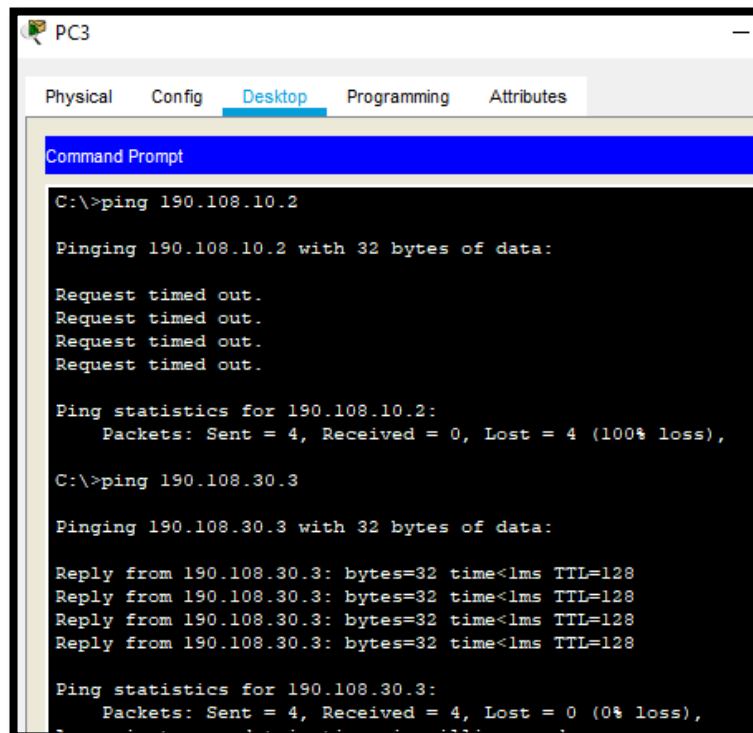
C:\>ping 190.108.20.3

Pinging 190.108.20.3 with 32 bytes of data:

Reply from 190.108.20.3: bytes=32 time<1ms TTL=128
Reply from 190.108.20.3: bytes=32 time=4ms TTL=128
Reply from 190.108.20.3: bytes=32 time=1ms TTL=128
Reply from 190.108.20.3: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Requested Reply times: 0 milliseconds
```

Figura 22. Prueba de Ping PC3(Vlan 30) a PC 10 (Vlan 10) y PC 23 (Vlan 30)



```
PC3
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 190.108.10.2

Pinging 190.108.10.2 with 32 bytes of data:

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

Ping statistics for 190.108.10.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Requested Reply times: 0 milliseconds

C:\>ping 190.108.30.3

Pinging 190.108.30.3 with 32 bytes of data:

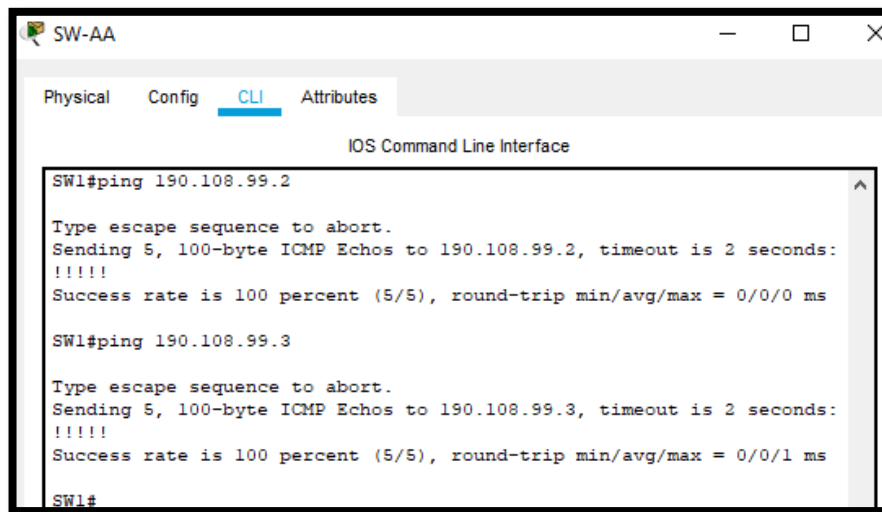
Reply from 190.108.30.3: bytes=32 time<1ms TTL=128
Reply from 190.108.30.3: bytes=32 time<1ms TTL=128
Reply from 190.108.30.3: bytes=32 time<1ms TTL=128
Reply from 190.108.30.3: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Requested Reply times: 0 milliseconds
```

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

Previo a realizar las pruebas sabemos técnicamente que cuando un equipo está en la misma Vlan y tienen configurada una IP del mismo segmento de red deberá tener conectividad.

Figura 23. Prueba de Ping Origen SW SW-AA a SW-BB y SW-CC

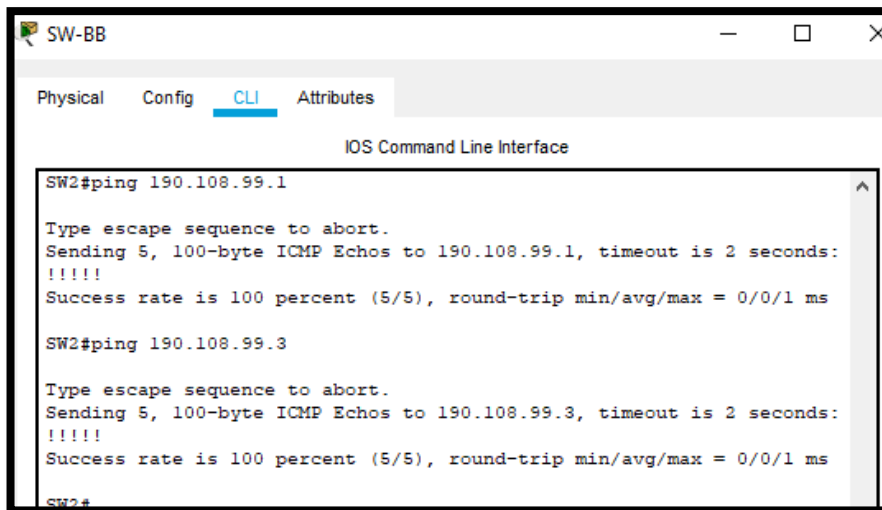


```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
SW1#ping 190.108.99.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

SW1#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

SW1#
```

Figura 24. Prueba de Ping Origen SW SW-BB a SW-AA y SW-CC

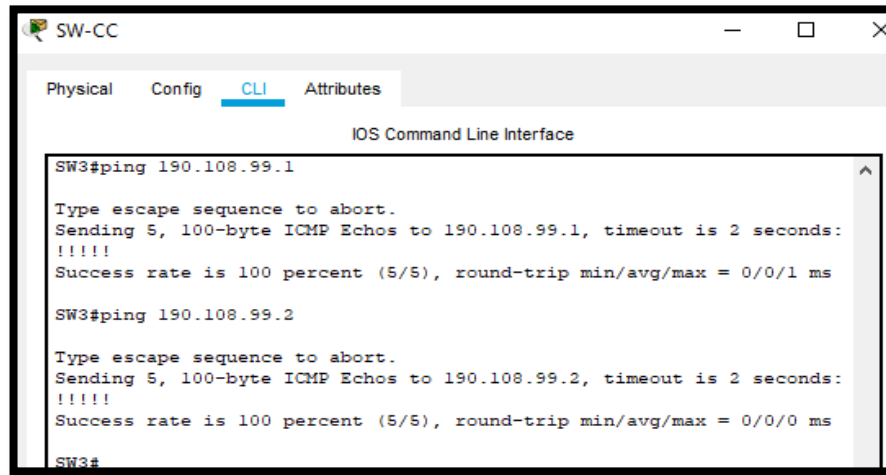


```
SW-BB
Physical Config CLI Attributes
IOS Command Line Interface
SW2#ping 190.108.99.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

SW2#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

SW2#
```

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



```
SW-CC
Physical Config CLI Attributes
IOS Command Line Interface
SW3#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

SW3#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 = 0/0/0 ms

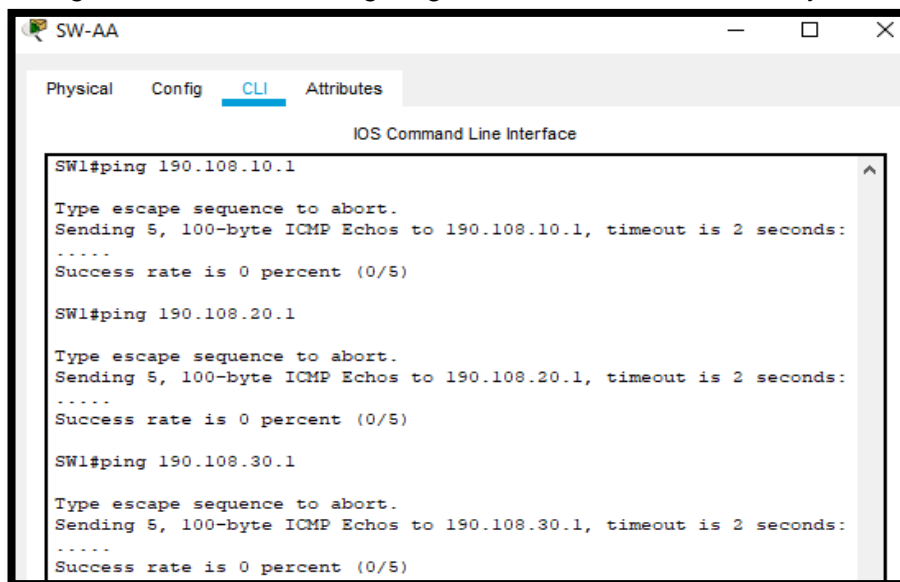
SW3#
```

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

Previo a realizar las pruebas sabemos técnicamente que cuando un equipo está en diferente Vlan y tienen configurada una IP en distintos segmentos de red, no tendrán conectividad, Ping, traza...

Solo en caso de que existiera un enrutador con las configuraciones necesarias para que a través de este exista conectividad entre Vlans y Segmentos de red. Teniendo en cuenta lo mencionado anteriormente sabemos no tendremos respuesta ping a ningún PC

Figura26. Prueba de Ping Origen SW SW-AA a PC1, PC2 y PC3



```
SW-AA
Physical Config CLI Attributes
IOS Command Line Interface
SW1#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)

SW1#ping 190.108.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW1#ping 190.108.30.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Figura 27. Prueba de Ping Origen SW SW-BB a PC10, PC12 y PC13

```
SW-BB
Physical Config CLI Attributes
IOS Command Line Interface
SW2#ping 190.108.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW2#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)

SW2#ping 190.108.30.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW2#
```

Figura 28. Prueba de Ping Origen SW SW-CC a PC20, PC22 y PC23

```
SW-CC
Physical Config CLI Attributes
IOS Command Line Interface
SW3#ping 190.108.10.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW3#ping 190.108.20.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SW3#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)

SW3#
```


CONCLUSIONES

En el desarrollo de esta actividad se puso en practica conceptos aprendidos y trabajados durante el curso, lo cual es un éxito ya que el objetivo de este trabajo consistía en evaluar nuestro aprendizaje y fue puesto en practica en el desarrollo de estos escenarios propuestos. Trabajamos las tres primeras capas del modelo OSI donde debíamos en la capa física debíamos seleccionar los equipos necesarios y realizar las conexiones correspondientes correctamente, en capa dos trabajamos la VLANS en el Escenario numero dos, configurando puertos troncales, SW en modo Clientes y Server. En capa 3 trabajamos todo el tema de enrutamiento como lo es el BGP, y rutas estáticas en el Escenario numero uno, allí configuramos distintos segmentos y verificamos que los distintos router aprendieran por BGP.

El desarrollo de este trabajo se hizo en Packet Tracert, diseñado por Cisco para generar un ambiente similar a los equipos reales, pude identificar que el programa GNS3 hoy en día es mas completo ya que podemos cargar distintas imágenes e IOS a los routers, permitiendo hacer configuraciones mas avanzadas, de las cuales muchas de ellas el programa Packet Tracert no soporta, sin embargo, para la gran mayoría de laboratorios pude desarrollarlos en este.

En este punto de aprendizaje podemos saber que el área de las redes Cisco es muy amplio y que nos debemos estar actualizando constantemente, tener nuestros conocimientos claros y organizados es una estrategia correcta, ya que con el pasar del tiempo hay cosas que se nos pueden pasar. En el desarrollo de este trabajo me encontré con cosas que no recordaba y dado que tengo la información bien documentada pude avanzar en el desarrollo.

BIBLIOGRAFÍA

Casos Prácticos de BGP. (30 de Octubre de 2008). Obtenido de Cisco: Recuperado de https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocolbgp/26634-bgp-toc.html

From, R., Frahim, E. (2015). CISCO Press (Ed). Spanning Tree Implementation. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. Recuperado de <https://1drv.ms/b/s!AmIJYe-NT1InWR0hoMxgBNv1CJ>

García, V. S. (04 de Julio de 2017). Diseño de Redes con BGP. Obtenido de Universitat Politècnica de València. Recuperado de: <https://riunet.upv.es/bitstream/handle/10251/91691/S%C3%81NCHEZ%20-%20Dise%C3%B1o%20de%20redes%20con%20BGP.pdf?sequence=1>

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYe-NT1InMfy2rhPZHwEoWx>