# EVALUACIÓN FINAL
# PRUEBA DE HABILIDADES PRÁCTICAS CCNP

**MAGDA LORENA LEGUIZAMÓN RIVERA**
**C.C. 1019047874**
**GRUPO: 208014_1**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA**
**ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA**
**INGENIERÍA ELECTRÓNICA**
**BOGOTÁ D.C.**
**2019**

# EVALUACIÓN FINAL
# PRUEBA DE HABILIDADES PRÁCTICAS CCNP

**MAGDA LORENA LEGUIZAMÓN RIVERA**
**C.C. 1019047874**
**GRUPO: 208014_1**

**Trabajo de grado para optar el título de Ingeniería Electrónica**
**DIPLOMADO DE PROFUNDIZACIÓN CCNP**

**TUTOR**
**GERARDO GRANADOS ACUÑA**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA**
**ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA**
**INGENIERÍA ELECTRÓNICA**
**BOGOTÁ D.C.**
**2019**

**Nota de aceptación**

_____

_____

_____

_____

_____

**Firma del presidente del Jurado**

_____

**Firma del Jurado**

_____

**Firma del jurado**

**Bogotá D.C, 30 de enero de 2019**

## Dedicatoria

A Dios, por estar conmigo en cada paso que he dado en esta vida que me ha permitido tener, por poder superar cada uno de los obstáculos que se me presentaron durante todo el período de estudio profesional, por fortalecer mi corazón y mi mente y por cada una de las personas que ha puesto en mi camino para acompañarme en mi crecimiento tanto personal como profesional.

A mi madre María Zenaida Rivera por darme la vida, por el amor que me ha brindado, por creer en mi y porque siempre recibi una voz de aliento cuando pensé desfallecer al no ver los resultados de mi esfuerzo de forma inmediata. Gracias mamá!

A mi abuela Fermina Molina (QEPD) por haber cuidado de mi en mi niñes e infundir en mi el deseo de estudiar y terminar una carrera profesional, tu me inspiraste a cumplir mis sueños y eres mi motiviación para cumplir mis objetivos y metas; ya que espero que siempre te sientas orgullosa de mi.

A todos mis amigos por compartir los buenos y malos momentos, por impulsarme a continuar y cumplir con mis sueños, por estar siempre cuando los he necesitado.

A todos los profesores con los que tuve clase, por sus enseñanzas, su dedicación y su tiempo.

A todos los que formaron parte de este camino que me llevo a culminar esta carrera tan bonita como lo es la Ingeniería electónica.

## CONTENIDO

Pág.

# LISTA DE FIGURAS

Pág.

# LISTA DE ANEXOS

Pág.

# GLOSARIO

**ANCHO DE BANDA:** cantidad de datos que puede ser enviada o recibida a través de una conexión de red en un periodo de tiempo determinado. Generalmente está dado en bites por segundo (BPS), kilobites por segundo (kbps), o megabites por segundo (mps).

**BGP (Border Gateway Protocol):** conocido como protocolo de puerta de enlace de frontera, permite el intercambio de información entre grandes nodos de Internet encontrando el camino mas eficiente para transferir una gran cantidad de información entre dos puntos de red.

**CONECTIVIDAD:** medida en los nodos o componentes de una red que están conectados entre sí y la facilidad o velocidad con la que pueden intercambiar información. Esta permite que los datos fluyan en forma bidireccional.

**DHCP:** protocolo de configuración dinámica de host, es de tipo cliente/servidor mediante el cual un servidor de red DHCP asigna de forma dinámica las direcciones IP y otros parámetros de configuración de red a los diferentes dispositivos conectados.

**DIRECCIÓN IP:** dirección de protocolo de Internet, es un número único e irrepetible con el cual se identifica una computadora conectada a una red que conrre con el protocolo IP. Dicho Número IP es asignado de manera permanente (estática) o temporal (dinámica) a cada equipo conectado a la red.

**DTP (Dynamic Trunk Protocol):** el protocolo de enlace dinámico fue creado por Cisco Systems, se utiliza para gestionar de forma dinámica la configuración del enlace troncal entre dos switches CISCO.

**EIGRP:** protocolo de enrutamiento de puerta de enlace interior, es un protocolo de encaminamiento de estado de enlace, propiedad de Cisco Systems que ofrece lo mejor de los algoritmos de vector de distancias y del estado de enlace.

**ENRUTAMIENTO:** proceso en el que se busca identificar la mejor ruta (ruta más corta) para reenviar paquetes entre redes; teniendo en cuenta diferentes factores como la tabla de enrutamiento, la métrica, la distancia administrativa, el ancho de banda, etc.

**GATEWAY – PASARELA O PUERTA DE ACCESO:** computador que realiza la conversión de protocolos entre diferentes tipos de redes o aplicaciones. Por ejemplo, una puerta de acceso podría conectar una red de área local a un mainframe. Una puerta de acceso de correo electrónico, o de mensajes, convierte mensajes entre dos diferentes protocolos de mensajes.

**INTERFAZ:** es la conexión entre ordenadores o máquinas con el exterior, sea cual sea la comunicación entre distintos niveles. En software es la parte de un programa que permite el flujo de información entre un usuario y la aplicación, o entre la aplicación y otros programas o periféricos. Esa parte de un programa

está constituida por un conjunto de comandos y métodos que permiten estas intercomunicaciones.

**LOOPBACK:** es una interfaz de red virtual. Utiliza las direcciones del rango '127.0.0.0/8', de las cuales se utiliza de forma mayoritaria, la '127.0.0.1' por ser la primera de dicho rango, añadiendo '::1' para el caso de IPv6 ('127.0.0.1::1').

**OSPF (Open Shortest Path First):** es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos. (Primer camino más corto).

**PING:** en redes de computadoras es un comando que permite diagnosticar el estado, velocidad y calidad de una red determinada por medio del envío de paquetes ICMP de solicitud (ICMP Echo Request) y de respuesta (ICMP Echo Reply).

**ROUTER:** es un dispositivo que proporciona conectividad a nivel de red (en el nivel tres en el modelo OSI). Se encarga de establecer qué ruta se destinará a cada paquete de datos dentro de una red.

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

**VLAN (Red de Área Local Virtual):** es un método que permite crear redes que lógicamente son independientes, aunque estas se encuentren dentro de una misma red física. De esta forma, un usuario podría disponer de varias VLANs dentro de un mismo router o switch.

**VTP (Vlan Trunking Protocol):** es un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite centralizar y simplificar la administración en un dominio de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos. VTP opera en 3 modos distintos:

- Servidor: modo por defecto, se pueden crear, eliminar o modificar VLANs. Su cometido es anunciar su configuración al resto de switches del mismo dominio VTP y sincronizar dicha configuración con la de otros servidores, basándose en los mensajes VTP recibidos a través de sus enlaces trunk.
- Cliente: no se pueden crear, eliminar o modificar VLANs, tan sólo sincronizar esta información basándose en los mensajes VTP recibidos de servidores en el propio dominio. Un reinicio del switch borra la información de la VLAN.
- Transparente: La información VLAN en los switches que trabajen en este modo sólo se puede modificar localmente. Su nombre se debe a que no procesa las actualizaciones VTP recibidas, tan sólo las reenvía a los switches del mismo dominio.

## RESUMEN

El objetivo principal de este trabajo es la sustentación de la evaluación - prueba de habilidades prácticas CCNP, dando solución a tres escenarios de red donde se utilizan diferentes protocolos de comunicación realizando la respectiva configuración de cada dispositivo de acuerdo con la topología de red implememtada, con el fin de poner en práctica las competencias y habilidades desarrolladas a lo largo del diplomado.

**Palabras clave:**

- ✓ CCNP
- ✓ Red
- ✓ Protocolos de comunicación
- ✓ Topología de red
- ✓ Configuración

## INTRODUCCION

En el presente trabajo de grado se evidenciará la implementación de configuraciones para topologías de red orientadas a CCNP Routing (ROUTE) & Switched Networks (SWITCH), documentando la configuración realizada a cada uno de los dispositivos presentes en los tres escenarios propuestos para el desarrollo de la evaluación de habilidades prácticas del diplomado de profundización en CCNP, y describiendo detalladamente el paso a paso de cada una de las etapas realizadas implementando los diferentes protócolos de comunicación como OSPF, EIGRP, EBGP y VTP. Además, se hace uso de los diferentes comandos que permiten verificar la conectividad en tre los dispositivos de una red, como **ping, traceroute, show ip route**, entre otros.

El desarrollo de estas actividades permite comprender que es posible planificar, implementar, verificar y solucionar problemas de redes empresariales locales y de área amplia, partiendo de conocimientos previos y fundamentos de redes.

La simulación de las soluciones realizadas se hace a través del software PACKET TRACER y/o GSN3.

# 1. ESCENARIO 1.

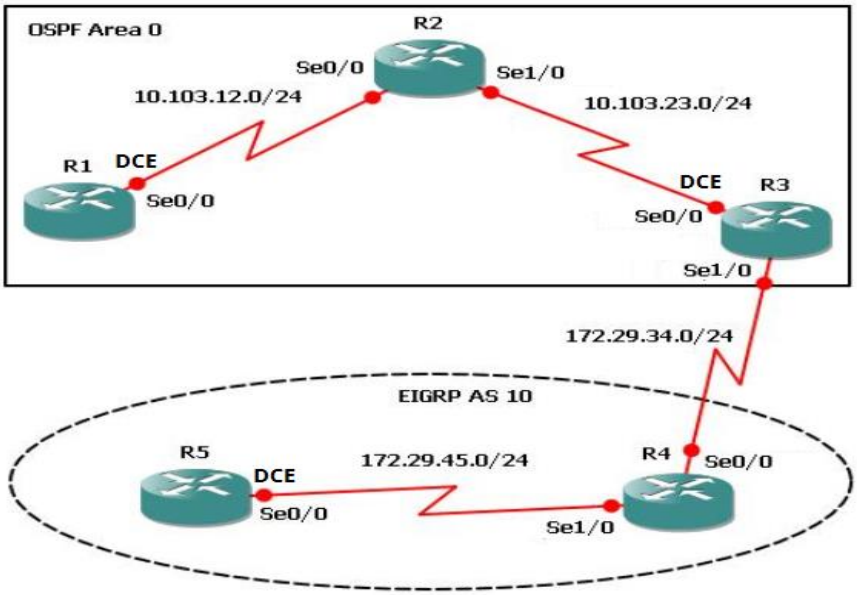


Figura 1. Escenario 1

## 1.1. PASO 1

Aplique las configuraciones iniciales y los protocolos de enrutamiento para los routers R1, R2, R3, R4 y R5 según el diagrama. No asigne passwords en los routers. Configurar las interfaces con las direcciones que se muestran en la topología de red.

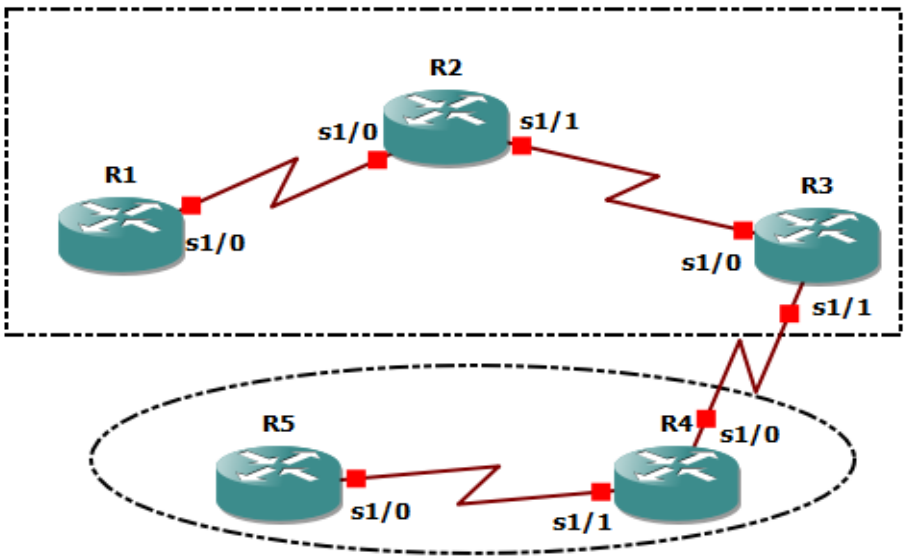


Figura 2. Escenario 1 implementado en GNS3

En la Figura 2, se implementa la topología de red descrita en el escenario 1 en el software de simulación GNS3 empleando la plantilla del router CISCO C7200 con versión de IOS 15.2, realizando las configuraciones iniciales en cada uno de los routers:

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#no ip domain-lookup
R1(config)#line con 0
R1(config-line)#logging synchronous
R1(config-line)#exec-timeout 0 0
R1(config-line)#int s1/0
R1(config-if)#ip address 10.103.12.1 255.255.255.0
R1(config-if)#clock rate 64000
R1(config-if)#bandwidth 64
R1(config-if)#no shutdown
R1(config-if)#
*Jan 29 00:02:46.671: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
R1(config-if)#
*Jan 29 00:02:47.679: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R1(config-if)#
```

```
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#no ip domain-lookup
R2(config)#line con 0
R2(config-line)#logging synchronous
R2(config-line)#exec-timeout 0 0
R2(config-line)#int s1/0
R2(config-if)#ip address 10.103.12.2 255.255.255.0
R2(config-if)#int s1/1
R2(config-if)#ip address 10.103.23.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#
*Jan 29 00:08:17.351: %LINK-3-UPDOWN: Interface Serial1/1, changed state to up
R2(config-if)#
*Jan 29 00:08:18.359: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/1, changed state to up
R2(config-if)#int s1/0
R2(config-if)#no shutdown
R2(config-if)#
*Jan 29 00:08:32.935: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
R2(config-if)#
```

*Jan 29 00:08:33.943: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up

R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#no ip domain-lookup
R3(config)#line con 0
R3(config-line)#logging synchronous
R3(config-line)#exec-timeout 0 0
R3(config-line)#int s1/0
R3(config-if)#ip address 10.103.23.2 255.255.255.0
R3(config-if)#clock rate 64000
R3(config-if)#bandwidth 64
R3(config-if)#no shutdown
R3(config-if)#
*Jan 29 00:15:44.067: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
R3(config-if)#
*Jan 29 00:15:45.075: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R3(config-if)#int s1/1
R3(config-if)#ip address 172.29.34.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#
*Jan 29 00:16:19.667: %LINK-3-UPDOWN: Interface Serial1/1, changed state to up
R3(config-if)#
*Jan 29 00:16:20.675: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/1, changed state to up

R4#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#line con 0
R4(config-line)#logging synchronous
R4(config-line)#exec-timeout 0 0
R4(config-line)#int s1/0
R4(config-if)#ip address 172.29.34.2 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#int s1/1
R4(config-if)#ip address 172.29.45.2 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#
*Jan 29 00:25:10.435: %LINK-3-UPDOWN: Interface Serial1/1, changed state to up
R4(config-if)#

*Jan 29 00:25:11.443: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/1, changed state to up

R5#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R5(config)#no ip domain-lookup
R5(config)#line con 0
R5(config-line)#logging synchronous
R5(config-line)#exec-timeout 0 0
R5(config-line)#int s1/0
R5(config-if)#ip address 172.29.45.1 255.255.255.0
R5(config-if)#clock rate 64000
R5(config-if)#bandwidth 64
R5(config-if)#no shutdown
R5(config-if)#
*Jan 29 00:33:57.675: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
R5(config-if)#
*Jan 29 00:33:58.683: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R5(config-if)#

## 1.2. PASO 2

Cree cuatro nuevas interfaces de Loopback en R1 utilizando la asignación de direcciones 10.1.0.0/22 y configure esas interfaces para participar en el área 0 de OSPF.

R1(config)#interface Loopback0
R1(config-if)#
*Jan 29 00:45:05.675: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R1(config-if)#ip address 10.1.0.1 255.255.255.0
R1(config-if)#interface Loopback1
R1(config-if)#
*Jan 29 00:45:49.603: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#interface Loopback2
R1(config-if)#
*Jan 29 00:46:29.055: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback2, changed state to up
R1(config-if)#ip address 10.1.2.1 255.255.255.0
R1(config-if)#interface Loopback3
R1(config-if)#

```
*Jan 29 00:46:57.899: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback3, changed state to up
R1(config-if)#ip address 10.1.3.1 255.255.255.0
R1(config-if)#router ospf 100
R1(config-router)#network 10.1.0.0 255.255.252.0 area 0.0.0.0
R1(config-router)#
```

### 1.3. PASO 3

Cree cuatro nuevas interfaces de Loopback en R5 utilizando la asignación de direcciones 172.5.0.0/22 y configure esas interfaces para participar en el Sistema Autónomo EIGRP 10.

```
R5(config)#interface Loopback4
R5(config-if)#
*Jan 29 00:51:47.999: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback4, changed state to up
R5(config-if)#ip address 172.5.4.1 255.255.255.0
R5(config-if)#interface Loopback5
R5(config-if)#
*Jan 29 00:52:59.195: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback5, changed state to up
R5(config-if)#ip address 172.5.5.1 255.255.255.0
R5(config-if)#interface Loopback6
R5(config-if)#
*Jan 29 00:53:15.467: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback6, changed state to up
R5(config-if)#ip address 172.5.6.1 255.255.255.0
R5(config-if)#interface Loopback7
R5(config-if)#
*Jan 29 00:53:43.035: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback7, changed state to up
R5(config-if)#ip address 172.5.7.1 255.255.255.0
R5(config-if)#router eigrp 10
R5(config-router)#network 172.5.0.0 255.255.252.0
R5(config-router)#
```

### 1.4. PASO 4

Analice la tabla de enrutamiento de R3 y verifique que R3 está aprendiendo las nuevas interfaces de Loopback mediante el comando **show ip route**.

Se verifica la tabla de enrutamiento de R3 y se observa que el dispositivo está aprendiendo las nuevas interfaces de Loopback:

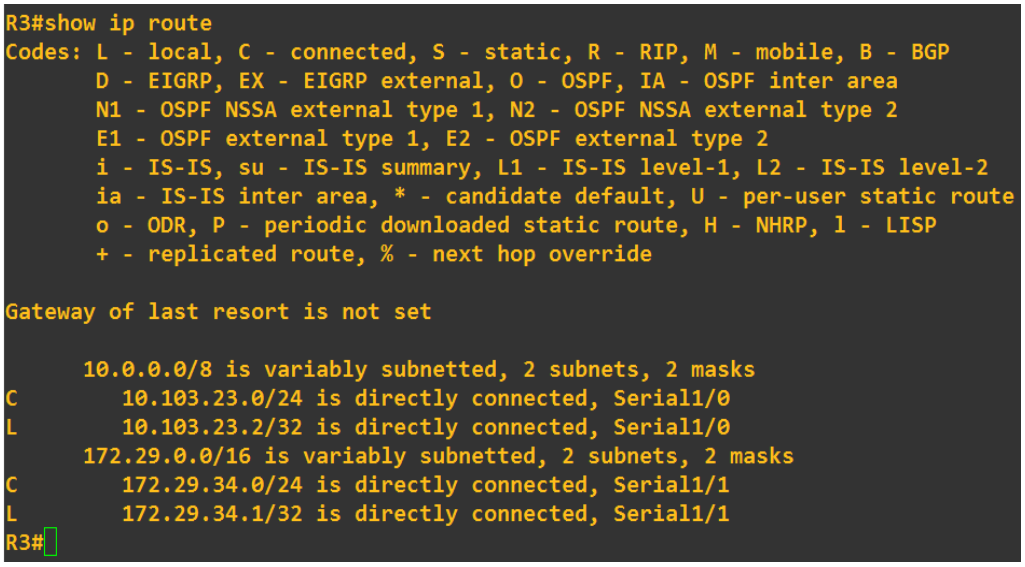


Figura 3. Resultado de Comando show ip route en R3

## 1.5. PASO 5

Configure R3 para redistribuir las rutas EIGRP en OSPF usando el costo de 50000 y luego redistribuya las rutas OSPF en EIGRP usando un ancho de banda T1 y 20,000 microsegundos de retardo.

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router eigrp 10
R3(config-router)#redistribute ospf 10 metric 50000 100 255 1 1500
R3(config-router)#network 10.1.0.0 255.255.252.0
R3(config-router)#auto-summary
R3(config-router)#exit
R3(config)#router ospf 10
R3(config-router)#log-adjacency-changes
R3(config-router)#redistribute eigrp 10 subnets
R3(config-router)#network 172.5.0.0 255.255.0.0 area 0
R3(config-router)#
```

## 1.6. PASO 6

Verifique en R1 y R5 que las rutas del sistema autónomo opuesto existen en su tabla de enrutamiento mediante el comando **show ip route**.

```
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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 10 subnets, 2 masks
C        10.1.0.0/24 is directly connected, Loopback0
L        10.1.0.1/32 is directly connected, Loopback0
C        10.1.1.0/24 is directly connected, Loopback1
L        10.1.1.1/32 is directly connected, Loopback1
C        10.1.2.0/24 is directly connected, Loopback2
L        10.1.2.1/32 is directly connected, Loopback2
C        10.1.3.0/24 is directly connected, Loopback3
L        10.1.3.1/32 is directly connected, Loopback3
C        10.103.12.0/24 is directly connected, Serial1/0
L        10.103.12.1/32 is directly connected, Serial1/0
R1#
```

Figura 4. Resultado de Comando show ip route en R1

```
R5#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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      172.5.0.0/16 is variably subnetted, 8 subnets, 2 masks
C        172.5.4.0/24 is directly connected, Loopback4
L        172.5.4.1/32 is directly connected, Loopback4
C        172.5.5.0/24 is directly connected, Loopback5
L        172.5.5.1/32 is directly connected, Loopback5
C        172.5.6.0/24 is directly connected, Loopback6
L        172.5.6.1/32 is directly connected, Loopback6
C        172.5.7.0/24 is directly connected, Loopback7
L        172.5.7.1/32 is directly connected, Loopback7
      172.29.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.29.45.0/24 is directly connected, Serial1/0
L        172.29.45.1/32 is directly connected, Serial1/0
R5#
```

Figura 5. Resultado de Comando show ip route en R5

De acuerdo con el resultado obetenido a través del comando **show ip route** de las tablas de enrutamiento del router R1 y del router R5 se comprueba que las rutas del sistema autonomo opuesto existen en cada uno de los dos dispositivos.

## 2. ESCENARIO 2.

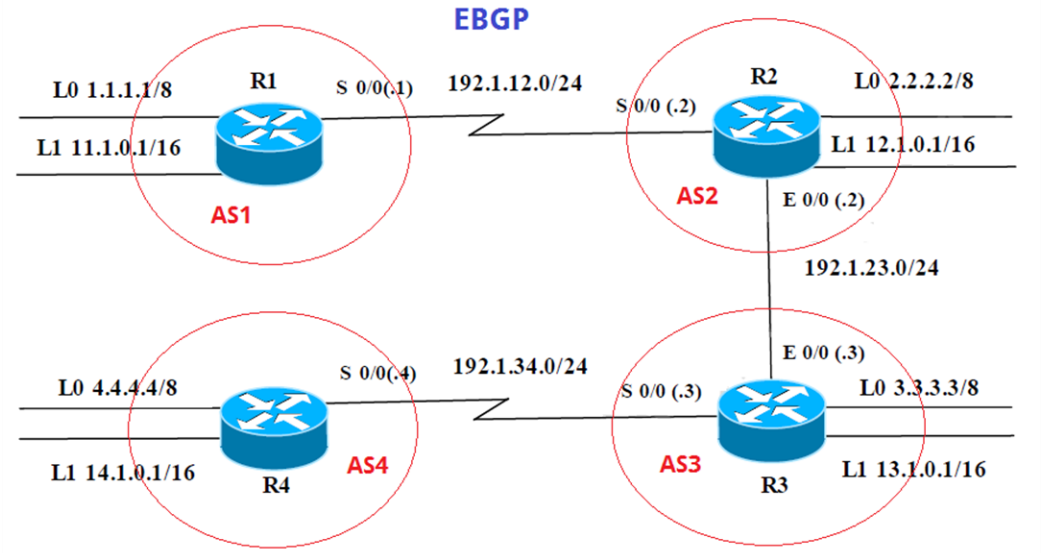


Figura 6. Escenario 2

Información de configuración de los Routers:

**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 |

**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 |

**R3**

| Interfaz | Dirección IP | Máscara |
|---|---|---|
| **Loopback 0** | 3.3.3.3 | 255.0.0.0 |
| **Loopback 1** | 13.1.0.1 | 255.255.0.0 |
| **E 0/0** | 192.1.23.3 | 255.255.255.0 |
| **S 0/0** | 192.1.34.3 | 255.255.255.0 |

**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 |

## 2.1. PASO 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 11.11.11.11 para R1 y como 22.22.22.22 para R2. Presente el paso a con los comandos utilizados y la salida del comando **show ip route**.

El primer paso que se realiza es implementar la topología de red descrita en el escenario 2, en el software GNS3 empleando la plantilla del router CISCO C7200 con versión de IOS 15.2 y realizar las configuraciones de loa parámetros iniciales de cada Router.

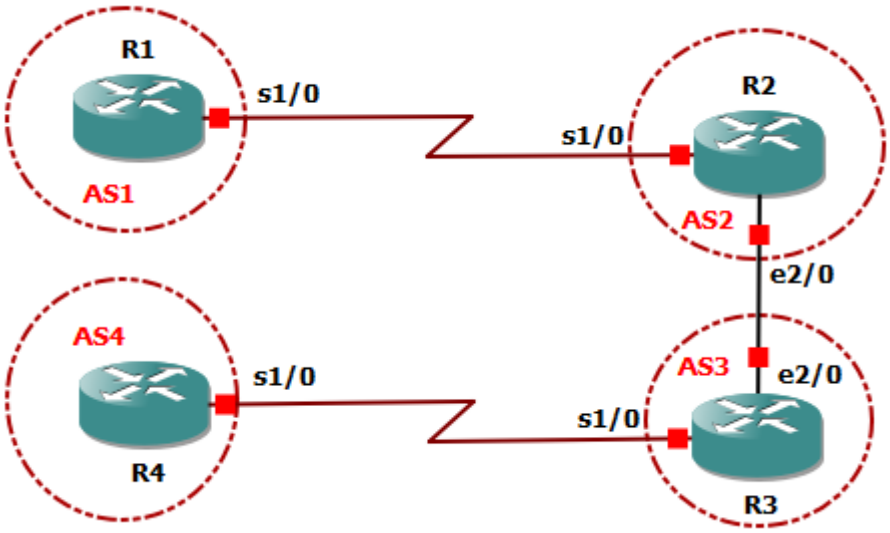


Figura 7. Escenario 2 implementado en GNS3

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface Loopback0
R1(config-if)#
*Jan 29 02:22:04.191: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R1(config-if)#ip address 1.1.1.1 255.0.0.0
R1(config-if)#interface Loopback1
R1(config-if)#
*Jan 29 02:22:43.655: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
R1(config-if)#ip address 11.1.0.1 255.255.0.0
R1(config-if)#interface s1/0
R1(config-if)#ip address 192.1.12.1 255.255.255.0
```

```
R1(config-if)#no shutdown
R1(config-if)#
*Jan 29 02:23:21.383: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
R1(config-if)#
*Jan 29 02:23:22.387: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R1(config-if)#

R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface Lo0
R2(config-if)#
*Jan 29 02:25:25.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R2(config-if)#ip address 2.2.2.2 255.0.0.0
R2(config-if)#interface Lo1
R2(config-if)#
*Jan 29 02:25:42.431: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
R2(config-if)#ip address 12.1.0.1 255.255.0.0
R2(config-if)#interface Ethernet2/0
R2(config-if)#ip address 192.1.23.2 255.255.255.0
R2(config-if)#interface s1/0
R2(config-if)#ip address 192.1.12.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#
*Jan 29 02:26:49.087: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
R2(config-if)#
*Jan 29 02:26:50.095: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R2(config-if)#

R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface Lo0
R3(config-if)#
*Jan 29 02:28:20.311: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R3(config-if)#ip address 3.3.3.3 255.0.0.0
R3(config-if)#interface Lo1
R3(config-if)#
*Jan 29 02:29:02.235: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
R3(config-if)#ip address 13.1.0.1 255.255.0.0
```

```
R3(config-if)#interface Ethernet2/0
R3(config-if)#ip address 192.1.23.3 255.255.255.0
R3(config-if)#interface s1/0
R3(config-if)#ip address 192.1.34.3 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#
*Jan 29 02:30:21.147: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
R3(config-if)#
*Jan 29 02:30:22.155: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R3(config-if)#
```

```
R4#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#interface Lo0
R4(config-if)#
*Jan 29 02:31:40.603: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R4(config-if)#ip address 4.4.4.4 255.0.0.0
R4(config-if)#interface Lo1
R4(config-if)#
*Jan 29 02:31:55.163: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
R4(config-if)#ip address 14.1.0.1 255.255.0.0
R4(config-if)#interface s1/0
R4(config-if)#ip address 192.1.34.4 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#
*Jan 29 02:32:47.763: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
R4(config-if)#
*Jan 29 02:32:48.771: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
R4(config-if)#
```

Teniendo configurados los parámetros iniciales de cada router, se procede a realizar la configuración de protocolo BGP.

Configuración de relación de Vecino entre R1 y R2:

```
R1(config)#router bgp 200
R1(config-router)#neighbor 192.1.12.2 remote-as 100
R1(config-router)#network 10.1.1.1
```

Configuración de relación de Vecino entre R2 y R1:

```
R2(config)#router bgp 300
R2(config-router)#neighbor 192.1.12.3 remote-as 100
R2(config-router)#network 2.2.2.2
```

Y finalmente se realiza el anunciamiento de las direcciones BGP y la codificación de los routers R1 y R2 respectivamente:

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router rip
R1(config-router)#network 2.2.2.2
R1(config-router)#redistribute bgp 200
R1(config-router)#router bgp 200
R1(config-router)#neighbor 11.11.11.11 remote-as 300
R1(config-router)#neighbor 11.11.11.11 distribute-list 1 out
R1(config-router)#redistribute rip
R1(config-router)#access-list 1 permit 2.2.2.2 255.0.0.0
```

```
R2(config)#router rip
R2(config-router)#network 1.1.1.1
R2(config-router)#redistribute bgp 300
R2(config-router)#router bgp 300
R2(config-router)#neighbor 22.22.22.22 remote-as 200
R2(config-router)#neighbor 22.22.22.22 distribute-list 1 out
R2(config-router)#redistribute rip
R2(config-router)#access-list 1 permit 1.1.1.1 255.0.0.0
```

Se verifica la tabla de enrutamiento de los routers con el comando **show ip route**

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      1.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        1.0.0.0/8 is directly connected, Loopback0
L        1.1.1.1/32 is directly connected, Loopback0
      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
      192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.12.0/24 is directly connected, Serial1/0
L        192.1.12.1/32 is directly connected, Serial1/0
R1#
```

Figura 8. Resultado de comando show ip route en R1

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      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
      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, Serial1/0
L        192.1.12.2/32 is directly connected, Serial1/0
      192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.23.0/24 is directly connected, Ethernet2/0
L        192.1.23.2/32 is directly connected, Ethernet2/0
R2#
```

Figura 9. Resultado de comando show ip route en R2

## 2.2. PASO 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 33.33.33.33. Presente el paso a con los comandos utilizados y la salida del comando **show ip route**.

Se realiza la configuración de vecino entre R2 y R3:

R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router bgp 300
R2(config-router)#neighbor 192.1.12.3 remote-as 100
R2(config-router)#network 3.3.3.3

Se realiza la configuración de vecino entre R3 y R2:

R3(config)#router bgp 400
R3(config-router)#neighbor 192.1.12.3 remote-as 100
R3(config-router)#network 2.2.2.2

Y se realiza el anunciamiento de las direcciones BGP y la codificación del router R3:

R3(config-router)#router rip
R3(config-router)#network 2.2.2.2
R3(config-router)#redistribute bgp 400

R3(config-router)#router bgp 400
R3(config-router)#neighbor 33.33.33.33 remote-as 300
R3(config-router)#neighbor 33.33.33.33 distribute-list 1 out
R3(config-router)#redistribute rip
R3(config-router)#access-list 1 permit 2.2.2.2 255.0.0.0

Se verifica tabla de enrutamiento de 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      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
      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, Ethernet2/0
L        192.1.23.3/32 is directly connected, Ethernet2/0
      192.1.34.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.1.34.0/24 is directly connected, Serial1/0
L        192.1.34.3/32 is directly connected, Serial1/0
R3#
```

Figura 10. Resultado de comando show ip route en R3

## 2.3. PASO 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 44.44.44.44. 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**.

Se realiza la configuración de vecino entre R3 y R4:

R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router bgp 400
R3(config-router)#neighbor 192.1.34.2 remote-as 100
R3(config-router)#network 4.4.4.4

Se realiza la configuración de vecino entre R4 y R3:

```
R4#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#router bgp 500
R4(config-router)#neighbor 192.1.34.2 remote-as 100
R4(config-router)#network 3.3.3.3
```

Se realiza el anunciamiento de las direcciones de Loopback en BGP para R4, teniendo en cuenta la codificación y el enrutamiento estático en la interfaz Loopback 0:

```
R4(config-router)#router rip
R4(config-router)#network 3.3.3.3
R4(config-router)#redistribute bgp 500
R4(config-router)#router bgp 500
R4(config-router)#
R4(config-router)#neighbor 44.44.44.44 remote-as 400
R4(config-router)#neighbor 44.44.44.44 distribute-list 1 out
R4(config-router)#access-list 1 permit 3.3.3.3 255.0.0.0
```

Se verifica tabla de enrutamiento de 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

      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, Serial1/0
L        192.1.34.4/32 is directly connected, Serial1/0
R4#
```

Figura 11. Resultado de comando show ip route en R3

# 3. ESCENARIO 3.

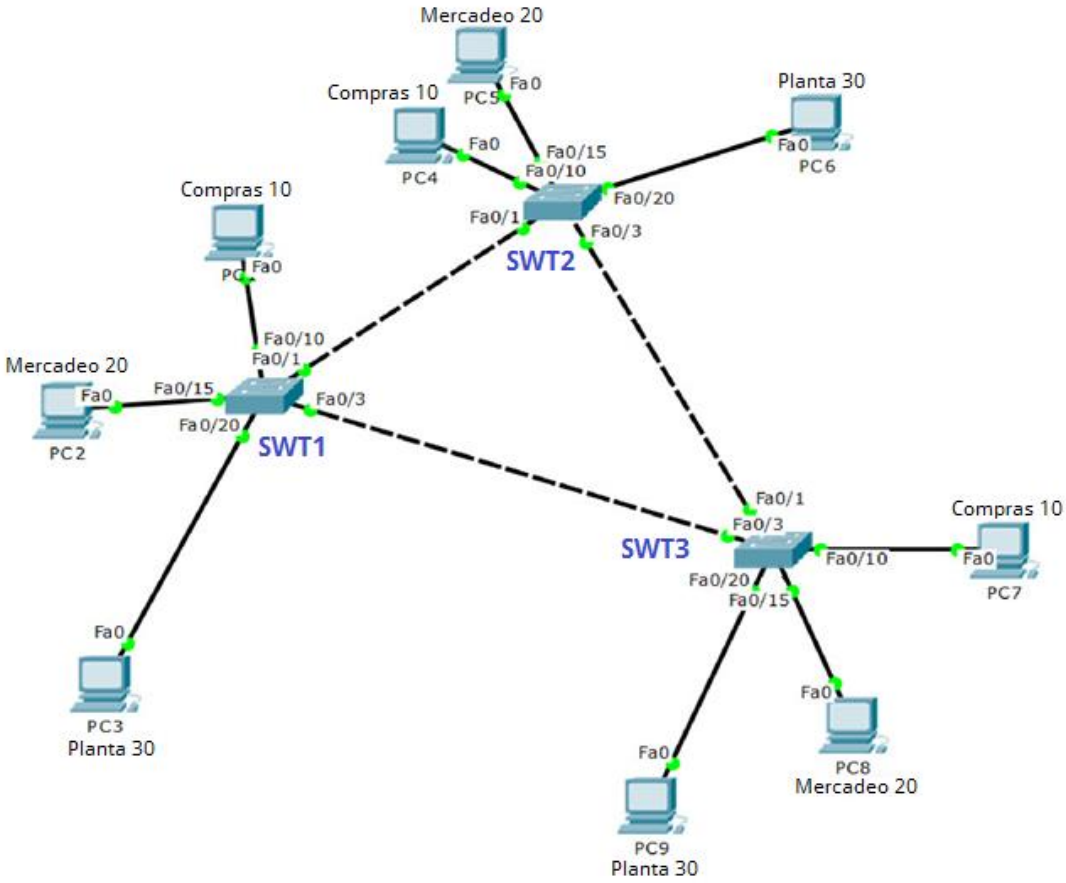


Figura 12. Escenario 3

## 3.1. CONFIGURAR VTP

### 3.1.1. Paso 1

Todos los switches se configurarán para usar VTP para las actualizaciones de VLAN. El switch SWT2 se configurará como el servidor. Los switches SWT1 y SWT3 se configurarán como clientes. Los switches estarán en el dominio VPT llamado CCNP y usando la contraseña cisco.

Para poder dar solución al escenario de red tres, se implemeta la topología de red en el software de simulación Packet Tracer utilizando el switch de CISCO 2960 y computadores genericos; este se puede observar en la figura 13. Teniendo la red implementada se inicia con las configuraciones requeridas, iniciando con el Switch que se desea sea el servidor (SWT2):

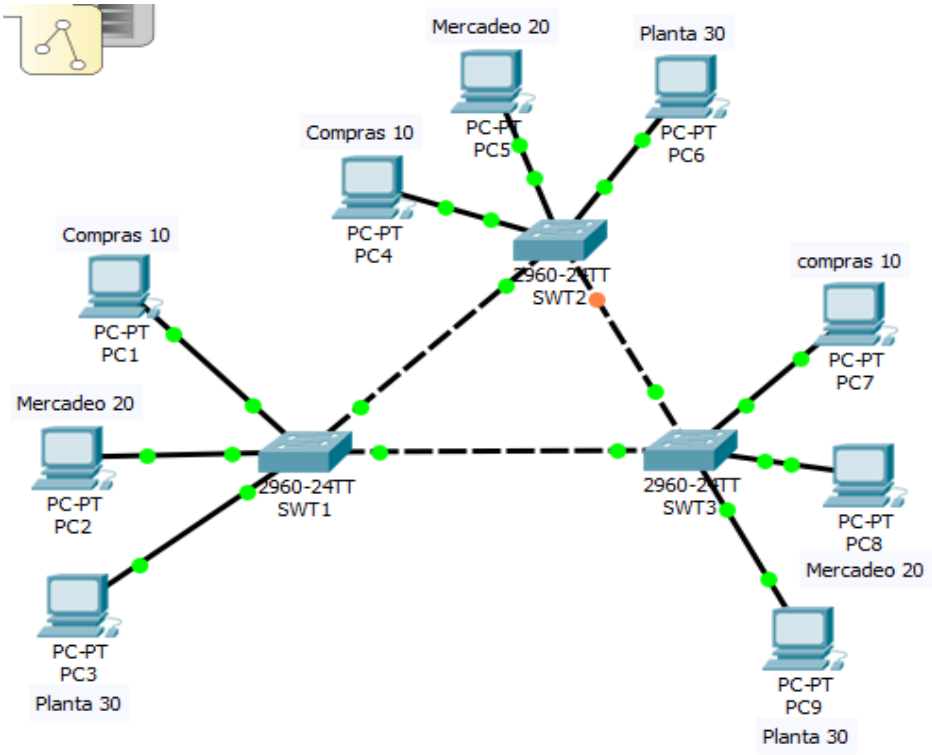


Figura 13. Escenario 3 implementado en Packet Tracer

```
Switch>enable
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
Switch(config)#vtp mode server
Device mode already VTP SERVER.
Switch(config)#vtp password cisco
Setting device VLAN database password to cisco
Switch(config)#hostname SWT2
SWT2(config)#
```

En seguida se realiza la configuración de los switches en modo cliente:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SWT1
SWT1(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SWT1(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWT1(config)#vtp password cisco
```

```
Setting device VLAN database password to cisco
SWT1(config)#

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SWT3
SWT3(config)#vtp domain CCNP
Changing VTP domain name from NULL to CCNP
SWT3(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWT3(config)#vtp password cisco
Setting device VLAN database password to cisco
SWT3(config)#
```

### 3.1.2. Paso 2

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

```
SWT1#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
SWT1#
```

Figura 14. Estado VTP SWT1

```
SWT2#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)
SWT2#
```

Figura 15. Estado VTP SWT1

```
SWT3#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
SWT3#
```

Figura 16. Estado VTP SWT1

## 3.2. CONFIGURAR DTP (DYNAMIC TRUNKING PROTOCOL)

### 3.2.1. Paso 1

Configure un enlace troncal ("trunk") dinámico entre SWT1 y SWT2. Debido a que el modo por defecto es **dynamic auto**, solo un lado del enlace debe configurarse como **dynamic desirable.**

SWT1(config)#int fa0/1
SWT1(config-if)#switchport mode dynamic desirable
SWT1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

### 3.2.2. Paso 2

Verifique el enlace "trunk" entre SWT1 y SWT2 usando el comando **show interfaces trunk.**

```
SWT1#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       desirable    n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

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

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

SWT1#
```

Figura 17. Enlace trunk en SWT1

```
SWT2#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005

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

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

SWT2#
```

Figura 18. Enlace trunk en SWT2

### 3.2.3. Paso 3

Entre SWT1 y SWT3 configure un enlace "trunk" estático utilizando el comando **switchport mode trunk** en la interfaz F0/3 de SWT1.

SWT1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWT1(config)#int fa0/3
SWT1(config-if)#switchport mode trunk
SWT1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

SWT1#

### 3.2.4. Paso 4

Verifique el enlace "trunk" el comando **show interfaces trunk** en SWT1.

```
SWT1#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       desirable    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

SWT1#
```

Figura 19. Interfaces trunk en SWT1

### 3.2.5. Paso 5

Configure un enlace "trunk" permanente entre SWT2 y SWT3.

Un enlace “trunk” permanente entre dos switch, corresponde a la configuración de un enlace troncal estático en cada interfaz que interconecta los dos dispositivos, para este caso la interfa Fa0/3 en el switch 2 y Fa0/1 en el 3:

SWT2(config)#int fa0/3
SWT2(config-if)#switchport mode trunk
SWT2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
SWT2(config-if)#

SWT3(config)#int fa0/1
SWT3(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

SWT3(config-if)#switchport mode trunk
SWT3(config-if)#

Se verifica las interfaces en los dos switch:

```
SWT2#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       auto         n-802.1q       trunking      1
Fa0/3       on           802.1q         trunking      1

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

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

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

SWT2#
```

Figura 20. Interfaces trunk en SWT2

```
SWT3#show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/3       auto         n-802.1q       trunking      1

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

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

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

SWT3#
```

Figura 21. Interfaces trunk en SWT2

## 3.3. AGREGAR VLANs Y ASIGNAR PUERTOS

### 3.3.1. Paso 1

En STW1 agregue la VLAN 10. En STW2 agregue las VLANS Compras (10), Mercadeo (20), Planta (30) y Admon (99).

```
SWT1>enable
SWT1#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWT1(config)#vlan 10
VTP VLAN configuration not allowed when device is in CLIENT mode.
SWT1(config)#
```

```
SWT2>enable
SWT2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWT2(config)#vlan 10
SWT2(config-vlan)#name Compras
SWT2(config-vlan)#exit
SWT2(config)#vlan 20
SWT2(config-vlan)#name Mercadeo
SWT2(config-vlan)#exit
SWT2(config)#vlan 30
SWT2(config-vlan)#name Planta
SWT2(config-vlan)#exit
SWT2(config)#vlan 99
SWT2(config-vlan)#name Admon
SWT2(config-vlan)#
```

### 3.3.2. Paso 2

Verifique que las VLANs han sido agregadas correctamente.

```
SWT1#show vlan

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
20   Mercadeo                         active
30   Planta                           active
99   Admon                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Figura 22. Vlan's en SWT1

```
SWT2#show vlan

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
20   Mercadeo                         active
30   Planta                           active
99   Admon                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Figura 23. Vlan's en SWT2

### 3.3.3. Paso 3

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

X = número de cada PC particular

```
SWT1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWT1(config)#int fa0/10
SWT1(config-if)#switchport mode access
SWT1(config-if)#switchport access vlan 10
SWT1(config-if)#exit
SWT1(config)#int fa0/15
SWT1(config-if)#switchport mode access
SWT1(config-if)#switchport access vlan 20
SWT1(config-if)#exit
SWT1(config)#int fa0/20
SWT1(config-if)#switchport mode access
SWT1(config-if)#switchport access vlan 30
SWT1(config-if)#
```

### 3.3.4. Paso 4

Configure el puerto F0/10 en modo de acceso para SWT1, SWT2 y SWT3 y asígnelo a la VLAN 10.

```
SWT1(config)#int fa0/10
SWT1(config-if)#switchport mode access
SWT1(config-if)#switchport access vlan 10

SWT2(config)#int fa0/10
SWT2(config-if)#switchport mode access
SWT2(config-if)#switchport access vlan 10

SWT3(config)#int fa0/10
SWT3(config-if)#switchport mode access
SWT3(config-if)#switchport access vlan 10
```

### 3.3.5. Paso 5

Repita el procedimiento para los puertos F0/15 y F0/20 en SWT1, SWT2 y SWT3. Asigne las VLANs y las direcciones IP de los PCs de acuerdo con la tabla de arriba.

```
SWT1(config)#int fa0/15
SWT1(config-if)#switchport mode access
SWT1(config-if)#switchport access vlan 20
SWT1(config-if)#exit
SWT1(config)#int fa0/20
SWT1(config-if)#switchport mode access
SWT1(config-if)#switchport access vlan 30
```

```
SWT2(config)#int fa0/15
SWT2(config-if)#switchport mode access
SWT2(config-if)#switchport access vlan 20
SWT2(config-if)#exit
SWT2(config)#int fa0/20
SWT2(config-if)#switchport mode access
SWT2(config-if)#switchport access vlan 30

SWT3(config)#int fa0/15
SWT3(config-if)#switchport mode access
SWT3(config-if)#switchport access vlan 20
SWT3(config-if)#exit
SWT3(config)#int fa0/20
SWT3(config-if)#switchport mode access
SWT3(config-if)#switchport access vlan 30
```

Se configura las Ips de los PCs, de acuerdo con la VLAN a la que pertenecen y el número de cada PC partícular:

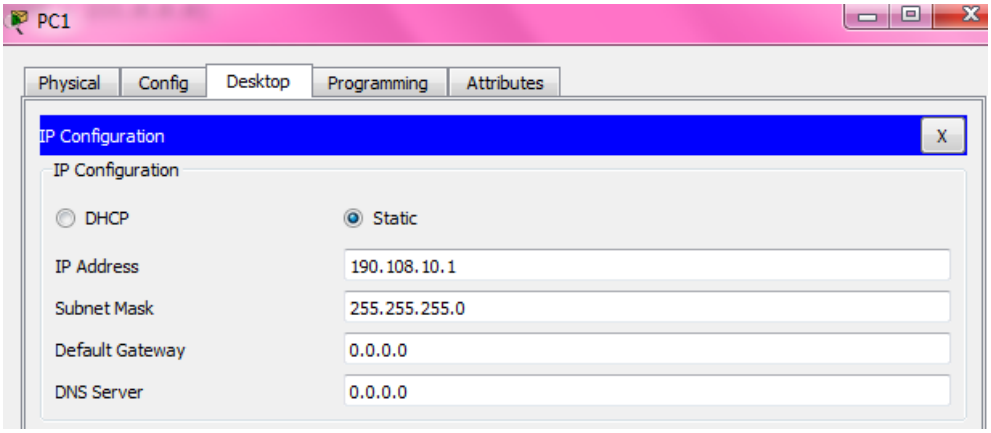


Figura 24. Configuración IP PC VLAN 10

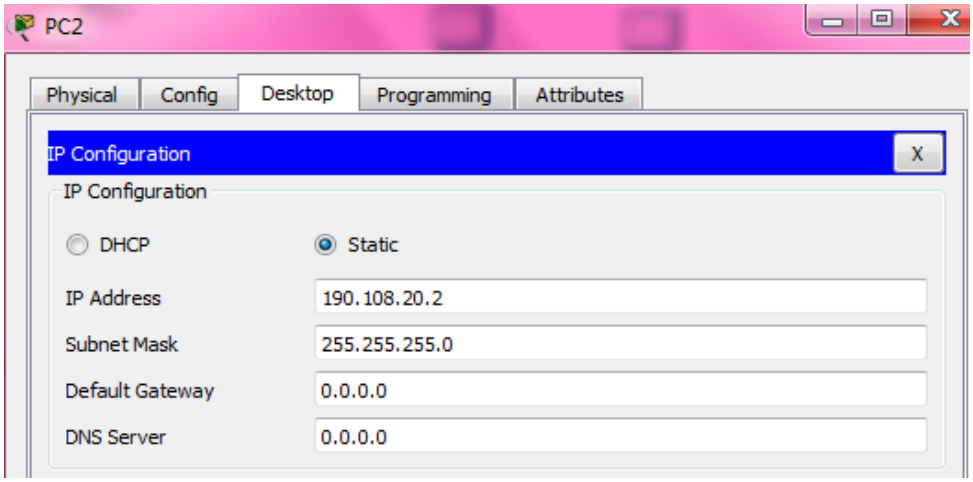


Figura 25. Configuración IP PC VLAN 20

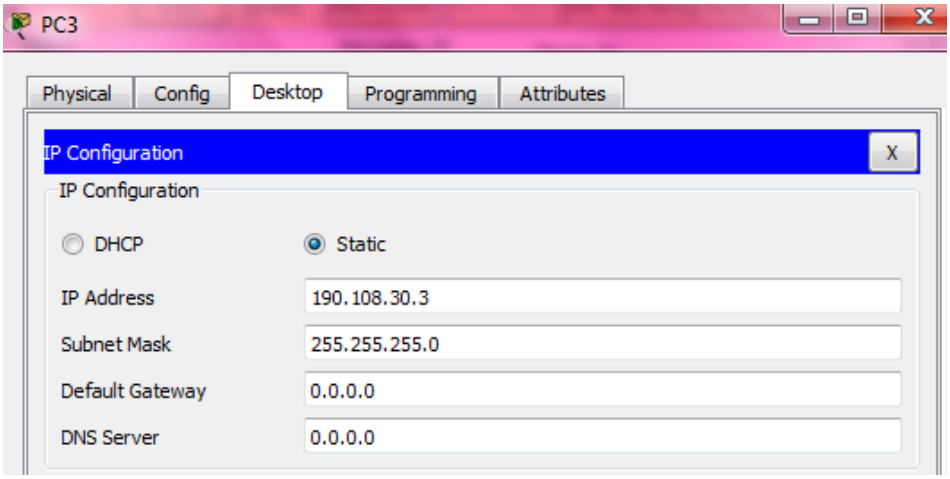


Figura 26. Configuración IP PC VLAN 30

## 3.4. 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.

| Equipo | Interfaz | Dirección IP | Máscara |
|---|---|---|---|
| SWT1 | VLAN 99 | 190.108.99.1 | 255.255.255.0 |
| SWT2 | VLAN 99 | 190.108.99.2 | 255.255.255.0 |
| SWT3 | VLAN 99 | 190.108.99.3 | 255.255.255.0 |

SWT1(config)#int vlan 99
SWT1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

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

SWT1(config-if)#ip address 190.108.99.1 255.255.255.0
SWT1(config-if)#no shutdown

SWT2(config)#int vlan 99
SWT2(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
SWT2(config-if)#ip address 190.108.99.2 255.255.255.0

SWT2(config-if)#no shutdown

SWT3(config)#int vlan 99
SWT3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

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

SWT3(config-if)#ip address 190.108.99.3 255.255.255.0
SWT3(config-if)#no shutdown

## 3.5. VERIFICAR LA CONECTIVIDAD EXTREMO A EXTREMO

### 3.5.1. Paso 1

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

Para verificar la conexión de extremo a extremo entre los PCs, se realiza ping desde el PC1 que se encuentra conectado al SWT1 y VLAN10 a cada uno de los PCs que se encuentran conectados en el SWT2 y SWT3:

```
Packet Tracer PC Command Line 1.0
C:\>
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=27ms TTL=128
Reply from 190.108.10.4: bytes=32 time=3ms TTL=128
Reply from 190.108.10.4: bytes=32 time=3ms TTL=128
Reply from 190.108.10.4: bytes=32 time<1ms 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 = 0ms, Maximum = 27ms, Average = 8ms

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=13ms TTL=128
Reply from 190.108.10.7: bytes=32 time<1ms TTL=128
Reply from 190.108.10.7: bytes=32 time=4ms TTL=128
Reply from 190.108.10.7: bytes=32 time=9ms 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 = 13ms, Average = 6ms
```

Figura 27. Ping desde PC1 a PC4 y PC 7

El ping desde el PC1 al PC4 y PC7 es éxitoso, debido a que los PCs pertenecen a la misma VLAN y mismo segmento de red.

```
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),

C:\>ping 190.108.20.8

Pinging 190.108.20.8 with 32 bytes of data:

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

Ping statistics for 190.108.20.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\>ping 190.108.30.6

Pinging 190.108.30.6 with 32 bytes of data:

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

Ping statistics for 190.108.30.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.30.9

Pinging 190.108.30.9 with 32 bytes of data:

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

Ping statistics for 190.108.30.9:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figura 28. Ping desde PC1 a PC5, PC8, PC6 y PC9

El ping desde el PC1 a los PCs 5, 6, 8 Y 9 NO es éxitoso, debido a que los PCs NO pertenecen a la misma VLAN ni al mismo segmento de red.

Por lo tanto, se puede concluir que entre los PCs que se encuentran en la misma VLAN el ping será exitoso, mientras que entre los PCs de diferente VLANs no se tendrá respuesta exitosa de ping; es decir que no hay conexión entre dichos equipos.

### 3.5.2. Paso 2

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

```
SWT1>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 = 0/1/6 ms

SWT1>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 = 0/3/15 ms
```

Figura 29. Ping desde SWT1 a los switch SWT2 y SWT3

```
SWT2>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

SWT2>ping 190.108.99.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.99.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms
```

Figura 30. Ping desde SWT2 a los switch SWT1 y SWT3

```
SWT3>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

SWT3>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 = 0/1/3
ms
```

Figura 31. Ping desde SWT3 a los switch SWT1 y SWT2

### 3.5.3. Paso 3

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

```
SWT1>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)

SWT1>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)

SWT1>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)

SWT1>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)

SWT1>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)

SWT1>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 32. Ping desde SWT1 a los PCs

El ping desde cada Switch a cada PC no tiene éxito debido a que no pertenecen a la misma VLAN ni al mismo segmento de red.

# 4. CONCLUSIONES

- Los protocolos de enrutamiento permiten implementar diferentes tipo de red de acuerdo con la necesidad de un usuario, facilitando la conexión entre diferentes dispositivos y tipos de red.

- El protocolo OSPF facilita la implementación de grandes redes, ya que por medio de este se puede establecer la mejor ruta para la transmisión de información bidireccional mejorando el tiempo de transmisión y disminuyendo la perdida de datos.

- EL protócolo de enrutamiento BGP se diferencia de los demás protocolos por su método para determinar la mejor ruta, ya que se basa en políticas; teniendo en cuenta diferente variables, como la ruta AS, el peso, la preferencia local, MED, etc.

- El protócolo VTP permite administrar la adición, eliminación y modificación de VLANs a nivel general de una red desde un único switch configurado como servidor.

- Las VLAN permiten realizar la segmentación de una red de acuerdo con las diferentes necesidades de un usuario sin importar su ubicación física, permitiendo y/o bloqueando la comunicación entre dispositivos especificos de acuerdo con el segmento a que pertenezca cada dispositivo.

- El diplomado de profundización CCNP permite adquirir el conocimiento necesario para el desarrollo de habilidades y competencias útiles en la configuración de redes y su diferentes dispositivos de red, en especial la adminitración de switches y enrutadores.

- Los software de simulación GNS3 y Packet Tracer son herramientas indispensables en el estudio de redes y comunicaciones, ya que permiten fortalecer las habilidades implementando diferentes topologías de red que pueden ser útiles en la vida real; en grades organizaciones.

## BIBLIOGRAFÍA

FROOM, Richard y FRAHIM, Erum. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115. 1 ed. Indianapolis: CISCO Press, 2015, 785 p. Recuperado desde: https://1drv.ms/b/s!AmIJYei-NT1IlnWR0hoMxgBNv1CJ

TEARE, Diane, VACHON, Bob y GRAZIANI, Rick. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. 1 ed. Indianapolis: CISCO Press, 2015, 768 p. Recuperado desde: https://1drv.ms/b/s!AmIJYei-NT1IlnMfy2rhPZHwEoWx

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Introducción a la configuración de Switches y Routers. [OVA] Bogotá: UNAD, 2015. Recuperado de: https://1drv.ms/u/s!AmIJYei- NT1IhgL9QChD1m9EuGqC

# ANEXOS

## Anexo A. Simulación GNS3 Escenario 1

Escenario1_HabilidadesPrácticasCCNP.gns3

## Anexo B. Simulación GNS3 Escenario 2

Escenario2_HabilidadesPrácticasCCNP.gns3

## Anexo C. Simulación Packet Tracer Escenario 3

Escenario3_HabilidadesPrácticasCCNP.pkt