

EVALUACIÓN FINAL  
PRUEBA DE HABILIDADES CISCO CCNP

OMAR OSWALDO GARAVITO JEJÉN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BASICAS, TECNOLOGÍA E INGENIERÍA  
INGENIERÍA DE TELECOMUNICACIONES  
BOGOTÁ D.C.

2019

EVALUACIÓN FINAL  
PRUEBA DE HABILIDADES PRÁCTICAS CISCO CCNP

OMAR OSWALDO GARAVITO JEJÉN

Sustentación de Diplomado de Profundización CISCO-CCNP para optar al título de  
Ingeniero de Telecomunicaciones

MSc. Gerardo Granados Acuña  
Director del Diplomado de Profundización Cisco-CCNP

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

2019

NOTA DE ACEPTACION

---

---

---

---

---

---

---

---

Presidente del jurado

---

Jurado

---

Jurado

## CONTENIDO

	pág.
INTRODUCCIÓN.....	11
1. DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES.....	12
1.1. ESCENARIO 1.....	12
1.1.1. Configuración inicial .....	12
1.1.2. Enrutamiento.....	16
1.1.3. Análisis de enrutamiento .....	19
1.1.4. Redistribución de rutas.....	20
1.2. ESCENARIO 2.....	22
1.2.1. Configuración inicial .....	22
1.2.2. Enrutamiento BGP .....	26
1.3. ESCENARIO 3.....	33
1.3.1. Configuración VTP .....	33
1.3.2. Configurar DTP (Dynamic Trunking Protocol).....	36
1.3.3. Configuración troncal estática .....	37
1.3.4. Configuración troncal permanente.....	38
1.3.5. Agregar VLANs .....	40
1.3.6. Configuración de direccionamiento .....	42
1.3.7. Asignación de puertos a las VLAN .....	42
1.3.8. Configuración de las direcciones IP en los Switch.....	44
1.3.9. Verificación de la conectividad Extremo a Extremo .....	46
2. CONCLUSIONES.....	53
BIBLIOGRAFÍA.....	54

## LISTA DE FIGURAS

	pág.
Figura 1. Descripción gráfica de la topología del escenario 1. ....	12
Figura 2. Ping interfaz vecina R1 .....	15
Figura 3. Ping interfaz vecina R2 .....	15
Figura 4. Ping interfaz vecina R3 .....	15
Figura 5. Ping interfaz vecina R4 .....	16
Figura 6. Ping interfaz vecina R5 .....	16
Figura 7. Rutas aprendidas en R3 .....	19
Figura 8. Rutas aprendidas en R1 por redistribución .....	21
Figura 9. Rutas aprendidas en R5 por redistribución .....	21
Figura 10. Descripción gráfica de la topología del escenario 2. ....	22
Figura 11. Ping interfaz vecina R1 .....	25
Figura 12. Ping interfaz vecina R2 .....	25
Figura 13. Ping interfaz vecina R3 .....	25
Figura 14. Ping interfaz vecina R4 .....	25
Figura 15. Confirmación de vecindad entre R1 y R2.....	27
Figura 16. Verificación rutas BGP en R1 .....	27
Figura 17. Verificación rutas BGP en R2 .....	28
Figura 18. Confirmación de vecindad entre R2 y R3.....	29
Figura 19. Verificación rutas BGP en R2 .....	29
Figura 20. Verificación rutas BGP en R3 .....	30

Figura 21. Confirmación de vecindad entre R3 y R4.....	31
Figura 22. Verificación rutas BGP en R3 .....	32
Figura 23. Verificación rutas BGP en R4 .....	32
Figura 24. Topología Escenario 3 .....	33
Figura 25. Verificación modo de operación SWT1 .....	35
Figura 26. Verificación modo de operación SWT2 .....	35
Figura 27. Verificación modo de operación SWT3 .....	35
Figura 28. Verificación DTP en F0/1 de SWT1 .....	36
Figura 29. Verificación modo troncal en F0/1 de SWT2 .....	37
Figura 30.. Verificación modo troncal de F0/3 en SWT1 .....	38
Figura 31.. Verificación modo troncal permanente en F0/3 de SWT2 .....	39
Figura 32. Verificación modo troncal permanente en F0/1 de SWT3 .....	39
Figura 33. Verificación VLANS en SWT1 .....	40
Figura 34. Verificación VLANS en SWT2.....	41
Figura 35. Verificación VLANS en SWT3.....	41
Figura 36. Comprobación de la difusión de la VLAN 99 en SWT3 .....	45
Figura 37. Ping desde PC1 (VLAN10) a PC4 (VLAN10), PC5 (VLAN20) y PC9 (VLAN30).....	46
Figura 38. Ping desde PC6 (VLAN30) a PC1 (VLAN10), PC8 (VLAN20) y PC9 (VLAN30).....	47
Figura 39. Ping desde PC8 (VLAN20) a PC4 (VLAN10), PC5 (VLAN20) y PC3 (VLAN30).....	48
Figura 40. Ping desde SWT1 (VLAN99) a SWT2 (VLAN99) y a SWT3 (VLAN99)	49
Figura 41. Ping desde SWT2 (VLAN99) a SWT1 (VLAN99) y a SWT3 (VLAN99)	49

Figura 42. Ping desde SWT3 (VLAN99) a SWT1 (VLAN99) y a SWT2 (VLAN99)	50
Figura 43. Ping desde SWT1 (VLAN99) a PC1 (VLAN10), PC2 (VLAN20) y PC3 (VLAN30).....	51
Figura 44. Ping desde SWT2 (VLAN99) a PC4 (VLAN10), PC5 (VLAN20) y PC6 (VLAN30).....	51
Figura 45. Ping desde SWT3 (VLAN99) a PC7 (VLAN10), PC8 (VLAN20) y PC9 (VLAN30).....	52

## LISTA DE TABLAS

pág.

Tabla 1. Direccionamiento Escenario 1.....	13
Tabla 2. Direccionamiento Escenario 2.....	23
Tabla 3. Asociación VLAN e IP ** X = número de cada PC en la topología .....	42
Tabla 4. Direccionamiento de los PC .....	42
Tabla 5. Direccionamiento SVI VLAN 99 .....	44



## GLOSARIO

**CCNP (Cisco Certified Network Professional):** Es un nivel intermedio de certificación de la compañía .3 Para obtener esta certificación, se han de superar varios exámenes, clasificados según la empresa en 3 módulos. Esta certificación, es la intermedia de las certificaciones generales de Cisco, no está tan valorada como el CCIE, pero sí, mucho más que el CCNA.

**Packet Tracer:** Es un simulador gráfico de red que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos. Este software es proporcionado por la plataforma *NetAcad* de *Cisco Systems*, lo que permite que esté estrechamente relacionado con este diplomado.

**Networking:** Es una red de computadoras, también llamada red de ordenadores, red de comunicaciones de datos o red informática conjunto de equipos informáticos y software reconectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

**Protocolos de red:** Conjunto de normas standard que especifican el método para enviar y recibir datos entre varios ordenadores. Es una convención que controla o permite la conexión, comunicación, y transferencia de datos entre dos puntos finales.

**VLAN:** 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 propone de manera práctica la solución a tres escenarios que involucran configuración de dispositivos Cisco. Durante su desarrollo se describe la forma de implementar las características necesarias de cada equipo para cumplir con el propósito planteado.

Principalmente se abordan dos temas fundamentales en el ejercicio de la configuración de redes, por una parte, se implementan protocolos de enrutamiento dinámico, entre ellos OSPF, EIGRP y BGP, estos permiten lograr comunicación entre diferentes subredes de manera controlada y segura, descubriendo rutas automáticamente y optimizando el flujo de datos en la red, el principio de funcionamiento de estos tres protocolos es similar, pero los separan ciertas características que dependerán de la necesidad que se quiera solventar.

Por otro lado, se implementa otra técnica muy común en el presente, y es la configuración de VLAN en un switch, esta permite segmentar y controlar el tráfico de una red, sea para dividir áreas determinadas o como método de seguridad.

Palabras Clave: CCNP, CISCO, NETWORKING, TELECOMUNICACIONES, ENRUTAMIENTO, VLAN, SWITCH, ROUTER, PROTOCOLOS.

## INTRODUCCIÓN

El siguiente informe hace parte de la evaluación final del diplomado de profundización Cisco CCNP, en este se ponen a prueba de manera práctica los conocimientos y habilidades que se obtuvieron durante el desarrollo de cada unidad, abordando contenidos referentes a la implementación de VLAN y Protocolos de enrutamiento.

El objetivo principal, es dar solución a las necesidades de tres escenarios preconcebidos por medio del diseño y configuración de una red y sus respectivas configuraciones.

La metodología se basa en el montaje y configuración de cada escenario de manera simulada haciendo uso del software Packet Tracer, el cual permite realizar y visualizar las conexiones físicas y ejecutar comandos como en cualquier sistema IOS de Cisco Systems.

Se documentó un paso a paso que describe cada procedimiento y los respectivos comandos necesarios para su realización.

Cada comando para activar y administrar estas características se muestra a continuación, junto a su sintaxis general y el modo de configuración en el que tiene que ser ejecutado para implementar en otros escenarios similares.

# 1. DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

## 1.1. ESCENARIO 1

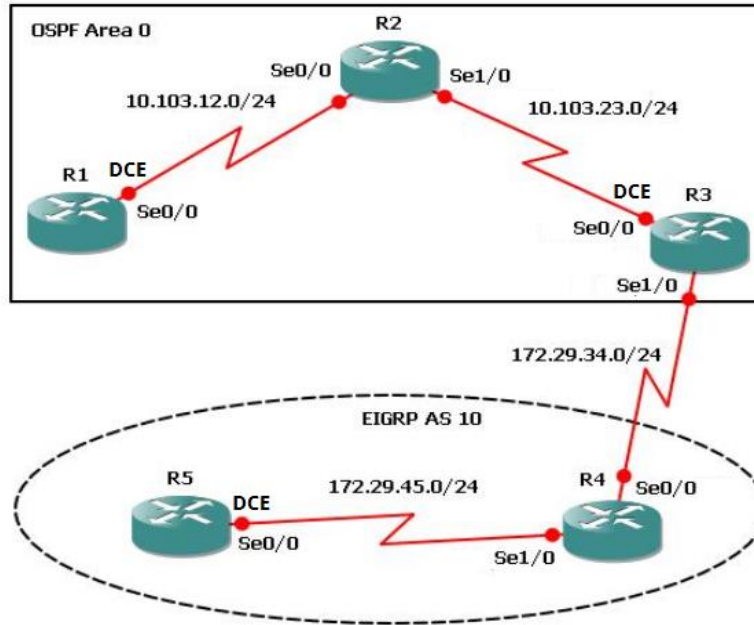


Figura 1. Descripción gráfica de la topología del escenario 1.

### 1.1.1. Configuración inicial

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

#### 1.1.1.1. Direccionamiento

La siguiente tabla muestra el consolidado de direccionamiento y su asociación a cada interfaz física de los dispositivos.

Dispositivo	Interfaz	Dirección IP	Mascara de Red
R1	Serial 0/0 (DCE)	10.103.12.1	255.255.255.0
R2	Serial 0/0	10.103.12.2	255.255.255.0
	Serial 1/0	10.103.23.1	255.255.255.0
R3	Serial 0/0 (DCE)	10.103.23.2	255.255.255.0

	Serial 1/0	172.29.34.1	255.255.255.0
R4	Serial 0/0	172.29.34.2	255.255.255.0
	Serial 1/0	172.29.45.1	255.255.255.0
R5	Serial 0/0 (DCE)	172.29.45.2	255.255.255.0

Tabla 1. Direccionamiento Escenario 1

Con los datos de la tabla anterior se realiza la configuración de cada una de las interfaces de los routers, la sintaxis para la configuración del nombre del host y la configuración y activación de interfaces es la siguiente:

**Nota:** Se ejecutan los comandos en el modo *exec privilegiado (Router#)*

```
configure terminal
hostname <nombre del router>
interface <nombre y número de la interface>
ip address <dirección ip> < mascara>
no shutdown
```

Adicionalmente en las interfaces señaladas como DCE se ejecuta el comando:

```
clock rate <velocidad del reloj>
```

## R1

```
configure terminal
hostname R1
no ip domain-lookup
interface Serial 0/0/0
ip address 10.103.12.1 255.255.255.0
clock rate 128000
no shutdown
```

## R2

```
configure terminal
hostname R2
no ip domain-lookup
interface Serial 0/0/0
ip address 10.103.12.2 255.255.255.0
no shutdown
```

```
interface Serial 0/1/0
ip address 10.103.23.1 255.255.255.0
no shutdown
```

### **R3**

```
configure terminal
hostname R3
no ip domain-lookup
interface Serial 0/0/0
ip address 10.103.23.2 255.255.255.0
clock rate 128000
no shutdown
interface Serial 0/1/0
ip address 172.29.34.1 255.255.255.0
no shutdown
```

### **R4**

```
configure terminal
hostname R4
no ip domain-lookup
interface Serial 0/0/0
ip address 172.29.34.2 255.255.255.0
no shutdown
interface Serial 0/1/0
ip address 172.29.45.1 255.255.255.0
no shutdown
```

### **R5**

```
configure terminal
hostname R5
no ip domain-lookup
interface Serial 0/0/0
ip address 172.29.45.2 255.255.255.0
```

```
clock rate 128000
```

```
no shutdown
```

### 1.1.1.2. Prueba de conectividad

Para comprobar la correcta configuración y activación de las interfaces se realiza una prueba de ping en dirección a la IP de las interfaces vecinas de cada router. Es suficiente si se realiza de manera exitosa desde alguno de los dos lados del enlace.

```
R1#ping 10.103.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.103.12.2, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/6
ms
R1#
```

*Figura 2. Ping interfaz vecina R1*

```
R2#ping 10.103.23.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.103.23.2, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/5
ms
R2#
```

*Figura 3. Ping interfaz vecina R2*

```
R3#ping 172.29.34.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.34.2, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/5
ms
R3#
```

*Figura 4. Ping interfaz vecina R3*

```

R4#
%SYS-5-CONFIG_I: Configured from console by console
ping 172.29.45.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.45.2, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/5
ms
R4#

```

Figura 5. Ping interfaz vecina R4

```

R5#ping 172.29.45.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.45.1, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/6
ms
R5#

```

Figura 6. Ping interfaz vecina R5

### 1.1.2. Enrutamiento

Luego de que las pruebas de enlace sean exitosas se configuran los protocolos de enrutamiento señalados en la topología, se sigue la siguiente sintaxis para la configuración del protocolo indicado:

Nota: Se ejecutan los comandos en el modo *global configuration (Router(config)#)*

#### 1.1.2.1. OSPF

```
router ospf <id del proceso>
```

```
network <ip de la red conectada> < mascara wildcard> área <número de área>
```

#### R1

```
router ospf 1
```

```
network 10.103.12.0 0.0.0.255 area 0
```

#### R2

```
router ospf 1
```

```
network 10.103.12.0 0.0.0.255 area 0
```

```
network 10.103.23.0 0.0.0.255 area 0
```



### R3

```
router ospf 1
network 10.103.23.0 0.0.0.255 area 0
```

### 1.1.2.2. EIGRP

```
router eigrp <número de AS>
network <ip de la red conectada> < mascara wildcard>
```

### R3

```
router eigrp 10
network 172.29.34.0 0.0.0.255
```

### R4

```
router eigrp 10
network 172.29.34.0 0.0.0.255
network 172.29.45.0 0.0.0.255
```

### R5

```
router eigrp 10
network 172.29.45.0 0.0.0.255
```

### 1.1.2.3. Interfaces Loopback en OSPF

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.

La sintaxis para la configuración de interfaces *loopback* es la siguiente:

```
interface lo <número de interfaz loopback>
ip address <dirección ip>
```

**Nota:** Se ejecutan los comandos en el modo *global configuration (Router(config)#)*

## R1

```
interface Lo 0
ip address 10.1.0.1 255.255.252.0
interface Lo 1
ip address 10.1.4.1 255.255.252.0
interface Lo 2
ip address 10.1.8.1 255.255.252.0
interface Lo 3
ip address 10.1.12.1 255.255.252.0
exit
router ospf 1
network 10.1.0.0 0.0.3.255 area 0
network 10.1.4.0 0.0.3.255 area 0
network 10.1.8.0 0.0.3.255 area 0
network 10.1.12.0 0.0.3.255 area 0
```

### 1.1.2.4. Interfaces *Loopback* en EIGRP

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.

Nota: Se ejecutan los comandos en el modo *global configuration (Router(config)#)*

## R5

```
interface Lo 0
ip address 172.5.0.1 255.255.252.0
interface Lo 1
ip address 172.5.4.1 255.255.252.0
interface Lo 2
ip address 172.5.8.1 255.255.252.0
interface Lo 3
ip address 172.5.12.1 255.255.252.0
exit
```

```

router eigrp 10

network 172.5.0.1 0.0.3.255

network 172.5.4.1 0.0.3.255

network 172.5.8.1 0.0.3.255

network 172.5.12.1 0.0.3.255

```

### 1.1.3. Análisis de enrutamiento

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 marcan en rojo las rutas a las interfaces *loopback* aprendidas por OSPF mientras que las aprendidas por EIGRP se marcan en azul.

```

R3#sh 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

    10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
O•   10.1.0.1/32 [110/129] via 10.103.23.1, 00:10:26, Serial0/0/0
O•   10.1.4.1/32 [110/129] via 10.103.23.1, 00:10:26, Serial0/0/0
O•   10.1.8.1/32 [110/129] via 10.103.23.1, 00:10:26, Serial0/0/0
O•   10.1.12.1/32 [110/129] via 10.103.23.1, 00:10:26, Serial0/0/0
O    10.103.12.0/24 [110/128] via 10.103.23.1, 00:25:39, Serial0/0/0
C    10.103.23.0/24 is directly connected, Serial0/0/0
L    10.103.23.2/32 is directly connected, Serial0/0/0
    172.5.0.0/22 is subnetted, 4 subnets
D•   172.5.0.0/22 [90/2809856] via 172.29.34.2, 00:01:02, Serial0/1/0
D•   172.5.4.0/22 [90/2809856] via 172.29.34.2, 00:01:02, Serial0/1/0
D•   172.5.8.0/22 [90/2809856] via 172.29.34.2, 00:01:02, Serial0/1/0
D•   172.5.12.0/22 [90/2809856] via 172.29.34.2, 00:01:02, Serial0/1/0
    172.29.0.0/16 is variably subnetted, 3 subnets, 2 masks
C    172.29.34.0/24 is directly connected, Serial0/1/0
L    172.29.34.1/32 is directly connected, Serial0/1/0
D    172.29.45.0/24 [90/2681856] via 172.29.34.2, 00:25:27, Serial0/1/0

R3#

```

Figura 7. Rutas aprendidas en R3

#### 1.1.4. Redistribución de rutas

##### 1.1.4.1. Configuración

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.

Para redistribución de EIGRP en OSPF se utiliza la siguiente estructura de comando:

```
router ospf <id proceso>
redistribute eigrp <número as> metric <valor costo> subnets
```

Y para redistribución de OSPF en EIGRP se digita el comando con los siguientes parámetros:

```
Router eigrp <número as>
Redistribute ospf <id proceso> metric <BW en Kbits/seg> <confiabilidad 0-255> <BW Efectivo 1-255> <MTU de la ruta>
```

**Nota:** Se ejecutan los comandos en el modo *global configuration (Router(config)#)*

### R3

```
router ospf 1
redistribute eigrp 10 metric 50000 subnets
exit
router eigrp 10
redistribute ospf 1 metric 1544 2000 255 1 1500
```

##### 1.1.4.2. Verificación

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

Se señalan en color rojo las rutas EIGRP redistribuidas por OSPF que el router 1 ha aprendido y con color azul las rutas OSPF redistribuidas por EIGRP que el router 5 ha aprendido, confirmando la correcta distribución de rutas entre protocolos.

R1

```
R1#sh 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

    10.0.0.0/8 is variably subnetted, 11 subnets, 3 masks
C       10.1.0.0/22 is directly connected, Loopback0
L       10.1.0.1/32 is directly connected, Loopback0
C       10.1.4.0/22 is directly connected, Loopback1
L       10.1.4.1/32 is directly connected, Loopback1
C       10.1.8.0/22 is directly connected, Loopback2
L       10.1.8.1/32 is directly connected, Loopback2
C       10.1.12.0/22 is directly connected, Loopback3
L       10.1.12.1/32 is directly connected, Loopback3
C       10.103.12.0/24 is directly connected, Serial0/0/0
L       10.103.12.1/32 is directly connected, Serial0/0/0
O       10.103.23.0/24 [110/128] via 10.103.12.2, 01:40:35, Serial0/0/0
    172.5.0.0/22 is subnetted, 4 subnets
O E2*   172.5.0.0/22 [110/50000] via 10.103.12.2, 00:10:29, Serial0/0/0
O E2*   172.5.4.0/22 [110/50000] via 10.103.12.2, 00:10:29, Serial0/0/0
O E2*   172.5.8.0/22 [110/50000] via 10.103.12.2, 00:10:29, Serial0/0/0
O E2*   172.5.12.0/22 [110/50000] via 10.103.12.2, 00:10:29, Serial0/0/0
    172.29.0.0/24 is subnetted, 2 subnets
O E2*   172.29.34.0/24 [110/50000] via 10.103.12.2, 00:10:29, Serial0/0/0
O E2*   172.29.45.0/24 [110/50000] via 10.103.12.2, 00:10:29, Serial0/0/0

R1#
```

Figura 8. Rutas aprendidas en R1 por redistribución

R5

```
R5#sh 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

    10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
D EX*   10.1.0.1/32 [170/3193856] via 172.29.45.1, 00:04:49, Serial0/0/0
D EX*   10.1.4.1/32 [170/3193856] via 172.29.45.1, 00:04:49, Serial0/0/0
D EX*   10.1.8.1/32 [170/3193856] via 172.29.45.1, 00:04:49, Serial0/0/0
D EX*   10.1.12.1/32 [170/3193856] via 172.29.45.1, 00:04:49, Serial0/0/0
D EX*   10.103.12.0/24 [170/3193856] via 172.29.45.1, 00:04:49, Serial0/0/0
D EX*   10.103.23.0/24 [170/3193856] via 172.29.45.1, 00:04:49, Serial0/0/0
    172.5.0.0/16 is variably subnetted, 8 subnets, 2 masks
C       172.5.0.0/22 is directly connected, Loopback0
L       172.5.0.1/32 is directly connected, Loopback0
C       172.5.4.0/22 is directly connected, Loopback1
L       172.5.4.1/32 is directly connected, Loopback1
C       172.5.8.0/22 is directly connected, Loopback2
L       172.5.8.1/32 is directly connected, Loopback2
C       172.5.12.0/22 is directly connected, Loopback3
L       172.5.12.1/32 is directly connected, Loopback3
    172.29.0.0/16 is variably subnetted, 3 subnets, 2 masks
D       172.29.34.0/24 [90/2681856] via 172.29.45.1, 01:41:34, Serial0/0/0
C       172.29.45.0/24 is directly connected, Serial0/0/0
L       172.29.45.2/32 is directly connected, Serial0/0/0

R5#
```

Figura 9. Rutas aprendidas en R5 por redistribución

## 1.2. ESCENARIO 2

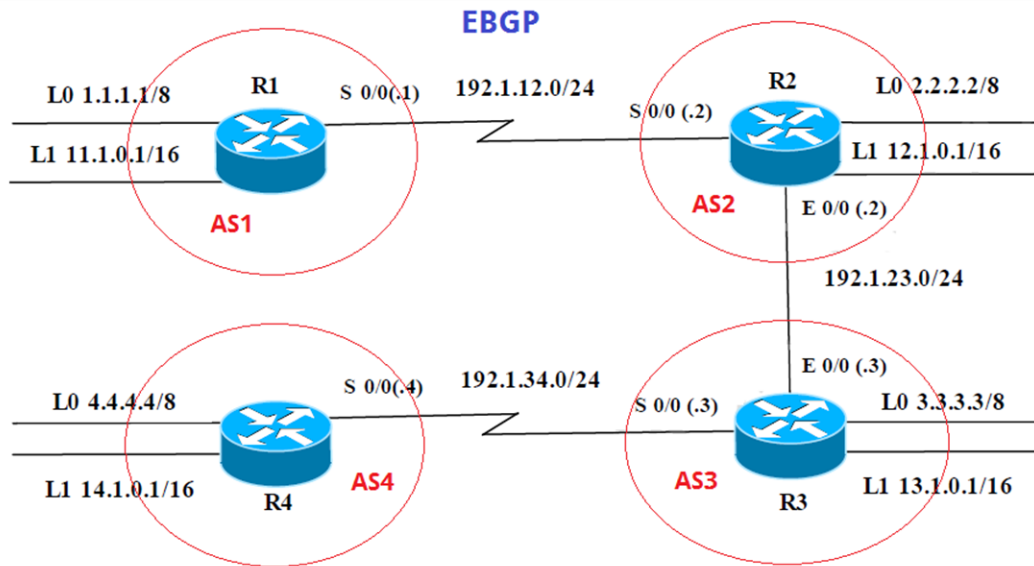


Figura 10. Descripción gráfica de la topología del escenario 2.

### 1.2.1. Configuración inicial

R1	Interfaz	Dirección IP	Máscara
	<b>Loopback 0</b>	1.1.1.1	255.0.0.0
	<b>Loopback 1</b>	11.1.0.1	255.255.0.0
	<b>S 0/0</b>	192.1.12.1	255.255.255.0
R2	Interfaz	Dirección IP	Máscara
	<b>Loopback 0</b>	2.2.2.2	255.0.0.0
	<b>Loopback 1</b>	12.1.0.1	255.255.0.0
	<b>S 0/0</b>	192.1.12.2	255.255.255.0
	<b>E 0/0</b>	192.1.23.2	255.255.255.0
R3	Interfaz	Dirección IP	Máscara
	<b>Loopback 0</b>	3.3.3.3	255.0.0.0
	<b>Loopback 1</b>	13.1.0.1	255.255.0.0
	<b>E 0/0</b>	192.1.23.3	255.255.255.0
	<b>S 0/0</b>	192.1.34.3	255.255.255.0

R4	Interfaz	Dirección IP	Máscara
	<b>Loopback 0</b>	4.4.4.4	255.0.0.0
	<b>Loopback 1</b>	14.1.0.1	255.255.0.0
	<b>S 0/0</b>	192.1.34.4	255.255.255.0

Tabla 2. Direccionamiento Escenario 2

Se configuran el nombre del dispositivo y se configuran y activan las interfaces con las direcciones asociadas a la tabla anterior siguiendo la misma sintaxis del escenario anterior.

Nota: Se ejecutan los comandos en el modo *global configuration (Router(config)#)*

## R1

```
hostname R1
no ip domain-lookup
interface loopback 0
ip address 1.1.1.1 255.0.0.0
interface loopback 1
ip address 11.1.0.1 255.255.0.0
interface Serial 1/0/0
ip address 192.1.12.1 255.255.255.0
no shutdown
```

## R2

```
hostname R2
no ip domain-lookup
interface loopback 0
ip address 2.2.2.2 255.0.0.0
interface loopback 1
ip address 12.1.0.1 255.255.0.0
interface Serial 1/0/0
```

```
ip address 192.1.12.2 255.255.255.0
no shutdown
interface fastethernet 0/0
ip address 192.1.23.2 255.255.255.0
no shutdown
```

### **R3**

```
hostname R3
no ip domain-lookup
interface loopback 0
ip address 3.3.3.3 255.0.0.0
interface loopback 1
ip address 13.1.0.1 255.255.0.0
interface Serial 1/0/0
ip address 192.1.34.3 255.255.255.0
no shutdown
interface fastethernet 0/0
ip address 192.1.23.3 255.255.255.0
no shutdown
```

### **R4**

```
hostname R4
no ip domain-lookup
interface loopback 0
ip address 4.4.4.4 255.0.0.0
interface loopback 1
ip address 14.1.0.1 255.255.0.0
interface Serial 1/0/0
ip address 192.1.34.4 255.255.255.0
no shutdown
```



### 1.2.1.1. Comprobación de conectividad

Se realiza la comprobación de conectividad con un ping a la IP del router vecino, si es exitoso se demuestra que la configuración fue correcta:

```
R1#ping 192.1.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.12.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/9 ms
R1#
```

*Figura 11. Ping interfaz vecina R1*

```
R2#ping 192.1.23.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.23.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/3 ms
R2#
```

*Figura 12. Ping interfaz vecina R2*

```
R3#ping 192.1.34.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.34.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms
R3#
```

*Figura 13. Ping interfaz vecina R3*

```
R4#ping 192.1.34.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.1.34.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/6 ms
R4#
```

*Figura 14. Ping interfaz vecina R4*

## 1.2.2. Enrutamiento BGP

### 1.2.2.1. Sintaxis

La sintaxis para establecer una relación de vecinos BGP y anunciar las redes conectadas es la siguiente:

```
router bgp <numero de AS>
bgp router-id <número de ID>
network <dirección red conectada> mask < mascara de subred>
neighbor <dirección del vecino> remote-as <número de as vecino>
```

**Nota:** Se ejecutan los comandos en el modo *global configuration (Router(config)#)*

### 1.2.2.2. R1 y R2

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*.

#### R1

```
router bgp 1
bgp router-id 11.11.11.11
network 192.1.12.0 mask 255.255.255.0
network 1.0.0.0 mask 255.0.0.0
network 11.1.0.0 mask 255.255.0.0
neighbor 192.1.12.2 remote-as 2
```

#### R2

```
router bgp 2
bgp router-id 22.22.22.22
network 192.1.12.0 mask 255.255.255.0
network 2.0.0.0 mask 255.0.0.0
network 12.1.0.0 mask 255.255.0.0
neighbor 192.1.12.1 remote-as 1
```

Ambos routers muestran de manera correcta una notificación de que la relación de vecinos entre R1 y R2 se estableció correctamente.

```
R1(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.12.2 Up
R2(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.12.1 Up
```

Figura 15. Confirmación de vecindad entre R1 y R2

### 1.2.2.3. Verificación de BGP

Se ejecuta el comando *show ip route* para verificar las rutas BGP aprendidas, están señaladas en color azul.

```
R1#sh ip route
Codes: C - connected, S - static, I - IGRP, 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

C    1.0.0.0/8 is directly connected, Loopback0
B    2.0.0.0/8 [20/0] via 192.1.12.2, 00:00:00
     11.0.0.0/16 is subnetted, 1 subnets
C    11.1.0.0 is directly connected, Loopback1
     12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 192.1.12.2, 00:00:00
C    192.1.12.0/24 is directly connected, Serial11/0/0

R1#
R1#
```

Figura 16. Verificación rutas BGP en R1

```

R2#sh ip route
Codes: C - connected, S - static, I - IGRP, 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
C 2.0.0.0/8 is directly connected, Loopback0
  11.0.0.0/16 is subnetted, 1 subnets
B 11.1.0.0 [20/0] via 192.1.12.1, 00:00:00
  12.0.0.0/16 is subnetted, 1 subnets
C 12.1.0.0 is directly connected, Loopback1
C 192.1.12.0/24 is directly connected, Serial1/0/0
C 192.1.23.0/24 is directly connected, FastEthernet0/0

R2#

```

Figura 17. Verificación rutas BGP en R2

#### 1.2.2.4. R2 y R3

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**.

Nota: Se ejecutan los comandos en el modo *global configuration (Router(config)#)*

#### R2

```

router bgp 2
network 192.1.23.0 mask 255.255.255.0
neighbor 192.1.23.3 remote-as 3

```

#### R3

```

router bgp 3
bgp router-id 33.33.33.33
network 192.1.23.0 mask 255.255.255.0

```

```

network 3.0.0.0 mask 255.0.0.0
network 13.1.0.0 mask 255.255.0.0
neighbor 192.1.23.2 remote-as 2

```

Ambos routers muestran de manera correcta una notificación de que la relación de vecinos entre R2 y R3 se estableció correctamente.

```

R2(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.23.3 Up
R3(config-router)#%BGP-5-ADJCHANGE: neighbor 192.1.23.2 Up

```

Figura 18. Confirmación de vecindad entre R2 y R3

#### 1.2.2.5. Verificación de BGP

Se ejecuta el comando `show ip route` para verificar las rutas BGP aprendidas de esta relación que están señaladas en color verde.

R2

```

R2#sh ip route
Codes: C - connected, S - static, I - IGRP, 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
C    2.0.0.0/8 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 [20/0] via 192.1.12.1, 00:00:00
     12.0.0.0/16 is subnetted, 1 subnets
C    12.1.0.0 is directly connected, Loopback1
     13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0 [20/0] via 192.1.23.3, 00:00:00
C    192.1.12.0/24 is directly connected, Serial1/0/0
C    192.1.23.0/24 is directly connected, FastEthernet0/0

R2#

```

Figura 19. Verificación rutas BGP en R2

## R3

```
R3#sh ip route
Codes: C - connected, S - static, I - IGRP, 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
C 3.0.0.0/8 is directly connected, Loopback0
  11.0.0.0/16 is subnetted, 1 subnets
B 11.1.0.0 [20/0] via 192.1.23.2, 00:00:00
  12.0.0.0/16 is subnetted, 1 subnets
B 12.1.0.0 [20/0] via 192.1.23.2, 00:00:00
  13.0.0.0/16 is subnetted, 1 subnets
C 13.1.0.0 is directly connected, Loopback1
B 192.1.12.0/24 [20/0] via 192.1.23.2, 00:00:00
C 192.1.23.0/24 is directly connected, FastEthernet0/0
C 192.1.34.0/24 is directly connected, Serial1/0/0

R3#
```

Figura 20. Verificación rutas BGP en R3

### 1.2.2.6. R3 y R4

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*.

Nota: Se ejecutan los comandos en el modo *global configuration (Router(config)#)*

## R3

```
router bgp 3
network 192.1.34.0 mask 255.255.255.0
neighbor 192.168.34.4 remote-as 4
```

## R4

```
router bgp 4
bgp router-id 44.44.44.44
network 4.4.4.4 mask 255.255.0.0
network 14.1.0.0 mask 255.255.0.0
network 192.1.34.0 mask 255.255.255.0
neighbor 192.168.34.3 remote-as 3
exit
```

Ambos routers muestran de manera correcta una notificación de que la relación de vecinos entre R3 y R4 se estableció correctamente, para el caso de R4 lo hace desde la ruta estática hacia la red 3.0.0.0.

```
R3#%BGP-5-ADJCHANGE: neighbor 192.1.34.4 Up
R4#%BGP-5-ADJCHANGE: neighbor 192.1.34.3 Up
```

Figura 21. Confirmación de vecindad entre R3 y R4

### 1.2.2.7. Verificación BGP

Se ejecuta el comando *show ip route* para verificar las rutas BGP aprendidas de esta relación que están señaladas en color rojo, demostrando la correcta detección de rutas de extremo a extremo.

## R3

```
R3#sh ip rou
Codes: C - connected, S - static, I - IGRP, 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
C    3.0.0.0/8 is directly connected, Loopback0
B    4.0.0.0/8 [20/0] via 192.1.34.4, 00:00:00
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.23.2, 00:00:00
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.23.2, 00:00:00
     13.0.0.0/16 is subnetted, 1 subnets
C       13.1.0.0 is directly connected, Loopback1
     14.0.0.0/16 is subnetted, 1 subnets
B       14.1.0.0 [20/0] via 192.1.34.4, 00:00:00
B    192.1.12.0/24 [20/0] via 192.1.23.2, 00:00:00
C    192.1.23.0/24 is directly connected, FastEthernet0/0
C    192.1.34.0/24 is directly connected, Serial1/0/0

R3#
```

Figura 22. Verificación rutas BGP en R3

## R4

```
R4#sh ip route
Codes: C - connected, S - static, I - IGRP, 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
C    4.0.0.0/8 is directly connected, Loopback0
     11.0.0.0/16 is subnetted, 1 subnets
B       11.1.0.0 [20/0] via 192.1.34.3, 00:00:00
     12.0.0.0/16 is subnetted, 1 subnets
B       12.1.0.0 [20/0] via 192.1.34.3, 00:00:00
     13.0.0.0/16 is subnetted, 1 subnets
B       13.1.0.0 [20/0] via 192.1.34.3, 00:00:00
     14.0.0.0/16 is subnetted, 1 subnets
C       14.1.0.0 is directly connected, Loopback1
B    192.1.12.0/24 [20/0] via 192.1.34.3, 00:00:00
B    192.1.23.0/24 [20/0] via 192.1.34.3, 00:00:00
C    192.1.34.0/24 is directly connected, Serial1/0/0

R4#
```

Figura 23. Verificación rutas BGP en R4



### 1.3. ESCENARIO 3

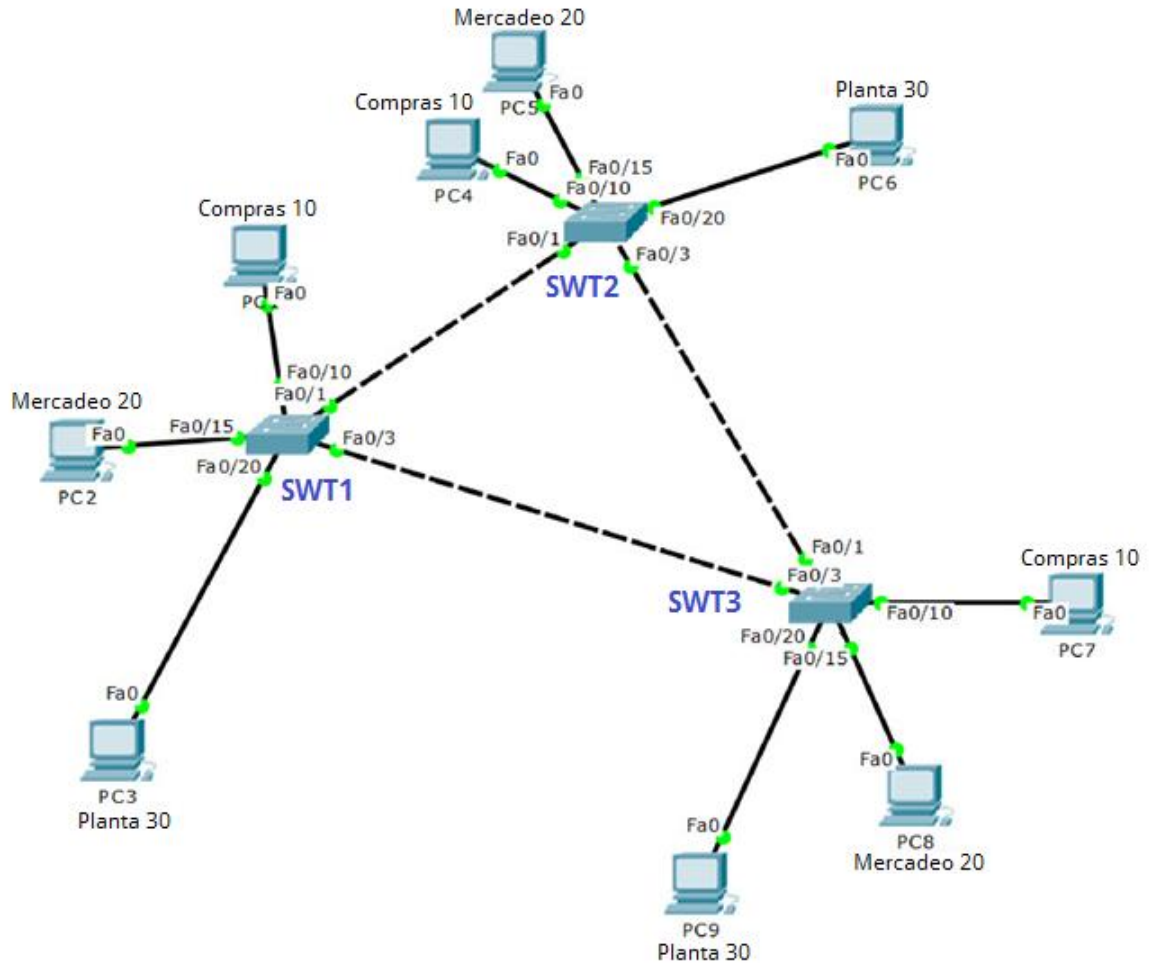


Figura 24. Topología Escenario 3

#### 1.3.1. Configuración VTP

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

### 1.3.1.1. Sintaxis

La sintaxis de los comandos para con configuración de los parámetros VTP es la siguiente:

```
vtp mode <rol vtp>
vtp domain <nombre del dominio vtp>
vtp password <contraseña del dominio>
```

**Nota:** Se ejecutan los comandos en el modo *global configuration (Router(config)#)*

#### SWT1

```
hostname SWT1
vtp mode client
vtp domain CCNP
vtp password cisco
```

#### SWT2

```
hostname SWT2
vtp mode server
vtp domain CCNP
vtp password cisco
```

#### SWT3

```
hostname SWT3
vtp mode client
vtp domain CCNP
vtp password cisco
```

### 1.3.1.2. Verificación

Se ejecuta el comando *show vtp status* y se verifica el modo de operación, el nombre del dominio y la existencia de la contraseña en cada uno de los switch.

## SWT1

```
SWT1#sh vtp sta
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 25. Verificación modo de operación SWT1

## SWT2

```
SWT2#sh vtp sta
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 26. Verificación modo de operación SWT2

## SWT3

```
SWT3#sh vtp sta
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 27. Verificación modo de operación SWT3

### 1.3.2. Configurar DTP (Dynamic Trunking Protocol)

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*.

Para cambiar el modo a *dynamic desirable* en uno de los lados del enlace SWT1/SWT2 se elige la interfaz *Fast Ethernet 0/1* de SWT1. Se ejecutan los siguientes comandos desde el modo de *configuración global*.

```
interface FastEthernet0/1
switchport mode dynamic desirable
```

#### 1.3.2.1. Verificación DTP

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

SWT1

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

Port      Vlans allowed on trunk
Fa0/1     1-1005

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

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

SWT1#
```

Figura 28. Verificación DTP en F0/1 de SWT1

La configuración tuvo efecto en Fa0/1 y ahora está establecida como *desiderable*.

## SWT2

```
SWT2#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
```

Figura 29. Verificación modo troncal en F0/1 de SWT2

Como SWT1 configuró F0/1 en modo troncal SWT2 de manera automática pone su F0/1 como troncal.

### 1.3.3. Configuración troncal estática

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

Se ejecutan los siguientes comandos en el modo *configuración global*:

#### SWT1

```
interface fastethernet 0/3
switchport mode trunk
```

### 1.3.3.1. Verificación troncal estática

Se verifica el enlace "*trunk*" el comando *show interfaces trunk* en SWT1.

```
SWT1#sh int 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     none

SWT1#
```

Figura 30.. Verificación modo troncal de F0/3 en SWT1

La interfaz F0/3 de SWT1 se muestra como *on* al establecerla explícitamente como una interfaz troncal.

### 1.3.4. Configuración troncal permanente

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

Para establecer un enlace troncal permanente se deben instaurar las interfaces F0/3 de SWT2 y F0/1 de SWT 3 como enlaces troncales explícitamente, para ello se utilizan los siguientes comandos desde el modo *configuración global*:

#### SW2

```
interface fastethernet 0/3
```

```
switchport mode trunk
```

#### SW3

```
interface fastethernet 0/1
```

```
switchport mode trunk
```

### 1.3.4.1. Verificación enlace troncal permanente

Como comprobación de la correcta configuración se emite el comando *show interface trunk* y se verifica que se reflejen los cambios deseados.

SWT2

```
SWT2#sh 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     1

SWT2#
```

Figura 31.. Verificación modo troncal permanente en F0/3 de SWT2

SWT3

```
SWT3#sh 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     none
Fa0/3     none

SWT3#
```

Figura 32. Verificación modo troncal permanente en F0/1 de SWT3

### 1.3.5. Agregar VLANs

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

Al intentar agregar alguna VLAN en SWT1 restringe su creación debido al modo cliente VTP en el que está configurado, entonces basta con crearlas en SWT2 y automáticamente se agregaran en los otros dos switch.

Nota: Se ejecutan los comandos en el modo *global configuration (Router(config)#)*

#### SWT2

```
vlan 10
name Compras
vlan 20
name Mercadeo
vlan 30
name Planta
```

#### 1.3.5.1. Verificación de que las VLAN se agregaron correctamente.

Se comprueba en los tres switch emitiendo el comando *show vlan brief*, se evidencia que los clientes (SWT1 y SWT3) recibieron la configuración de la *vlan* desde el servidor (SW2). Se resaltan en color rojo en los resultados.

#### SWT1

```
SWT1#sh vlan bri
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
1002 fddi-default         active
1003 token-ring-default  active
1004 fddinet-default     active
1005 trnet-default       active
SWT1#
```

Figura 33. Verificación VLANS en SWT1



## SWT2

```
SWT2#sh vlan bri
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
1002 fddi-default           active
1003 token-ring-default     active
1004 fddinet-default        active
1005 trnet-default          active
SWT2#
```

Figura 34. Verificación VLANS en SWT2

## SWT3

```
SWT3#sh vlan bri
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
1002 fddi-default           active
1003 token-ring-default     active
1004 fddinet-default        active
1005 trnet-default          active
SWT3#
```

Figura 35. Verificación VLANS en SWT3

### 1.3.6. Configuración de direccionamiento

Se asocian los puertos a las VLAN y se configuran las direcciones IP de acuerdo con la siguiente tabla.

Interfaz	VLAN	Direcciones IP de los PC
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

Tabla 3. Asociación VLAN e IP \*\* X = número de cada PC en la topología

El direccionamiento de los PC se configura directamente en la NIC de cada uno y se realiza de acuerdo con la siguiente tabla:

Grupo	Nombre PC	IP	Mascara
SWT1	PC1	190.108.10.1	255.255.255.0
	PC2	190.108.20.2	255.255.255.0
	PC3	190.108.30.3	255.255.255.0
SWT2	PC4	190.108.10.4	255.255.255.0
	PC5	190.108.20.5	255.255.255.0
	PC6	190.108.30.6	255.255.255.0
SWT3	PC7	190.108.10.7	255.255.255.0
	PC8	190.108.20.8	255.255.255.0
	PC9	190.108.30.9	255.255.255.0

Tabla 4. Direccionamiento de los PC

### 1.3.7. Asignación de puertos a las VLAN

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

Se emiten los siguientes comandos desde el modo de *configuración global*:

### SWT1

```
interface fastethernet 0/10
switchport mode access
switchport access vlan 10
```

### SWT 2

```
interface fastethernet 0/10
switchport mode access
switchport access vlan 10
```

### SWT3

```
interface fastethernet 0/10
switchport mode access
switchport access vlan 10
```

Se repite el procedimiento para los puertos F0/15 y F0/20 en SWT1, SWT2 y SWT3. Se asigna las VLAN y las direcciones IP de los PC de acuerdo con la tabla 3 y 4.

### SWT1

```
interface fastethernet 0/15
switchport mode access
switchport access vlan 20
interface fastethernet 0/20
switchport mode access
switchport access vlan 30
```

### SWT 2

```
interface fastethernet 0/15
switchport mode access
switchport access vlan 20
interface fastethernet 0/20
```

```
switchport mode access
switchport access vlan 30
```

### SWT3

```
interface fastethernet 0/15
switchport mode access
switchport access vlan 20
interface fastethernet 0/20
switchport mode access
switchport access vlan 30
```

#### 1.3.8. Configuración de las direcciones IP en los Switch.

En cada uno de los Switch se asigna 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

Tabla 5. Direccionamiento SVI VLAN 99

Se emiten los siguientes comandos desde el modo *configuración global* para configurar la IP de cada SVI para la VLAN 99, la VLAN 99 solo es necesario crearla en la SWT2 y automáticamente se creará en SWT1 y SWT3 por estar en modo cliente.

### SWT 1

```
interface VLAN 99
ip address 190.108.99.1 255.255.255.0
no shutdown
```

## SWT 2

```
vlan 99  
  
interface VLAN 99  
  
ip address 190.108.99.2 255.255.255.0  
  
no shutdown
```

## SWT 3

```
interface VLAN 99  
  
ip address 190.108.99.3 255.255.255.0  
  
no shutdown
```

### 1.3.8.1. Verificación de direccionamiento de la VLAN 99

Se emite el comando *show vlan brief* para verificar la creación y difusión de la VLAN 99.

```
SWT3#sh vlan bri  
  
VLAN Name                Status    Ports  
-----  
1    default                active    Fa0/2, Fa0/4, Fa0/5, Fa0/6  
                                           Fa0/7, Fa0/8, Fa0/9, Fa0/11  
                                           Fa0/12, Fa0/13, Fa0/14, Fa0/16  
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/21  
                                           Fa0/22, Fa0/23, Fa0/24, Gig0/1  
                                           Gig0/2  
10   Compras                active    Fa0/10  
20   Mercadeo              active    Fa0/15  
30   Planta                active    Fa0/20  
99   VLAN0099              active  
1002 fddi-default          active  
1003 token-ring-default  active  
1004 fddinet-default     active  
1005 trnet-default       active  
SWT3#
```

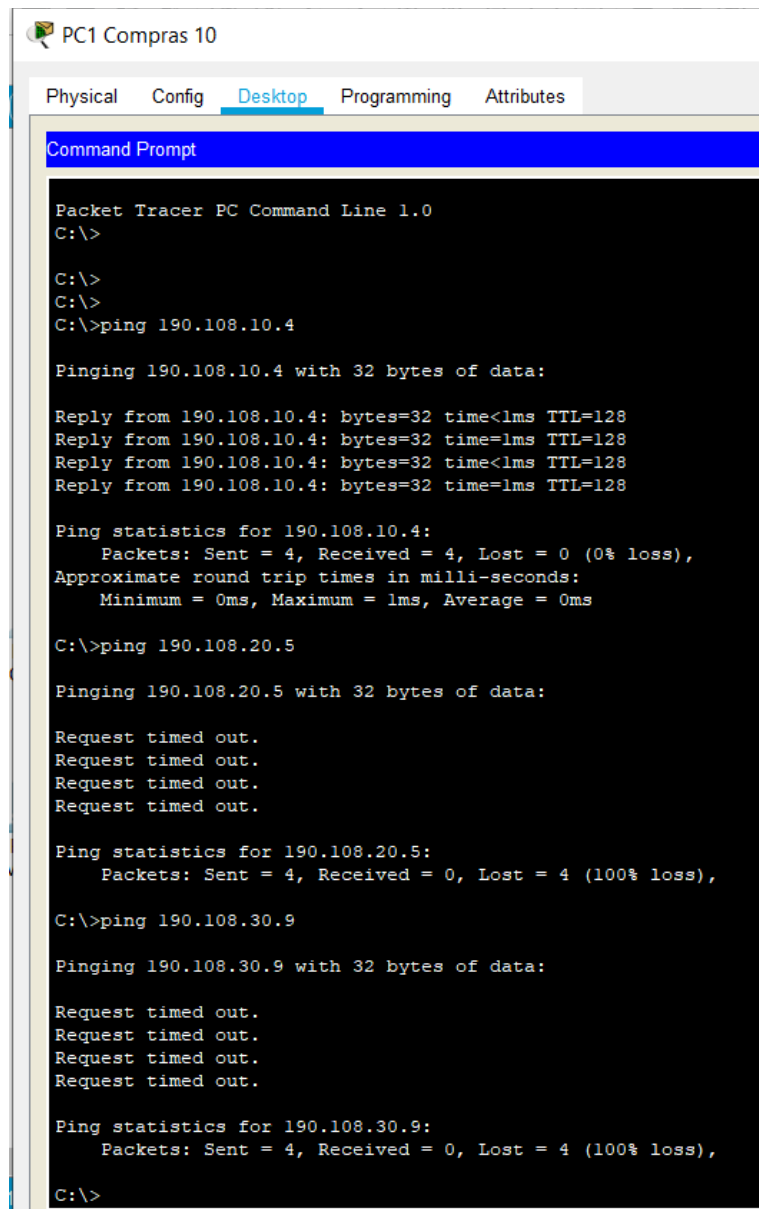
Figura 36. Comprobación de la difusión de la VLAN 99 en SWT3

### 1.3.9. Verificación de la conectividad Extremo a Extremo

#### 1.3.9.1. Desde cada PC a los demás

Se toman tres PC de muestra, con diferentes ubicaciones en la topología y se verifica por medio de ping la conectividad a tres PC de diferentes SW y VLAN con el fin de definir cuales ping tienen éxito.

PC1 en SWT1 y VLAN 10



```
PC1 Compras 10
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>
C:\>
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<1ms TTL=128
Reply from 190.108.10.4: bytes=32 time=1ms TTL=128
Reply from 190.108.10.4: bytes=32 time<1ms 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 = 1ms, Average = 0ms

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 190.108.30.9

Pinging 190.108.30.9 with 32 bytes of data:

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

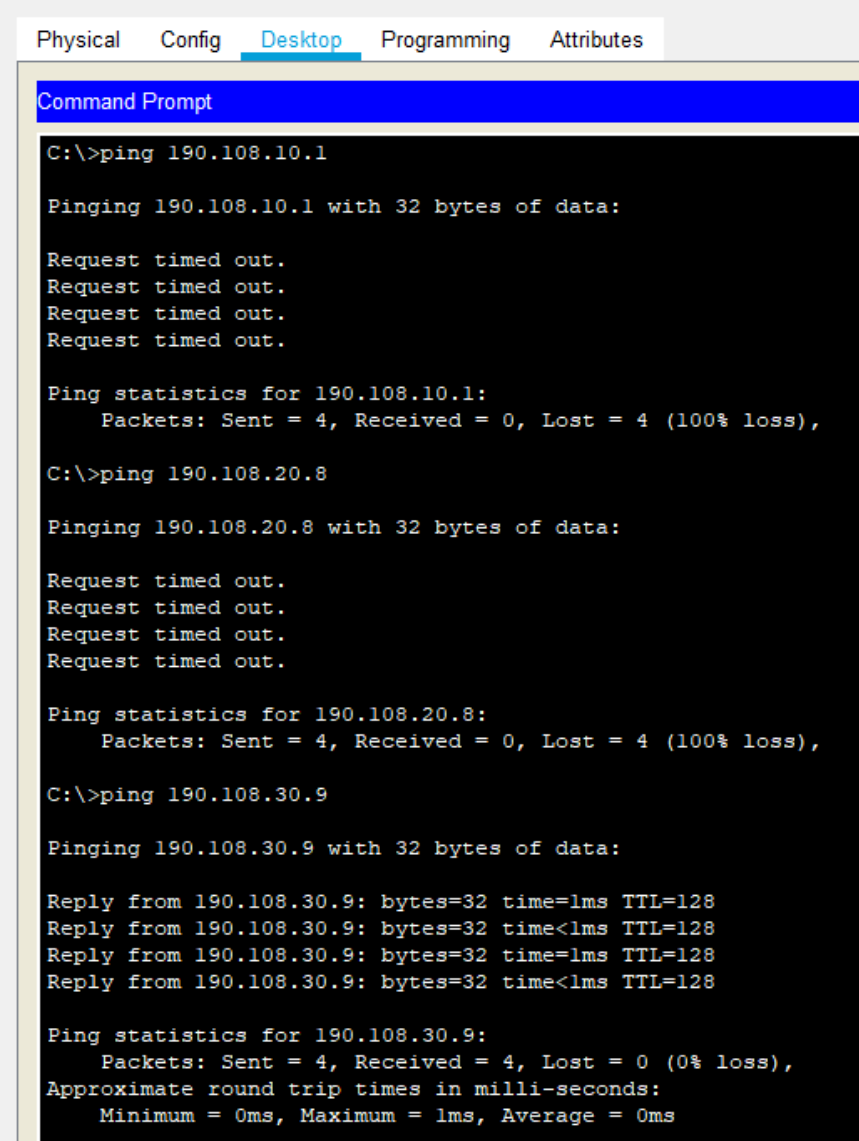
Ping statistics for 190.108.30.9:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Figura 37. Ping desde PC1 (VLAN10) a PC4 (VLAN10), PC5 (VLAN20) y PC9 (VLAN30)

## PC6 en SWT2 y VLAN 20

PC6 Planta 30



```
Physical  Config  Desktop  Programming  Attributes
Command Prompt
C:\>ping 190.108.10.1

Pinging 190.108.10.1 with 32 bytes of data:

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

Ping statistics for 190.108.10.1:
    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 190.108.30.9

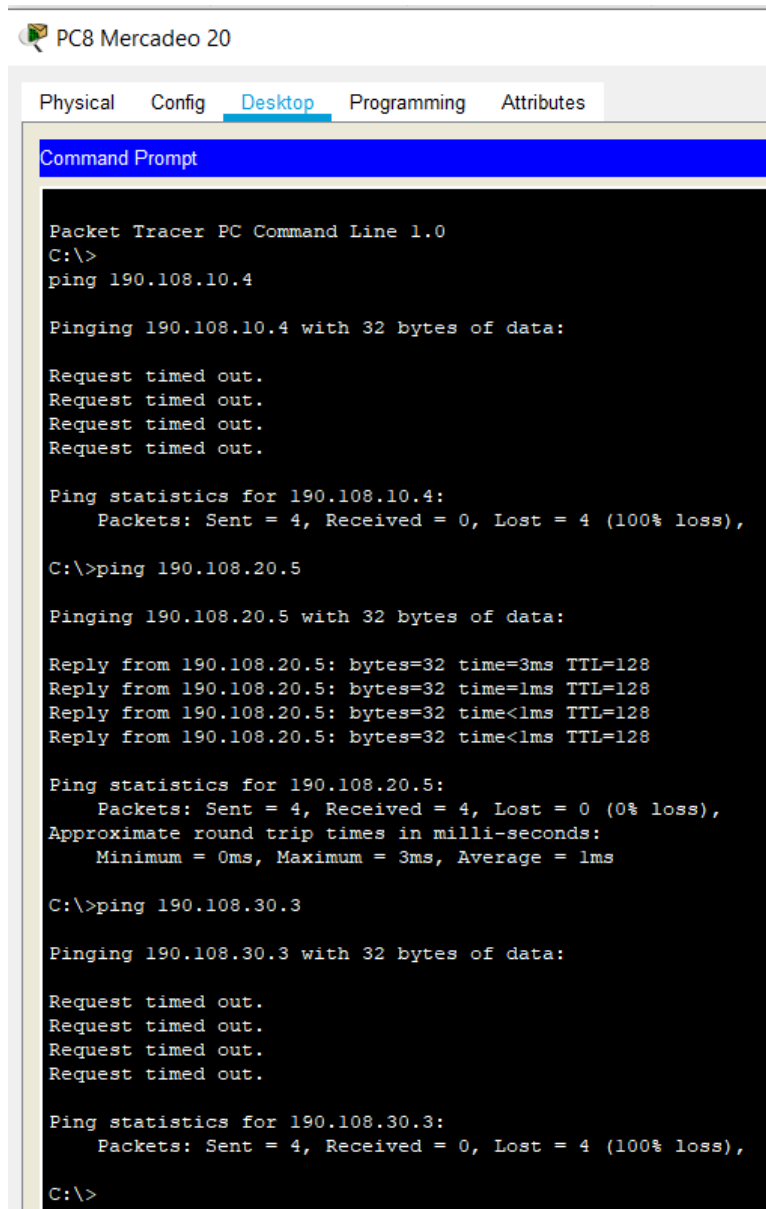
Pinging 190.108.30.9 with 32 bytes of data:

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

Ping statistics for 190.108.30.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figura 38. Ping desde PC6 (VLAN30) a PC1 (VLAN10), PC8 (VLAN20) y PC9 (VLAN30)

## PC8 en SWT3 y VLAN 30



```
PC8 Mercadeo 20
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>
ping 190.108.10.4

Pinging 190.108.10.4 with 32 bytes of data:

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

Ping statistics for 190.108.10.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.20.5

Pinging 190.108.20.5 with 32 bytes of data:

Reply from 190.108.20.5: bytes=32 time=3ms TTL=128
Reply from 190.108.20.5: bytes=32 time=1ms TTL=128
Reply from 190.108.20.5: bytes=32 time<1ms TTL=128
Reply from 190.108.20.5: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.20.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms

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),

C:\>
```

Figura 39. Ping desde PC8 (VLAN20) a PC4 (VLAN10), PC5 (VLAN20) y PC3 (VLAN30)

Únicamente tienen éxito los pings cuyo equipo de origen y destino estén conectados a la misma VLAN y adicionalmente a la misma subred. Los pings entre VLAN diferentes o subredes diferentes no tienen éxito.



### 1.3.9.2. Desde cada switch a los demás

Se emiten verificaciones de ping desde cada switch a los otros dos, esto usando la IP que se configuró en la SVI de la VLAN 99 en cada uno de ellos.

Desde SWT1

```
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 = 0/0/0 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 = 0/0/1 ms

SWT1#
```

Figura 40. Ping desde SWT1 (VLAN99) a SWT2 (VLAN99) y a SWT3 (VLAN99)

Desde SWT2

```
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 = 0/0/0 ms

SWT2#
```

Figura 41. Ping desde SWT2 (VLAN99) a SWT1 (VLAN99) y a SWT3 (VLAN99)

Desde 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 = 0/0/0 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 = 0/1/8 ms

SWT3#|
```

*Figura 42. Ping desde SWT3 (VLAN99) a SWT1 (VLAN99) y a SWT2 (VLAN99)*

Los pings tuvieron éxito debido a que todas las SVI fueron creadas en la VLAN 99 y cuyas direcciones asignadas corresponden a una única subred.

#### 1.3.9.3. Desde cada switch a cada PC

Se emiten verificaciones de ping desde cada switch a los equipos que tienen conectados, los cuales pertenecen a las VLAN 10, 20 y 30 y a las tres subredes asociadas a cada una, esto para que permita probar la totalidad de variables y establecer si es posible tener comunicación.

## Desde SWT1

```
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#
```

Figura 43. Ping desde SWT1 (VLAN99) a PC1 (VLAN10), PC2 (VLAN20) y PC3 (VLAN30)

## Desde SWT2

```
SWT2#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)

SWT2#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)

SWT2#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)

SWT2#
```

Figura 44. Ping desde SWT2 (VLAN99) a PC4 (VLAN10), PC5 (VLAN20) y PC6 (VLAN30)

Desde SWT3

```
SWT3#ping 190.108.10.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.7, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SWT3#ping 190.108.20.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.8, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SWT3#ping 190.108.30.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.9, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

SWT3#
```

*Figura 45. Ping desde SWT3 (VLAN99) a PC7 (VLAN10), PC8 (VLAN20) y PC9 (VLAN30)*

Ninguno de los pings tiene éxito debido a que el origen de la conexión es la SVI de cada uno de los switch, estas últimas pertenecen a la VLAN 99 y a la subred 190.108.90.x que son totalmente diferentes a cualquiera de los PC, es por esto que no es posible establecer una conexión desde un switch a un PC de la topología.

## 2. CONCLUSIONES

- Los protocolos de enrutamiento son la base del principio de escalabilidad y flexibilidad de las redes de datos.
- Las principales diferencias entre protocolos de enrutamiento radican en los parámetros necesarios para ser implementados, además de las características propias de funcionamiento y seguridad que cada uno ofrece.
- La redistribución de rutas busca asegurar la compatibilidad del enrutamiento entre redes diferentes, independientemente del protocolo que se use.
- Las interfaces loopback aseguran comunicación permanente entre vecindades en protocolos en los que tienen que declararse las direcciones del next hop.
- Las VLAN permiten restringir físicamente el acceso entre redes diferentes, logrando segmentar un switch según las necesidades de cada administrador de red.
- Cuando se trabaja con VLAN en diferentes switch es de extrema utilidad el protocolo VTP, que, por medio de la creación de un dominio, la creación de roles de servidor y cliente, difunden las VLAN creadas en todos los switch, facilitando su configuración y ahorrando tiempo.
- Para la conexión entre switch es necesaria la creación de enlaces troncales, en lo que una interfaz asume ese rol y permite el tráfico de todas las VLAN hacia un switch que haga parte de la topología.

## BIBLIOGRAFÍA

Diane Teare, Bob Vachon, Rick Graziani. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide: OSPF Implementation. Indianápolis: CISCO Press 2015, Disponible en: <https://1drv.ms/b/s!AmlJYei-NT1InMfy2rhPZHwEoWx>

Diane Teare, Bob Vachon, Rick Graziani. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide: EIGRP Implementation. Indianápolis: CISCO Press 2015, Disponible en: <https://1drv.ms/b/s!AmlJYei-NT1InMfy2rhPZHwEoWx>

Diane Teare, Bob Vachon, Rick Graziani. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide: BGP Implementation. Indianápolis: CISCO Press, 2015, Disponible en: <https://1drv.ms/b/s!AmlJYei-NT1InMfy2rhPZHwEoWx>

Froom Richard, Frahim Erum. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: CISCO Press, 2015, Disponible en: <https://1drv.ms/b/s!AmlJYei-NT1InWR0hoMxgBNv1CJ>