

EVALUACIÓN FINAL  
PRUEBA DE HABILIDADES PRACTICAS CCNP

BRIAN STEVE GONZALEZ PRIETO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
INGENIERIA DE TELECOMUNICACIONES  
DIPLOMADO CISCO CCNP  
BOGOTA D.C  
2019

# EVALUACIÓN PRUEBA DE HABILIDADES PRACTICAS CCNP

BRIAN STEVE GONZALEZ PRIETO

Diplomado de profundización cisco CCNP prueba de  
Habilidades prácticas

Gerardo Granados Acuña

Magíster en Telemática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

INGENIERIA DE TELECOMUNICACIONES

DIPLOMADO CISCO CCNP

BOGOTA D.C

2019

NOTA DE ACEPTACION

---

---

---

---

---

---

---

Presidente del jurado \_\_\_\_\_

Jurado \_\_\_\_\_

Jurado \_\_\_\_\_

Bogotá 05 de septiembre de 2019

## CONTENIDO

INTRODUCCIÓN	10
ESCENARIO 1	11
ESCENARIO 2	20
ESCENARIO 3	33
CONCLUSIONES	51
BIBLIOGRAFÍA	52

## LISTA DE TABLAS

Tabla 1 Direccionamiento de Routers	22
Tabla 2 Direccionamiento de Vlans	45
Tabla 3 Direccionamiento ip Switches	47

## LISTA DE FIGURAS

Figura 1. Escenario 1	13
Figura 2. Tabla enrutamiento R3	19
Figura 3. Tabla enrutamiento R1	21
Figura 4. Tabla de enrutamiento R5	21
Figura 5. Escenario 2	22
Figura 6. Configuración R1	29
Figura 7. Configuración R2	30
Figura 8. Configuración R3	32
Figura 9. Configuración R4	34
Figura 10. Escenario 3	35
Figura 11. Configuración SWT1	37
Figura 12. Configuración SWT2	38
Figura 13. Configuración SWT3	38
Figura 14. Verificación interfaces SWT1	40
Figura 15. Verificación interfaces SWT2	40
Figura 16. Verificación interfaces trunk SWT1	42
Figura 17. Verificación Vlans SWT 1	43
Figura 18. Verificación Vlans SWT 2	44

Figura 19. Verificación conexión extremo a extremo	48
Figura 20. Conexión Switch Ping from SW1 to SW2 & SW3	48
Figura 21. Conexión Switch Ping from SW2 to SW1 & SW3	49
Figura 22. Conexión Switch Ping from SW3 to SW1 & SW2	49
Figura 23. Ping SWT3	51
Figura 24. Ping SWT2	51

## GLOSARIO

**Gns3:** Es un simulador gráfico de red lanzado en 2008, que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos, permitiendo la combinación de dispositivos tanto reales como virtuales.

Para permitir completar simulaciones, GNS3 está estrechamente vinculada con:

- Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarios imágenes IOS de Cisco Systems.<sup>4</sup>
- Dynagen, un front-end basado en texto para Dynamips
- Qemu y VirtualBox, para permitir utilizar máquinas virtuales como un *firewall* PIX.
- **VPCS**, un emulador de PC con funciones básicas de *networking*
- **IOU** (IOS on Unix), compilaciones especiales de IOS provistas por Cisco para correr directamente en sistemas UNIX y derivados.

**Networking:** En el mundo de las computadoras, el concepto de networking aplica a las redes de cómputo para vincular dos o más dispositivos informáticos con el propósito de compartir datos. Las redes están construidas con una mezcla de hardware y software, incluyendo el cableado necesario para conectar los equipos..

**Protocolos de red:** En informática y telecomunicación, un protocolo de comunicaciones es un sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física

**Vlan:** Una VLAN, acrónimo de virtual LAN, 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

## RESUMEN

La prueba de habilidades prácticas o Hands on skills de cisco, hace parte de las actividades propuestas para llevar a cabo la culminación del Diplomado de Profundización CCNP, con el fin de identificar las habilidades obtenidas durante la parte teórica y laboratorios desarrollados durante el curso. Como principal aspecto se debe analizar y ofrecer una solución a los escenarios propuestos aplicando los conocimientos de Networking. Por lo que se ha establecido fechas para realizar el desarrollo de la guía y para esto se debe acompañar de una documentación específica evidenciando así cada línea de comando para los protocolos de red y pantallazos de pruebas de conectividad y tablas de enrutamiento correspondientes a cada dispositivo en su escenario correspondiente. Para finalizar se dará respuesta a las interrogantes que acompañan los ítems del último escenario, dando soporte a las simulaciones planteadas y a los resultados obtenidos.

Se utilizarán software de simulaciones y emulaciones de red como los son GNS3 y Packet Tracer,

Palabras Clave: CCNP, CISCO, Networking, Telecomunicaciones

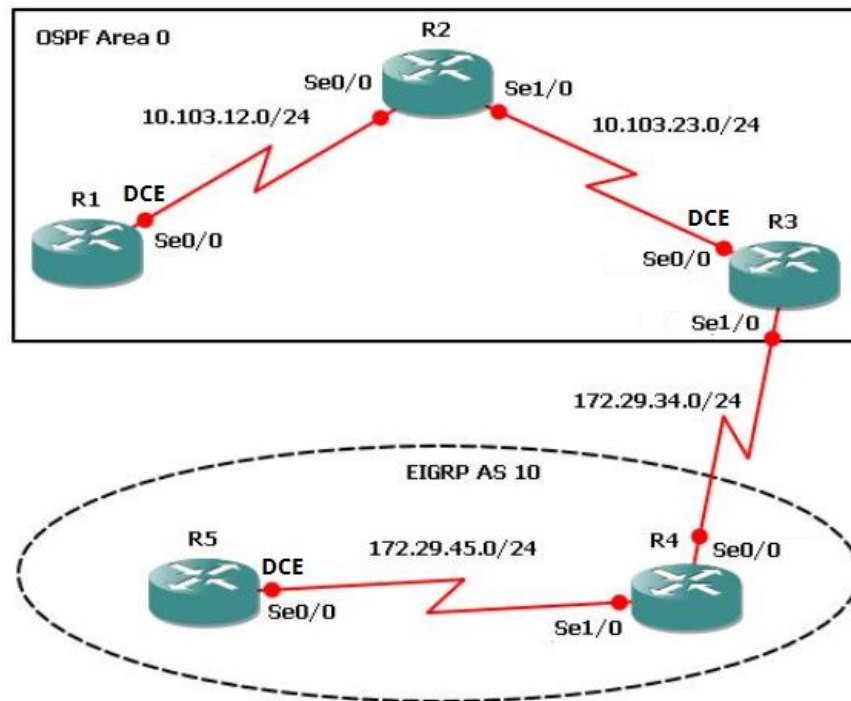
## INTRODUCCIÓN

Las comunicaciones son indispensables en la actualidad y para cada empresa y/o negocio local se requiere de una conexión a internet con el fin de transferir, almacenar y administrar información de cualquier magnitud.

A continuación se evidencia el desarrollo de la prueba de habilidades o Hands on skills del diplomado de profundización Cisco CCNP, en el cual se adjuntan los comandos paso a paso de acuerdo a los escenarios propuestos, se evidencia mediante pantallazos el resultado exitoso del funcionamiento de las conexiones establecidas.

Posteriormente se da respuesta a las preguntas indicadas en la guía justificando así los resultados obtenidos en las simulaciones. El desarrollo de los escenarios propuestos se realizó mediante las herramientas GNS3 y Packet trackert. Como finalidad de este laboratorio se adquieren habilidades con el material proporcionado a lo largo del curso para que sean aplicadas a escenarios reales bajo los estándares y protocolos que caracterizan a los dispositivos Cisco.

Figura 1. Escenario 1



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.

### Router 1:

Se procede a realizar implementación de direccionamiento a la interfaz y configuración de protocolo de enrutamiento (OSPF) con su respectivo Id y area

Enable

configure terminal

interface s1/0

```
ip address 10.103.12.1 255.255.255.0
```

```
clock rate 128000
```

```
bandwidth 128
```

```
no shutdown
```

```
exit
```

```
router ospf 1
```

```
router-id 1.1.1.1
```

```
network 10.103.12.0 0.0.0.255 area 0
```

```
exit
```

## **Router 2**

Se procede a realizar implementación de direccionamiento a la interfaz y configuración de protocolo de enrutamiento (OSPF) con su respectivo Id y area

```
enable
```

```
configure terminal
```

```
interface s1/0
```

```
ip address 10.103.12.2 255.255.255.0
```

```
no shutdown
```

```
exit
```

```
interface s1/1
ip address 10.103.23.1 255.255.255.0
no shutdown
exit
router ospf 1
router-id 2.2.2.2
network 10.103.12.0 0.0.0.255 area 0
network 10.103.23.0 0.0.0.255 area 0
exit
```

### **Router 3**

Se procede a realizar implementación de direccionamiento a la interfaz y configuración de protocolo de enrutamiento (OSPF) con su respectivo Id y area

```
interface s1/1
ip address 10.103.23.2 255.255.255.0
clock rate 128000
bandwidth 128
no shutdown
exit
interface s1/2
ip address 172.29.34.1 255.255.255.0
```

```
no shutdown

router ospf 1

router-id 3.3.3.3

network 10.103.23.0 0.0.0.255 area 0

exit
```

#### **Router 4**

Se procede a realizar implementación de direccionamiento a la interfaz y configuración de protocolo de enrutamiento (EIGRP) con su respectivo Id

```
interface s1/2

ip address 172.29.34.2 255.255.255.0

no shutdown

exit

interface s1/0

ip address 172.29.45.1 255.255.255.0

no shutdown

exit

router eigrp 10

eigrp router-id 4.4.4.4

network 172.29.34.0 255.255.255.0

network 172.29.45.0 255.255.255.0
```

exit

### **Router 5**

Se procede a realizar implementación de direccionamiento a la interfaz y configuración de protocolo de enrutamiento (EIGRP) con su respectivo Id

```
interface s1/0
```

```
ip address 172.29.45.2 255.255.255.0
```

```
no shutdown
```

```
exit
```

```
router eigrp 10
```

```
eigrp router-id 5.5.5.5
```

```
network 172.29.45.0 255.255.255.0
```

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.

### **Router 1:**

Se procede a configurar interfaces Loopback mediante direccionamiento solicitado.

```
enable
configure terminal
interface loopback 1
ip address 10.1.1.1 255.255.252.0
ip ospf 1 area 0
exit
interface loopback 2
ip address 10.1.10.1 255.255.252.0
ip ospf 1 area 0
exit
interface loopback 3
ip address 10.1.15.1 255.255.252.0
ip ospf 1 area 0
exit
interface loopback 4
ip address 10.1.4.1 255.255.252.0
ip ospf 1 area 0
exit
```

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.

### **Router 5**

Se procede a configurar interfaces Loopback mediante direccionamiento solicitado.

```
interface loopback 1
ip address 172.5.1.1 255.255.252.0
exit
interface loopback 2
ip address 172.5.10.1 255.255.252.0
exit
```

```

interface loopback 3
ip address 172.5.15.1 255.255.252.0
exit
interface loopback 4
ip address 172.5.4.1 255.255.252.0
exit

```

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 realizan pruebas del enrutamiento asignado usando el R3 quien debe aprender las rutas asignadas en el R1 y R5 mediante Show Ip Route

Figura 2. Tabla enrutamiento R3

```

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
        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, 7 subnets, 2 masks
O       10.1.1.1/32 [110/846] via 10.103.23.1, 00:03:07, Serial1/1
O       10.1.4.1/32 [110/846] via 10.103.23.1, 00:03:07, Serial1/1
O       10.1.10.1/32 [110/846] via 10.103.23.1, 00:03:07, Serial1/1
O       10.1.15.1/32 [110/846] via 10.103.23.1, 00:03:07, Serial1/1
O       10.103.12.0/24 [110/845] via 10.103.23.1, 00:03:07, Serial1/1
C       10.103.23.0/24 is directly connected, Serial1/1
L       10.103.23.2/32 is directly connected, Serial1/1
       172.5.0.0/22 is subnetted, 4 subnets
D       172.5.0.0 [90/2809856] via 172.29.34.2, 00:03:20, Serial1/2
D       172.5.4.0 [90/2809856] via 172.29.34.2, 00:03:20, Serial1/2
D       172.5.8.0 [90/2809856] via 172.29.34.2, 00:03:20, Serial1/2
D       172.5.12.0 [90/2809856] via 172.29.34.2, 00:03:20, Serial1/2
       172.29.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.29.34.0/24 is directly connected, Serial1/2
L       172.29.34.1/32 is directly connected, Serial1/2
L       172.29.45.0/24 [90/2681856] via 172.29.34.2, 00:03:20, Serial1/2

```

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.

Se procede a establecer redistribución de los protocolos de enrutamiento usando los parámetros solicitados de la siguiente forma:

**Router 3**

```
enable
configure terminal
router eigrp 10
redistribute ospf 1 metric 100000 20000 255 255 1500
exit
router ospf 1
redistribute eigrp 10 metric 50000 subnets
exit
end
```

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***.

Posterior a la redistribución, los routers R1 y R5, deben poder identificar las sub redes creadas en las interfaces loopback, se validara mediante el comando show ip route en el router 1 y 5 de la siguiente forma:

Figura 3. Tabla De Enrutamiento R1

```

R1
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, 11 subnets, 3 masks
C   10.1.0.0/22 is directly connected, Loopback1
L   10.1.1.1/32 is directly connected, Loopback1
C   10.1.4.0/22 is directly connected, Loopback4
L   10.1.4.1/32 is directly connected, Loopback4
C   10.1.8.0/22 is directly connected, Loopback2
L   10.1.10.1/32 is directly connected, Loopback2
C   10.1.12.0/22 is directly connected, Loopback3
L   10.1.15.1/32 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
D   10.103.23.0/24 [110/845] via 10.103.12.2, 00:04:28, Serial1/0
O   172.5.0.0/22 is subnetted, 4 subnets
O E2 172.5.0.0 [110/50000] via 10.103.12.2, 00:04:37, Serial1/0
O E2 172.5.4.0 [110/50000] via 10.103.12.2, 00:04:37, Serial1/0
O E2 172.5.8.0 [110/50000] via 10.103.12.2, 00:04:37, Serial1/0
O E2 172.5.12.0 [110/50000] via 10.103.12.2, 00:04:37, Serial1/0
O   172.29.0.0/24 is subnetted, 2 subnets
O E2 172.29.34.0 [110/50000] via 10.103.12.2, 00:04:37, Serial1/0
O E2 172.29.45.0 [110/50000] via 10.103.12.2, 00:04:37, Serial1/0

```

R5:

Figura 4. Tabla enrutamiento R5

```

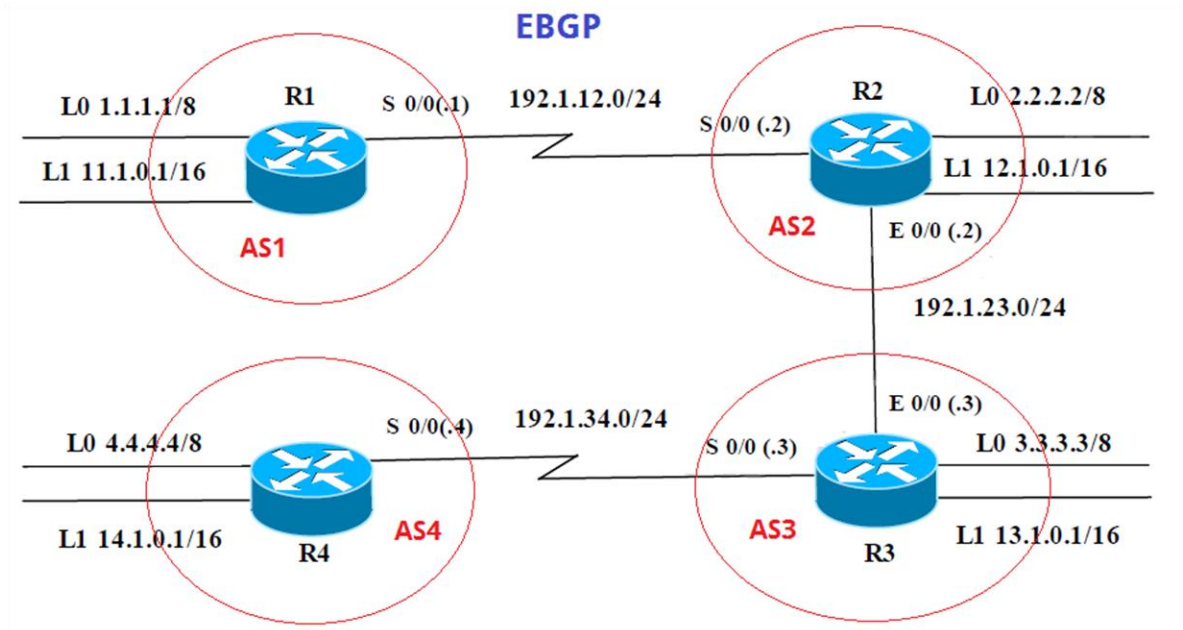
R5
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
D EX 10.1.1.1/32 [170/7801856] via 172.29.45.1, 00:04:56, Serial1/0
D EX 10.1.4.1/32 [170/7801856] via 172.29.45.1, 00:04:56, Serial1/0
D EX 10.1.10.1/32 [170/7801856] via 172.29.45.1, 00:04:56, Serial1/0
D EX 10.1.15.1/32 [170/7801856] via 172.29.45.1, 00:04:56, Serial1/0
D EX 10.103.12.0/24 [170/7801856] via 172.29.45.1, 00:04:56, Serial1/0
D EX 10.103.23.0/24 [170/7801856] via 172.29.45.1, 00:05:09, Serial1/0
O   172.5.0.0/16 is variably subnetted, 8 subnets, 2 masks
C   172.5.0.0/22 is directly connected, Loopback1
L   172.5.1.1/32 is directly connected, Loopback1
C   172.5.4.0/22 is directly connected, Loopback4
L   172.5.4.1/32 is directly connected, Loopback4
C   172.5.8.0/22 is directly connected, Loopback2
L   172.5.10.1/32 is directly connected, Loopback2
C   172.5.12.0/22 is directly connected, Loopback3
L   172.5.15.1/32 is directly connected, Loopback3
O   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, 00:05:09, Serial1/0
C   172.29.45.0/24 is directly connected, Serial1/0
L   172.29.45.2/32 is directly connected, Serial1/0

```

Figura 5. Escenario 2



Información para configuración de los Routers

Tabla 1. Direccionamiento de Routers

R1	Interfaz	Dirección IP	Máscara
	Loopback 0	1.1.1.1	255.0.0.0

R2	Interfaz		
	Dirección IP	Máscara	
	Loopback 0	2.2.2.2	255.0.0.0
R3	Interfaz		
	Dirección IP	Máscara	
	Loopback 0	3.3.3.3	255.0.0.0
	E 0/0	192.1.23.3	255.255.255.0

R4	Interfaz		
	Dirección IP	Máscara	
	Loopback 0	4.4.4.4	255.0.0.0

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**.

Se procede a implementar direccionamiento mediante interfaces loopback con los Id's correspondientes, adicional se configura direccionamiento en los enlaces seriales de cada router:

#### **Router 1:**

```
enable
```

```
configure terminal
```

```
Interface Loopback 0
```

```
ip address 1.1.1.1 255.0.0.0
```

```
exit
```

```
Interface Loopback 1
```

```
ip address 11.1.0.1 255.255.0.0
```

```
exit
```

```
interface s1/0
```

```
ip address 192.1.12.1 255.255.255.0
```

```
clockrate 64000
```

no shutdown

exit

end

wr

## **Router 2**

configure terminal

interface loopback 0

ip address 2.2.2.2 255.0.0.0

exit

interface loopBack 1

ip address 12.1.0.1 255.255.0.0

exit

interface s1/0

ip address 192.1.12.2 255.255.255.0

no shutdown

exit

```
interface fastEthernet 0/0  
  
ip address 192.1.23.2 255.255.255.0  
  
no shutdown  
  
exit  
  
end  
  
wr
```

### **Router 3**

```
enable  
  
configure terminal  
  
interface loopBack 0  
  
ip address 3.3.3.3 255.0.0.0  
  
exit  
  
interface loopBack 1  
  
ip address 13.1.0.1 255.255.0.0  
  
exit  
  
interface fastEthernet 0/0
```

```
ip address 192.1.23.3 255.255.255.0
```

```
no shutdown
```

```
exit
```

```
interface s1/0
```

```
ip address 192.1.34.3 255.255.255.0
```

```
no shutdown
```

```
exit
```

```
end
```

```
wr
```

#### **Router 4**

```
enable
```

```
configure terminal
```

```
interface loopBack 0
```

```
ip address 4.4.4.4 255.0.0.0
```

```
exit
```

```
interface loopBack 1
```

```
ip address 14.1.0.1 255.255.0.0
```

```
exit  
  
interface s1/0  
  
ip address 192.1.34.4 255.255.255.0  
  
Clockrate 64000  
  
no shutdown  
  
exit  
  
end  
  
wr
```

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.

Se realiza configuración de protocolo BGP y se asigna router vecino de acuerdo a lo indicado

### **Router 1**

```
router bgp 1  
  
bgp router-id 11.11.11.11
```

neighbor 192.1.12.2 remote-as 2

network 1.0.0.0 mask 255.0.0.0

network 11.1.0.0 mask 255.255.0.0

Figura 6. Configuración R1

```
R1#sh i
*May 22 20:13:00.959: %SYS-5-CONFIG_I: Configured from console by console
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
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#
```

## Router 2

enable

configure terminal

router bgp 2

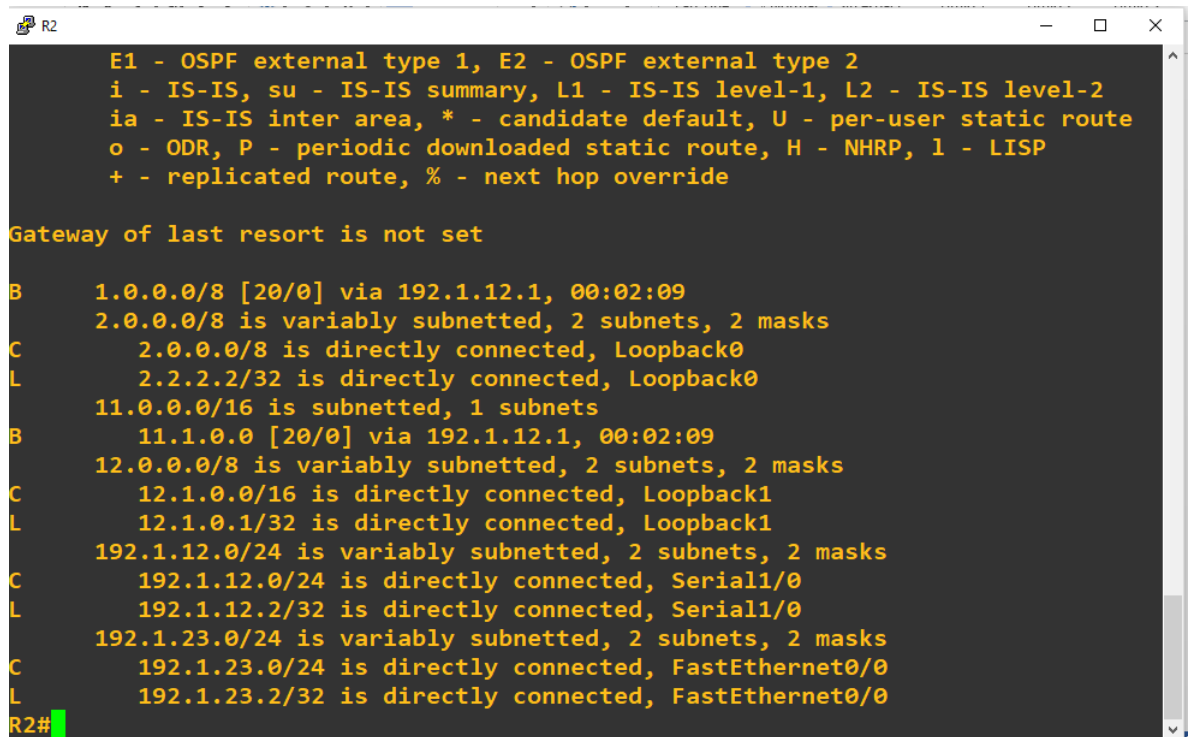
bgp router-id 22.22.22.22

```
neighbor 192.1.12.1 remote-as 1

network 2.0.0.0 mask 255.0.0.0

network 12.1.0.0 mask 255.255.0.0
```

Figura 7. Configuración R2



```
R2
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

B    1.0.0.0/8 [20/0] via 192.1.12.1, 00:02:09
C    2.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
L    2.0.0.0/8 is directly connected, Loopback0
L    2.2.2.2/32 is directly connected, Loopback0
C    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 192.1.12.1, 00:02:09
C    12.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
L    12.1.0.0/16 is directly connected, Loopback1
L    12.1.0.1/32 is directly connected, Loopback1
C    192.1.12.0/24 is variably subnetted, 2 subnets, 2 masks
L    192.1.12.0/24 is directly connected, Serial1/0
L    192.1.12.2/32 is directly connected, Serial1/0
C    192.1.23.0/24 is variably subnetted, 2 subnets, 2 masks
L    192.1.23.0/24 is directly connected, FastEthernet0/0
L    192.1.23.2/32 is directly connected, FastEthernet0/0
R2#
```

2. Configure una relación de vecino BGP entre R2 y R3. R2 ya debería estar configurado en **AS2** y R3 debería estar en **AS3**. Anuncie las direcciones de Loopback de R3 en BGP. Codifique el ID del router R3 como 33.33.33.33. Presente el paso a con los comandos utilizados y la salida del comando **show ip route**.

Se realiza configuración se vecino entre router 2 y 3, se configura Id se Router 3 de acuerdo a lo indicado. Se valida funcionamiento mediante Show Ip Route

### **Router 2**

enable

configure terminal

router bgp 2

neighbor 192.1.23.3 remote-as 3

### **Router 3**

enable

configure terminal

router bgp 3

bgp router-id 33.33.33.33

neighbor 192.1.23.2 remote-as 2

network 3.0.0.0 mask 255.0.0.0

network 13.1.0.0 mask 255.255.0.0

Figura 8. Configuración R3

```
R3
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

B   1.0.0.0/8 [20/0] via 192.1.23.2, 00:00:27
B   2.0.0.0/8 [20/0] via 192.1.23.2, 00:00:27
   3.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   3.0.0.0/8 is directly connected, Loopback0
L   3.3.3.3/32 is directly connected, Loopback0
   11.0.0.0/16 is subnetted, 1 subnets
B   11.1.0.0 [20/0] via 192.1.23.2, 00:00:27
   12.0.0.0/16 is subnetted, 1 subnets
B   12.1.0.0 [20/0] via 192.1.23.2, 00:00:27
   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, FastEthernet0/0
L   192.1.23.3/32 is directly connected, FastEthernet0/0
   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#
```

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.

Por último se procede a configurar relación entre Router 3 y 4. Se configuran Id correspondientes, se evidencia funcionamiento mediante Show Ip Route

### **Router 3**

enable

configure terminal

router bgp 3

neighbor 192.1.34.4 remote-as 4

### **Router 4**

enable

configure terminal

router bgp 4

bgp router-id 44.44.44.44

neighbor 192.1.34.3 remote-as 3

network 4.0.0.0 mask 255.0.0.0

exit

ip route 3.0.0.0 255.0.0.0 192.1.34.3

router bgp 4

network 14.1.0.0 mask 255.255.0.0

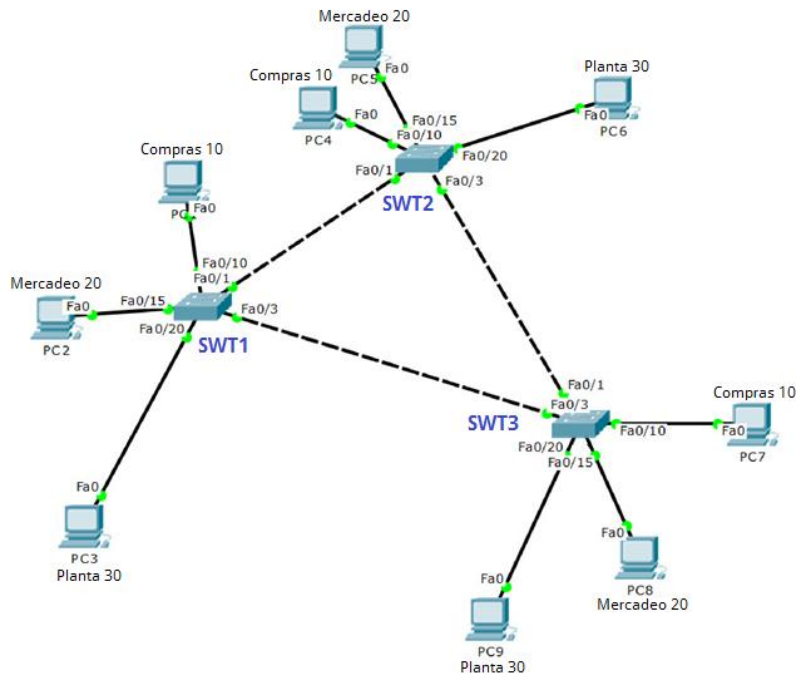
Figura 9. Configuración R4

```
R4
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

B    1.0.0.0/8 [20/0] via 192.1.34.3, 00:12:40
B    2.0.0.0/8 [20/0] via 192.1.34.3, 00:12:40
S    3.0.0.0/8 [1/0] via 192.1.34.3
    4.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    4.0.0.0/8 is directly connected, Loopback0
L    4.4.4.4/32 is directly connected, Loopback0
    11.0.0.0/16 is subnetted, 1 subnets
B    11.1.0.0 [20/0] via 192.1.34.3, 00:12:40
    12.0.0.0/16 is subnetted, 1 subnets
B    12.1.0.0 [20/0] via 192.1.34.3, 00:12:40
    13.0.0.0/16 is subnetted, 1 subnets
B    13.1.0.0 [20/0] via 192.1.34.3, 00:12:40
    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
```

Figura 10. Escenario 3



## A. Configurar VTP

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.

Se procede a realizar configuración VTP (dominio, versión y modo) en cada Switch. Estableciendo como servidor el Switch 2, los switches 1 y 3 se encontraran en modo cliente

### Switch 1

enable

configure terminal

```
vtp domain CCNP  
vtp version 2  
vtp mode client  
vtp password cisco  
end
```

### **Switch 2**

Se establece VTP Server de acuerdo a lo indicado

```
enable  
configure terminal  
vtp domain CCNP  
vtp version 2  
vtp mode server  
vtp password cisco  
end
```

### **Switch 3**

```
enable  
configure terminal  
vtp domain CCNP  
vtp version 2
```

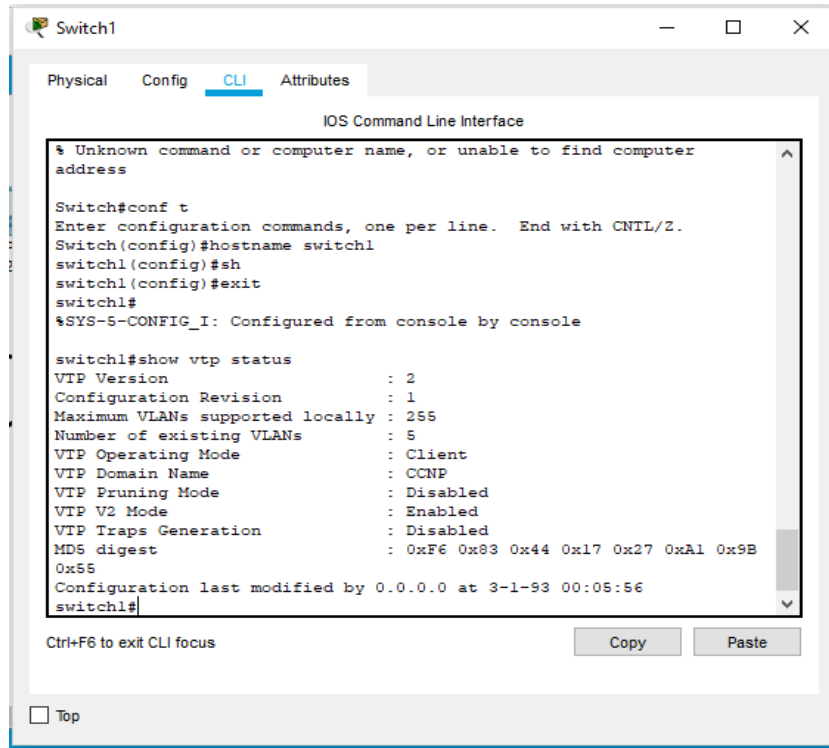
vtp mode client

vtp password cisco

end

2. Verifique las configuraciones mediante el comando **show vtp status**.  
**Switch 1**

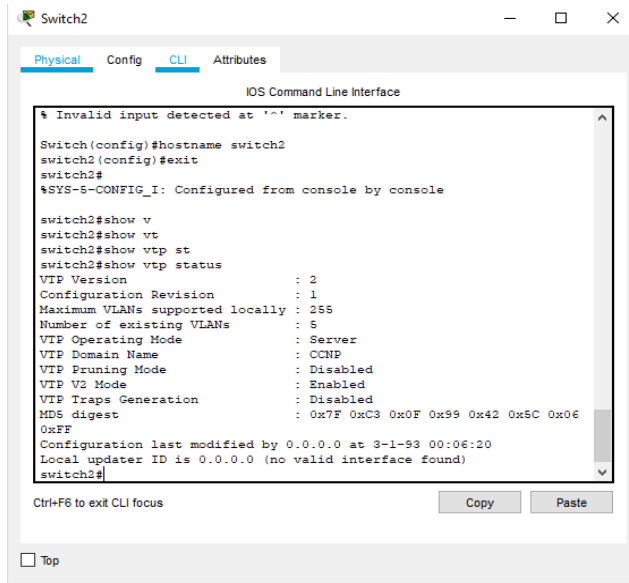
Figura 11. Configuración SWT1



```
Switch1
Physical Config CLI Attributes
IOS Command Line Interface
% Unknown command or computer name, or unable to find computer
address
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname switch1
switch1(config)#sh
switch1(config)#exit
switch1#
%SYS-5-CONFIG_I: Configured from console by console
switch1#show vtp status
VTP Version           : 2
Configuration Revision : 1
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          : Enabled
VTP Traps Generation : Disabled
MDS digest           : 0xF6 0x83 0x44 0x17 0x27 0xA1 0x9B
0x55
Configuration last modified by 0.0.0.0 at 3-1-93 00:05:56
switch1#
```

## Switch 2

Figura 12. Configuración SWT2

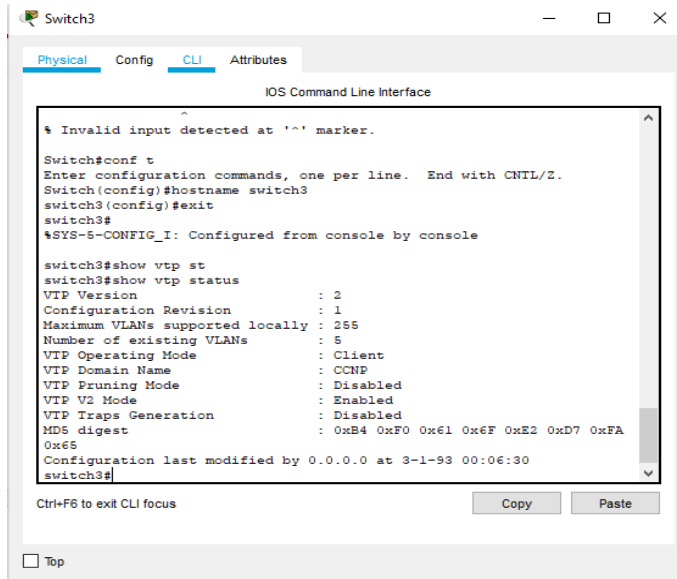


```
Switch2
Physical Config CLI Attributes
IOS Command Line Interface
% Invalid input detected at '^' marker.
Switch(config)#hostname switch2
switch2(config)#exit
switch2#
%SYS-5-CONFIG_I: Configured from console by console

switch2#show v
switch2#show vt
switch2#show vtp st
switch2#show vtp status
VTP Version          : 2
Configuration Revision : 1
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         : Enabled
VTP Traps Generation : Disabled
MD5 digest          : 0x7F 0xC3 0x0F 0x99 0x42 0x5C 0x06
0xFF
Configuration last modified by 0.0.0.0 at 3-1-93 00:06:20
Local updater ID is 0.0.0.0 (no valid interface found)
switch2#
Ctrl+F6 to exit CLI focus
Copy Paste
Top
```

## Switch 3

Figura 13. Configuración SWT3



```
Switch3
Physical Config CLI Attributes
IOS Command Line Interface
% Invalid input detected at '^' marker.
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname switch3
switch3(config)#exit
switch3#
%SYS-5-CONFIG_I: Configured from console by console

switch3#show vtp st
switch3#show vtp status
VTP Version          : 2
Configuration Revision : 1
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         : Enabled
VTP Traps Generation : Disabled
MD5 digest          : 0xB4 0xF0 0x61 0x6F 0xE2 0xD7 0xFA
0x65
Configuration last modified by 0.0.0.0 at 3-1-93 00:06:30
switch3#
Ctrl+F6 to exit CLI focus
Copy Paste
Top
```

## **B. Configurar DTP (Dynamic Trunking Protocol)**

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.

Se procede a trunkalizar puertos que comunica el Switch 1 y 2 de la siguiente forma

### **Switch 1**

enable

configure terminal

interface f0/1

switchport mode trunk

switchport mode dynamic desirable

### **Switch 2**

Se realiza mismo procedimiento en Switch 2

enable

configure terminal

interface fa0/1

switchport mode trunk

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

### Switch 1

Figura 14. Verificación interfaces SWT1

```

switch1
-----
Physical Config CLI Attributes
IOS Command Line Interface

switch1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up

switch1(config-if)#exit
switch1(config)#exit
switch1#
%SYS-5-CONFIG_I: Configured from console by console

switch1#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

switch1#
  
```

### Switch 2

Figura 15. Verificación interfaces SWT2

```

switch2
-----
Physical Config CLI Attributes
IOS Command Line Interface

switch2#
switch2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch2(config)#interface fa0/1
switch2(config-if)#switchport mode trunk
switch2(config-if)#exit
switch2(config)#exit
switch2#
%SYS-5-CONFIG_I: Configured from console by console

switch2#show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     on        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

switch2#
  
```

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

Se trunkaliza interfaz solicitada en el Switch 1 de la siguiente forma:

**Switch 1**

enable

configure terminal

interface fa0/3

switchport mode trunk

**Switch 3**

enable

Configure terminal

interface fa0/3

switchport mode trunk

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

Figura 16. Verificación interfaces trunk SWT1

```

Switch1
Physical Config CLI Attributes
IOS Command Line Interface
changed state to up
switch1(config-if)#exit
switch1(config)#exit
switch1#
%%SYS-5-CONFIG_I: Configured from console by console

switch1#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

switch1#
  
```

- Configure un enlace "trunk" permanente entre SWT2 y SWT3.  
Se procede a realizar configuración de puerto trunkalizado entre Switch 2 y 3 usando la interfaz fa0/3

**Switch 2**

enable  
configure terminal  
interface fa0/3  
switchport mode trunk

**Switch 3**

enable  
configure terminal  
interface fa0/1

Switchport mode trunk

### C. Agregar VLANs y asignar puertos.

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

Se procede a añadir VLAN indicadas mediante el siguiente comando, sin embargo solo permitirá la creación de VLAN un Switch cuando el modo de VTP es servidor como se observa en el Switch 2.

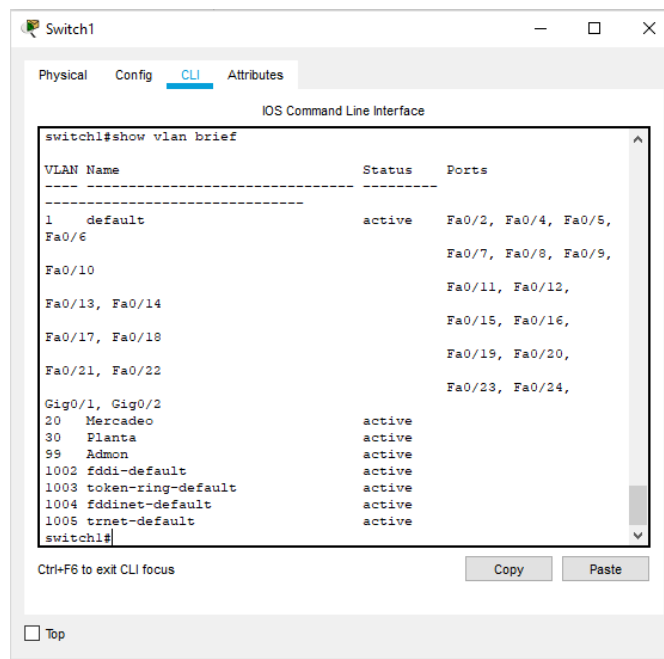
#### Switch 1

enable

configure terminal

vlan 10 (No es permitida la creación ya que el modo de VTP es Cliente)

Figura 17. Verificación Vlans



```
switch1#show vlan brief
VLAN Name                Status    Ports
-----
1    default                 active    Fa0/2, Fa0/4, Fa0/5,
Fa0/6                    Fa0/7, Fa0/8, Fa0/9,
Fa0/10                   Fa0/11, Fa0/12,
Fa0/13, Fa0/14          Fa0/15, Fa0/16,
Fa0/17, Fa0/18          Fa0/19, Fa0/20,
Fa0/21, Fa0/22          Fa0/23, Fa0/24,
Gig0/1, Gig0/2
20   Mercadeo                active
30   Planta                  active
99   Admon                   active
1002 fddi-default            active
1003 token-ring-default    active
1004 fddinet-default       active
1005 trnet-default         active
switch1#
```

## Switch 2

enable

configure terminal

vlan 10

name Compras

vlan 20

name Mercadeo

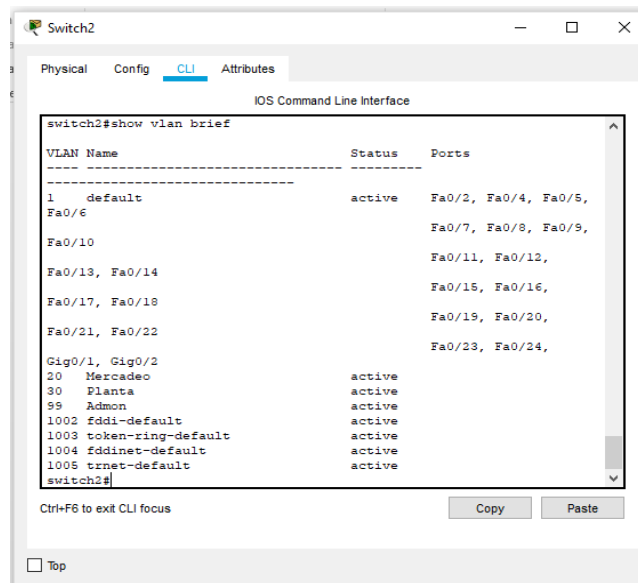
vlan 30

name Planta

vlan 99

name Admon

Figura 18. Verificación Vlans SWT 2



```
switch2#show vlan brief
```

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

switch2#

Ctrl+F6 to exit CLI focus

Copy Paste

Top

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

Tabla 2. Direccionamiento de VLANS

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

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

Se procede a taggear interfaces en VLAN correspondiente en cada Switch de la siguiente forma:

**Switch 1**

```
enable
configure terminal
interface fa0/10
switchport access vlan 10
```

**Switch 2**

```
enable
configure terminal
interface fa0/10
switchport access vlan 10
```

### **Switch 3**

```
enable
configure terminal
interface fa0/10
switchport access vlan 10
```

3. 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.

### **Switch 1**

```
enable
configure terminal
interface fa0/15
switchport access vlan 20
exit
interface fa0/20

switchport access vlan 30
```

### **Switch 2**

```
enable

configure terminal

interface fa0/15
switchport access vlan 20
exit
interface fa0/20
```

```
switchport access vlan 30
```

### Switch 3

```
enable
```

```
configure terminal
```

```
interface fa0/15
```

```
switchport access vlan 20
```

```
exit
```

```
interface fa0/20
```

```
switchport access vlan 30
```

#### D. Configurar las direcciones IP en los Switches.

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

Tabla 3. Direccionamiento IP Switches

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

Se procede a asignar dirección IP para las VLAN indicadas en la VLAN 99 para cada switch

### **Switch 1**

enable

configure terminal

interface vlan 99

ip address 190.108.99.1 255.255.255.0

no shutdown

### **Switch 2**

enable

configure terminal

int vlan 99

ip address 190.108.99.2 255.255.255.0

no shutdown

### **Switch 3**

enable

configure terminal

interface vlan 99

ip address 190.108.99.3 255.255.255.0

no shutdown

## E. Verificar la conectividad Extremo a Extremo

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

Figura 19. Verificación conexión extremo a extremo

```
C:\>ping 190.108.10.30
Pinging 190.108.10.30 with 32 bytes of data:
Reply from 190.108.10.30: bytes=32 time<1ms TTL=128
Reply from 190.108.10.30: bytes=32 time<1ms TTL=128
Reply from 190.108.10.30: bytes=32 time<1ms TTL=128
Reply from 190.108.10.30: bytes=32 time<1ms TTL=128

Ping statistics for 190.108.10.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 190.108.20.30
Pinging 190.108.20.30 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

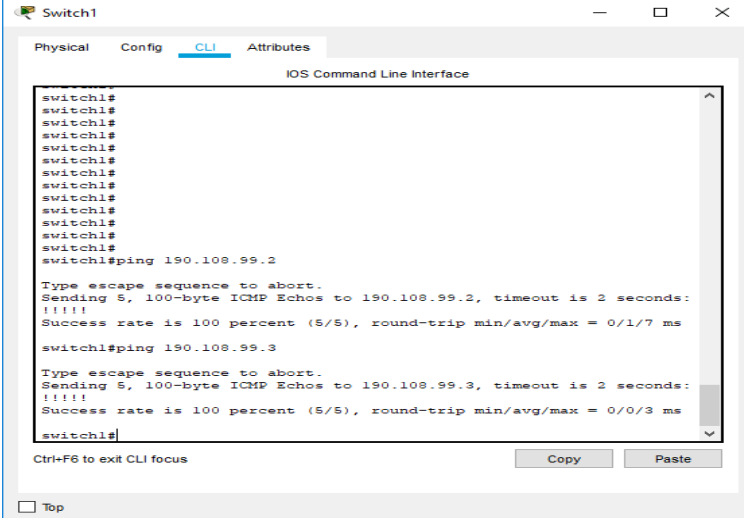
Ping statistics for 190.108.20.30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 190.108.30.30
Pinging 190.108.30.30 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

El ping es exitoso únicamente entre los PC's que se encuentran configurados en la misma VLAN

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

Figura 20. Conexión Switch Ping from SW1 to SW2 & SW3



```
Switch1
Physical Config CLI Attributes
IOS Command Line Interface

switch1#
switch1#
switch1#
switch1#
switch1#
switch1#
switch1#
switch1#
switch1#
switch1#
switch1#
switch1#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 = 0/1/7 ms
switch1#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 = 0/0/3 ms
switch1#
```

Figura 21. Conexión Switch Ping from SW2 to SW1 & SW3

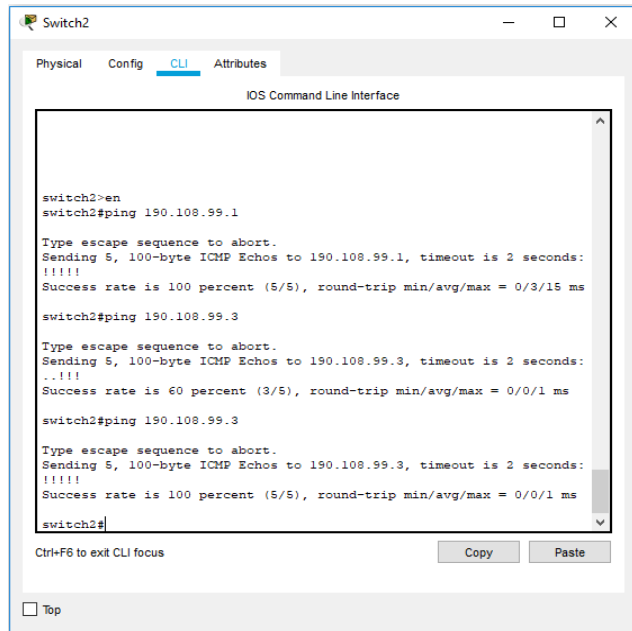
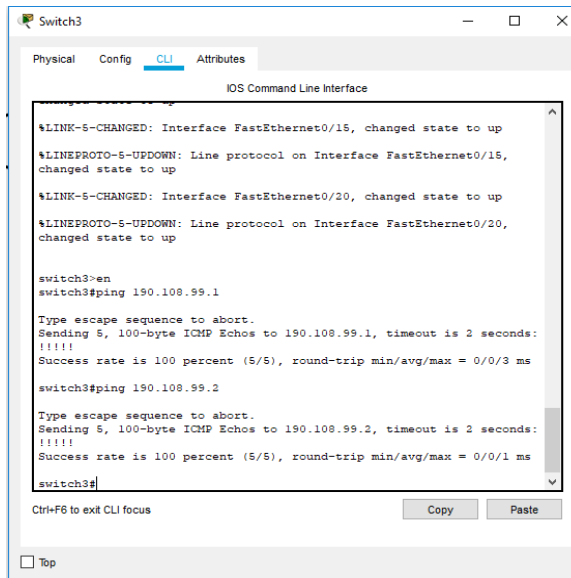


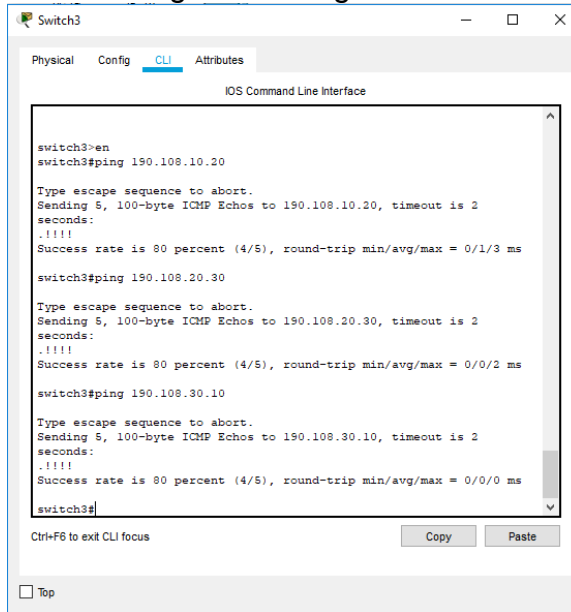
Figura 22. Conexión Switch Ping from SW3 to SW1 & SW2



La conectividad entre Switch es correcta y responde a ping debido a que los 3 switches se encuentran configurados respectivamente en la VLAN 99

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

Figura 23. Ping SWT3



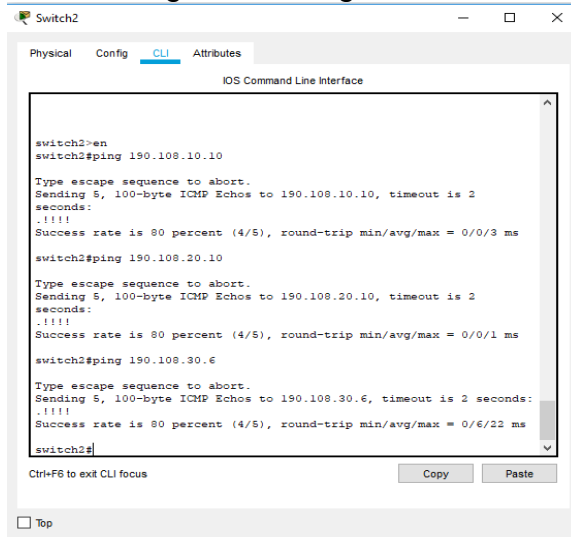
```
switch3>en
switch3#ping 190.108.10.20
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.20, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/1/3 ms

switch3#ping 190.108.20.30
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.30, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/2 ms

switch3#ping 190.108.30.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.30.10, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

switch3#
```

Figura 24 .Ping SWT2



```
switch2>en
switch2#ping 190.108.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.10.10, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/3 ms

switch2#ping 190.108.20.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.108.20.10, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

switch2#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 80 percent (4/5), round-trip min/avg/max = 0/6/22 ms

switch2#
```

El ping es exitoso debido a que la segmentación de redes distribuida entre VLAN's es correcta y proporciona la correcta conectividad a los Pc's, adicional los switchs tienen en sus tablas ARP la dirección MAC de todos los equipos conectados a las VLAN's por lo cual los pueden alcanzar

## CONCLUSIONES

- Por medio de VLAN podemos proporcionar un orden organizacional a una red robusta con el fin de distribuir segmentos y conectividad de redes y subredes
- Mediante protocolos de enrutamiento podemos interconectar routers cuyo segmento de red es diferente configurando de tal forma para determinar la ruta más viable para el envío correcto de paquetes de datos
- El diplomado de profundización CCNP nos permite adquirir habilidades de análisis y configuración para redes robustas

## REFERENCIAS

- Froom, R., Frahim, E. (2015). CISCO Press (Ed). Fundamentals Review. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115.
- Froom, R., Frahim, E. (2015). CISCO Press (Ed). Campus Network Design Fundamentals. Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide CCNP SWITCH 300-115
- Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Basic Network and Routing Concepts. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101.
- Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). EIGRP Implementation. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101