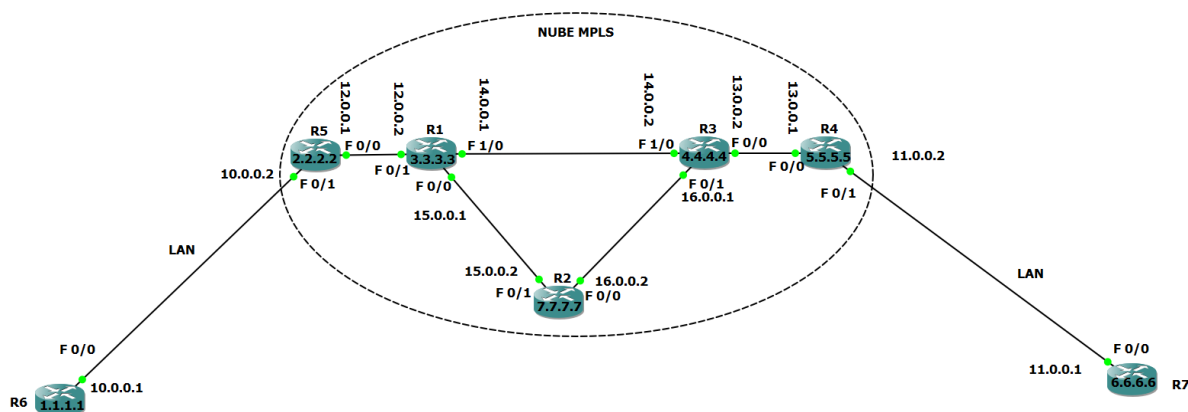


LABORATORIO VPN - MPLS

Tener presente, se debió configurar OSPF y MPLS solo en la nube MPLS, en los router R6 y R7, solo direccionamiento estático, para poder iniciar este laboratorio.



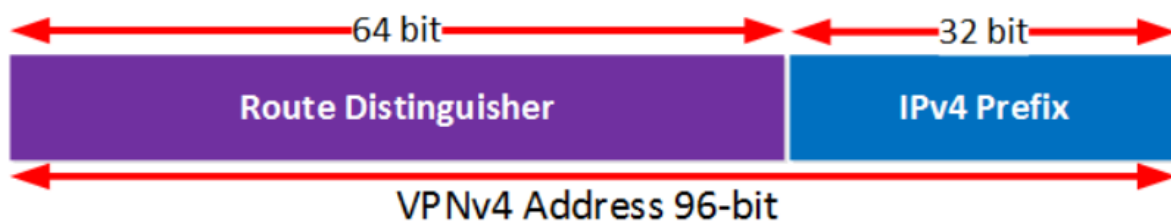
NOTA: las direcciones Loopback de los router R5-R6-R4-R7 deben tener mascara 32, así:

```
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
```

CREAR Y ASIGNAR VRF:

Los VRF permiten que el espacio de direcciones IP se reutilice entre dominios de enrutamiento aislados. Por ejemplo, suponga que tiene que conectarse a tres sitios de clientes, todos los cuales utilizan 192.168.0.0/24 como su red local. Podemos asignar a cada cliente su propio VRF para que las redes superpuestas se mantengan aisladas unas de otras en sus respectivos dominios de enrutamiento.

RD (Distinguidor de ruta)



Esto funciona bien, pero necesitamos una forma de realizar un seguimiento de qué ruta 192.168.0.0/24 pertenece a qué cliente. Aquí es donde entran los distintivos de ruta. Como su nombre lo indica, un distinguidor de ruta (RD), distingue un conjunto de rutas (un VRF) de otro. Es un número único antepuesto a cada ruta dentro de un VRF para identificarlo como perteneciente a ese VRF o

cliente en particular. Un RD se transporta junto con una ruta a través de BGP cuando se intercambian rutas VPN con otros enrutadores PE.

Utilizaremos un distintivo de ruta para cada VRF en forma de ASN:NN . En nuestro caso el ASN sería el sistema autónomo de la VRF de la institución Universidad de Manizales, escogimos 1, pero puede ser cualquier valor y el NN normalmente es una etiqueta para distinguir el usuario, en nuestro caso también escogimos el 1. La configuración VRF debe realizarse en ambos enrutadores PE.

Cuando las rutas VPN se anuncian entre los enrutadores PE a través de BGP, el RD se incluye como parte de la ruta junto con el prefijo IP. Por ejemplo, una ruta para 192.0.2.0/24 en VRF UM se anuncia efectivamente como 1: 1 : 192.0.2.0/24

RT - Route Targets (objetivo de ruta):

Example:

Route Target (8 bytes)	
Type 0	100:1
Type 1	192.168.1.1:1
Type 2	65538:10

Two types of RT:

- Export RT
- Import RT

Si los RD solo se usarán para indicar la VPN, la comunicación entre sitios de diferentes VPN sería problemática. Un sitio de la Compañía A no podría hablar con un sitio de la Compañía B porque los

RD no coincidiría. El concepto de tener sitios de la Compañía A que puedan comunicarse con los sitios de la Compañía B se llama extranet VPN. La comunicación entre sitios está controlada por otra función de VPN MPLS llamada RT.

Un RT es una comunidad extendida BGP que indica qué rutas deben importarse de BGP al VRF. El comando `route-target both` se utiliza como acceso directo para los dos comandos `route-target import` y `route-target export`, que aparecen por separado en la configuración en ejecución.

Para la configuración tendremos asignados los router de la siguiente manera:

R5: PE1

R4: PE2

R6: CE1

R7: CE2

La creación de las VRF se realiza solo en los router PE:

```
R5#configure term
Enter configuration commands, one per line.  End with CNTL/Z.
R5(config)#ip vrf UM
R5(config-vrf)#rd 1:1
R5(config-vrf)#route-target both 1:1
R5(config-vrf)#exit
```

```
R4#configure term
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#ip vrf UM
R4(config-vrf)#rd 1:1
R4(config-vrf)#route-target both 1:1
R4(config-vrf)#exit
```

Comando de verificación configuración:

```
R5#sh run | begin vrf
ip vrf UM
  rd 1:1
  route-target export 1:1
  route-target import 1:1
```

```
R4#sh run | begin vrf
ip vrf UM
  rd 1:1
  route-target export 1:1
  route-target import 1:1
```

Asignar las interfaces apropiadas a cada VRF y volver a aplicar sus direcciones IP. (Asignar una interfaz a un VRF automáticamente lo borra de cualquier dirección IP configurada.

```
R5(config)#interface fast 0/1
R5(config-if)#ip vrf forwarding UM
% Interface FastEthernet0/1 IP address 10.0.0.2 removed due to enabling VRF UM
R5(config-if)#ip address 10.0.0.2 255.255.255.252
R5(config-if)#exit
R5(config)#exit
```

```
R4(config)#interface fast 0/1
R4(config-if)#ip vrf forwarding UM
% Interface FastEthernet0/1 IP address 11.0.0.2 removed due to enabling VRF UM
R4(config-if)#ip address 11.0.0.2 255.255.255.252
R4(config-if)#exit
R4(config)#exit
```

El comando `show ip vrf interfaces` puede usarse para verificar la asignación y direccionamiento de la interfaz VRF.

```
R5#sh ip vrf interfaces
Interface          IP-Address      VRF          Protocol
Fa0/1              10.0.0.2        UM           up

R4#sh ip vrf inter
R4#sh ip vrf interfaces
Interface          IP-Address      VRF          Protocol
Fa0/1              11.0.0.2        UM           up
```

Para realizar un diagnóstico de comunicación, hacemos un ping vrf, así:

```
R5#ping vrf UM 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
R5#
R5#ping vrf UM 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/17/24 ms
--"
```

```
R4#ping vrf UM 11.0.0.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 11.0.0.1, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/37/64 ms
```

```
R4#
```

```
R4#ping vrf UM 11.0.0.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 11.0.0.2, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Tener en cuenta que la VRF solo se configure en los router PE, por tanto, en los router CE el ping se genera de forma normal.UM

```
R6#ping 10.0.0.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

```
R6#
```

```
R6#ping 10.0.0.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/15/24 ms
```

```
R7#ping 11.0.0.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 11.0.0.1, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
R7#
```

```
R7#ping 11.0.0.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 11.0.0.2, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/30/48 ms
```

,

CONFIGURAR BGP EN LOS ROUTER PE

Anunciar rutas VRF de un enrutador PE a otro, debemos configurar BGP este protocolo admite la publicación de rutas VPN, que son más largas que las rutas normales debido a la adición de un distintivo de ruta de 64 bits (que asignamos bajo la configuración VRF).

BGP se ejecuta solo en los enrutadores PE: los enrutadores P dependen completamente del proveedor IGP y MPLS para reenviar el tráfico a través de la red del proveedor, y los enrutadores CE no tienen conocimiento de rutas fuera de su propio VRF.

Ambos enrutadores PE existen en BGP AS 1, pero puede colocarse cualquier valor entre: 1-65535 en nuestro ejemplo utilizamos el número 1.

```
R5#configure term
Enter configuration commands, one per line.  End with CNTL/Z.
R5(config)#router bgp 1
R5(config-router)#neighbor 5.5.5.5 remote-as 1
R5(config-router)#neighbor 5.5.5.5 update-source loopback 0
R5(config-router)#address-family vpnv4
R5(config-router-af)#neighbor 5.5.5.5 activate
R5(config-router-af)#exit
R5(config-router)#exit
R5(config)#exit

R4#configure term
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#router bgp 1
R4(config-router)#neighbor 2.2.2.2 remote-as 1
R4(config-router)#neighbor 2.2.2.2 update-source loopback 0
R4(config-router)#address-family vpnv4
R4(config-router-af)#neighbor 2.2.2.2 activate
R4(config-router-af)#exit
R4(config-router)#
R4(config-router)#exit
R4(config)#exit
```

Con el siguiente comando podemos validar el correcto funcionamiento, observamos la configuración en ejecución del proceso BGP en cualquiera de los enrutadores PE, notamos que ha aparecido un poco más de configuración de la que proporcionamos.

Además de la familia de direcciones VPNv4, se han creado automáticamente familias de direcciones para los dos VRF del cliente. Además, se ha agregado soporte para cadenas comunitarias extendidas a la configuración vecina VPNv4 (resaltadas en color amarillo).

```

R5#sh running-config | section router bgp
router bgp 1
  bgp log-neighbor-changes
  neighbor 5.5.5.5 remote-as 1
  neighbor 5.5.5.5 update-source Loopback0
  !
  address-family ipv4
  neighbor 5.5.5.5 activate
  no auto-summary
  no synchronization
  exit-address-family
  !
  address-family vpnv4
  neighbor 5.5.5.5 activate
  neighbor 5.5.5.5 send-community extended
  exit-address-family
  !
  address-family ipv4 vrf UM
  no synchronization
  exit-address-family

```

Se debe comprobar si los enrutadores han formado una adyacencia vecina BGP, con el siguiente comando:

```

R5#sh bgp vpnv4 unicast all summary
BGP router identifier 2.2.2.2, local AS number 1
BGP table version is 1, main routing table version 1

Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
5.5.5.5       4     1      8       8        1    0   0 00:05:05      0
R5#

```

```

R4#sh bgp vpnv4 unicast all summary
BGP router identifier 5.5.5.5, local AS number 1
BGP table version is 1, main routing table version 1

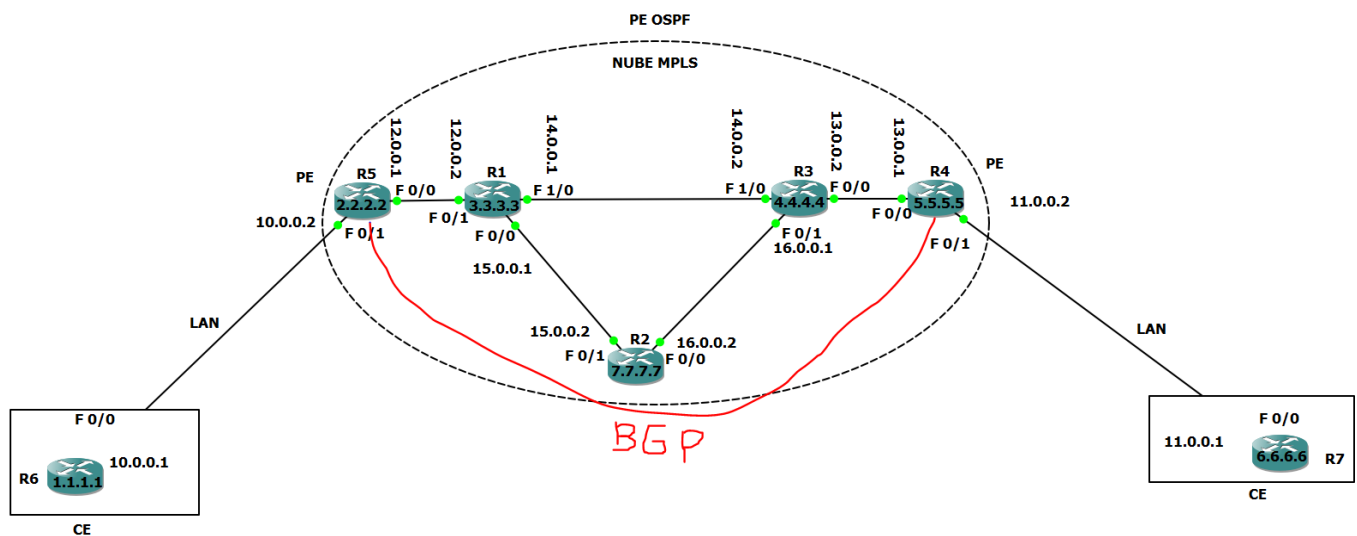
Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
2.2.2.2       4     1      9       9        1    0   0 00:06:16      0
R4#

```

CONFIGURAR PE – CE OSPF

Se configuró BGP entre los dos enrutadores PE. Ahora, configurar un IGP entre cada enrutador PE y sus enrutadores CE adjuntos para intercambiar rutas con los sitios del cliente. Usar OSPF para este laboratorio, pero podríamos usar fácilmente otro IGP como EIGRP o RIP.

Aunque estamos usando OSPF entre cada uno de los enrutadores CE y su enrutador PE, estos procesos OSPF están aislados de la topología OSPF del proveedor. La topología de enrutamiento general se verá así:



Asignar OSPF entre los router PE y CE:

```
R5#configure term
Enter configuration commands, one per line.  End with CNTL/Z.
R5(config)#router ospf 2 vrf UM
R5(config-router)#network 10.0.0.0 0.0.0.255 area 0
R5(config-router)#exit
R5(config)#exit
```



```
R4#configure term
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#router ospf 2 vrf UM
R4(config-router)#network 11.0.0.0 0.0.0.255 area 0
R4(config-router)#
R4(config-router)#
R4(config-router)#exit
R4(config)#exit
```

```
R6#configure term
Enter configuration commands, one per line.  End with CNTL/Z.
R6(config)#router ospf 2
R6(config-router)#network 10.0.0.0 0.0.0.255 area 0
R6(config-router)#network 1.1.1.1 0.0.0.0 area 0
R6(config-router)#exit
```

```
R7(config)#router ospf 2
R7(config-router)#network 11.0.0.0 0.0.0.255 area 0
R7(config-router)#network 6.6.6.6 0.0.0.0 area 0
R7(config-router)#exit
R7(config)#exit
```

Para verificar la configuración ingresamos el comando siguiente, el cual nos muestra si hay conectividad con el router CE que está conectado directamente por las interfaces físicas:

C – Directamente conectada

O – Fue notificada por OSPF

```
R5#sh ip route vrf UM
```

Routing Table: UM

Codes: 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

Gateway of last resort is not set

```

    1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1 [110/11] via 10.0.0.1, 00:01:43, FastEthernet0/1
    10.0.0.0/30 is subnetted, 1 subnets
C       10.0.0.0 is directly connected, FastEthernet0/1
```

```
R4#sh ip route vrf UM
```

```
Routing Table: UM
```

```
Codes: 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
```

```
Gateway of last resort is not set
```

```
6.0.0.0/32 is subnetted, 1 subnets  
O 6.6.6.6 [110/11] via 11.0.0.1, 00:03:39, FastEthernet0/1  
11.0.0.0/30 is subnetted, 1 subnets  
C 11.0.0.0 is directly connected, FastEthernet0/1
```

CONFIGURAR RUTA DE DISTRIBUCIÓN:

Se tiene la red troncal MPLS y BGP en funcionamiento, y los router CE están enviando rutas a los router PE dentro de sus VRF. El último paso es unir todo mediante la redistribución de rutas desde los procesos OSPF del lado del usuario (UM) a BGP y viceversa en los router PE.

Primero se configura la redistribución de rutas CE en cada VRF en BGP. Esto se realiza bajo la familia de direcciones BGP IPv4 para cada VRF.

```
R5#configure term  
Enter configuration commands, one per line. End with CNTL/Z.  
R5(config)#router bgp 1  
R5(config-router)#address-family ipv4 vrf UM  
R5(config-router-af)#redistribute ospf 2  
R5(config-router-af)#exit  
R5(config-router)#exit
```

```
R4#configure term  
Enter configuration commands, one per line. End with CNTL/Z.  
R4(config)#router bgp 1  
R4(config-router)#address-family ipv4 vrf UM  
R4(config-router-af)#redistribute ospf 2  
R4(config-router-af)#exit  
R4(config-router)#exit
```

Esto permite la redistribución de rutas OSPF en BGP para el transporte a través de la red de proveedores entre los dos sitios. Se puede verificar las rutas aprendidas de los sitios del usuario (las redes 1.1.1.1/32 y 6.6.6.6/32) ahora aparecen en las tablas BGP para sus respectivos VRF y las rutas VPNv4.

```
R5#sh ip bgp vpnv4 vrf UM
BGP table version is 9, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
Route Distinguisher: 1:1 (default for vrf UM)					
*> 1.1.1.1/32	10.0.0.1	11		32768	?
*>i6.6.6.6/32	5.5.5.5	11	100	0	?
*> 10.0.0.0/30	0.0.0.0	0		32768	?
*>i11.0.0.0/30	5.5.5.5	0	100	0	?

```
R4#sh ip bgp vpnv4 vrf UM
BGP table version is 9, local router ID is 5.5.5.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
Route Distinguisher: 1:1 (default for vrf UM)					
*>i1.1.1.1/32	2.2.2.2	11	100	0	?
*> 6.6.6.6/32	11.0.0.1	11		32768	?
*>i10.0.0.0/30	2.2.2.2	0	100	0	?
*> 11.0.0.0/30	0.0.0.0	0		32768	?

El último paso es completar la redistribución en la dirección opuesta: de BGP a los procesos OSPF del usuario.

```
R5#configure term
Enter configuration commands, one per line. End with CNTL/Z.
R5(config)#router ospf 2
R5(config-router)#redistribute bgp 1 subnets
R5(config-router)#exit
R5(config)#exit
```

```

R4#configure term
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#router ospf 2
R4(config-router)#redistribute bgp 1 subnets
R4(config-router)#exit
R4(config)#exit

```

Ya está toda la configuración realizada.

VERIFICACIÓN:

Validación de conectividad de extremo a extremo entre los enrutadores CE dentro de cada VRF. Ambos router para cada usuario deben tener tablas de enrutamiento completas:

```

R6#sh ip route
Codes: 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

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
C        1.1.1.1 is directly connected, Loopback0
      6.0.0.0/32 is subnetted, 1 subnets
O IA     6.6.6.6 [110/21] via 10.0.0.2, 02:51:23, FastEthernet0/0
      10.0.0.0/30 is subnetted, 1 subnets
C        10.0.0.0 is directly connected, FastEthernet0/0
      11.0.0.0/30 is subnetted, 1 subnets
O IA     11.0.0.0 [110/11] via 10.0.0.2, 02:51:23, FastEthernet0/0

```

```

R7#sh ip route
Codes: 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

Gateway of last resort is not set

      1.0.0.0/32 is subnetted, 1 subnets
O IA     1.1.1.1 [110/21] via 11.0.0.2, 02:52:19, FastEthernet0/0
      6.0.0.0/32 is subnetted, 1 subnets
C        6.6.6.6 is directly connected, Loopback0
      10.0.0.0/30 is subnetted, 1 subnets
O IA     10.0.0.0 [110/11] via 11.0.0.2, 02:52:19, FastEthernet0/0
      11.0.0.0/30 is subnetted, 1 subnets
C        11.0.0.0 is directly connected, FastEthernet0/0

```

Se observa que las rutas OSPF enviadas entre dos sitios que pertenecen al mismo cliente aparecen como rutas entre áreas (IA). Deberíamos poder hacer ping desde un router CE a otro. (no necesitamos especificar un VRF al hacerlo porque los enrutadores CE no tienen conocimiento de que están en un VRF).

```
R6#ping 6.6.6.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/76/124 ms
R6#
R6#ping 6.6.6.6 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 6.6.6.6, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/70/96 ms
```

```
R7#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/80/100 ms
R7#
R7#ping 1.1.1.1 source loopback 0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 6.6.6.6
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/79/108 ms
```

También podemos realizar un seguimiento de la ruta:

```
R6#traceroute 6.6.6.6

Type escape sequence to abort.
Tracing the route to 6.6.6.6

 0 10.0.0.2 24 msec 40 msec 32 msec
 1 12.0.0.2 [MPLS: Labels 20/25 Exp 0] 84 msec 108 msec 92 msec
 2 14.0.0.2 [MPLS: Labels 16/25 Exp 0] 76 msec 80 msec 96 msec
 3 11.0.0.2 [MPLS: Label 25 Exp 0] 100 msec 48 msec 40 msec
 4 11.0.0.1 112 msec 80 msec 112 msec
```

```

R7#traceroute 1.1.1.1

Type escape sequence to abort.
Tracing the route to 1.1.1.1

 0 11.0.0.2 36 msec 28 msec 24 msec
 1 13.0.0.2 [MPLS: Labels 19/25 Exp 0] 84 msec 76 msec 100 msec
 2 14.0.0.1 [MPLS: Labels 18/25 Exp 0] 76 msec 76 msec 72 msec
 3 10.0.0.2 [MPLS: Label 25 Exp 0] 32 msec 68 msec 40 msec
 4 10.0.0.1 76 msec 32 msec 72 msec

```

Se puede observar la etiqueta de transporte 20 y la etiqueta VPN 25 en CE1

La etiqueta de transporte 19 y la etiqueta VPN 25 en CE2

En conclusión, lo que se realizó fue que los router CE anuncian rutas a los router PE que los redistribuyen en BGP para que se conviertan en rutas VPNv4, estas rutas se intercambian de un router PE a otro.

```

R5#sh mpls forwarding-table
Local  Outgoing  Prefix      Bytes tag  Outgoing     Next Hop
tag    tag or VC  or Tunnel Id switched   interface
16     Pop tag    14.0.0.0/24 0          Fa0/0       12.0.0.2
17     Untagged   3.3.3.3/32  0          Fa0/0       12.0.0.2
18     Pop tag    15.0.0.0/24 0          Fa0/0       12.0.0.2
19     16         16.0.0.0/24 0          Fa0/0       12.0.0.2
20     17         13.0.0.0/24 0          Fa0/0       12.0.0.2
21     19         4.4.4.4/32  0          Fa0/0       12.0.0.2
22     20         5.5.5.5/32  0          Fa0/0       12.0.0.2
23     21         7.7.7.7/32  0          Fa0/0       12.0.0.2
24     22         193.10.10.0/24 0          Fa0/0       12.0.0.2
25     Untagged   1.1.1.1/32[V] 12600      Fa0/1       10.0.0.1
26     Aggregate 10.0.0.0/30[V] 5064

```

```

R4#s mpls forwar
R4#show mpls forwarding-table
Local  Outgoing  Prefix      Bytes tag  Outgoing     Next Hop
tag    tag or VC  or Tunnel Id switched   interface
16     Untagged   4.4.4.4/32  0          Fa0/0       13.0.0.2
17     Pop tag    14.0.0.0/24 0          Fa0/0       13.0.0.2
18     Pop tag    16.0.0.0/24 0          Fa0/0       13.0.0.2
19     17         15.0.0.0/24 0          Fa0/0       13.0.0.2
20     18         12.0.0.0/24 0          Fa0/0       13.0.0.2
21     19         2.2.2.2/32  0          Fa0/0       13.0.0.2
22     20         3.3.3.3/32  0          Fa0/0       13.0.0.2
23     21         7.7.7.7/32  0          Fa0/0       13.0.0.2
24     22         193.10.10.0/24 0          Fa0/0       13.0.0.2
25     Untagged   6.6.6.6/32[V] 10830      Fa0/1       11.0.0.1
26     Aggregate 11.0.0.0/30[V] 6104

```

También podemos validar que las tablas LFIB cambiaron, aunque solo en los router PE y se ingresaron etiquetas agregadas (Aggregate), son asignadas por enrutadores (PE) en el contexto MPLS - VPN a todas las direcciones IP locales para un VRF dado para ahorrar espacio en la etiqueta.