Servicios y funciones de IOS XR L2VPN

Contenido

Introducción
1. Servicios punto a punto y multipunto
1.1 Servicio Point-to-Point
1.2 Servicio multipunto
2. Circuitos de acoplamiento
2.1 Circuito virtual Ethernet ASR 9000
2.1.1 Coincidencia de interfaz entrante
2.1.2 Manipulación de VLAN
2.2 Comportamiento del router Cisco IOS XR sin EVC (CRS y XR12000)
3. Servicio Point-to-Point
3.1 Conmutación local
3.1.1 Interfaz principal
3.1.2 Subinterfaces y manipulación de VLAN
3.2 Servicios de cable privado virtual
3.2.1 Descripción general
3.2.2 Estado de acoplamiento de CA y PW
3.2.3 PW de tipo 4 y tipo 5
3.2.4 PW multisegmento
3.2.5 Redundancia
3.3 CDP
3.3.1 CDP no habilitado en la interfaz principal de L2VPN PE
3.3.2 CDP habilitado en la interfaz principal de L2VPN PE
3.4 Árbol de extensión
4. Servicio multipunto
4.1 Conmutación local
4.2 MST completo
4.3 BVI
4.4 VPLS
4.4.1 Descripción general
4.4.2 Tipos de PW y etiquetas transportadas
4.4.3 Detección automática y señalización
4.4.4 Vaciados y retiradas de MAC
4.4.5 H-VPLS
4.4.6 Grupos de horizontes divididos (SHG)
4.4.7 Redundancia
4.5 Control de tormentas de tráfico
4.6 Movimientos de MAC

4.7 Detección IGMP y MLD
5. Temas adicionales sobre L2VPN
5.1 Equilibrio de carga
5.2 Registro
5.3 ethernet-services access-list
5.4 ethernet egress-filter

Introducción

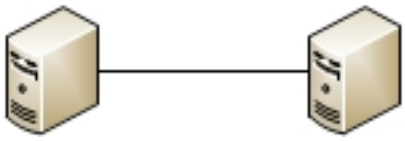
Este documento describe las topologías básicas de VPN de capa 2 (L2) (L2VPN). Es útil presentar ejemplos básicos para demostrar el diseño, los servicios, las características y la configuración. Consulte la Guía de Configuración de Servicios Ethernet y L2VPN del Router de Servicios de Agregación de la Serie ASR 9000 de Cisco, Versión 4.3.x para obtener información adicional.

1. Servicios punto a punto y multipunto

La función L2VPN proporciona la capacidad de proporcionar servicios punto a punto y multipunto.

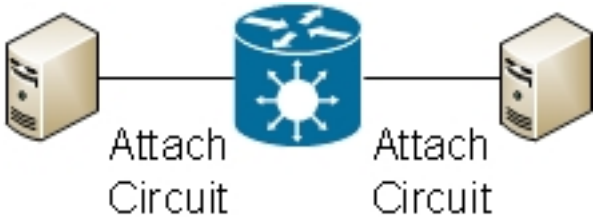
1.1 Servicio Point-to-Point

El servicio punto a punto básicamente emula un circuito de transporte entre dos nodos extremos para que los nodos extremos parezcan estar conectados directamente sobre un link punto a punto. Se puede utilizar para conectar dos sitios.

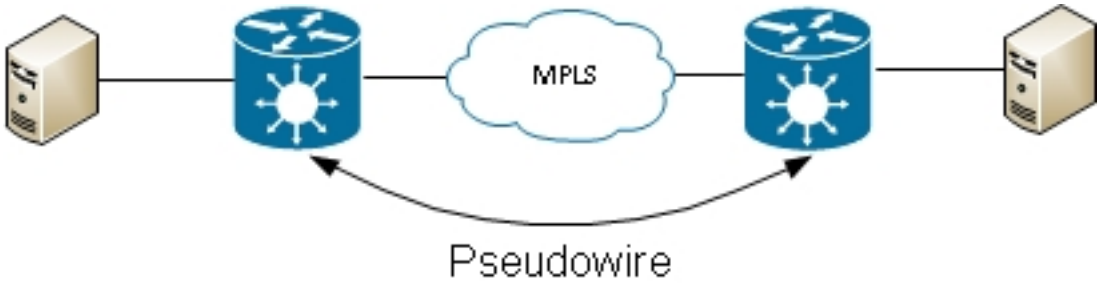


En realidad, puede haber varios routers entre los dos nodos extremos y puede haber varios diseños para proporcionar el servicio punto a punto.

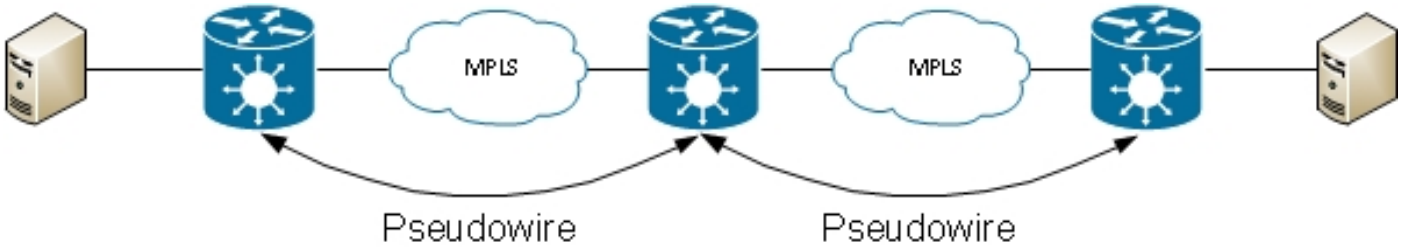
Un router puede realizar el switching local entre dos de sus interfaces:



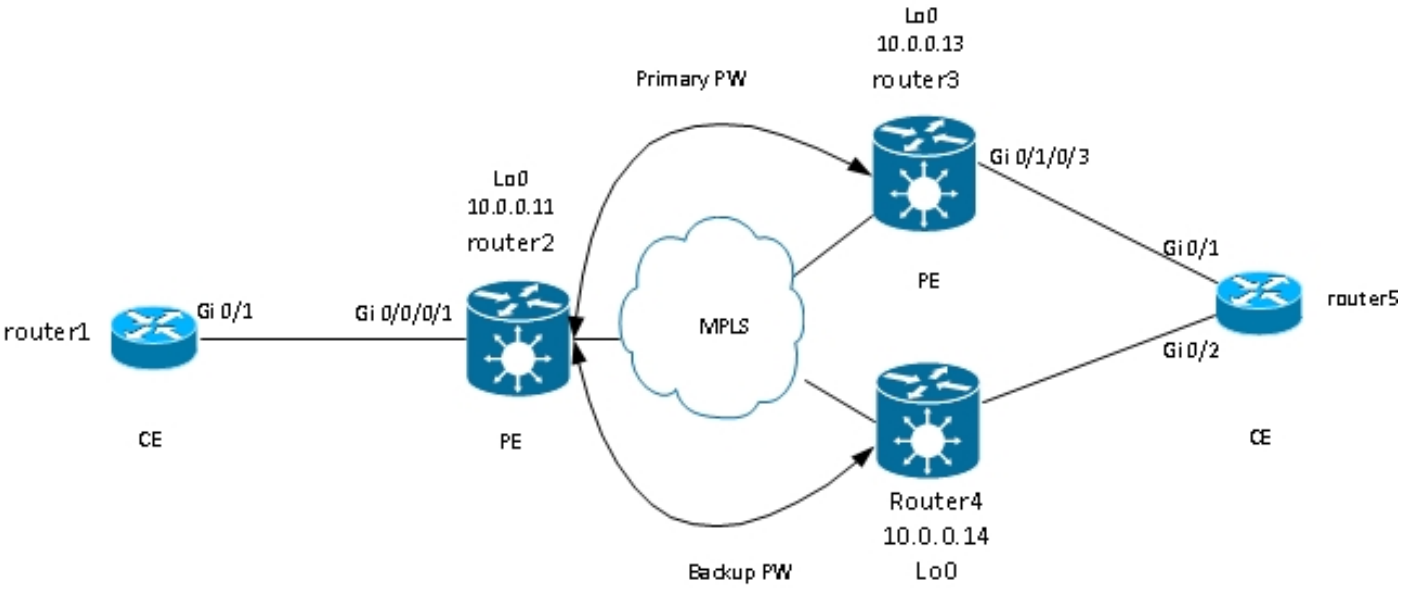
También puede haber un pseudowire (PW) de Multiprotocol Label Switching (MPLS) entre dos routers:



Un router puede conmutar tramas entre dos PW; en este caso, se trata de un PW multisegmento:



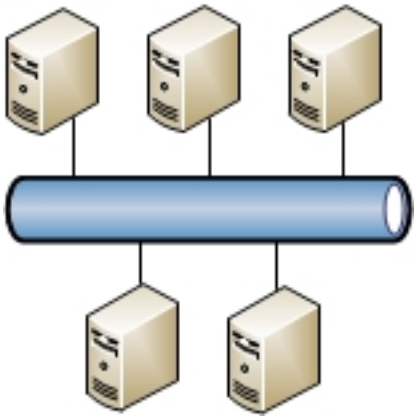
La redundancia está disponible a través de la función de redundancia PW:



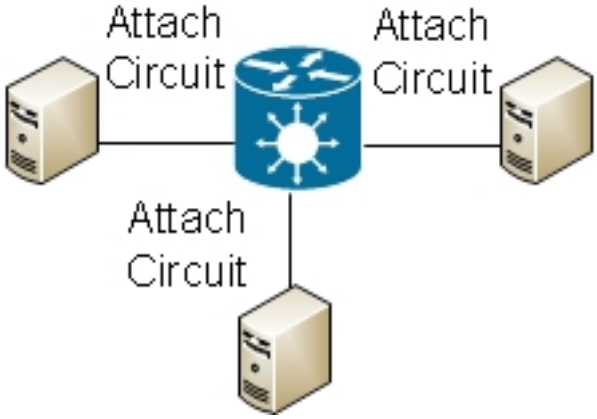
Hay otros diseños disponibles, pero no todos pueden aparecer aquí.

1.2 Servicio multipunto

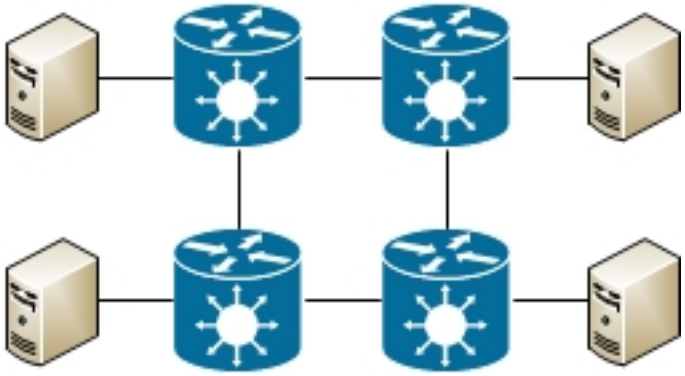
El servicio multipunto emula un dominio de difusión para que todos los hosts conectados en ese dominio de puente parezcan estar conectados lógicamente al mismo segmento Ethernet:



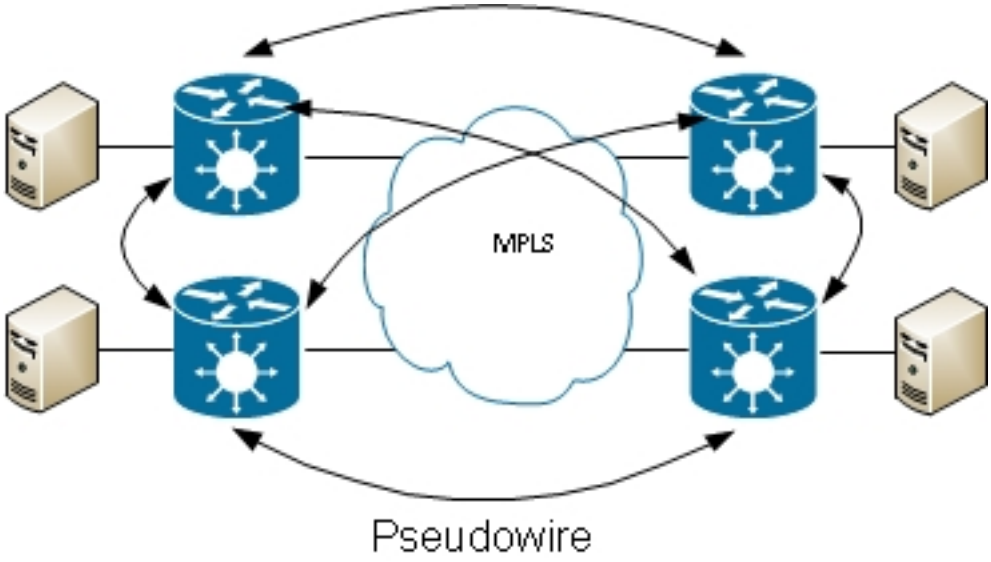
Todos los hosts se pueden conectar al mismo router/switch:



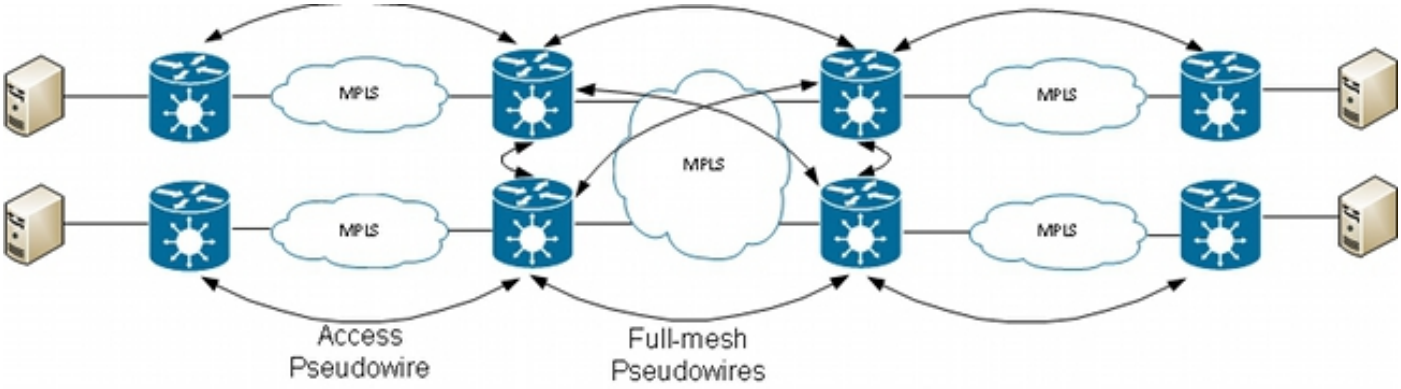
Varios switches pueden realizar la conmutación Ethernet tradicional; se debe utilizar el árbol de expansión para romper los loops:



Los servicios de LAN privada virtual (VPLS) le permiten ampliar el dominio de difusión entre varios sitios mediante MPLS PW:



VPLS jerárquico se puede utilizar para aumentar la escalabilidad:



2. Circuitos de acoplamiento

2.1 Circuito virtual Ethernet ASR 9000

2.1.1 Coincidencia de interfaz entrante

Las reglas básicas para los circuitos de conexión (AC) incluyen:

- Se debe recibir un paquete en una interfaz configurada con la palabra clave *l2transport* para que la función L2VPN lo procese.
- Esta interfaz puede ser una interfaz principal, donde el comando **l2transport** se configura en el modo de configuración de la interfaz, o una subinterfaz, donde la palabra clave *l2transport* se configura después del número de la subinterfaz.
- Una búsqueda de coincidencias más larga determina la interfaz entrante del paquete. La búsqueda de coincidencias más larga verifica estas condiciones en este orden para hacer coincidir el paquete entrante con una subinterfaz:

    1. La trama entrante tiene dos etiquetas dot1q y coincide con una subinterfaz configurada con las mismas dos etiquetas dot1q (tunelización 802.1Q o QinQ). Esta es la coincidencia

más larga posible.
2. La trama entrante tiene dos etiquetas dot1q y coincide con una subinterfaz configurada con la misma etiqueta dot1q first y *any* para la segunda etiqueta.
3. La trama entrante tiene una etiqueta dot1q y coincide con una subinterfaz configurada con la misma etiqueta dot1q y la palabra clave *exact*.
4. La trama entrante tiene una o más etiquetas dot1q y coincide con una subinterfaz configurada con una de las etiquetas dot1q.
5. La trama entrante no tiene etiquetas dot1q y coincide con una subinterfaz configurada con el comando **encapsulation untagged**.
6. La trama entrante no coincide con ninguna otra subinterfaz, por lo que coincide con una subinterfaz configurada con el comando **encapsulation default**.
7. La trama entrante no coincide con ninguna otra subinterfaz, por lo que coincide con la interfaz principal configurada para *l2transport*.

- En los routers tradicionales que no utilizan el modelo de conexión virtual Ethernet (EVC), las etiquetas VLAN configuradas bajo la subinterfaz se eliminan (saltan) de la trama antes de que sean transportadas por la función L2VPN.
- En un router de servicios de agregación de la serie ASR 9000 de Cisco que utiliza la infraestructura de EVC, la acción predeterminada es conservar las etiquetas existentes. Utilice el comando **rewrite** para modificar el valor predeterminado.
- Si hay una Interfaz Virtual de Bridge (BVI) en el dominio de bridge, todas las etiquetas entrantes deben ser reventadas porque la BVI es una interfaz ruteada sin ninguna etiqueta. Consulte la sección BVI para obtener más información.

Estos son algunos ejemplos que ilustran estas reglas:

1. Un ejemplo básico es cuando todo el tráfico recibido en un puerto físico debe ser transportado, tenga o no una etiqueta VLAN. Si configura **l2transport** en la interfaz principal, la función L2VPN transporta todo el tráfico recibido en ese puerto físico:

```
interface GigabitEthernet0/0/0/2
l2transport
```

   Si hay subinterfaces de esa interfaz principal, la interfaz principal detecta cualquier trama que no haya coincidido con ninguna subinterfaz; esta es la regla de coincidencia más larga.

2. Las interfaces y subinterfaces del paquete se pueden configurar como l2transport:

```
interface Bundle-Ether1
l2transport
```

3. Utilice **encapsulation default** bajo una subinterfaz l2transport para hacer coincidir cualquier tráfico etiquetado o no etiquetado que no haya sido coincidente por otra subinterfaz con una coincidencia más larga. (Consulte El Ejemplo 4). La palabra clave *l2transport* se configura en el nombre de la subinterfaz, no en la subinterfaz como en la interfaz principal:

```
interface GigabitEthernet0/1/0/3.1 l2transport
encapsulation default
```

   Configure **encapsulation untagged** si desea que sólo coincidan las tramas no etiquetadas.

4. Cuando haya varias subinterfaces, ejecute la prueba de coincidencia más larga en la trama entrante para determinar la interfaz entrante:

```
interface GigabitEthernet0/1/0/3.1 l2transport
encapsulation default
!
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
!
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 2 second-dot1q 3
```

   En esta configuración, tenga en cuenta que:

   - Una trama QinQ con una etiqueta VLAN externa 2 y una etiqueta VLAN interna 3 podría coincidir con las subinterfaces .1, .2 o .3, pero está asignada a la subinterfaz .3 debido a la regla de coincidencia más larga. Dos etiquetas en .3 son más largas que una etiqueta en .2 y más largas que ninguna etiqueta en .1.
   - Una trama QinQ con una etiqueta VLAN externa 2 y una etiqueta VLAN interna 4 se asigna a la subinterfaz .2 porque la **encapsulación dot1q 2** puede coincidir con tramas dot1q con solo la etiqueta VLAN 2, pero también puede coincidir con tramas QinQ con una etiqueta externa 2. Consulte el Ejemplo 5 (la palabra clave *exact*) si no desea hacer coincidir las tramas QinQ.
   - Una trama QinQ con una etiqueta VLAN externa 3 coincide con la subinterfaz .1.
   - Una trama dot1q con una etiqueta VLAN 2 coincide con la subinterfaz .2.
   - Una trama dot1q con una etiqueta VLAN 3 coincide con la subinterfaz .1.

5. Para hacer coincidir una trama dot1q y no una trama QinQ, utilice la palabra clave *exact*:

```
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2 exact
```

   Esta configuración no coincide con las tramas QinQ con una etiqueta VLAN externa 2 porque sólo coincide con tramas con exactamente una etiqueta VLAN.

6. Utilice la palabra clave *untagged* para hacer coincidir sólo las tramas sin etiqueta, como los paquetes de Cisco Discovery Protocol (CDP) o las unidades de datos de protocolo de puente de árbol de extensión múltiple (MST) (BPDU):

```
interface GigabitEthernet0/1/0/3.1 l2transport
encapsulation default
!
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation untagged
!
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
```

   En esta configuración, tenga en cuenta que:

   - Las tramas Dot1q con una etiqueta VLAN 3 o las tramas QinQ con una etiqueta externa 3 coinciden con las subinterfaces .3.

- El resto de las tramas dot1q o QinQ coinciden con la subinterfaz .1.
- Las tramas sin una etiqueta VLAN coinciden con la subinterfaz .2.

7. La palabra clave *any* se puede utilizar como comodín:

```
interface GigabitEthernet0/1/0/3.4 l2transport
encapsulation dot1q 4 second-dot1q any
!
interface GigabitEthernet0/1/0/3.5 l2transport
encapsulation dot1q 4 second-dot1q 5
```

Ambas subinterfaces .4 y .5 podrían coincidir con tramas QinQ con etiquetas 4 y 5, pero las tramas se asignan a las subinterfaces .5 porque son más específicas. Esta es la regla de coincidencia más larga.

8. Se pueden utilizar rangos de etiquetas VLAN:

```
interface GigabitEthernet0/1/0/3.6 l2transport
encapsulation dot1q 6-10
```

9. Se pueden enumerar múltiples valores o rangos de etiquetas VLAN para la primera o segunda etiqueta dot1q:

```
interface GigabitEthernet0/1/0/3.7 l2transport
encapsulation dot1q 6 , 7 , 8-10
!
interface GigabitEthernet0/1/0/3.11 l2transport
encapsulation dot1q 11 second-dot1q 1 , 2 , 3 , 4-6 , 10
```

Puede enumerar un máximo de nueve valores. Si se requieren más valores, se deben asignar a otra subinterfaz. Agrupe los valores en un rango para acortar la lista.

10. El comando **encapsulation dot1q second-dot1q** utiliza el Ethertype 0x8100 para las etiquetas externas e internas porque este es el método de Cisco para encapsular tramas QinQ. Sin embargo, según IEEE, el Ethertype 0x8100 debe reservarse para tramas 802.1q con una etiqueta VLAN, y una etiqueta externa con Ethertype 0x88a8 debe utilizarse para tramas QinQ. La etiqueta externa con Ethertype 0x88a8 se puede configurar con la palabra clave *dot1ad*:

```
interface GigabitEthernet0/1/0/3.12 l2transport
encapsulation dot1ad 12 dot1q 100
```

11. Para utilizar el antiguo Ethertype 0x9100 o 0x9200 para las etiquetas externas QinQ, utilice el comando **dot1q tunneling ethertype** en la interfaz principal de la subinterfaz QinQ:

```
interface GigabitEthernet0/1/0/3
 dot1q tunneling ethertype [0x9100|0x9200]
!
interface GigabitEthernet0/1/0/3.13 l2transport
encapsulation dot1q 13 second-dot1q 100
```

La etiqueta externa tiene un Ethertype de 0x9100 o 0x9200, y la etiqueta interna tiene el

dot1q Ethertype 0x8100.

12. Una trama entrante se puede asignar a una subinterfaz, según la dirección MAC de origen:

```
interface GigabitEthernet0/1/0/3.14 l2transport
encapsulation dot1q 14 ingress source-mac 1.1.1
```

2.1.2 Manipulación de VLAN

El comportamiento predeterminado de una plataforma basada en EVC es mantener las etiquetas VLAN en la trama entrante.

```
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
```

En esta configuración, una trama dot1q entrante con una etiqueta VLAN 3 mantiene su etiqueta VLAN 3 cuando se reenvía la trama. Una trama QinQ entrante con una etiqueta VLAN externa 3 y una etiqueta interna 100 mantiene ambas etiquetas sin cambios cuando se reenvía la trama.

Sin embargo, la infraestructura de EVC le permite manipular las etiquetas con el comando **rewrite**, de modo que pueda hacer pop (quitar), traducir o empujar (agregar) etiquetas a la pila de etiquetas de VLAN entrante.

Aquí hay varios ejemplos:

- La palabra clave *pop* le permite quitar una etiqueta QinQ de una trama dot1q entrante. Este ejemplo quita la etiqueta externa 13 de la trama QinQ entrante y reenvía la trama con la etiqueta dot1q 100 en la parte superior:

```
interface GigabitEthernet0/1/0/3.13 l2transport
encapsulation dot1q 13 second-dot1q 100
rewrite ingress tag pop 1 symmetric
```

El comportamiento es siempre simétrico, lo que significa que la etiqueta externa 13 se abre en la dirección de ingreso y se empuja en la dirección de egreso.

- La palabra clave *translate* le permite reemplazar una o dos etiquetas entrantes por una o dos etiquetas nuevas:

```
RP/0/RSP0/CPU0:router2(config-subif)#interface GigabitEthernet0/1/0/3.3
l2transport
RP/0/RSP0/CPU0:router2(config-subif)# encapsulation dot1q 3
RP/0/RSP0/CPU0:router2(config-subif)#rewrite ingress tag translate ?
1-to-1 Replace the outermost tag with another tag
1-to-2 Replace the outermost tag with two tags
2-to-1 Replace the outermost two tags with one tag
2-to-2 Replace the outermost two tags with two other tags
RP/0/RSP0/CPU0:router2(config-subif)#rewrite ingress tag translate 1-to-1 ?
dot1ad Push a Dot1ad tag
dot1q Push a Dot1Q tag
RP/0/RSP0/CPU0:router2(config-subif)#rewrite ingress tag translate 1-to-1
dot1q 4
RP/0/RSP0/CPU0:router2(config-subif)#show config
```

```
Building configuration...
!! IOS XR Configuration 4.3.0
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
rewrite ingress tag translate 1-to-1 dot1q 4 symmetric
!
end
```

La palabra clave *symmetric* se agrega automáticamente porque es el único modo admitido.

- La palabra clave *push* le permite agregar una etiqueta QinQ a una trama dot1q entrante:

```
interface GigabitEthernet0/1/0/3.4 l2transport
encapsulation dot1q 4
rewrite ingress tag push dot1q 100 symmetric
```

Una etiqueta QinQ externa 100 se agrega a la trama entrante con una etiqueta dot1q 4. En la dirección de salida, aparece la etiqueta QinQ.

2.2 Comportamiento del router Cisco IOS XR sin EVC (CRS y XR12000)

La sintaxis para la coincidencia de VLAN en las plataformas que no son EVC no utiliza la palabra clave *encapsulation*:

```
RP/0/RP0/CPU0:router1#config
RP/0/RP0/CPU0:router1(config)#int gig 0/0/0/2.3 l2transport
RP/0/RP0/CPU0:router1(config-subif)#dot1q ?
vlan Configure a VLAN ID on the subinterface
RP/0/RP0/CPU0:router1(config-subif)#dot1q vlan ?
<1-4094> Configure first (outer) VLAN ID on the subinterface
RP/0/RP0/CPU0:router1(config-subif)#dot1q vlan 3 ?
<1-4094> Configure second (inner 802.1Q) VLAN ID on the subinterface
any Match frames with any second 802.1Q VLAN ID

RP/0/RP0/CPU0:router1(config-subif)#dot1q vlan 3 100
```

La manipulación de etiquetas VLAN no se puede configurar, porque el único comportamiento posible es hacer estallar todas las etiquetas que se especifican en los comandos **dot1q** o **dot1ad**. Esto se hace de forma predeterminada, por lo que no hay ningún comando **rewrite**.

3. Servicio Point-to-Point

Notas:

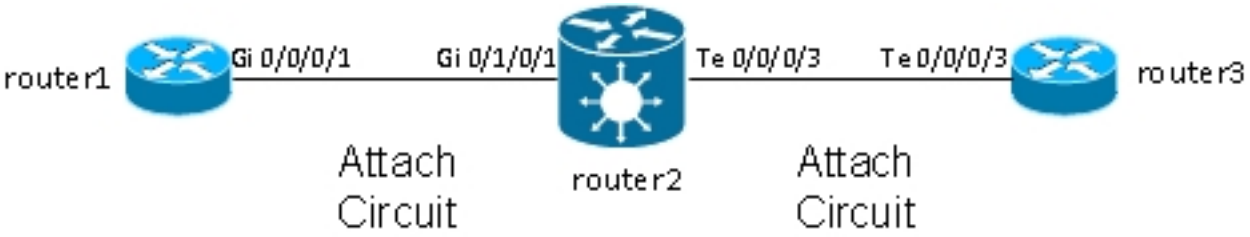
Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

3.1 Conmutación local

3.1.1 Interfaz principal

La topología básica es una conexión cruzada local entre dos interfaces principales:



El Router2 toma todo el tráfico recibido en Gi 0/1/0/1 y lo reenvía a Te 0/0/0/3 y viceversa.

Aunque el router1 y el router3 parecen tener un cable directo adosado en esta topología, este no es el caso porque el router2 se traduce realmente entre las interfaces TenGigE y GigabitEthernet. El Router 2 puede ejecutar funciones en estas dos interfaces; una lista de control de acceso (ACL), por ejemplo, puede descartar tipos específicos de paquetes o un policy-map para dar forma o limitar la velocidad del tráfico de baja prioridad.

Se configura una conexión cruzada punto a punto básica entre dos interfaces principales que se configuran como l2transport en el router2:

```
interface GigabitEthernet0/1/0/1
l2transport
!
!
interface TenGigE0/0/0/3
l2transport
!
!
l2vpn
xconnect group test
p2p p2p1
interface TenGigE0/0/0/3
interface GigabitEthernet0/1/0/1
!
```

En el router1 y el router3, las interfaces principales se configuran con CDP y una dirección IPv4:

```
RP/0/RP0/CPU0:router1#sh run int Gi 0/0/0/1
interface GigabitEthernet0/0/0/1
cdp
ipv4 address 10.1.1.1 255.255.255.0
!

RP/0/RP0/CPU0:router1#
RP/0/RP0/CPU0:router1#sh cdp nei Gi 0/0/0/1
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater

Device ID Local Intrfce Holdtme Capability Platform Port ID
router3.cisco.c Gi0/0/0/1        132     R          ASR9K Ser Te0/0/0/3
RP/0/RP0/CPU0:router1#ping 10.1.1.2
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/8/32 ms
```

El Router1 ve al Router3 como un vecino CDP y puede hacer ping a 10.1.1.2 (la dirección de interfaz del Router3) como si los dos routers estuvieran conectados directamente.

Debido a que no hay ninguna subinterfaz configurada en el router2, las tramas entrantes con una etiqueta VLAN se transportan de manera transparente cuando las subinterfaces dot1q se configuran en el router1 y el router3:

```
RP/0/RP0/CPU0:router1#sh run int gig 0/0/0/1.2
interface GigabitEthernet0/0/0/1.2
ipv4 address 10.1.2.1 255.255.255.0
dot1q vlan 2
!

RP/0/RP0/CPU0:router1#ping 10.1.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/5 ms
```

Después de 10,000 pings del router1 al router3, puede utilizar los comandos **show interface** y **show l2vpn** para asegurarse de que las solicitudes de ping recibidas por el router2 en una CA se reenvíen en la otra CA y que las respuestas de ping se manejen de la misma manera en sentido inverso.

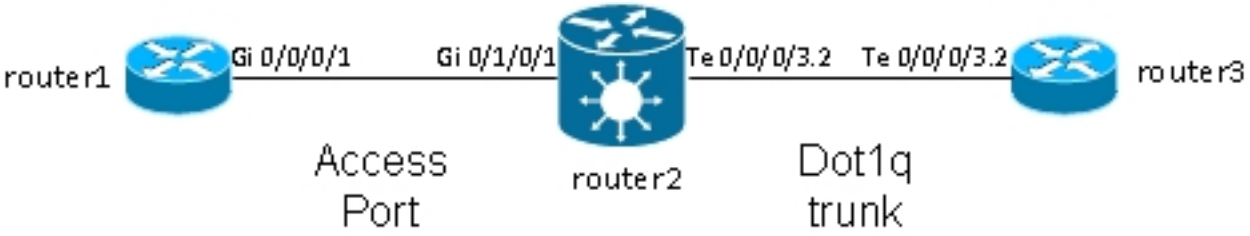
```
RP/0/RSP0/CPU0:router2#sh int gig 0/1/0/1
GigabitEthernet0/1/0/1 is up, line protocol is up
Interface state transitions: 1
Hardware is GigabitEthernet, address is 0024.986c.63f1 (bia 0024.986c.63f1)
Description: static lab connection to acdc 0/0/0/1 - dont change
Layer 2 Transport Mode
MTU 1514 bytes, BW 1000000 Kbit (Max: 1000000 Kbit)
reliability 255/255, txload 0/255, rxload 0/255
Encapsulation ARPA,
Full-duplex, 1000Mb/s, SXFD, link type is force-up
output flow control is off, input flow control is off
loopback not set,
Last input 00:00:00, output 00:00:00
Last clearing of "show interface" counters 00:01:07
5 minute input rate 28000 bits/sec, 32 packets/sec
5 minute output rate 28000 bits/sec, 32 packets/sec
10006 packets input, 1140592 bytes, 0 total input drops
0 drops for unrecognized upper-level protocol
Received 0 broadcast packets, 6 multicast packets
0 runts, 0 giants, 0 throttles, 0 parity
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
10007 packets output, 1140832 bytes, 0 total output drops
Output 0 broadcast packets, 7 multicast packets
0 output errors, 0 underruns, 0 applique, 0 resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions


RP/0/RSP0/CPU0:router2#sh int ten 0/0/0/3
TenGigE0/0/0/3 is up, line protocol is up
Interface state transitions: 3
Hardware is TenGigE, address is 0024.98ea.038b (bia 0024.98ea.038b)
Layer 1 Transport Mode is LAN
```

```
Description: static lab connection to putin 0/0/0/3 - dont change
Layer 2 Transport Mode
MTU 1514 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
reliability 255/255, txload 0/255, rxload 0/255
Encapsulation ARPA,
Full-duplex, 10000Mb/s, LR, link type is force-up
output flow control is off, input flow control is off
loopback not set,
Last input 00:00:00, output 00:00:06
Last clearing of "show interface" counters 00:01:15
5 minute input rate 27000 bits/sec, 30 packets/sec
5 minute output rate 27000 bits/sec, 30 packets/sec
10008 packets input, 1140908 bytes, 0 total input drops
0 drops for unrecognized upper-level protocol
Received 0 broadcast packets, 8 multicast packets
0 runts, 0 giants, 0 throttles, 0 parity
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
10006 packets output, 1140592 bytes, 0 total output drops
Output 0 broadcast packets, 6 multicast packets
0 output errors, 0 underruns, 0 applique, 0 resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions


RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
---------------------- ------------------------- -------------------------
test p2p1 UP Te0/0/0/3 UP Gi0/1/0/1 UP
------------------------------------------------------------------------------
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test det

Group test, XC p2p1, state is up; Interworking none
AC: TenGigE0/0/0/3, state is up
Type Ethernet
MTU 1500; XC ID 0x1080001; interworking none
Statistics:
packets: received 10008, sent 10006
bytes: received 1140908, sent 1140592
AC: GigabitEthernet0/1/0/1, state is up
Type Ethernet
MTU 1500; XC ID 0x1880003; interworking none
Statistics:
packets: received 10006, sent 10008
bytes: received 1140592, sent 1140908

RP/0/RSP0/CPU0:router2#sh l2vpn forwarding interface gigabitEthernet 0/1/0/1
   hardware ingress detail location 0/1/CPU0
Local interface: GigabitEthernet0/1/0/1, Xconnect id: 0x1880003, Status: up
Segment 1
AC, GigabitEthernet0/1/0/1, Ethernet port mode, status: Bound
Statistics:
packets: received 10022, sent 10023
bytes: received 1142216, sent 1142489
packets dropped: PLU 0, tail 0
bytes dropped: PLU 0, tail 0
Segment 2
AC, TenGigE0/0/0/3, Ethernet port mode, status: Bound

Platform AC context:
Ingress AC: Local Switch, State: Bound
```

```
Flags: Remote is Simple AC
XID: 0x00580003, SHG: None
Ingress uIDB: 0x0003, Egress uIDB: 0x0003, NP: 3, Port Learn Key: 0
NP3
Ingress uIDB:
Flags: L2, Status
Stats Ptr: 0x0d842c, uIDB index: 0x0003, Wire Exp Tag: 0
BVI Bridge Domain: 0, BVI Source XID: 0x01000000
VLAN1: 0, VLAN1 etype: 0x0000, VLAN2: 0, VLAN2 etype: 0x0000
L2 ACL Format: 0, L2 ACL ID: 0, IPV4 ACL ID: 0, IPV6 ACL ID: 0
QOS ID: 0, QOS Format ID: 0
Local Switch dest XID: 0x00000001
UIDB IF Handle: 0x00000000, Source Port: 1, Num VLANs: 0
Xconnect ID: 0x00580003, NP: 3
Type: AC, Remote type: AC
Flags: Learn enable
uIDB Index: 0x0003, LAG pointer: 0x0000
Split Horizon Group: None

RP/0/RSP0/CPU0:router2#sh l2vpn forwarding interface Te 0/0/0/3 hardware egress
   detail location 0/0/CPU0
Local interface: TenGigE0/0/0/3, Xconnect id: 0x1080001, Status: up
Segment 1
AC, TenGigE0/0/0/3, Ethernet port mode, status: Bound
Statistics:
packets: received 10028, sent 10027
bytes: received 1143016, sent 1142732
packets dropped: PLU 0, tail 0
bytes dropped: PLU 0, tail 0
Segment 2
AC, GigabitEthernet0/1/0/1, Ethernet port mode, status: Bound

Platform AC context:
Egress AC: Local Switch, State: Bound
Flags: Remote is Simple AC
XID: 0x00000001, SHG: None
Ingress uIDB: 0x0007, Egress uIDB: 0x0007, NP: 0, Port Learn Key: 0
NP0
Egress uIDB:
Flags: L2, Status, Done
Stats ptr: 0x000000
VPLS SHG: None
L2 ACL Format: 0, L2 ACL ID: 0, IPV4 ACL ID: 0, IPV6 ACL ID: 0
VLAN1: 0, VLAN1 etype: 0x0000, VLAN2: 0, VLAN2 etype: 0x0000
UIDB IF Handle: 0x04000240, Search VLAN Vector: 0
QOS ID: 0, QOS format: 0
Xconnect ID: 0x00000001, NP: 0
Type: AC, Remote type: AC
Flags: Learn enable
uIDB Index: 0x0007, LAG pointer: 0x0000
Split Horizon Group: None
```

3.1.2 Subinterfaces y manipulación de VLAN

En la terminología del software Cisco IOS®, este ejemplo tiene un AC que es como una interfaz de acceso en modo switchport y una subinterfaz dot1q que es como un trunk:



Normalmente, esta topología utiliza un dominio de bridge porque normalmente hay más de dos puertos en la VLAN, aunque puede utilizar una conexión cruzada punto a punto si sólo hay dos puertos. En esta sección se describe cómo las capacidades de reescritura flexible le ofrecen varias maneras de manipular la VLAN.

3.1.2.1 Interfaz principal y subinterfaz Dot1q

En este ejemplo, la interfaz principal está en un lado y la subinterfaz dot1q está en el otro lado:

Ésta es la interfaz principal en el router1:

```
RP/0/RP0/CPU0:router1#sh run int gig 0/0/0/1
interface GigabitEthernet0/0/0/1
description static lab connection to router2 0/1/0/1
cdp
ipv4 address 10.1.1.1 255.255.255.0
!
```

Esta es la subinterfaz dot1q en el router2:

```
RP/0/RSP0/CPU0:router2#sh run int gig 0/1/0/1
interface GigabitEthernet0/1/0/1
description static lab connection to router1 0/0/0/1
l2transport

RP/0/RSP0/CPU0:router2#sh run int ten 0/0/0/3.2
interface TenGigE0/0/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric

RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p2
interface TenGigE0/0/0/3.2
interface GigabitEthernet0/1/0/1
```

Ahora hay una palabra clave *l2transport* en el nombre de subinterfaz de TenGigE0/0/0/3.2. El Router3 envía tramas dot1q con la etiqueta 2, que coinciden con la subinterfaz TenGigE0/0/0/3.2 en el router2.

La etiqueta entrante 2 se elimina en la dirección de ingreso mediante el comando **rewrite ingress tag pop 1 symmetric**. Dado que la etiqueta se ha eliminado en la dirección de ingreso en TenGigE0/0/0/3.2, los paquetes se envían sin etiqueta en la dirección de egreso en GigabitEthernet0/1/0/1.

El Router1 envía tramas sin etiqueta, que coinciden con la interfaz principal

GigabitEthernet0/1/0/1.

No hay ningún comando **rewrite** en GigabitEthernet0/1/0/1, por lo que no se abre, empuja o traduce ninguna etiqueta.

Cuando los paquetes tienen que ser reenviados fuera de TenGigE0/0/0/3.2, la etiqueta dot1q 2 es empujada debido a la palabra clave *symmetric* en el comando **rewrite ingress tag pop 1**. El comando muestra una etiqueta en la dirección de ingreso pero empuja simétricamente una etiqueta en la dirección de egreso. Este es un ejemplo en el router3:

```
RP/0/RSP0/CPU0:router3#sh run int ten 0/0/0/3.2
interface TenGigE0/0/0/3.2
ipv4 address 10.1.1.2 255.255.255.0
encapsulation dot1q 2
```

Supervise los contadores de la subinterfaz con los mismos comandos **show interface** y **show l2vpn**:

```
RP/0/RSP0/CPU0:router2#clear counters
Clear "show interface" counters on all interfaces [confirm]
RP/0/RSP0/CPU0:router2#clear l2vpn forwarding counters
RP/0/RSP0/CPU0:router2#
RP/0/RSP0/CPU0:router2#
RP/0/RSP0/CPU0:router2#sh int TenGigE0/0/0/3.2
TenGigE0/0/0/3.2 is up, line protocol is up
Interface state transitions: 1
Hardware is VLAN sub-interface(s), address is 0024.98ea.038b
Layer 2 Transport Mode
MTU 1518 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
reliability Unknown, txload Unknown, rxload Unknown
Encapsulation 802.1Q Virtual LAN,
Outer Match: Dot1Q VLAN 2
Ethertype Any, MAC Match src any, dest any
loopback not set,
Last input 00:00:00, output 00:00:00
Last clearing of "show interface" counters 00:00:27
1000 packets input, 122000 bytes
0 input drops, 0 queue drops, 0 input errors
1002 packets output, 122326 bytes
0 output drops, 0 queue drops, 0 output errors


RP/0/RSP0/CPU0:router2#sh l2vpn xconnect detail

Group test, XC p2p2, state is up; Interworking none
AC: TenGigE0/0/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0x1080001; interworking none
Statistics:
packets: received 1001, sent 1002
bytes: received 118080, sent 118318
drops: illegal VLAN 0, illegal length 0
AC: GigabitEthernet0/1/0/1, state is up
Type Ethernet
MTU 1500; XC ID 0x1880003; interworking none
Statistics:
packets: received 1002, sent 1001
bytes: received 114310, sent 114076
```

Como se esperaba, el número de paquetes recibidos en TenGigE0/0/0/3.2 coincide con el número de paquetes enviados en GigabitEthernet0/1/0/1 y viceversa.

3.1.2.2 Subinterfaz con encapsulación

En lugar de la interfaz principal en GigabitEthernet0/1/0/1, puede utilizar una subinterfaz con **encapsulation default** para capturar todas las tramas o con **encapsulation untagged** para hacer coincidir sólo las tramas sin etiquetar:

```
RP/0/RSP0/CPU0:router2#sh run interface GigabitEthernet0/1/0/1.1
interface GigabitEthernet0/1/0/1.1 l2transport
encapsulation untagged

RP/0/RSP0/CPU0:router2#sh run int TenGigE0/0/0/3.2
interface TenGigE0/0/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric

RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p3
interface TenGigE0/0/0/3.2
interface GigabitEthernet0/1/0/1.1
```

3.1.2.3 Dirección de entrada en GigabitEthernet0/1/0/1.1

En lugar de la etiqueta emergente 2 en la dirección de ingreso en TenGigE0/0/0/3.2, puede presionar la etiqueta 2 en la dirección de ingreso en GigabitEthernet0/1/0/1.1 y no hacer nada en TenGigE0/0/0/3.2:

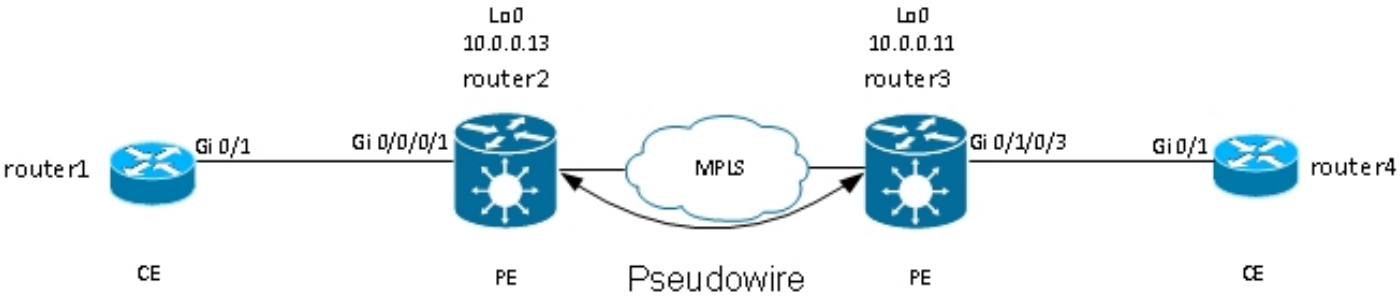
```
RP/0/RSP0/CPU0:router2#sh run int  TenGigE0/0/0/3.2
interface TenGigE0/0/0/3.2 l2transport
encapsulation dot1q 2

RP/0/RSP0/CPU0:router2#sh run interface GigabitEthernet0/1/0/1.1
interface GigabitEthernet0/1/0/1.1 l2transport
encapsulation untagged
rewrite ingress tag push dot1q 2 symmetric

RP/0/RSP0/CPU0:router2#sh run int TenGigE0/0/0/3.2
interface TenGigE0/0/0/3.2 l2transport
encapsulation dot1q 2

RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p3
interface TenGigE0/0/0/3.2
interface GigabitEthernet0/1/0/1.1
```

Por lo tanto, puede ver que el modelo EVC con los comandos **encapsulation** y **rewrite** le brinda una gran flexibilidad para igualar y manipular las etiquetas VLAN.

3.2 Servicios de cable privado virtual

3.2.1 Descripción general

Los servicios de cable privado virtual (VPWS), también conocidos como Ethernet sobre MPLS (EoMPLS), permiten que dos dispositivos L2VPN Provider Edge (PE) tunelen el tráfico L2VPN sobre una nube MPLS. Los dos PE L2VPN se conectan típicamente en dos sitios diferentes con un núcleo MPLS entre ellos. Los dos AC conectados en cada L2VPN PE están enlazados por un PW sobre la red MPLS, que es el MPLS PW.



Cada PE necesita tener una etiqueta MPLS para alcanzar el loopback del PE remoto. Esta etiqueta, normalmente denominada etiqueta de protocolo de gateway interior (IGP), se puede aprender a través del protocolo de distribución de etiquetas MPLS (LDP) o de la ingeniería de tráfico MPLS (TE).

Los dos PE establecen una sesión MPLS LDP dirigida entre ellos para que puedan establecer y controlar el estado del PW. Un PE anuncia al otro PE la etiqueta MPLS para la identificación de PW.

Nota: Aunque BGP se puede utilizar para la señalización, no se trata en este documento.

El tráfico recibido por el router2 en su CA local se encapsula en una pila de etiquetas MPLS:

- La etiqueta MPLS externa es la etiqueta IGP para alcanzar el loopback del router 3. Ésta podría ser la etiqueta implícita-nula si las etiquetas están conectadas directamente; esto significa que no se agregará ninguna etiqueta IGP.
- La etiqueta MPLS interna es la etiqueta PW anunciada por el router 3 a través de la sesión LDP de destino.
- Puede haber una palabra de control PW después de las etiquetas MPLS, dependiendo de la configuración y el tipo de encapsulación. La palabra control no se utiliza de forma predeterminada en las interfaces Ethernet y debe configurarse explícitamente cuando sea necesario.
- La trama L2 transportada sigue en el paquete.
- Algunas etiquetas VLAN se transportan a través del PW, dependiendo de la configuración y del tipo de PW.

El penúltimo salto, justo antes del router3 en el núcleo MPLS, muestra la etiqueta IGP o la reemplaza con una etiqueta null explícita. Por lo tanto, la etiqueta significativa superior en la trama recibida por el router3 es la etiqueta PW que el router3 señaló al router2 para el PW. Por lo tanto, el router3 sabe que el tráfico recibido con esa etiqueta MPLS debe conmutarse a la CA conectada al router4.

En el ejemplo anterior, primero debe verificar si cada L2VPN tiene una etiqueta MPLS para el loopback del PE remoto. Este es un ejemplo de cómo verificar las etiquetas en el router2:

```
RP/0/RSP1/CPU0:router2#sh mpls forwarding prefix 10.0.0.11/32
Local Outgoing Prefix Outgoing Next Hop Bytes
Label Label or ID Interface Switched
------ ----------- ------------------ ------------ --------------- ------------
16008 16009 10.0.0.11/32 Te0/0/0/1 10.0.23.2 681260
```

La configuración de CA sigue siendo la misma:

```
RP/0/RSP1/CPU0:router2#sh run int gig 0/0/0/1.2
Wed May 1 13:56:07.668 CEST
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
```

Debido a que no hay un comando **rewrite ingress pop**, la etiqueta VLAN 2 entrante se transporta a través del PW. Consulte los PW de tipo 4 y 5 para obtener más información.

La configuración L2VPN especifica el AC local y el PE L2VPN remoto con un ID de PW que debe coincidir en cada lado y debe ser único para cada vecino:

```
RP/0/RSP1/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p4
interface GigabitEthernet0/0/0/1.2
neighbor 10.0.0.11 pw-id 222
```

La configuración correspondiente en el router 3 es:

```
RP/0/RSP0/CPU0:router3#sh run int gig 0/1/0/3.2
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
!

RP/0/RSP0/CPU0:router3#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p4
interface GigabitEthernet0/1/0/3.2
neighbor 10.0.0.13 pw-id 222
```

Utilice el comando **show l2vpn xconnect detail** para ver los detalles de la conexión cruzada:

```
RP/0/RSP1/CPU0:router2#sh l2vpn xconnect group test xc-name p2p4 detail

Group test, XC p2p4, state is up; Interworking none
AC: GigabitEthernet0/0/0/1.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1504; XC ID 0x840006; interworking none
Statistics:
packets: received 186, sent 38448
bytes: received 12644, sent 2614356
drops: illegal VLAN 0, illegal length 0
PW: neighbor 10.0.0.11, PW ID 222, state is up ( established )
PW class not set, XC ID 0xc0000004
```

```
Encapsulation MPLS, protocol LDP
Source address 10.0.0.13
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------------------
Label 16026                          16031
Group ID 0x4000280 0x6000180
Interface GigabitEthernet0/0/0/1.2       GigabitEthernet0/1/0/3.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225476
Create time: 30/04/2013 16:30:58 (21:31:00 ago)
Last time status changed: 30/04/2013 16:36:42 (21:25:16 ago)
Statistics:
packets: received 38448, sent 186
bytes: received 2614356, sent 12644
```

En esta configuración, tenga en cuenta que:

- La unidad de transmisión máxima (MTU) de la CA es 1504 porque la etiqueta de entrada de la CA no está activada. La MTU debe coincidir en cada lado o el PW no se activará.
- Se recibieron 186 paquetes en la CA y se enviaron en el PW como se esperaba.
- Se recibieron 38448 paquetes en el PW y se enviaron en el AC como se esperaba.
- La etiqueta local en el router2 es 16026 y es la etiqueta que el router3 utiliza como etiqueta interna. Los paquetes se reciben en el router 2 con esa etiqueta MPLS como etiqueta superior porque la etiqueta IGP ha sido reventada por el penúltimo salto MPLS. El Router 2 sabe que las tramas entrantes con esa etiqueta PW deben conmutarse a AC Gi 0/0/0/1.2:

```
RP/0/RSP1/CPU0:router2#sh mpls forwarding labels 16026
Local Outgoing Prefix Outgoing Next Hop Bytes
Label Label or ID Interface Switched
------ ----------- ------------------ ------------ --------------- ------------
16026  Pop         PW(10.0.0.11:222)  Gi0/0/0/1.2  point2point     2620952
```

3.2.2 Estado de acoplamiento de CA y PW

En una conexión cruzada punto a punto, la CA y el PW están acoplados. Por lo tanto, si la CA deja de funcionar, el L2VPN PE envía señales a través de LDP al PE remoto indicando que el estado de PW debe ser inactivo. Esto activa la convergencia cuando se configura la redundancia PW. Consulte la sección Redundancia para obtener más detalles.

En este ejemplo, la CA está inactiva en el router 2 y está enviando el estado PW 'AC Down' al router 3:

```
RP/0/RSP1/CPU0:router2#sh l2vpn xconnect group test xc-name p2p4 detail
Wed May 1 23:38:55.542 CEST

Group test, XC p2p4, state is down; Interworking none
AC: GigabitEthernet0/0/0/1.2, state is down
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1504; XC ID 0x840006; interworking none
Statistics:
packets: received 186, sent 38544
bytes: received 12644, sent 2620884
drops: illegal VLAN 0, illegal length 0
PW: neighbor 10.0.0.11, PW ID 222, state is down ( remote standby )
PW class not set, XC ID 0xc0000004
Encapsulation MPLS, protocol LDP
Source address 10.0.0.13
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------------------
Label 16026 16031
Group ID 0x4000280 0x6000180
Interface GigabitEthernet0/0/0/1.2 GigabitEthernet0/1/0/3.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x6 (AC Down) in Notification message
MIB cpwVcIndex: 3221225476
Create time: 30/04/2013 16:30:58 (1d07h ago)
Last time status changed: 01/05/2013 14:05:07 (09:33:47 ago)
Statistics:
packets: received 38544, sent 186
bytes: received 2620884, sent 12644
```

El Router 3 sabe que el PW debería estar inactivo porque el AC remoto está inactivo:

```
RP/0/RSP0/CPU0:router3#sh l2vpn xconnect group test xc-name p2p4 detail

Group test, XC p2p4, state is down; Interworking none
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1504; XC ID 0xc40003; interworking none
Statistics:
packets: received 38545, sent 186
bytes: received 2620952, sent 12644
drops: illegal VLAN 0, illegal length 0
 PW: neighbor 10.0.0.13, PW ID 222, state is down ( local ready )
PW class not set, XC ID 0xc0000005
Encapsulation MPLS, protocol LDP
```

```
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------------------
Label 16031 16026
Group ID 0x6000180 0x4000280
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------------------
Incoming Status (PW Status TLV):
Status code: 0x6 (AC Down) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225477
Create time: 30/04/2013 16:37:57 (1d07h ago)
Last time status changed: 01/05/2013 14:11:33 (09:35:50 ago)
Statistics:
packets: received 186, sent 38545
bytes: received 12644, sent 2620952
```

3.2.3 PW de tipo 4 y tipo 5

Se pueden utilizar dos tipos de PW: tipo 4 y tipo 5.

- Un PW de tipo 4 se conoce como PW basado en VLAN. Se supone que el PE de ingreso no debe remover las etiquetas VLAN entrantes que se deben transportar a través del PW.

  En las plataformas basadas en EVC como ASR 9000, el problema es que los AC entrantes podrían tener un comando de **reescritura** que reventara las etiquetas VLAN entrantes, por lo que podría no haber ninguna etiqueta VLAN para transportarse a través del PW. Para hacer frente a esta posibilidad, las plataformas EVC insertan una etiqueta de VLAN ficticia 0 en la parte superior de la trama para los PW de tipo 4. Los PW de tipo 4 se configuran con el comando **transport-mode vlan**. El PE remoto debe estar basado en EVC y debe comprender que la etiqueta VLAN superior es la etiqueta ficticia que se eliminará.

  Sin embargo, si utiliza un PW de tipo 4 entre una plataforma EVC y una plataforma que no es EVC, esto podría dar lugar a problemas de interoperabilidad. La plataforma que no es EVC no considera la etiqueta VLAN superior como la etiqueta VLAN ficticia y, en su lugar, reenvía la trama con la etiqueta VLAN ficticia 0 como la etiqueta externa. Las plataformas EVC tienen la capacidad de manipular las etiquetas VLAN recibidas en la trama entrante con el comando **rewrite**. Los resultados de esa manipulación de VLAN se transportan a través del tipo 4 PW con la etiqueta ficticia adicional 0 en la parte superior.

  Las versiones recientes del software Cisco IOS XR ofrecen la capacidad de utilizar un PW de

tipo 4 sin utilizar la etiqueta ficticia 0 con el comando **transport-mode vlan passthrough**. La manipulación de etiquetas de VLAN en el punto de flujo Ethernet (EFP) debe garantizar que al menos una etiqueta permanezca porque debe haber una etiqueta de VLAN transportada en un PW de tipo 4 y porque, en este caso, no hay ninguna etiqueta ficticia que cumpla ese requisito. Las etiquetas que permanecen en la trama después de la reescritura de la etiqueta de interfaz entrante se transportan de manera transparente a través del PW.

- Un PW de tipo 5 se conoce como PW basado en puerto Ethernet. El PE de ingreso transporta las tramas recibidas en una interfaz principal o después de que las etiquetas de subinterfaz se hayan eliminado cuando el paquete se recibe en una subinterfaz. No hay ningún requisito para enviar una trama etiquetada a través de un PW de tipo 5, y las plataformas basadas en EVC no agregan ninguna etiqueta ficticia. Las plataformas basadas en EVC tienen la capacidad de manipular las etiquetas VLAN recibidas en la trama entrante con el comando **rewrite**. Los resultados de esa manipulación de VLAN se transportan a través del PW de tipo 5, ya sea etiquetado o no etiquetado.

De forma predeterminada, los PE L2VPN intentan negociar un PW de tipo 5, como se muestra en este ejemplo:

```
RP/0/RSP1/CPU0:router2#sh l2vpn xconnect group test det | i " PW type"
PW type Ethernet, control word disabled, interworking none
PW type Ethernet Ethernet
```

El tipo de PW Ethernet indica un tipo 5 PW.

Esta es una captura de sabueso de una solicitud ARP enviada por el router1 y encapsulada por el router2 sobre el PW al router3:

```
Frame 38: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
Ethernet II, Src: Cisco_2f:dc:04 (00:0b:60:2f:dc:04), Dst: Cisco_1e:93:50
(00:24:f7:1e:93:50)
MultiProtocol Label Switching Header, Label: 16031, Exp: 0, S: 1, TTL: 251
Ethernet II, Src: Cisco_03:1f:46 (00:1d:46:03:1f:46), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 2
Address Resolution Protocol (request)
```

La etiqueta MPLS 16031 es la etiqueta PW anunciada por el router3. La captura del sabueso se ha tomado entre el penúltimo salto y el router 3, por lo que no hay etiqueta IGP.

La trama Ethernet encapsulada comienza inmediatamente después de la etiqueta PW. Puede haber una palabra de control PW, pero no está configurada en este ejemplo.

Incluso si es un PW de tipo 5, la etiqueta de VLAN entrante 2 recibida en la CA por el router2 se transporta porque no hay un comando **rewrite** que la active en la CA. Los resultados que provienen de la CA después del procesamiento de reescritura se transportan porque no hay reventado automático de etiquetas en las plataformas basadas en EVC. Observe que no hay una etiqueta de VLAN ficticia 0 con un PW de tipo 5.

Si configuró con el comando **rewrite ingress tag pop 1 symmetric**, no habría ninguna etiqueta VLAN transportada a través del PW.

Este es un ejemplo de un PW tipo 4 con la configuración de una clase pw en el router2 y el router3.

Nota: Si configura un tipo 4 en un solo lado, el PW permanece inactivo e informa 'Error: el tipo PW no coincide.'

```
l2vpn
pw-class VLAN
encapsulation mpls
transport-mode vlan
!
!
xconnect group test
p2p p2p4
neighbor 10.0.0.11 pw-id 222
pw-class VLAN
!
!
!
!
```

El tipo de PW Ethernet VLAN indica un tipo 4 PW.

```
RP/0/RSP1/CPU0:router2#sh l2vpn xconnect group test det | i " PW type"
PW type Ethernet VLAN, control word disabled, interworking none
PW type Ethernet VLAN Ethernet VLAN
```

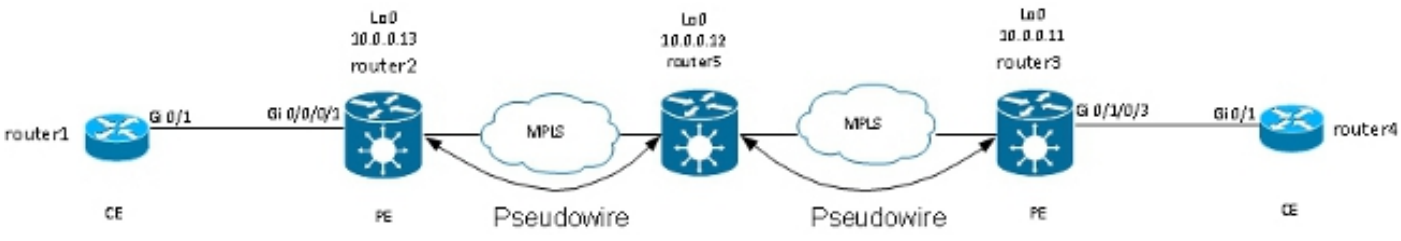
Ahora hay una etiqueta ficticia 0 insertada en la parte superior de la trama que se transporta:

```
Frame 15: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: Cisco_2f:dc:04 (00:0b:60:2f:dc:04), Dst: Cisco_1e:93:50
(00:24:f7:1e:93:50)
MultiProtocol Label Switching Header, Label: 16031, Exp: 0, S: 1, TTL: 251
Ethernet II, Src: Cisco_03:1f:46 (00:1d:46:03:1f:46), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 0
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 2
Address Resolution Protocol (request)
```

El PE basado en EVC de salida elimina la etiqueta ficticia y reenvía la trama con la etiqueta 2 en su AC local. El PE de egreso aplica la manipulación de etiqueta local configurada en su AC en la trama recibida en el PW. Si su AC local está configurado como **rewrite ingress tag pop 1 symmetric**, la etiqueta configurada debe ser empujada en la dirección de salida, por lo que una nueva etiqueta es empujada sobre la etiqueta 2 recibida en el PW. El comando rewrite es muy flexible, pero debe evaluar cuidadosamente lo que desea lograr a cada lado del PW.

3.2.4 PW multisegmento

Es posible tener un L2VPN PE que tenga un PW, en lugar de una interfaz física, como un AC:



El Router5 recibe paquetes en el PW del router2 y conmuta los paquetes de su otro PW al

router3. Por lo tanto, el router 5 está conmutando entre PW para crear un PW multisegmento entre el router 2 y el router 3.

La configuración en el router2 ahora apunta al router5 como el PE remoto:

```
RP/0/RSP1/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p5
interface GigabitEthernet0/0/0/1.2
neighbor 10.0.0.12 pw-id 222
!
!
!
!
```

La configuración en el router5 es básica:

```
RP/0/RSP0/CPU0:router5#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p5
neighbor 10.0.0.11 pw-id 223
!
neighbor 10.0.0.13 pw-id 222
!
description R2-R5-R3
!
!
!
```

El comando **description** es opcional y se inserta en un valor de longitud de tipo (TLV) de conmutación PW que envía el router5 a cada PE remoto (router2 y router3). La **descripción** es útil cuando necesita resolver un problema de PW cuando hay un router en el medio que hace conmutación PW.

Ingrese el comando **sh l2vpn xconnect** para revisar el TLV de conmutación PW:

```
RP/0/RSP0/CPU0:router5#sh l2vpn xconnect group test det

Group test, XC p2p5, state is down; Interworking none
Description: R2-R5-R3
PW: neighbor 10.0.0.11, PW ID 223, state is down ( provisioned )
PW class not set, XC ID 0xc0000002
Encapsulation MPLS, protocol LDP
Source address 10.0.0.12
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------------------
Label 16042 unknown
Group ID 0x4000280 0x0
Interface GigabitEthernet0/0/0/1.2 unknown
MTU 1504 unknown
Control word disabled unknown
PW type Ethernet unknown
```

```
VCCV CV type 0x2 0x0
(none)
(LSP ping verification)
VCCV CC type 0x4 0x0
(none)
(TTL expiry)
------------ ------------------------------ ------------------------------
Outgoing PW Switching TLVs (Label Mapping message):
Local IP Address: 10.0.0.12, Remote IP Address: 10.0.0.13, PW ID: 222
Description: R1-R5-R3
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Statistics for MS-PW:
packets: received 0
bytes: received 0
MIB cpwVcIndex: 3221225474
Create time: 02/05/2013 15:37:53 (00:34:43 ago)
Last time status changed: 02/05/2013 16:12:30 (00:00:06 ago)
Last time PW went down: 02/05/2013 16:12:30 (00:00:06 ago)
PW: neighbor 10.0.0.13, PW ID 222, state is up ( established )
PW class not set, XC ID 0xc0000001
Encapsulation MPLS, protocol LDP
Source address 10.0.0.12
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------------------
Label 16043 16056
Group ID 0x6000180 0x4000280
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x4 0x6
(router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing PW Switching TLVs (Label Mapping message):
Local IP Address: 10.0.0.12, Remote IP Address: 10.0.0.11, PW ID: 223
Description: R2-R5-R3
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Statistics for MS-PW:
packets: received 0
bytes: received 0
MIB cpwVcIndex: 0
Create time: 02/05/2013 15:37:53 (00:34:43 ago)
Last time status changed: 02/05/2013 16:12:35 (00:00:01 ago)
Last time PW went down: 02/05/2013 16:12:30 (00:00:06 ago)
```

El Router 5 envía un TLV de conmutación PW al router 3 con los detalles de su PW al router 2 y envía un TLV de conmutación PW al router 2 con los detalles de su PW al router 3.

3.2.5 Redundancia

Se puede utilizar un PW punto a punto para conectar dos sitios, pero estos dos sitios deben permanecer conectados en caso de un fallo de CA o PE.

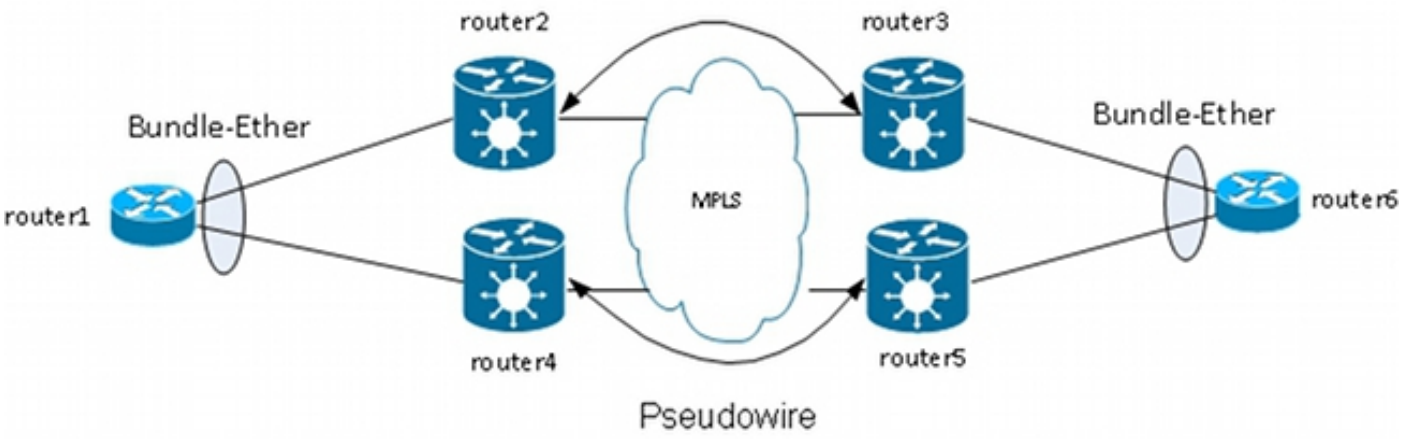
3.2.5.1 Redundancia de núcleo

Si realiza cualquier cambio de topología que afecte el re-ruteo en el núcleo MPLS, MPLS PW hereda la nueva trayectoria inmediatamente.

3.2.5.2 Paquete sobre PW

Un dispositivo de borde del cliente (CE) se puede conectar al PE a través de un conjunto Ethernet para proporcionar redundancia de link si hay una falla de link de miembro del conjunto entre el CE y el PE. El conjunto permanece activo incluso si un miembro del link del conjunto deja de funcionar. Tenga en cuenta que esto no proporciona redundancia PE porque una falla PE hace que todo el conjunto quede inactivo.

Un método para la redundancia es tener varios circuitos transportados por PW punto a punto. Cada circuito es un miembro de un agrupamiento Ethernet entre dos CE:



El PE no termina el agrupamiento y en su lugar transporta las tramas de manera transparente a través del PW, incluidas las tramas del Protocolo de control de agregación de enlaces (LACP) que los CE intercambian entre ellos.

Con este diseño, la pérdida de un AC o un PE hace que un miembro del conjunto deje de funcionar, pero el conjunto permanece activo.

> **Nota**: ASR 9000 no transportó las BPDU de LACP a través de L2VPN en versiones anteriores a la versión 4.2.1 del software Cisco IOS XR.

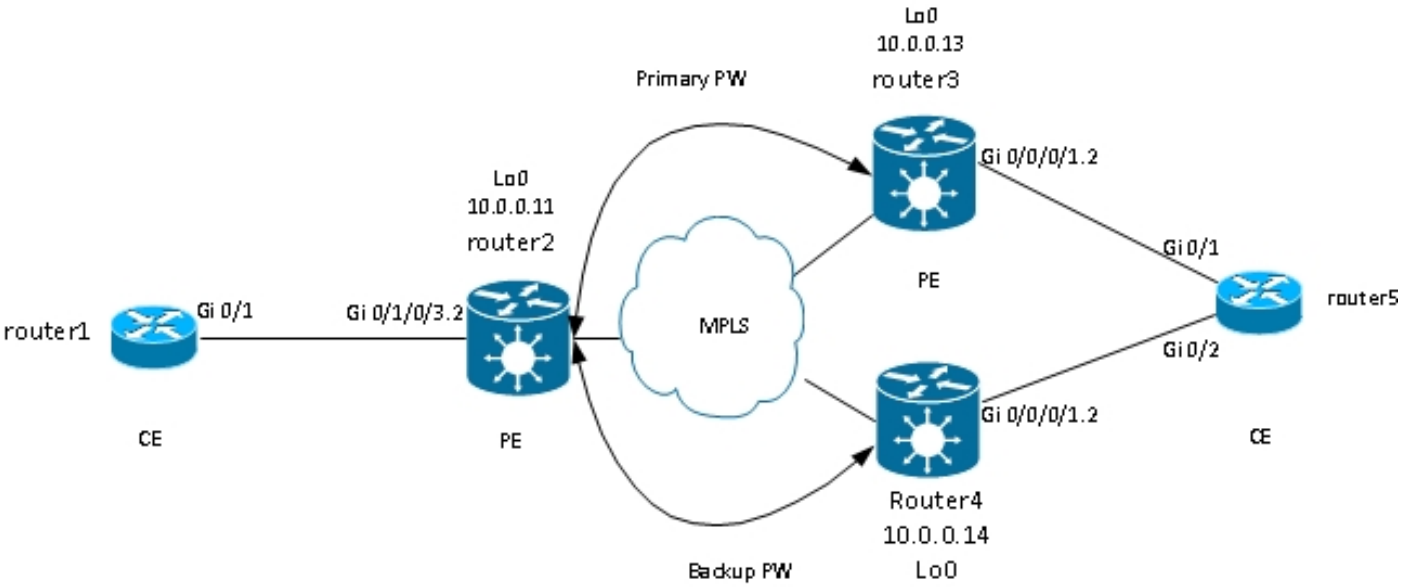
El CE sigue siendo un único punto de fallo en este diseño. Otras funciones de redundancia que se pueden utilizar en el CE incluyen:

- Grupo de agregación de enlaces de varios chasis (MC-LAG)
- Clustering de virtualización de red (nV) ASR 9000
- Virtual Switching System (VSS) en switches Cisco IOS
- Canal de puerto virtual (vPC) en switches Cisco Nexus

Desde la perspectiva del PE, existe una conexión punto a punto simple entre un AC y un MPLS PW.

3.2.5.3 Redundancia de PW

Los PE también pueden proporcionar redundancia con una función llamada Redundancia de PW.



El router 2 tiene un PW principal al router 3. El tráfico del router1 al router6 fluye a través de ese PW primario en circunstancias normales. El router 2 también tiene un PW de respaldo al router 4 en espera en caliente pero, en circunstancias normales, no fluye tráfico a través de ese PW.

Si hay un problema con el PW primario, con el PE remoto del PW primario (router3), o con el AC en el PE remoto (router3), el router2 activa inmediatamente el PW de respaldo y el tráfico comienza a fluir a través de él. El tráfico vuelve al PW principal cuando se resuelve el problema.

La configuración en el router2 es:

```
RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p6
interface GigabitEthernet0/1/0/3.2
neighbor 10.0.0.13 pw-id 222
backup neighbor 10.0.0.14 pw-id 222
!
!
!
!
!
```

La configuración estándar en el router3 y el router4 es:

```
RP/0/RSP1/CPU0:router3#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p6
interface GigabitEthernet0/0/0/1.2
```

```
neighbor 10.0.0.11 pw-id 222
!
!
!
!
```

En condiciones estables, el PW al router3 está activo y el PW al router4 está en estado de espera:

```
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
---------------------- ------------------ --------------------------
test p2p6 UP Gi0/1/0/3.2 UP 10.0.0.13 222 UP
Backup
10.0.0.14 222 SB
------------------------------------------------------------------------
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test det

Group test, XC p2p6, state is up; Interworking none
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1504; XC ID 0xc40003; interworking none
Statistics:
packets: received 51412, sent 25628
bytes: received 3729012, sent 1742974
drops: illegal VLAN 0, illegal length 0
PW: neighbor 10.0.0.13, PW ID 222, state is up ( established )
PW class not set, XC ID 0xc0000005
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ --------------------------- --------------------------
Label 16049 16059
Group ID 0x6000180 0x4000280
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ --------------------------- --------------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225477
Create time: 03/05/2013 15:04:03 (00:21:26 ago)
Last time status changed: 03/05/2013 15:17:34 (00:07:55 ago)
MAC withdraw message: send 0 receive 0
Statistics:
```

```
packets: received 25628, sent 51412
bytes: received 1742974, sent 3729012

Backup PW:
PW: neighbor 10.0.0.14, PW ID 222, state is standby ( all ready )
Backup for neighbor 10.0.0.13 PW ID 222 ( inactive )
PW class not set, XC ID 0xc0000006
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ --------------------------- -------------------------
Label 16050 289971
Group ID 0x6000180 0x4000100
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ --------------------------- -------------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x20 (Standby) in Notification message
MIB cpwVcIndex: 3221225478
Create time: 03/05/2013 15:04:03 (00:21:26 ago)
Last time status changed: 03/05/2013 15:17:34 (00:07:55 ago)
MAC withdraw message: send 0 receive 0
RP/0/RSP0/CPU0:router2#
```

Dado que el estado de CA y el estado de PW están acoplados, el router3 envía señales de "CA inactiva" al router2 cuando la CA del router3 deja de funcionar. El Router 2 desactiva su PW principal y activa el PW de respaldo:

```
RP/0/RSP0/CPU0:May  3 15:34:08.772 : l2vpn_mgr[1121]: %L2-L2VPN_PW-3-UPDOWN :
Pseudowire with address 10.0.0.13, id 222, state is Down
RP/0/RSP0/CPU0:May 3 15:34:08.772 : l2vpn_mgr[1121]: %L2-L2VPN_PW-3-UPDOWN :
Pseudowire with address 10.0.0.14, id 222, state is Up

RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
------------------------ --------------------- --------------------------
test p2p6 UP Gi0/1/0/3.2 UP 10.0.0.13 222 DN
Backup
10.0.0.14 222 UP
------------------------------------------------------------------------------
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test det

Group test, XC p2p6, state is up; Interworking none
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
```

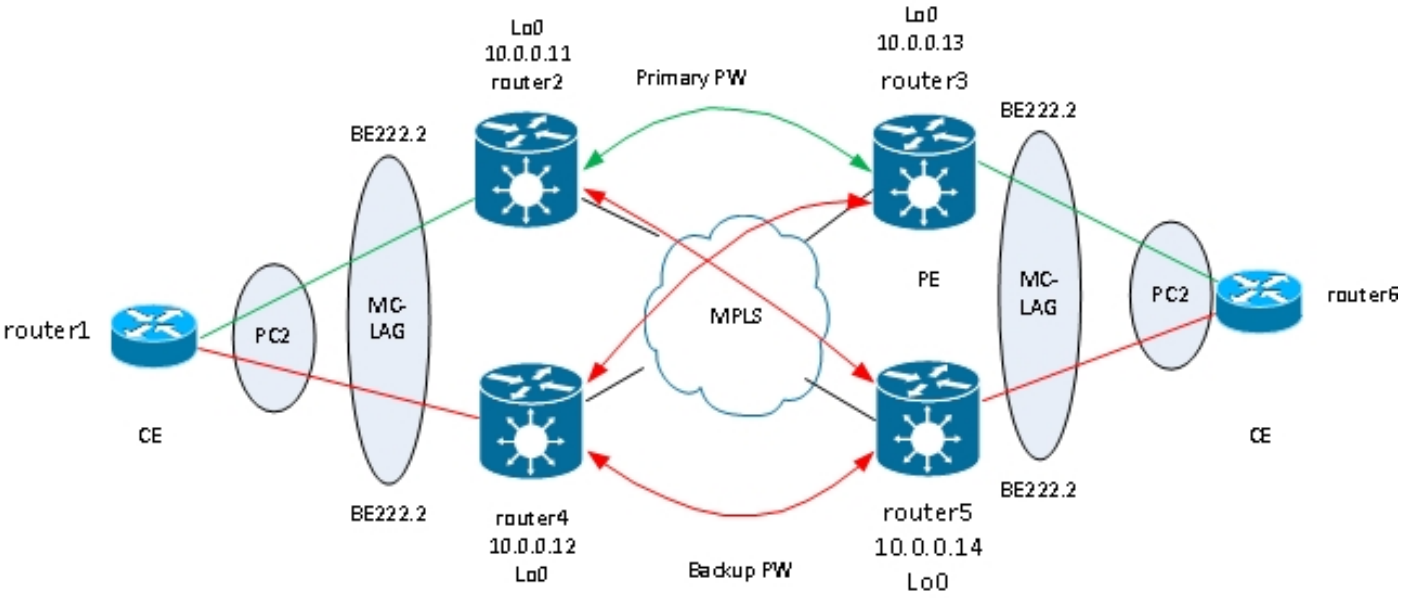
```
MTU 1504; XC ID 0xc40003; interworking none
Statistics:
packets: received 51735, sent 25632
bytes: received 3752406, sent 1743230
drops: illegal VLAN 0, illegal length 0
PW: neighbor 10.0.0.13, PW ID 222, state is down ( local ready )
PW class not set, XC ID 0xc0000005
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ --------------------------
Label 16049 16059
Group ID 0x6000180 0x4000280
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ --------------------------
Incoming Status (PW Status TLV):
Status code: 0x6 (AC Down) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225477
Create time: 03/05/2013 15:04:03 (00:30:14 ago)
Last time status changed: 03/05/2013 15:34:08 (00:00:09 ago)
MAC withdraw message: send 0 receive 0

Backup PW:
PW: neighbor 10.0.0.14, PW ID 222, state is up ( established )
Backup for neighbor 10.0.0.13 PW ID 222 ( active )
PW class not set, XC ID 0xc0000006
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------ ----------------------------
Label 16050 289971
Group ID 0x6000180 0x4000100
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------ ----------------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing Status (PW Status TLV):
```

```
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225478
Create time: 03/05/2013 15:04:03 (00:30:14 ago)
Last time status changed: 03/05/2013 15:34:08 (00:00:09 ago)
MAC withdraw message: send 0 receive 0
Statistics:
packets: received 25632, sent 51735
bytes: received 1743230, sent 3752406
RP/0/RSP0/CPU0:router2#
```

Cuando la CA en el router3 vuelve a estar activa, el router2 reactiva el PW primario al router3 y el PW al router4 vuelve a un estado en espera.

El PW de respaldo también se activa cuando el router3 deja de funcionar y el router2 pierde la ruta a su loopback.

El siguiente paso lógico es introducir la redundancia de PW bidireccional con dos PE en cada sitio:



Sin embargo, esta malla completa de PW encuentra un problema cuando dos PW están activos al mismo tiempo que un loop se introduce en la red. El loop debe romperse, generalmente mediante el uso del Spanning Tree Protocol (STP). Sin embargo, no desea que la inestabilidad del árbol de extensión en un sitio se propague al otro sitio. Por lo tanto, es mejor no ejecutar el spanning tree en estos PW y no fusionar el spanning tree entre los dos sitios . Es más sencillo si solo hay un enlace lógico entre los dos sitios, de modo que no se requiere ningún árbol de extensión.

Una solución es utilizar un paquete MC-LAG entre los dos PE en un sitio y su CE local. Sólo uno de los dos PE tiene activos sus miembros del paquete para que su PW al sitio remoto esté activo. El otro PE tiene sus miembros de agrupamiento en estado de espera y tiene su PW en el sitio remoto inactivo. Con un solo PW activo entre los dos sitios, no se introduce ningún loop. El PE con el PW activo también tiene un PW en espera para el segundo PE en el sitio remoto.

En condiciones estables, los miembros activos del conjunto se encuentran en el router2 y el router3, y el PW activo se encuentra entre ellos. Esta es la configuración en el router 3:

```
RP/0/RSP1/CPU0:router3#sh run redundancy
redundancy
```

```
iccp
group 2
mlacp node 1
mlacp system mac 0200.0000.0002
mlacp system priority 1
mlacp connect timeout 0
member
neighbor 10.0.0.14
!
backbone
interface TenGigE0/0/0/0
interface TenGigE0/0/0/1
!
isolation recovery-delay 300
!
!
!

RP/0/RSP1/CPU0:router3#sh run int bundle-ether 222
interface Bundle-Ether222
lacp switchover suppress-flaps 100
mlacp iccp-group 2
mlacp switchover type revertive
mlacp switchover recovery-delay 40
mlacp port-priority 1
mac-address 0.0.2
bundle wait-while 0
bundle maximum-active links 1
load-interval 30
!

RP/0/RSP1/CPU0:router3#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p7
interface Bundle-Ether222.2
neighbor 10.0.0.11 pw-id 222
backup neighbor 10.0.0.12 pw-id 222
!
!
!
!
!
RP/0/RSP1/CPU0:router3#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
------------------------ ---------------------- ----------------------------
test p2p7 UP BE222.2 UP 10.0.0.11 222 UP
Backup
10.0.0.12 222 DN
------------------------------------------------------------------------------

RP/0/RSP1/CPU0:router3#sh bundle bundle-ether 222

Bundle-Ether222
Status: Up
Local links : 1 / 0 / 1
Local bandwidth : 1000000 (1000000) kbps
MAC address (source): 0000.0000.0002 (Configured)
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
```

```
Maximum active links: 1
Wait while timer: Off
Load balancing: Default
LACP: Operational
Flap suppression timer: 100 ms
Cisco extensions: Disabled
mLACP: Operational
ICCP Group: 2
Role: Active
Foreign links : 0 / 1
Switchover type: Revertive
Recovery delay: 40 s
Maximize threshold: 1 link
IPv4 BFD: Not configured

Port Device State Port ID B/W, kbps
-------------------- --------------- -------- -------------- ----------
Gi0/0/0/1 Local Active 0x8001, 0x9001 1000000
Link is Active
Gi0/0/0/1 10.0.0.14 Standby 0x8002, 0xa002 1000000
Link is marked as Standby by mLACP peer
```

En el router 5, el miembro del agrupamiento local y el PW primario al router 2 están en estado de espera, y el PW de respaldo al router 4 está inactivo:

```
RP/0/RSP1/CPU0:router5#sh run redundancy
redundancy
iccp
group 2
mlacp node 2
mlacp system mac 0200.0000.0002
mlacp system priority 1
mlacp connect timeout 0
member
neighbor 10.0.0.13
!
backbone
interface TenGigE0/1/0/0
interface TenGigE0/1/0/1
!
isolation recovery-delay 300
!
!
!

RP/0/RSP1/CPU0:router5#sh run int bundle-ether 222
interface Bundle-Ether222
lacp switchover suppress-flaps 100
mlacp iccp-group 2
mlacp switchover type revertive
mlacp switchover recovery-delay 40
mac-address 0.0.2
bundle wait-while 0
bundle maximum-active links 1
load-interval 30
!

RP/0/RSP1/CPU0:router5#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p7
interface Bundle-Ether222.2
neighbor 10.0.0.11 pw-id 222
```

```
backup neighbor 10.0.0.12 pw-id 222
!
!
!
!
!

RP/0/RSP1/CPU0:router5#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
------------------------ ---------------------- --------------------------
test p2p7 DN BE222.2 UP 10.0.0.11 222 SB
Backup
10.0.0.12 222 DN
------------------------------------------------------------------------------
RP/0/RSP1/CPU0:router5#sh bundle bundle-ether 222

Bundle-Ether222
Status: mLACP hot standby
Local links : 0 / 1 / 1
Local bandwidth : 0 (0) kbps
MAC address (source): 0000.0000.0002 (Configured)
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
Maximum active links: 1
Wait while timer: Off
Load balancing: Default
LACP: Operational
Flap suppression timer: 100 ms
Cisco extensions: Disabled
mLACP: Operational
ICCP Group: 2
Role: Standby
Foreign links : 1 / 1
Switchover type: Revertive
Recovery delay: 40 s
Maximize threshold: 1 link
IPv4 BFD: Not configured

Port Device State Port ID B/W, kbps
-------------------- ------------ ----------- -------------- ----------
Gi0/0/0/1 Local Standby 0x8002, 0xa002 1000000
mLACP peer is active
Gi0/0/0/1 10.0.0.13 Active 0x8001, 0x9001 1000000
Link is Active
```

En el router6, el miembro del conjunto al router3 está activo, mientras que el miembro del conjunto al router5 está en estado de espera:

```
router6#sh etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator

M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
```

```
Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
------+-------------+-----------+-----------------------------------------------
2 Po2(SU) LACP Gi0/1(P) Gi0/2(w)
```

Cuando el miembro del conjunto en el router3 deja de funcionar, el router6 tiene su miembro activo en el router5:

```
router6#sh etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator

M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port


Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
------+-------------+-----------+-----------------------------------------------
2 Po2(SU) LACP Gi0/1(D) Gi0/2(P)
```

Dado que el bundle-ether222 está inactivo en el router5, el PW acoplado al router2 se desactiva al mismo tiempo:

```
RP/0/RSP1/CPU0:router3#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
------------------------ -------------------- ----------------------------
test p2p7 DN BE222.2 DN 10.0.0.11 222 DN
Backup
10.0.0.12 222 DN
------------------------------------------------------------------------------
```

El Router2 detecta que su PW al router3 está inactivo y activa su PW de respaldo al router5:

```
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
------------------------ -------------------- ----------------------------
test p2p7 UP BE222.2 UP 10.0.0.13 222 DN
Backup
10.0.0.14 222 UP
------------------------------------------------------------------------------
```

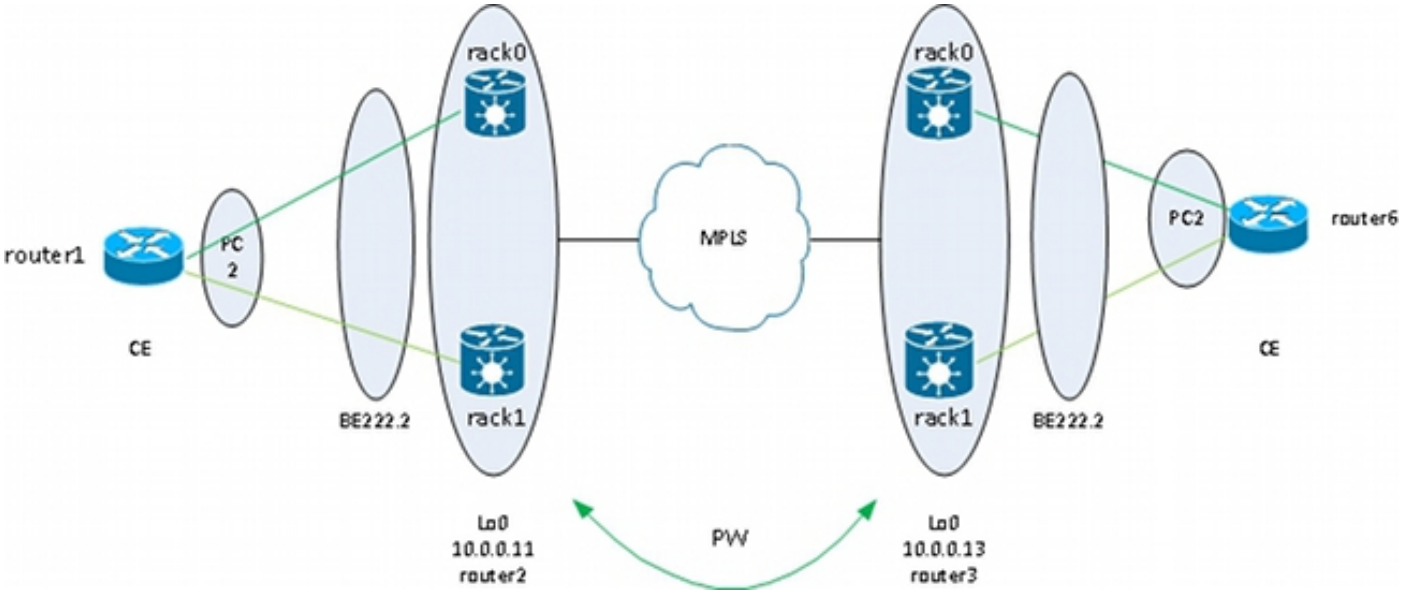
El router 5 tiene su miembro de agrupamiento activo, así como su PW principal al router 2:

```
RP/0/RSP1/CPU0:router5#sh bundle bundle-ether 222

Bundle-Ether222
Status: Up
Local links : 1 / 0 / 1
Local bandwidth : 1000000 (1000000) kbps
MAC address (source): 0000.0000.0002 (Configured)
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
Maximum active links: 1
Wait while timer: Off
Load balancing: Default
LACP: Operational
Flap suppression timer: 100 ms
Cisco extensions: Disabled
mLACP: Operational
ICCP Group: 2
Role: Active
Foreign links : 0 / 1
Switchover type: Revertive
Recovery delay: 40 s
Maximize threshold: 1 link
IPv4 BFD: Not configured

Port Device State Port ID B/W, kbps
-------------------- ---------- ----------- -------------- ----------
Gi0/0/0/1 Local Active 0x8002, 0xa002 1000000
Link is Active
Gi0/0/0/1 10.0.0.13 Configured 0x8003, 0x9001 1000000
Link is down
RP/0/RSP1/CPU0:router5#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
------------------------ ---------------------- ----------------------------
test p2p7 UP BE222.2 UP 10.0.0.11 222 UP
Backup
10.0.0.12 222 DN
------------------------------------------------------------------------------
```

3.2.5.4 Clúster perimetral ASR 9000 nV

El diseño anterior basado en la redundancia MC-LAG y PW funciona bien para la redundancia pero, debido a que algunos miembros del conjunto están en estado de espera, no transportan tráfico en condiciones estables.

Si desea que todos los miembros del paquete estén activos, incluso en condiciones estables, puede utilizar un clúster ASR 9000 con miembros del paquete del CE conectados a cada rack del PE:



Este diseño ofrece redundancia frente a un fallo de enlace de miembro de paquete entre el CE y el PE, un fallo de rack y un fallo de enlace de núcleo, siempre que el clúster esté conectado de forma dual al núcleo MPLS y haya redundancia en el núcleo. Los dos racks no tienen por qué estar ubicados de forma conjunta y podrían estar en ubicaciones diferentes. Los links entre racks no se representan en este diagrama.

Si desea redundancia en el CE, puede utilizar una solución de varios chasis para el CE:

- MC-LAG
- Clustering ASR 9000 nV
- VSS
- vPC

La configuración del clúster ASR 9000 es muy básica:

```
interface TenGigE0/0/0/8
bundle id 222 mode on
!
interface TenGigE1/0/0/8
bundle id 222 mode on
!
interface Bundle-Ether222
!
interface Bundle-Ether222.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
l2vpn
xconnect group test
p2p p2p8
interface Bundle-Ether222.2
neighbor 10.0.0.13 pw-id 8
!
!
!
!
```

Cisco recomienda que configure una dirección MAC estática del sistema LACP y una dirección MAC de agrupamiento para evitar un cambio de dirección MAC causado por un switchover de controlador de estanterías designado. Este ejemplo muestra cómo encontrar las direcciones:

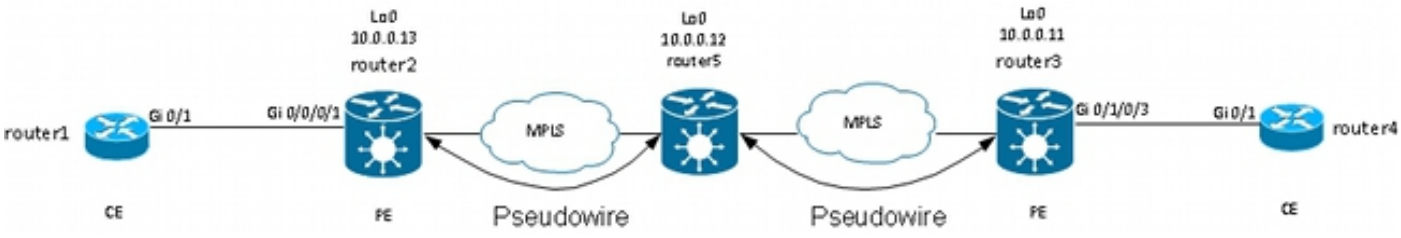
```
RP/1/RSP0/CPU0:router2#sh int bundle-ether 222 | i address is
Hardware is Aggregated Ethernet interface(s), address is 0024.f71e.d309
Internet address is Unknown
RP/1/RSP0/CPU0:router2#
RP/1/RSP0/CPU0:router2#conf
RP/1/RSP0/CPU0:router2(config)#int bundle-ether 222
RP/1/RSP0/CPU0:router2(config-if)#mac-address 0024.f71e.d309
RP/1/RSP0/CPU0:router2(config-if)#commit
RP/1/RSP0/CPU0:router2(config-if)#end
RP/1/RSP0/CPU0:router2#
RP/1/RSP0/CPU0:router2#sh lacp system-id

Priority MAC Address
-------- -----------------
0x8000 00-24-f7-1e-d3-05
RP/1/RSP0/CPU0:router2#
RP/1/RSP0/CPU0:router2#conf
RP/1/RSP0/CPU0:router2(config)#lacp system mac 0024.f71e.d305
RP/1/RSP0/CPU0:router2(config)#commit
RP/1/RSP0/CPU0:router2(config)#end
```

En resumen, este es el bundle-ether 222 con un miembro en cada rack (diez 0/0/0/8 en el rack 0 y diez 1/0/0/8 en el rack 1) y la subinterfaz del bundle configurada para una conexión cruzada punto a punto:

```
RP/1/RSP0/CPU0:router2#sh l2vpn xconnect group test
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
------------------------ ---------------------- --------------------------
test p2p8 UP BE222.2 UP 10.0.0.13 8 UP
------------------------------------------------------------------------------
```

3.3 CDP

Los routers y switches de Cisco normalmente envían paquetes CDP sin etiquetas dot1q. Existen varios escenarios que determinan lo que sucede con estos paquetes CDP cuando son recibidos por un router IOS XR configurado para una conexión cruzada:



En esta topología, el router1 puede ver su router PE local2 como un vecino CDP o el router CE remoto4, según la configuración.

3.3.1 CDP no habilitado en la interfaz principal de L2VPN PE

Los paquetes CDP del CE L2VPN se transportan a través de la conexión cruzada. Los dos CE L2VPN se ven entre sí (con el uso del comando **show cdp neighbors**) si la interfaz principal está

configurada como l2transport o si hay una subinterfaz que coincide con las tramas CDP sin etiqueta.

Este es un ejemplo de la interfaz principal:

```
interface GigabitEthernet0/0/0/1
l2transport
!
!
l2vpn
xconnect group test
p2p p2p8
interface GigabitEthernet0/0/0/1
neighbor 10.0.0.11 pw-id 8
!
!
!
!
```

Este es un ejemplo de una subinterfaz sin etiqueta:

```
interface GigabitEthernet0/0/0/1.1 l2transport
encapsulation untagged
!
l2vpn
xconnect group test
p2p p2p8
interface GigabitEthernet0/0/0/1.1
neighbor 10.0.0.11 pw-id 8
!
!
!
!
```

En estos dos ejemplos, los paquetes CDP se transportan a través de la conexión cruzada, y los CE se ven entre sí como vecinos CDP. El CE no ve el PE como un vecino CDP:

```
router1#sh cdp nei gigabitEthernet 0/1
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID Local Intrfce Holdtme Capability Platform Port ID
router4 Gig 0/1 168 R S ME-3400G- Gig 0/1
```

3.3.2 CDP habilitado en la interfaz principal de L2VPN PE

El PE procesa los paquetes CDP sin etiqueta, y el PE y el CE se ven como vecinos. Sin embargo, el CE no ve el CE remoto cuando CDP está habilitado en la interfaz principal del PE L2VPN.

Tenga en cuenta que:

- No puede configurar CDP en una interfaz principal que está configurada como l2transport.
- El PE intercepta los paquetes CDP cuando el CDP se configura en la interfaz principal no L2transport. Esto ocurre incluso si hay una subinterfaz l2transport configurada para coincidir con los paquetes CDP sin etiqueta (con el uso de los comandos **encapsulation untagged** o

encapsulation default). En este caso, los paquetes CDP no se transportan al sitio remoto.

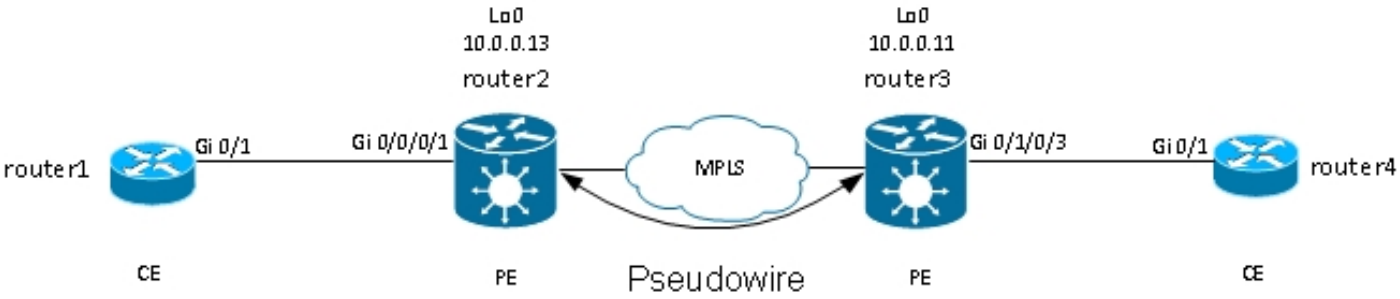
3.4 Árbol de extensión

Si el CE L2VPN es un switch Ethernet y está enviando BPDU de spanning tree al PE L2VPN, estas BPDU se manejan como tráfico regular y se transportan según la configuración de L2VPN.

Las BPDU STP o MST se envían sin etiqueta y se transportan a través de la conexión cruzada punto a punto si la interfaz principal está configurada como l2transport o si hay una subinterfaz l2transport configurada con los comandos **encapsulation untagged** o **encapsulation default**.

Per VLAN Spanning Tree Plus (PVST+) o Rapid PVST+ (PVRST+) envían BPDU etiquetadas que se transportan si hay una subinterfaz l2transport que coincida con la etiqueta dot1q de las BPDU.

Este es un ejemplo de topología:



El router 2 y el router 3 transportan tramas sin etiqueta y tramas con dot1q tag 2:

```
interface GigabitEthernet0/0/0/1.1 l2transport
encapsulation untagged
!
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
l2vpn
xconnect group test
p2p p2p8
interface GigabitEthernet0/0/0/1.2
neighbor 10.0.0.11 pw-id 8
!
!
p2p p2p9
interface GigabitEthernet0/0/0/1.1
neighbor 10.0.0.11 pw-id 9
!
!
!
!
```

El Switch1 recibe las BPDU no etiquetadas en la VLAN1 y las BPDU etiquetadas en la VLAN2 del switch4; su puerto raíz está en Gi0/1 hacia el switch4:

```
switch1#sh spanning-tree vlan 1

VLAN0001
```

```
Spanning tree enabled protocol ieee
Root ID Priority 32768
Address 0024.985e.6a00
Cost 8
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Root FWD 4 128.1 P2p

switch1#sh spanning-tree vlan 2

VLAN0002
Spanning tree enabled protocol ieee
Root ID Priority 32770
Address 0019.552b.b580
Cost 4
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32770 (priority 32768 sys-id-ext 2)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 15

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Root FWD 4 128.1 P2p
```

Con esta configuración, el dominio de árbol de expansión en el sitio A se fusiona con el dominio de árbol de expansión en el lado B. Un problema potencial es que la inestabilidad del árbol de expansión en un sitio podría propagarse al otro sitio.

Si está seguro de que un sitio está conectado sólo a través de un PW a otro sitio y de que no hay ningún enlace de puerta trasera que pueda introducir un bucle físico, es una buena idea no ejecutar un árbol de extensión en los dos sitios. Esto mantiene los dos dominios de árbol de expansión aislados. Para hacer esto, configure un spanning tree bpdufilter en los CE, o configure una lista de acceso de servicios ethernet en los PE para borrar tramas con la dirección MAC de destino utilizada por las BPDU. Una lista de acceso de servicios Ethernet en los PE se puede utilizar para descartar tramas con la MAC de destino de BPDU u otros tipos de protocolos L2 que no desee reenviar a través de PW.

Esta es una lista de acceso que puede utilizar en cada (sub)interfaz de l2transport que se transporta entre los dos sitios:

```
ethernet-services access-list block-invalid-frames
10 deny any 0180.c200.0000 0000.0000.000f
20 deny any host 0180.c200.0010
30 deny any host 0100.0c00.0000
40 deny any host 0100.0ccc.cccc
50 deny any host 0100.0ccc.cccd
60 deny any host 0100.0ccd.cdce
70 permit any any
!
```

```
RP/0/RSP1/CPU0:router2#sh run int GigabitEthernet0/0/0/1.1
interface GigabitEthernet0/0/0/1.1 l2transport
encapsulation untagged
ethernet-services access-group block-invalid-frames ingress
ethernet-services access-group block-invalid-frames egress
!

RP/0/RSP1/CPU0:router2#sh run int GigabitEthernet0/0/0/1.2
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
ethernet-services access-group block-invalid-frames ingress
ethernet-services access-group block-invalid-frames egress
!
```

La ACL de servicios Ethernet comienza a descartar las BPDU:

```
RP/0/RSP1/CPU0:router2#sh access-lists ethernet-services block-invalid-frames
hardware ingress location 0/0/CPU0
ethernet-services access-list block-invalid-frames
10 deny any 0180.c200.0000 0000.0000.000f (41 hw matches)
20 deny any host 0180.c200.0010
30 deny any host 0100.0c00.0000
40 deny any host 0100.0ccc.cccc
50 deny any host 0100.0ccc.cccd (63 hw matches)
60 deny any host 0100.0ccd.cdce
70 permit any any (8 hw matches)
```

El switch1 ya no recibe las BPDU del switch4, por lo que el switch1 es ahora la raíz:

```
switch1#sh spanning-tree vlan 1

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 001d.4603.1f00
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 15

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- ----------------------
Gi0/1 Desg FWD 4 128.1 P2p

switch1#sh spanning-tree vlan 2

VLAN0002
Spanning tree enabled protocol ieee
Root ID Priority 32770
Address 001d.4603.1f00
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32770 (priority 32768 sys-id-ext 2)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 15
```

```
Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- ---------------------
Gi0/1 Desg FWD 4 128.1 P2p
```

El riesgo de inhabilitar el spanning tree en un link es el siguiente: si se crea una conexión de puerta trasera entre los sitios, se introduce un loop físico y el spanning tree no puede romper el loop. Por lo tanto, cuando inhabilite el spanning tree sobre un PW, asegúrese de que no haya links redundantes entre los sitios y que el PW siga siendo la única conexión entre los sitios.

Si hay varias conexiones entre sitios, utilice una solución como VPLS junto con una versión de gateway de acceso del árbol de extensión, como MST Access Gateway (MSTAG) o PVST+ Access Gateway (PVSTAG). Consulte la sección Servicio multipunto para obtener más detalles.

4. Servicio multipunto

> **Notas:**
>
> Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.
>
> La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

Consulte Implementación de Servicios de Capa 2 Multipunto para obtener una descripción completa de las funciones de L2 multipunto.

Con solo dos interfaces en una conexión cruzada punto a punto, un switch L2VPN toma todo lo recibido en un lado y lo reenvía en el otro lado.

Cuando hay más de dos interfaces en un dominio de bridge, un switch Ethernet tiene que tomar una decisión de switching para determinar hacia dónde reenviar tramas en función de su dirección MAC de destino. El switch realiza el aprendizaje de MAC basado en la dirección MAC de origen de las tramas que recibe y crea una tabla de direcciones MAC.

El switch reenvía las tramas con este método:

- Las tramas de difusión se inundan en todos los puertos. Utilice el control de tormentas para limitar la velocidad de inundación de la transmisión.
- Las tramas de multidifusión se inundan en todos los puertos del dominio de puente, excepto cuando se configura la detección de protocolo de administración de grupos de Internet (IGMP) o detección de escucha de multidifusión (MLD). Utilice el control de tormentas para limitar la velocidad de inundación de multidifusión.
- Las tramas de unidifusión con una dirección MAC de destino que no forma parte de la tabla de direcciones MAC del dominio de bridge (unidifusión desconocida) se inundan en todos los puertos del dominio de bridge. Utilice el control de tormentas para limitar la velocidad de inundación unicast desconocida.
- Las tramas de unidifusión con una dirección MAC de destino que forma parte de la tabla de direcciones MAC del dominio de bridge se reenvían al puerto donde se ha aprendido la

dirección MAC de destino.

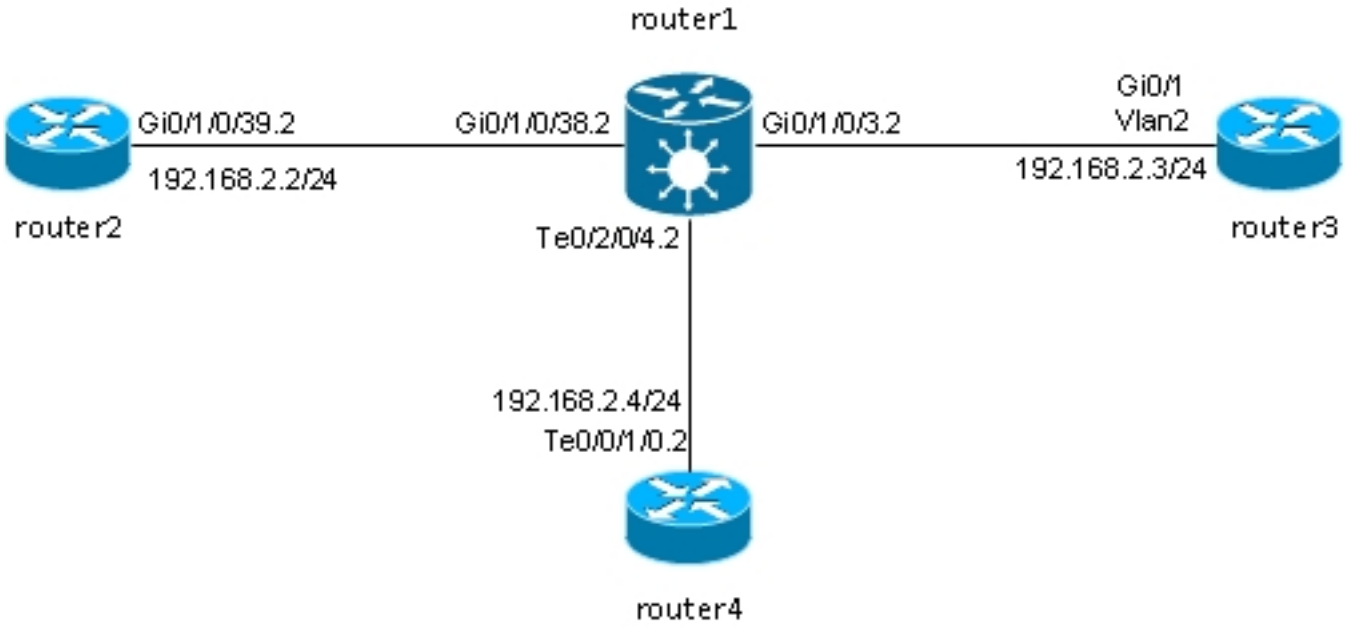
En el software Cisco IOS XR, un dominio de broadcast o una LAN emulada se denomina dominio de bridge. Esto es similar a una VLAN en la terminología del software Cisco IOS, excepto que una VLAN en IOS está vinculada a un número de VLAN que se utiliza como etiqueta dot1q en los trunks. Un dominio de bridge en el software Cisco IOS XR no está vinculado a un número de etiqueta de VLAN dot1q. Puede utilizar el modelo EVC para manipular las etiquetas dot1q y tener subinterfaces dot1q con diferentes números de VLAN dot1q en el mismo dominio de bridge o para tener interfaces sin etiqueta.

Un dominio de bridge es básicamente un dominio de broadcast donde se inundan las transmisiones y las tramas multicast. Una tabla de direcciones MAC está asociada con cada dominio de bridge (a menos que el aprendizaje de MAC esté inhabilitado manualmente por la configuración, lo cual es muy raro). Esto generalmente corresponde a una subred IPv4 o IPv6 donde todos los hosts en el dominio de bridge están conectados directamente.

Los dominios de puente pueden agruparse dentro de un grupo de puente. Esta es una manera conveniente de verificar la configuración. Puede ejecutar un comando show para un grupo de bridges en lugar de un comando show para cada dominio de bridge. Un grupo de bridges no tiene una tabla de direcciones mac ni otras asociaciones; sólo se utiliza para la configuración y los comandos show.

4.1 Conmutación local

Este es un ejemplo muy básico:



Los routers 2, 3 y 4 se conectan a través de ASR 9000, que simula una LAN entre estos tres routers.

Éstas son las configuraciones de interfaz en esos tres routers:

```
RP/0/RSP0/CPU0:router2#sh run int gig 0/1/0/39.2
interface GigabitEthernet0/1/0/39.2
```

```
ipv4 address 192.168.2.2 255.255.255.0
encapsulation dot1q 2
!

router3#sh run int gig 0/1
Building configuration...

Current configuration : 203 bytes
!
interface GigabitEthernet0/1
port-type nni
switchport access vlan 2
switchport trunk allowed vlan 1,2
switchport mode trunk
end

router3#sh run int vlan 2
Building configuration...

Current configuration : 61 bytes
!
interface Vlan2
ip address 192.168.2.3 255.255.255.0
end

router3#

RP/0/RSP0/CPU0:router4#sh run int ten 0/0/1/0.2
interface TenGigE0/0/1/0.2
ipv4 address 192.168.2.4 255.255.255.0
encapsulation dot1q 2
!
```

El router1 recibe los paquetes con la etiqueta dot1q 2 y los reenvía a los otros routers con la etiqueta dot1q 2.

En este escenario básico, hay dos opciones en los AC:

1. Dado que todos los AC utilizan la etiqueta dot1q 2, puede mantenerla en la trama y reenviar la trama en la interfaz de egreso con la misma etiqueta dot1q recibida en la interfaz de ingreso. El comando **rewrite ingress tag pop 1 symmetric** no es necesario.

2. Puede hacer estallar la etiqueta 2 de dot1q entrante en la dirección de ingreso y presionar simétricamente la etiqueta 2 de dot1q en la dirección de egreso. Aunque esto no es necesario en este escenario básico, es una buena idea configurar el dominio de bridge de esta manera al principio porque proporciona más flexibilidad para el futuro. A continuación, se muestran dos ejemplos de cambios que pueden producirse después de la configuración inicial:

   - Si una interfaz BVI ruteada se introduce más adelante en el dominio de bridge, los paquetes deben procesarse en BVI sin etiquetas. Consulte la sección para obtener más información.
   - Más adelante se agrega un nuevo AC, que utiliza una etiqueta dot1q diferente. La etiqueta dot1q 2 aparecería en la dirección de ingreso, y la otra etiqueta dot1q sería empujada en la nueva interfaz en la dirección de egreso y viceversa.BVI

Abra las etiquetas dot1q en cada CA del router1:

```
RP/0/RSP0/CPU0:router1#sh run int GigabitEthernet0/1/0/3.2
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!

RP/0/RSP0/CPU0:router1#sh run int GigabitEthernet0/1/0/38.2
interface GigabitEthernet0/1/0/38.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!

RP/0/RSP0/CPU0:router1#sh run int TenGigE0/2/0/4.2
interface TenGigE0/2/0/4.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
```

Vea la configuración del dominio de bridge con estos tres AC:

```
RP/0/RSP0/CPU0:router1#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain engineering
interface TenGigE0/2/0/4.2
!
interface GigabitEthernet0/1/0/3.2
!
interface GigabitEthernet0/1/0/38.2
!
!
!
!
```

El dominio de bridge se debe configurar en un grupo de bridges. Si se necesitan otros dominios de puente de este cliente, se pueden configurar en el mismo grupo de puente, customer1. Si los nuevos dominios de puente pertenecen a un cliente diferente, puede crear un nuevo grupo de puente. Estos ejemplos utilizan el cliente para agrupar los dominios de bridge, pero los dominios de bridge se pueden agrupar según cualquier criterio.

Utilice el comando **show run l2vpn bridge group customer1 bridge-domain engineering** para mostrar la configuración del bridge-domain.

Utilice el comando **show run l2vpn bridge group customer1** para ver la configuración de todos los dominios de puente.

Utilice el comando **show l2vpn bridge-domain bd-name engineering** o el comando **show l2vpn bridge-domain group customer1** para mostrar información sobre el dominio de puente.

```
RP/0/RSP0/CPU0:router1#show l2vpn bridge-domain group customer1 bd-name
engineering
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 3 (3 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up)
List of ACs:
```

```
Gi0/1/0/3.2, state: up, Static MAC addresses: 0
Gi0/1/0/38.2, state: up, Static MAC addresses: 0
Te0/2/0/4.2, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
RP/0/RSP0/CPU0:router1#show l2vpn bridge-domain group customer1 bd-name
engineering det
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 6
Filter MAC addresses:
Create time: 28/05/2013 17:17:03 (00:18:06 ago)
No status change since creation
ACs: 3 (3 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40003; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 185066, sent 465
bytes: received 13422918, sent 34974
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
```

```
packets: 0, bytes: 0
AC: GigabitEthernet0/1/0/38.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40005; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 8, sent 12287
bytes: received 770, sent 892418
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
AC: TenGigE0/2/0/4.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0x1040001; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 463, sent 11839
bytes: received 35110, sent 859028
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
List of Access PWs:
List of VFIs:
```

Utilice el comando **show l2vpn bridge-domain group customer1 bd-name engineering det** si desea verificar que los paquetes se reciben y se envían en cada CA.

Agregue la palabra clave *mac-address* al comando **show l2vpn forwarding bridge-domain** si desea verificar la tabla mac-address:

```
RP/0/RSP0/CPU0:router1#show l2vpn forwarding bridge-domain customer1:
engineering mac-address location 0/1/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
------------------------------------------------------------------------------
0019.552b.b581 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0024.986c.6417 dynamic Gi0/1/0/38.2 0/1/CPU0 0d 0h 0m 0s N/A
6c9c.ed3e.e484 dynamic Te0/2/0/4.2 0/2/CPU0 0d 0h 0m 0s N/A
```

Las tarjetas de línea ejecutan el aprendizaje de MAC en hardware cada vez que se recibe una trama en el dominio de bridge. También hay una memoria caché de software de la tabla de direcciones mac, pero esta tabla de software no se puede actualizar continuamente para que coincida con las entradas de hardware. Cuando se ingresa el comando **show** en código reciente, intenta resincronizar la tabla de software con la tabla de hardware. Después de un máximo de 15 segundos, imprime el estado actual de la tabla de direcciones mac de software, incluso si la resincronización no está completa (por ejemplo, si la tabla es grande). Utilice el comando **l2vpn resynchronize forwarding mac-address-table** para resincronizar las tablas de software y hardware manualmente.

```
RP/0/RSP0/CPU0:router1#term mon
RP/0/RSP0/CPU0:router1#l2vpn resynchronize forwarding mac-address-table
location 0/1/CPU0
RP/0/RSP0/CPU0:router1#LC/0/1/CPU0:May 28 18:25:35.734 : vkg_l2fib_mac_cache[357]
%PLATFORM-
PLAT_L2FIB_MAC_CACHE-6-RESYNC_COMPLETE : The resynchronization of the MAC
address table is complete
0/1/CPU0

RP/0/RSP0/CPU0:router1#show l2vpn forwarding bridge-domain customer1:engineering
mac-address location 0/1/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
------------------------------------------------------------------------------
0019.552b.b581 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
6c9c.ed3e.e484 dynamic Te0/2/0/4.2 0/2/CPU0 0d 0h 0m 0s N/A
```

Un mensaje de syslog indica cuándo se completa el proceso de resincronización, por lo que es útil tener **terminal monitor** habilitado para ver el mensaje.

La columna Resync Age (Edad de resincronización) muestra la última vez que se resincronizó la dirección MAC desde la tabla de hardware.

La palabra clave *location* es la ubicación de una tarjeta de línea entrante o saliente. Las direcciones MAC se intercambian entre las tarjetas de línea en el hardware, por lo que las direcciones MAC deben conocerse en cada tarjeta de línea donde haya un AC o un PW. La palabra clave *detail* podría proporcionar una versión más actualizada de la tabla de software:

```
RP/0/RSP0/CPU0:router1#show l2vpn forwarding bridge-domain customer1:
engineering mac-address detail location 0/1/CPU0

Bridge-domain name: customer1:engineering, id: 5, state: up
MAC learning: enabled
MAC port down flush: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC Secure: disabled, Logging: disabled
DHCPv4 snooping: profile not known on this node
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
IGMP snooping: disabled, flooding: enabled
Bridge MTU: 1500 bytes
Number of bridge ports: 3
Number of MAC addresses: 4
Multi-spanning tree instance: 0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location


GigabitEthernet0/1/0/3.2, state: oper up
Number of MAC: 2
Statistics:
packets: received 187106, sent 757
bytes: received 13571342, sent 57446
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic arp inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0

Mac Address: 0019.552b.b581, LC learned: 0/1/CPU0
Resync Age: 0d 0h 0m 0s, Flag: local


Mac Address: 0019.552b.b5c3, LC learned: 0/1/CPU0
Resync Age: 0d 0h 0m 0s, Flag: local


GigabitEthernet0/1/0/38.2, state: oper up
Number of MAC: 1
Statistics:
packets: received 18, sent 14607
bytes: received 1950, sent 1061882
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic arp inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0

Mac Address: 0024.986c.6417, LC learned: 0/1/CPU0
Resync Age: 0d 0h 0m 0s, Flag: local
```

```
TenGigE0/2/0/4.2, state: oper up
Number of MAC: 1
Statistics:
packets: received 0, sent 0
bytes: received 0, sent 0
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic arp inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0

Mac Address: 6c9c.ed3e.e484, LC learned: 0/2/CPU0
Resync Age: 0d 0h 0m 0s, Flag: remote
```

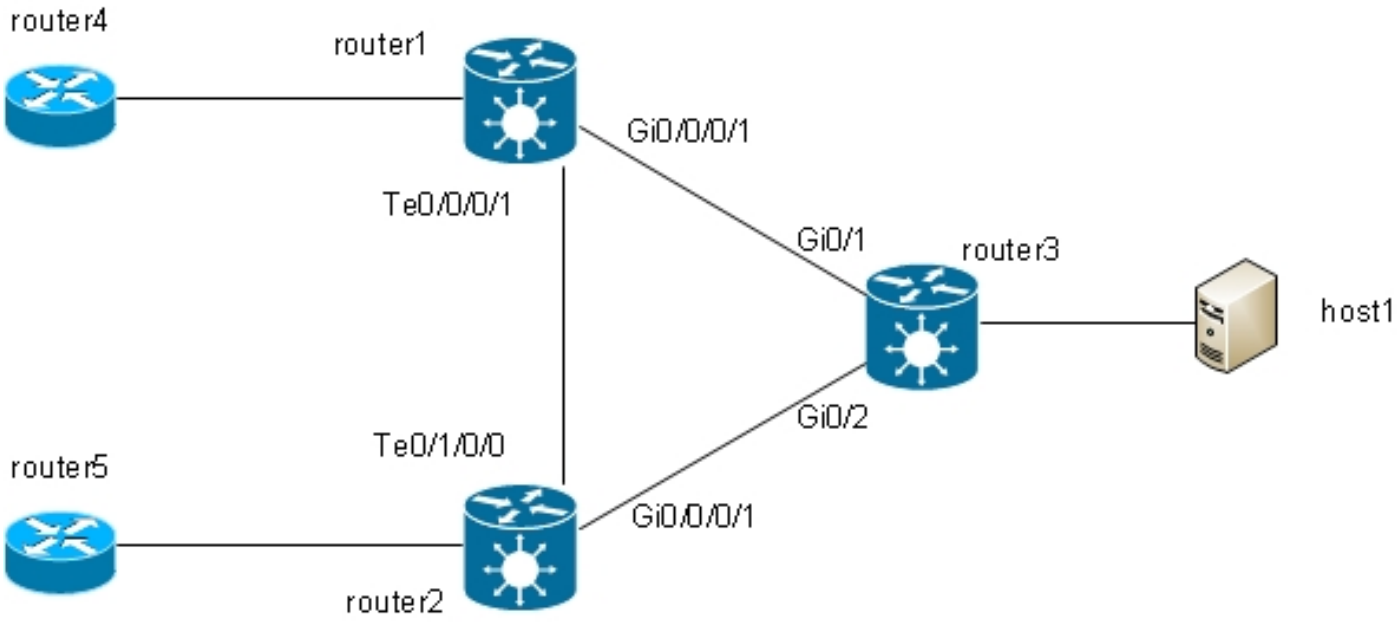
La versión detallada del comando proporciona el número total de direcciones MAC aprendidas en el dominio de bridge, así como el número de direcciones MAC aprendidas en cada CA.

La palabra clave *hardware* sondea la tabla de direcciones mac de hardware directamente desde los motores de reenvío de ingreso o egreso:

```
RP/0/RSP0/CPU0:router1#show l2vpn forwarding bridge-domain customer1:
engineering mac-address hardware ingress location 0/1/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
------------------------------------------------------------------------------
0019.552b.b581 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0024.986c.6417 dynamic Gi0/1/0/38.2 0/1/CPU0 0d 0h 0m 0s N/A
6c9c.ed3e.e484 dynamic Te0/2/0/4.2 0/2/CPU0 0d 0h 0m 0s N/A
RP/0/RSP0/CPU0:router1#show l2vpn forwarding bridge-domain customer1:
engineering mac-address hardware egress location 0/2/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
------------------------------------------------------------------------------
0019.552b.b581 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 14s N/A
0019.552b.b5c3 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 1s N/A
0024.986c.6417 dynamic Gi0/1/0/38.2 0/1/CPU0 0d 0h 0m 10s N/A
6c9c.ed3e.e484 dynamic Te0/2/0/4.2 0/2/CPU0 0d 0h 0m 13s N/A
RP/0/RSP0/CPU0:router1#
```

4.2 MST completo

Los ejemplos anteriores de conmutación local eran básicos porque sólo los routers estaban conectados al dominio de bridge. Sin embargo, una vez que comience a conectar los switches L2, podría introducir un loop y necesitar el STP para romper el loop:



En esta topología, el router1, el router2 y el router3 se configuran con un dominio de puente con todas sus interfaces en el diagrama. Si el router4 envía una transmisión, como una solicitud ARP, al router1, el router1 la inunda al router2 y al router3, el router2 la inunda al router3 y el router3 la inunda al router2. Esto da como resultado un loop y una tormenta de difusión.

Para romper el loop, utilice un STP. Existen varios tipos de STP, pero el software Cisco IOS XR ofrece solamente una implementación completa, el MST.

También hay versiones de gateway de acceso de los protocolos admitidos en el software Cisco IOS XR, como PVSTAG y MSTAG. Se trata de versiones estáticas y limitadas del protocolo que se utilizan en topologías específicas, normalmente con VPLS, y se describen en las secciones MSTAG y PVSTAG. En el software Cisco IOS XR, MST es la única opción si hay una topología con múltiples switches y si se requiere una implementación completa de spanning tree.

Se configuran dos subinterfaces en cada router y se agregan a un dominio de bridge. Para el router 1, la configuración es:

```
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface GigabitEthernet0/0/0/1.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!
interface TenGigE0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface TenGigE0/0/0/1.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!
l2vpn
bridge group customer1
bridge-domain finance
interface TenGigE0/0/0/1.3
!
interface GigabitEthernet0/0/0/1.3
```

```
!
!
bridge-domain engineering
interface TenGigE0/0/0/1.2
!
interface GigabitEthernet0/0/0/1.2
!
!
!
!
```

MST está configurado en la interfaz principal. En este ejemplo, la VLAN 2 se asigna a la instancia 1, y todas las demás VLAN siguen siendo la instancia predeterminada 0. (Una configuración más realista dividiría las VLAN uniformemente entre instancias).

La selección del puente raíz dentro de una red STP está determinada por la prioridad configurada y el ID de puente incrustado de cada dispositivo. El dispositivo con la prioridad más baja, o con la prioridad más baja igual pero el ID de puente más bajo, se selecciona como el puente raíz. En este ejemplo, el router3 se configura con una prioridad más baja que el router1 para la instancia 0, por lo que el router3 es la raíz para la instancia 0. El router1 tiene una prioridad más baja que el router3 para la instancia 1, por lo que el router1 es la raíz para la instancia 1.

Esta es la configuración para el router1:

```
spanning-tree mst customer1
name customer1
revision 1
instance 0
priority 28672
!
instance 1
vlan-ids 2
priority 24576
!
interface TenGigE0/0/0/1
!
interface GigabitEthernet0/0/0/1
!
!
```

Esta es la configuración en el router 3:

```
spanning-tree mode mst
spanning-tree extend system-id
!
spanning-tree mst configuration
name customer1
revision 1
instance 1 vlan 2
!
spanning-tree mst 0 priority 24576
spanning-tree mst 1 priority 28672
```

El nombre, la revisión y la asignación de VLAN a instancia deben ser iguales en todos los switches.

Ahora, verifique el estado del árbol de expansión en el router1:

```
RP/0/RSP1/CPU0:router1#sh spanning-tree mst customer1
```

```
Role: ROOT=Root, DSGN=Designated, ALT=Alternate, BKP=Backup, MSTR=Master
State: FWD=Forwarding, LRN=Learning, BLK=Blocked, DLY=Bringup Delayed

Operating in dot1q mode


MSTI 0 (CIST):

VLANS Mapped: 1,3-4094

CIST Root Priority 24576
Address 001d.4603.1f00
Ext Cost 0

Root ID Priority 24576
Address 001d.4603.1f00
Int Cost 20000
Max Age 20 sec, Forward Delay 15 sec


Bridge ID Priority 28672 (priority 28672 sys-id-ext 0)
Address 4055.3912.f1e6
Max Age 20 sec, Forward Delay 15 sec
Max Hops 20, Transmit Hold count 6


Interface Port ID Role State Designated Port ID
Pri.Nbr Cost Bridge ID Pri.Nbr
------------ ------- --------- ---- ----- -------------------- -------
Gi0/0/0/1 128.2 20000 ROOT FWD 24576 001d.4603.1f00 128.1
Te0/0/0/1 128.1 2000 DSGN FWD 28672 4055.3912.f1e6 128.1


MSTI 1:

VLANS Mapped: 2

Root ID Priority 24576
Address 4055.3912.f1e6
This bridge is the root
Int Cost 0
Max Age 20 sec, Forward Delay 15 sec


Bridge ID Priority 24576 (priority 24576 sys-id-ext 0)
Address 4055.3912.f1e6
Max Age 20 sec, Forward Delay 15 sec
Max Hops 20, Transmit Hold count 6


Interface Port ID Role State Designated Port ID
Pri.Nbr Cost Bridge ID Pri.Nbr
------------ ------- --------- ---- ----- -------------------- -------
Gi0/0/0/1 128.2 20000 DSGN FWD 24576 4055.3912.f1e6 128.2
Te0/0/0/1 128.1 2000 DSGN FWD 24576 4055.3912.f1e6 128.1
```

El Router3 es la raíz para la instancia 0, por lo que el Router1 tiene su puerto raíz en Gi0/0/0/1 hacia el Router3. El Router 1 es la raíz de la instancia 1, por lo que el Router 1 es el puente designado en todas las interfaces para esa instancia.

El Router 2 está bloqueado, por ejemplo, 0 en Te0/1/0/0:

```
RP/0/RSP1/CPU0:router2#sh spanning-tree mst customer1
Role: ROOT=Root, DSGN=Designated, ALT=Alternate, BKP=Backup, MSTR=Master
State: FWD=Forwarding, LRN=Learning, BLK=Blocked, DLY=Bringup Delayed

Operating in dot1q mode


MSTI 0 (CIST):

VLANS Mapped: 1,3-4094

CIST Root Priority 24576
Address 001d.4603.1f00
Ext Cost 0

Root ID Priority 24576
Address 001d.4603.1f00
Int Cost 20000
Max Age 20 sec, Forward Delay 15 sec


Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address f025.72a7.b13e
Max Age 20 sec, Forward Delay 15 sec
Max Hops 20, Transmit Hold count 6


Interface Port ID Role State Designated Port ID
Pri.Nbr Cost Bridge ID Pri.Nbr
------------ ------- --------- ---- ----- -------------------- -------
Gi0/0/0/1 128.2 20000 ROOT FWD 24576 001d.4603.1f00 128.2
Te0/1/0/0    128.1   2000      ALT  BLK   28672 4055.3912.f1e6 128.1


MSTI 1:

VLANS Mapped: 2

Root ID Priority 24576
Address 4055.3912.f1e6
Int Cost 2000
Max Age 20 sec, Forward Delay 15 sec


Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address f025.72a7.b13e
Max Age 20 sec, Forward Delay 15 sec
Max Hops 20, Transmit Hold count 6


Interface Port ID Role State Designated Port ID
Pri.Nbr Cost Bridge ID Pri.Nbr
------------ ------- --------- ---- ----- -------------------- -------
Gi0/0/0/1 128.2 20000 DSGN FWD 32768 f025.72a7.b13e 128.2
Te0/1/0/0 128.1 2000 ROOT FWD 24576 4055.3912.f1e6 128.1
RP/0/RSP1/CPU0:router2#
```

Te0/1/0/0.2 está reenviando mientras Te0/1/0/0.3 está bloqueado. Cuando el valor STP Blocked es 0x0, la condición es false, por lo que la interfaz está reenviando; cuando el valor STP Blocked es 0x1, la condición es true, por lo que la interfaz está bloqueada.

Utilice el comando **show uidb data** para confirmar esto y mostrar los datos de la interfaz que están presentes en el procesador de red:

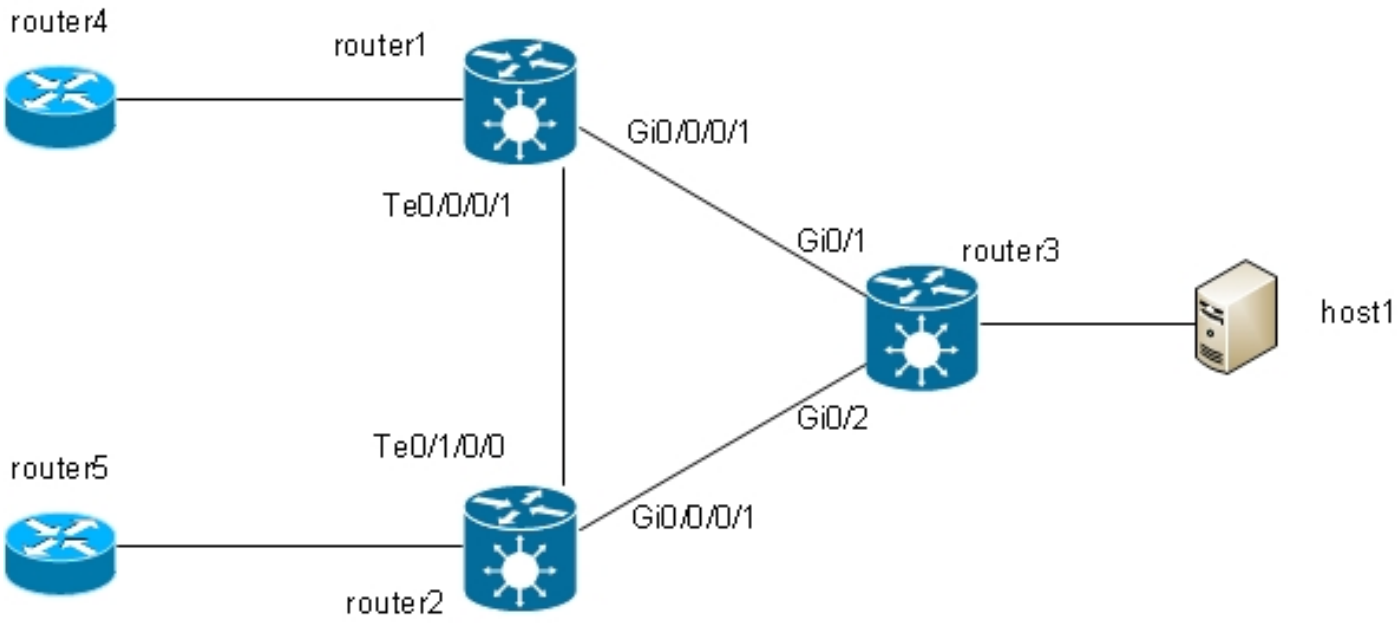
```
RP/0/RSP1/CPU0:router2#sh uidb data location 0/1/CPU0 TenGigE0/1/0/0.2
ingress | i Blocked
STP Blocked                     0x0
RP/0/RSP1/CPU0:router2#sh uidb data location 0/1/CPU0 TenGigE0/1/0/0.3
ingress | i Blocked
STP Blocked                     0x1
```

4.3 BVI

La configuración de un dominio de bridge crea un dominio L2. Para salir de ese dominio L2, conecte los routers L3 que rutean entre los hosts dentro del dominio de bridge y el mundo exterior. En el diagrama anterior, el host1 podría utilizar el router4 o el router5 para salir de la subred local y alcanzar Internet.

Los routers 1 y 2 donde se configuran los dominios de puente son routers ASR 9000, que pueden enrutar tráfico IPv4 e IPv6. Así que estos dos routers podrían sacar el tráfico IP del dominio de puente y rutearlo a Internet ellos mismos, en lugar de depender de routers L3. Para hacer esto, debe configurar una BVI, que es una interfaz L3 que se conecta a un dominio de bridge para rutear paquetes dentro y fuera del dominio de bridge.

Así es como se ve lógicamente:



Esta es la configuración:

```
RP/0/RSP1/CPU0:router1#sh run int bvi 2
interface BVI2
ipv4 address 192.168.2.1 255.255.255.0
!

RP/0/RSP1/CPU0:router1#sh run int bvi 3
interface BVI3
ipv4 address 192.168.3.1 255.255.255.0
!
```

```
RP/0/RSP1/CPU0:router1#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface TenGigE0/0/0/1.3
!
interface GigabitEthernet0/0/0/1.3
!
routed interface BVI3
!
bridge-domain engineering
interface TenGigE0/0/0/1.2
!
interface GigabitEthernet0/0/0/1.2
!
routed interface BVI2
!
!
!
RP/0/RSP1/CPU0:router1#sh run int gig 0/0/0/1.2
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
```

Una BVI es una interfaz L3 sin etiqueta, por lo que si desea que la BVI procese los paquetes recibidos en las AC del dominio de puente, las AC deben configurarse para que aparezcan todas las etiquetas entrantes. De lo contrario, la BVI no puede entender la etiqueta y descarta los paquetes. No hay manera de configurar una subinterfaz dot1q en una BVI, por lo que las etiquetas deben abrirse en la entrada de los AC como se hizo en Gi0/0/0/1.2 en el ejemplo anterior.

Dado que una interfaz BVI es una interfaz virtual, existen algunas restricciones en las funciones que se pueden habilitar. Estas restricciones se documentan en Configuración del Ruteo y Bridging Integrados en el Cisco ASR 9000 Series Router: Restricciones para Configurar IRB. Estas funciones no se admiten en las interfaces BVI de ASR 9000:

- Listas de control de acceso (ACL). Sin embargo, las ACL L2 se pueden configurar en cada puerto L2 del dominio de bridge.
- IP Fast Reroute (FRR)
- Netflow
- MoFRR (solo multidifusión y redireccionamiento rápido)
- MPLS Label Switching
- mVPNv4
- Quality of Service (QoS)
- Duplicación del tráfico
- Interfaz no numerada para BVI
- Supervisión de vídeo (Vidmon)

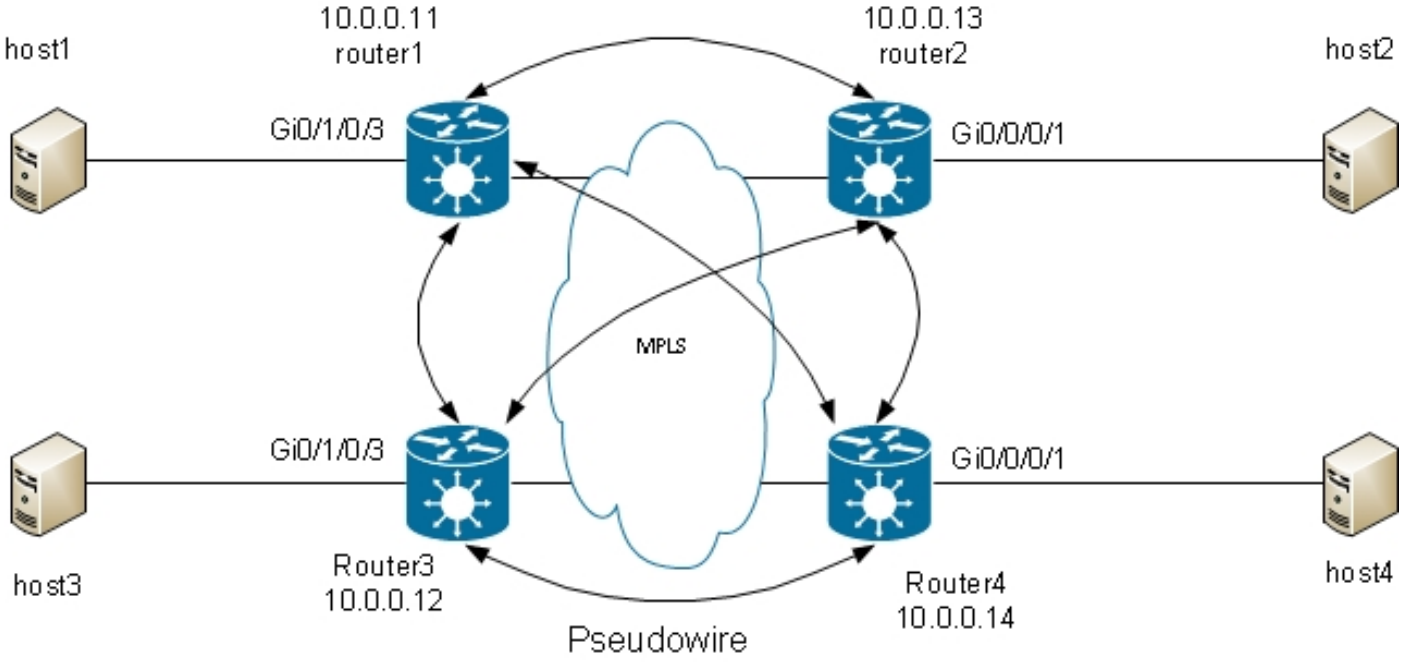
La BVI puede estar en una configuración de reenvío y ruteo virtual (VRF), de modo que el tráfico recibido en la BVI se reenvíe a través de MPLS, pero se debe utilizar *el modo de asignación de etiquetas por vrf*.

Si se requiere una de estas funciones restringidas, no se puede utilizar una BVI. Otra solución es utilizar un cable de loopback externo entre dos puertos en el router, donde un puerto está en el dominio de bridge y un puerto está configurado como una interfaz ruteada normal donde se pueden configurar todas las funciones.

4.4 VPLS

4.4.1 Descripción general

VPLS proporciona la capacidad de combinar dominios de puente en varios sitios en un gran dominio de puente a través de MPLS PW. Los hosts en los diferentes sitios parecen estar conectados directamente al mismo segmento de L2 porque su tráfico se encapsula de manera transparente sobre la malla completa de MPLS PWs entre los PE L2VPN:



Se requiere una malla completa de PW para garantizar que cada host pueda recibir tráfico de todos los demás hosts. La consecuencia es que un PE L2VPN no reenvía una trama recibida en un PW VPLS sobre sus otros PW VPLS. Debe haber una malla completa de PW, por lo que cada PE recibe el tráfico directamente y no necesita reenviar el tráfico entre los PW ya que el reenvío causaría un loop. Esto se denomina regla de horizonte dividido.

El router está ejecutando el aprendizaje de MAC. Una vez que una dirección MAC está presente en la tabla de direcciones MAC, usted reenvía solamente la trama para esa dirección MAC de destino a través del PW al PE L2VPN del cual se ha aprendido esta dirección MAC. Esto evita la duplicación innecesaria del tráfico en el núcleo. Las difusiones y multidifusiones se inundan en todos los PW para garantizar que todos los hosts puedan recibirlas. Una función como la indagación IGMP es útil porque permite que las tramas multicast se envíen a PEs solamente donde hay receptores o routers multicast. Esto reduce la cantidad de tráfico en el núcleo, aunque todavía hay varias copias de los mismos paquetes que se deben enviar a cada PE cuando hay interés por ese grupo.

La malla completa de los PW se debe configurar en una instancia de reenvío virtual (VFI):

```
RP/0/RSP0/CPU0:router1#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/1/0/3.3
```

```
!
vfi customer1-finance
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
vfi customer1-engineering
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!
```

Los PW configurados bajo el VFI son aquellos que están completamente mallados en el núcleo. Forman parte del mismo grupo de horizonte dividido (SHG) para garantizar que las tramas recibidas en un PW no se reenvíen a otro PW.

Es posible configurar los PW de acceso, que se consideran un tipo de AC y no se configuran bajo el VFI. Consulte la sección para obtener más información.

La configuración en el router2, el router3 y el router4 es muy similar, y todos tienen los otros tres routers como vecinos bajo el VFI.

```
RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain bd-name engineering detail
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 6
Filter MAC addresses:
Create time: 28/05/2013 17:17:03 (23:06:02 ago)
```

```
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.2, state is upH-VPLS
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40003; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 234039, sent 7824
bytes: received 16979396, sent 584608
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )
PW class not set, XC ID 0xc0000009
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ----------------------
Label 16049 16042
Group ID 0x5 0x1
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ----------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225481
Create time: 29/05/2013 15:36:17 (00:46:49 ago)
Last time status changed: 29/05/2013 15:57:36 (00:25:29 ago)
```

```
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 555, sent 285
bytes: received 36308, sent 23064
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.13, PW ID 2, state is up ( established )
PW class not set, XC ID 0xc000000a
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ----------------------
Label 16050 16040
Group ID 0x5 0x3
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ----------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225482
Create time: 29/05/2013 15:36:17 (00:46:49 ago)
Last time status changed: 29/05/2013 16:00:56 (00:22:09 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 184, sent 158
bytes: received 12198, sent 14144
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
PW class not set, XC ID 0xc000000b
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ----------------------
Label 16051 289974
Group ID 0x5 0x6
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
```

```
------------ ------------------------------ ----------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225483
Create time: 29/05/2013 15:36:17 (00:46:49 ago)
Last time status changed: 29/05/2013 16:02:38 (00:20:27 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 137
bytes: received 0, sent 12064
DHCPv4 snooping: disabled
IGMP Snooping profile: none
VFI Statistics:
drops: illegal VLAN 0, illegal length 0
```

La etiqueta local para el PW a 10.0.0.12 es 16049, lo que significa que las tramas Ethernet se reciben con la etiqueta 16049. La decisión de switching se basa en esta etiqueta MPLS porque el penúltimo salto MPLS debería haber reventado la etiqueta IGP. Puede que todavía haya una etiqueta nula explícita, pero la decisión de conmutación se basa en la etiqueta PW:

```
RP/0/RSP0/CPU0:router1#sh mpls forwarding labels 16049
Local Outgoing Prefix Outgoing Next Hop Bytes
Label Label or ID Interface Switched
------ ----------- ------------------ ------------ --------------- ----------
16049  Pop         PW(10.0.0.12:2)    BD=5         point2point     58226
```

El comando **show mpls forwarding labels** para la etiqueta proporciona el número de dominio de bridge, que puede utilizar para encontrar la dirección mac de destino y el PW (neighbor y pw-id) donde se recibió el paquete. A continuación, puede crear entradas en la tabla de direcciones mac que apunten a ese vecino:

```
RP/0/RSP0/CPU0:router1#sh l2vpn forwarding bridge-domain customer1:
engineering mac-address location 0/1/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
------------------------------------------------------------------------------
0019.552b.b5c3 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0024.985e.6a01 dynamic (10.0.0.12, 2) 0/1/CPU0 0d 0h 0m 0s N/A
0024.985e.6a42 dynamic (10.0.0.12, 2) 0/1/CPU0 0d 0h 0m 0s N/A
001d.4603.1f42 dynamic (10.0.0.13, 2) 0/1/CPU0 0d 0h 0m 0s N/A
```

4.4.2 Tipos de PW y etiquetas transportadas

Los VPLS PW se negocian como PW de tipo 5 (Ethernet) de forma predeterminada. Lo que entra en la CA después de cualquier manipulación de etiqueta VLAN (cuando se configura el comando **rewrite**) se envía a través de PW.

La versión 4.1.0 del software Cisco IOS XR para señalización LDP y la versión 4.3.1 con BGP le permiten configurar una clase pw bajo un vecino y configurar el **modo de transporte vlan passthrough** bajo la clase pw. Esto negocia un PW de tipo 4 (VLAN Ethernet) de conexión virtual (VC), que transporta lo que salga de la CA después de la manipulación de la etiqueta VLAN cuando se configura el comando **rewrite**.

La manipulación de la etiqueta VLAN en el EFP garantiza que quede al menos una etiqueta VLAN

en la trama porque necesita una etiqueta dot1q en la trama si hay PW de tipo VC 4. No se agrega ninguna etiqueta ficticia 0 a la trama cuando se utiliza el modo de **transporte vlan passthrough**.

No se admite una mezcla de PW de tipo 4 y tipo 5 bajo el mismo VFI. Todos los PW deben ser del mismo tipo.

```
RP/0/RSP0/CPU0:router1#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
bridge group customer1
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
vfi customer1-engineering
neighbor 10.0.0.12 pw-id 2
pw-class VC4-PT
!
neighbor 10.0.0.13 pw-id 2
pw-class VC4-PT
!
neighbor 10.0.0.14 pw-id 2
pw-class VC4-PT
!
!
!
!
!

RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain bd-name engineering detail |
i "PW:|PW type"
MAC withdraw for Access PW: enabled
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )
PW type Ethernet VLAN, control word disabled, interworking none
PW type Ethernet VLAN Ethernet VLAN
PW: neighbor 10.0.0.13, PW ID 2, state is up ( established )
PW type Ethernet VLAN, control word disabled, interworking none
PW type Ethernet VLAN Ethernet VLAN
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
PW type Ethernet VLAN, control word disabled, interworking none
PW type Ethernet VLAN Ethernet VLAN
```

4.4.3 Detección automática y señalización

Los informes se basaban en la configuración manual de todos los vecinos bajo el VFI. Se utilizó MPLS LDP para la señalización del PW con el vecino.ejemplos anteriores

Cuando agregue un nuevo PE VPLS a la red, configure el PE para tener un PW para todos los PE existentes en cada uno de sus dominios de puente locales. Todos los PE existentes se deben volver a configurar para tener un PW en el nuevo PE porque todos los PE deben tener una malla completa. Esto podría convertirse en un desafío operativo a medida que aumente el número de PE y dominios de puente.

Una solución es hacer que los PE detecten otros PE automáticamente a través de BGP. Aunque también hay un requisito de malla completa para IBGP, puede ser levantado mediante el uso de reflectores de ruta. Por lo tanto, un nuevo PE se configura típicamente para hacer peer con un pequeño número de reflectores de ruta, todos los otros PE reciben sus actualizaciones y el nuevo PE recibe las actualizaciones de los otros PE.

Para detectar otros PE a través de BGP, cada PE se configura para la *familia de direcciones vpls-vpws* y anuncia en BGP los dominios de puente en los que desean participar. Una vez que se descubren los otros PE que forman parte del mismo dominio de puente, se establece un PW para cada uno de ellos. BGP es el protocolo utilizado para esta detección automática.

Hay dos opciones para la señalización del PW a los PE descubiertos automáticamente: BGP y LDP. En estos ejemplos, usted convierte la topología anterior a la detección automática de BGP con la señalización BGP y la señalización LDP.

4.4.3.1 Detección automática BGP y señalización BGP

Configure la **familia de direcciones l2vpn vpls-vpws** bajo router bgp y los vecinos, que son otros PE o los reflectores de ruta:

```
router bgp 65000
address-family l2vpn vpls-vpws
!
neighbor-group IOX-LAB-RR
address-family l2vpn vpls-vpws
!
neighbor 10.0.0.3
use neighbor-group IOX-LAB-RR
!
neighbor 10.0.0.10
use neighbor-group IOX-LAB-RR
!
```

La nueva familia de direcciones se activa con los vecinos, pero ningún PE ha anunciado su participación en un dominio de puente:

```
RP/0/RSP0/CPU0:router1#sh bgp neighbor 10.0.0.3 | i Address family L2VPN
Address family L2VPN VPLS: advertised and received

P/0/RSP0/CPU0:router1#sh bgp l2vpn vpls summary
BGP router identifier 10.0.0.11, local AS number 65000
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0 RD version: 3890838096
BGP main routing table version 77
BGP scan interval 60 secs

BGP is operating in STANDALONE mode.


Process RcvTblVer bRIB/RIB LabelVer ImportVer SendTblVer StandbyVer
Speaker 77 77 77 77 77 77

Neighbor Spk AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down St/PfxRcd
10.0.0.3 0 65000 252950 53252 77 0 0 1w0d 0
10.0.0.10 0 65000 941101 47439 77 0 0 00:10:18 0
```

Configure **autodiscovery bgp** y **signaling-protocol bgp** en el modo de configuración de L2VPN bridge-domain. La configuración en el router1 es:

```
RP/0/RSP0/CPU0:router1#sh run l2vpn bridge group customer1
l2vpn
```

```
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/1/0/3.3
!
vfi customer1-finance
vpn-id 3
autodiscovery bgp
rd auto
route-target 0.0.0.1:3
signaling-protocol bgp
ve-id 11
!
!
!
!
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
vfi customer1-engineering
vpn-id 2
autodiscovery bgp
rd auto
route-target 0.0.0.1:2
signaling-protocol bgp
ve-id 11
!
!
!
!
!
!
```

La configuración en el router2 es:

```
RP/0/RSP1/CPU0:router2#sh run l2vpn bridge group customer1
Thu May 30 15:25:55.638 CEST
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/0/0/1.3
!
vfi customer1-finance
vpn-id 3
autodiscovery bgp
rd auto
route-target 0.0.0.1:3
signaling-protocol bgp
ve-id 13
!
!
!
!
bridge-domain engineering
interface GigabitEthernet0/0/0/1.2
!
vfi customer1-engineering
vpn-id 2
autodiscovery bgp
rd auto
route-target 0.0.0.1:2
signaling-protocol bgp
ve-id 13
!
```

```
!
!
!
!
!
```

El vpn-id y el route-target son iguales en los diferentes PE para cada dominio de bridge, pero cada PE tiene un identificador de borde virtual (VE-ID) único. Cada PE detecta los otros PE en la VPN a través de BGP y utiliza BGP para señalar los PW. El resultado es una malla completa de PW:

```
RP/0/RSP0/CPU0:router1#sh bgp l2vpn vpls summary
BGP router identifier 10.0.0.11, local AS number 65000
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0 RD version: 3890838096
BGP main routing table version 103
BGP scan interval 60 secs

BGP is operating in STANDALONE mode.


Process RcvTblVer bRIB/RIB LabelVer ImportVer SendTblVer StandbyVer
Speaker 103 103 103 103 103 103

Neighbor Spk AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down St/PfxRcd
10.0.0.3 0 65000 254944 53346 103 0 0 1w0d 6
10.0.0.10 0 65000 944859 47532 103 0 0 01:40:22 6

RP/0/RSP0/CPU0:router1#sh bgp l2vpn vpls
BGP router identifier 10.0.0.11, local AS number 65000
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0 RD version: 3890838096
BGP main routing table version 103
BGP scan interval 60 secs

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 Rcvd Label Local Label
Route Distinguisher: 10.0.0.11:32769 (default for vrf customer1:finance)
*> 11:10/32 0.0.0.0 nolabel 16060
*>i12:10/32 10.0.0.12 16060 nolabel
*>i13:10/32 10.0.0.13 16060 nolabel
*>i14:10/32 10.0.0.14 289959 nolabel
Route Distinguisher: 10.0.0.11:32770 (default for vrf customer1:engineering)
*> 11:10/32 0.0.0.0 nolabel 16075
*>i12:10/32 10.0.0.12 16075 nolabel
*>i13:10/32 10.0.0.13 16075 nolabel
*>i14:10/32 10.0.0.14 289944 nolabel
Route Distinguisher: 10.0.0.12:32768
*>i12:10/32 10.0.0.12 16060 nolabel
* i 10.0.0.12 16060 nolabel
Route Distinguisher: 10.0.0.12:32769
*>i12:10/32 10.0.0.12 16075 nolabel
* i 10.0.0.12 16075 nolabel
Route Distinguisher: 10.0.0.13:32769
*>i13:10/32 10.0.0.13 16060 nolabel
* i 10.0.0.13 16060 nolabel
Route Distinguisher: 10.0.0.13:32770
*>i13:10/32 10.0.0.13 16075 nolabel
```

```
* i 10.0.0.13 16075 nolabel
Route Distinguisher: 10.0.0.14:32768
*>i14:10/32 10.0.0.14 289959 nolabel
* i 10.0.0.14 289959 nolabel
Route Distinguisher: 10.0.0.14:32769
*>i14:10/32 10.0.0.14 289944 nolabel
* i 10.0.0.14 289944 nolabel

Processed 14 prefixes, 20 paths
```

Éstos son los prefijos anunciados por el router3 (10.0.0.13) como se ven en el router1; los prefijos se reciben a través de los dos reflectores de ruta, 10.0.0.3 y 10.0.0.10:

```
RP/0/RSP0/CPU0:router1#sh bgp l2vpn vpls rd 10.0.0.13:32770 13:10/32
BGP routing table entry for 13:10/32, Route Distinguisher: 10.0.0.13:32770
Versions:
Process bRIB/RIB SendTblVer
Speaker 92 92
Last Modified: May 30 15:10:44.100 for 01:23:38
Paths: (2 available, best #1)
Not advertised to any peer
Path #1: Received by speaker 0
Not advertised to any peer
Local
10.0.0.13 (metric 5) from 10.0.0.3 (10.0.0.13)
Received Label 16075
Origin IGP, localpref 100, valid, internal, best, group-best,
import-candidate, not-in-vrf, import suspect
Received Path ID 0, Local Path ID 1, version 92
Extended community: RT:0.0.0.1:2 L2VPN:19:0:1500
Originator: 10.0.0.13, Cluster list: 10.0.0.3
Block Size:10
Path #2: Received by speaker 0
Not advertised to any peer
Local
10.0.0.13 (metric 5) from 10.0.0.10 (10.0.0.13)
Received Label 16075
Origin IGP, localpref 100, valid, internal, not-in-vrf, import suspect
Received Path ID 0, Local Path ID 0, version 0
Extended community: RT:0.0.0.1:2 L2VPN:19:0:1500
Originator: 10.0.0.13, Cluster list: 10.0.0.10
Block Size:10
RP/0/RSP0/CPU0:router1#sh bgp l2vpn vpls rd 10.0.0.13:32769 13:10/32
BGP routing table entry for 13:10/32, Route Distinguisher: 10.0.0.13:32769
Versions:
Process bRIB/RIB SendTblVer
Speaker 93 93
Last Modified: May 30 15:10:44.100 for 01:25:02
Paths: (2 available, best #1)
Not advertised to any peer
Path #1: Received by speaker 0
Not advertised to any peer
Local
10.0.0.13 (metric 5) from 10.0.0.3 (10.0.0.13)
Received Label 16060
Origin IGP, localpref 100, valid, internal, best, group-best,
import-candidate, not-in-vrf, import suspect
Received Path ID 0, Local Path ID 1, version 93
Extended community: RT:0.0.0.1:3 L2VPN:19:0:1500
Originator: 10.0.0.13, Cluster list: 10.0.0.3
Block Size:10
Path #2: Received by speaker 0
Not advertised to any peer
```

```
Local
10.0.0.13 (metric 5) from 10.0.0.10 (10.0.0.13)
Received Label 16060
Origin IGP, localpref 100, valid, internal, not-in-vrf, import suspect
Received Path ID 0, Local Path ID 0, version 0
Extended community: RT:0.0.0.1:3 L2VPN:19:0:1500
Originator: 10.0.0.13, Cluster list: 10.0.0.10
Block Size:10
```

El Router1 ha establecido algunos PW:

```
RP/0/RSP0/CPU0:router1#sh l2vpn discovery bridge-domain

Service Type: VPLS, Connected
List of VPNs (2 VPNs):
Bridge group: customer1, bridge-domain: finance, id: 3, signaling
protocol: BGP
List of Local Edges (1 Edges):
Local Edge ID: 11, Label Blocks (1 Blocks)
Label base Offset Size Time Created
---------- ------ ---- -------------------
16060 10 10 05/30/2013 15:07:39
List of Remote Edges (3 Edges):
Remote Edge ID: 12, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created
---------- ------ ---- ------------ -------------------
16060 10 10 10.0.0.12 05/30/2013 15:09:53
Remote Edge ID: 13, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created
---------- ------ ---- ------------ -------------------
16060 10 10 10.0.0.13 05/30/2013 15:10:43
Remote Edge ID: 14, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created
---------- ------ ---- ------------ -------------------
289959 10 10 10.0.0.14 05/30/2013 15:11:22

Bridge group: customer1, bridge-domain: engineering, id: 5, signaling
protocol: BGP
List of Local Edges (1 Edges):
Local Edge ID: 11, Label Blocks (1 Blocks)
Label base Offset Size Time Created
---------- ------ ---- -------------------
16075 10 10 05/30/2013 15:08:54
List of Remote Edges (3 Edges):
Remote Edge ID: 12, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created
---------- ------ ---- ------------ -------------------
16075 10 10 10.0.0.12 05/30/2013 15:09:53
Remote Edge ID: 13, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created
---------- ------ ---- ------------ -------------------
16075 10 10 10.0.0.13 05/30/2013 15:10:43
Remote Edge ID: 14, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created
---------- ------ ---- ------------ -------------------
289944 10 10 10.0.0.14 05/30/2013 15:11:22

RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain autodiscovery bgp
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
```

```
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of VFIs:
VFI customer1-finance (up)
Neighbor 10.0.0.12 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 3, state: up, Static MAC addresses: 0
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0

RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain group customer1
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.3, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-finance (up)
Neighbor 10.0.0.12 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 3, state: up, Static MAC addresses: 0
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.2, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0

RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain group customer1 detail
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
```

```
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 4
Filter MAC addresses:
Create time: 29/05/2013 15:36:17 (1d01h ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.3, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [3, 3]
MTU 1500; XC ID 0xc40006; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 10120, sent 43948
bytes: received 933682, sent 2989896
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
List of Access PWs:
List of VFIs:
VFI customer1-finance (up)
VPN-ID: 3, Auto Discovery: BGP, state is Provisioned
(Service Connected)
Route Distinguisher: (auto) 10.0.0.11:32769
Import Route Targets:
0.0.0.1:3
Export Route Targets:
0.0.0.1:3
Signaling protocol: BGP
Local VE-ID: 11 , Advertised Local VE-ID : 11
VE-Range: 10
PW: neighbor 10.0.0.12, PW ID 3, state is up ( established )
PW class not set, XC ID 0xc000000c
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP
Source address 10.0.0.11
PW type VPLS, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

MPLS Local Remote
------------ ------------------------------ ------------------
```

```
Label 16062 16061
MTU 1500 1500
Control word disabled disabled
PW type VPLS VPLS
VE-ID 11 12
------------ ------------------------------ ------------------
MIB cpwVcIndex: 3221225484
Create time: 30/05/2013 15:09:52 (01:29:44 ago)
Last time status changed: 30/05/2013 15:09:52 (01:29:44 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 2679, sent 575
bytes: received 171698, sent 51784
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.13, PW ID 3, state is up ( established )
PW class not set, XC ID 0xc000000e
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP
Source address 10.0.0.11
PW type VPLS, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

MPLS Local Remote
------------ ------------------------------ ------------------
Label 16063 16061
MTU 1500 1500
Control word disabled disabled
PW type VPLS VPLS
VE-ID 11 13
------------ ------------------------------ ------------------
MIB cpwVcIndex: 3221225486
Create time: 30/05/2013 15:10:43 (01:28:54 ago)
Last time status changed: 30/05/2013 15:10:43 (01:28:54 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 11, sent 574
bytes: received 1200, sent 51840
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.14, PW ID 3, state is up ( established )
PW class not set, XC ID 0xc0000010
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP
Source address 10.0.0.11
PW type VPLS, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

MPLS Local Remote
------------ ------------------------------ ------------------
Label 16064 289960
MTU 1500 1500
Control word disabled disabled
PW type VPLS VPLS
VE-ID 11 14
------------ ------------------------------ ------------------
MIB cpwVcIndex: 3221225488
Create time: 30/05/2013 15:11:22 (01:28:15 ago)
Last time status changed: 30/05/2013 15:11:22 (01:28:15 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
```

```
packets: received 0, sent 561
bytes: received 0, sent 50454
DHCPv4 snooping: disabled
IGMP Snooping profile: none
VFI Statistics:
drops: illegal VLAN 0, illegal length 0
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 6
Filter MAC addresses:
Create time: 28/05/2013 17:17:03 (1d23h ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40007; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 243532, sent 51089
bytes: received 17865888, sent 3528732
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
List of Access PWs:
```

```
List of VFIs:
VFI customer1-engineering (up)
VPN-ID: 2, Auto Discovery: BGP, state is Provisioned
(Service Connected)
Route Distinguisher: (auto) 10.0.0.11:32770
Import Route Targets:
0.0.0.1:2
Export Route Targets:
0.0.0.1:2
Signaling protocol: BGP
Local VE-ID: 11 , Advertised Local VE-ID : 11
VE-Range: 10
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )
PW class not set, XC ID 0xc000000d
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP
Source address 10.0.0.11
PW type VPLS, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

MPLS Local Remote
------------ ------------------------------ ------------------
Label 16077 16076
MTU 1500 1500
Control word disabled disabled
PW type VPLS VPLS
VE-ID 11 12
------------ ------------------------------ ------------------
MIB cpwVcIndex: 3221225485
Create time: 30/05/2013 15:09:52 (01:29:45 ago)
Last time status changed: 30/05/2013 15:09:52 (01:29:45 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 2677, sent 574
bytes: received 171524, sent 51670
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.13, PW ID 2, state is up ( established )
PW class not set, XC ID 0xc000000f
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP
Source address 10.0.0.11
PW type VPLS, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

MPLS Local Remote
------------ ------------------------------ ------------------
Label 16078 16076
MTU 1500 1500
Control word disabled disabled
PW type VPLS VPLS
VE-ID 11 13
------------ ------------------------------ ------------------
MIB cpwVcIndex: 3221225487
Create time: 30/05/2013 15:10:43 (01:28:54 ago)
Last time status changed: 30/05/2013 15:10:43 (01:28:54 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 17, sent 572
bytes: received 1560, sent 51636
DHCPv4 snooping: disabled
IGMP Snooping profile: none
```

```
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
PW class not set, XC ID 0xc0000011
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP
Source address 10.0.0.11
PW type VPLS, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

MPLS Local Remote
------------ ------------------------------ ------------------
Label 16079 289945
MTU 1500 1500
Control word disabled disabled
PW type VPLS VPLS
VE-ID 11 14
------------ ------------------------------ ------------------
MIB cpwVcIndex: 3221225489
Create time: 30/05/2013 15:11:22 (01:28:16 ago)
Last time status changed: 30/05/2013 15:11:22 (01:28:16 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 559
bytes: received 0, sent 50250
DHCPv4 snooping: disabled
IGMP Snooping profile: none
VFI Statistics:
drops: illegal VLAN 0, illegal length 0
```

4.4.3.2 Detección automática BGP y señalización LDP

La configuración BGP con el comando **address-family l2vpn vpls-vpws** es exactamente la misma que con la señalización BGP. La configuración L2VPN se modifica para utilizar la señalización LDP con el comando **signaling-protocol ldp**.

Se utiliza la misma configuración en los cuatro PE:

```
router bgp 65000
address-family l2vpn vpls-vpws
!
neighbor-group IOX-LAB-RR
address-family l2vpn vpls-vpws
!
neighbor 10.0.0.3
use neighbor-group IOX-LAB-RR
!
neighbor 10.0.0.10
use neighbor-group IOX-LAB-RR
!
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/1/0/3.3
!
vfi customer1-finance
vpn-id 3
autodiscovery bgp
rd auto
route-target 0.0.0.1:3
signaling-protocol ldp
```

```
vpls-id 65000:3
!
!
!
!
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
vfi customer1-engineering
vpn-id 2
autodiscovery bgp
rd auto
route-target 0.0.0.1:2
signaling-protocol ldp
      vpls-id 65000:2
!
!
!
!
!
!
```

El vpls-id está formado por el número del Sistema Autónomo BGP (AS) y el vpn-id.

Tres comandos show del router1 ilustran que los PW se han establecido con los PE detectados:

```
RP/0/RSP0/CPU0:router1#sh l2vpn discovery

Service Type: VPLS, Connected
List of VPNs (2 VPNs):
Bridge group: customer1, bridge-domain: finance, id: 3,
signaling protocol: LDP
VPLS-ID: 65000:3
Local L2 router id: 10.0.0.11
List of Remote NLRI (3 NLRIs):
Local Addr Remote Addr Remote L2 RID Time Created
--------------- --------------- --------------- -------------------
10.0.0.11 10.0.0.12 10.0.0.12 05/30/2013 17:10:18
10.0.0.11 10.0.0.13 10.0.0.13 05/30/2013 17:10:18
10.0.0.11 10.0.0.14 10.0.0.14 05/30/2013 17:11:46

Bridge group: customer1, bridge-domain: engineering, id: 5,
signaling protocol: LDP
VPLS-ID: 65000:2
Local L2 router id: 10.0.0.11
List of Remote NLRI (3 NLRIs):
Local Addr Remote Addr Remote L2 RID Time Created
--------------- --------------- --------------- -------------------
10.0.0.11 10.0.0.12 10.0.0.12 05/30/2013 17:10:18
10.0.0.11 10.0.0.13 10.0.0.13 05/30/2013 17:10:18
10.0.0.11 10.0.0.14 10.0.0.14 05/30/2013 17:11:46

RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain group customer1
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.3, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
```

```
VFI customer1-finance (up)
Neighbor 10.0.0.12 pw-id 65000:3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 65000:3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 65000:3, state: up, Static MAC addresses: 0
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.2, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.12 pw-id 65000:2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 65000:2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 65000:2, state: up, Static MAC addresses: 0

RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain group customer1 det
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 4
Filter MAC addresses:
Create time: 29/05/2013 15:36:17 (1d01h ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.3, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [3, 3]
MTU 1500; XC ID 0xc40006; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
```

```
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 10362, sent 45038
bytes: received 956240, sent 3064016
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
List of Access PWs:
List of VFIs:
VFI customer1-finance (up)
VPN-ID: 3, Auto Discovery: BGP, state is Provisioned
(Service Connected)
Route Distinguisher: (auto) 10.0.0.11:32769
Import Route Targets:
0.0.0.1:3
Export Route Targets:
0.0.0.1:3
Signaling protocol: LDP
AS Number: 65000
VPLS-ID: 65000:3
L2VPN Router ID: 10.0.0.11
PW: neighbor 10.0.0.12, PW ID 65000:3, state is up ( established )
PW class not set, XC ID 0xc0000003
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------
Label 16006 16033
BGP Peer ID 10.0.0.11 10.0.0.12
LDP ID 10.0.0.11 10.0.0.12
AII 10.0.0.11 10.0.0.12
AGI 65000:3 65000:3
Group ID 0x3 0x0
Interface customer1-finance customer1-finance
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225475
Create time: 30/05/2013 17:10:18 (00:06:32 ago)
Last time status changed: 30/05/2013 17:10:24 (00:06:25 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 190, sent 40
bytes: received 12160, sent 3600
```

```
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.13, PW ID 65000:3, state is up ( established )
PW class not set, XC ID 0xc0000004
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------
Label 16016 16020
BGP Peer ID 10.0.0.11 10.0.0.13
LDP ID 10.0.0.11 10.0.0.13
AII 10.0.0.11 10.0.0.13
AGI 65000:3 65000:3
Group ID 0x3 0x4
Interface customer1-finance customer1-finance
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225476
Create time: 30/05/2013 17:10:18 (00:06:32 ago)
Last time status changed: 30/05/2013 17:10:27 (00:06:22 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 40
bytes: received 0, sent 3600
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.14, PW ID 65000:3, state is up ( established )
PW class not set, XC ID 0xc0000009
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------
Label 16049 289970
BGP Peer ID 10.0.0.11 10.0.0.14
LDP ID 10.0.0.11 10.0.0.14
AII 10.0.0.11 10.0.0.14
AGI 65000:3 65000:3
Group ID 0x3 0x4
Interface customer1-finance customer1-finance
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
```

```
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225481
Create time: 30/05/2013 17:11:46 (00:05:04 ago)
Last time status changed: 30/05/2013 17:11:51 (00:04:59 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 31
bytes: received 0, sent 2790
DHCPv4 snooping: disabled
IGMP Snooping profile: none
VFI Statistics:
drops: illegal VLAN 0, illegal length 0
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 6
Filter MAC addresses:
Create time: 28/05/2013 17:17:03 (1d23h ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40007; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
```

```
Static MAC addresses:
Statistics:
packets: received 243774, sent 52179
bytes: received 17888446, sent 3602852
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
VPN-ID: 2, Auto Discovery: BGP, state is Provisioned (Service Connected)
Route Distinguisher: (auto) 10.0.0.11:32770
Import Route Targets:
0.0.0.1:2
Export Route Targets:
0.0.0.1:2
Signaling protocol: LDP
AS Number: 65000
VPLS-ID: 65000:2
L2VPN Router ID: 10.0.0.11
PW: neighbor 10.0.0.12, PW ID 65000:2, state is up ( established )
PW class not set, XC ID 0xc0000005
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------
Label 16027 16042
BGP Peer ID 10.0.0.11 10.0.0.12
LDP ID 10.0.0.11 10.0.0.12
AII 10.0.0.11 10.0.0.12
AGI 65000:2 65000:2
Group ID 0x5 0x1
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 0
Create time: 30/05/2013 17:10:18 (00:06:33 ago)
Last time status changed: 30/05/2013 17:10:24 (00:06:26 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 190, sent 41
bytes: received 12160, sent 3690
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.13, PW ID 65000:2, state is up ( established )
```

```
PW class not set, XC ID 0xc0000006
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------
Label 16043 16021
BGP Peer ID 10.0.0.11 10.0.0.13
LDP ID 10.0.0.11 10.0.0.13
AII 10.0.0.11 10.0.0.13
AGI 65000:2 65000:2
Group ID 0x5 0x3
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 0
Create time: 30/05/2013 17:10:18 (00:06:33 ago)
Last time status changed: 30/05/2013 17:10:27 (00:06:23 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 40
bytes: received 0, sent 3600
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.14, PW ID 65000:2, state is up ( established )
PW class not set, XC ID 0xc000000a
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------
Label 16050 289974
BGP Peer ID 10.0.0.11 10.0.0.14
LDP ID 10.0.0.11 10.0.0.14
AII 10.0.0.11 10.0.0.14
AGI 65000:2 65000:2
Group ID 0x5 0x6
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
```

```
------------ ------------------------------ ------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225482
Create time: 30/05/2013 17:11:46 (00:05:05 ago)
Last time status changed: 30/05/2013 17:11:51 (00:05:00 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 31
bytes: received 0, sent 2790
DHCPv4 snooping: disabled
IGMP Snooping profile: none
VFI Statistics:
drops: illegal VLAN 0, illegal length 0
```

4.4.4 Vaciados y retiradas de MAC

El reenvío en VPLS se basa en la tabla de direcciones MAC, que se construye dinámicamente al aprender las direcciones MAC de origen de las tramas que se reciben. Si hay un cambio de topología en un dominio de bridge, un host puede volverse accesible a través de un vecino AC o VPLS diferente. Es posible que el tráfico de ese host no llegue a su destino si las tramas se siguen reenviando según la tabla de direcciones mac existente.

Para un PE L2VPN, hay varias maneras de detectar un cambio de topología:

- Un puerto en el dominio de bridge sube o baja.
- Una BPDU de Notificación de cambio de topología (TCN) de árbol de expansión se procesa cuando el PE L2VPN ejecuta la implementación MST completa o un protocolo de gateway de acceso al árbol de expansión. Es posible que el link que falla no sea local en el PE, pero puede estar más lejos en la topología. El PE intercepta el TCN.

Cuando un PE L2VPN detecta un cambio de topología, realiza dos acciones:

1. El PE purga la tabla de direcciones mac de los dominios de puente afectados por el cambio de topología. Cuando el PE se configura para PVSTAG o para el Rapid Spanning Tree Access Gateway (PVRSTAG) por VLAN, una TCN BPDU detectada en una subinterfaz VLAN afecta a todas las VLAN y dominios de puente en esa interfaz física.
2. El PE envía señales a los vecinos VPLS a través de un mensaje de retiro de MAC MPLS LDP que deben vaciar su tabla de direcciones MAC. Todos los PE L2VPN remotos que reciben el mensaje LDP de retiro de MAC vacian sus tablas de direcciones mac y el tráfico se inunda nuevamente. Las tablas de direcciones MAC se reconstruyen en función de la nueva topología.

El comportamiento predeterminado del mensaje de retiro de MAC en caso de inestabilidad del puerto ha cambiado con el tiempo:

- Tradicionalmente, en el software Cisco IOS XR, un PE L2VPN enviaba mensajes de retiro de MAC cuando un AC se apagaba. La intención era hacer que los PE remotos vaciaran sus tablas de direcciones MAC para el dominio de bridge impactado de modo que las direcciones MAC que apuntan detrás del puerto caído se aprendan de otro puerto.
- Sin embargo, esto creó un problema de interoperabilidad con algunos PE remotos que siguen RFC 4762 y purgan las direcciones MAC que apuntan a todos los PE excepto el que está enviando el mensaje de retiro MAC. RFC 4762 asume que un PE enviaría un mensaje de

retiro MAC cuando un AC aparece pero no cuando un AC se desactiva. Después de Cisco IOS XR Software Release 4.2.1, el comportamiento predeterminado es enviar mensajes de retiro de MAC LDP solamente cuando se activa un puerto de dominio de bridge para cumplir mejor con el RFC. Se agregó un comando de configuración para volver al comportamiento anterior.

Este es un comando show con el comportamiento predeterminado después de la versión 4.2.1 del software Cisco IOS XR:

```
RP/0/RSP1/CPU0:router3#sh l2vpn bridge-domain bd-name engineering det |
i "PW:|VFI|neighbor|MAC w"
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of VFIs:
VFI customer1-engineering (up)
PW: neighbor 10.0.0.11, PW ID 2, state is up ( established )
MAC withdraw message: send 0 receive 0
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )
MAC withdraw message: send 0 receive 4
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
MAC withdraw message: send 0 receive 2
VFI Statistics:
```

La línea importante es la 'MAC remove sent on bridge port down', que ahora está inhabilitada de forma predeterminada después de la versión 4.2.1 del software Cisco IOS XR. El comando también proporciona el número de mensajes de retiro MAC enviados y recibidos en el dominio de bridge. Un alto número de mensajes de retiro indica inestabilidad en el dominio de bridge.

Ésta es la configuración que vuelve al comportamiento anterior:

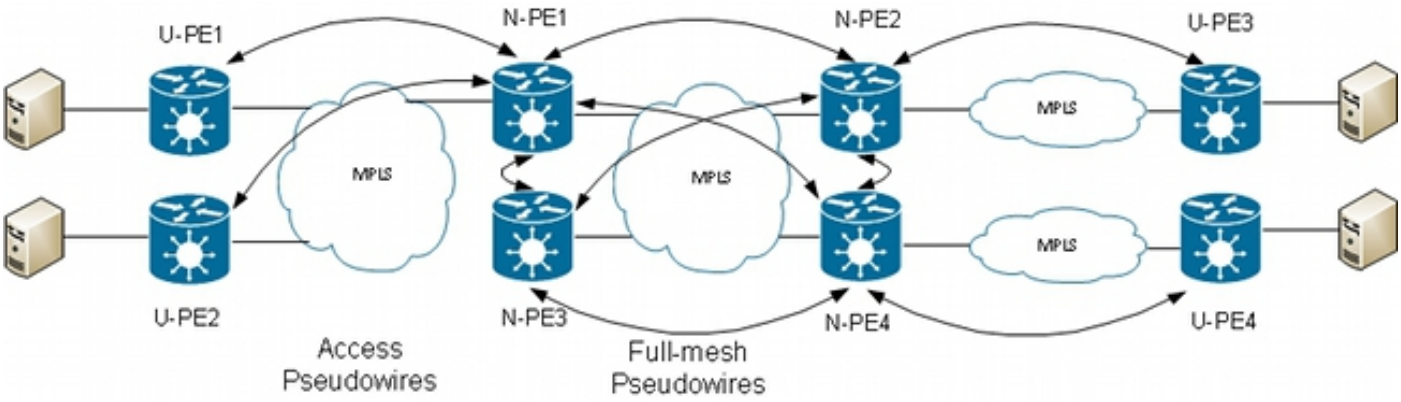
```
l2vpn
bridge group customer1
bridge-domain finance
mac
withdraw state-down
!
!
!
!
```

4.4.5 H-VPLS

VPLS requiere una malla completa de PW entre los PE L2VPN para garantizar que cualquier PE pueda alcanzar, en un salto, un host detrás de cualquier otro PE sin la necesidad de que un PE refleje las tramas de un PW a otro PW. Esta es la base para la regla de horizonte dividido, que impide que un PE reenvíe tramas de un PW a otro PW. Incluso en casos especiales, cuando la dirección MAC de destino en la tabla de direcciones MAC apunta a otro PW, la trama se descarta.

Una malla completa de PW significa que el número de PW podría llegar a ser muy alto a medida que el número de PE crece, por lo que esto podría introducir problemas de escalabilidad.

Puede disminuir el número de PW en esta topología con una jerarquía de PE:



En esta topología, tenga en cuenta que:

- Un dispositivo de borde del proveedor del usuario (U-PE) tiene CA en los CE.
- El dispositivo U-PE transporta el tráfico CE a través de un PW punto a punto MPLS a un dispositivo de extremo del proveedor de red (N-PE).
- El N-PE es un PE VPLS de núcleo que está completamente mallado con otros N-PE.
- En el N-PE, el PW que viene del U-PE se considera un PW de acceso muy parecido a un AC. El U-PE no forma parte de la malla con los otros N-PE, por lo que el N-PE puede considerar el PW de acceso como un AC y reenviar el tráfico de ese PW de acceso a los PW de núcleo que forman parte de la malla completa VPLS.
- Los PW de núcleo entre N-PE se configuran bajo una VFI para garantizar que la regla de horizonte dividido se aplique a todos los PW de núcleo configurados bajo la VFI.
- Los PW de acceso de U-PE no se configuran en una VFI, por lo que no pertenecen al mismo SHG que los PW de VFI. El tráfico se puede reenviar desde un PW de acceso a un PW de VFI y viceversa.
- Los U-PE pueden utilizar la función de redundancia de PW para tener un PW principal a un N-PE principal y tener un PW en espera a un N-PE en espera. El modo de espera toma el control cuando el PW primario deja de funcionar.

Este es un ejemplo donde U-PE1 (10.0.0.15) se configura con redundancia PW a N-PE1 (10.0.0.11) y N-PE2 (10.0.0.12):

```
RP/0/RP0/CPU0:U-PE1#sh run int ten 0/1/0/5.2
interface TenGigE0/1/0/5.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!

RP/0/RP0/CPU0:U-PE1#sh run l2vpn xconnect group customer1
l2vpn
xconnect group customer1
p2p engineering-0-1-0-5
interface TenGigE0/1/0/5.2
neighbor 10.0.0.11 pw-id 15
backup neighbor 10.0.0.12 pw-id 15
!
!
!
!
!

RP/0/RP0/CPU0:U-PE1#sh l2vpn xconnect group customer1
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
```

```
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
---------------------- ---------------------- ----------------------------
customer1 engineering-0-1-0-5
UP Te0/1/0/5.2 UP 10.0.0.11 15 UP
Backup
10.0.0.12 15 SB
------------------------------------------------------------------------------
```

El PW a 10.0.0.12 está en estado de espera. En N-PE1, hay un PW de acceso a 10.0.0.15 y un AC que no están bajo el VFI.

N-PE1 está aprendiendo algunas direcciones MAC a través del PW de acceso y los PW de VFI:

```
RP/0/RSP0/CPU0:N-PE1#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
bridge group customer1
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
neighbor 10.0.0.15 pw-id 15
!
vfi customer1-engineering
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!
RP/0/RSP0/CPU0:N-PE1#sh l2vpn bridge-domain bd-name engineering
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 4 (4 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.2, state: up, Static MAC addresses: 0
List of Access PWs:
Neighbor 10.0.0.15 pw-id 15, state: up, Static MAC addresses: 0
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0
RP/0/RSP0/CPU0:N-PE1#sh l2vpn forwarding bridge-domain customer1:engineering
mac-address location 0/0/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
------------------------------------------------------------------------------
6c9c.ed3e.e46d dynamic (10.0.0.15, 15) 0/0/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A
0024.985e.6a42 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A
```

```
001d.4603.1f42 dynamic (10.0.0.13, 2) 0/0/CPU0 0d 0h 0m 0s N/A
```

En N-PE2 (10.0.0.12), el PW de acceso se encuentra en estado de espera:

```
RP/0/RSP0/CPU0:N-PE2#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
bridge group customer1
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
neighbor 10.0.0.15 pw-id 15
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!
RP/0/RSP0/CPU0:N-PE2#sh l2vpn bridge-domain bd-name engineering
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 1, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 4 (3 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.2, state: up, Static MAC addresses: 0
List of Access PWs:
Neighbor 10.0.0.15 pw-id 15, state: standby, Static MAC addresses: 0
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.11 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0
```

4.4.6 Grupos de horizontes divididos (SHG)

La regla de horizonte dividido dicta que una trama recibida en un VFI PW no se puede reenviar sobre otro VFI PW. Los VFI N-PE deben tener una malla completa.

Este horizonte dividido se aplica a través de un SHG:

- Los miembros de un SHG no pueden reenviar tramas entre sí, pero pueden reenviar tramas a miembros de otros SHG.
- Todos los PW de VFI se asignan a SHG 1 de forma predeterminada. Esto garantiza que no haya reenvío entre los PW de VFI para que se aplique la regla de horizonte dividido. Los paquetes recibidos en un PW de VFI se pueden reenviar a los AC y a los PW de acceso porque no forman parte del mismo SHG.
- Todos los AC y los PW de acceso no forman parte de un grupo SHG de forma predeterminada, lo que significa que los paquetes recibidos en un AC o PW de acceso se pueden reenviar a otro AC o PW de acceso en el mismo dominio de puente.

- Los AC y los PW de acceso se pueden asignar al SHG 2 con el comando **split-horizon group** si el objetivo es evitar el reenvío entre ellos.

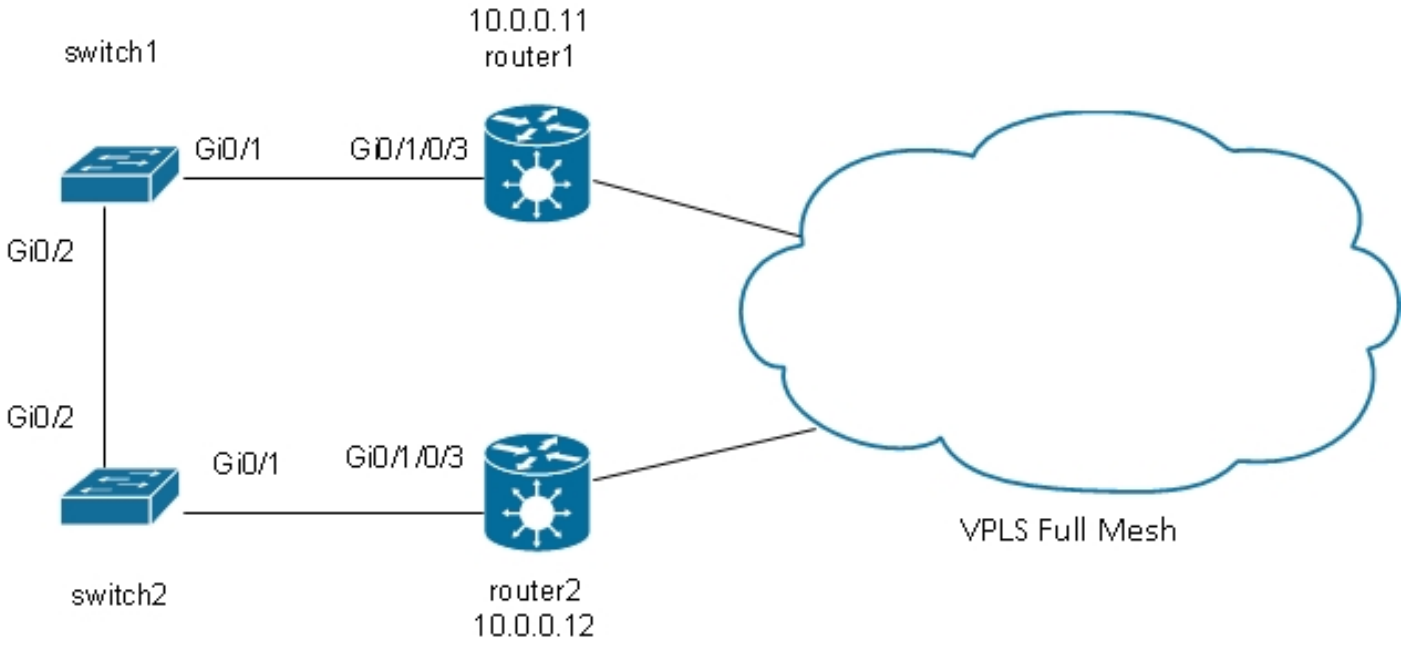
```
RP/0/RSP0/CPU0:N-PE1#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
bridge group customer1
bridge-domain engineering
interface GigabitEthernet0/0/0/1.2
split-horizon group
!
interface GigabitEthernet0/1/0/3.2
split-horizon group
!
neighbor 10.0.0.15 pw-id 15
split-horizon group
!
vfi customer1-engineering
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!
```

En esta configuración, no hay reenvío entre Gi 0/0/0/1.2 y Gi 0/1/0/3.2, Gi 0/0/0/1.2 y 10.0.0.15, o Gi 0/1/0/3.2 y 10.0.0.15. Pero todavía puede haber reenvío de tráfico entre los AC y los PW de VFI porque forman parte de SHG diferentes (1 y 2).

```
RP/0/RSP0/CPU0:N-PE1#sh l2vpn bridge-domain bd-name engineering detail  |
i "state is|List of|VFI|Split"
Split Horizon Group: none
ACs: 2 (1 up), VFIs: 1, PWs: 4 (4 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/0/0/1.2, state is unresolved
Split Horizon Group: enabled
AC: GigabitEthernet0/1/0/3.2, state is up
Split Horizon Group: enabled
List of Access PWs:
PW: neighbor 10.0.0.15, PW ID 15, state is up ( established )
Split Horizon Group: enabled
List of VFIs:
VFI customer1-engineering (up)
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )
PW: neighbor 10.0.0.13, PW ID 2, state is up ( established )
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
VFI Statistics:
```

4.4.7 Redundancia

En un intento de introducir redundancia, es posible que tenga un sitio que esté conectado de forma dual al dominio VPLS:



Si un host conectado al switch1 envía una transmisión, el switch1 la reenvía al router1 y al switch2. El Router1 tiene una malla completa de PW, por lo que hay un PW al Router2, y el Router1 reenvía la transmisión a través de ese PW. El Router2 reenvía el broadcast al switch2, que lo reenvía al switch1. Esto da como resultado un loop físico.

4.4.7.1 Árbol de extensión

La implementación MST completa no funciona con VPLS porque esa implementación envía MST BPDU en una interfaz principal para controlar el estado de reenvío de todas las VLAN en esa interfaz. Con VPLS, hay VFI para cada dominio de puente, por lo que no puede enviar BPDU en una interfaz principal para todas esas VFI.

Las BPDU del árbol de expansión se transportan sobre VPLS y PW punto a punto de forma predeterminada.

Si el switch1 y el switch2 envían BPDU por VLAN o BPDU de MST sin etiqueta y si las BPDU coinciden con las subinterfaces de transporte l2 en el router1 y el router2, las BPDU se transportan a través de VPLS. Los switches ven las BPDU de los demás en las interfaces Gi 0/1, y el spanning tree rompe el loop y bloquea un puerto.

El switch 2 es la raíz de la VLAN 2:

```
switch2#sh spanning-tree vlan 2

MST0
Spanning tree enabled protocol mstp
Root ID Priority 32768
Address 0024.985e.6a00
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address 0024.985e.6a00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Desg FWD 20000 128.1 P2p Bound(PVST)
Gi0/2 Desg FWD 20000 128.2 P2p Bound(PVST)
```

El Switch1 tiene su puerto raíz en Gi 0/1 y está bloqueando Gi 0/2:

```
switch1#sh spanning-tree vlan 2

VLAN0002
Spanning tree enabled protocol ieee
Root ID Priority 32768
Address 0024.985e.6a00
Cost 4
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32770 (priority 32768 sys-id-ext 2)
Address 0019.552b.b580
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Root FWD 4 128.1 P2p
Gi0/2 Altn BLK 4 128.2 P2p
```

El problema es que las BPDU también se transportan a sitios remotos y la inestabilidad del árbol de expansión en un sitio se propaga a todos los sitios conectados al dominio VPLS. Es más seguro aislar cada sitio y no transportar BPDU sobre VPLS.

Una solución es el uso de una versión de gateway de acceso del STP. Ésta es una implementación limitada del protocolo, donde los PE L2VPN se configuran para enviar algunas BPDU estáticas para que aparezcan conectadas a la raíz del árbol de expansión. El PE L2VPN no transporta las BPDU recibidas de los CE a los sitios remotos, por lo que cada sitio tiene su propio dominio de árbol de expansión.

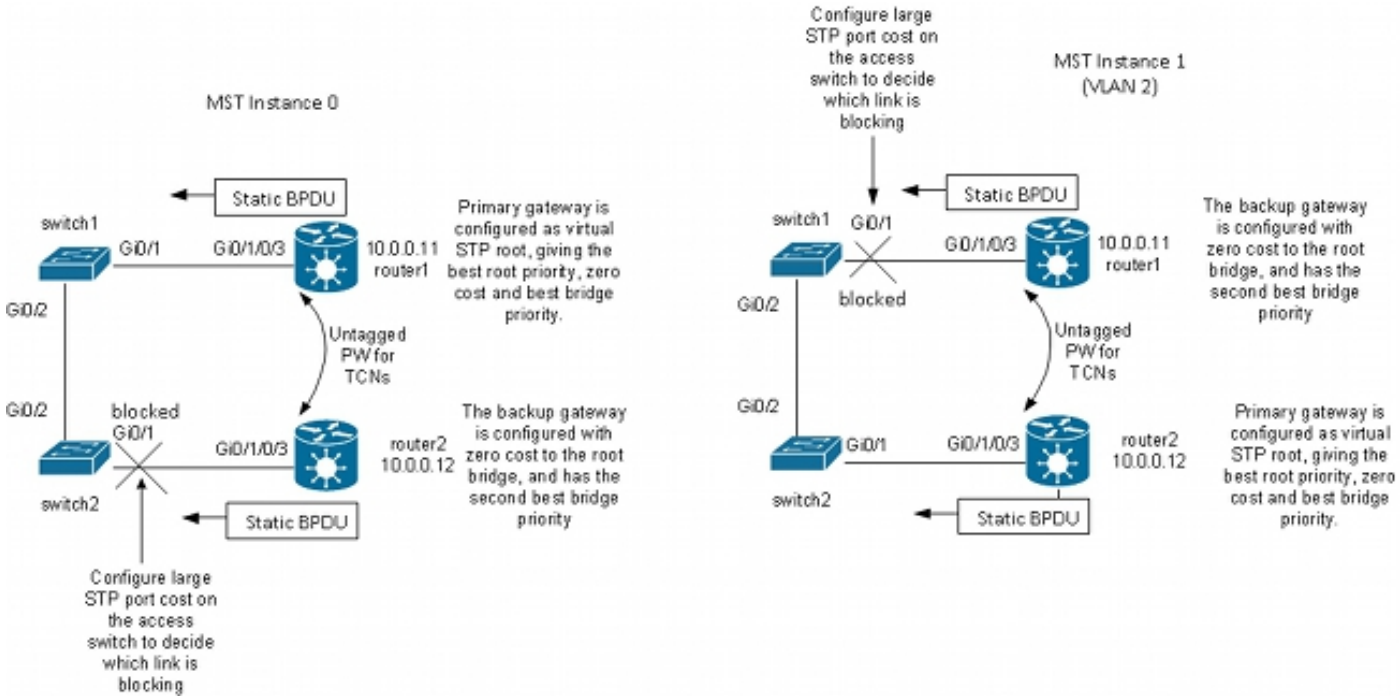
4.4.7.2 MSTAG

Como se explicó en la sección Spanning Tree, MST envía BPDU sin etiqueta, pero estas BPDU controlan el estado de reenvío de todas las VLAN en la interfaz.

Las VLAN se pueden agrupar en varias instancias y cada instancia tiene su propio estado de reenvío.

Las VLAN generalmente se agrupan de modo que el tráfico pueda distribuirse uniformemente entre varias trayectorias. Cuando hay dos trayectorias, la mitad del tráfico pertenece a una instancia que está reenviando en la primera trayectoria y bloqueando en la segunda trayectoria. La otra mitad del tráfico pertenece a una instancia que está bloqueando la primera trayectoria y reenviando la segunda trayectoria. Esto permite el balanceo de carga entre los dos trayectos en condiciones estables. De lo contrario, tendrá una ruta que normalmente estará bloqueada por completo y solo se activará cuando la ruta principal esté inactiva.

Esta es una topología típica de MSTAG:



En este ejemplo de laboratorio, la instancia 1 tiene VLAN 2 y la instancia 0 tiene las otras VLAN. (En un escenario más realista, las VLAN se distribuyen entre instancias múltiples para lograr un buen equilibrio de carga de tráfico entre las instancias.) Debido a que algunas VLAN tienen mucho más tráfico que otras, no siempre hay el mismo número de VLAN en cada instancia.

Esta es la configuración para la instancia 0 de MST:

- El Router1 y el Router2 están enviando algunas BPDU estáticas basadas en la configuración MSTAG. No están procesando las BPDU entrantes de la red ni están intentando ejecutar una implementación completa. Con MSTAG, los dos PE L2VPN simplemente envían BPDU estáticas basadas en su configuración MSTAG.
- El Router 1 se configura para atraer el tráfico de la instancia 0 apareciendo como la raíz para esa instancia.
- El Router 2 se configura con la segunda mejor prioridad de raíz para la instancia 0, de modo que se convierta en la nueva raíz en caso de falla del Router 1 o falla de CA entre el switch 1 y el Router 1.
- El Switch2 está configurado con un alto costo de spanning tree en el puerto Gi 0/1 al router2 para asegurarse de que su trayectoria primaria a la raíz esté en Gig 0/2 a través del switch1 y el router1.
- El Switch2 selecciona Gi 0/2 como puerto raíz para instance0 y selecciona Gi 0/1 como puerto alternativo en caso de que se pierda la raíz.
- Por lo tanto, el tráfico de ese sitio en las VLAN que pertenecen a la instancia 0 llega a otros sitios a través de VPLS a través del router 1.

Para la instancia 1 de MST (VLAN 2), la configuración se invierte:

- El Router 2 se configura para atraer el tráfico de la instancia 1 aparentando ser la raíz para esa instancia.
- El Router1 se configura con la segunda mejor prioridad de raíz para la instancia 1, de modo que se convierta en la nueva raíz en caso de falla del Router2 o falla de CA entre el switch2 y el Router2.

- El Switch1 está configurado con un alto costo de spanning tree en el puerto Gi 0/1 al router1 para asegurarse de que su trayectoria primaria a la raíz esté en Gig 0/2 a través del switch2 y el router2.
- El Switch1 selecciona Gi 0/2 como puerto raíz para la instancia 1 y selecciona Gi 0/1 como puerto alternativo en caso de que se pierda la raíz.
- Por lo tanto, el tráfico de ese sitio en las VLAN que pertenecen a la instancia 1 (VLAN 2 en este ejemplo) llega a otros sitios a través de VPLS a través del router 2.
- Debe haber una subinterfaz en el router1 y el router2 para capturar los TCN sin etiqueta y reenviarlos a través de un PW punto a punto al otro router. Debido a que el switch1 y el switch2 podrían perder sus links directos y quedar aislados entre sí, el router1 y el router2 deben reenviar las TCN entre ellos a través de ese PW punto a punto.
- Los PE también interceptan los TCN, vacian sus tablas de direcciones MAC y envían la retirada de MAC LDP a los PE remotos.

Esta es la configuración en el router1:

```
RP/0/RSP0/CPU0:router1#sh run int gigabitEthernet 0/1/0/3.*
interface GigabitEthernet0/1/0/3.1 l2transport
encapsulation untagged
!
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
ethernet-services access-group filter-stp egress
!
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
ethernet-services access-group filter-stp egress
!

RP/0/RSP0/CPU0:router1#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/1/0/3.3
!
vfi customer1-finance
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
vfi customer1-engineering
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
```

```
!

RP/0/RSP0/CPU0:router1#sh run l2vpn xconnect group customer1
l2vpn
xconnect group customer1
p2p mstag-gi-0-1-0-3
interface GigabitEthernet0/1/0/3.1
neighbor 10.0.0.13 pw-id 103
!
!
!
!

RP/0/RSP0/CPU0:router1#sh run spanning-tree mstag customer1-0-1-0-3
spanning-tree mstag customer1-0-1-0-3
interface GigabitEthernet0/1/0/3.1
name customer1
revision 1
bridge-id 0000.0000.0001
instance 0
root-id 0000.0000.0001
priority 4096
root-priority 4096
!
instance 1
vlan-ids 2
root-id 0000.0000.0002
priority 8192
root-priority 4096
!
!
!

RP/0/RSP0/CPU0:router1#sh spanning-tree mstag customer1-0-1-0-3
GigabitEthernet0/1/0/3.1
Pre-empt delay is disabled
Name: customer1
Revision: 1
Max Age: 20
Provider Bridge: no
Bridge ID: 0000.0000.0001
Port ID: 1
External Cost: 0
Hello Time: 2
Active: yes
BPDUs sent: 3048
MSTI 0 (CIST):
VLAN IDs: 1,3-4094
Role: Designated
Bridge Priority: 4096
Port Priority: 128
Cost: 0
Root Bridge: 0000.0000.0001
Root Priority: 4096
Topology Changes: 369
MSTI 1
VLAN IDs: 2
Role: Designated
Bridge Priority: 8192
Port Priority: 128
Cost: 0
Root Bridge: 0000.0000.0002
Root Priority: 4096
Topology Changes: 322
```

En esta configuración, tenga en cuenta que:

- En la instancia 0 de MST, el bridge raíz es 0000.0000.0001, que es el ID de bridge del router1.
- En la instancia 1 de MST, el bridge raíz es 0000.0000.0002, que es el ID de bridge del router2.
- La prioridad de puente del router1 es 4096 en la instancia 0 (para convertirse en la raíz) y 8192 en la instancia 1 (para convertirse en la segunda mejor raíz).
- La prioridad de puente del router1 es 8192 en la instancia 0 (para convertirse en la segunda mejor raíz) y 4096 en la instancia 1 (para convertirse en la raíz).
- La conexión cruzada punto a punto en GigabitEthernet0/1/0/3.1 lleva las TCN MST sin etiqueta al otro router.

Se ha configurado una ACL de salida en las subinterfaces dot1q para descartar BPDU por VLAN que podrían ser enviadas por otro sitio que aún no se ha migrado a MST. Esta configuración evita que el switch CE declare que la interfaz es incoherente cuando recibe una BPDU por VLAN en una interfaz configurada para MST.

La configuración en el router2 es muy similar:

```
RP/0/RSP0/CPU0:router2#sh run int gig 0/1/0/3.*
interface GigabitEthernet0/1/0/3.1 l2transport
encapsulation untagged
!
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
ethernet-services access-group filter-stp egress
!
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
ethernet-services access-group filter-stp egress
!

RP/0/RSP0/CPU0:router2#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/1/0/3.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
```

```
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!

RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group customer1
l2vpn
xconnect group customer1
p2p mstag-gi-0-1-0-3
interface GigabitEthernet0/1/0/3.1
neighbor 10.0.0.13 pw-id 103
!
!
!
!

RP/0/RSP0/CPU0:router2#sh run spanning-tree mstag customer1-0-1-0-3
spanning-tree mstag customer1-0-1-0-3
interface GigabitEthernet0/1/0/3.1
name customer1
revision 1
bridge-id 0000.0000.0002
instance 0
root-id 0000.0000.0001
priority 8192
root-priority 4096
!
instance 1
vlan-ids 2
root-id 0000.0000.0002
priority 4096
root-priority 4096
!
!
!

RP/0/RSP0/CPU0:router2#sh spanning-tree mstag customer1-0-1-0-3
GigabitEthernet0/1/0/3.1
Pre-empt delay is disabled
Name: customer1
Revision: 1
Max Age: 20
Provider Bridge: no
Bridge ID: 0000.0000.0002
Port ID: 1
External Cost: 0
Hello Time: 2
Active: yes
BPDUs sent: 3186
MSTI 0 (CIST):
VLAN IDs: 1,3-4094
Role: Designated
Bridge Priority: 8192
Port Priority: 128
Cost: 0
Root Bridge: 0000.0000.0001
Root Priority: 4096
Topology Changes: 365
MSTI 1
VLAN IDs: 2
Role: Designated
Bridge Priority: 4096
```

```
Port Priority: 128
Cost: 0
Root Bridge: 0000.0000.0002
Root Priority: 4096
Topology Changes: 177
```

Esta es la configuración básica en el switch 1:

```
switch1#sh run | b spanning-tree
spanning-tree mode mst
spanning-tree extend system-id
!
spanning-tree mst configuration
name customer1
revision 1
instance 1 vlan 2
!
switch1#sh run int gig 0/1 | i spanning
spanning-tree mst 1 cost 100000

switch1#sh spanning-tree

MST0
Spanning tree enabled protocol mstp
Root ID Priority 4096
Address 0000.0000.0001
Cost 0
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address 0019.552b.b580
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Root FWD 20000 128.1 P2p
Gi0/2 Desg FWD 20000 128.2 P2p



MST1
Spanning tree enabled protocol mstp
Root ID Priority 4097
Address 0000.0000.0002
Cost 40000
Port 2 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0019.552b.b580
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Altn BLK 100000 128.1 P2p
Gi0/2 Root FWD 20000 128.2 P2p
```

Por lo tanto, el tráfico en la instancia 0 se reenvía a través del router1 y el tráfico en la instancia 1 se reenvía a través del switch2 y el router2.

La configuración en el switch2 utiliza los mismos comandos que el switch1:

```
switch2#sh run | b spanning
spanning-tree mode mst
spanning-tree extend system-id
!
spanning-tree mst configuration
name customer1
revision 1
instance 1 vlan 2
!
switch2#sh run int gig 0/1 | i spanning
spanning-tree mst 0 cost 100000

switch2#sh spanning-tree

MST0
Spanning tree enabled protocol mstp
Root ID Priority 4096
Address 0000.0000.0001
Cost 0
Port 2 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address 0024.985e.6a00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Altn BLK 100000 128.1 P2p
Gi0/2 Root FWD 20000 128.2 P2p



MST1
Spanning tree enabled protocol mstp
Root ID Priority 4097
Address 0000.0000.0002
Cost 20000
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0024.985e.6a00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Root FWD 20000 128.1 P2p
Gi0/2 Desg FWD 20000 128.2 P2p
```

El switch2 pasa por el switch1 y el router1 para la instancia0 y a través del router2 para la instancia1.

El tráfico se carga balanceado porque una instancia sale del sitio a través del router1 y la otra instancia sale del sitio a través del router2.

Si el link entre el router1 y el switch1 está inactivo, ambas instancias pasan a través del router2.

```
switch1#sh spanning-tree

MST0
```

```
Spanning tree enabled protocol mstp
Root ID Priority 4096
Address 0000.0000.0001
Cost 0
Port 2 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address 0019.552b.b580
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/2 Root FWD 20000 128.2 P2p



MST1
Spanning tree enabled protocol mstp
Root ID Priority 4097
Address 0000.0000.0002
Cost 40000
Port 2 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0019.552b.b580
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/2 Root FWD 20000 128.2 P2p


switch2#sh spanning-tree

MST0
Spanning tree enabled protocol mstp
Root ID Priority 4096
Address 0000.0000.0001
Cost 0
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address 0024.985e.6a00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Root FWD 100000 128.1 P2p
Gi0/2 Desg FWD 20000 128.2 P2p



MST1
Spanning tree enabled protocol mstp
Root ID Priority 4097
Address 0000.0000.0002
Cost 20000
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
```

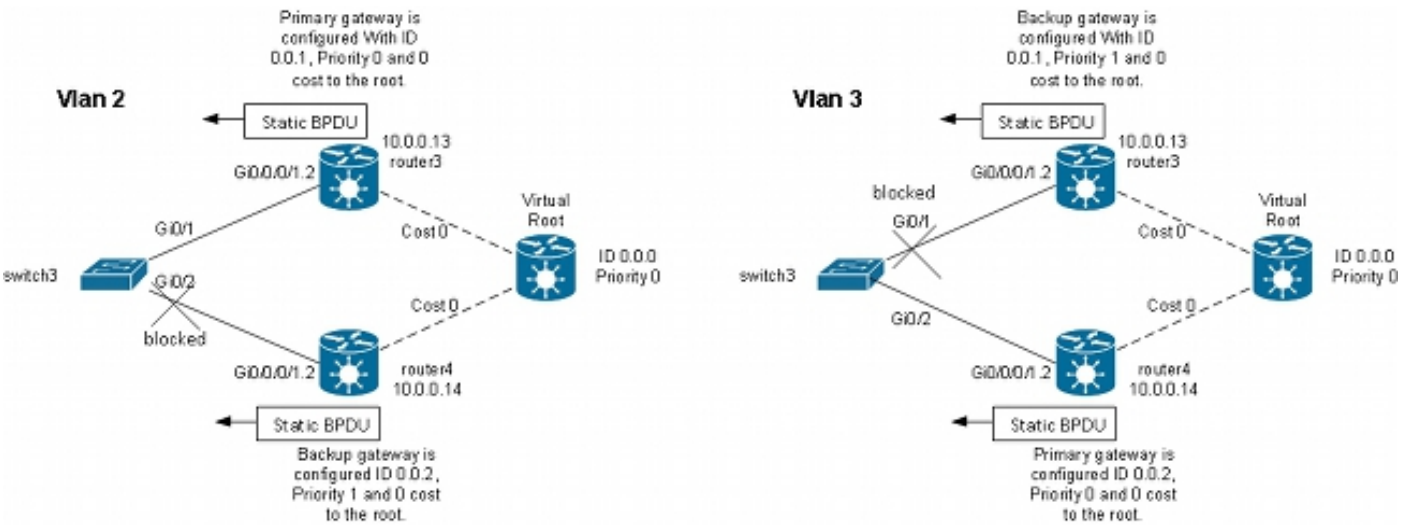
```
Address 0024.985e.6a00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Root FWD 20000 128.1 P2p
Gi0/2 Desg FWD 20000 128.2 P2p
```

La convergencia rápida se puede lograr en este tipo de falla porque la trayectoria a través de la segunda mejor raíz ya estaba seleccionada como la trayectoria alternativa. Con MSTAG, las BPDU de MST no se transportan a través de VPLS, por lo que los sitios se aíslan de la inestabilidad en otros sitios.

4.4.7.3 PVSTAG o PVRSTAG

MSTAG es el protocolo de gateway de acceso preferido para VPLS porque utiliza el árbol de expansión rápida y porque es escalable con su uso de instancias en lugar de BPDU en cada VLAN.

Si un sitio no se puede migrar a MST y la única solución es seguir ejecutando PVST+ o PVRST, puede utilizar PVSTAG o PVRSTAG, pero la implementación se limita a una topología específica:



En esta topología, la restricción más importante es que solo puede haber un switch CE. No puede tener dos switches como en la topología MSTAG. En MSTAG, puede configurar un PW punto a punto para transportar el tráfico sin etiqueta (incluidas las TCN de BPDU) de un PE al otro cuando el sitio se divide en dos partes. Con PVST y PVRST, las TCN se envían etiquetadas para que coincidan con la misma subinterfaz que el tráfico de datos que se transportará a través de VPLS. El router tendría que identificar las BPDU según la dirección MAC y el tipo de protocolo para reenviar las TCN al otro lado. Debido a que esto no es compatible actualmente, existe el requisito de tener solo un dispositivo CE.

Otro requisito en las versiones anteriores a Cisco IOS XR Software Release 4.3.0 es que las interfaces de agrupamiento no se pueden utilizar como AC. Esta restricción se ha eliminado en la versión 4.3.0 del software Cisco IOS XR.

El principio es muy similar al del MSTAG. El router PVSTAG envía BPDU estáticas para que el CE parezca estar conectado a switches que están conectados directamente a la raíz (virtual) con un costo 0. Para balancear la carga del tráfico, algunas VLAN se pueden configurar con la raíz en

el router3 y otras con la raíz en el router4.

Este es un ejemplo de configuración en el router 3:

```
RP/0/RSP1/CPU0:router3#sh run int gigabitEthernet 0/0/0/1.*
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface GigabitEthernet0/0/0/1.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!

RP/0/RSP1/CPU0:router3#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/0/0/1.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface GigabitEthernet0/0/0/1.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!

RP/0/RSP1/CPU0:router3#sh run spanning-tree pvstag customer1-0-0-0-1
spanning-tree pvstag customer1-0-0-0-1
interface GigabitEthernet0/0/0/1
vlan 2
root-priority 0
root-id 0000.0000.0000
root-cost 0
priority 0
bridge-id 0000.0000.0001
!
vlan 3
root-priority 0
root-id 0000.0000.0000
root-cost 0
priority 1
bridge-id 0000.0000.0001
!
!
```

```
!

RP/0/RSP1/CPU0:router3#sh spanning-tree pvstag customer1-0-0-0-1
GigabitEthernet0/0/0/1
VLAN 2
Pre-empt delay is disabled
Sub-interface: GigabitEthernet0/0/0/1.2 (Up)
Max Age: 20
Root Priority: 0
Root Bridge: 0000.0000.0000
Cost: 0
Bridge Priority: 0
Bridge ID: 0000.0000.0001
Port Priority: 128
Port ID 1
Hello Time: 2
Active: Yes
BPDUs sent: 202821
Topology Changes: 0
VLAN 3
Pre-empt delay is disabled
Sub-interface: GigabitEthernet0/0/0/1.3 (Up)
Max Age: 20
Root Priority: 0
Root Bridge: 0000.0000.0000
Cost: 0
Bridge Priority: 1
Bridge ID: 0000.0000.0001
Port Priority: 128
Port ID 1
Hello Time: 2
Active: Yes
BPDUs sent: 202821
Topology Changes: 0
```

Este es un ejemplo de configuración en el router4:

```
RP/0/RSP1/CPU0:router4#sh run int gig 0/0/0/1.*
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface GigabitEthernet0/0/0/1.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!

RP/0/RSP1/CPU0:router4#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/0/0/1.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
!
!
bridge-domain engineering
```

```
interface GigabitEthernet0/0/0/1.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
!
!
!
!

RP/0/RSP1/CPU0:router4#sh run spanning-tree pvstag customer1-0-0-0-1
spanning-tree pvstag customer1-0-0-0-1
interface GigabitEthernet0/0/0/1
vlan 2
root-priority 0
root-id 0000.0000.0000
root-cost 0
priority 1
bridge-id 0000.0000.0002
!
vlan 3
root-priority 0
root-id 0000.0000.0000
root-cost 0
priority 0
bridge-id 0000.0000.0002
!
!
!

RP/0/RSP1/CPU0:router4#sh spanning-tree pvstag customer1-0-0-0-1
GigabitEthernet0/0/0/1
VLAN 2
Pre-empt delay is disabled
Sub-interface: GigabitEthernet0/0/0/1.2 (Up)
Max Age: 20
Root Priority: 0
Root Bridge: 0000.0000.0000
Cost: 0
Bridge Priority: 1
Bridge ID: 0000.0000.0002
Port Priority: 128
Port ID 1
Hello Time: 2
Active: Yes
BPDUs sent: 202799
Topology Changes: 0
VLAN 3
Pre-empt delay is disabled
Sub-interface: GigabitEthernet0/0/0/1.3 (Up)
Max Age: 20
Root Priority: 0
Root Bridge: 0000.0000.0000
Cost: 0
Bridge Priority: 0
Bridge ID: 0000.0000.0002
Port Priority: 128
Port ID 1
Hello Time: 2
Active: Yes
```

```
BPDUs sent: 202799
Topology Changes: 0
```

Este es un ejemplo de configuración en el switch CE3:

```
switch3#sh spanning-tree vlan 2

VLAN0002
Spanning tree enabled protocol ieee
Root ID Priority 0
Address 0000.0000.0000
Cost 4
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32770 (priority 32768 sys-id-ext 2)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Root FWD 4 128.1 P2p
Gi0/2 Altn BLK 4 128.2 P2p

switch3#sh spanning-tree vlan 3

VLAN0003
Spanning tree enabled protocol ieee
Root ID Priority 0
Address 0000.0000.0000
Cost 4
Port 2 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32771 (priority 32768 sys-id-ext 3)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface Role Sts Cost Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1 Altn BLK 4 128.1 P2p
Gi0/2 Root FWD 4 128.2 P2p
```

La configuración de PVSTAG es muy similar a la de MSTAG, excepto en que la prioridad raíz y la prioridad del gateway principal se configuran como 4096 y la prioridad del gateway de respaldo se configura como 8192 en el ejemplo de MSTAG.

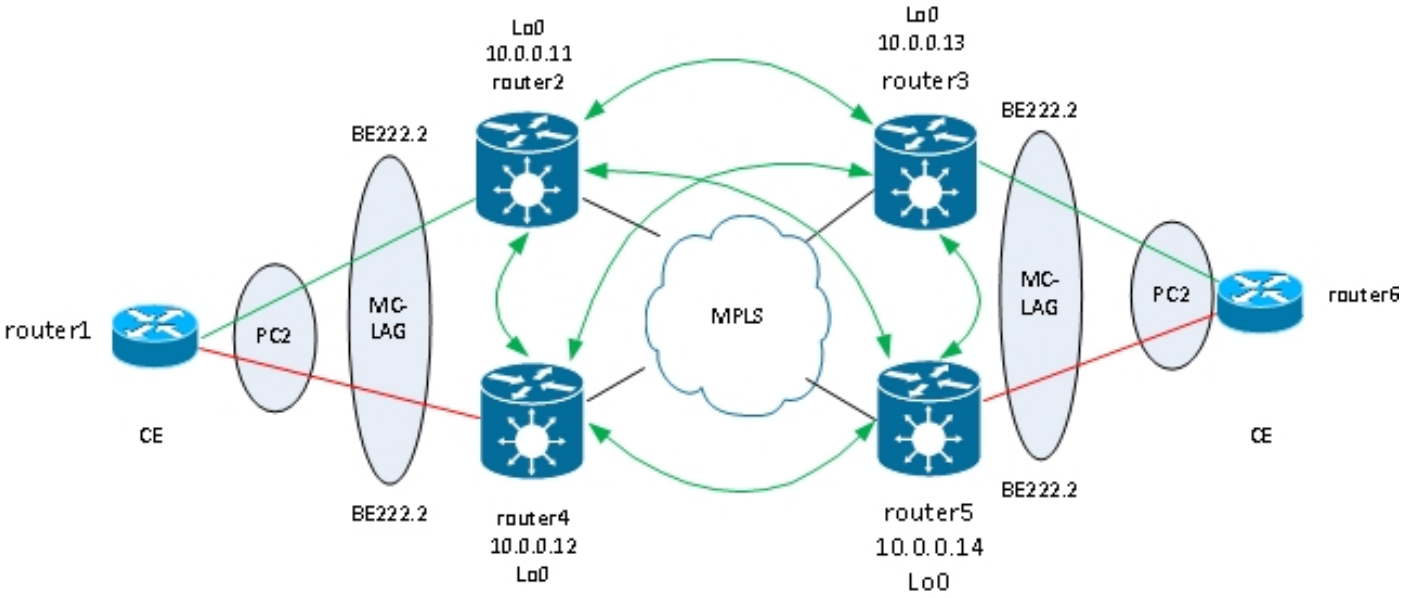
Todos los demás switches de los dominios deben tener prioridades más altas que las configuradas en PVSTAG o PVRSTAG.

Puede ajustar el costo de la interfaz en los switches CE para influir en qué puerto se convierte en el puerto raíz y qué puerto se bloquea.

4.4.7.4 MC-LAG

La configuración MC-LAG con VPLS es más sencilla que los PW punto a punto con redundancia PW bidireccional. En lugar de un PW principal y tres PW en espera, los PE solo necesitan una

malla completa de PW VPLS, que es estándar con VPLS:



En esta topología, tenga en cuenta que:

- MC-LAG se ejecuta entre los dos VPLS PE de la izquierda: router2 y router4.
- En condiciones normales, los miembros del conjunto están activos entre el router1 y el router2 y en estado de espera entre el router1 y el router4.
- El Router2 tiene las subinterfaces de agrupamiento configuradas bajo dominios de puente VPLS, por lo que el Router2 reenvía el tráfico a los PE VPLS remotos. Hay dos sitios ilustrados en el diagrama de topología, pero podría haber muchos más.
- Los PE remotos aprenden las direcciones MAC del router1 y los dispositivos posteriores a través del router2, por lo que los PE reenvían el tráfico para estas direcciones MAC de destino a través del router2.
- Cuando el link entre el router1 y el router2 deja de funcionar o cuando el router2 deja de funcionar, el miembro del conjunto entre el router1 y el router4 se activa.
- Al igual que el router 2, el router 4 tiene sus subinterfaces de agrupamiento configuradas en dominios de puente VPLS.
- Cuando las subinterfaces del conjunto se activan en el router4, el router4 envía mensajes de retiro de MAC LDP a los PE VPLS remotos para hacerles saber que hay un cambio de topología.

Esta es la configuración en el router 3:

```
RP/0/RSP1/CPU0:router3#sh run redundancy
redundancy
iccp
group 2
mlacp node 1
mlacp system mac 0200.0000.0002
mlacp system priority 1
mlacp connect timeout 0
member
neighbor 10.0.0.14
!
backbone
interface TenGigE0/0/0/0
```

```
interface TenGigE0/0/0/1
!
isolation recovery-delay 300
!
!
!

RP/0/RSP1/CPU0:router3#sh run int bundle-ether 222
interface Bundle-Ether222
lacp switchover suppress-flaps 100
mlacp iccp-group 2
mlacp switchover type revertive
mlacp switchover recovery-delay 40
mlacp port-priority 1
mac-address 0.0.2
bundle wait-while 0
bundle maximum-active links 1
load-interval 30
!

RP/0/RSP1/CPU0:router3#sh run int bundle-ether 222.*
interface Bundle-Ether222.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface Bundle-Ether222.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!

RP/0/RSP1/CPU0:router3#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface Bundle-Ether222.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface Bundle-Ether222.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!
```

Una vez configurado el paquete MC-LAG, agréguelo en la configuración VPLS como cualquier otro AC.

Ésta es la configuración correspondiente en el router5:

```
RP/0/RSP1/CPU0:router5#sh run redundancy
redundancy
iccp
group 2
mlacp node 2
mlacp system mac 0200.0000.0002
mlacp system priority 1
mlacp connect timeout 0
member
neighbor 10.0.0.13
!
backbone
interface TenGigE0/1/0/0
interface TenGigE0/1/0/1
!
isolation recovery-delay 300
!
!
!

RP/0/RSP1/CPU0:router5#sh run int bundle-ether 222
interface Bundle-Ether222
lacp switchover suppress-flaps 100
mlacp iccp-group 2
mlacp switchover type revertive
mlacp switchover recovery-delay 40
mac-address 0.0.2
bundle wait-while 0
bundle maximum-active links 1
load-interval 30
!

RP/0/RSP1/CPU0:router5#sh run int bundle-ether 222.*
interface Bundle-Ether222.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface Bundle-Ether222.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!

RP/0/RSP1/CPU0:router5#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface Bundle-Ether222.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
!
!
bridge-domain engineering
interface Bundle-Ether222.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
```

```
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
!
!
!
!
```

En circunstancias normales, el miembro del conjunto entre el router3 y el router6 está activo y el miembro entre el router5 y el router6 está en estado de espera:

```
RP/0/RSP1/CPU0:router3#sh bundle bundle-ether 222

Bundle-Ether222
Status: Up
Local links : 1 / 0 / 1
Local bandwidth : 1000000 (1000000) kbps
MAC address (source): 0000.0000.0002 (Configured)
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
Maximum active links: 1
Wait while timer: Off
Load balancing: Default
LACP: Operational
Flap suppression timer: 100 ms
Cisco extensions: Disabled
mLACP: Operational
ICCP Group: 2
Role: Active
Foreign links : 0 / 1
Switchover type: Revertive
Recovery delay: 40 s
Maximize threshold: 1 link
IPv4 BFD: Not configured

Port Device State Port ID B/W, kbps
-------------------- ------------ ----------- -------------- ----------
Gi0/0/0/1 Local Active 0x0001, 0x9001 1000000
Link is Active
Gi0/0/0/1 10.0.0.14 Standby 0x8000, 0xa002 1000000
Link is marked as Standby by mLACP peer
RP/0/RSP1/CPU0:router3#

router6#sh etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator

M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port


Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
------+-------------+-----------+-----------------------------------------------
```

```
2 Po2(SU) LACP Gi0/1(P) Gi0/2(w)

router6#
```

El tráfico del CE se recibe en el router 3 y se reenvía a los PE remotos:

```
RP/0/RSP1/CPU0:router3#sh l2vpn bridge-domain group customer1
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 4, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
BE222.3, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-finance (up)
Neighbor 10.0.0.11 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.12 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 3, state: up, Static MAC addresses: 0
Bridge group: customer1, bridge-domain: engineering, id: 3, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
BE222.2, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.11 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0

RP/0/RSP1/CPU0:router3#sh l2vpn forwarding bridge-domain customer1:
engineering mac location 0/0/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
------------------------------------------------------------------------------
001d.4603.1f01 dynamic BE222.2 0/0/CPU0 0d 0h 0m 0s N/A
001d.4603.1f42 dynamic BE222.2 0/0/CPU0 0d 0h 0m 0s N/A
6c9c.ed3e.e46d dynamic (10.0.0.11, 2) 0/0/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A
```

El último comando ilustra que el router3 está aprendiendo algunas direcciones MAC en su agrupamiento y que los miembros activos están en el router3. En el router 5, no hay una dirección MAC aprendida sobre el agrupamiento ya que el miembro local está en estado de espera:

```
RP/0/RSP1/CPU0:router5#sh l2vpn forwarding bridge-domain customer1:engineering
mac location 0/0/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
------------------------------------------------------------------------------
6c9c.ed3e.e46d dynamic (10.0.0.11, 2) 0/0/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A
001d.4603.1f01 dynamic (10.0.0.13, 2) 0/0/CPU0 0d 0h 0m 0s N/A
```

Cuando el miembro del conjunto entre el router3 y el router6 deja de funcionar, el miembro del conjunto se activa en el router5. Los PE de MC-LAG VPLS envían un mensaje de retiro de MAC LDP para que los PE remotos purguen sus tablas de direcciones MAC y aprendan la dirección MAC a través del nuevo router PE MC-LAG activo5.

El Router2 recibe un mensaje de retiro MAC del router3 y del router5 cuando el miembro del conjunto MC-LAG activo se mueve del router3 al router5:

```
RP/0/RSP0/CPU0:router2#sh l2vpn bridge-domain group customer1 detail |
i "state is|withd|bridge-domain"
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
AC: GigabitEthernet0/1/0/3.3, state is up
PW: neighbor 10.0.0.12, PW ID 3, state is up ( established )
MAC withdraw message: send 0 receive 0
PW: neighbor 10.0.0.13, PW ID 3, state is up ( established )
MAC withdraw message: send 0 receive 1
PW: neighbor 10.0.0.14, PW ID 3, state is up ( established )
MAC withdraw message: send 0 receive 1
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
AC: GigabitEthernet0/0/0/1.2, state is unresolved
AC: GigabitEthernet0/1/0/3.2, state is up
PW: neighbor 10.0.0.15, PW ID 15, state is up ( established )
MAC withdraw message: send 2 receive 0
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )
MAC withdraw message: send 0 receive 0
PW: neighbor 10.0.0.13, PW ID 2, state is up ( established )
MAC withdraw message: send 0 receive 1
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
MAC withdraw message: send 0 receive 1
```

Las direcciones MAC en el router 2 se mueven del router 3 (10.0.0.13) al router 5 (10.0.0.14):

```
RP/0/RSP0/CPU0:router2#sh l2vpn forwarding bridge-domain customer1:
engineering mac-address location 0/0/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
------------------------------------------------------------------------------
6c9c.ed3e.e46d dynamic (10.0.0.15, 15) 0/0/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A
001d.4603.1f02 dynamic (10.0.0.14, 2) 0/0/CPU0 0d 0h 0m 0s N/A
001d.4603.1f42 dynamic (10.0.0.14, 2) 0/0/CPU0 0d 0h 0m 0s N/A
```

Con MC-LAG, un sitio puede utilizar un solo paquete para adjuntarlo a los otros sitios a través de VPLS. MC-LAG proporciona el link y la redundancia PE, pero lógicamente sigue siendo una interfaz de agrupamiento para alcanzar otros sitios. El árbol de expansión no es necesario en ese conjunto, y se podría configurar un filtro BPDU en el CE para garantizar que las BPDU no se intercambien entre sitios a través de VPLS.

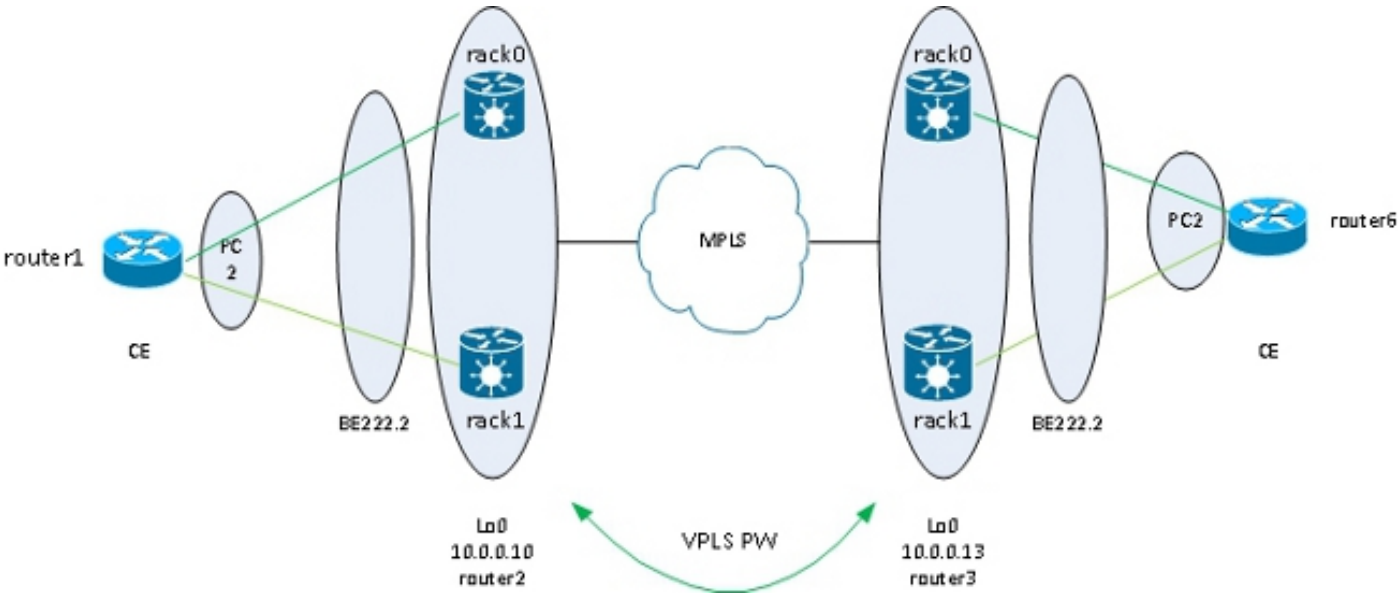
Otra opción es la configuración de una lista de acceso de servicios Ethernet en las CA del

conjunto para descartar las direcciones MAC de destino de las BPDU de modo que las BPDU no se transporten entre sitios. Sin embargo, si se introduce un link de puerta trasera entre los sitios, el spanning tree no puede romper el loop porque no se está ejecutando en el conjunto MC-LAG. Por lo tanto, evalúe cuidadosamente si debe inhabilitar el spanning tree en el conjunto MC-LAG. Si la topología entre sitios se mantiene cuidadosamente, es bueno tener redundancia a través de MC-LAG sin la necesidad de un árbol de expansión.

4.4.7.5 Clúster perimetral ASR 9000 nV

La solución MC-LAG proporcionó redundancia sin necesidad de utilizar un árbol de extensión. Un inconveniente es que los miembros del conjunto de un MC-LAG PE están en estado de espera, por lo que es una solución de espera activa que no maximiza el uso del link.

Otra opción de diseño es el uso de un clúster ASR 9000 nV Edge para que los CE puedan tener miembros de conjunto en cada rack de clúster que estén activos al mismo tiempo:



Otra ventaja de esta solución es que se reduce el número de PW porque solo hay un PW por clúster para cada clúster en cada sitio. Cuando hay dos PE por sitio, cada PE debe tener un PW para cada uno de los dos PE de cada sitio.

La sencillez de la configuración es otra ventaja. La configuración parece una configuración VPLS muy básica con un dominio de bridge con paquetes de AC y PW de VFI:

```
RP/1/RSP0/CPU0:router2#sh bundle bundle-ether 222

Bundle-Ether222
Status: Up
Local links : 2 / 0 / 2
Local bandwidth : 20000000 (20000000) kbps
MAC address (source): 0024.f71e.d309 (Configured)
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
Maximum active links: 64
Wait while timer: 2000 ms
Load balancing: Default
LACP: Not operational
Flap suppression timer: Off
```

```
Cisco extensions: Disabled
mLACP: Not configured
IPv4 BFD: Not configured

Port Device State Port ID B/W, kbps
-------------------- ------------ ----------- -------------- ----------
Te0/0/0/8 Local Active 0x8000, 0x0005 10000000
Link is Active
Te1/0/0/8 Local Active 0x8000, 0x0001 10000000
Link is Active

RP/1/RSP0/CPU0:router2#sh run int bundle-ether 222.2
interface Bundle-Ether222.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!

RP/1/RSP0/CPU0:router2#sh run int bundle-ether 222.3
interface Bundle-Ether222.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!

RP/1/RSP0/CPU0:router2#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface Bundle-Ether222.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface Bundle-Ether222.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!

RP/1/RSP0/CPU0:router2#sh l2vpn bridge-domain group customer1
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 4 (4 up), PBBs: 0 (0 up)
```

```
List of ACs:
BE222.3, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-finance (up)
Neighbor 10.0.0.11 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.12 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 3, state: up, Static MAC addresses: 0
Bridge group: customer1, bridge-domain: engineering, id: 4, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 4 (4 up), PBBs: 0 (0 up)
List of ACs:
BE222.2, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.11 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0
```

La redundancia la proporciona el paquete de CA doblemente conectado a los dos racks para que el paquete permanezca activo en caso de fallo del miembro del paquete o fallo del rack.

Cuando un sitio está conectado al dominio VPLS solamente a través de un clúster, la topología es similar a MC-LAG con respecto al árbol de expansión. Por lo tanto, el spanning tree no es necesario en ese conjunto, y se podría configurar un filtro BPDU en el CE para garantizar que las BPDU no se intercambien entre los sitios a través de VPLS.

Otra opción es la configuración de una lista de acceso de servicios Ethernet en las CA del conjunto para descartar las direcciones MAC de destino de las BPDU de modo que las BPDU no se transporten entre sitios. Sin embargo, si se introduce un link de puerta trasera entre los sitios, el spanning tree no puede romper el loop porque no se está ejecutando en el conjunto CE-PE. Por lo tanto, evalúe cuidadosamente si debe inhabilitar el árbol de expansión en ese paquete CE-PE. Si la topología entre sitios se mantiene cuidadosamente, es bueno tener redundancia a través del clúster sin la necesidad de un árbol de expansión.

4.4.7.6 Multi-alojamiento de servicios basados en ICCP (ICCP-SM) (PMCLAG (Pseudo MCLAG) y Activo/Activo)

Hay una nueva función introducida en la versión 4.3.1 para superar la limitación de MC-LAG, donde algunos links de agrupamiento no se utilizan ya que permanecen en modo de espera. En la nueva función, llamada *Pseudo MCLAG*, todos los links desde el DHD a los Puntos de Conexión (PoAS) están en uso, pero las VLAN se dividen entre los diferentes paquetes:

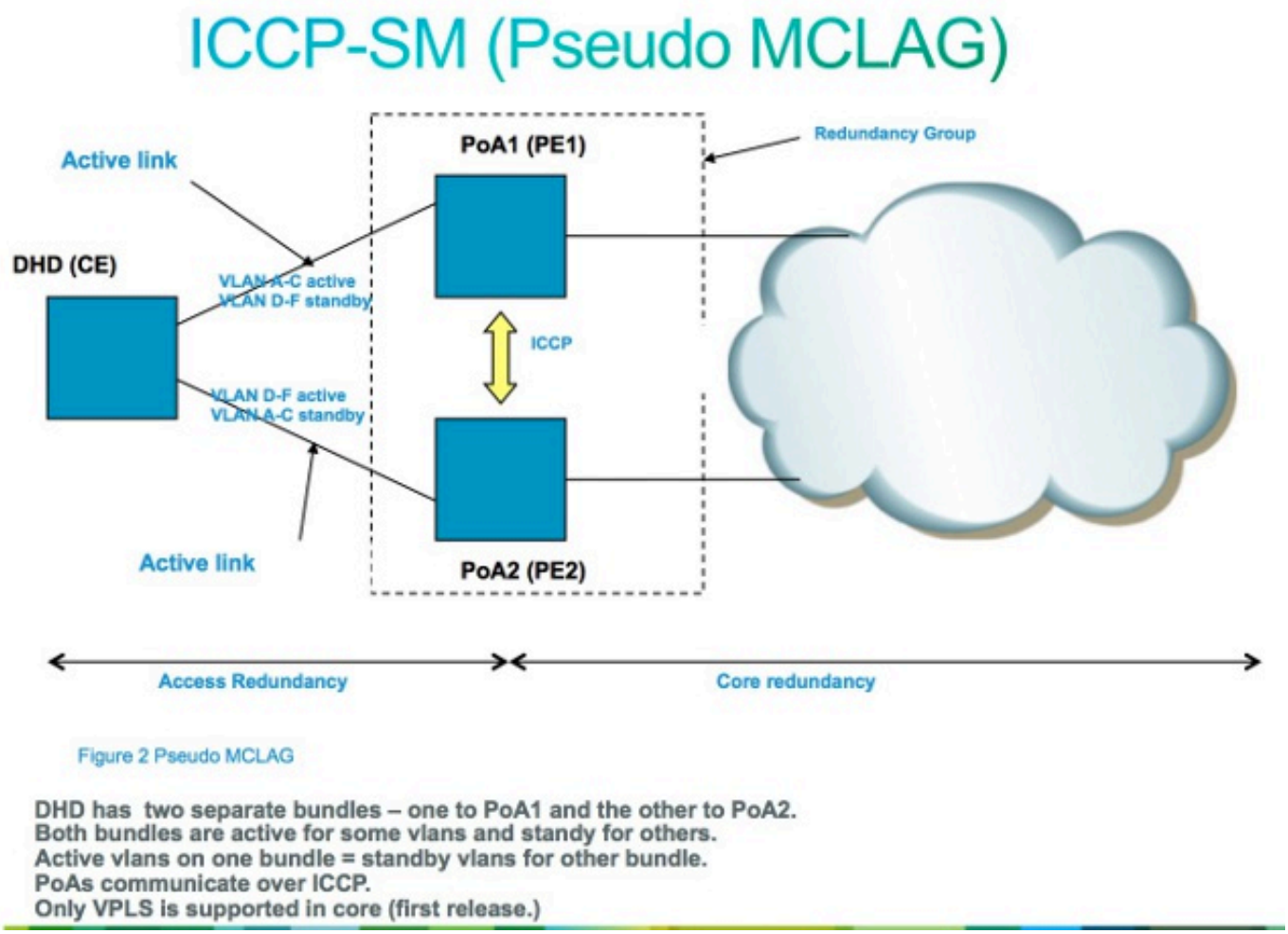


Figure 2 Pseudo MCLAG

4.5 Control de tormentas de tráfico

En un dominio de broadcast L2, existe el riesgo de que un host se comporte mal y envíe una alta velocidad de tramas de broadcast o multicast que deben inundarse en todas partes en el dominio de bridge. Otro riesgo es la creación de un loop L2 (que no se interrumpe por el spanning tree), que resulta en un loop de paquetes de broadcast y multicast. Una alta tasa de paquetes de broadcast y multicast afecta el rendimiento de los hosts en los dominios de broadcast.

El rendimiento de los dispositivos de switching en la red también podría verse afectado por la replicación de una trama de entrada (transmisión, multidifusión o una trama de unidifusión desconocida) en varios puertos de salida en el dominio de puente. La creación de varias copias del mismo paquete puede requerir muchos recursos, dependiendo del lugar dentro del dispositivo en el que se debe replicar el paquete. Por ejemplo, la replicación de una difusión en varias ranuras diferentes no es un problema debido a las capacidades de replicación multidifusión del fabric. El rendimiento de un procesador de red puede verse afectado cuando tiene que crear varias copias del mismo paquete para enviarlas a algunos puertos que el procesador de red está gestionando.

Para proteger los dispositivos en caso de tormenta, la función de control de tormentas de tráfico le permite configurar una velocidad máxima de difusiones, multidifusión y unidifusión desconocida para que se acepten en un dominio de puente AC. Consulte la Guía de Configuración del Sistema de Seguridad del Router de Servicios de Agregación Cisco ASR 9000 Series, Release 4.3.x: Implementación del Control de Tormenta de Tráfico bajo un Puente VPLS para obtener más detalles.

El control de tormentas de tráfico no se admite en interfaces AC de paquetes ni PW de VFI, pero sí en PW de acceso y AC que no son de paquetes. La función está deshabilitada de forma predeterminada; a menos que configure el control de tormentas, acepta cualquier velocidad de difusiones, multidifusión y unidifusión desconocida.

A continuación se muestra un ejemplo de configuración:

```
RP/0/RSP0/CPU0:router2#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
bridge group customer1
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
storm-control unknown-unicast pps 10000
storm-control multicast pps 10000
storm-control broadcast pps 1000
!
neighbor 10.0.0.15 pw-id 15
storm-control unknown-unicast pps 10000
storm-control multicast pps 10000
storm-control broadcast pps 1000
!
vfi customer1-engineering
neighbor 10.0.0.10 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!

RP/0/RSP0/CPU0:router2#sh l2vpn bridge-domain bd-name engineering det
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 6
Filter MAC addresses:
```

```
Create time: 28/05/2013 17:17:03 (1w1d ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 5 (5 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40007; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control:
       Broadcast: enabled(1000)
       Multicast: enabled(10000)
       Unknown unicast: enabled(10000)
Static MAC addresses:
Statistics:
packets: received 251295, sent 3555258
bytes: received 18590814, sent 317984884
Storm control drop counters:
        packets: broadcast 0, multicast 0, unknown unicast 0
        bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
<snip>
```

Los contadores de caídas de control de tormentas siempre están presentes en la salida del comando **show l2vpn bridge-domain detail**. Debido a que la función está inhabilitada de forma predeterminada, los contadores comienzan a notificar caídas sólo cuando la función se ha configurado.

Las velocidades configuradas pueden variar según el patrón de tráfico de una red a otra. Antes de configurar una velocidad, Cisco recomienda que entienda la velocidad de las tramas de difusión, multidifusión o unidifusión desconocida en circunstancias normales. A continuación, agregue un margen en la velocidad configurada por encima de la velocidad normal.

4.6 Movimientos de MAC

En caso de inestabilidad de la red como una inestabilidad de interfaz, se puede aprender una dirección MAC de una nueva interfaz. Esta es la convergencia de red normal, y la tabla de direcciones MAC se actualiza dinámicamente.

Sin embargo, los movimientos constantes de MAC a menudo indican inestabilidad de la red, como inestabilidad severa durante un loop L2. La función de seguridad de direcciones MAC le permite informar sobre movimientos de direcciones MAC y tomar medidas correctivas como cerrar un puerto infractor.

Incluso si no se configura una acción correctiva, puede configurar el comando **logging** para que se le avise de la inestabilidad de la red a través de los mensajes de movimiento MAC:

```
l2vpn
bridge group customer1
bridge-domain engineering
mac
secure
action none
logging
!
!
```

En este ejemplo, la acción se configura en none, por lo que no se hace nada cuando se detecta un movimiento de MAC excepto que se registra un mensaje de syslog. Este es un mensaje de ejemplo:

```
LC/0/0/CPU0:Dec 13 13:38:23.396 : l2fib[239]:
%L2-L2FIB-5-SECURITY_MAC_SECURE_VIOLATION_AC : MAC secure in AC
GigabitEthernet0_0_0_4.1310 detected violated packet - source MAC:
0000.0000.0001, destination MAC: 0000.0001.0001; action: none
```

4.7 Detección IGMP y MLD

De forma predeterminada, las tramas multicast se inundan en todos los puertos de un dominio de bridge. Cuando se utilizan transmisiones de alta velocidad, como los servicios de televisión por IP (IPTV), puede haber una cantidad significativa de tráfico reenviado en todos los puertos y replicado a través de varios PW. Si todas las transmisiones de TV se reenvían a través de una interfaz, esto podría congestionar los puertos. La única opción es la configuración de una función como la indagación IGMP o MLD, que intercepta los paquetes de control multicast para rastrear los receptores y los routers multicast y reenviar los flujos en los puertos solamente cuando sea apropiado.

Consulte la Guía de Configuración de Multicast del Router de Servicios de Agregación Cisco ASR 9000 Series, Release 4.3.x para obtener más información sobre estas funciones.

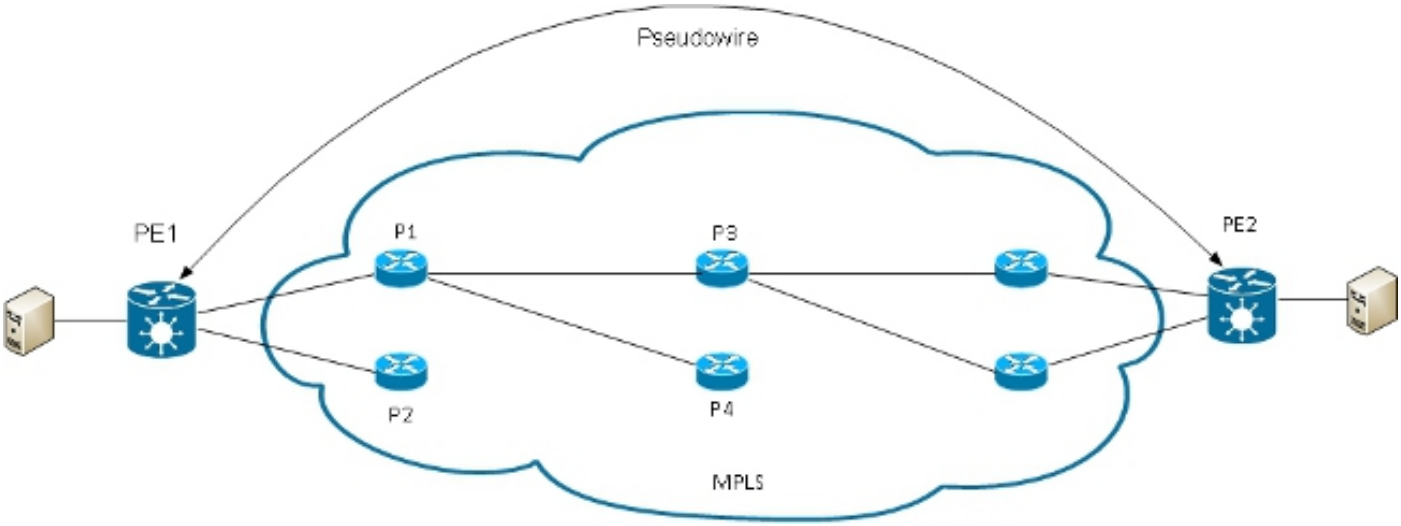
5. Temas adicionales sobre L2VPN

> **Notas:**
>
> Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.
>
> La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

5.1 Equilibrio de carga

Cuando un PE L2VPN necesita enviar una trama a través de un PW MPLS, la trama Ethernet se encapsula en una trama MPLS con una o más etiquetas MPLS; hay al menos una etiqueta PW y quizás una etiqueta IGP para alcanzar el PE remoto.

La trama MPLS es transportada por la red MPLS al PE L2VPN remoto. Normalmente, hay varias rutas para alcanzar el PE de destino:



Nota: No todos los enlaces están representados en este diagrama.

PE1 puede elegir entre P1 y P2 como el primer router P MPLS hacia PE2. Si se selecciona P1, PE1 elige entre P3 y P4, etc. Las rutas disponibles se basan en la topología IGP y la ruta de túnel MPLS TE.

Los proveedores de servicios MPLS prefieren que todos los enlaces se utilicen por igual en lugar de un enlace congestionado con otros enlaces infrautilizados. Este objetivo no siempre es fácil de alcanzar porque algunos PW transportan mucho más tráfico que otros y porque la trayectoria tomada por un tráfico PW depende del algoritmo de hashing utilizado en el núcleo. Varios PW de ancho de banda alto podrían ser hackeados a los mismos links, lo que crea congestión.

Un requisito muy importante es que todos los paquetes de un flujo sigan el mismo trayecto. De lo contrario, esto provoca tramas fuera de servicio, que podrían afectar a la calidad o el rendimiento de las aplicaciones.

El balanceo de carga en una red MPLS en los routers de Cisco se basa generalmente en los datos que siguen la etiqueta MPLS inferior.

- Si los datos inmediatamente después de que la etiqueta inferior comience con 0x4 o 0x6, un router IP MPLS asume que hay un paquete IPv4 o IPv6 dentro del paquete MPLS e intenta balancear la carga basándose en un hash de las direcciones IPv4 o IPv6 de origen y destino extraídas de la trama. En teoría, esto no debería aplicarse a una trama Ethernet que se encapsula y transporta a través de un PW porque la dirección MAC de destino sigue la etiqueta inferior. Sin embargo, recientemente se han asignado algunos rangos de direcciones MAC que comienzan con 0x4 y 0x6. El router IP MPLS podría considerar incorrectamente que el encabezado Ethernet es en realidad un encabezado IPv4 y aplicar hash a la trama basándose en lo que supone que son las direcciones de origen y destino IPv4. Las tramas Ethernet de un PW pueden ser troceadas en diferentes trayectorias en el núcleo MPLS, lo

que conduce a tramas fuera de secuencia en el PW y problemas de calidad de la aplicación. La solución es la configuración de una palabra de control bajo una clase pw que se puede conectar a un punto a punto o a VPLS PW. La palabra control se inserta inmediatamente después de las etiquetas MPLS. La palabra control no comienza con 0x4 o 0x6, por lo que se evita el problema.

```
RP/1/RSP0/CPU0:router#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
pw-class control-word
encapsulation mpls
control-word
!
!
bridge group customer1
bridge-domain engineering
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
pw-class control-word
!
<snip>
RP/1/RSP0/CPU0:router#sh l2vpn bridge-domain bd-name engineering det
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 4, state: up,
ShgId: 0, MSTi: 0
<snip>
List of VFIs:
VFI customer1-engineering (up)
PW: neighbor 10.0.0.11, PW ID 2, state is up ( established )
PW class control-word, XC ID 0xc000000a
Encapsulation MPLS, protocol LDP
Source address 10.0.0.10
PW type Ethernet, control word enabled, interworking none
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------
Label 281708 16043
Group ID 0x4 0x5
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word enabled enabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x7 0x7
(control word) (control word)
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------
```

- Si los datos inmediatamente posteriores a la parte inferior de la pila de etiquetas MPLS no comienzan con 0x4 o 0x6, el router IP se equilibra de carga según la etiqueta inferior. Todo el tráfico de un PW sigue el mismo trayecto, por lo que no se producen paquetes fuera de orden, pero esto podría conducir a la congestión en algunos links en caso de PW de ancho de banda alto. Con la versión 4.2.1 del software Cisco IOS XR, ASR 9000 admite la función de PW Flow Aware Transport (FAT). Esta función se ejecuta en los PE L2VPN, donde se negocia entre los dos extremos de un punto a punto o VPLS PW. El PE L2VPN de entrada

detecta los flujos en la configuración de CA y L2VPN e inserta una nueva etiqueta de flujo MPLS debajo de la etiqueta MPLS PW en la parte inferior de la pila de etiquetas MPLS. El PE de entrada detecta flujos basados en las direcciones MAC de origen y destino (predeterminado) o en las direcciones IPv4 de origen y destino (configurable). El uso de las direcciones MAC es el predeterminado; se recomienda el uso de direcciones IPv4, pero debe configurarse manualmente.

Con la función FAT PW, el PE L2VPN de ingreso inserta una etiqueta MPLS inferior por src-dst-mac o por src-dst-ip. Los routers IP MPLS (entre los PE) hacen hash de tramas sobre las trayectorias disponibles y, a continuación, llegan al PE de destino basándose en esa etiqueta de flujo FAT PW en la parte inferior de la pila MPLS. Esto generalmente proporciona una mejor utilización del ancho de banda en el núcleo a menos que un PW lleve solamente un pequeño número de conversaciones src-dst-mac o src-dst-ip. Cisco recomienda utilizar una palabra de control para evitar tener direcciones MAC que comiencen con 0x4 y 0x6 inmediatamente después de la etiqueta de flujo. Esto garantiza que el hash esté correctamente basado en las seudo direcciones IP y no en la etiqueta de flujo.

Con esta función, el tráfico de un PW se carga equilibrado en varias rutas del núcleo cuando está disponible. El tráfico de aplicaciones no sufre de paquetes fuera de orden porque todo el tráfico del mismo origen (MAC o IP) al mismo destino (MAC o IP) sigue la misma ruta.

Este es un ejemplo de configuración:

```
l2vpn
pw-class fat-pw
encapsulation mpls
control-word
load-balancing
flow-label both
!
!
!
bridge group customer1
bridge-domain engineering
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
pw-class fat-pw


RP/1/RSP0/CPU0:router#sh l2vpn bridge-domain bd-name engineering det
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 4, state: up,
ShgId: 0, MSTi: 0
<snip>
List of VFIs:
VFI customer1-engineering (up)
PW: neighbor 10.0.0.11, PW ID 2, state is up ( established )
PW class fat-pw, XC ID 0xc000000a
Encapsulation MPLS, protocol LDP
Source address 10.0.0.10
PW type Ethernet, control word enabled, interworking none
Sequencing not set
Load Balance Hashing: src-dst-ip
Flow Label flags configured (Tx=1,Rx=1), negotiated (Tx=1,Rx=1)

PW Status TLV in use
```

```
MPLS Local Remote
------------ ------------------------------ ------------------
Label 281708 16043
Group ID 0x4 0x5
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word enabled enabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x7 0x7
(control word) (control word)
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ------------------
```

5.2 Registro

Se pueden configurar diferentes tipos de mensajes de registro en el modo de configuración L2VPN. Configure el registro de l2vpn para recibir alertas de syslog para eventos L2VPN, y configure el registro de pseudowire para determinar cuándo cambia el estado de un PW:

```
l2vpn
logging
bridge-domain
pseudowire
nsr
!
```

Si se configuran muchos PW, los mensajes podrían inundar el registro.

5.3 ethernet-services access-list

Puede utilizar una lista de acceso de servicios Ethernet para descartar el tráfico de hosts específicos o verificar si un router está recibiendo paquetes de un host en una interfaz de transporte L2:

```
RP/0/RSP0/CPU0:router#sh run ethernet-services access-list count-packets
ethernet-services access-list count-packets
10 permit host 001d.4603.1f42 host 0019.552b.b5c3
20 permit any any
!

RP/0/RSP0/CPU0:router#sh run int gig 0/1/0/3.2
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
ethernet-services access-group count-packets egress
!

RP/0/RSP0/CPU0:router#sh access-lists ethernet-services count-packets
hardware egress location 0/1/CPU0
ethernet-services access-list count-packets
10 permit host 001d.4603.1f42 host 0019.552b.b5c3 (5 hw matches)
20 permit any any (30 hw matches)
```

Las coincidencias de hardware sólo se pueden ver con la palabra clave *hardware*. Utilice la palabra clave *ingress* o *egress* dependiendo de la dirección del grupo de acceso. También se

especifica la ubicación de la tarjeta de línea de la interfaz donde se aplica la lista de acceso.

También puede aplicar una lista de acceso ipv4 en una interfaz l2transport como una función de seguridad o resolución de problemas:

```
RP/0/RSP0/CPU0:router#sh run ipv4 access-list count-pings
ipv4 access-list count-pings
10 permit icmp host 192.168.2.1 host 192.168.2.2
20 permit ipv4 any any
!

RP/0/RSP0/CPU0:router#sh run int gig 0/1/0/3.2
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
ipv4 access-group count-pings ingress
!

RP/0/RSP0/CPU0:router#sh access-lists ipv4 count-pings hardware ingress
location 0/1/CPU0
ipv4 access-list count-pings
10 permit icmp host 192.168.2.1 host 192.168.2.2 (5 hw matches)
20 permit ipv4 any any (6 hw matches)
```

5.4 ethernet egress-filter

En la dirección de salida de un AC, suponga que no hay un comando **rewrite ingress tag pop <> symmetric** que determine las etiquetas VLAN de salida. En ese caso, no hay ninguna verificación para asegurarse de que la trama saliente tenga las etiquetas VLAN correctas según el comando **encapsulation**.

Este es un ejemplo de configuración:

```
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
!
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
!
interface GigabitEthernet0/1/0/39.2 l2transport
encapsulation dot1q 2
!
l2vpn
bridge group customer2
bridge-domain test
interface GigabitEthernet0/1/0/3.2
!
interface GigabitEthernet0/1/0/3.3
!
interface GigabitEthernet0/1/0/39.2
!
!
!
!
```

En esta configuración, tenga en cuenta que:

- Una transmisión recibida con una etiqueta dot1q 2 en GigabitEthernet0/1/0/39.2 mantiene su

etiqueta entrante porque no hay un comando **rewrite ingress**.

- Esa transmisión se inunda de GigabitEthernet0/1/0/3.2 con su etiqueta dot1q 2, pero eso no causa un problema porque GigabitEthernet0/1/0/3.2 también está configurado con la etiqueta dot1q 2.
- Esa transmisión también se inunda de GigabitEthernet0/1/0/3.3, que mantiene su etiqueta original 2 porque no hay un comando **rewrite** en GigabitEthernet0/1/0/3.3. El comando **encapsulation dot1q 3** en GigabitEthernet0/1/0/3.3 no se verifica en la dirección de salida.
- El resultado es que, para una transmisión recibida con la etiqueta 2 en GigabitEthernet0/1/0/39, hay dos transmisiones con la etiqueta 2 saliendo de GigabitEthernet0/1/0/3. Ese tráfico duplicado podría causar algunos problemas en la aplicación.
- La solución es la configuración de *ethernet egress-filter strict* para garantizar que los paquetes salgan de la subinterfaz con las etiquetas VLAN correctas. De lo contrario, los paquetes no se reenvían y se descartan.

```
interface GigabitEthernet0/1/0/3.2 l2transport
ethernet egress-filter strict
!
interface GigabitEthernet0/1/0/3.3 l2transport
ethernet egress-filter strict
!
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).