# Servicios y características IOS XR L2VPN

## Contenido

# Introducción

Este documento describe las topologías de la capa básica 2 (L2) VPN (L2VPN). Es útil presentar los ejemplos básicos para demostrar el diseño, los servicios, las características, y la configuración. Vea el router L2VPN de los servicios de la agregación de las 9000 Series de Cisco ASR y los servicios Ethernet guía de configuración, la versión 4.3.x para la información adicional.

# 1. Servicios de punto a punto y de múltiples puntos

La característica L2VPN proporciona la capacidad de proporcionar los servicios de punto a punto y de múltiples puntos.

## 1.1 Servicio Point-to-Point

El servicio Point-to-Point emula básicamente a un circuito del transporte entre los Nodos del dos extremos así que los nodos extremos aparecen ser conectados directamente sobre un enlace punto a punto. Esto se puede utilizar para conectar dos sitios.

En la realidad, puede haber routeres múltiples entre los Nodos del dos extremos, y puede haber diseños múltiples para proporcionar el servicio Point-to-Point.

Un router puede hacer el Local Switching entre dos de sus interfaces:

Puede también haber un pseudowire del Multiprotocol Label Switching (MPLS) (picovatio) entre dos Routers:

Un router puede las tramas de Switch entre dos PWs; en este caso, esto es un multi-segmento picovatio:

La Redundancia está disponible a través de la función de redundancia picovatio:

Otros diseños están disponibles, pero no se pueden todos enumerar aquí.

## 1.2 Servicio de múltiples puntos

El servicio de múltiples puntos emula a un dominio de broadcast de modo que todos los host

conectados en ese dominio de Bridge aparezcan ser conectados lógicamente con el mismo segmento Ethernet:

Todos los host se pueden conectar con el mismo router/el Switch:

Los switches múltiples pueden hacer el Ethernet Switching tradicional; el atravesar - el árbol se debe utilizar para romper los loopes:

Los servicios virtuales del LAN privado (VPL) le dejan extender el dominio de broadcast entre los sitios múltiples usando MPLS PWs:

Los VPL jerárquicos se pueden utilizar para aumentar el scalability:

# 2. Circuitos de la conexión

## Circuito virtual de los Ethernetes del 2.1 ASR 9000

### 2.1.1 El corresponder con de la interfaz entrante

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

- Un paquete se debe recibir en una interfaz configurada con la palabra clave *l2transport* para ser procesado por la característica L2VPN.
- Esta interfaz puede ser una interfaz principal, donde el comando **l2transport** se configura bajo modo de configuración de la interfaz, o una subinterfaz, donde la palabra clave *l2transport* se configura después del número de la subinterfaz.
- Las operaciones de búsqueda más largas del emparejamiento determinan la interfaz entrante del paquete. Las operaciones de búsqueda más largas de la coincidencia marcan estas condiciones en esta orden para hacer juego el paquete entrante a una subinterfaz:

    1. La trama entrante tiene dos etiquetas del dot1q y hace juego una subinterfaz configurada con las mismas dos etiquetas del dot1q (802.1Q que hace un túnel, o QinQ). Ésta es la coincidencia posible más larga.
    2. La trama entrante tiene dos etiquetas del dot1q y hace juego una subinterfaz configurada con el mismo dot1q primero marca con etiqueta y *ningunos* para la segunda etiqueta.
    3. La trama entrante tiene una etiqueta del dot1q y hace juego una subinterfaz configurada con la misma etiqueta del dot1q y la palabra clave *exacta*.
    4. La trama entrante tiene una o más etiquetas del dot1q y hace juego una subinterfaz configurada con una de las etiquetas del dot1q.
    5. La trama entrante no tiene ninguna etiqueta del dot1q y hace juego una subinterfaz configurada con el comando **untagged de la encapsulación**.
    6. La trama entrante no puede hacer juego ninguna otra subinterfaz, así que hace juego una subinterfaz configurada con el **comando default de la encapsulación**.
    7. La trama entrante no puede hacer juego ninguna otra subinterfaz, así que hace juego la interfaz principal que se configura para *l2transport*.

- En los Router tradicionales que no utilizan el modelo de la conexión virtual de los Ethernetes (EVC), las etiquetas del VLA N configuradas bajo subinterfaz se quitan (hecho estallar) de la trama antes de que sean transportadas por la característica L2VPN.
- En las 9000 Series de Cisco ASR una agregación mantiene al router que utiliza la infraestructura EVC, la acción predeterminada es preservar las etiquetas existentes. Utilice el comando de la **reescritura** de modificar el valor por defecto.
- Si hay un (BVI) del Interfaz Virtual de Bridge en el dominio de Bridge, todas las etiquetas entrantes deben ser hechas estallar porque el BVI es una interfaz ruteada sin ninguna etiqueta. Vea la sección BVI para los detalles.

Aquí están varios ejemplos que ilustran estas reglas:

1. Un ejemplo básico es cuando todo el tráfico recibido en un puerto físico debe ser transportado, independientemente de si tiene una etiqueta del VLA N. Si usted configura **l2transport** bajo interfaz principal, todo el tráfico recibido en ese puerto físico es transportado por la característica L2VPN:

   ```
   interface GigabitEthernet0/0/0/2
   l2transport
   ```
   Si hay subinterfaces de esa interfaz principal, la interfaz principal coge cualquier trama que no fuera correspondida con por ninguna subinterfaz; ésta es la regla más larga de la coincidencia.

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

   ```
   interface Bundle-Ether1
   l2transport
   ```
3. Utilice el **valor por defecto de la encapsulación** bajo subinterfaz l2transport para hacer juego cualquier haber marcado con etiqueta o tráfico sin Tags que no haya sido correspondido con por otra subinterfaz con una coincidencia más larga. (Véase el ejemplo 4). La palabra clave *l2transport* se configura en el nombre de la subinterfaz, no bajo subinterfaz como en la interfaz principal:

   ```
   interface GigabitEthernet0/1/0/3.1 l2transport
   encapsulation default
   ```
   Configure la **encapsulación untagged** si usted quiere hacer juego solamente las tramas sin Tags.

4. Cuando hay subinterfaces múltiples, funcione con la prueba de la cerilla 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, observe eso:

   - Una trama de QinQ con una etiqueta externa 2 del VLA N y una etiqueta interna 3 del VLA N podría hacer juego la .1, .2, o .3 subinterfaz pero se asigna a la .3 subinterfaz debido a la regla más larga de la coincidencia. Dos etiquetas en .3 son más largas de una etiqueta en

.2 y más largas que ninguna etiqueta en .1.
- Una trama de QinQ con una etiqueta externa 2 del VLA N y una etiqueta interna 4 del VLA N se asigna a la .2 subinterfaz porque el **dot1q 2 de la encapsulación** puede hacer juego las tramas del dot1q con apenas la etiqueta 2 del VLA N pero puede también hacer juego las tramas de QinQ con una etiqueta externa 2. refiere al ejemplo 5 (la palabra clave *exacta*) si usted no quiere hacer juego las tramas de QinQ.
- Una trama de QinQ con una etiqueta externa 3 del VLA N hace juego la .1 subinterfaz.
- Una trama del dot1q con una etiqueta 2 del VLA N hace juego la .2 subinterfaz.
- Una trama del dot1q con una etiqueta 3 del VLA N hace juego la .1 subinterfaz.

5. Para hacer juego una trama del dot1q y no una trama de QinQ, utilice la palabra clave *exacta*:

```
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2 exact
```
Esta configuración no hace juego las tramas de QinQ con una etiqueta externa 2 del VLA N porque hace juego solamente las tramas con exactamente una etiqueta del VLA N.

6. Utilice la palabra clave *untagged* para hacer juego solamente las tramas sin Tags tales como paquetes o Múltiples Árboles de expansión (MST) Unidades (BPDU) del Cisco Discovery Protocol (CDP):

```
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, observe eso:

- Las tramas del dot1q con un VLA N marcan 3 con etiqueta o las tramas de QinQ con una etiqueta externa 3 hacen juego la .3 subinterfaz.
- El resto de dot1q o de las tramas de QinQ hace juego la .1 subinterfaz.
- Capítulos sin una coincidencia de etiqueta del VLA N la .2 subinterfaz.

7. *La cualquier* palabra clave 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 hacer juego las tramas de QinQ con las etiquetas 4 y 5, pero las tramas se asignan a la .5 subinterfaz porque es más específica. Ésta es la regla más larga de la coincidencia.

8. Los rangos de las etiquetas del VLA N pueden ser utilizados:

```
interface GigabitEthernet0/1/0/3.6 l2transport
encapsulation dot1q 6-10
```
9. Los valores o los rangos de la etiqueta del VLAN múltiple pueden ser mencionados para la

primera o segunda etiqueta del 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
```
Usted puede enumerar un máximo de nueve valores. Si se requieren más valores, deben ser asignados a otra subinterfaz. Valores de grupo en un rango para acortar la lista.

10. El comando del **dot1q second-dot1q de la encapsulación** utiliza el Ethertype 0x8100 para las etiquetas externas e internas porque éste es el método de Cisco para encapsular las tramas de QinQ. Según IEEE, sin embargo, el Ethertype 0x8100 debe ser reservado para las tramas 802.1q con una etiqueta del VLA N, y una etiqueta externa con el Ethertype 0x88a8 se debe utilizar para las tramas de QinQ. La etiqueta externa con el 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 Ethertype viejo 0x9100 o 0x9200 para las etiquetas externas de QinQ, utilice el **dot1q que hace un túnel el** comando del **ethertype** bajo interfaz principal de la subinterfaz de 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 de 0x9200, y la etiqueta interna tiene el Ethertype 0x8100 del dot1q.

12. Una trama entrante se puede asignar a una subinterfaz, sobre la base del MAC Address de origen:

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

### 2.1.2 Manipulación del VLA N

El comportamiento predeterminado de una plataforma EVC-basada es guardar las etiquetas del VLA N en la trama entrante.

```
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
```
En esta configuración, una trama entrante del dot1q con una etiqueta 3 del VLA N guarda su etiqueta 3 del VLA N cuando se remite la trama. Una trama entrante de QinQ con una etiqueta externa 3 del VLA N y una etiqueta interna 100 mantiene ambas etiquetas sin cambios cuando se remite la trama.

Pero, la infraestructura EVC permite que usted manipule las etiquetas con el comando de la **reescritura**, así que usted puede hacer estallar (quitar), traducir, o las etiquetas del empuje (agregue) al stack entrante de la etiqueta del VLA N.

Aquí están varios ejemplos:

- La palabra clave del *estallido* le deja quitar una etiqueta de QinQ de una trama entrante del dot1q. Este ejemplo quita la etiqueta externa 13 del bastidor entrante de QinQ y adelante del bastidor con la etiqueta 100 del dot1q en el top:

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

El comportamiento es siempre simétrico, así que significa que la etiqueta externa 13 está hecha estallar en la dirección de ingreso y empujada hacia adentro la dirección de salida.

- La palabra clave del *traducir* le deja substituir uno o dos etiquetas entrantes por uno o dos nuevas etiquetas:

```
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 *simétrica* se agrega automáticamente porque es el único modo soportado.

- La palabra clave del *empuje* le deja agregar una etiqueta de QinQ a una trama entrante del dot1q:

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

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

## 2.2 Comportamiento del router del Cisco IOS XR NON-EVC (CRS y XR12000)

El sintaxis para el VLA N que corresponde con en las Plataformas NON-EVC no utiliza la *palabra clave de la encapsulación*:

```
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 la etiqueta del VLA N no puede ser configurada, porque el único comportamiento posible es hacer estallar todas las etiquetas que se especifican en el **dot1q** o los comandos **dot1ad**. Esto se hace por abandono, tan allí no es ningún comando de la **reescritura**.

# 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 del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

## 3.1 Local Switching

### 3.1.1 Interfaz principal

La topología básica es un Cross Connect local entre dos interfaces principales:

El router2 lleva todo el tráfico recibido en el soldado enrollado en el ejército 0/1/0/1 y adelante él Te 0/0/0/3 y vice versa.

Mientras que el router1 y el router3 aparecen tener un cable continuo directo en esta topología, éste no es el caso porque el router2 está traduciendo realmente entre las interfaces de TenGigE y del gigabitethernet. El router2 puede funcionar con las características en estas dos interfaces; un Access Control List (ACL), por ejemplo, puede caer los tipos específicos de paquetes o de un directiva-mapa para formar o de tráfico de la prioridad baja del tarifa-límite.

Un Cross Connect de punto a punto básico se configura entre dos interfaces principales que se configuren 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 el CDP y un direccionamiento del 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 el router3 como vecino CDP y puede hacer ping 10.1.1.2 (el direccionamiento de la interfaz del router3) como si el dos Routers fuera conectado directamente.

Porque no hay subinterfaz configurada en el router2, las tramas entrantes con una etiqueta del VLA N se transportan transparente cuando las subinterfaces del 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 ping del router1 al router3, usted puede utilizar la **interfaz de la demostración** y los comandos de la **demostración l2vpn** para asegurarse de que los pedidos de ping recibidos por el router2 en un AC están remitidos en el otro AC y de que las contestaciones del ping están manejadas la misma manera en el revés.

```
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 del VLA N

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

Esta topología utiliza típicamente un dominio de Bridge porque hay generalmente más de dos puertos en el VLA N, aunque usted pueda utilizar un Cross Connect de punto a punto si hay solamente dos puertos. Esta sección describe cómo las capacidades flexibles de la reescritura le dan las diferentes formas de manipular el VLA N.

#### Interfaz principal de 3.1.2.1 y subinterfaz del dot1q

En este ejemplo, la interfaz principal está en un lado, y la subinterfaz del 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
!
```

Ésta es la subinterfaz del 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 la subinterfaz de TenGigE0/0/0/3.2. El router3 envía las tramas del dot1q con la etiqueta 2, que hacen juego la subinterfaz TenGigE0/0/0/3.2 en el router2.

La etiqueta entrante 2 es quitada en la dirección de ingreso por el comando **simétrico del estallido 1 de la etiqueta del ingreso de la reescritura**. Puesto que la etiqueta se ha quitado en la dirección de ingreso en el TenGigE0/0/0/3.2, los paquetes se envían untagged en la dirección de salida en GigabitEthernet0/1/0/1.

El router1 envía las tramas sin Tags, que hacen juego la interfaz principal GigabitEthernet0/1/0/1.

No hay comando de la **reescritura** en GigabitEthernet0/1/0/1, así que no se hace estallar, se avanza, o se traduce ninguna etiqueta.

Cuando los paquetes tienen que ser remitidos de TenGigE0/0/0/3.2, la etiqueta 2 del dot1q es avanzado debido a la palabra clave *simétrica* en el **comando 1 del estallido de la etiqueta del ingreso de la reescritura**. Los estallidos del comando una etiqueta en la dirección de ingreso pero avanzan simétricamente una etiqueta en la dirección de salida. Esto 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
```

Monitoree los contadores de la subinterfaz con la misma **interfaz de la demostración** y **muestre los** comandos **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 hace juego el número de paquetes enviados en GigabitEthernet0/1/0/1 y vice versa.

#### Subinterfaz de 3.1.2.2 con la encapsulación

En vez de la interfaz principal en GigabitEthernet0/1/0/1, usted puede utilizar una subinterfaz con el **valor por defecto de la encapsulación** para coger todas las tramas o con la **encapsulación untagged** para hacer juego solamente las tramas sin Tags:

```
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
```

#### Dirección de ingreso de 3.1.2.3 en GigabitEthernet0/1/0/1.1

Bastante que la etiqueta 2 del estallido en la dirección de ingreso en TenGigE0/0/0/3.2, usted puede avanzar la etiqueta 2 en la dirección de ingreso en GigabitEthernet0/1/0/1.1 y no hacer cualquier cosa 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
```

Así, usted puede ver que el modelo EVC con los comandos de la **encapsulación** y de la **reescritura** le da la gran flexibilidad para hacer juego y para manipular las etiquetas del VLA N.

## 3.2 Agencias de noticias privadas virtuales

### 3.2.1 Descripción

Las agencias de noticias privadas virtuales (VPWS), también conocidas como Ethernet por MPLS (EoMPLS), permiten que dos dispositivos del borde del proveedor L2VPN (PE) hagan un túnel el tráfico L2VPN sobre una nube MPLS. Los dos L2VPN PE están conectados típicamente en dos diversos sitios con una base MPLS entre ellos. Los dos AC conectados en cada L2VPN PE son conectados por un picovatio sobre la red MPLS, que es el MPLS picovatio.

Cada PE necesita tener una escritura de la etiqueta MPLS para alcanzar el loopback del telecontrol PE. Esta escritura de la etiqueta, generalmente llamada la escritura de la etiqueta del Interior Gateway Protocol (IGP), puede ser docta con el Protocolo de distribución de etiquetas (LDP) o la Ingeniería de tráfico MPLS (TE) MPLS.

Los dos PE establecen a una sesión LDP apuntada MPLS entre ellos mismos así que pueden establecer y controlar el estatus del picovatio. Un PE hace publicidad al otro PE de la escritura de la etiqueta MPLS para la identificación picovatio.

Nota: Mientras que el BGP se puede utilizar para señalar, no se cubre en este documento.

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

- La escritura de la etiqueta externa MPLS es la escritura de la etiqueta IGP para alcanzar el loopback del router3. Ésta podría ser la escritura de la etiqueta implícito-nula si las escrituras de la etiqueta están conectadas directamente; esto significa que no se añadiría al final del fichero ninguna escritura de la etiqueta IGP.
- La escritura de la etiqueta interna MPLS es la escritura de la etiqueta picovatio de divulgación por el router3 a través de la sesión LDP apuntada.
- Puede haber una palabra de control picovatio después de que las escrituras de la etiqueta MPLS, dependiendo de la configuración y del tipo de encapsulación. La palabra de control no se utiliza por abandono en las interfaces de Ethernet y debe ser configurada explícitamente cuando está necesitada.
- La trama transportada L2 sigue en el paquete.
- Algunas etiquetas del VLA N se transportan sobre el picovatio, dependiendo de la configuración y del tipo picovatio.

El penúltimo salto, momentos antes que router3 en la base MPLS, hace estallar la escritura de la etiqueta IGP o la substituye por una Etiqueta NULL explícita. Así, la escritura de la etiqueta significativa superior en la trama recibida por el router3 es la escritura de la etiqueta picovatio que el router3 señaló al router2 para el picovatio. Así pues, el router3 sabe que el tráfico recibido con esa escritura de la etiqueta MPLS se debe conmutar al AC conectado con router4.

En el ejemplo anterior, usted debe en primer lugar controle si cada L2VPN tiene una escritura de la etiqueta MPLS para el loopback del telecontrol PE. Éste es un ejemplo de cómo a las etiquetas de comprobación 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 AC sigue siendo lo mismo:

```
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
```

Porque no hay comando del **estallido del ingreso de la reescritura**, la etiqueta entrante 2 del VLA N se transporta sobre el picovatio. Véase el tipo 4 y 5 PWs para los detalles.

La configuración L2VPN especifica el AC local y el telecontrol L2VPN PE con un picovatio ID que deba hacer juego en cada lado y deba 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 router3 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 detail del xconnect de la demostración l2vpn** para ver los detalles en el Cross Connect:

```
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, observe eso:

- La Unidad máxima de transmisión (MTU) (MTU) del AC es 1504 porque la etiqueta entrante en el AC no se hace estallar. El MTU debe hacer juego en cada lado, o el picovatio no sube.
- 186 paquetes fueron recibidos en el AC y enviados en el picovatio como se esperaba.
- 38448 paquetes fueron recibidos en el picovatio y enviados en el AC como se esperaba.
- La escritura de la etiqueta local en el router2 es 16026 y es la escritura de la etiqueta que el router3 utiliza como la escritura de la etiqueta interna. Los paquetes se reciben en el router2 con esa escritura de la etiqueta MPLS mientras que la escritura de la etiqueta superior porque la escritura de la etiqueta IGP ha sido hecha estallar por el penúltimo salto MPLS. El router2 sabe que las tramas entrantes con esa escritura de la etiqueta picovatio se deben conmutar al soldado enrollado en el ejército 0/0/0/1.2 AC:

```
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 picovatios y el AC juntaron el estatus

En un Cross Connect de punto a punto, se juntan el AC y el picovatio. Así pues, si va el AC abajo, el L2VPN PE señala vía el LDP al telecontrol PE que el estatus picovatio debe estar abajo. Esto acciona la convergencia cuando se configura la Redundancia picovatio. Vea la sección de redundancia para los detalles.

En este ejemplo, el AC está abajo en el router2 y está enviando el estatus “AC abajo” picovatio al router3:

```
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 router3 sabe que el picovatio debe estar abajo porque el telecontrol AC está abajo:

```
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 Tipo 4 y tipo 5 PWs

Dos tipos de PWs pueden ser utilizados - el tipo 4 y el tipo 5.

- Conocen a un tipo 4 picovatios como picovatio VLAN basado. El ingreso PE no se supone para quitar las etiquetas entrantes del VLA N que deben ser transportadas sobre el picovatio.

  En las Plataformas EVC-basadas tales como el ASR 9000, el problema es que los AC entrantes pudieron tener un comando de la **reescritura** que hace estallar las etiquetas entrantes del VLA N, tan allí no pudieron ser cualquier etiqueta del VLA N que se transportará sobre el picovatio. Para dirigir esta posibilidad, las Plataformas EVC insertan una etiqueta simulada 0 del VLA N encima de la trama para el tipo 4 PWs. Configuran al tipo 4 PWs con el **comando vlan transporte-MODE**. El telecontrol PE se debe EVC-basar y debe entender que la etiqueta superior del VLA N es la etiqueta simulada que se eliminará.

  Sin embargo, si usted utiliza un tipo 4 picovatios entre una plataforma EVC y una plataforma NON-EVC, esto pudo llevar a los problemas de interoperabilidad. La plataforma NON-EVC no considera la etiqueta superior del VLA N como la etiqueta simulada del VLA N y en lugar de otro adelante la trama con la etiqueta simulada 0 del VLA N como la etiqueta externa. Las Plataformas EVC tienen la capacidad de manipular las etiquetas del VLA N recibidas en la trama entrante con el comando de la **reescritura**. Los resultados de esa manipulación del VLA N se transportan sobre el tipo 4 picovatios con la etiqueta simulada adicional 0 en el top.

  Las versiones recientes del Software Cisco IOS XR ofrecen la capacidad de utilizar un tipo 4 picovatios sin el uso de la etiqueta simulada 0 con el comando **vlan del passthrough transporte-MODE**. La manipulación de la etiqueta del VLA N en los Ethernetes fluye la punta (EFP) debe asegurarse de que por lo menos sigue habiendo una etiqueta porque debe haber etiqueta del VLA N transportada en un tipo 4 picovatios y porque, en este caso, no hay etiqueta simulada que cumple ese requisito. Las etiquetas que sigue habiendo en la trama después de que la reescritura de la etiqueta de la interfaz entrante se transporte transparente con el picovatio.

- Conocen a un tipo 5 picovatios como acceso basado picovatio de los Ethernetes. Las tramas de transportes del ingreso PE recibidas en una interfaz principal o después de que se hayan quitado las etiquetas de la subinterfaz cuando el paquete se recibe en una subinterfaz. No hay requisito de enviar una trama marcada con etiqueta sobre un tipo 5 picovatios, y no se agrega ninguna etiqueta simulada por las Plataformas EVC-basadas. Las Plataformas EVC-basadas tienen la capacidad de manipular las etiquetas del VLA N recibidas en la trama entrante con el comando de la **reescritura**. Los resultados de esa manipulación del VLA N se transportan sobre el tipo 5 picovatios, están marcados con etiqueta o untagged.

Por abandono, el L2VPN PE intenta negociar un tipo 5 picovatios, como se ve 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 Ethernet del tipo picovatio indica un tipo 5 picovatios.

Ésta es una captura del sniffer de un pedido ARP enviado por el router1 y encapsulado por el router2 sobre el picovatio 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 escritura de la etiqueta 16031 MPLS es la escritura de la etiqueta picovatio de divulgación por el router3. La captura del sniffer se ha tomado entre el penúltimo salto y el router3, tan allí no es ninguna escritura de la etiqueta IGP.

La trama Ethernet encapsulada comienza inmediatamente después de la escritura de la etiqueta picovatio. Puede haber una palabra de control picovatio, pero no se configura en este ejemplo.

Incluso si es un tipo 5 picovatios, la etiqueta entrante 2 del VLA N recibida en el AC por el router2 se transporta porque no hay comando de la **reescritura** que lo hace estallar en el AC. Los resultados que vienen del AC después de que se transporte el proceso de la reescritura porque no hay etiqueta automática haciendo estallar en las Plataformas EVC-basadas. Note que no hay etiqueta simulada 0 del VLA N con un tipo 5 picovatios.

Si usted configurara con el comando **simétrico del estallido 1 de la etiqueta del ingreso de la reescritura**, no habría etiqueta del VLA N transportada sobre el picovatio.

Aquí está un ejemplo de un tipo 4 picovatios con la configuración de una picovatio-clase en el router2 y el router3.

> Nota: Si usted configura un tipo 4 en un lado solamente, el picovatio permanece abajo y señala el “error: Tipo picovatio unido mal.”

```
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
!
!
!
!
```

Las redes Ethernet VLAN del tipo picovatio indican un tipo 4 picovatios.

```
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 simulada 0 insertada encima de la trama que es transportada:

```
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 EVC-basado salida quita la etiqueta simulada y adelante la trama con la etiqueta 2 en su AC local. La salida PE aplica la manipulación local de la etiqueta configurada en su AC en la trama recibida en el picovatio. Si su AC local se configura como **estallido 1 de la etiqueta del ingreso de la reescritura simétrico**, la etiqueta configurada se debe empujar hacia adentro la dirección de salida, así que una nueva etiqueta se avanza encima de la etiqueta 2 recibida en el picovatio. El comando de la reescritura es muy flexible pero usted debe evaluar cuidadosamente lo que usted quiere alcanzar en cada lado del picovatio.

### 3.2.4 Multisegment picovatio

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

Router5 recibe los paquetes en el picovatio del router2 y conmuta los paquetes en su otro picovatio al router3. Router5 está conmutando tan entre PWs para crear un multisegment picovatio entre el router2 y el router3.

La configuración en el router2 ahora señala en router5 como el telecontrol PE:

```
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 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 Type Length Value de la transferencia picovatio (TLV) que es enviado por router5 a cada telecontrol PE (router2 y router3). La descripción es útil cuando usted necesita resolver problemas un problema picovatio cuando hay un router en el centro que hace la transferencia picovatio.

Ingrese el comando sh del xconnect l2vpn para revisar el picovatio que conmuta el TLV:

```
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)
```

Router5 envía un picovatio que conmuta el TLV al router3 con los detalles de su picovatio al router2 y envía un picovatio que conmutan el TLV al router2 con los detalles de su picovatio al router3.

## 3.2.5 Redundancia

Un Punto a punto picovatio se puede utilizar para conectar dos sitios, pero estos dos sitios deben seguir conectados en caso de un error PE o AC.

#### Redundancia del núcleo de 3.2.5.1

Si usted realiza algún cambio de la topología que afecte al desplazamiento en la base MPLS, el MPLS picovatio hereda la nueva trayectoria inmediatamente.

#### Conjunto de 3.2.5.2 sobre PWs

Un dispositivo de la frontera del cliente (CE) se puede conectar con el PE a través de un conjunto de los Ethernetes para proporcionar la redundancia de link si hay una falla de link de los miembros del agrupamiento entre el CE y el PE. El conjunto permanece para arriba incluso si va un miembro del link de agrupamientos abajo. Observe que esto no proporciona la Redundancia PE porque un error PE derriba al conjunto entero.

Un método para la Redundancia es hacer los circuitos múltiples transportar por PWs de punto a

punto. Cada circuito es un miembro de un conjunto de los Ethernetes entre dos CE:

El PE no termina el conjunto y en lugar de otro las tramas de transportes transparente sobre el picovatio, incluyendo las tramas del protocolo link aggregation control (LACP) que los CE intercambian entre ellas.

Con este diseño, la pérdida de un AC o un PE causa a los miembros del agrupamiento va abajo, pero el conjunto permanece para arriba.

> Nota: El LACP BPDU no fue transportado sobre el L2VPN por el ASR 9000 en las versiones anterior que la versión 4.2.1 del Software Cisco IOS XR.

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

- Grupo de la agregación del link del Multichassis (MC-LAG)
- Clúster de la virtualización de la red ASR 9000 (nanovoltio)
- Sistema de transferencia virtual (VSS) en el Switches del Cisco IOS
- Canal del puerto virtual (vPC) en el Switches del nexo de Cisco

Desde la perspectiva del PE, hay una conexión Point-to-Point simple entre un AC y un MPLS picovatio.

#### Redundancia de 3.2.5.3 picovatio

Los PE pueden también proporcionar la Redundancia con una característica llamada Redundancia picovatio.

El router2 tiene un picovatio primario al router3. El tráfico del router1 a router6 fluye sobre ese picovatio primario en circunstancias normales. El router2 también tiene un respaldo picovatio a router4 en la espera en caliente pero, en circunstancias normales, ningunos flujos de tráfico sobre ese picovatio.

Si hay un problema con el picovatio primario, con el telecontrol PE del picovatio primario (router3), o con el AC en el telecontrol PE (router3), el router2 activa inmediatamente el respaldo picovatio, y el tráfico comienza a atravesarlo. El tráfico se mueve de nuevo al picovatio primario 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 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
!
!
!
!
```

Bajo condiciones estables, el picovatio al router3 es activo, y el picovatio a router4 está en un estado 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#
```

Porque se juntan el estatus AC y el estatus picovatio, el router3 señala el “AC abajo” al router2 cuando va el AC en el router3 abajo. El router2 derriba su picovatio primario y activa el respaldo picovatio:

```
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 viene el AC en el router3 salvaguardia, el router2 reactiva el picovatio primario al router3, y el picovatio a router4 vuelve a un estado espera.

El respaldo picovatio también se activa cuando va el router3 abajo, y el router2 pierde la ruta a su loopback.

El paso lógico siguiente es introducir la Redundancia bidireccional picovatio con dos PE en cada sitio:

Sin embargo, esta interconexión total de PWs encuentra un problema cuando dos PWs son activos al mismo tiempo un loop se introduce en la red. El loop necesita estar roto, generalmente por medio del Spanning Tree Protocol (STP). Sin embargo, usted no quiere atravesar - inestabilidad del árbol en un sitio a propagar al otro sitio. Así, es mejor no ejecutar atravesar - árbol en estos PWs y no combinar atravesar - el árbol entre los dos sitios. Es más simple si hay apenas un link lógico entre los dos sitios de modo que el ningún atravesar - se requiere el árbol.

Una solución es utilizar a un conjunto MC-LAG entre los dos PE en un sitio y su CE local. Solamente uno de los dos PE tiene su active de los miembros del agrupamiento de modo que su picovatio al sitio remoto sea activo. El otro PE tiene sus miembros del agrupamiento en el estado espera y tiene su picovatio al sitio remoto abajo. Con solamente un active picovatio entre los dos sitios, no se introduce ningún loop. El PE con el picovatio activo también tiene un picovatio espera al segundo PE en el sitio remoto.

Bajo condiciones estables, los miembros del agrupamiento activos están en el router2 y el router3, y el picovatio activo está entre ellos. Ésta es la configuración en el router3:

```
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 router5, los miembros del agrupamiento locales y el picovatio primario al router2 están en el estado espera, y el respaldo picovatio a router4 está abajo:

```
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 router6, los miembros del agrupamiento al router3 son activos, mientras que los miembros del agrupamiento a router5 están en el estado 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 van los miembros del agrupamiento en el router3 abajo, router6 tiene su miembro activo a 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)
```

Puesto que el bundle-ether222 está abajo en router5, el picovatio juntado al router2 va abajo 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 picovatio al router3 está abajo y activa su respaldo picovatio a 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
------------------------------------------------------------------------------
```

Router5 tiene sus miembros del agrupamiento activos así como su picovatio primario al router2:

```
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
------------------------------------------------------------------------------
```

#### Cluster del borde de 3.2.5.4 ASR 9000 nanovoltio

El diseño anterior basado en los trabajos de la Redundancia MC-LAG y picovatio muy bien para la Redundancia sino, porque algunos miembros del agrupamiento están en el estado espera, ellos no lleva el tráfico bajo condiciones constantes.

Si usted quiere todo el active de los miembros del agrupamiento, incluso bajo condiciones estables, usted puede utilizar un cluster ASR 9000 con los miembros del agrupamiento del CE conectado con cada estante del PE:

Este diseño ofrece la Redundancia contra una falla de link de los miembros del agrupamiento entre el CE y el PE, un error del estante, y una falla de link de la base - mientras el cluster dual se asocia a la base MPLS y hay Redundancia en la base. Los dos estantes no tienen que ser coimplantados y podrían estar en las ubicaciones diferentes. los links del Inter-estante no se representan en este diagrama.

Si usted quiere la Redundancia en el CE, usted puede utilizar una solución del multichassis para el CE:

- MC-LAG
- Clúster ASR 9000 nanovoltio
- VSS
- vPC

La configuración en el cluster 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 le recomienda configura una dirección MAC estática del sistema LACP y una dirección MAC del conjunto para evitar un cambio de la dirección MAC causado por un intercambio señalado del controlador de estante. Este ejemplo muestra cómo encontrar los direccionamientos:

```
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, éste es el conjunto-éter 222 con un miembro en cada estante (diez 0/0/0/8 en 1/0/0/8 del estante 0 y diez en el estante 1) y la subinterfaz del conjunto configurada para un Cross Connect de 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 routeres Cisco y el Switches envían generalmente los paquetes CDP sin las etiquetas del dot1q. Hay los varios escenarios que determinan qué sucede a estos paquetes CDP cuando él es recibida por un router IOS XR configurado para un Cross Connect:

En esta topología, el router1 puede ver su router2 local PE como un vecino CDP o el telecontrol CE router4, dependiendo de la configuración.

### 3.3.1 CDP no habilitado en la interfaz principal de L2VPN PE

Los paquetes CDP del L2VPN CE se transportan sobre el Cross Connect. Los dos L2VPN CE se ven (con el uso del **comando show cdp neighbors**) si la interfaz principal se configura como l2transport o si hay una subinterfaz que corresponde con las tramas CDP untagged.

Éste 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
!
!
!
!
```

Éste es un ejemplo de una subinterfaz untagged:

```
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 sobre el Cross Connect, y los CE se ven como vecinos CDP. El CE no ve el PE como 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 untagged, y el PE y el CE se ven como vecinos. Sin embargo, el CE no ve el telecontrol CE cuando el CDP se habilita en la interfaz principal del L2VPN PE.

Tenga en cuenta que:

- Usted no puede configurar el CDP en una interfaz principal que se configure como l2transport.
- El PE intercepta los paquetes CDP cuando el CDP se configura en la interfaz principal non-l2transport. Esto ocurre incluso si hay una subinterfaz l2transport configurada para hacer juego los paquetes CDP untagged (con el uso de la **encapsulación untagged** o de los **comandos default de la encapsulación**). Los paquetes CDP no se transportan al sitio remoto

en este caso.

## 3.4 Spanning-tree

Si el L2VPN CE es un switch de Ethernet y está enviando atravesar - el árbol BPDU al L2VPN PE, estos BPDU se maneja como tráfico normal y se transporta según la configuración L2VPN.

El STP o el MST BPDU se envía untagged y se transporta con el Cross Connect de punto a punto si la interfaz principal se configura como l2transport o si hay una subinterfaz l2transport configurada con la **encapsulación untagged** o los **comandos default de la encapsulación**.

Por el árbol de expansión de VLAN más (PVST+) o PVST+ rápido (PVRST+) envíe los BPDU marcados con etiqueta se transportan que si hay una subinterfaz l2transport que hace juego la etiqueta del dot1q de los BPDU.

Esto es un ejemplo de topología:

El router2 y el router3 son tramas sin Tags y tramas de transporte con la etiqueta 2 del dot1q:

```
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 los BPDU untagged en el VLAN1 y los BPDU marcados con etiqueta en el VLAN2 de switch4; su puerto raíz está en Gi0/1 hacia 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 del árbol en el sitio A se combina con atravesar - el dominio del árbol que atraviesa en el lado B. Un problema potencial es que atravesando - la inestabilidad del árbol en un sitio pudo propagar al otro sitio.

Si usted se siente confiado que un sitio está conectado solamente con un picovatio con otro sitio y que no hay link trasero que podría introducir un loop físico, es una buena idea no ejecutar atravesar - árbol sobre los dos sitios. Esto guarda los dos el atravesar - los dominios del árbol aislados. Para hacer esto, configurar atravesar - bpdufilter del árbol en los CE, o configurar una lista de acceso de los servicios Ethernet en los PE para caer las tramas con la dirección MAC del destino usada por los BPDU. Una lista de acceso de los servicios Ethernet en los PE se puede utilizar para caer las tramas con el MAC de destino BPDU u otras clases de protocolos L2 que usted no quiera remitir sobre el picovatio.

Ésta es una lista de acceso que usted podría utilizar bajo cada interfaz (sub) l2transport que se está transportando 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
!
```

Los servicios Ethernet ACL comienzan a caer los 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 no recibe los BPDU de switch4 más, así que switch1 ahora es 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 que atraviesa - el árbol en un link es éste: si una conexión backdoor (Puerta de servicio) se crea entre los sitios, introduce un loop físico, y atravesar - el árbol no puede romper el loop. Así pues, cuando usted inhabilita atravesar - el árbol sobre un picovatio, se asegura de que no haya links redundantes entre los sitios y de que el picovatio sigue siendo la única conexión entre los sitios.

Si hay conexiones múltiples entre los sitios, utilice una solución como los VPL junto con una versión del gateway de acceso de atravesar - árbol, tal como gateway de acceso MST (MSTAG) o gateway de acceso PVST+ (PVSTAG). Vea la sección en el servicio de múltiples puntos para los

detalles.

## 4. Servicio de múltiples puntos

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

Vea implementar los servicios de múltiples puntos de la capa 2 para una descripción completa de las características de múltiples puntos L2.

Con solamente dos interfaces en un Cross Connect de punto a punto, un Switch L2VPN toma todo recibida en el lado y adelante él en el otro lado.

Cuando hay más de dos interfaces en un dominio de Bridge, un switch de Ethernet tiene que tomar una decisión de Switching para determinar donde remitir las tramas basadas en su MAC address del destino. El Switch hace el aprendizaje de MAC basado en el MAC Address de origen de los bastidores que recibe y construye un mac-address-table.

Del Switch las tramas adelante en este método:

- Las tramas de broadcast se inundan a todos los puertos. Utilice el control de tormentas para limitar la tarifa de la inundación de broadcast.
- Las tramas de multidifusión se inundan a todos los puertos en el dominio de Bridge, excepto cuando se configura el Internet Group Management Protocol (IGMP) o el snooping de la detección del módulo de escucha del Multicast (MLD). Utilice el control de tormentas para limitar la tarifa de la inundación de multidifusión.
- Las tramas de unidifusión con una dirección MAC del destino que no sea parte del mac-address-table del dominio de Bridge (unidifusión desconocida) se inundan en todos los puertos en el dominio de Bridge. Utilice el control de tormentas para limitar la tarifa de la inundación de la unidifusión desconocida.
- Las tramas de unidifusión con una dirección MAC del destino que sea parte del mac-address-table del dominio de Bridge se remiten al puerto en donde se ha aprendido la dirección MAC del destino.

En el Software Cisco IOS XR, un dominio de broadcast o un LAN emulado se llama un dominio de Bridge. Esto es similar a un VLA N en la terminología del Cisco IOS Software, salvo que un VLA N en el IOS se conecta a un número VLAN que se utilice como la etiqueta del dot1q en los trunks. Un dominio de Bridge en el Software Cisco IOS XR no se conecta a un número de Tag del VLA N del dot1q. Usted puede utilizar el modelo EVC para manipular las etiquetas del dot1q y tener subinterfaces del dot1q con diversos números VLAN del dot1q en el mismo dominio de Bridge o tener interfaces untagged.

Un dominio de Bridge es básicamente un dominio de broadcast donde se inundan los broadcasts

y las tramas de multidifusión. Un mac-address-table se asocia a cada dominio de Bridge (a menos que el aprendizaje de MAC es inhabilitado manualmente por la configuración, que es muy rara). Esto corresponde generalmente a una subred del IPv4 o del IPv6 donde todos los host en el dominio de Bridge están conectados directamente.

Los dominios de Bridge se pueden agrupar dentro de un Grupo de Bridge. Esto es una manera conveniente de marcar la configuración. Usted puede ejecutar un comando show para un Grupo de Bridge en vez de un comando show para cada dominio de Bridge. Un Grupo de Bridge no tiene un mac-address-table u otras asociaciones; apenas se utiliza para la configuración y los comandos show.

## 4.1 Local Switching

Esto es mismo un ejemplo básico:

El router2, el router3, y router4 están conectados con un ASR 9000, que simula un LAN entre eso tres Routers.

Éstas son las configuraciones de la interfaz en eso 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
!
```

Los paquetes son recibidos por el router1 con la etiqueta 2 del dot1q y remitidos al otro Routers con la etiqueta 2. del dot1q.

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

1. Puesto que todos los AC están utilizando la etiqueta 2 del dot1q, usted puede guardarla en la trama y delantero la trama en la interfaz de egreso con la misma etiqueta del dot1q según lo recibido en la interfaz de ingreso. El comando **simétrico del estallido 1 de la etiqueta del ingreso de la reescritura** no se requiere.

2. Usted puede hacer estallar la etiqueta entrante 2 del dot1q en la dirección de ingreso y avanzar simétricamente la etiqueta 2 del dot1q en la dirección de salida. Mientras que esto no se requiere en este escenario básico, es una buena idea configurar el dominio de Bridge de este modo al principio porque proporciona más flexibilidad para el futuro. Aquí están dos ejemplos de los cambios que pudieron ocurrir después de la configuración inicial:

   - Si una interfaz BVI ruteada se introduce más adelante en el dominio de Bridge, los paquetes se deben procesar en el BVI sin las etiquetas. Vea la sección para los detalles.
   - Un nuevo AC, que utiliza una diversa etiqueta del dot1q, se agrega más adelante. La etiqueta 2 del dot1q sería hecha estallar en la dirección de ingreso, y la otra etiqueta del dot1q sería avanzada en la nueva interfaz en la dirección de salida y vice versa el .BVI

Haga estallar las etiquetas del dot1q en cada AC en el 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 bajo Grupo de Bridge. Si otros dominios de Bridge de este cliente son necesarios, pueden ser configurados bajo mismo Grupo de Bridge, customer1. Si los nuevos dominios de Bridge pertenecen a un diverso cliente, usted puede crear a un nuevo Grupo de Bridge. Estos ejemplos utilizan al cliente para agrupar los dominios de Bridge, pero los

dominios de Bridge se pueden agrupar por cualquier criterio.

Utilice el comando de la **ingeniería del dominio de Bridge del customer1 del Grupo de Bridge del funcionamiento l2vpn de la demostración** para visualizar la configuración del dominio de Bridge.

Utilice el comando del **customer1 del Grupo de Bridge del funcionamiento l2vpn de la demostración** para ver la configuración de todos los dominios de Bridge.

Utilice el comando de la **ingeniería del bd-nombre del dominio de Bridge de la demostración l2vpn** o el mostrar información del comando del **customer1 del grupo del dominio de Bridge de la demostración l2vpn** para sobre el dominio de Bridge.

```
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 del **det de la ingeniería del bd-nombre del customer1 del grupo del dominio de Bridge de la demostración l2vpn** si usted quiere marcar que los paquetes están recibidos y enviados encendido cada AC.

Agregue la palabra clave del *MAC address al* **comando bridge domain de la expedición de la demostración l2vpn** si usted quiere marcar el mac-address-table:

```
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
```

El aprendizaje de MAC es ejecutado en hardware por el linecards cada vez que una trama se recibe en el dominio de Bridge. Hay también un caché del software del mac-address-table, pero esta tabla del software no se puede poner al día continuamente para hacer juego las entradas del hardware. Cuando ingresan al **comando show** en el código reciente, intenta resincronizar la tabla del software con la tabla del hardware. Después de un máximo de 15 segundos, imprime al estado actual del mac-address-table del software, incluso si la resincronización no es completa (por ejemplo, si la tabla es grande). Utilice el **l2vpn resincronizan el** comando del **mac-address-table de la expedición** para resincronizar las tablas de software y del soporte físico 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 cuando el proceso resincronización es completo, así que es útil hacer el **monitor terminal** habilitar para ver el mensaje.

La columna de la edad de la RESYNC visualiza la última vez que el MAC address fue resincronizado de la tabla del hardware.

La palabra clave de la *ubicación* es la ubicación de un linecard entrante o saliente. Las direcciones MAC se intercambian entre el linecards en hardware, así que las direcciones MAC se deben saber en cada linecard donde hay un AC o un picovatio. La palabra clave del *detalle* pudo proporcionar una versión más actualizada de la tabla del 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 bajo cada AC.

La palabra clave del *hardware* sondea el mac-address-table del hardware directamente de los motores de reenvío del ingreso o de la salida:

```
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 lleno

Los ejemplos anteriores del Local Switching eran básicos porque solamente el Routers fue conectado con el dominio de Bridge. Una vez que usted comienza a conectar el Switches L2, sin embargo, usted puede ser que introduzca un loop y necesite el STP para romper el loop:

En esta topología, el router1, el router2, y el router3 cada uno se configuran con un dominio de Bridge con todas sus interfaces en el diagrama. Si router4 envía un broadcast, tal como un pedido ARP, al router1, el router1 lo inunda al router2 y al router3, el router2 lo inunda al router3, y el router3 lo inunda al router2. Esto da lugar a un loop y a una tormenta de broadcast.

Para romper el loop, utilice un STP. Hay tipos múltiples de STP, pero ofertas del Software Cisco IOS XR solamente una instrumentación total, el MST.

Hay también versiones del gateway de acceso de los protocolos soportados en el Software Cisco IOS XR, tal como PVSTAG y MSTAG. Éstas son versiones estáticas, limitadas del protocolo utilizar en las topologías específicas, típicamente con los VPL, y se describen en las secciones MSTAG y PVSTAG. En el Software Cisco IOS XR, el MST es la única opción si hay una topología con los switches múltiples y si el atravesar completo - se requiere la implementación del árbol.

Dos subinterfaces se configuran en cada router y se agregan a un dominio de Bridge. Para el router1, 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
!
!
```

```
!
!
```
El MST se configura en la interfaz principal. En este ejemplo, el VLAN2 se asigna para citar como ejemplo 1, y el resto de los VLA N siguen siendo el caso predeterminado 0. (A más configuración realística partiría los VLA N uniformemente entre los casos.)

La selección del Root Bridge dentro de una red STP es determinada por la prioridad configurada y el Bridge ID integrado de cada dispositivo. El dispositivo con la prioridad más baja, o con la prioridad más baja igual pero el Bridge ID más bajo, se selecciona como el Root Bridge. En este ejemplo, el router3 se configura con un router1 por ejemplo 0 de la prioridad baja entonces, así que el router3 es la raíz por ejemplo que 0. router1 tienen un router3 por ejemplo 1 de la prioridad baja entonces, así que el router1 es la raíz por ejemplo 1.

Ésta 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
!
!
```
Ésta es la configuración en el router3:

```
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 el mapeo de VLAN a instancia deben ser lo mismo en todo el Switches.

Ahora, marque atravesar - estatus del árbol 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 por ejemplo 0, así que el router1 tiene su puerto raíz en Gi0/0/0/1 hacia el router3. El router1 es la raíz por ejemplo 1, así que el router1 es el Bridge designado en todas las interfaces para ese caso.

El router2 se bloquea 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 remitiendo mientras que se bloquea Te0/1/0/0.3. Cuando el valor bloqueado STP es 0x0, la condición es falsa, así que la interfaz está remitiendo; cuando el valor bloqueado STP es 0x1, la condición es verdad, así que se bloquea la interfaz.

Utilice el **comando data del uidb de la demostración** para confirmar esto y visualizar 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 ese dominio L2, conecte al Routers L3 que rutea entre los host dentro del dominio de Bridge y el mundo exterior. En el

diagrama anterior, host1 podía utilizar router4 o router5 para salir la subred local y alcanzar Internet.

El router1 y el router2 donde se configuran los dominios de Bridge son los 9000 Router ASR, que pueden rutear el tráfico del IPv4 y del IPv6. Este dos Routers podría tomar tan el dominio de Bridge de los del tráfico IP y rutearlo a Internet ellos mismos, en vez de la confianza en el Routers L3. Para hacer esto, usted necesita configurar un BVI, que es una interfaz L3 que conecta en los paquetes de Routes de un dominio de Bridge para dentro y fuera del dominio de Bridge.

Éste es cómo parece lógicamente:

Ésta 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
!
```

Un BVI es una interfaz untagged L3, así que si usted quiere tener el proceso BVI los paquetes recibidos en los AC del dominio de Bridge, los AC se deben configurar para hacer estallar todas las etiquetas entrantes. Si no, el BVI no puede entender la etiqueta y cae los paquetes. No hay manera de configurar una subinterfaz del dot1q en un BVI, así que las etiquetas deben ser ingreso hecho estallar en los AC como fue hecho en Gi0/0/0/1.2 en el ejemplo anterior.

Puesto que una interfaz BVI es una interfaz virtual, hay algunas restricciones en las características que pueden ser habilitadas. Estas restricciones se documentan en configurar los Ruteo y Bridging integrados en el 9000 Series Router de Cisco ASR: Restricciones para configurar el IRB. Estas características no se soportan en las interfaces BVI en el ASR 9000:

- Listas de control de acceso (ACL). Sin embargo, el L2 ACL se puede configurar en cada puerto L2 del dominio de Bridge.
- Fast ReRoute IP (FRR)
- Netflow
- MoFRR (el Multicast solamente rápido reencamina)
- Switching por etiquetas MPLS
- mVPNv4
- Calidad del servicio (QoS)
- Imagen réplica del tráfico
- Interfaz sin numerar para el BVI
- Supervisión video (Vidmon)

El BVI puede estar en una configuración del ruteo virtual y de la expedición (VRF), para remitir el tráfico recibido en el BVI sobre el MPLS, pero el por-*VRF escritura de la etiqueta-asignación-MODE* debe ser utilizado.

Si una de estas características restrictas se requiere, usted no puede utilizar un BVI. Otra solución es utilizar un cable de External Loopback entre dos puertos en el router, donde está un puerto en el dominio de Bridge y un puerto se configura como interfaz ruteada normal donde todas las características pueden ser configuradas.

## 4.4 VPL

### 4.4.1 Descripción

Los VPL proporcionan la capacidad de combinar los dominios de Bridge en los sitios múltiples en un dominio de Bridge grande con MPLS PWs. Los host en los diversos sitios aparecen ser conectados directamente con el mismo segmento L2 porque su tráfico transparente se encapsula sobre la interconexión total de MPLS PWs entre L2VPN PE:

Una interconexión total de PWs se requiere para asegurarse de que cada host pueda recibir el tráfico del resto de los host. La consecuencia es que un L2VPN PE no remite una trama recibida en VPL picovatio sobre sus otros VPL PWs. Debe haber una interconexión total de PWs, así que cada PE recibe el tráfico directamente y no necesita remitir el tráfico entre PWs puesto que el envío causaría un loop. Esto se llama la regla de división del horizonte.

El router es aprendizaje de MAC corriente. Una vez que una dirección MAC está presente en el mac-address-table, usted remite solamente la trama para esa dirección MAC del destino sobre el picovatio al L2VPN PE del donde esta dirección MAC se ha aprendido. Esto evita la duplicación innecesaria del tráfico en la base. Los broadcasts y los Multicast se inundan sobre todo el PWs para asegurarse de que todos los host pueden recibirlos. Una característica tal como IGMP Snooping es útil porque permite que las tramas de multidifusión sean enviadas a los PE solamente donde hay receptores o routeres de multidifusión. Esto reduce la cantidad de tráfico en la base, aunque todavía haya copias múltiples de los mismos paquetes que se deben enviar a cada PE cuando hay interés para ese grupo.

La interconexión total de PWs se debe configurar bajo caso 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
!
!
!
!
!
```

El PWs configurado bajo el VFI es los que se enredan completamente en la base. Son parte del mismo grupo del horizonte de la fractura (SHG) para aseegurarse que las tramas recibidas en un picovatio no están remitidas a otro picovatio.

Es posible configurar el acceso PWs, que se consideran un tipo de AC y no se configuran bajo el VFI. Vea la sección para los detalles.

La configuración en el router2, el router3, y router4 es muy similar, y todo tienen el otro 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 escritura de la etiqueta local para el picovatio a 10.0.0.12 es 16049, así que significa que las tramas Ethernet están recibidas con la escritura de la etiqueta 16049. La decisión de Switching se basa en esta escritura de la etiqueta MPLS porque el penúltimo salto MPLS debe haber hecho estallar la escritura de la etiqueta IGP. Pudo todavía haber Etiqueta NULL explícita, pero la decisión de Switching se basa en la escritura de la etiqueta picovatio:

```
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
```

Los mpls de la demostración que remiten el comando de las escrituras de la etiqueta para la escritura de la etiqueta dan el número del dominio de Bridge, que usted puede utilizar para encontrar la dirección MAC de destino y el picovatio (vecino y picovatio-identificación) donde el paquete fue recibido. Usted puede entonces crear las entradas en el mac-address-table que señalan en 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
```

### Tipos 4.4.2 picovatios y etiquetas transportadas

Los VPL PWs se negocian como tipo 5 (los Ethernetes) PWs por abandono. Sea cual sea entra en el AC después de cualquier manipulación de la etiqueta del VLA N (cuando se configura el comando de la reescritura) se envía sobre el picovatio.

La versión 4.1.0 del Software Cisco IOS XR para la señalización LDP y la versión 4.3.1 con el BGP le dejaron configurar una picovatio-clase bajo un vecino y configurar el passthrough vlan del modo de transporte bajo picovatio-clase. Esto negocia una conexión virtual (VC) - el tipo 4 (las redes Ethernet VLAN) picovatio, que transporta sea cual sea sale del AC después de la manipulación de la etiqueta del VLA N cuando se configura el comando de la reescritura.

La manipulación de la etiqueta del VLA N en el EFP se asegura de que haya por lo menos una etiqueta del VLA N dejada en la trama porque usted necesita una etiqueta del dot1q en la trama si hay VC-tipo 4 PWs. No se agrega ninguna etiqueta simulada 0 a la trama cuando usted utiliza al **modo de paso a través directo vlan del modo de transporte**.

Una mezcla del tipo 4 y del tipo 5 PWs bajo el mismo VFI no se soporta. Todo el PWs debe 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 Autodetección y señalización

Fueron basados en la configuración manual de todos los vecinos bajo el VFI. El MPLS LDP fue utilizado para la señalización del picovatio con los ejemplos neighbor.previous

Cuando usted agrega nuevos VPL PE a la red, configure el PE para tener un picovatio a todos los PE existentes en cada uno de sus dominios de Bridge locales. Todos los PE existentes se deben entonces configurar de nuevo para tener un picovatio al nuevo PE porque todos los PE deben ser enredados completamente. Esto pudo convertirse en un desafío operativo mientras que el número de PE y los dominios de Bridge aumentan.

Una solución es hacer que los PE descubran otros PE automáticamente con el BGP. Mientras que hay también un requisito del full-mesh para el IBGP, puede ser levantado por el uso de los reflectores de ruta. Así pues, un nuevo PE se configura típicamente para mirar con una pequeña cantidad de reflectores de ruta, el resto de los PE reciben sus actualizaciones, y el nuevo PE

recibe las actualizaciones de los otros PE.

Para descubrir otros PE con el BGP, cada PE se configura para la direccionamiento-*familia VPL-vpws* y hace publicidad en el BGP de los dominios de Bridge en los cuales quieren participar. Una vez que se descubren los otros PE que son parte del mismo dominio de Bridge, un picovatio se establece a cada uno de ellos. El BGP es el protocolo usado para este autodetección.

Hay dos opciones para la señalización del picovatio a los PE descubierto automáticamente: BGP y LDP. En estos ejemplos, usted convierte la topología anterior al autodetección BGP con la señalización BGP y la señalización LDP.

#### Autodetección de 4.4.3.1 BGP y señalización BGP

Configure a la direccionamiento-**familia l2vpn los VPL-vpws** bajo el BGP del router 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 direccionamiento-familia hace activa con los vecinos, pero ningún PE todavía ha hecho publicidad de su participación en un dominio de Bridge:

```
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 el **BGP del autodetección** y el **BGP del Signaling Protocol** bajo modo de configuración del dominio de Bridge L2VPN. 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
!
!
!
```

```
!
!
!
```

La vpn-identificación y la ruta-blanco son lo mismo en los diversos PE para cada dominio de Bridge, pero cada PE tiene un identificador virtual único del borde (VE-ID). Cada PE descubre los otros PE en el VPN con el BGP y utiliza el BGP para señalar el PWs. El resultado es una interconexión total de PWs:

```
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 des divulgación por el router3 (10.0.0.13) según lo visto en el router1; los prefijos se reciben con 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 algún PWs:

```
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
```

#### Autodetección de 4.4.3.2 BGP y señalización LDP

La configuración BGP con el comando de la direccionamiento-**familia l2vpn VPL-vpws** es exactamente lo mismo que con la señalización BGP. La configuración L2VPN se modifica para utilizar la señalización LDP con el comando del **ldp del Signaling Protocol**.

La misma configuración se utiliza 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
!
!
!
!
!
!
```

La vpl-identificación se hace del número de Sistema autónomo (AS) BGP y de la VPN-identificación.

Tres comandos show del router1 ilustran que el PWs se ha establecido con los PE descubiertos:

```
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 Rubores y retiros MAC

La expedición en los VPL se basa en el mac-address-table, que es construida dinámicamente aprendiendo los MAC Address de origen de los bastidores que son recibidos. Si hay un cambio de la topología en un dominio de Bridge, un host pudo llegar a ser accesible con un diverso AC o los VPL vecinos. Trafique para ese host no pudo alcanzar su destino si las tramas continúan siendo remitidas según el mac-address-table existente.

Para un L2VPN PE, hay diferentes formas de detectar un cambio de la topología:

- Un puerto en el dominio de Bridge va hacia arriba o hacia abajo.
- Se procesa una notificación cambia la topología del árbol de expansión (TCN) BPDU cuando el L2VPN PE ejecuta la implementación completa MST o atravesar - protocolo del gateway de acceso del árbol. El link que fallaba no pudo ser local en el PE sino pudo estar más lejos ausente en la topología. El PE intercepta el TCN.

Cuando un L2VPN PE detecta un cambio de la topología, toma dos medidas:

1. El PE vacia el mac-address-table de los dominios de Bridge afectados por el cambio de la topología. Cuando el PE se configura para el gateway de acceso rápido del Spanning-tree PVSTAG o del por el VLAN (PVRSTAG), un TCN BPDU detectado en una subinterfaz del VLAN afecta a todos los VLA N y dominios de Bridge en esa interfaz física.
2. El PE señala a los vecinos VPL a través de un mensaje del retiro MPLS LDP MAC que deben vaciar su mac-address-table. Todo el telecontrol L2VPN PE que recibe el mensaje del retiro LDP MAC vacia sus tablas de direcciones MAC, y el tráfico se inunda otra vez. Se reconstruyen las tablas de direcciones MAC basaron en la nueva topología.

El comportamiento predeterminado del mensaje del retiro MAC en caso de la inestabilidad del puerto ha cambiado en un cierto plazo:

- Tradicionalmente en el Software Cisco IOS XR, un L2VPN PE envió los mensajes del retiro MAC cuando iba un AC abajo. El intento era hacer que el telecontrol PE vacie sus tablas de la dirección MAC para el dominio de Bridge afectado de modo que las direcciones MAC que señalan detrás del puerto tragado fueran doctas de otro puerto.
- Sin embargo, esto creó los problemas de interoperabilidad con un poco de telecontrol PE que sigue el RFC 4762 y purga las direcciones MAC que señalan en todos los PE excepto el que está enviando el mensaje del retiro MAC. El RFC 4762 asume que un PE enviaría un mensaje del retiro MAC cuando sube un AC pero no cuando va un AC abajo. Después de que la versión 4.2.1 del Software Cisco IOS XR, el comportamiento predeterminado sea enviar los mensajes del retiro LDP MAC solamente cuando un puerto del dominio de Bridge sube para cumplir mejor con el RFC. Agregaron a un comando configuration para invertir al viejo comportamiento.

Esto es comando show con el comportamiento predeterminado después de que 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 el “MAC retira abajo encendido enviado el puerto de Bridge,” que ahora se inhabilita por abandono después de que la versión 4.2.1 del Software Cisco IOS XR. El comando también da el número de mensajes del retiro MAC enviados y recibidos en el dominio de Bridge. Un número alto de mensajes del retiro indica la inestabilidad en el dominio de Bridge.

Ésta es la configuración que invierte al viejo comportamiento:

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

### 4.4.5 H-VPLS

Los VPL requieren una interconexión total de PWs entre L2VPN PE para asegurarse de que cualquier PE pueda alcanzar, en un salto, un host detrás de cualquier otro PE sin la necesidad de un PE de reflejar las tramas a partir de un picovatio a otro picovatio. Ésta es la base para la regla de división del horizonte, que previene un PE de las tramas de la expedición a partir de un picovatio a otro picovatio. Incluso en los casos especiales, adonde la dirección MAC del destino en el mac-address-table señala en otro picovatio, se cae la trama.

Una interconexión total de PWs significa que el número de PWs pudo llegar a ser muy tan alto que el número de PE crece, así que éste pudo introducir los problemas de ampliación.

Usted puede disminuir el número de PWs en esta topología con una jerarquía de los PE:

En esta topología, observe eso:

- Un dispositivo del borde del proveedor del usuario (U-PE) tiene AC a los CE.
- El dispositivo U-PE transporta el tráfico CE sobre un Punto a punto picovatio MPLS a un dispositivo del borde del proveedor de la red (N-PE).
- El N-PE es una base VPL PE que se enreda completamente con otros N-PE.
- En el N-PE, el picovatio que viene del U-PE se considera un acceso picovatio como un AC. El U-PE no es parte de la malla con los otros N-PE, así que el N-PE puede considerar el acceso

picovatio como AC y el tráfico delantero de ese acceso picovatio a la base PWs que es parte de la interconexión total VPL.
- La base PWs entre los N-PE se configura bajo un VFI para asegurarse de que la regla de división del horizonte está aplicada a toda la base PWs configurado bajo el VFI.
- El acceso PWs de los U-PE no se configura bajo un VFI, así que no pertenecen al mismo SHG que el VFI PWs. El tráfico se puede remitir de un acceso picovatio a un VFI picovatio y vice versa.
- Los U-PE pueden utilizar la función de redundancia picovatio para tener un picovatio primario a un N-PE primario y tener un picovatio espera a un N-PE espera. El recurso seguro asume el control cuando va el picovatio primario abajo.

Esto es un ejemplo donde U-PE1 (10.0.0.15) se configura con la Redundancia picovatio a N-PE1 (10.0.0.11) y a 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 picovatio a 10.0.0.12 está en el estado espera. En N-PE1, hay un acceso picovatio a 10.0.0.15 y un AC que no están bajo el VFI.

N-PE1 está aprendiendo algunas direcciones MAC sobre el acceso picovatio y el VFI PWs:

```
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 acceso picovatio está en el estado 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 partidos del horizonte (SHGs)

La regla de división del horizonte dicta que una trama recibida en un VFI picovatio no se puede remitir sobre otro VFI picovatio. VFI N-PE debe ser enredado completamente.

Este horizonte de la fractura se aplica con un SHG:

- Los miembros a partir de un SHG no pueden remitir las tramas el uno al otro, sino pueden remitir las tramas a los miembros del otro SHGs.
- Todos los VFI PWs se asignan a SHG 1 por abandono. Esto se asegura de que no haya expedición entre VFI PWs para aplicar la regla de división del horizonte. Los paquetes recibidos en un VFI picovatio se pueden remitir a AC y al acceso PWs porque no son parte del mismo SHG.
- Todos los AC y acceso PWs no son parte de al grupo SHG por abandono, así que significa que los paquetes recibidos en un AC o un acceso picovatio se pueden remitir a otro AC o acceso picovatio en el mismo dominio de Bridge.
- Los AC y el acceso PWs se pueden asignar al SHG 2 con el **comando group del horizonte partido** si la meta es evitar el envío entre él.

```
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 expedición entre el soldado enrollado en el ejército 0/0/0/1.2 y el soldado enrollado en el ejército 0/1/0/3.2, el soldado enrollado en el ejército 0/0/0/1.2 y 10.0.0.15, o el soldado enrollado en el ejército 0/1/0/3.2 y 10.0.0.15. Pero puede todavía haber reenvío de tráfico entre los AC y el VFI PWs porque son parte de diverso SHGs (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 por introducir la Redundancia, usted puede ser que tenga un sitio que es dual asociado a los VPL el dominio:

Si un host conectado con switch1 envía un broadcast, switch1 adelante él al router1 y a switch2. El router1 tiene una interconexión total de PWs, tan hay un picovatio al router2, y router1 adelante el broadcast sobre ese picovatio. Router2 adelante el broadcast a switch2, que adelante él a switch1. Esto da lugar a un loop físico.

#### Spanning-tree de 4.4.7.1

La implementación completa MST no trabaja con los VPL porque esa implementación envía MST BPDU en una interfaz principal para controlar al estado de reenvío de todos los VLA N en esa interfaz. Con los VPL, hay VFIs para cada dominio de Bridge, así que usted no puede enviar los BPDU en una interfaz principal para todos los esos VFIs.

El Spanning-tree BPDU se transporta sobre los VPL y PWs de punto a punto por abandono.

Si switch1 y switch2 están enviando el por el VLAN BPDU o MST untagged BPDU y si los BPDU hacen juego las subinterfaces l2transport en el router1 y el router2, los BPDU se transportan con los VPL. El Switches considera los BPDU de cada uno en las interfaces del soldado enrollado en el ejército 0/1, y atravesar - el árbol rompe el loop y bloquea un puerto.

El Switch2 es la raíz para el VLAN2:

```
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 el soldado enrollado en el ejército 0/1 y está bloqueando el soldado enrollado en el ejército 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 los BPDU también están transportados a los sitios remotos, y atravesando - la inestabilidad del árbol en un sitio propaga a todos los sitios conectados con el dominio VPL. Es más seguro aislar cada sitio y no transportar los BPDU sobre los VPL.

Una solución es uso de una versión del gateway de acceso del STP. Ésta es una aplicación limitada del protocolo, donde el L2VPN PE se configura para enviar algunos BPDU estáticos para aparecer conectado con la raíz del árbol de expansión. El L2VPN PE no transporta los BPDU recibidos de los CE a los sitios remotos, así que cada sitio tiene su propio atravesar - dominio del árbol.

#### 4.4.7.2 MSTAG

Como se explica en la sección del Spanning-tree, el MST envía el control BPDU untagged, pero estos BPDU el estado de reenvío de todos los VLA N en la interfaz.

Los VLA N se pueden agrupar en las instancias múltiples, y cada caso tiene su propio estado de reenvío.

Los VLA N se agrupan generalmente para poder separarse el tráfico uniformemente entre los trayectos múltiples. Cuando hay dos trayectorias, la mitad del tráfico pertenece a un caso que esté remitiendo en la primera trayectoria y esté bloqueando en la segunda trayectoria. La otra mitad del tráfico pertenece a un caso que esté bloqueando en la primera trayectoria y esté

remitiendo en la segunda trayectoria. Esto permite loadbalancing entre las dos trayectorias bajo condiciones estables. Si no, usted tiene una trayectoria que ordinariamente se bloquee y llegue a ser totalmente activa solamente cuando el trayecto principal está abajo.

Aquí está una topología típica MSTAG:

En este ejemplo del laboratorio, el caso 1 tiene VLAN2, y el caso 0 tiene los otros VLA N. (En un más escenario realista, los VLA N se separan entre la instancia múltiple para alcanzar el buen tráfico loadbalancing entre los casos.) Porque algunos VLA N tienen mucho más tráfico que otros, no hay siempre el mismo número de VLA N en cada caso.

Ésta es la configuración para el caso 0 MST:

- El router1 y el router2 están enviando algunos BPDU estáticos basados en la configuración MSTAG. No están procesando los BPDU entrantes de la red ni están intentando funcionar con una instrumentación total. Con MSTAG, los dos L2VPN PE apenas envían los BPDU estáticos basados en su configuración MSTAG.
- El router1 es configurado para atraer el tráfico del caso 0 apareciendo ser la raíz para ese caso.
- El router2 se configura con la prioridad raíz por ejemplo 0 del segundo mejor, de modo que se convierta en la nueva raíz en caso del error del router1 o del error AC entre switch1 y el router1.
- El Switch2 se configura con un alto que atraviesa - coste del árbol en el soldado enrollado en el ejército 0/1 del puerto al router2 para asegurarse de que su trayecto principal a la raíz está en el carruaje 0/2 switch1 directo y el router1.
- El Switch2 selecciona el soldado enrollado en el ejército 0/2 como puerto raíz para instance0 y selecciona el soldado enrollado en el ejército 0/1 como puerto alternativo en caso de que se pierda la raíz.
- Así, el tráfico de ese sitio en los VLA N que pertenecen para citar como ejemplo 0 alcanza otros sitios sobre los VPL con el router1.

Para el caso 1 MST (se invierte el VLA N 2), la configuración:

- El router2 es configurado para atraer el tráfico del caso 1 apareciendo ser la raíz para ese caso.
- El router1 se configura con la prioridad raíz por ejemplo 1 del segundo mejor, de modo que se convierta en la nueva raíz en caso del error del router2 o del error AC entre switch2 y el router2.
- El Switch1 se configura con un alto que atraviesa - coste del árbol en el soldado enrollado en el ejército 0/1 del puerto al router1 para asegurarse de que su trayecto principal a la raíz está en el carruaje 0/2 switch2 directo y el router2.
- El Switch1 selecciona el soldado enrollado en el ejército 0/2 como puerto raíz por ejemplo 1 y selecciona el soldado enrollado en el ejército 0/1 como puerto alternativo en caso de que se pierda la raíz.
- Así, el tráfico de ese sitio en los VLA N que pertenecen para citar como ejemplo 1 (VLAN2 en este ejemplo) alcanza otros sitios sobre los VPL con el router2.
- Debe haber una subinterfaz en el router1 y el router2 para coger los TCN untagged y remitirlos a través de un Punto a punto picovatio al otro router. Porque switch1 y switch2 podrían perder sus links directos y convertirse aisló de uno a, el router1 y el router2 deben

remitir los TCN entre ellos a través de ese Punto a punto picovatio.

- Los PE también interceptan los TCN, vacian sus tablas de direcciones MAC, y envían el retiro LDP MAC al telecontrol PE.

Ésta 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, observe eso:

- En el caso 0 MST, el Root Bridge es 0000.0000.0001, que es el Bridge ID del router1.
- En el caso 1 MST, el Root Bridge es 0000.0000.0002, que es el Bridge ID del router2.
- La prioridad de Bridge del router1 es 4096 en el caso 0 (hacer la raíz) y 8192 en el caso 1 (hacer la raíz del segundo mejor).
- La prioridad de Bridge del router1 es 8192 en el caso 0 (hacer la raíz del segundo mejor) y 4096 en el caso 1 (hacer la raíz).
- El Cross Connect de punto a punto en GigabitEthernet0/1/0/3.1 lleva el MST untagged TCN al otro router.

Una salida ACL se ha configurado en las subinterfaces del dot1q para caer el por el VLAN BPDU que se pudo enviar por otro sitio que no se ha emigrado al MST todavía. Esta configuración evita que el Switch CE declare que la interfaz como contrario cuando recibe un por el VLAN BPDU en una interfaz configurada para el 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
```

Ésta 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
```

Así, el tráfico en el caso 0 se remite con el router1 y el tráfico en el caso 1 se remite con switch2 y el router2.

La configuración en switch2 utiliza los mismos comandos que 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 con switch1 y el router1 para instance0 y con el router2 para instance1.

El tráfico loadbalanced porque un caso sale el sitio con el router1 y el otro caso sale el sitio con el router2.

Si el link entre el router1 y switch1 está abajo, ambos casos pasan con el 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 alcanzar en este tipo de error porque la trayectoria a través de la raíz del segundo mejor fue seleccionada ya como el trayecto alterno. Con MSTAG, el MST BPDU no se transporta sobre los VPL así que los sitios se aísla de la inestabilidad en otros sitios.

#### 4.4.7.3 PVSTAG o PVRSTAG

MSTAG es el protocolo preferido del gateway de acceso para los VPL porque utiliza el rapid que atraviesa - árbol y porque es scalable con su uso de los casos bastante que los BPDU en cada VLA N.

Si un sitio no se puede emigrar al MST y la única solución es guardar el ejecutar del PVST+ o de PVRST, usted puede utilizar PVSTAG o PVRSTAG, pero la implementación se limita a una topología específica:

En esta topología, la restricción más importante es que puede haber solamente un Switch CE. Usted no puede tener dos Switches como en la topología MSTAG. En MSTAG, usted puede configurar un Punto a punto picovatio para transportar el tráfico sin Tags (BPDU incluyendo TCN) a partir de un PE al otro cuando el sitio está partido en dos porciones. Con el PVST y PVRST, los TCN se envían marcados con etiqueta así que hacen juego la misma subinterfaz que el tráfico de datos que se transportará sobre los VPL. El router tendría que identificar los BPDU basados en la dirección MAC y el Tipo de protocolo para remitir los TCN al otro lado. Porque esto no se soporta, hay actualmente un requisito de tener solamente un dispositivo CE.

Otro requisito en las versiones que la versión 4.3.0 del Software Cisco IOS XR es anterior que las interfaces del conjunto no se pueden utilizar como AC. Esta restricción se ha suprimido en la versión 4.3.0 del Software Cisco IOS XR.

El principio es mucho el lo mismo que con MSTAG. El router PVSTAG envía los BPDU estáticos de modo que el CE aparezca ser conectado con el Switches que está conectado directamente con la raíz (virtual) con un loadbalance del coste 0. para el tráfico, algunos VLA N se pueda configurar con la raíz en el router3 y otros con la raíz en router4.

Esto es un ejemplo de configuración en el router3:

```
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
```

Esto es un ejemplo de configuración en 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
```

Esto es un ejemplo de configuración en el CE switch3:

```
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 para PVSTAG es muy similar a MSTAG salvo que la prioridad raíz y la prioridad del gateway principal se configuran mientras que 4096 y la prioridad del gateway de backup se configura como 8192 en el ejemplo MSTAG.

El resto del Switches en los dominios debe tener prioridades más arriba que las que está configuradas en PVSTAG o PVRSTAG.

Usted puede ajustar el coste de la interfaz en el Switches CE para influenciar que el puerto se convierte en el puerto raíz y que se bloquea el puerto.

#### 4.4.7.4 MC-LAG

La configuración MC-LAG con los VPL es más simple que PWs de punto a punto con la Redundancia bidireccional picovatio. En vez de un picovatio primario y de tres PWs espera, los PE necesitan solamente una interconexión total de VPL PWs, que es estándar con los VPL:

En esta topología, observe eso:

- MC-LAG se ejecuta entre los dos VPL PE a la izquierda: router2 y router4.
- En condiciones normales, los miembros del agrupamiento son activos entre el router1 y el router2 y en el estado espera entre el router1 y router4.
- El router2 tiene las subinterfaces del conjunto configuradas bajo dominios de Bridge VPL, tan router2 adelante el tráfico al telecontrol VPL PE. Hay dos sitios ilustrados en el Diagrama de topología pero podría haber mucho más.
- El telecontrol PE aprende las direcciones MAC del router1 y los dispositivos detrás con el router2, así que los PE remiten el tráfico para estos direccionamientos del MAC de destino con el router2.
- Cuando va el link entre el router1 y el router2 abajo o cuando va el router2 abajo, los miembros del agrupamiento entre el router1 y router4 van active.
- Como el router2, router4 tiene sus subinterfaces del conjunto configuradas bajo dominios de Bridge VPL.
- Cuando las subinterfaces del conjunto suben en router4, router4 envía los mensajes del retiro LDP MAC al telecontrol VPL PE para dejarlos saber que hay un cambio de la topología.

Ésta es la configuración en el router3:

```
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 que configuran al conjunto MC-LAG, agreguela bajo configuración VPL como cualquier otro AC.

Ésta es la configuración correspondiente en 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, los miembros del agrupamiento entre el router3 y router6 es activos, y el miembro entre router5 y router6 está en el estado 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 router3 y se remite al telecontrol PE:

```
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 comando más reciente ilustra que el router3 está aprendiendo que algunas direcciones MAC en su conjunto y los miembros activos están en el router3. En router5, no hay dirección MAC aprendida sobre el conjunto pues el miembro local está en el estado 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 van los miembros del agrupamiento entre el router3 y router6 abajo, los miembros del agrupamiento hacen activos en router5. Los MC-LAG VPL PE envían un mensaje del retiro LDP MAC de modo que el telecontrol PE purgue sus tablas de direcciones MAC y aprenda la dirección MAC a través del nuevo active MC-LAG PE router5.

El router2 recibe los mensajes de un retiro MAC del router3 y de router5 cuando los miembros del agrupamiento activos MC-LAG se trasladan desde el router3 a 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 router2 se mueven desde el router3 (10.0.0.13) a router5 (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 a un solo conjunto que se asociará a los otros sitios con los VPL. MC-LAG proporciona el link y la Redundancia PE, pero sigue siendo lógicamente un bundle interface para alcanzar otros sitios. El Spanning-tree no se requiere en ese conjunto, y un filtro BPDU se podría configurar en el CE para asegurarse de que los BPDU no están intercambiados entre los sitios sobre los VPL.

Otra opción es configuración de una lista de acceso de los servicios Ethernet en los AC en el conjunto para caer los direccionamientos del MAC de destino de los BPDU así que los BPDU no se transportan entre los sitios. Sin embargo, si un link trasero se introduce entre los sitios, atravesando - el árbol no puede romper el loop porque no se está ejecutando en el conjunto MC-LAG. Así pues, evalúe cuidadosamente si inhabilitar atravesar - árbol en el conjunto MC-LAG. Si la topología entre los sitios se mantiene cuidadosamente, es agradable tener Redundancia con MC-LAG sin la necesidad de atravesar - árbol.

### Cluster del borde de 4.4.7.5 ASR 9000 nanovoltio

La solución MC-LAG proporcionó a la Redundancia sin la necesidad de utilizar atravesar - árbol. Una desventaja es que los miembros del agrupamiento a un MC-LAG PE están en el estado espera, así que es una solución activo-espera que no maximiza el uso del link.

Otra opción del diseño es uso de un cluster del borde ASR 9000 nanovoltio de modo que los CE puedan tener los miembros del agrupamiento a cada estante del cluster que son todos activos al mismo tiempo:

Otra ventaja de esta solución es que el número de PWs está reducido porque hay solamente un picovatio por el cluster para cada uno de los clusteres en cada sitio. Cuando hay dos PE por el sitio, cada PE debe tener un picovatio a cada uno de los dos PE en cada sitio.

La simplicidad de la configuración es otra ventaja. La configuración parece una configuración muy básica VPL con un dominio de Bridge con el conjunto AC y VFI PWs:

```
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 es proporcionada por el conjunto AC dual-homed a los dos estantes de modo que el conjunto permanezca para arriba en caso del error de los miembros del agrupamiento o del error del estante.

Cuando un sitio se asocia al dominio VPL solamente a través de un cluster, la topología es similar

a MC-LAG en lo que respecta a atravesar - árbol. Tan atravesando - el árbol no se requiere en ese conjunto, y un filtro BPDU se podría configurar en el CE para asegurarse de que los BPDU no están intercambiados entre los sitios sobre los VPL.

Otra opción es configuración de una lista de acceso de los servicios Ethernet en los AC en el conjunto para caer los direccionamientos del MAC de destino de los BPDU así que los BPDU no se transportan entre los sitios. Sin embargo, si un link trasero se introduce entre los sitios, atravesando - el árbol no puede romper el loop porque no se está ejecutando en el conjunto CE-PE. Así pues, evalúe cuidadosamente si inhabilitar atravesar - árbol en ese conjunto CE-PE. Si la topología entre los sitios se mantiene cuidadosamente, es agradable tener Redundancia a través del cluster sin la necesidad de atravesar - árbol.

#### 4.4.7.6 ICCP-basó el multi-homing del servicio (ICCP-SM) (PMCLAG (pseudo MCLAG) y activo/el Active)

Hay una nueva función introducida en la versión 4.3.1 para superar la limitación de MC-LAG, donde están tan inusitados algunos links de agrupamientos que sigue habiendo en el modo de reserva. En la nueva función, llamada *Pseudo MCLAG*, todos los links del DHD a los puntos de acoplamiento (PoAs) son funcionando, pero los VLA N están partidos entre los diversos conjuntos:

## 4.5 Control de tormentas del tráfico

En un dominio de broadcast L2, hay el riesgo que un host pudo comportarse mal y enviar una alta velocidad de broadcast o de las tramas de multidifusión que se debe inundar por todas partes en el dominio de Bridge. Otro riesgo es creación de un loop L2 (que no está quebrado atravesando - árbol), que da lugar a la colocación de los broadcasts y de los paquetes de los Multicast. Una alta velocidad de los broadcasts y de los paquetes de los Multicast afecta el funcionamiento de los host en los dominios de broadcast.

El funcionamiento de los dispositivos de Switching en la red se pudo también afectar por la replicación de un bastidor entrado (broadcast, Multicast o una trama de la unidifusión desconocida) a los puertos de egreso múltiples en el dominio de Bridge. La creación de las copias múltiples del mismo paquete puede ser uso intensivo de recurso, dependiendo del lugar dentro del dispositivo en donde el paquete tiene que ser replicado. Por ejemplo, replicar un broadcast a diversos slots múltiples no es un problema debido a las capacidades de la replicación de multidifusión de la tela. El funcionamiento de un procesador de red pudo ser afectado cuando tiene que crear las copias múltiples del mismo paquete que se enviará en algunos puertos que el procesador de red esté manejando.

Para proteger los dispositivos en caso de una tormenta, la característica del control de tormentas del tráfico le deja configurar una velocidad máxima de los broadcasts, de Multicast y de las unidifusiones desconocidas que se validarán en un dominio de Bridge AC. Vea la guía de configuración de la seguridad del sistema del router de los servicios de la agregación de las 9000 Series de Cisco ASR, la versión 4.3.x: Implementar el control de tormentas del tráfico bajo un Bridge VPL para los detalles.

El control de tormentas del tráfico no se soporta en las interfaces o VFI PWs del conjunto un AC, sino se soporta en el NON-conjunto AC y el acceso PWs. La característica se inhabilita por abandono; a menos que usted configure el control de tormentas, usted valida cualquier índice de broadcasts, de Multicast, y de unidifusiones desconocidas.

Aquí está 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 del control de tormentas están siempre presentes en la salida del comando detail del dominio de Bridge de la demostración l2vpn. Porque la característica se inhabilita por abandono, los contadores comienzan a señalar los descensos solamente cuando se ha configurado la característica.

Las velocidades configuradas pudieron variar sobre el patrón de tráfico a partir de una red a otra red. Antes de configurar una tarifa, Cisco le recomienda entiende el índice de bastidores del broadcast, del Multicast o de la unidifusión desconocida en circunstancias normales. Entonces agregue un margen en la velocidad configurada sobre la tarifa normal.

## 4.6 El MAC se mueve

En caso de la inestabilidad de la red como un flap de la interfaz, una dirección MAC pudo ser docta de una nueva interfaz. Ésta es convergencia de la red normal, y el mac-address-table se pone al día dinámicamente.

Sin embargo, los movimientos constantes MAC indican a menudo la inestabilidad de la red, tal como inestabilidad severa durante un loop L2. La función de seguridad del MAC address le deja señalar los movimientos MAC y tomar las acciones correctivas tales como apagar un puerto que ofende.

Incluso si una acción correctiva no se configura, usted puede configurar el comando logging así que le alertan de la inestabilidad de la red a través de los mensajes del movimiento MAC:

```
l2vpn
bridge group customer1
```

```
bridge-domain engineering
mac
secure
action none
logging
!
!
```

En este ejemplo, la acción se configura a ningunos, así que no se hace nada cuando se detecta un movimiento MAC salvo que se registra un mensaje de Syslog. Esto 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 IGMP y MLD snooping

Por abandono, las tramas de multidifusión se inundan a todos los puertos en un dominio de Bridge. Cuando usted está utilizando la alta velocidad fluye como los servicios de la televisión IP (IPTV), pudo haber una cantidad significativa de tráfico remitida en todos los puertos y replicada sobre PWs múltiple. Si todas las secuencias TV se remiten sobre una interfaz, ésta pudo congestionar los puertos. La única opción es configuración de una característica tal como IGMP o MLD snooping, que intercepta los paquetes de control de multidifusión para seguir a los receptores y los routeres de multidifusión y las secuencias delanteras en los puertos solamente cuando es apropiado.

Vea la guía de configuración del Multicast del router de los servicios de la agregación de las 9000 Series de Cisco ASR, la versión 4.3.x para más información sobre estas características.

## 5. Temas adicionales L2VPN

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

### 5.1 Loadbalancing

Cuando un L2VPN PE necesita enviar una trama sobre un MPLS picovatio, la trama Ethernet se encapsula en una trama MPLS con una o más escrituras de la etiqueta MPLS; hay por lo menos una escritura de la etiqueta picovatio y quizás una escritura de la etiqueta IGP para alcanzar el telecontrol PE.

La trama MPLS es transportada por la red MPLS al telecontrol L2VPN PE. Hay típicamente trayectos múltiples para alcanzar el destino PE:

Nota: No todos los links se representan en este diagrama.

El PE1 puede elegir entre el P1 y el P2 como el primer router MPLS P hacia el PE2. Si se selecciona el P1, el PE1 después elige entre el p3 y el P4, y así sucesivamente. Los trayectos disponibles se basan en la topología IGP y la trayectoria del túnel del MPLS TE.

Los proveedores de servicio MPLS prefieren tener todos los links utilizados igualmente bastante que un link congestionado con otros links inutilizados. Esta meta no es siempre fácil de alcanzar porque algún PWs lleva mucho más tráfico que otros y porque la trayectoria tomada por un tráfico picovatio depende del algoritmo de troceo usado en la base. El ancho de banda alto múltiple PWs se pudo desmenuzar a los mismos links, que crea la congestión.

Un requisito muy importante es que todos los paquetes a partir de un flujo deben seguir la misma trayectoria. Si no, esto lleva a las tramas fuera de servicio, que pudieron afectar la calidad o el funcionamiento de las aplicaciones.

Loadbalancing en una red MPLS en los routeres Cisco se basa típicamente sobre los datos que siguen la escritura de la etiqueta de la parte inferior MPLS.

- Si los datos inmediatamente después de la etiqueta inferior comienzan con 0x4 o 0x6, un router MPLS P asume que hay un paquete del IPv4 o del IPv6 dentro del paquete MPLS e intenta al loadbalance basado en un hash de los direccionamientos de la fuente y del IPv4 o del IPv6 del destino extraídos de la trama. En la teoría, esto no debe aplicarse a una trama Ethernet que se encapsule y se transporte sobre un picovatio porque la dirección MAC del destino sigue la etiqueta inferior. Pero algunos rangos de MAC Addresses que comienzan con 0x4 y 0x6 se han asignado recientemente. El router MPLS P pudo considerar incorrectamente que el encabezado Ethernet es realmente una encabezado del IPv4 y desmenuzar la trama basada sobre lo que asume son las direcciones de origen y de destino del IPv4. Las tramas Ethernet de un picovatio se pudieron desmenuzar sobre diversas trayectorias en la base MPLS, que lleva al out-of-sequence las tramas en los problemas de calidad picovatio y de la aplicación. La solución es configuración de una control-palabra bajo picovatio-clase que se pueda asociar a un Punto a punto o a VPL picovatio. Se inserta la palabra de control inmediatamente después que las escrituras de la etiqueta MPLS. La palabra de control no comienza con 0x4 o 0x6 así 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 después que la parte inferior de la pila de etiquetas MPLS no comienza con 0x4 o 0x6, los loadbalances del router P basaron sobre la etiqueta inferior. Todo el tráfico a partir de un picovatio sigue la misma trayectoria, así que los paquetes defectuosos no ocurren, pero éste pudo llevar a la congestión en algunos links en caso del ancho de banda alto PWs. Con la versión 4.2.1 del Software Cisco IOS XR, el ASR 9000 soporta la característica enterada picovatio del transporte del flujo (FAT). Esta característica se ejecuta en el L2VPN PE, donde se negocia entre los dos finales de un Punto a punto o de VPL picovatio. El ingreso L2VPN PE detecta los flujos en el AC y la configuración L2VPN e inserta una nueva escritura de la etiqueta del flujo MPLS debajo de la escritura de la etiqueta picovatio MPLS en la parte inferior de la pila de etiquetas MPLS. El ingreso PE detecta los flujos basados sobre los MAC Address de origen y destino (valor por defecto) o los direccionamientos de la fuente y del IPv4 del destino (configurables). El uso de las direcciones MAC es el valor por defecto; el uso de los direccionamientos del IPv4 se recomienda, pero se debe configurar manualmente.

  Con la característica FAT picovatio, el ingreso L2VPN PE inserta una escritura de la etiqueta inferior MPLS por el Src-dst-mac o por el Src-dst-ip. El Routers MPLS P (entre los PE) desmenuza las tramas sobre los trayectos disponibles, después alcanza el destino PE basado en esa escritura de la etiqueta del flujo FAT picovatio en la parte inferior del stack MPLS. Esto proporciona generalmente un uso del ancho de banda mucho mejor en la base a menos que un picovatio lleve solamente una pequeña cantidad de Src-dst-mac o conversaciones del Src-dst-ip. Cisco recomienda que usted utiliza una palabra de control así que usted puede evitar tener direcciones MAC que comiencen con 0x4 y 0x6 inmediatamente después que la escritura de la etiqueta del flujo. Esto se asegura que el hash esté basado correctamente sobre los pseudo IP Addresses y que no basado en la escritura de la etiqueta del flujo.

  Con esta característica, el tráfico a partir de un picovatio loadbalanced sobre los trayectos

múltiples en la base cuando está disponible. El tráfico de aplicación no sufre de los paquetes defectuosos porque todo el tráfico de la misma fuente (MAC o IP) al mismo destino (MAC o IP) sigue la misma trayectoria.

Esto 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 Registración

Diversos tipos de mensajes de registración pueden ser configurados en el modo de configuración L2VPN. Configure la orden de apertura de sesión l2vpn para recibir las alertas del Syslog para los eventos L2VPN, y el pseudowire de registración de la configuración para determinar cuando los cambios de estado picovatio:

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

Si mucho se configura PWs, los mensajes pudieron inundar el registro.

## lista de acceso de 5.3 servicios Ethernet

Usted puede utilizar una lista de acceso de los servicios Ethernet para caer el tráfico de los host específicos o verificarlo si un router está consiguiendo los paquetes de un host en una interfaz l2transport:

```
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 del hardware se pueden considerar solamente con la palabra clave del *hardware*. Utilice la palabra clave del *ingreso* o de la *salida* dependiendo de la dirección del acceso-grupo. La ubicación del linecard de la interfaz donde está aplicada la lista de acceso también se especifica.

Usted puede también aplicar una lista de acceso ipv4 en una interfaz l2transport como una Seguridad o característica de Troubleshooting:

```
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)
```

## salida-filtro de 5.4 Ethernetes

En la dirección de salida de un AC, suponga que no hay comando **simétrico del <> del estallido de la etiqueta del ingreso de la reescritura** que determina las etiquetas del VLA N de la salida. En ese caso, no hay control para asegurarse de que la trama de salida tiene las etiquetas correctas del VLA N según el **comando encapsulation**.

Esto 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, observe eso:

- Un broadcast recibido con una etiqueta 2 del dot1q en GigabitEthernet0/1/0/39.2 guarda su etiqueta entrante porque no hay comando del **ingreso de la reescritura**.
- Ese broadcast se inunda fuera de GigabitEthernet0/1/0/3.2 con su etiqueta 2 del dot1q, pero ése no causa un problema porque GigabitEthernet0/1/0/3.2 también se configura con la etiqueta 2. del dot1q.
- Ese broadcast también se inunda fuera de GigabitEthernet0/1/0/3.3, que guarda su etiqueta original 2 porque no hay comando de la **reescritura** en GigabitEthernet0/1/0/3.3. No llegan al **comando 3 del dot1q de la encapsulación** en GigabitEthernet0/1/0/3.3 la dirección de salida.
- El resultado es que, porque uno transmitido recibido con la etiqueta 2 en GigabitEthernet0/1/0/39, allí es dos broadcasts con la salida de la etiqueta 2 de GigabitEthernet0/1/0/3. Que el tráfico duplicado pudo causar una cierta aplicación publica.
- La solución es configuración del salida-*filtro de los Ethernetes estricta* para asegurarse de que los paquetes dejan la subinterfaz con las etiquetas correctas del VLA N. Si no, los paquetes no se remiten y se caen.

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