Serviços e recursos de L2VPN IOS XR

Contents

Introduction

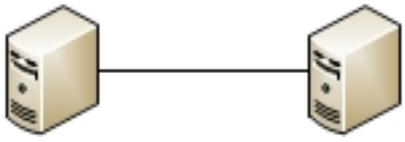
Este documento descreve as topologias VPN (L2VPN) básicas da camada 2 (L2). É útil apresentar exemplos básicos para demonstrar o projeto, os serviços, os recursos e a configuração. Consulte o Guia de Configuração de Serviços L2VPN e Ethernet do Roteador de Serviços de Agregação Cisco ASR 9000 Series, Versão 4.3.x para obter informações adicionais.

1. Serviços ponto a ponto e multiponto

O recurso L2VPN fornece a capacidade de fornecer serviços ponto-a-ponto e multiponto.

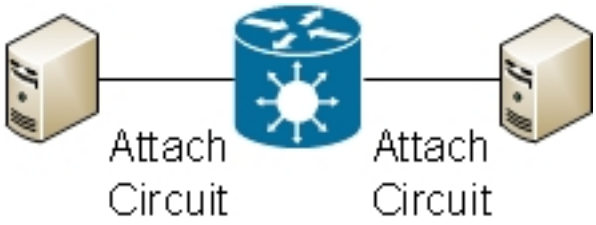
1.1 Serviço Point-to-Point

O serviço ponto-a-ponto basicamente emula um circuito de transporte entre dois nós finais para que os nós finais pareçam estar diretamente conectados em um link ponto-a-ponto. Isso pode ser usado para conectar dois sites.

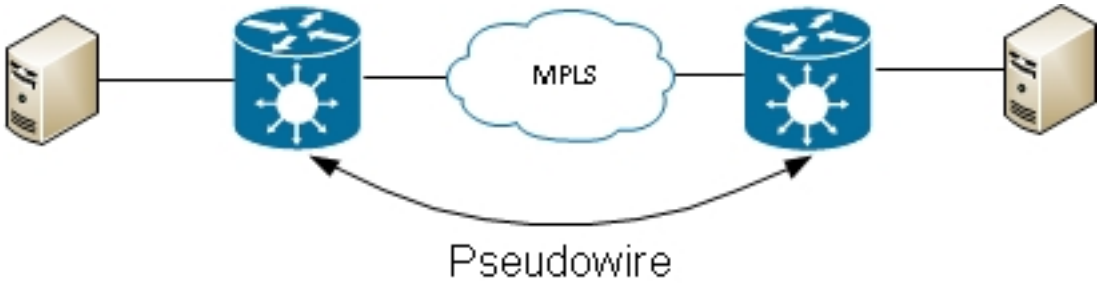


Na realidade, pode haver vários roteadores entre os dois nós finais e pode haver vários designs para fornecer o serviço ponto-a-ponto.

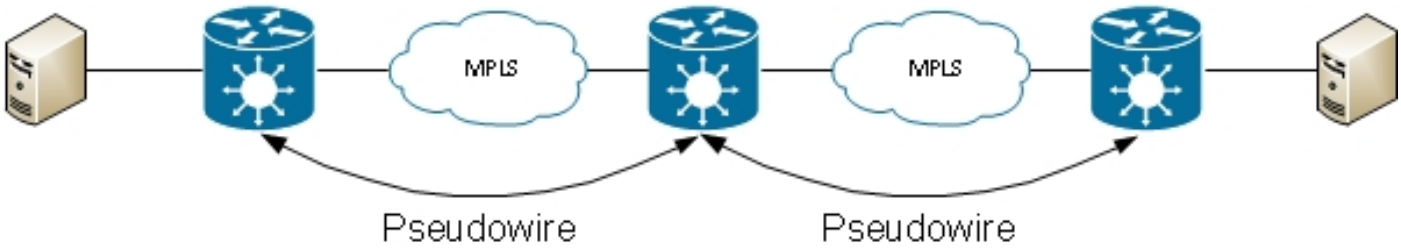
Um roteador pode fazer switching local entre duas de suas interfaces:



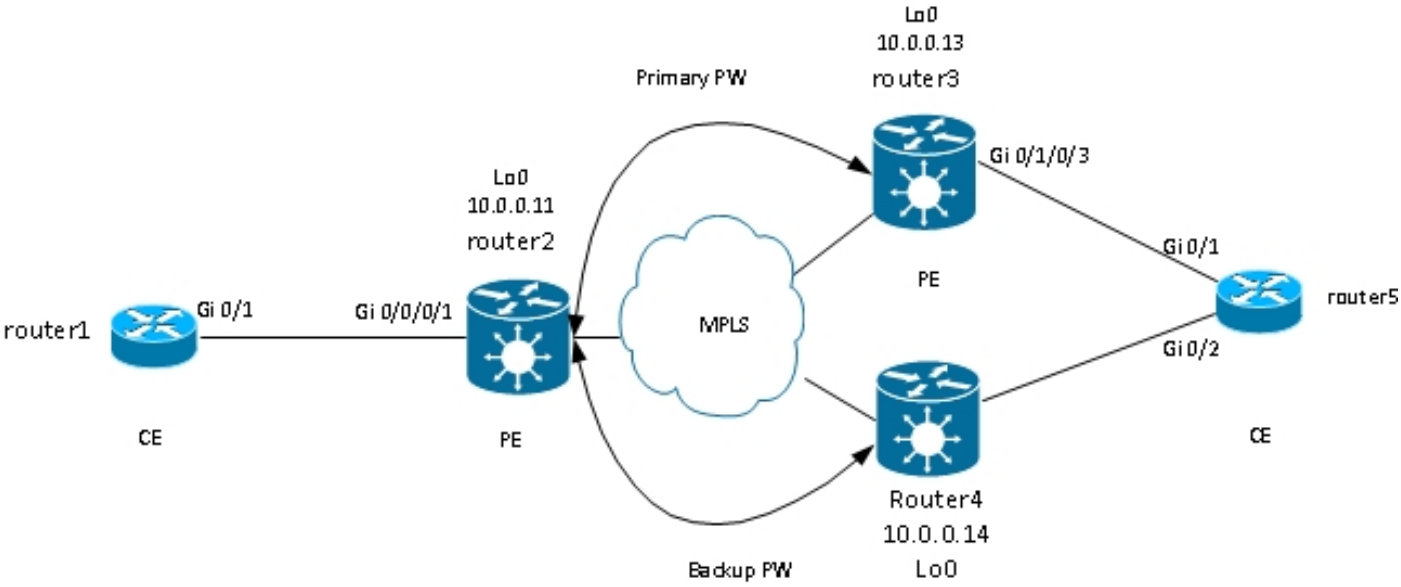
Também pode haver um pseudofio (PW) de Multiprotocol Label Switching (MPLS) entre dois roteadores:



Um roteador pode comutar quadros entre dois PWs; nesse caso, este é um PW de vários segmentos:



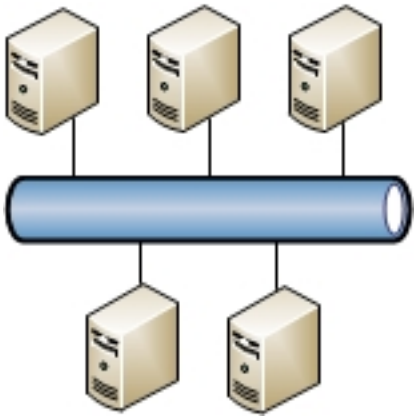
A redundância está disponível através do recurso de redundância PW:



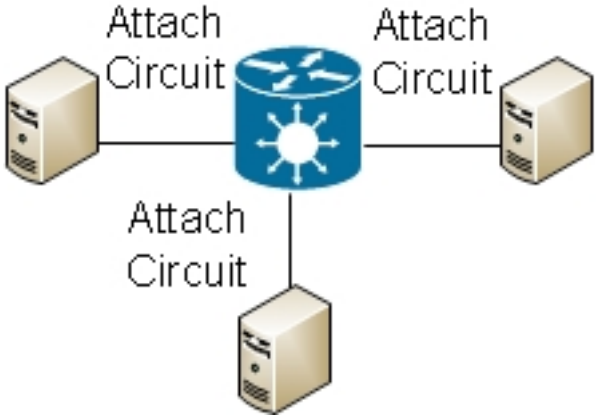
Outros designs estão disponíveis, mas não podem ser listados aqui.

1.2 Serviço Multiponto

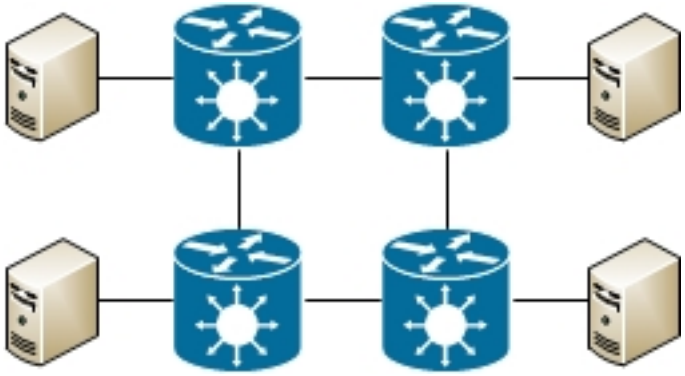
O serviço multiponto emula um domínio de broadcast para que todos os hosts conectados nesse domínio de bridge pareçam estar logicamente conectados ao mesmo segmento Ethernet:



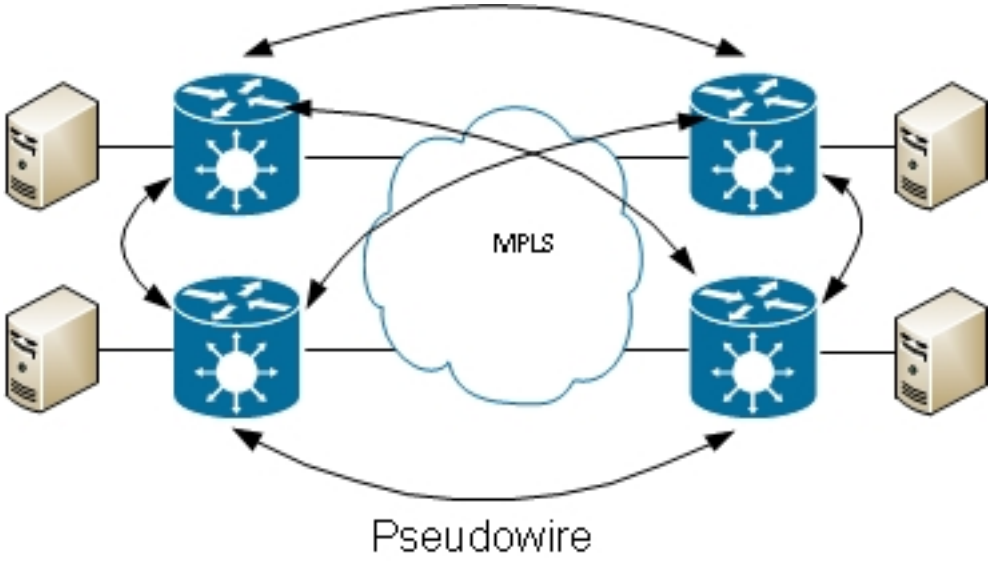
Todos os hosts podem ser conectados ao mesmo roteador/switch:



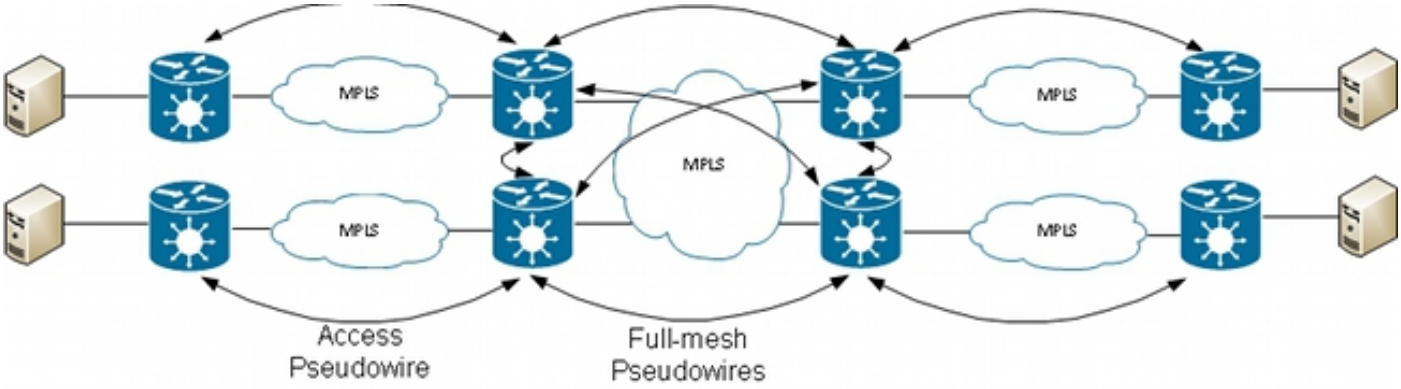
Vários switches podem fazer o switching Ethernet tradicional; o spanning tree deve ser usado para quebrar loops:



O Virtual Private LAN Services (VPLS) permite estender o domínio de broadcast entre vários locais usando PWs MPLS:



O VPLS hierárquico pode ser usado para aumentar a escalabilidade:



2. Circuitos de fixação

2.1 Circuito virtual Ethernet ASR 9000

2.1.1 Correspondência da interface de entrada

As regras básicas para circuitos de conexão (ACs) incluem:

- Um pacote deve ser recebido em uma interface configurada com a palavra-chave *l2transport* para ser processado pelo recurso L2VPN.
- Essa interface pode ser uma interface principal, em que o comando **l2transport** é configurado no modo de configuração da interface, ou uma subinterface, em que a palavra-chave *l2transport* é configurada após o número da subinterface.
- Uma pesquisa de correspondência mais longa determina a interface de entrada do pacote. A pesquisa de correspondência mais longa verifica essas condições nesta ordem para corresponder o pacote recebido a uma subinterface:

  1. O quadro de entrada tem duas marcas dot1q e corresponde a uma subinterface configurada com as mesmas duas marcas dot1q (encapsulamento 802.1Q ou QinQ). Esta

é a correspondência mais longa possível.
2. O quadro de entrada tem duas tags dot1q e corresponde a uma subinterface configurada com a mesma tag dot1q first e *any* para a segunda tag.
3. O quadro de entrada tem uma marca dot1q e corresponde a uma subinterface configurada com a mesma marca dot1q e a palavra-chave *exato*.
4. O quadro de entrada tem uma ou mais marcas dot1q e corresponde a uma subinterface configurada com uma das marcas dot1q.
5. O quadro de entrada não tem tags dot1q e corresponde a uma subinterface configurada com o comando **encapsulation untagged**.
6. O quadro de entrada não corresponde a nenhuma outra subinterface, portanto ele corresponde a uma subinterface configurada com o comando **encapsulation default**.
7. O quadro de entrada não corresponde a nenhuma outra subinterface, portanto, corresponde à interface principal configurada para *l2transport*.

- Em roteadores tradicionais que não usam o modelo Ethernet Virtual Connection (EVC), as marcas de VLAN configuradas na subinterface são removidas (exibidas) do quadro antes de serem transportadas pelo recurso L2VPN.
- Em um Cisco ASR 9000 Series Aggregation Services Router que usa a infraestrutura EVC, a ação padrão é preservar as marcas existentes. Use o comando **rewrite** para modificar o padrão.
- Se houver uma BVI (Bridge Virtual Interface, interface virtual de ponte) no domínio de ponte, todas as marcas de entrada deverão ser removidas, pois a BVI é uma interface roteada sem nenhuma marca. Consulte a seção BVI para obter detalhes.

Aqui estão vários exemplos que ilustram essas regras:

1. Um exemplo básico é quando todo o tráfego recebido em uma porta física deve ser transportado, independentemente de ter ou não uma marca de VLAN. Se você configurar **l2transport** na interface principal, todo o tráfego recebido nessa porta física será transportado pelo recurso L2VPN:

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

   Se houver subinterfaces dessa interface principal, a interface principal capturará qualquer quadro que não tenha sido correspondido por nenhuma subinterface; essa é a regra de correspondência mais longa.

2. As interfaces e subinterfaces do pacote podem ser configuradas como l2transport:

```
interface Bundle-Ether1
l2transport
```

3. Use **encapsulation default** em uma subinterface l2transport para corresponder a qualquer tráfego marcado ou não marcado que não tenha sido correspondido por outra subinterface com uma correspondência mais longa. (Consulte o Exemplo 4). A palavra-chave *l2transport* é configurada no nome da subinterface, não na subinterface como na interface principal:

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

Configure o **encapsulamento não marcado** se quiser corresponder apenas quadros não marcados.

4. Quando houver várias subinterfaces, execute o teste de correspondência mais longa no quadro de entrada para determinar a interface de entrada:

```
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
```

Nesta configuração, observe que:

- Um quadro QinQ com uma tag 2 de VLAN externa e uma tag 3 de VLAN interna pode corresponder às subinterfaces .1, .2 ou .3, mas é atribuído à subinterface .3 devido à regra de correspondência mais longa. Duas marcas em .3 são maiores que uma marca em .2 e maiores que nenhuma marca em .1.
- Um quadro QinQ com uma tag 2 de VLAN externa e uma tag 4 de VLAN interna é atribuído à subinterface .2 porque o **encapsulamento dot1q 2** pode corresponder quadros dot1q apenas com a tag 2 de VLAN, mas também pode corresponder quadros QinQ com uma tag 2 externa. Consulte o Exemplo 5 (a palavra-chave *exata*) se não desejar corresponder os quadros QinQ.
- Um quadro QinQ com uma tag 3 de VLAN externa corresponde à subinterface .1.
- Um quadro dot1q com uma marca de VLAN 2 corresponde à subinterface .2.
- Um quadro dot1q com uma marca de VLAN 3 corresponde à subinterface .1.

5. Para corresponder um quadro dot1q e não um quadro QinQ, use a palavra-chave *exact*:

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

Essa configuração não corresponde a quadros QinQ com uma tag 2 de VLAN externa porque ela corresponde apenas a quadros com exatamente uma tag de VLAN.

6. Use a palavra-chave *untagged* para corresponder apenas quadros não marcados, como pacotes Cisco Discovery Protocol (CDP) ou Multiple Spanning Tree (MST) Bridge Protocol Data Units (BPDUs):

```
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
```

Nesta configuração, observe que:

- Os quadros Dot1q com uma tag 3 de VLAN ou os quadros QinQ com uma tag 3 externa correspondem às subinterfaces .3.
- Todos os outros quadros dot1q ou QinQ correspondem à subinterface .1.
- Os quadros sem uma marca de VLAN correspondem à subinterface .2.

7. A palavra-chave *any* pode ser usada como caractere curinga:

```
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 as subinterfaces .4 e .5 poderiam corresponder quadros QinQ com as marcas 4 e 5, mas os quadros são atribuídos às subinterfaces .5 porque é mais específico. Esta é a regra de correspondência mais longa.

8. Intervalos de marcas de VLAN podem ser usados:

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

9. Vários valores ou intervalos de tag de VLAN podem ser listados para a primeira ou segunda tag 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
```

   Você pode listar um máximo de nove valores. Se mais valores forem necessários, eles deverão ser atribuídos a outra subinterface. Agrupar valores em um intervalo para reduzir a lista.

10. O comando **encapsulation dot1q second-dot1q** usa o Ethertype 0x8100 para as tags externa e interna porque este é o método Cisco para encapsular quadros QinQ. De acordo com o IEEE, no entanto, o Ethertype 0x8100 deve ser reservado para quadros 802.1q com uma marca de VLAN, e uma marca externa com Ethertype 0x88a8 deve ser usada para quadros QinQ. A tag externa com Ethertype 0x88a8 pode ser configurada com a palavra-chave *dot1ad*:

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

11. Para usar o antigo Ethertype 0x9100 ou 0x9200 para as tags externas QinQ, use o comando **dot1q tunneling ethertype** na interface principal da subinterface QinQ:

```
interface GigabitEthernet0/1/0/3
 dot1q tunneling ethertype [0x9100|0x9200]
```

```
!
interface GigabitEthernet0/1/0/3.13 l2transport
encapsulation dot1q 13 second-dot1q 100
```

A marca externa tem um Ethertype de 0x9100 ou 0x9200, e a marca interna tem o Ethertype 0x8100 dot1q.

12. Um quadro de entrada pode ser atribuído a uma subinterface, com base no endereço MAC origem:

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

2.1.2 Manipulação de VLAN

O comportamento padrão de uma plataforma baseada em EVC é manter as tags de VLAN no quadro de entrada.

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

Nessa configuração, um quadro dot1q de entrada com uma marca de VLAN 3 mantém sua marca de VLAN 3 quando o quadro é encaminhado. Um quadro QinQ de entrada com uma tag 3 de VLAN externa e uma tag 100 interna mantém ambas as tags inalteradas quando o quadro é encaminhado.

Mas, a infraestrutura do EVC permite manipular as tags com o comando **rewrite**, para que você possa fazer pop-ups (remover), transladar ou empurrar (adicionar) tags para a pilha de tags de VLAN de entrada.

Aqui estão vários exemplos:

- A palavra-chave *pop* permite remover uma tag QinQ de um quadro dot1q de entrada. Este exemplo remove a tag externa 13 do quadro QinQ recebido e encaminha o quadro com a tag dot1q 100 no topo:

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

O comportamento é sempre simétrico, o que significa que a tag externa 13 é exibida na direção de entrada e empurrada na direção de saída.

- A palavra-chave *translate* permite substituir uma ou duas marcas de entrada por uma ou duas novas marcas:

```
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
```

A palavra-chave *symmetric* é adicionada automaticamente porque é o único modo com suporte.

- A palavra-chave *push* permite adicionar uma marca QinQ a um quadro dot1q de entrada:

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

Um QinQ tag 100 externo é adicionado ao quadro de entrada com um dot1q tag 4. Na direção de saída, a marca QinQ é exibida.

2.2 Comportamento do roteador Cisco IOS XR não EVC (CRS e XR12000)

A sintaxe para correspondência de VLAN nas plataformas não EVC não usa a palavra-chave *encapsulation*:

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

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

Não é possível configurar a manipulação de marcas de VLAN, pois o único comportamento possível é remover todas as marcas especificadas nos comandos **dot1q** ou **dot1ad**. Isso é feito por padrão, portanto, não há nenhum comando **rewrite**.

3. Serviço Point-to-Point

Notas:

Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

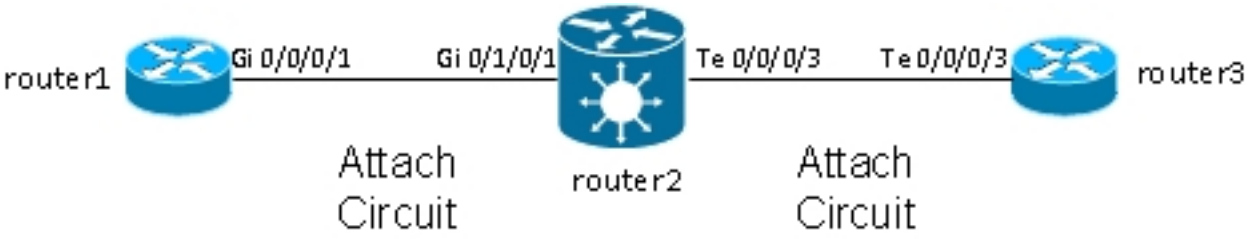
A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com

alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

3.1 Comutação local

3.1.1 Interface principal

A topologia básica é uma conexão cruzada local entre duas interfaces principais:



O Roteador 2 recebe todo o tráfego recebido na Gi 0/1/0/1 e o encaminha para a Gi 0/0/0/3 e vice-versa.

Embora o roteador 1 e o roteador 3 pareçam ter um cabo back-to-back direto nessa topologia, esse não é o caso porque o roteador 2 está, na verdade, convertendo entre as interfaces TenGigE e GigabitEthernet. O Roteador2 pode executar recursos nessas duas interfaces; uma lista de controle de acesso (ACL), por exemplo, pode descartar tipos específicos de pacotes ou um mapa de políticas para modelar ou limitar a taxa do tráfego de baixa prioridade.

Uma conexão cruzada básica ponto-a-ponto é configurada entre duas interfaces principais configuradas como l2transport no roteador2:

```
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
!
```

Em router1 e router3, as interfaces principais são configuradas com CDP e um endereço 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
```

O Roteador 1 vê o Roteador 3 como um vizinho CDP e pode fazer ping em 10.1.1.2 (o endereço da interface do Roteador 3) como se os dois roteadores estivessem diretamente conectados.

Como não há subinterface configurada no roteador 2, os quadros de entrada com uma marca de VLAN são transportados de forma transparente quando as subinterfaces dot1q são configuradas no roteador 1 e no roteador 3:

```
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
```

Depois de 10.000 pings do roteador 1 para o roteador 3, você pode usar os comandos **show interface** e **show l2vpn** para garantir que as solicitações de ping recebidas pelo roteador 2 em uma AC sejam encaminhadas na outra AC e que as respostas do ping sejam tratadas da mesma forma no sentido inverso.

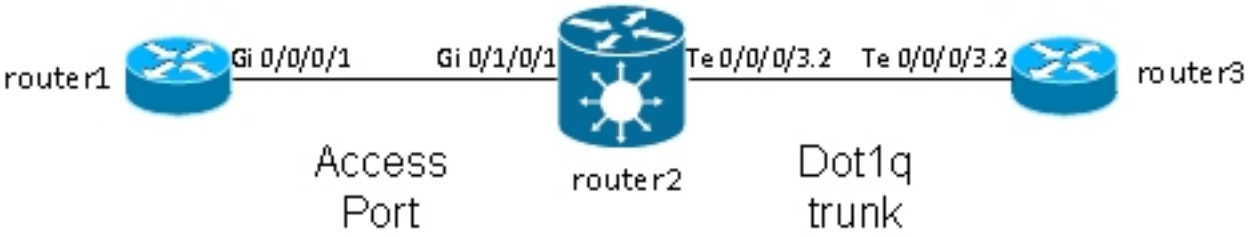
```
RP/0/RSP0/CPU0:router2#sh int gig 0/1/0/1
GigabitEthernet0/1/0/1 is up, line protocol is up
Interface state transitions: 1
Hardware is GigabitEthernet, address is 0024.986c.63f1 (bia 0024.986c.63f1)
Description: static lab connection to acdc 0/0/0/1 - dont change
Layer 2 Transport Mode
MTU 1514 bytes,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

```
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions


RP/0/RSP0/CPU0:router2#sh int ten 0/0/0/3
TenGigE0/0/0/3 is up, line protocol is up
Interface state transitions: 3
Hardware is TenGigE, address is 0024.98ea.038b (bia 0024.98ea.038b)
Layer 1 Transport Mode is LAN
Description: static lab connection to putin 0/0/0/3 - dont change
Layer 2 Transport Mode
MTU 1514 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
reliability 255/255, txload 0/255, rxload 0/255
Encapsulation ARPA,
Full-duplex, 10000Mb/s, LR, link type is force-up
output flow control is off, input flow control is off
loopback not set,
Last input 00:00:00, output 00:00:06
Last clearing of "show interface" counters 00:01:15
5 minute input rate 27000 bits/sec, 30 packets/sec
5 minute output rate 27000 bits/sec, 30 packets/sec
10008 packets input, 1140908 bytes, 0 total input drops
0 drops for unrecognized upper-level protocol
Received 0 broadcast packets, 8 multicast packets
0 runts, 0 giants, 0 throttles, 0 parity
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
10006 packets output, 1140592 bytes, 0 total output drops
Output 0 broadcast packets, 6 multicast packets
0 output errors, 0 underruns, 0 applique, 0 resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions


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

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

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

RP/0/RSP0/CPU0:router2#sh l2vpn forwarding interface gigabitEthernet 0/1/0/1
   hardware ingress detail location 0/1/CPU0
Local interface: GigabitEthernet0/1/0/1, Xconnect id: 0x1880003, Status: up
Segment 1
AC, GigabitEthernet0/1/0/1, Ethernet port mode, status: Bound
Statistics:
```

```
packets: received 10022, sent 10023
bytes: received 1142216, sent 1142489
packets dropped: PLU 0, tail 0
bytes dropped: PLU 0, tail 0
Segment 2
AC, TenGigE0/0/0/3, Ethernet port mode, status: Bound

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

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

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

3.1.2 Subinterfaces e manipulação de VLAN

Na terminologia do Cisco IOS® Software, este exemplo tem um AC que é como uma interface de acesso do modo switchport e uma subinterface dot1q que é como um tronco:



Normalmente, essa topologia usa um domínio de ponte porque geralmente há mais de duas portas na VLAN, embora você possa usar uma conexão cruzada ponto a ponto se houver apenas duas portas. Esta seção descreve como os recursos flexíveis de regravação oferecem várias maneiras de manipular a VLAN.

3.1.2.1 Interface Principal e Subinterface Dot1q

Neste exemplo, a interface principal está em um lado e a subinterface dot1q está no outro lado:

Esta é a interface principal no roteador 1:

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

Esta é a subinterface dot1q no roteador2:

```
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
```

Agora existe uma palavra-chave *l2transport* no nome da subinterface de TenGigE0/0/0/3.2. O Roteador 3 envia quadros dot1q com tag 2, que correspondem à subinterface TenGigE0/0/0/3.2 no Roteador 2.

A marca de entrada 2 é removida na direção de ingresso pelo comando **rewrite ingress tag pop 1 symmetric**. Como a marca foi removida na direção de entrada em TenGigE0/0/0/3.2, os pacotes são enviados sem marca na direção de saída em GigabitEthernet0/1/0/1.

O Roteador 1 envia quadros não marcados, que correspondem à interface principal GigabitEthernet0/1/0/1.

Não há nenhum comando **rewrite** em GigabitEthernet0/1/0/1, portanto nenhuma tag é exibida, enviada ou traduzida.

Quando os pacotes precisam ser encaminhados para fora de TenGigE0/0/0/3.2, a tag dot1q 2 é enviada devido à palavra-chave *symmetric* no comando **rewrite ingress tag pop 1**. O comando exibe uma marca na direção de entrada, mas empurra simetricamente uma marca na direção de saída. Este é um exemplo em 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
```

Monitore os contadores de subinterface com os mesmos comandos **show interface** e **show l2vpn**:

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


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

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

Como esperado, o número de pacotes recebidos em TenGigE0/0/0/3.2 corresponde ao número de pacotes enviados em GigabitEthernet0/1/0/1 e vice-versa.

3.1.2.2 Subinterface com encapsulamento

Em vez da interface principal em GigabitEthernet0/1/0/1, você pode usar uma subinterface com **encapsulation default** para capturar todos os quadros ou com **encapsulation untagged** para corresponder apenas quadros não marcados:

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

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

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

3.1.2.3 Direção de entrada em GigabitEthernet0/1/0/1.1

Em vez da marca pop 2 na direção de ingresso em TenGigE0/0/0/3.2, você pode empurrar a marca 2 na direção de ingresso em GigabitEthernet0/1/0/1.1 e não fazer nada em TenGigE0/0/0/3.2:

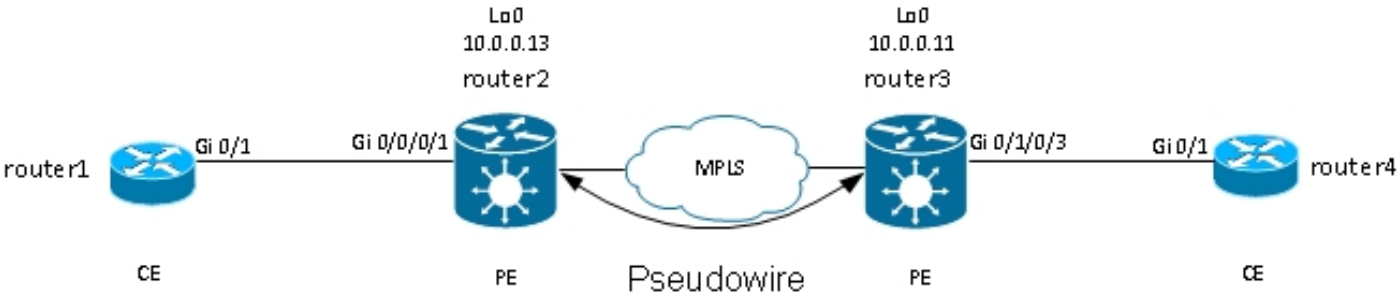
```
RP/0/RSP0/CPU0:router2#sh run int  TenGigE0/0/0/3.2
interface TenGigE0/0/0/3.2 l2transport
encapsulation dot1q 2

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
```

Assim, você pode ver que o modelo EVC com os comandos **encapsulation** e **rewrite** oferece grande flexibilidade para combinar e manipular tags de VLAN.

3.2 Serviços de telefonia privada virtual

3.2.1 Visão geral

O Virtual Private Wire Services (VPWS), também conhecido como Ethernet over MPLS (EoMPLS), permite que dois dispositivos L2VPN Provider Edge (PE) encapsulem o tráfego L2VPN em uma nuvem MPLS. Os dois PEs L2VPN são normalmente conectados em dois locais diferentes com um núcleo MPLS entre eles. Os dois ACs conectados em cada PE L2VPN são vinculados por um PW sobre a rede MPLS, que é o PW MPLS.



Cada PE precisa ter um rótulo MPLS para acessar o loopback do PE remoto. Esse rótulo, geralmente chamado de rótulo IGP (Interior Gateway Protocol), pode ser aprendido por meio do LDP (Label Distribution Protocol) ou do TE (Traffic Engineering) de MPLS.

Os dois PEs estabelecem uma sessão LDP de MPLS entre si para que possam estabelecer e controlar o status do PW. Um PE anuncia ao outro PE o rótulo MPLS para identificação de PW.

> **Observação**: embora o BGP possa ser usado para sinalização, ele não é abordado neste documento.

O tráfego recebido pelo roteador 2 em seu AC local é encapsulado em uma pilha de rótulos MPLS:

- O rótulo MPLS externo é o rótulo IGP para acessar o loopback do roteador 3. Pode ser o rótulo nulo implícito se os rótulos estiverem diretamente conectados; isso significa que nenhum rótulo IGP seria anexado.
- O rótulo MPLS interno é o rótulo PW anunciado pelo roteador 3 através da sessão LDP de destino.
- Pode haver uma palavra de controle PW após os rótulos MPLS, dependendo da configuração e do tipo de encapsulamento. A palavra de controle não é usada por padrão em interfaces Ethernet e deve ser configurada explicitamente quando necessário.
- O quadro L2 transportado segue no pacote.
- Algumas marcas de VLAN são transportadas pelo PW, dependendo da configuração e do tipo de PW.

O penúltimo salto, antes do roteador 3 no núcleo MPLS, exibe o rótulo IGP ou o substitui por um rótulo nulo explícito. Assim, o rótulo mais significativo no quadro recebido pelo roteador3 é o rótulo PW que o roteador3 sinalizou para o roteador2 para o PW. Assim, o roteador 3 sabe que o tráfego recebido com esse rótulo MPLS deve ser comutado para a CA conectada ao roteador 4.

No exemplo anterior, você deve primeiro verificar se cada L2VPN tem um rótulo MPLS para o loopback do PE remoto. Este é um exemplo de como verificar rótulos no roteador2:

```
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
```

A configuração AC ainda é a mesma:

```
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
```

Como não há nenhum comando **rewrite ingress pop**, a tag 2 de VLAN de entrada é transportada pelo PW. Consulte PWs tipo 4 e 5 para obter detalhes.

A configuração de L2VPN especifica o AC local e o PE de L2VPN remoto com um ID de PW que deve corresponder em cada lado e deve ser exclusivo para cada vizinho:

```
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
```

A configuração correspondente no roteador 3 é:

```
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
```

Use o comando **show l2vpn xconnect detail** para exibir detalhes da conexão cruzada:

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

Group test, XC p2p4, state is up; Interworking none
AC: GigabitEthernet0/0/0/1.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1504; XC ID 0x840006; interworking none
Statistics:
packets: received 186, sent 38448
bytes: received 12644, sent 2614356
drops: illegal VLAN 0, illegal length 0
PW: neighbor 10.0.0.11, PW ID 222, state is up ( established )
PW class not set, XC ID 0xc0000004
Encapsulation MPLS, protocol LDP
Source address 10.0.0.13
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
```

```
Sequencing not set

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

Nesta configuração, observe que:

- A unidade de transmissão máxima (MTU) da AC é 1504 porque a etiqueta de entrada na AC não é exibida. A MTU deve corresponder em cada lado, ou o PW não aparece.
- 186 pacotes foram recebidos no AC e enviados no PW como esperado.
- 38448 pacotes foram recebidos no PW e enviados no AC como esperado.
- O rótulo local em router2 é 16026 e é o rótulo que router3 usa como o rótulo interno. Os pacotes são recebidos no roteador 2 com esse rótulo MPLS como o rótulo superior, pois o rótulo IGP foi pulado pelo penúltimo salto MPLS. O Roteador2 sabe que os quadros de entrada com esse rótulo PW devem ser comutados para a Gi 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 Status acoplado PW e AC

Em uma conexão cruzada ponto-a-ponto, a CA e o PW são acoplados. Portanto, se o CA for desativado, o PE L2VPN sinalizará via LDP para o PE remoto que o status do PW deve ser desativado. Isso aciona a convergência quando a redundância de PW é configurada. Consulte a seção Redundância para obter detalhes.

Neste exemplo, a CA está inativa no roteador 2 e está enviando o status de PW 'AC Down' para o roteador 3:

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

```
Wed May 1 23:38:55.542 CEST

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

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

O Roteador 3 sabe que o PW deve estar desativado porque o AC remoto está desativado:

```
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 PWs tipo 4 e tipo 5

Dois tipos de PWs podem ser usados - tipo 4 e tipo 5.

- Um PW tipo 4 é conhecido como um PW baseado em VLAN. O PE de entrada não deve remover as tags de VLAN de entrada que devem ser transportadas pelo PW.

  Nas plataformas baseadas em EVC, como o ASR 9000, o problema é que os ACs de entrada podem ter um comando **rewrite** que exibe as tags de VLAN de entrada, de modo que pode não haver nenhuma tag de VLAN a ser transportada pelo PW. Para lidar com essa possibilidade, as plataformas EVC inserem uma tag 0 de VLAN fictícia no topo do quadro para PWs tipo 4. Os PWs tipo 4 são configurados com o comando **transport-mode vlan**. O PE remoto deve ser baseado em EVC e deve entender que a tag de VLAN superior é a tag fictícia a ser removida.

  No entanto, se você usar um PW tipo 4 entre uma plataforma EVC e uma plataforma não-EVC, isso pode levar a problemas de interoperabilidade. A plataforma não-EVC não considera a marca de VLAN superior como a marca de VLAN fictícia e, em vez disso, encaminha o quadro com a marca de VLAN fictícia 0 como a marca externa. As plataformas EVC têm a capacidade de manipular as tags de VLAN recebidas no quadro de entrada com o comando **rewrite**. Os resultados dessa manipulação de VLAN são transportados sobre o PW tipo 4 com a tag fictícia extra 0 no topo.

  Versões recentes do software Cisco IOS XR oferecem a capacidade de usar um PW tipo 4 sem usar a tag 0 fictícia com o comando **transport-mode vlan passthrough**. A manipulação da marca VLAN no Ethernet Flow Point (EFP) deve garantir que pelo menos uma marca

permaneça porque deve haver uma marca VLAN transportada em um PW tipo 4 e porque, nesse caso, não há nenhuma marca fictícia que atenda a esse requisito. As marcas que permanecem no quadro após a reescrita da marca da interface de entrada são transportadas de forma transparente através do PW.

- Um PW tipo 5 é conhecido como um PW baseado em porta Ethernet. O PE de entrada transporta quadros recebidos em uma interface principal ou após as marcas de subinterface terem sido removidas quando o pacote é recebido em uma subinterface. Não há nenhum requisito para enviar um quadro marcado sobre um PW tipo 5, e nenhuma marca fictícia é adicionada pelas plataformas baseadas em EVC. As plataformas baseadas em EVC têm a capacidade de manipular as tags de VLAN recebidas no quadro de entrada com o comando **rewrite**. Os resultados dessa manipulação de VLAN são transportados pelo PW tipo 5, seja marcado ou não.

Por padrão, os PEs L2VPN tentam negociar um PW tipo 5, como visto neste exemplo:

```
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
```

A Ethernet tipo PW indica um PW tipo 5.

Esta é uma captura de farejador de uma solicitação ARP enviada pelo roteador 1 e encapsulada pelo roteador 2 sobre o PW para o roteador 3:

```
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)
```

O rótulo MPLS 16031 é o rótulo PW anunciado pelo roteador 3. A captura do farejador foi feita entre o penúltimo salto e o roteador 3, portanto, não há rótulo IGP.

O quadro Ethernet encapsulado começa imediatamente após o rótulo PW. Pode haver uma palavra de controle PW, mas ela não está configurada neste exemplo.

Mesmo que seja um PW tipo 5, a VLAN tag 2 recebida na CA pelo roteador 2 é transportada porque não há nenhum comando **rewrite** que a exiba na CA. Os resultados que vêm do AC após o processamento de regravação são transportados porque não há estouro automático de tag nas plataformas baseadas em EVC. Observe que não há nenhuma tag de VLAN fictícia 0 com um PW tipo 5.

Se você configurou com o comando **rewrite ingress tag pop 1 symmetric**, não haveria nenhuma marca de VLAN transportada pelo PW.

Aqui está um exemplo de um PW tipo 4 com a configuração de um pw-class no roteador 2 e no roteador 3.

> **Observação**: se você configurar um tipo 4 em apenas um lado, o PW permanecerá inativo e relatará 'Erro: tipo de PW incompatível'.

```
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
!
!
!
!
```

A VLAN Ethernet tipo PW indica um PW tipo 4.

```
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
```

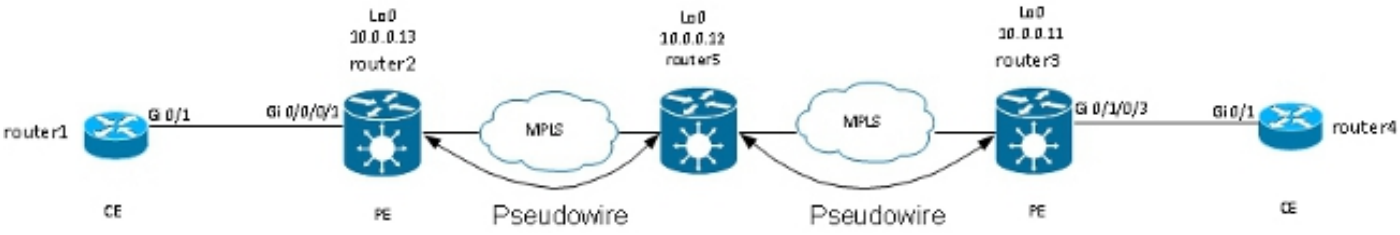
Agora há uma tag fictícia 0 inserida na parte superior do quadro que está sendo transportado:

```
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)
```

O PE de saída baseado em EVC remove a tag fictícia e encaminha o quadro com a tag 2 em seu AC local. O PE de saída aplica a manipulação de marca local configurada em seu AC no quadro recebido no PW. Se seu AC local estiver configurado como **rewrite ingress tag pop 1 symmetric**, a tag configurada deverá ser empurrada na direção de saída, para que uma nova tag seja empurrada sobre a tag 2 recebida no PW. O comando rewrite é muito flexível, mas você deve avaliar cuidadosamente o que deseja alcançar em cada lado do PW.

3.2.4 PW multissegmentos

Épossível ter um PE L2VPN que tenha um PW, em vez de uma interface física, como um AC:



O Roteador 5 recebe pacotes no PW do Roteador 2 e comuta os pacotes em seu outro PW para o Roteador 3. O roteador 5 está alternando entre PWs para criar um PW multissegmento entre o roteador 2 e o roteador 3.

A configuração no roteador 2 agora aponta para o roteador 5 como o PE remoto:

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

A configuração no roteador 5 é 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
!
!
!
```

O comando **description** é opcional e é inserido em um valor de comprimento de tipo (TLV) de switching PW que é enviado pelo roteador 5 para cada PE remoto (roteador 2 e roteador 3). A **descrição** é útil quando você precisa solucionar um problema de PW quando há um roteador no meio que faz switching de PW.

Insira o comando **sh l2vpn xconnect** para revisar o TLV de comutação PW:

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

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

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------------------
Label 16042 unknown
Group ID 0x4000280 0x0
Interface GigabitEthernet0/0/0/1.2 unknown
MTU 1504 unknown
Control word disabled unknown
PW type Ethernet unknown
VCCV CV type 0x2 0x0
(none)
(LSP ping verification)
VCCV CC type 0x4 0x0
```

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

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

O Roteador 5 envia um TLV de switching PW ao roteador 3 com os detalhes de seu PW ao roteador 2 e envia um TLV de switching PW ao roteador 2 com os detalhes de seu PW ao roteador 3.

3.2.5 Redundância

Um PW ponto a ponto pode ser usado para conectar dois locais, mas esses dois locais devem permanecer conectados em caso de falha de PE ou AC.

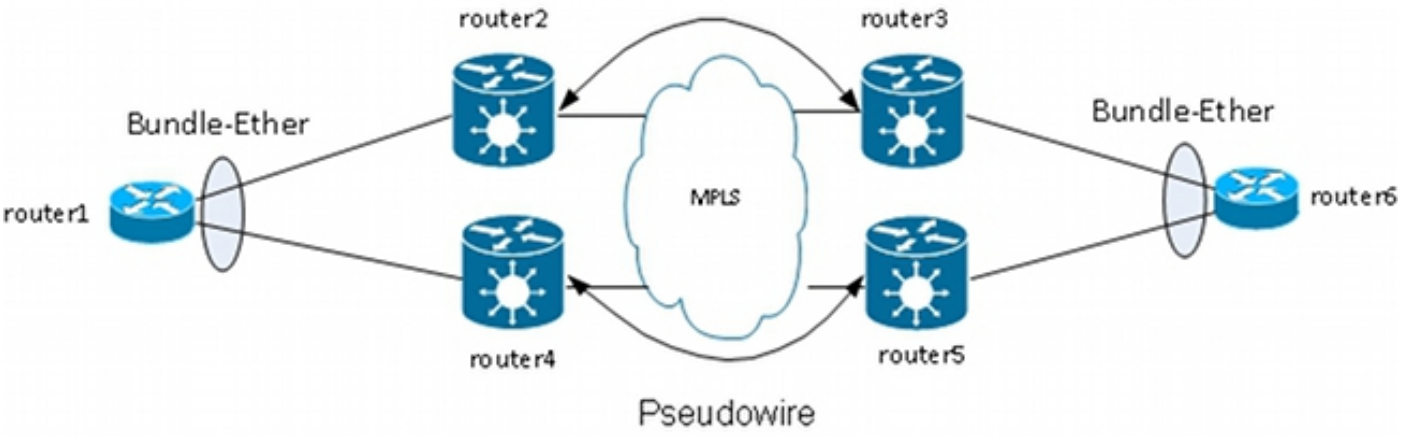
3.2.5.1 Redundância de núcleo

Se você fizer qualquer alteração de topologia que afete o reroteamento no núcleo do MPLS, o MPLS PW herdará o novo caminho imediatamente.

3.2.5.2 Pacote sobre PWs

Um dispositivo Customer Edge (CE) pode ser conectado ao PE por meio de um pacote Ethernet para fornecer redundância de link se houver uma falha de link de membro do pacote entre o CE e o PE. O pacote permanece ativo mesmo se um membro do link do pacote for desativado. Observe que isso não fornece redundância de PE porque uma falha de PE desativa todo o pacote.

Um método para redundância é ter vários circuitos transportados por PWs ponto a ponto. Cada circuito é um membro de um pacote Ethernet entre dois CEs:



O PE não termina o pacote e, em vez disso, transporta quadros de forma transparente sobre o PW, incluindo os quadros do LACP (Link Aggregation Control Protocol) que os CEs trocam entre eles.

Com esse design, a perda de um AC ou PE faz com que um membro do pacote seja desativado, mas o pacote permanece ativo.

> **Observação**: os BPDUs do LACP não foram transportados por L2VPN pelo ASR 9000 em versões anteriores ao Cisco IOS XR Software Release 4.2.1.

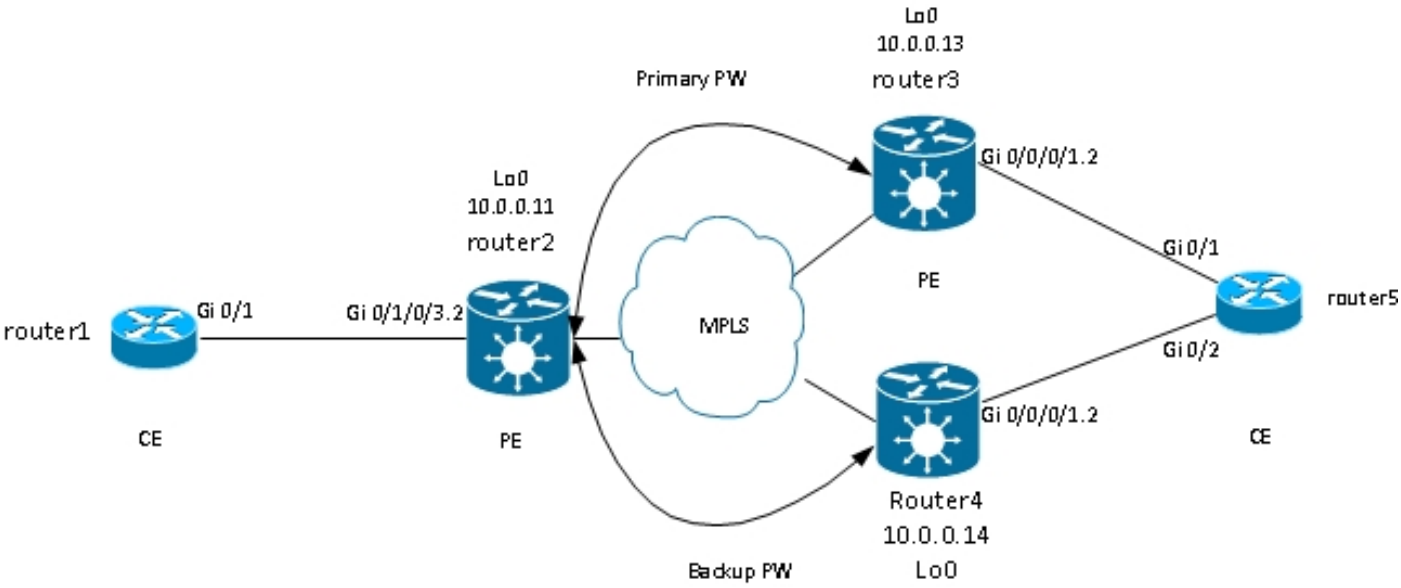
O CE ainda é um ponto único de falha neste projeto. Outros recursos de redundância que podem ser usados no CE incluem:

- Grupo de agregação de link multichassi (MC-LAG)
- Clustering de virtualização de rede (nV) do ASR 9000
- Virtual Switching System (VSS) em switches Cisco IOS
- Virtual Port Channel (vPC) em switches Cisco Nexus

Da perspectiva do PE, há uma conexão ponto a ponto simples entre um AC e um PW MPLS.

3.2.5.3 Redundância de PW

Os PEs também podem fornecer redundância com um recurso chamado Redundância de PW.



Router2 tem um PW primário para router3. O tráfego do roteador 1 para o roteador 6 flui sobre esse PW primário em circunstâncias normais. O Roteador2 também tem um PW de backup para o Roteador4 em hot standby, mas, em circunstâncias normais, nenhum tráfego flui sobre esse PW.

Se houver um problema com o PW primário, com o PE remoto do PW primário (roteador3), ou com o AC no PE remoto (roteador3), o roteador2 ativará imediatamente o PW de backup e o tráfego começará a fluir por ele. O tráfego volta para o PW primário quando o problema é resolvido.

A configuração no roteador 2 é:

```
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
!
!
!
!
!
```

A configuração padrão em router3 e router4 é:

```
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
!
!
```

```
!
!
```

Em condições estáveis, o PW para o roteador 3 está ativo e o PW para o roteador 4 está em um estado de espera:

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

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

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

PW Status TLV in use
MPLS Local Remote
------------ ------------------------ --------------------------
Label 16049 16059
Group ID 0x6000180 0x4000280
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------ --------------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225477
Create time: 03/05/2013 15:04:03 (00:21:26 ago)
Last time status changed: 03/05/2013 15:17:34 (00:07:55 ago)
MAC withdraw message: send 0 receive 0
Statistics:
packets: received 25628, sent 51412
bytes: received 1742974, sent 3729012
```

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

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

Como o status de AC e o status de PW estão acoplados, o roteador 3 sinaliza "AC desativado" para o roteador 2 quando a AC do roteador 3 é desativada. O Roteador2 desativa seu PW principal e ativa o PW de backup:

```
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
```

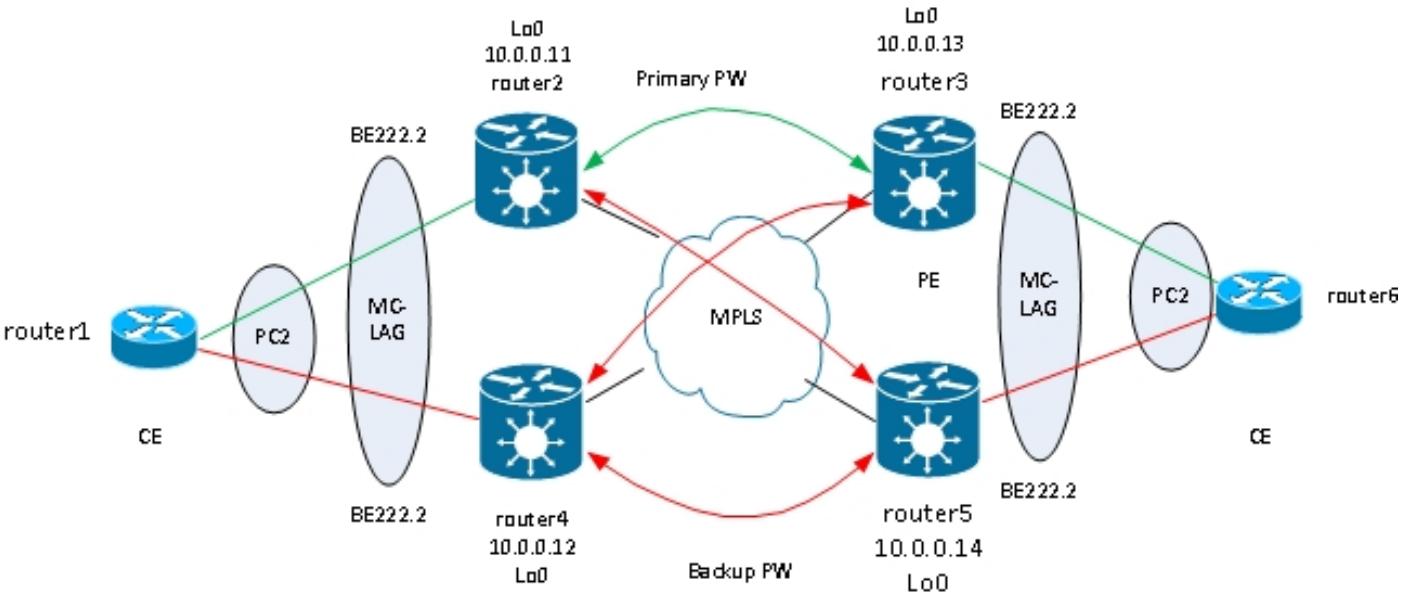
```
bytes: received 3752406, sent 1743230
drops: illegal VLAN 0, illegal length 0
PW: neighbor 10.0.0.13, PW ID 222, state is down ( local ready )
PW class not set, XC ID 0xc0000005
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW 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#
```

Quando a CA no roteador3 volta a funcionar, o roteador2 reativa o PW primário para o roteador3 e o PW para o roteador4 volta para o estado de standby.

O PW de backup também é ativado quando o roteador 3 fica inativo e o roteador 2 perde a rota para seu loopback.

A próxima etapa lógica é apresentar a redundância PW bidirecional com dois PEs em cada local:



No entanto, essa malha completa de PWs encontra um problema quando dois PWs estão ativos ao mesmo tempo em que um loop é introduzido na rede. O loop precisa ser interrompido, geralmente com o uso do Spanning Tree Protocol (STP). No entanto, você não deseja que a instabilidade do spanning tree em um site se propague para o outro site. Assim, é melhor não executar o spanning tree nesses PWs e não mesclar o spanning tree entre os dois sites . É mais simples se houver apenas um link lógico entre os dois sites, de modo que nenhuma spanning tree seja necessária.

Uma solução é usar um pacote MC-LAG entre os dois PEs em um local e seu CE local. Apenas um dos dois PEs tem seus membros de pacote ativos, de modo que seu PW para o local remoto esteja ativo. O outro PE tem seus membros de pacote no estado de standby e tem seu PW para o local remoto inoperante. Com apenas um PW ativo entre os dois locais, nenhum loop é introduzido. O PE com o PW ativo também tem um PW em espera para o segundo PE no local remoto.

Em condições estáveis, os membros ativos do pacote estão no roteador 2 e no roteador 3, e o PW ativo está entre eles. Esta é a configuração no roteador 3:

```
RP/0/RSP1/CPU0:router3#sh run redundancy
redundancy
iccp
group 2
```

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

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

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

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

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

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

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

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

No roteador5, o membro do pacote local e o PW primário para o roteador2 estão no estado de standby, e o PW de backup para o roteador4 está inoperante:

```
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
```

No roteador6, o membro do pacote para o roteador3 está ativo, enquanto o membro do pacote para o roteador5 está no estado de standby:

```
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)
```

Quando o membro do pacote no roteador3 é desativado, o roteador6 tem seu membro ativo para o roteador5:

```
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)
```

Como o pacote ether222 está inativo no roteador 5, o PW acoplado ao roteador 2 fica inativo ao mesmo tempo:

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

O Roteador2 detecta que seu PW para o Roteador3 está inoperante e ativa seu PW de backup para o Roteador5:

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

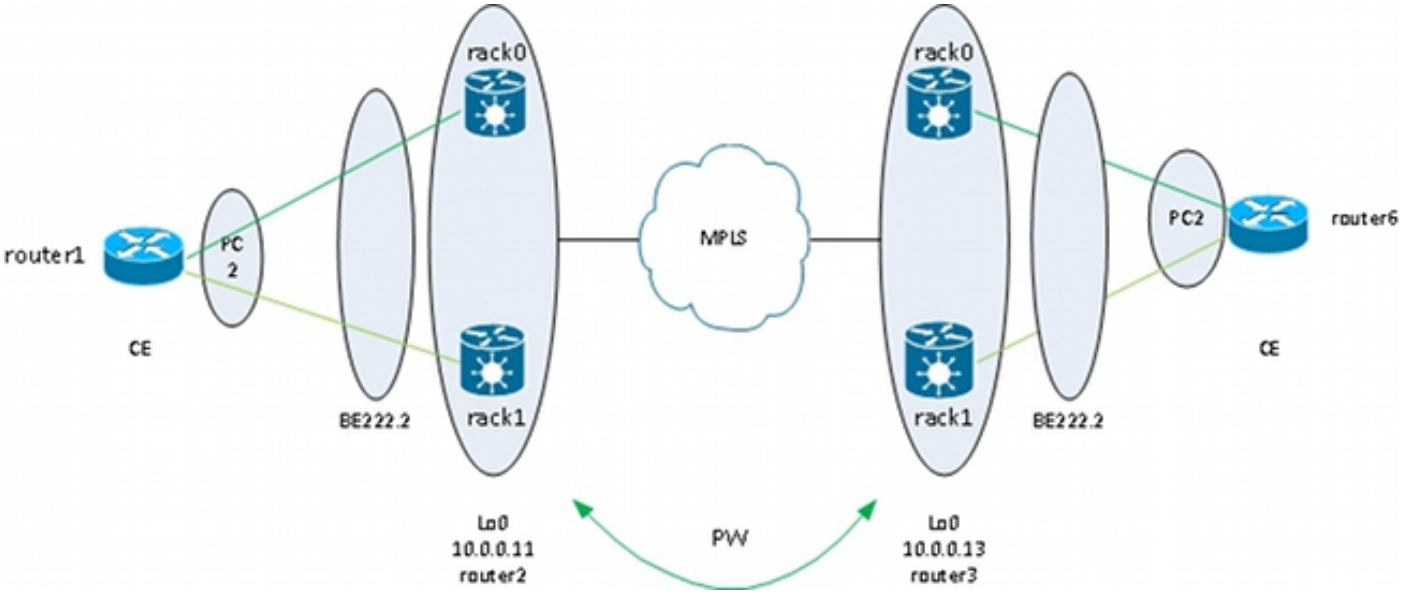
O Router5 tem seu membro de pacote ativo, bem como seu PW primário para o Router2:

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

3.2.5.4 Cluster de borda ASR 9000 nV

O projeto anterior baseado em redundância MC-LAG e PW funciona bem para redundância, mas, como alguns membros do pacote estão no estado de standby, eles não transportam tráfego sob condições estáveis.

Se desejar que todos os membros do pacote estejam ativos, mesmo sob condições estáveis, você poderá usar um cluster ASR 9000 com membros do pacote do CE conectados a cada rack do PE:



Esse design oferece redundância contra uma falha de link de membro do pacote entre o CE e o PE, uma falha de rack e uma falha de link de núcleo - desde que o cluster esteja duplamente conectado ao núcleo MPLS e haja redundância no núcleo. Os dois racks não precisam ser colocalizados e podem estar em locais diferentes. Os links entre racks não são representados neste diagrama.

Se desejar redundância no CE, você pode usar uma solução multichassi para o CE:

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

A configuração no cluster ASR 9000 é muito 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
!
!
!
!
```

A Cisco recomenda que você configure um endereço MAC estático do sistema LACP e um endereço MAC de pacote para evitar uma alteração de endereço MAC causada por um switchover de controlador de sub-bastidor designado. Este exemplo mostra como localizar os endereços:

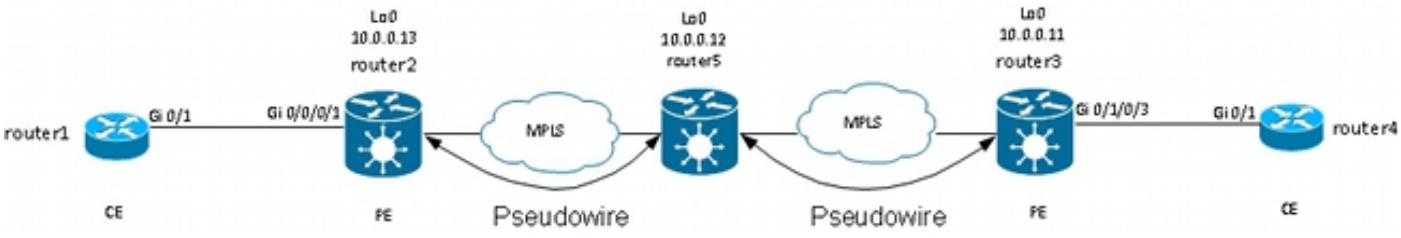
```
RP/1/RSP0/CPU0:router2#sh int bundle-ether 222 | i address is
Hardware is Aggregated Ethernet interface(s), address is 0024.f71e.d309
Internet address is Unknown
RP/1/RSP0/CPU0:router2#
RP/1/RSP0/CPU0:router2#conf
RP/1/RSP0/CPU0:router2(config)#int bundle-ether 222
RP/1/RSP0/CPU0:router2(config-if)#mac-address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

Em resumo, este é o pacote-ether 222 com um membro em cada rack (dez 0/0/0/8 no rack 0 e dez 1/0/0/8 no rack 1) e a subinterface do pacote configurada para uma conexão cruzada ponto a ponto:

```
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

Os roteadores e switches Cisco geralmente enviam pacotes CDP sem tags dot1q. Há vários cenários que determinam o que acontece a esses pacotes CDP quando eles são recebidos por um roteador IOS XR configurado para uma conexão cruzada:



Nessa topologia, o roteador 1 pode ver seu PE router2 local como um vizinho CDP ou o CE router4 remoto, dependendo da configuração.

3.3.1 CDP não ativado na interface principal do L2VPN PE

Os pacotes CDP do CE L2VPN são transportados pela conexão cruzada. Os dois CEs L2VPN se veem (com o uso do comando **show cdp neighbors**) se a interface principal estiver configurada

como l2transport ou se houver uma subinterface que corresponda aos quadros CDP não marcados.

Este é um exemplo da interface principal:

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

Este é um exemplo de uma subinterface não marcada:

```
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
!
!
!
!
```

Nesses dois exemplos, os pacotes CDP são transportados pela conexão cruzada e os CEs se veem como vizinhos CDP. O CE não vê o PE como um vizinho 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 ativado na interface principal do L2VPN PE

O PE processa os pacotes CDP não marcados e o PE e o CE se veem como vizinhos. No entanto, o CE não vê o CE remoto quando o CDP está habilitado na interface principal do L2VPN PE.

Observe que:

- Não é possível configurar o CDP em uma interface principal configurada como l2transport.
- O PE intercepta os pacotes CDP quando o CDP é configurado na interface não l2transport principal. Isso ocorre mesmo se houver uma subinterface l2transport configurada para

corresponder aos pacotes CDP não marcados (com o uso dos comandos **encapsulation untagged** ou **encapsulation default**). Os pacotes CDP não são transportados para o local remoto nesse caso.

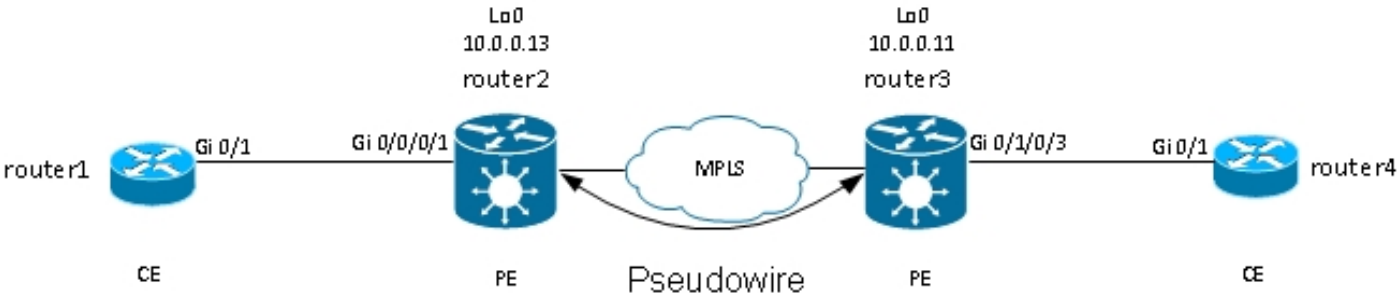
3.4 Árvore de abrangência

Se o CE de L2VPN for um switch Ethernet e estiver enviando BPDUs de spanning tree para o PE de L2VPN, esses BPDUs serão tratados como tráfego regular e serão transportados de acordo com a configuração de L2VPN.

As BPDUs de STP ou MST são enviadas sem marcas e transportadas através da conexão cruzada ponto a ponto se a interface principal estiver configurada como l2transport ou se houver uma subinterface l2transport configurada com os comandos **encapsulation untagged** ou **encapsulation default**.

Per VLAN Spanning Tree Plus (PVST+) ou Rapid PVST+ (PVRST+) enviam BPDUs marcadas que são transportadas se houver uma subinterface l2transport que corresponda à marca dot1q das BPDUs.

Este é um exemplo de topologia:



Router2 e router3 estão transportando quadros e quadros não marcados com dot1q tag 2:

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

O Switch 1 recebe as BPDUs não marcadas na VLAN 1 e as BPDUs marcadas na VLAN 2 do

switch 4; sua porta raiz está em Gi0/1 em direção ao switch 4:

```
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
```

Com essa configuração, o domínio de spanning tree no site A é mesclado com o domínio de spanning tree no lado B. Um possível problema é que a instabilidade do spanning tree em um site pode se propagar para o outro site.

Se você tiver certeza de que um local está conectado apenas por meio de um PW a outro local e de que não há nenhum link de backdoor que possa introduzir um loop físico, é recomendável não executar o spanning tree nos dois locais. Isso mantém os dois domínios de spanning tree isolados. Para fazer isso, configure um bpdufilter spanning tree nos CEs ou configure uma lista de acesso de serviços ethernet nos PEs para descartar quadros com o endereço MAC de destino usado pelos BPDUs. Uma lista de acesso de serviços Ethernet nos PEs pode ser usada para descartar quadros com o MAC de destino de BPDU ou outros tipos de protocolos L2 que você não deseja encaminhar pelo PW.

Esta é uma lista de acesso que você pode usar em cada (sub)interface l2transport que está sendo transportada entre os dois sites:

```
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
!
```

A ACL de serviços Ethernet começa a descartar as BPDUs:

```
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)
```

Switch1 não recebe mais os BPDUs de switch4, portanto switch1 agora é a raiz:

```
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
```

O risco de desativar o spanning tree em um link é este: se uma conexão backdoor é criada entre os sites, ela introduz um loop físico, e o spanning tree não pode quebrar o loop. Assim, quando você desabilitar o spanning tree em um PW, certifique-se de que não haja links redundantes entre os sites e que o PW permaneça a única conexão entre os sites.

Se houver várias conexões entre os sites, use uma solução como VPLS junto com uma versão de gateway de acesso da spanning tree, como MST Access Gateway (MSTAG) ou PVST+ Access Gateway (PVSTAG). Consulte a seção sobre Serviço Multiponto para obter detalhes.

4. Serviço Multiponto

> **Notas:**
>
> Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.
>
> A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

Consulte Implementação de Serviços de Camada 2 Multiponto para obter uma descrição completa dos recursos L2 multiponto.

Com apenas duas interfaces em uma conexão cruzada ponto-a-ponto, um switch L2VPN pega tudo o que é recebido de um lado e o encaminha do outro lado.

Quando há mais de duas interfaces em um domínio de bridge, um switch Ethernet precisa tomar uma decisão de switching para determinar para onde encaminhar os quadros com base no endereço MAC de destino. O switch realiza o aprendizado MAC com base no endereço MAC origem dos quadros que recebe e cria uma tabela de endereços MAC.

O switch encaminha quadros neste método:

- Os quadros de broadcast são inundados para todas as portas. Use o controle de tempestade para limitar a taxa de inundação de broadcast.
- Os quadros multicast são inundados para todas as portas no domínio de bridge, exceto quando o rastreamento de Internet Group Management Protocol (IGMP) ou Multicast Listener Discovery (MLD) está configurado. Use o controle de tempestade para limitar a taxa de inundação de multicast.
- Quadros unicast com um endereço MAC destino que não faz parte da tabela de endereços mac do domínio de bridge (unicast desconhecido) são inundados em todas as portas no

domínio de bridge. Use o controle de tempestade para limitar a taxa de inundação unicast desconhecida.
- Quadros unicast com um endereço MAC destino que faz parte da tabela de endereços mac do domínio de bridge são encaminhados para a porta onde o endereço MAC destino foi aprendido.

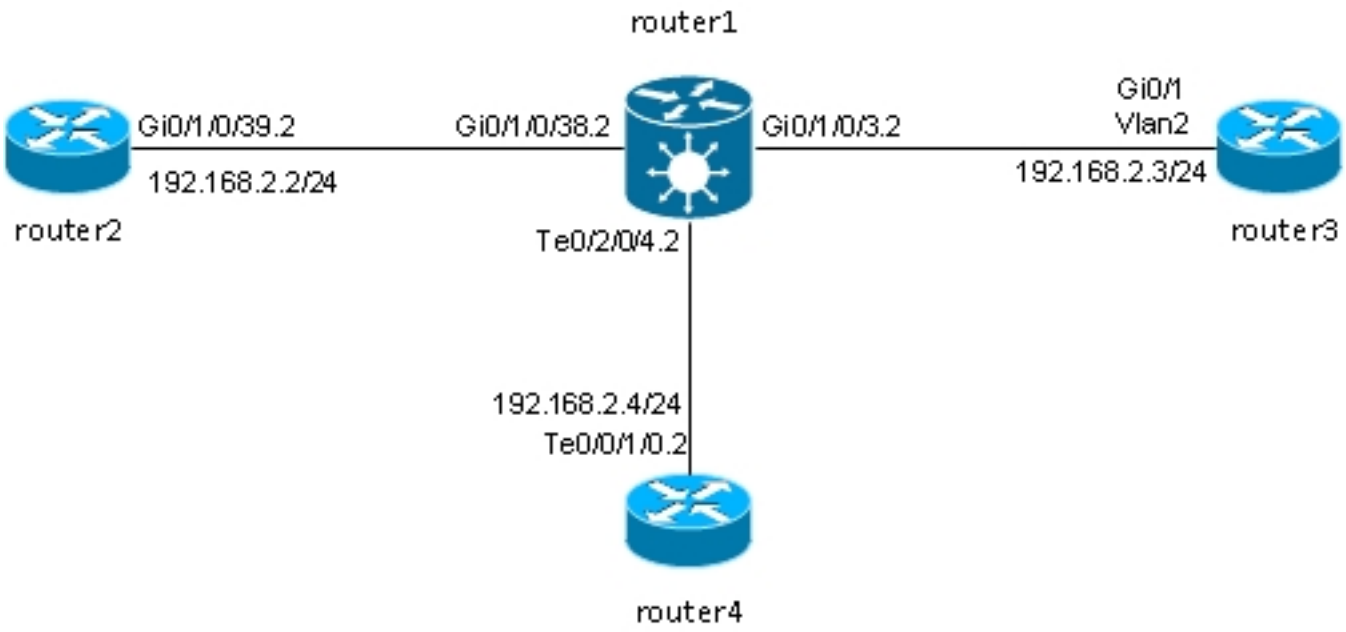
No software Cisco IOS XR, um domínio de broadcast ou uma LAN emulada é chamado de domínio de bridge. Isso é semelhante a uma VLAN na terminologia do software Cisco IOS, exceto que uma VLAN no IOS está vinculada a um número de VLAN que é usado como a marca dot1q nos troncos. Um domínio de bridge no software Cisco IOS XR não está vinculado a um número de tag de VLAN dot1q. Você pode usar o modelo EVC para manipular as tags dot1q e ter subinterfaces dot1q com diferentes números de VLAN dot1q no mesmo domínio de bridge ou para ter interfaces não marcadas.

Um domínio de bridge é basicamente um domínio de broadcast onde broadcasts e quadros multicast são inundados. Uma mac-address-table é associada a cada domínio de bridge (a menos que o aprendizado de MAC seja desabilitado manualmente pela configuração, o que é muito raro). Isso geralmente corresponde a uma sub-rede IPv4 ou IPv6 em que todos os hosts no domínio de bridge estão diretamente conectados.

Os domínios de bridge podem ser agrupados dentro de um grupo de bridge. Essa é uma maneira conveniente de verificar a configuração. Você pode executar um comando show para um grupo de pontes em vez de um comando show para cada domínio de pontes. Um grupo de pontes não tem uma mac-address-table ou outras associações; ele é usado apenas para comandos de configuração e show.

4.1 Comutação local

Este é um exemplo muito básico:



Router2, router3 e router4 estão conectados através de um ASR 9000, que simula uma LAN entre esses três roteadores.

Estas são as configurações de interface nesses três roteadores:

```
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
!
```

Os pacotes são recebidos pelo roteador 1 com a tag dot1q 2 e são encaminhados para os outros roteadores com a tag dot1q 2.

Neste cenário básico, há duas opções nos ACs:

1. Como todos os ACs estão usando a tag dot1q 2, você pode mantê-la no quadro e encaminhar o quadro na interface de saída com a mesma tag dot1q recebida na interface de entrada. O comando **rewrite ingress tag pop 1 symmetric** não é necessário.

2. Você pode abrir a tag dot1q de entrada 2 na direção de entrada e pressionar simetricamente a tag dot1q 2 na direção de saída. Embora isso não seja necessário neste cenário básico, é uma boa ideia configurar o domínio de bridge dessa maneira no início, pois ele fornece mais flexibilidade para o futuro. Aqui estão dois exemplos de alterações que podem ocorrer após a configuração inicial:

   - Se uma interface BVI roteada for introduzida posteriormente no domínio de ponte, os pacotes deverão ser processados no BVI sem marcas. Consulte a seção para obter detalhes.
   - Um novo AC, que usa uma tag dot1q diferente, é adicionado posteriormente. A tag dot1q 2 seria exibida na direção de entrada e a outra tag dot1q seria enviada para a nova

interface na direção de saída e vice-versa.BVI

Descarte as marcas dot1q em cada AC no roteador 1:

```
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
!
```

Visualize a configuração do domínio de bridge com estes três ACs:

```
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
!
!
!
!
```

O domínio de bridge deve ser configurado em um grupo de bridge. Se outros domínios de bridge desse cliente forem necessários, eles poderão ser configurados no mesmo grupo de bridge, customer1. Se novos domínios de bridge pertencerem a um cliente diferente, você poderá criar um novo grupo de bridge. Esses exemplos usam o cliente para agrupar domínios de bridge, mas os domínios de bridge podem ser agrupados por qualquer critério.

Use o comando **show run l2vpn bridge group customer1 bridge-domain engineering** para exibir a configuração do domínio de bridge.

Use o comando **show run l2vpn bridge group customer1** para exibir a configuração de todos os domínios de bridge.

Use o comando **show l2vpn bridge-domain bd-name engineering** ou o comando **show l2vpn bridge-domain group customer1** para exibir informações sobre o domínio de ponte.

```
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:
```

Use o comando **show l2vpn bridge-domain group customer1 bd-name engineering det** se quiser verificar se os pacotes são recebidos e enviados em cada AC.

Adicione a palavra-chave *mac-address* ao comando **show l2vpn forwarding bridge-domain** se quiser verificar a 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
```

O aprendizado de MAC é executado no hardware pelas placas de linha cada vez que um quadro é recebido no domínio de bridge. Há também um cache de software da mac-address-table, mas essa tabela de software não pode ser atualizada continuamente para corresponder às entradas de hardware. Quando o comando **show** é inserido em código recente, ele tenta ressincronizar a tabela de software com a tabela de hardware. Após um máximo de 15 segundos, ele imprime o estado atual do software mac-address-table, mesmo se a ressincronização não estiver completa (por exemplo, se a tabela for grande). Use o comando **l2vpn resynchronize forwarding mac-address-table** para ressincronizar manualmente as tabelas de software e hardware.

```
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
```

Uma mensagem de syslog indica quando o processo de ressincronização está concluído, portanto, é útil ter o **terminal monitor** habilitado para ver a mensagem.

A coluna Resync Age exibe a última vez que o endereço MAC foi ressincronizado a partir da tabela de hardware.

A palavra-chave *location* é o local de uma placa de linha de entrada ou de saída. Os endereços MAC são trocados entre placas de linha no hardware, portanto, os endereços MAC devem ser

conhecidos em cada placa de linha onde houver um AC ou um PW. A palavra-chave *detail* pode fornecer uma versão mais atualizada da tabela de software:

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

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


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

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


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


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

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


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

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

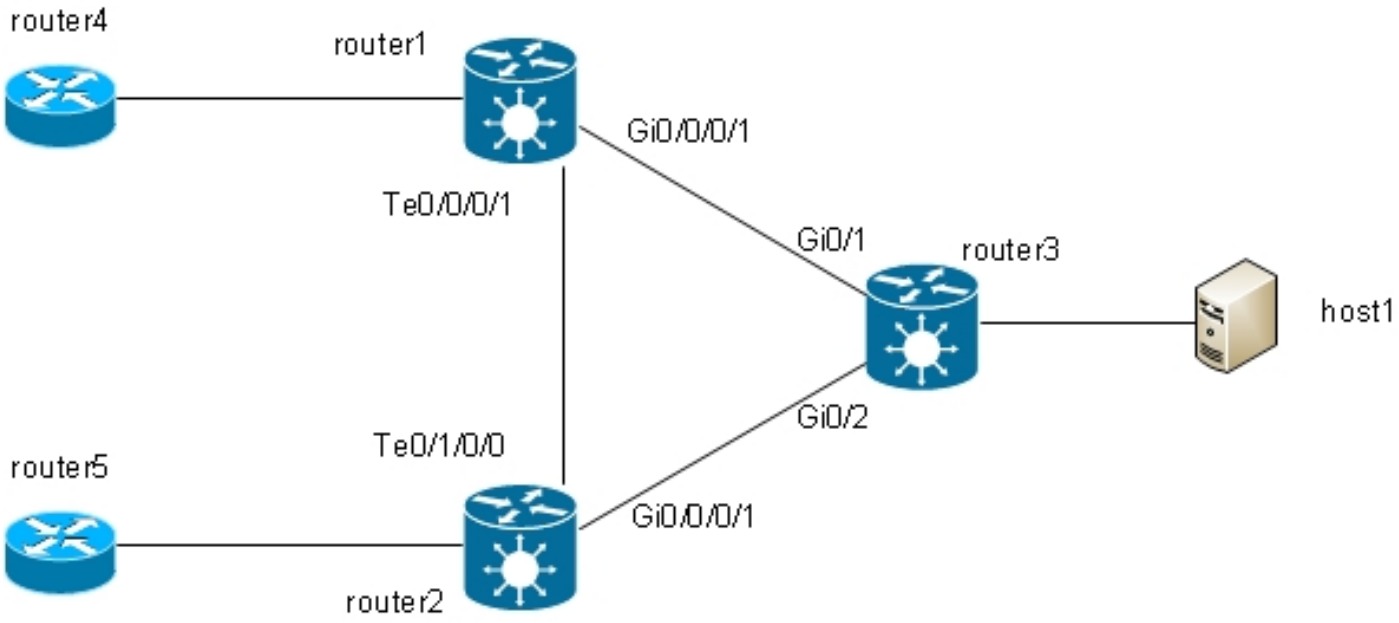
A versão detalhada do comando fornece o número total de endereços MAC aprendidos no domínio de bridge, bem como o número de endereços MAC aprendidos em cada AC.

A palavra-chave *hardware* pesquisa a tabela de endereços MAC do hardware diretamente dos mecanismos de encaminhamento de entrada ou saída:

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

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

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

4.2 MST completo

Os exemplos anteriores de switching local eram básicos porque somente os roteadores estavam conectados ao domínio de bridge. No entanto, quando você começar a conectar switches L2, poderá introduzir um loop e precisar do STP para interromper o loop:



Nessa topologia, router1, router2 e router3 são configurados com um domínio de bridge com todas as suas interfaces no diagrama. Se o roteador 4 enviar um broadcast, como uma solicitação ARP, para o roteador 1, o roteador 1 o despeja para o roteador 2 e o roteador 3, o roteador 2 o despeja para o roteador 3 e o roteador 3 o despeja para o roteador 2. Isso resulta em um loop e uma tempestade de broadcast.

Para interromper o loop, use um STP. Há vários tipos de STPs, mas o software Cisco IOS XR oferece apenas uma implementação completa, o MST.

Há também versões de gateway de acesso dos protocolos suportados no software Cisco IOS XR, como PVSTAG e MSTAG. Essas são versões estáticas e limitadas do protocolo para uso em topologias específicas, normalmente com VPLS, e são descritas nas seções MSTAG e PVSTAG. No software Cisco IOS XR, o MST é a única opção se houver uma topologia com vários switches e se for necessária uma implementação completa do spanning tree.

Duas subinterfaces são configuradas em cada roteador e adicionadas a um domínio de bridge. Para o roteador 1, a configuração é:

```
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
!
!
!
!
```

O MST é configurado na interface principal. Neste exemplo, a VLAN 2 é atribuída à instância 1 e todas as outras VLANs permanecem como a instância padrão 0. (Uma configuração mais realista dividiria as VLANs igualmente entre as instâncias.)

A seleção da bridge raiz dentro de uma rede STP é determinada pela prioridade configurada e pelo ID da bridge incorporada de cada dispositivo. O dispositivo com a prioridade mais baixa, ou com a prioridade mais baixa igual, mas com o ID de bridge mais baixo, é selecionado como a bridge raiz. Neste exemplo, o roteador 3 é configurado com uma prioridade mais baixa do que o roteador 1 para a instância 0, portanto, o roteador 3 é a raiz para a instância 0. Router1 tem uma prioridade mais baixa do que router3 para a instância 1, portanto router1 é a raiz para a instância 1.

Esta é a configuração do roteador 1:

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

Esta é a configuração no roteador 3:

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

O nome, a revisão e o mapeamento de VLAN para ocorrência devem ser os mesmos em todos os switches.

Agora, verifique o status do spanning tree no roteador 1:

```
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
```

Router3 é a raiz da instância 0, portanto router1 tem sua porta raiz em Gi0/0/0/1 em direção a router3. Router1 é a raiz para a instância 1, portanto router1 é a ponte designada em todas as interfaces para essa instância.

Router2 está bloqueado para a instância 0 em 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 encaminhando enquanto Te0/1/0/0.3 está bloqueado. Quando o valor de STP Bloqueado é 0x0, a condição é falsa, então a interface está encaminhando; quando o valor de STP Bloqueado é 0x1, a condição é verdadeira, então a interface é bloqueada.

Use o comando **show uidb data** para confirmar isso e exibir os dados da interface presentes no

processador de rede:

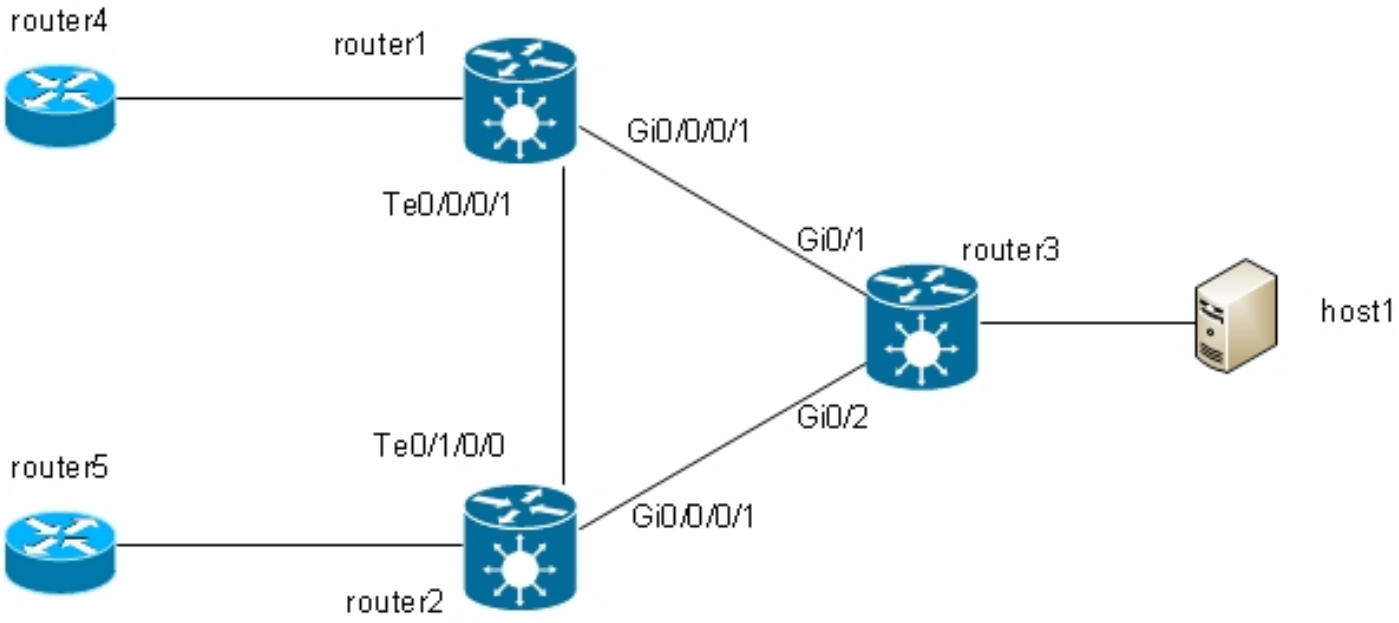
```
RP/0/RSP1/CPU0:router2#sh uidb data location 0/1/CPU0 TenGigE0/1/0/0.2
ingress | i Blocked
STP Blocked                      0x0
RP/0/RSP1/CPU0:router2#sh uidb data location 0/1/CPU0 TenGigE0/1/0/0.3
ingress | i Blocked
STP Blocked                      0x1
```

4,3 BVI

A configuração de um domínio de bridge cria um domínio L2. Para sair desse domínio L2, conecte os roteadores L3 que fazem o roteamento entre os hosts dentro do domínio de bridge e o mundo externo. No diagrama anterior, o host 1 podia usar o roteador 4 ou o roteador 5 para sair da sub-rede local e acessar a Internet.

O Roteador 1 e o Roteador 2 onde os domínios de ponte são configurados são roteadores ASR 9000, que podem rotear tráfego IPv4 e IPv6. Assim, esses dois roteadores poderiam retirar o tráfego IP do domínio de ponte e roteá-lo para a Internet em si, em vez de depender de roteadores L3. Para fazer isso, você precisa configurar um BVI, que é uma interface L3 que se conecta a um domínio de ponte para rotear pacotes dentro e fora do domínio de ponte.

Éassim que se parece logicamente:



Esta é a configuração:

```
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
!
```

Um BVI é uma interface L3 não marcada, portanto, se você quiser que o BVI processe os pacotes recebidos nos ACs do domínio de ponte, os ACs devem ser configurados para remover todas as marcas de entrada. Caso contrário, o BVI não pode entender a marca e descarta os pacotes. Não há como configurar uma subinterface dot1q em um BVI, portanto, as tags devem ser ativadas para ingresso nos ACs como foi feito em Gi0/0/0/1.2 no exemplo anterior.

Como uma interface BVI é uma interface virtual, há algumas restrições quanto aos recursos que podem ser ativados. Essas restrições estão documentadas em Configuração de Integrated Routing and Bridging no Cisco ASR 9000 Series Router: Restrições para Configuração do IRB. Esses recursos não são suportados nas interfaces BVI no ASR 9000:

- Access Control Lists (ACLs). No entanto, as ACLs L2 podem ser configuradas em cada porta L2 do domínio de bridge.
- Redirecionamento rápido de IP (FRR)
- Netflow
- MoFRR (Multicast only Fast Re-Route, Redirecionamento rápido apenas para multicast)
- Switching de rótulo MPLS
- VPNv4
- Quality of Service (QoS)
- Espelhamento de tráfego
- Interface não numerada para BVI
- Monitoramento de vídeo (Vidmon)

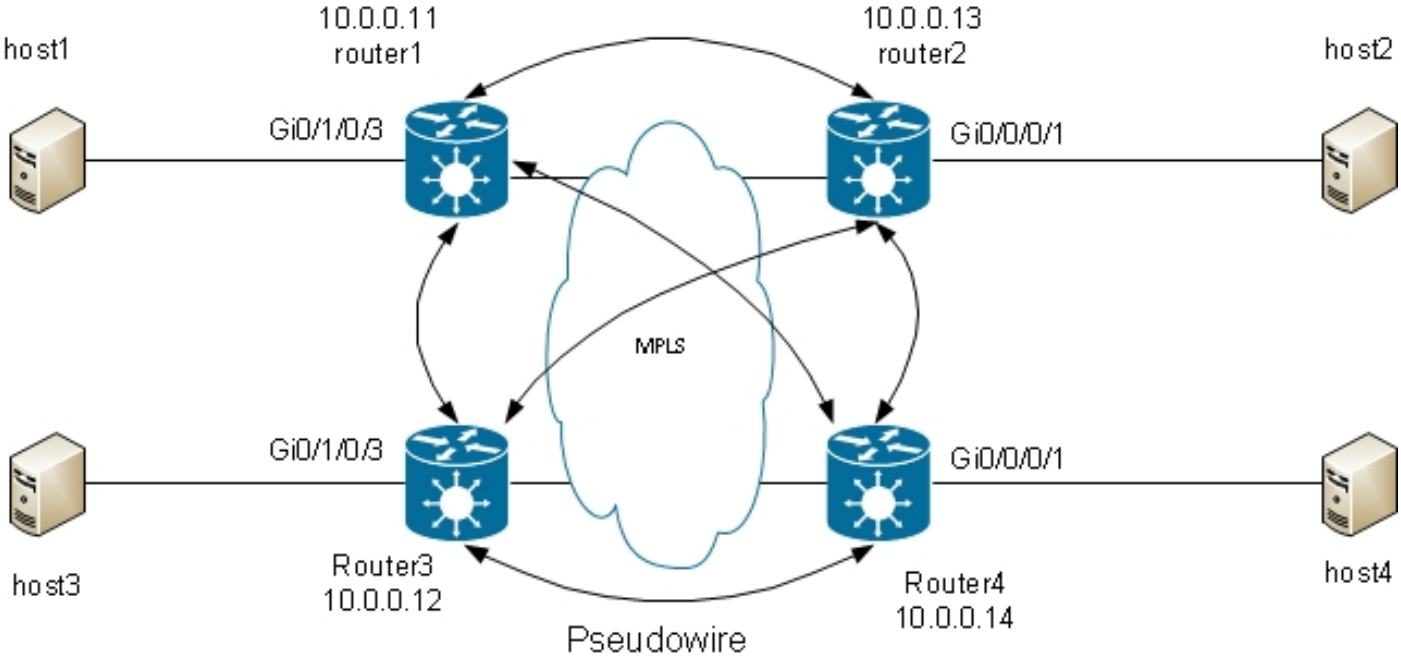
O BVI pode estar em uma configuração Virtual Routing and Forwarding (VRF), de modo que o tráfego recebido no BVI seja encaminhado por MPLS, mas *per-vrf label-allocation-mode* deve ser usado.

Se um desses recursos restritos for necessário, você não poderá usar um BVI. Outra solução é usar um cabo de loopback externo entre duas portas no roteador, onde uma porta está no domínio de bridge e uma porta é configurada como uma interface roteada normal, onde todos os recursos podem ser configurados.

4,4 VPLS

4.4.1 Visão geral

O VPLS oferece a capacidade de combinar domínios de bridge em vários locais em um grande domínio de bridge por meio de PWs MPLS. Os hosts em locais diferentes parecem estar diretamente conectados ao mesmo segmento L2 porque seu tráfego é encapsulado de forma transparente sobre a malha completa de PWs MPLS entre PEs L2VPN:



Uma malha completa de PWs é necessária para garantir que cada host possa receber tráfego de todos os outros hosts. A consequência é que um PE de L2VPN não encaminha um quadro recebido em um PW de VPLS sobre seus outros PWs de VPLS. Deve haver uma malha completa de PWs, para que cada PE receba o tráfego diretamente e não precise encaminhar o tráfego entre PWs, já que o encaminhamento causaria um loop. Isso é chamado de regra de split horizon.

O roteador está executando aprendizagem MAC. Quando um endereço MAC estiver presente na tabela de endereços MAC, você encaminhará somente o quadro para esse endereço MAC de destino sobre o PW para o L2VPN PE no qual esse endereço MAC foi aprendido. Isso evita a duplicação desnecessária de tráfego no núcleo. Os broadcasts e multicasts são inundados em todos os PWs para garantir que todos os hosts possam recebê-los. Um recurso como a espionagem de IGMP é útil porque permite que quadros multicast sejam enviados para PEs somente onde houver receptores ou roteadores multicast. Isso reduz a quantidade de tráfego no núcleo, embora ainda haja várias cópias dos mesmos pacotes que devem ser enviadas a cada PE quando houver interesse para esse grupo.

A malha completa de PWs deve ser configurada em uma Virtual Forwarding Instance (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
!
!
!
!
!
```

Os PWs configurados no VFI são aqueles que estão totalmente engrenados no núcleo. Eles fazem parte do mesmo grupo de split horizon (SHG) para garantir que os quadros recebidos em um PW não sejam encaminhados para outro PW.

Épossível configurar PWs de acesso, que são considerados um tipo de AC e não são configurados no VFI. Consulte a seção para obter detalhes.

A configuração em router2, router3 e router4 é muito semelhante e todos têm os outros três roteadores como vizinhos sob o 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
```

O rótulo local para o PW para 10.0.0.12 é 16049, o que significa que os quadros Ethernet são recebidos com o rótulo 16049. A decisão de comutação é baseada nesse rótulo MPLS porque o penúltimo salto MPLS deve ter estourado o rótulo IGP. Ainda pode haver um rótulo nulo explícito, mas a decisão de switching é baseada no rótulo PW:

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

O comando **show mpls forwarding labels** para o rótulo fornece o número de domínio de ponte, que você pode usar para encontrar o endereço MAC de destino e o PW (vizinho e pw-id) onde o pacote foi recebido. Em seguida, você pode criar entradas na mac-address-table que apontam para esse vizinho:

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

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

4.4.2 Tipos de PW e Tags Transportadas

Os PWs VPLS são negociados como PWs tipo 5 (Ethernet) por padrão. O que quer que entre no AC após qualquer manipulação de tag de VLAN (quando o comando **rewrite** é configurado) é enviado sobre o PW.

O Cisco IOS XR Software Release 4.1.0 para sinalização LDP e Release 4.3.1 com BGP permitem configurar um pw-class em um vizinho e configurar a **passagem de vlan do modo de transporte** em pw-class. Isso negocia um PW de conexão virtual (VC) tipo 4 (Ethernet VLAN), que transporta o que quer que saia do AC após a manipulação de marca de VLAN quando o comando **rewrite** é configurado.

A manipulação de tag de VLAN no EFP garante que haja pelo menos uma tag de VLAN restante

no quadro, pois você precisará de uma tag dot1q no quadro se houver PWs tipo VC 4. Nenhuma tag fictícia 0 é adicionada ao quadro quando você usa o modo **transport mode vlan passthrough**.

Não há suporte para uma combinação de PWs tipo 4 e tipo 5 sob o mesmo VFI. Todos os PWs devem ser do mesmo 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 Autodescoberta e sinalização

Eles foram baseados na configuração manual de todos os vizinhos sob o VFI. O LDP de MPLS foi usado para a sinalização do PW com o vizinho.exemplos anteriores

Quando você adiciona um novo PE de VPLS à rede, configure o PE para ter um PW para todos os PEs existentes em cada um de seus domínios de bridge locais. Todos os PEs existentes devem então ser reconfigurados para ter um PW para o novo PE, pois todos os PEs devem ser totalmente engrenados. Isso pode se tornar um desafio operacional à medida que o número de PEs e domínios de ponte aumenta.

Uma solução é fazer com que os PEs descubram outros PEs automaticamente através do BGP. Embora haja também um requisito de malha completa para o IBGP, ele pode ser levantado pelo uso de refletores de rota. Assim, um novo PE é normalmente configurado para fazer a correspondência com um pequeno número de refletores de rota, todos os outros PEs recebem suas atualizações e o novo PE recebe as atualizações dos outros PEs.

Para descobrir outros PEs através do BGP, cada PE é configurado para a *vpls-vpws address-family* e anuncia no BGP os domínios de bridge em que eles querem participar. Quando os outros PEs que fazem parte do mesmo domínio de bridge são descobertos, um PW é estabelecido para cada um deles. O BGP é o protocolo usado para esta descoberta automática.

Há duas opções para a sinalização do PW para os PEs descobertos automaticamente: BGP e LDP. Nesses exemplos, você converte a topologia anterior em descoberta automática de BGP com sinalização de BGP e sinalização de LDP.

4.4.3.1 Autodescoberta de BGP e sinalização de BGP

Configure a **família de endereços l2vpn vpls-vpws** no roteador bgp e os vizinhos, que são outros PEs ou os refletores de rota:

```
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
!
```

A nova família de endereços se torna ativa com os vizinhos, mas nenhum PE ainda anunciou sua participação em um domínio 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 **autodiscovery bgp** e **signaling-protocol bgp** no modo de configuração de domínio de ponte L2VPN. A configuração no roteador 1 é:

```
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
!
!
!
!
!
!
```

A configuração no roteador 2 é:

```
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
!
```

```
!
!
!
!
!
```

O vpn-id e o route-target são os mesmos nos PEs diferentes para cada domínio de bridge, mas cada PE tem um Identificador de Borda Virtual (VE-ID) exclusivo. Cada PE descobre os outros PEs na VPN através do BGP e usa o BGP para sinalizar os PWs. O resultado é uma malha cheia 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
```

Esses são os prefixos anunciados pelo roteador 3 (10.0.0.13) conforme visto no roteador 1; os prefixos são recebidos através dos dois refletores de rota, 10.0.0.3 e 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
```

O Roteador 1 estabeleceu alguns 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
```

4.4.3.2 Autodescoberta de BGP e sinalização LDP

A configuração de BGP com o comando **address-family l2vpn vpls-vpws** é exatamente a mesma que com a sinalização de BGP. A configuração L2VPN é modificada para usar a sinalização LDP com o comando **signaling-protocol ldp**.

A mesma configuração é usada em todos os quatro PEs:

```
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
!
!
!
!
!
!
```

O vpls-id é composto do número do Sistema Autônomo (AS) do BGP e do vpn-id.

Os três comandos show do roteador 1 ilustram que os PWs foram estabelecidos com os PEs descobertos:

```
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 Liberações e Retiradas de MAC

O encaminhamento no VPLS é baseado na tabela de endereços MAC, que é dinamicamente criada ao aprender os endereços MAC origem dos quadros que estão sendo recebidos. Se houver uma alteração de topologia em um domínio de bridge, um host pode se tornar acessível por meio de um vizinho AC ou VPLS diferente. O tráfego desse host pode não chegar ao seu destino se os quadros continuarem a ser encaminhados de acordo com a tabela de endereços MAC existente.

Para um PE L2VPN, há várias maneiras de detectar uma alteração de topologia:

- Uma porta no domínio de bridge fica ativa ou inativa.
- Um BPDU de notificação de alteração de topologia (TCN) de árvore de abrangência é processado quando o PE L2VPN executa a implementação MST completa ou um protocolo de gateway de acesso de árvore de abrangência. O link com falha pode não ser local no PE, mas pode estar mais distante na topologia. O PE intercepta o TCN.

Quando um PE L2VPN detecta uma alteração de topologia, ele executa duas ações:

1. O PE libera a mac-address-table dos domínios de bridge afetados pela alteração de topologia. Quando o PE é configurado para PVSTAG ou Per-VLAN Rapid Spanning Tree Access Gateway (PVRSTAG), um TCN BPDU detectado em uma subinterface de VLAN afeta todas as VLANs e domínios de bridge nessa interface física.
2. O PE sinaliza para os vizinhos VPLS através de uma mensagem de retirada de MAC LDP de MPLS que eles devem liberar sua tabela de endereços MAC. Todos os PEs L2VPN remotos que recebem a mensagem LDP de retirada de MAC liberam suas tabelas de endereços MAC e o tráfego é inundado novamente. As tabelas de endereços MAC são recriadas com base na nova topologia.

O comportamento padrão da mensagem de retirada MAC no caso de oscilação de porta mudou ao longo do tempo:

- Tradicionalmente, no software Cisco IOS XR, um PE L2VPN enviava mensagens de retirada de MAC quando um AC estava sendo desativado. A intenção era fazer com que os PEs remotos descarregassem suas tabelas de endereços MAC para o domínio de bridge afetado, de modo que os endereços MAC que apontassem para trás da porta inoperante fossem aprendidos de outra porta.

- No entanto, isso criou um problema de interoperabilidade com alguns PEs remotos que seguem o RFC 4762 e expurga os endereços MAC que apontam para todos os PEs, exceto aquele que está enviando a mensagem de retirada de MAC. O RFC 4762 supõe que um PE enviaria uma mensagem de retirada de MAC quando um AC é ativado, mas não quando um AC é desativado. Após o Cisco IOS XR Software Release 4.2.1, o comportamento padrão é enviar mensagens de retirada de LDP MAC somente quando uma porta de domínio de ponte é ativada para melhor cumprir com o RFC. Um comando de configuração foi adicionado para reverter ao comportamento antigo.

Este é um comando show com o comportamento padrão após o Cisco IOS XR Software Release 4.2.1:

```
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:
```

A linha importante é o "MAC draw sent on bridge port down", que agora está desabilitado por padrão após o Cisco IOS XR Software Release 4.2.1. O comando também fornece o número de mensagens de retirada MAC enviadas e recebidas no domínio de bridge. Um número alto de mensagens de retirada indica instabilidade no domínio de bridge.

Esta é a configuração que reverte para o comportamento antigo:

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

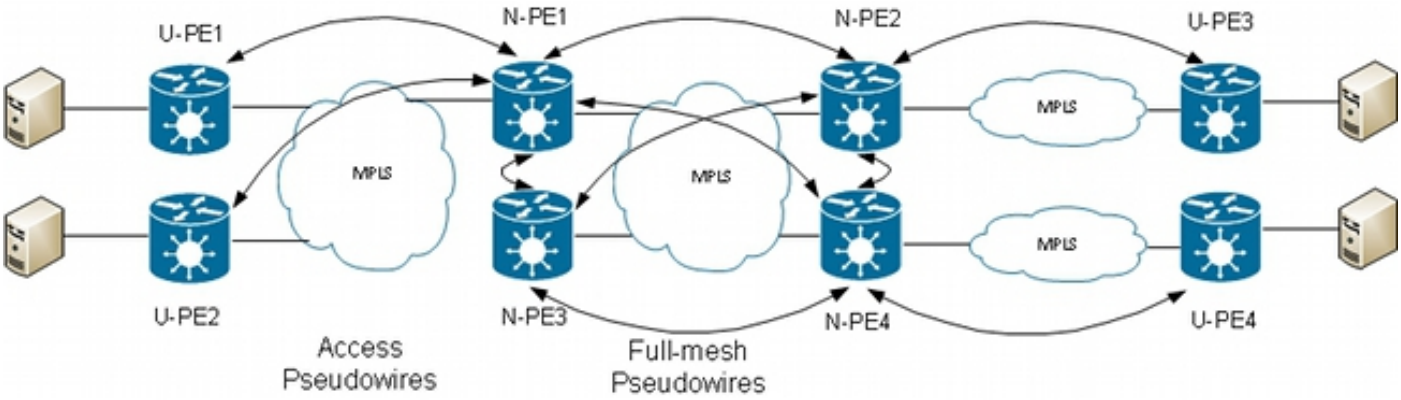
4.4.5 H-VPLS

O VPLS requer uma malha completa de PWs entre os PEs de L2VPN para garantir que qualquer PE possa alcançar, em um salto, um host atrás de qualquer outro PE sem a necessidade de um PE refletir quadros de um PW para outro PW. Essa é a base para a regra do split horizon, que impede que um PE encaminhe quadros de um PW para outro. Mesmo em casos especiais, onde o endereço MAC destino na tabela de endereços MAC aponta para outro PW, o quadro é descartado.

Uma malha completa de PWs significa que o número de PWs pode se tornar muito alto à medida

que o número de PEs cresce, portanto isso pode introduzir problemas de escalabilidade.

Você pode diminuir o número de PWs nessa topologia com uma hierarquia de PEs:



Nessa topologia, observe que:

- Um dispositivo U-PE (Provider Edge) de usuário tem CAs para os CEs.
- O dispositivo U-PE transporta o tráfego CE através de um PW ponto a ponto MPLS para um dispositivo de Borda do Provedor de rede (N-PE).
- O N-PE é um PE VPLS de núcleo que é totalmente engrenado com outros N-PEs.
- No N-PE, o PW proveniente do U-PE é considerado um PW de acesso muito parecido com um AC. O U-PE não faz parte da malha com os outros N-PEs, portanto, o N-PE pode considerar o PW de acesso como um AC e encaminhar o tráfego desse PW de acesso para os PWs do núcleo que fazem parte da malha completa do VPLS.
- Os PWs centrais entre N-PEs são configurados sob um VFI para garantir que a regra do split horizon seja aplicada a todos os PWs centrais configurados sob o VFI.
- Os PWs de acesso dos U-PEs não são configurados em um VFI, portanto, não pertencem ao mesmo SHG que os PWs de VFI. O tráfego pode ser encaminhado de um PW de acesso para um PW de VFI e vice-versa.
- Os U-PEs podem usar o recurso de redundância de PW para ter um PW primário para um N-PE primário e ter um PW standby para um N-PE standby. O standby assume quando o PW principal fica inativo.

Este é um exemplo onde U-PE1 (10.0.0.15) é configurado com redundância PW para N-PE1 (10.0.0.11) e 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
------------------------------------------------------------------------------
```

O PW para 10.0.0.12 está no estado de standby. No N-PE1, há um PW de acesso a 10.0.0.15 e um AC que não estão sob o VFI.

O N-PE1 está aprendendo alguns endereços MAC sobre o PW de acesso e os PWs de VFI:

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

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
```

```
--------------------------------------------------------------------------------
6c9c.ed3e.e46d dynamic (10.0.0.15, 15) 0/0/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A
0024.985e.6a42 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A
001d.4603.1f42 dynamic (10.0.0.13, 2) 0/0/CPU0 0d 0h 0m 0s N/A
```

No N-PE2 (10.0.0.12), o PW de acesso está no estado de standby:

```
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 Split Horizon (SHGs)

A regra do split horizon determina que um quadro recebido em um PW VFI não possa ser encaminhado em outro PW VFI. As NPEs VFI devem ser totalmente engrenadas.

Este split horizon é imposto por meio de um SHG:

- Os membros de um SHG não podem encaminhar quadros entre si, mas podem encaminhar quadros para membros de outros SHGs.
- Todos os PWs VFI são atribuídos ao SHG 1 por padrão. Isso garante que não haja encaminhamento entre PWs de VFI para que a regra de split horizon seja aplicada. Os pacotes recebidos em um PW VFI podem ser encaminhados para ACs e PWs de acesso porque não fazem parte do mesmo SHG.

- Todos os ACs e PWs de acesso não fazem parte de um grupo SHG por padrão, o que significa que os pacotes recebidos em um AC ou PW de acesso podem ser encaminhados para outro AC ou PW de acesso no mesmo domínio de bridge.
- ACs e PWs de acesso podem ser atribuídos ao SHG 2 com o comando **split-horizon group** se o objetivo for evitar o encaminhamento entre eles.

```
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
!
!
!
!
!
```

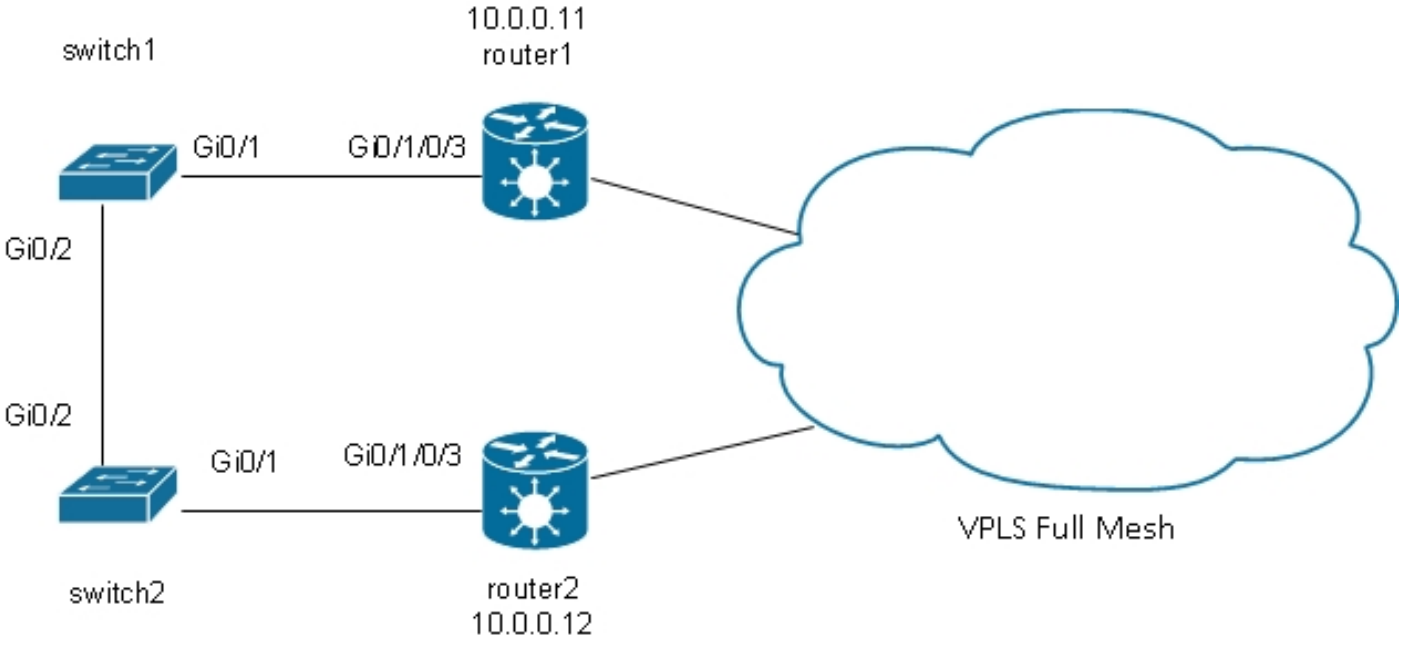
Nessa configuração, não há encaminhamento entre Gi 0/0/1.2 e Gi 0/1/0/3.2, Gi 0/0/0/1.2 e 10.0.0.15, ou Gi 0/1/0/3.2 e 10.0.0.15. Mas ainda pode haver encaminhamento de tráfego entre os ACs e os PWs VFI porque eles fazem parte de SHGs diferentes (1 e 2).

```
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 Redundância

Em uma tentativa de introduzir a redundância, você pode ter um site que esteja duplamente

conectado ao domínio VPLS:



Se um host conectado ao switch 1 envia um broadcast, o switch 1 o encaminha ao roteador 1 e ao switch 2. O Roteador 1 tem uma malha completa de PWs, portanto, há um PW para o Roteador 2 e o Roteador 1 encaminha o broadcast por esse PW. O Roteador 2 encaminha a transmissão para o switch 2, que a encaminha para o switch 1. Isso resulta em um loop físico.

4.4.7.1 Árvore Geradora

A implementação MST completa não funciona com VPLS porque essa implementação envia MST BPDUs em uma interface principal para controlar o estado de encaminhamento de todas as VLANs nessa interface. Com VPLS, existem VFIs para cada domínio de bridge, portanto, não é possível enviar BPDUs em uma interface principal para todas essas VFIs.

Os BPDUs de árvore de abrangência são transportados por VPLS e PWs ponto a ponto por padrão.

Se o switch1 e o switch2 estiverem enviando BPDUs por VLAN ou MST BPDUs não marcados e se as BPDUs corresponderem às subinterfaces l2transport em router1 e router2, as BPDUs serão transportadas através de VPLS. Os switches veem os BPDUs um do outro nas interfaces Gi 0/1 e o spanning tree quebra o loop e bloqueia uma porta.

Switch2 é a raiz da VLAN 2:

```
switch2#sh spanning-tree vlan 2

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

Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
```

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

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

O Switch 1 tem sua porta raiz na Gi 0/1 e está bloqueando a Gi 0/2:

```
switch1#sh spanning-tree vlan 2

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

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

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

O problema é que os BPDUs também são transportados para sites remotos, e a instabilidade do spanning tree em um site se propaga para todos os sites conectados ao domínio VPLS. É mais seguro isolar cada local e não transportar BPDUs sobre VPLS.

Uma solução é o uso de uma versão de gateway de acesso do STP. Essa é uma implementação limitada do protocolo, em que os PEs L2VPN são configurados para enviar alguns BPDUs estáticos a fim de parecerem conectados à raiz do spanning tree. O L2VPN PE não transporta os BPDUs recebidos dos CEs para os sites remotos, portanto cada site tem seu próprio domínio de spanning tree.

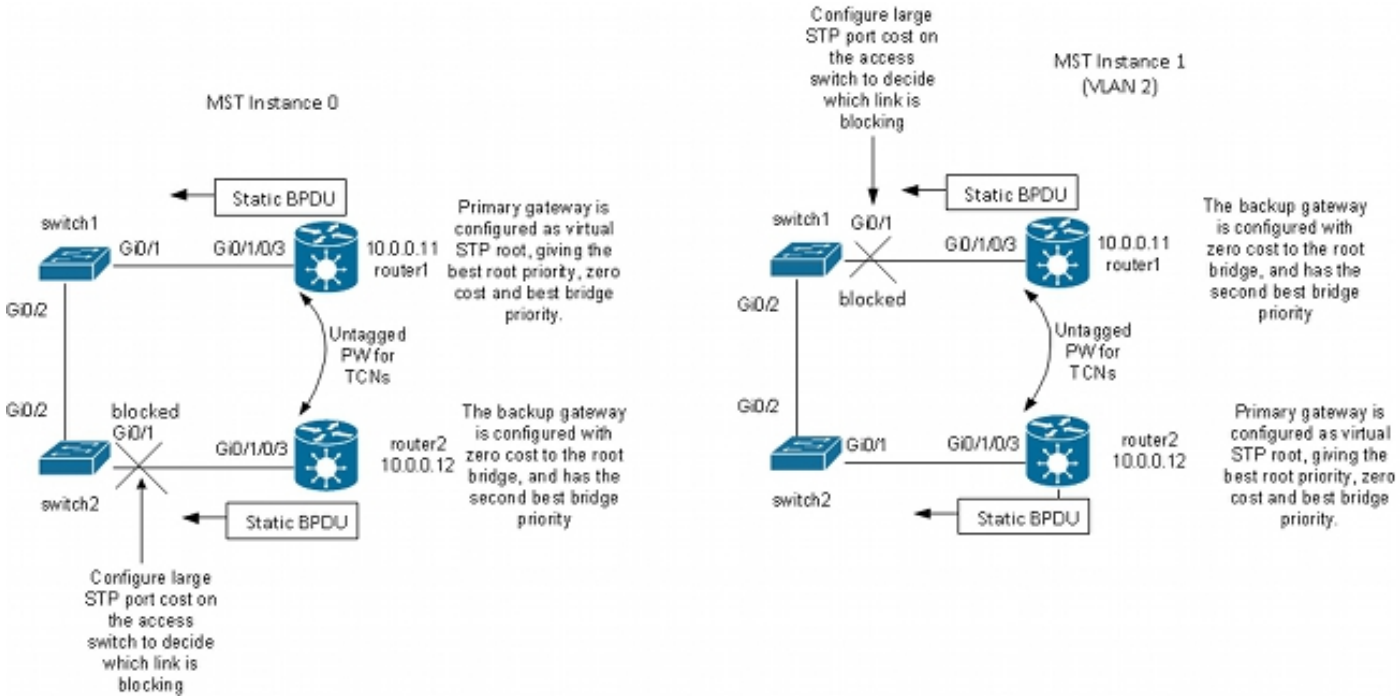
4.4.7.2 MSTAG

Como explicado na seção Spanning Tree, o MST envia BPDUs não marcadas, mas essas BPDUs controlam o estado de encaminhamento de todas as VLANs na interface.

As VLANs podem ser agrupadas em várias instâncias, e cada instância tem seu próprio estado de encaminhamento.

As VLANs são normalmente agrupadas para que o tráfego possa ser distribuído uniformemente entre vários caminhos. Quando há dois caminhos, metade do tráfego pertence a uma instância que está encaminhando no primeiro caminho e bloqueando no segundo caminho. A outra metade do tráfego pertence a uma instância que está bloqueando no primeiro caminho e encaminhando no segundo caminho. Isso permite o balanceamento de carga entre os dois caminhos em condições estáveis. Caso contrário, você terá um caminho que é normalmente bloqueado completamente e se tornará ativo somente quando o caminho principal estiver inativo.

Esta é uma topologia MSTAG típica:



Neste exemplo de laboratório, a instância 1 tem VLAN 2 e a instância 0 tem outras VLANs. (Em um cenário mais realista, as VLANs são distribuídas entre várias instâncias para obter um bom balanceamento de carga de tráfego entre as instâncias.) Como algumas VLANs têm muito mais tráfego do que outras, nem sempre há o mesmo número de VLANs em cada instância.

Esta é a configuração para a instância 0 do MST:

- Router1 e router2 estão enviando algumas BPDUs estáticas com base na configuração MSTAG. Eles não estão processando as BPDUs de entrada da rede ou tentando executar uma implementação completa. Com o MSTAG, os dois PEs L2VPN apenas enviam BPDUs estáticos com base em sua configuração de MSTAG.
- O Roteador 1 é configurado para atrair tráfego da instância 0, parecendo ser a raiz dessa instância.
- O Roteador 2 é configurado com a segunda melhor prioridade de raiz para a instância 0, de modo que ele se torne a nova raiz em caso de falha do Roteador 1 ou falha de CA entre o Switch 1 e o Roteador 1.
- Switch2 é configurado com um alto custo de spanning tree na porta Gi 0/1 para router2 para garantir que seu caminho primário para a raiz esteja no Gig 0/2 através de switch1 e router1.
- Switch2 seleciona Gi 0/2 como porta raiz para instance0 e seleciona Gi 0/1 como uma porta alternativa, caso a raiz seja perdida.
- Assim, o tráfego desse site nas VLANs pertencentes à instância 0 alcança outros sites sobre VPLS através do roteador 1.

Para a instância 1 do MST (VLAN 2), a configuração é revertida:

- O Roteador 2 é configurado para atrair tráfego da instância 1, parecendo ser a raiz dessa instância.
- O Roteador 1 é configurado com a segunda melhor prioridade de raiz para a instância 1, de modo que ele se torne a nova raiz em caso de falha do Roteador 2 ou falha de CA entre o Switch 2 e o Roteador 2.
- O Switch 1 é configurado com um alto custo de spanning tree na porta Gi 0/1 para o roteador

1 para garantir que seu caminho principal para a raiz esteja no Gig 0/2 através do switch 2 e do roteador 2.

- O Switch 1 seleciona Gi 0/2 como porta raiz para a instância 1 e seleciona Gi 0/1 como uma porta alternativa, caso a raiz seja perdida.
- Assim, o tráfego desse site nas VLANs pertencentes à instância 1 (VLAN 2 neste exemplo) alcança outros sites sobre VPLS através do roteador 2.
- Deve haver uma subinterface em router1 e router2 para capturar os TCNs não marcados e encaminhá-los através de um PW ponto a ponto para o outro roteador. Como o switch1 e o switch2 podem perder seus links diretos e se isolar um do outro, o roteador1 e o roteador2 devem encaminhar os TCNs entre eles através desse PW ponto a ponto.
- Os PEs também interceptam os TCNs, liberam suas tabelas de endereços MAC e enviam a retirada de LDP MAC para PEs remotos.

Esta é a configuração no roteador 1:

```
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
```

Nesta configuração, observe que:

- Na instância 0 do MST, a bridge raiz é 0000.0000.0001, que é o ID da bridge do roteador 1.
- Na instância 1 do MST, a bridge raiz é 0000.0000.0002, que é o ID da bridge do roteador 2.
- A prioridade de bridge do roteador 1 é 4096 na instância 0 (para se tornar a raiz) e 8192 na instância 1 (para se tornar a segunda melhor raiz).
- A prioridade de bridge do roteador 1 é 8192 na instância 0 (para se tornar a segunda melhor raiz) e 4096 na instância 1 (para se tornar a raiz).
- A conexão cruzada ponto a ponto em GigabitEthernet0/1/0/3.1 transporta os TCNs MST não marcados para o outro roteador.

Uma ACL de saída foi configurada nas subinterfaces dot1q para descartar BPDUs por VLAN que podem ser enviadas por outro site que ainda não foi migrado para o MST. Essa configuração impede que o switch CE declare que a interface está inconsistente quando recebe um BPDU por VLAN em uma interface configurada para MST.

A configuração no roteador 2 é muito semelhante:

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

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

```
!
!
!

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

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

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

```
Root Priority: 4096
Topology Changes: 177
```

Esta é a configuração básica no 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
```

Assim, o tráfego na instância 0 é encaminhado através do roteador 1 e o tráfego na instância 1 é encaminhado através do switch 2 e do roteador 2.

A configuração no switch2 usa os mesmos comandos que o 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
```

Switch2 passa por switch1 e roteador1 para a instância0 e por roteador2 para a instância1.

O tráfego tem balanceamento de carga porque uma instância sai do site através do roteador 1 e a outra instância sai do site através do roteador 2.

Se o link entre o roteador 1 e o switch 1 estiver inoperante, ambas as instâncias passarão pelo roteador 2.

```
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
```

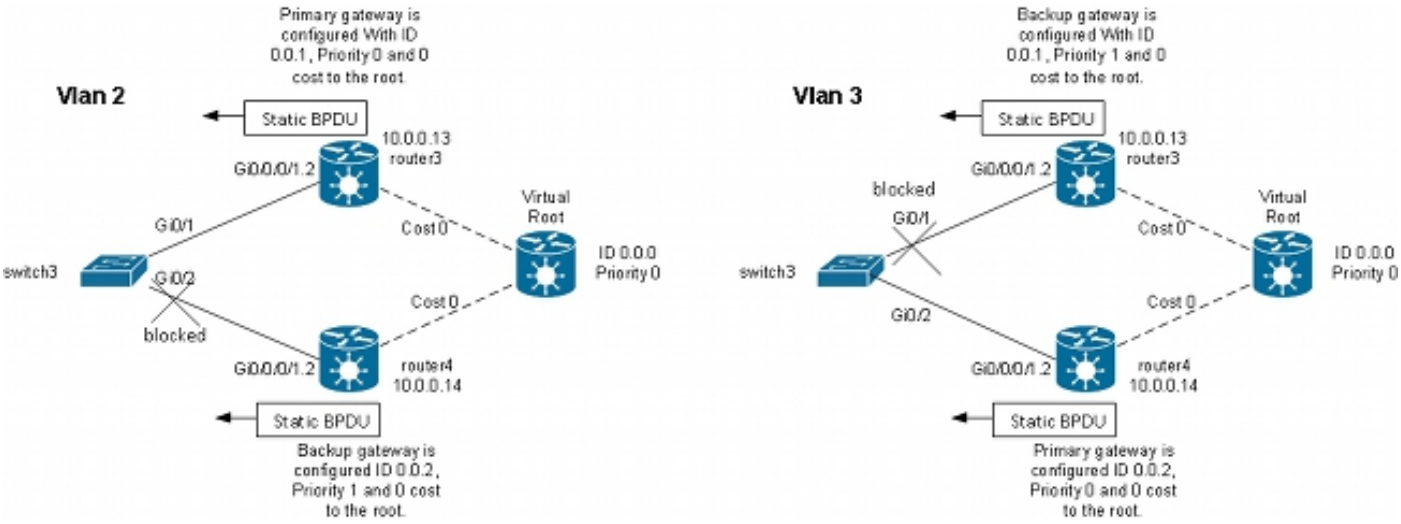
```
Interface Role Sts Cost Prio.Nbr Type
------------------ ---- --- --------- -------- ------------------------------
Gi0/1 Root FWD 20000 128.1 P2p
Gi0/2 Desg FWD 20000 128.2 P2p
```

A convergência rápida pode ser alcançada nesse tipo de falha porque o caminho através da segunda melhor raiz já foi selecionado como o caminho alternativo. Com o MSTAG, as BPDUs do MST não são transportadas por VPLS, de modo que os locais são isolados da instabilidade em outros locais.

4.4.7.3 PVSTAG ou PVRSTAG

O MSTAG é o protocolo de gateway de acesso preferencial para VPLS porque usa a árvore de abrangência rápida e porque é escalável com o uso de instâncias em vez de BPDUs em cada VLAN.

Se um site não puder ser migrado para o MST e a única solução for continuar executando o PVST+ ou o PVRST, você poderá usar o PVSTAG ou o PVRSTAG, mas a implementação será limitada a uma topologia específica:



Nessa topologia, a restrição mais importante é que pode haver apenas um switch CE. Você não pode ter dois switches como na topologia MSTAG. No MSTAG, você pode configurar um PW ponto a ponto para transportar o tráfego não marcado (incluindo os TCNs de BPDU) de um PE para outro quando o site é dividido em duas partes. Com o PVST e o PVRST, os TCNs são enviados marcados para que correspondam à mesma subinterface do tráfego de dados a ser transportado sobre VPLS. O roteador teria que identificar os BPDUs com base no endereço MAC e no tipo de protocolo para encaminhar os TCNs para o outro lado. Como isso não é suportado atualmente, há um requisito para ter apenas um dispositivo CE.

Outro requisito em versões anteriores ao Cisco IOS XR Software Release 4.3.0 é que as interfaces do pacote não podem ser usadas como ACs. Essa restrição foi eliminada no Cisco IOS XR Software Release 4.3.0.

O princípio é praticamente o mesmo que no caso do MSTAG. O roteador PVSTAG envia BPDUs estáticas para que o CE pareça estar conectado a switches que estão diretamente conectados à raiz (virtual) com um custo 0. Para fazer o balanceamento de carga do tráfego, algumas VLANs podem ser configuradas com a raiz no roteador3 e outras com a raiz no roteador4.

Este é um exemplo de configuração no roteador 3:

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

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

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

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

Este é um exemplo de configuração no roteador 4:

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

RP/0/RSP1/CPU0:router4#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/0/0/1.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
!
!
bridge-domain engineering
interface GigabitEthernet0/0/0/1.2
!
```

```
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
!
!
!
!

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

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

Este é um exemplo de configuração no switch CE3:

```
switch3#sh spanning-tree vlan 2

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

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

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

switch3#sh spanning-tree vlan 3

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

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

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

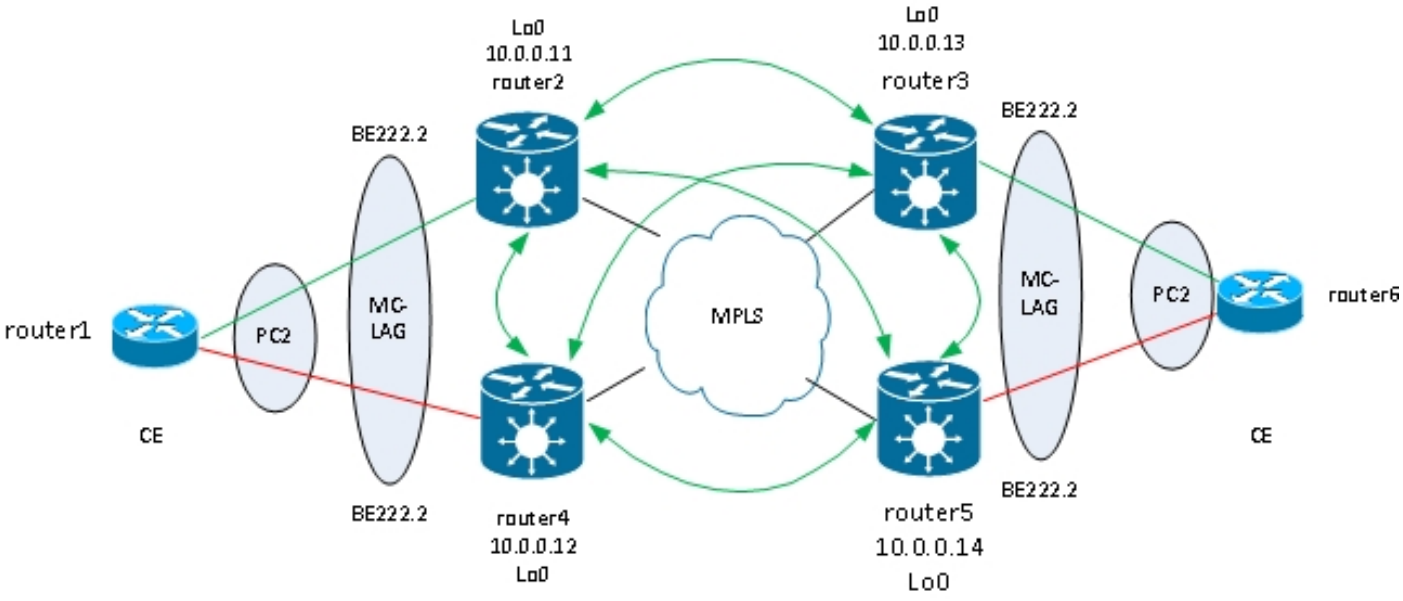
A configuração do PVSTAG é muito semelhante à do MSTAG, exceto que a prioridade de raiz e a prioridade do gateway primário são configuradas como 4096 e a prioridade do gateway de backup é configurada como 8192 no exemplo do MSTAG.

Todos os outros switches nos domínios devem ter prioridades maiores do que as configuradas no PVSTAG ou PVRSTAG.

Você pode ajustar o custo da interface nos switches CE para influenciar qual porta se torna a porta raiz e qual porta é bloqueada.

4.4.7.4 LAG DE MC

A configuração MC-LAG com VPLS é mais simples do que PWs ponto a ponto com redundância PW bidirecional. Em vez de um PW principal e três PWs em espera, os PEs precisam apenas de uma malha completa de PWs VPLS, que é padrão com VPLS:



Nessa topologia, observe que:

- O MC-LAG é executado entre os dois PEs VPLS à esquerda: router2 e router4.
- Em condições normais, os membros do pacote estão ativos entre o roteador 1 e o roteador 2 e em estado de espera entre o roteador 1 e o roteador 4.
- O Roteador2 tem as subinterfaces do pacote configuradas nos domínios de ponte VPLS, portanto o Roteador2 encaminha o tráfego para PEs VPLS remotos. Há dois locais ilustrados no diagrama de topologia, mas pode haver muitos outros.
- Os PEs remotos aprendem os endereços MAC do roteador 1 e os dispositivos atrás do roteador 2, portanto os PEs encaminham o tráfego para esses endereços MAC de destino através do roteador 2.
- Quando o link entre o roteador 1 e o roteador 2 é desativado ou quando o roteador 2 é desativado, o membro do pacote entre o roteador 1 e o roteador 4 fica ativo.
- Como o roteador 2, o roteador 4 tem suas subinterfaces de pacote configuradas em domínios de bridge VPLS.
- Quando as subinterfaces do pacote surgem no roteador 4, o roteador 4 envia mensagens de retirada de LDP MAC para os PEs de VPLS remotos para informá-los de que há uma alteração de topologia.

Esta é a configuração no roteador 3:

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

```
isolation recovery-delay 300
!
!
!

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

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

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

Depois que o pacote MC-LAG estiver configurado, adicione-o na configuração VPLS como qualquer outro AC.

Esta é a configuração correspondente no roteador 5:

```
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
!
!
!
!
!
```

Em circunstâncias normais, o membro do pacote entre o roteador3 e o roteador6 está ativo e o membro entre o roteador5 e o roteador6 está no estado de standby:

```
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#
```

O tráfego do CE é recebido no roteador 3 e encaminhado para PEs remotos:

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

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

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

O último comando ilustra que o roteador3 está aprendendo alguns endereços MAC em seu pacote e os membros ativos estão no roteador3. No roteador 5, não há nenhum endereço MAC aprendido no pacote, pois o membro local está no estado de standby:

```
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
```

Quando o membro do pacote entre o roteador3 e o roteador6 é desativado, o membro do pacote torna-se ativo no roteador5. Os PEs de VPLS MC-LAG enviam uma mensagem de retirada de LDP MAC para que os PEs remotos limpem suas tabelas de endereços MAC e aprendam o endereço MAC por meio do novo roteador MC-LAG PE5 ativo.

O Roteador 2 recebe mensagens de MAC de retirada do roteador 3 e do roteador 5 quando o membro ativo do pacote MC-LAG se move do roteador 3 para o roteador 5:

```
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
```

Os endereços MAC no roteador 2 se movem do roteador 3 (10.0.0.13) para o roteador 5 (10.0.0.14):

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

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

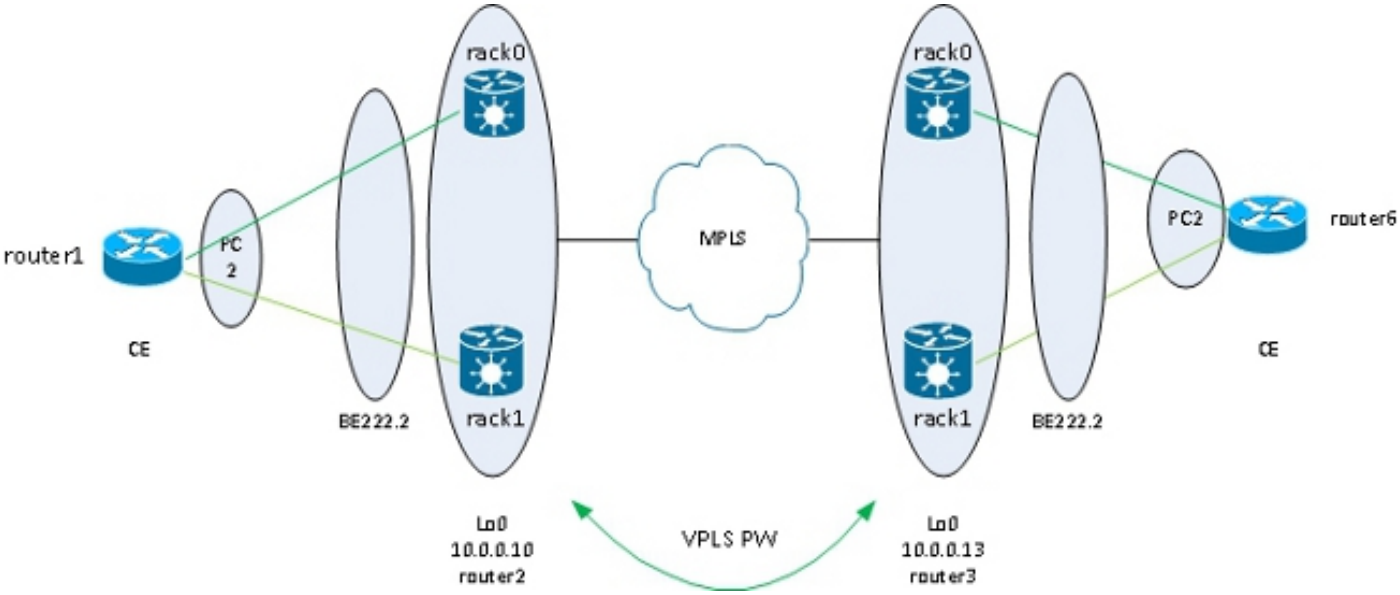
Com o MC-LAG, um local pode usar um único pacote para ser conectado aos outros locais através do VPLS. O MC-LAG fornece o link e a redundância PE, mas logicamente ainda é uma interface de pacote para acessar outros sites. A árvore de abrangência não é necessária nesse pacote, e um filtro de BPDU pode ser configurado no CE para garantir que BPDUs não sejam trocadas entre locais por VPLS.

Outra opção é a configuração de uma lista de acesso de serviços Ethernet nos ACs no pacote para descartar os endereços MAC de destino dos BPDUs para que os BPDUs não sejam transportados entre sites. No entanto, se um link backdoor for introduzido entre os sites, o spanning tree não poderá quebrar o loop porque ele não está sendo executado no pacote MC-LAG. Portanto, avalie cuidadosamente se o spanning tree deve ser desativado no pacote MC-LAG. Se a topologia entre os locais for cuidadosamente mantida, é bom ter redundância através de MC-LAG sem a necessidade de spanning tree.

4.4.7.5 Cluster de borda ASR 9000 nV

A solução MC-LAG forneceu redundância sem a necessidade de usar spanning tree. Uma desvantagem é que os membros do pacote para um PE MC-LAG estão no estado de standby, portanto, é uma solução ativa em standby que não maximiza o uso do link.

Outra opção de design é o uso de um cluster ASR 9000 nV Edge para que os CEs possam ter membros de pacote em cada rack de cluster que estejam ativos ao mesmo tempo:



Outro benefício dessa solução é que o número de PWs é reduzido porque há apenas um PW por cluster para cada um dos clusters em cada local. Quando há dois PEs por local, cada PE deve ter um PW para cada um dos dois PEs em cada local.

A simplicidade da configuração é outro benefício. A configuração se parece com uma configuração VPLS muito básica com um domínio de ponte com conjuntos de ACs e PWs VFI:

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

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

```
Flap suppression timer: Off
Cisco extensions: Disabled
mLACP: Not configured
IPv4 BFD: Not configured

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

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

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

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

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

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

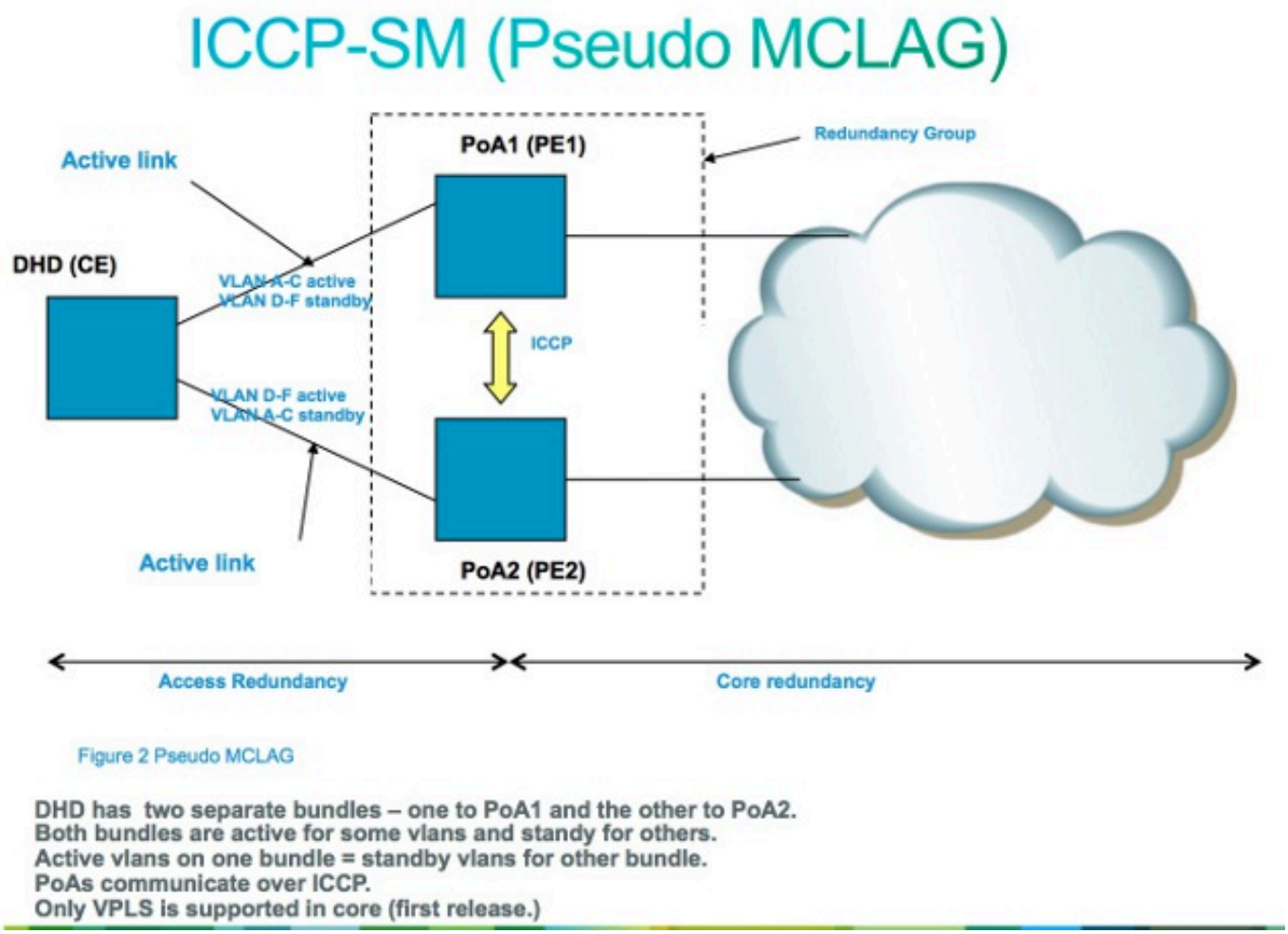
A redundância é fornecida pelo pacote AC dual homed para os dois racks de modo que o pacote permaneça ativo em caso de falha do membro do pacote ou do rack.

Quando um local é anexado ao domínio VPLS apenas por meio de um cluster, a topologia é semelhante ao MC-LAG com relação ao spanning tree. Portanto, o spanning tree não é necessário nesse pacote, e um filtro de BPDU pode ser configurado no CE para garantir que BPDUs não sejam trocadas entre locais através de VPLS.

Outra opção é a configuração de uma lista de acesso de serviços Ethernet nos ACs no pacote para descartar os endereços MAC de destino dos BPDUs para que os BPDUs não sejam transportados entre sites. No entanto, se um link backdoor for introduzido entre os sites, o spanning tree não poderá quebrar o loop porque ele não está sendo executado no pacote CE-PE. Portanto, avalie cuidadosamente se o spanning tree deve ser desativado nesse pacote CE-PE. Se a topologia entre os locais for cuidadosamente mantida, é bom ter redundância através do cluster sem a necessidade de spanning tree.

4.4.7.6 Hospedagem Múltipla de Serviços Baseada em ICCP (ICCP-SM) (PMCLAG (Pseudo-MCLAG) e Ativo/Ativo)

Há um novo recurso introduzido na versão 4.3.1 a fim de superar a limitação do MC-LAG, onde alguns links de pacotes não são usados, pois permanecem no modo de espera. No novo recurso, chamado *Pseudo MCLAG*, todos os links do DHD para os Pontos de Anexação (PoAs) estão em uso, mas as VLANs são divididas entre os diferentes pacotes:



4.5 Controle de Tempestade de Tráfego

Em um domínio de broadcast L2, há o risco de um host se comportar mal e enviar uma alta taxa de quadros de broadcast ou multicast que devem ser inundados em todo o domínio de bridge. Outro risco é a criação de um loop de L2 (que não é interrompido pelo spanning tree), que resulta em looping de pacotes de broadcasts e multicasts. Uma alta taxa de broadcasts e pacotes multicasts afeta o desempenho dos hosts nos domínios de broadcast.

O desempenho dos dispositivos de switching na rede também pode ser afetado pela replicação de um quadro de entrada (broadcast, multicast ou um quadro unicast desconhecido) para várias portas de saída no domínio de bridge. A criação de várias cópias do mesmo pacote pode consumir muitos recursos, dependendo do local dentro do dispositivo onde o pacote precisa ser replicado. Por exemplo, a replicação de um broadcast para vários slots diferentes não é um problema devido aos recursos de replicação multicast da malha. O desempenho de um processador de rede pode ser afetado quando tiver que criar várias cópias do mesmo pacote para serem enviadas em algumas portas que o processador de rede está tratando.

Para proteger dispositivos em caso de tempestade, o recurso de controle de tempestade de tráfego permite configurar uma taxa máxima de broadcasts, multicast e unicasts desconhecidos para serem aceitos em um AC de domínio de bridge. Consulte o Guia de Configuração de Segurança do Sistema do Roteador de Serviços de Agregação Cisco ASR 9000 Series, Release 4.3.x: Implementing Traffic Storm Control under a VPLS Bridge para obter detalhes.

O controle de tempestade de tráfego não é suportado em um pacote de interfaces AC ou PWs

VFI, mas é suportado em ACs e PWs de acesso sem pacote. O recurso é desativado por padrão; a menos que você configure o storm control (controle de tempestade), você aceita qualquer taxa de broadcasts, multicast e unicasts desconhecidos.

Aqui está um exemplo de configuração:

```
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>
```

Os contadores de queda do storm control estão sempre presentes na saída do comando **show l2vpn bridge-domain detail**. Como o recurso está desabilitado por padrão, os contadores começam a relatar quedas somente quando o recurso foi configurado.

As taxas configuradas podem variar de acordo com o padrão de tráfego de uma rede para outra. Antes de configurar uma taxa, a Cisco recomenda que você compreenda a taxa de quadros de broadcast, multicast ou unicast desconhecido sob circunstâncias normais. Em seguida, adicione uma margem na taxa configurada acima da taxa normal.

4.6 Mudanças de MAC

Em caso de instabilidade da rede, como uma oscilação de interface, um endereço MAC pode ser aprendido de uma nova interface. Essa é a convergência de rede normal, e a tabela de endereços mac é atualizada dinamicamente.

No entanto, as constantes movimentações de MAC frequentemente indicam instabilidade da rede, como instabilidade grave durante um loop de L2. O recurso de segurança de endereço MAC permite que você relate movimentações de endereços MAC e tome ações corretivas, como o desligamento de uma porta ofensiva.

Mesmo que uma ação corretiva não esteja configurada, você pode configurar o comando **logging**

para ser alertado sobre a instabilidade da rede através das mensagens de movimentação de MAC:

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

Neste exemplo, a ação é configurada para nenhum, portanto, nada é feito quando uma movimentação de MAC é detectada, exceto que uma mensagem de syslog é registrada. Esta é uma mensagem de exemplo:

```
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 Snooping IGMP e MLD

Por padrão, os quadros multicast são inundados para todas as portas em um domínio de bridge. Quando você estiver usando fluxos de alta taxa, como serviços de televisão IP (IPTV), pode haver uma quantidade significativa de tráfego encaminhado em todas as portas e replicado em vários PWs. Se todos os fluxos de TV forem encaminhados em uma interface, isso poderá congestionar portas. A única opção é a configuração de um recurso como o IGMP ou o snooping MLD, que intercepta pacotes de controle multicast para rastrear os receptores e roteadores multicast e encaminhar fluxos nas portas somente quando apropriado.

Consulte o Guia de Configuração Multicast do Cisco ASR 9000 Series Aggregation Services Router, Release 4.3.x para obter mais informações sobre esses recursos.

5. Tópicos L2VPN Adicionais

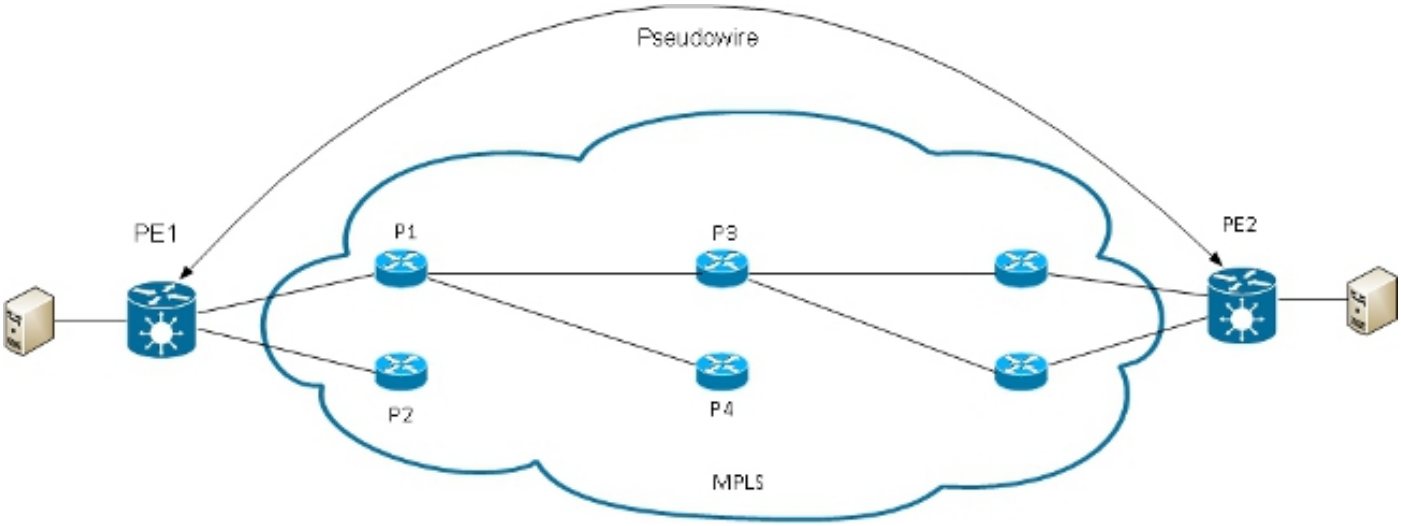
> **Notas:**
>
> Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.
>
> A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

5.1 Balanceamento de carga

Quando um PE L2VPN precisa enviar um quadro sobre um PW MPLS, o quadro Ethernet é

encapsulado em um quadro MPLS com um ou mais rótulos MPLS; há pelo menos um rótulo PW e talvez um rótulo IGP para alcançar o PE remoto.

O quadro MPLS é transportado pela rede MPLS para o L2VPN PE remoto. Normalmente, há vários caminhos para alcançar o PE de destino:



Observação: nem todos os links são representados neste diagrama.

O PE1 pode escolher entre P1 e P2 como o primeiro roteador MPLS P em direção ao PE2. Se P1 estiver selecionado, PE1 então escolhe entre P3 e P4, e assim por diante. Os caminhos disponíveis são baseados na topologia IGP e no caminho do túnel MPLS TE.

Os provedores de serviços MPLS preferem ter todos os links igualmente utilizados em vez de um link congestionado com outros links subutilizados. Esse objetivo nem sempre é fácil de alcançar porque alguns PWs transportam muito mais tráfego do que outros e porque o caminho tomado por um tráfego PW depende do algoritmo de hash usado no núcleo. Vários PWs de alta largura de banda podem ser divididos em hash para os mesmos links, o que cria congestionamento.

Um requisito muito importante é que todos os pacotes de um fluxo sigam o mesmo caminho. Caso contrário, os quadros ficarão fora de ordem, o que pode afetar a qualidade ou o desempenho dos aplicativos.

O balanceamento de carga em uma rede MPLS em roteadores Cisco geralmente é baseado nos dados que seguem o rótulo MPLS inferior.

- Se os dados imediatamente após o rótulo inferior começarem com 0x4 ou 0x6, um roteador IP MPLS assumirá que há um pacote IPv4 ou IPv6 dentro do pacote MPLS e tentará fazer o balanceamento de carga com base em um hash dos endereços IPv4 ou IPv6 origem e destino extraídos do quadro. Teoricamente, isso não deve ser aplicado a um quadro Ethernet que é encapsulado e transportado por um PW, pois o endereço MAC de destino segue o rótulo inferior. Recentemente, alguns intervalos de endereços MAC que começam com 0x4 e 0x6 foram atribuídos. O roteador IP MPLS pode considerar incorretamente que o cabeçalho Ethernet é na verdade um cabeçalho IPv4 e aplicar hash ao quadro com base no que ele supõe serem os endereços de origem e destino IPv4. Os quadros Ethernet de um PW podem ser divididos em hash em diferentes caminhos no núcleo MPLS, o que leva a quadros fora de sequência no PW e problemas de qualidade de aplicativo. A solução é a configuração de uma

palavra de controle em uma classe de PW que pode ser anexada a um PW ponto a ponto ou VPLS. A palavra de controle é inserida imediatamente após os rótulos MPLS. A palavra de controle não começa com 0x4 ou 0x6, portanto, o problema é evitado.

```
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)
------------ ------------------------------ ------------------
```

- Se os dados imediatamente após a parte inferior da pilha de rótulos MPLS não começarem com 0x4 ou 0x6, o roteador P fará o balanceamento de carga com base no rótulo inferior. Todo o tráfego de um PW segue o mesmo caminho, portanto, não ocorrem pacotes fora de ordem, mas isso pode levar a congestionamento em alguns links em caso de PWs de largura de banda alta. Com o Cisco IOS XR Software Release 4.2.1, o ASR 9000 suporta o recurso PW Flow Aware Transport (FAT). Esse recurso é executado nos PEs L2VPN, onde é negociado entre as duas extremidades de um PW ponto a ponto ou VPLS. O PE de L2VPN de entrada detecta fluxos na configuração de AC e L2VPN e insere um novo rótulo de fluxo de MPLS abaixo do rótulo MPLS de PW na parte inferior da pilha de rótulos de MPLS. O PE

de entrada detecta fluxos com base nos endereços MAC origem e destino (padrão) ou nos endereços IPv4 origem e destino (configuráveis). O uso dos endereços MAC é o padrão; o uso de endereços IPv4 é recomendado, mas deve ser configurado manualmente.

Com o recurso FAT PW, o L2VPN PE de entrada insere um rótulo MPLS inferior por src-dst-mac ou por src-dst-ip. Os roteadores P de MPLS (entre os PEs) criam quadros de hash nos caminhos disponíveis e, em seguida, alcançam o PE de destino com base no rótulo de fluxo de PW FAT na parte inferior da pilha de MPLS. Isso geralmente fornece uma utilização de largura de banda muito melhor no núcleo, a menos que um PW transporte apenas um pequeno número de conversações src-dst-mac ou src-dst-ip. A Cisco recomenda que você use uma palavra de controle para evitar ter endereços MAC que começam com 0x4 e 0x6 imediatamente após o rótulo de fluxo. Isso garante que o hash seja baseado corretamente nos pseudo-endereços IP e não no rótulo de fluxo.

Com esse recurso, o tráfego de um PW tem balanceamento de carga em vários caminhos no núcleo, quando disponível. O tráfego de aplicativos não sofre com pacotes fora de ordem porque todo o tráfego da mesma origem (MAC ou IP) para o mesmo destino (MAC ou IP) segue o mesmo caminho.

Este é um exemplo de configuração:

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


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

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ -----------------
Label 281708 16043
```

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

5.2 Registro

Diferentes tipos de mensagens de registro podem ser configurados no modo de configuração L2VPN. Configure o log l2vpn para receber alertas de syslog para eventos L2VPN e configure o pseudofio de log para determinar quando um status PW é alterado:

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

Se muitos PWs estiverem configurados, as mensagens podem inundar o registro.

5.3 lista de acesso de serviços ethernet

Você pode usar uma lista de acesso de serviços ethernet para descartar o tráfego de hosts específicos ou verificar se um roteador está recebendo pacotes de um host em uma interface 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)
```

As correspondências de hardware podem ser vistas apenas com a palavra-chave *hardware*. Use a palavra-chave *ingress* ou *egress* dependendo da direção do grupo de acesso. O local da placa de linha da interface onde a lista de acesso é aplicada também é especificado.

Você também pode aplicar uma lista de acesso ipv4 em uma interface l2transport como um recurso de segurança ou de solução de problemas:

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

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

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

5.4 filtro de saída ethernet

Na direção de saída de uma AC, suponha que não haja nenhum comando **rewrite ingress tag pop <> symmetric** que determine as tags de VLAN de saída. Nesse caso, não há nenhuma verificação para garantir que o quadro de saída tenha as marcas de VLAN corretas de acordo com o comando **encapsulation**.

Este é um exemplo de configuração:

```
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
!
!
!
!
```

Nesta configuração, observe que:

- Um broadcast recebido com uma tag dot1q 2 em GigabitEthernet0/1/0/39.2 mantém sua tag de entrada porque não há nenhum comando **rewrite ingress**.
- Esse broadcast é enviado para fora de GigabitEthernet0/1/0/3.2 com seu dot1q tag 2, mas

isso não causa um problema porque GigabitEthernet0/1/0/3.2 também é configurado com o dot1q tag 2.

- Esse broadcast também é despejado de GigabitEthernet0/1/0/3.3, que mantém sua tag 2 original porque não há nenhum comando **rewrite** em GigabitEthernet0/1/0/3.3. O comando **encapsulation dot1q 3** em GigabitEthernet0/1/0/3.3 não é verificado na direção de saída.
- O resultado é que, para um broadcast recebido com a tag 2 em GigabitEthernet0/1/0/39, há dois broadcasts com a tag 2 saindo de GigabitEthernet0/1/0/3. Esse tráfego duplicado pode causar alguns problemas de aplicativo.
- A solução é a configuração do *filtro de saída Ethernet strict* para garantir que os pacotes saiam da subinterface com as tags VLAN corretas. Caso contrário, os pacotes não serão encaminhados e serão descartados.

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.