

IOS XR L2VPN-services en -functies

Inhoud

[Inleiding](#)

[1. Point-to-Point en Multipoint services](#)

[1.1 Point-to-Point Service](#)

[1.2 Multipoint service](#)

[2. Bijlagecircuits](#)

[2.1 ASR 900 Ethernet virtueel circuit](#)

[2.1.1 Inkomende interfacematching](#)

[2.1.2 VLAN-manipulatie](#)

[2.2 Gedrag van Cisco IOS XR non-EVC router \(CRS en XR12000\)](#)

[3. Point-to-Point Service](#)

[3.1 Lokale switching](#)

[3.1.1 Hoofdinterface](#)

[3.1.2 Subinterfaces en VLAN-manipulatie](#)

[3.2 Virtual Private Wire-services](#)

[3.2.1 Overzicht](#)

[3.2.2 PW- en AC-gekoppelde status](#)

[3.2.3 PW's van type 4 en type 5](#)

[3.2.4 Multisegment PW](#)

[3.2.5 Redundantie](#)

[3.3 CDP](#)

[3.3.1 CDP niet ingeschakeld op hoofdinterface van L2VPN PE](#)

[3.3.2 CDP ingeschakeld op hoofdinterface van L2VPN PE](#)

[3.4 Spanning Tree](#)

[4. Multipoint service](#)

[4.1 Lokale switching](#)

[4.2 Volledig MST](#)

[4.3 BVI](#)

[4.4 VPLS](#)

[4.4.1 Overzicht](#)

[4.4.2 PW-typen en getransporteerde tags](#)

[4.4.3 Automatische detectie en signalering](#)

[4.4.4 MAC-flushes en -opnames](#)

[4.4.5 H-VPLS](#)

[4.4.6 Splitsen van horizontale groepen \(SHG's\)](#)

[4.4.7 Redundantie](#)

[4.5 Stormcontrole in het verkeer](#)

[4.6 MAC-bewegingen](#)

[4.7 IGMP- en MLD-controle](#)

[5. Aanvullende L2VPN-onderwerpen](#)

[5.1 Taakverdeling](#)

[5.2 Vastlegging](#)

[5.3 Ethernet-services toegangslijst](#)

[5.4 Ethernet uitgaande filter](#)

Inleiding

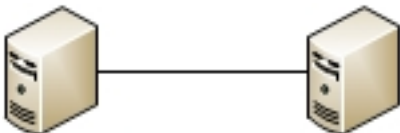
Dit document beschrijft eenvoudige Layer 2 (L2) VPN (L2VPN)-topologieën. Het is nuttig om basisvoorbeelden voor te stellen om ontwerp, de diensten, eigenschappen, en configuratie aan te tonen. Raadpleeg de [configuratiehandleiding voor Cisco ASR 9000 Series aggregatieservices voor L2VPN en Ethernet services, release 4.3.x](#) voor meer informatie.

1. Point-to-Point en Multipoint services

De L2VPN-functie biedt de mogelijkheid om point-to-point en multipoint services te leveren.

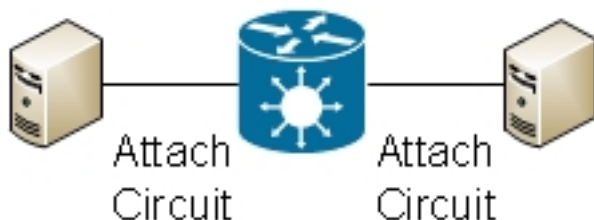
1.1 Point-to-Point Service

De point-to-point service emuleert in principe een transportcircuit tussen twee eindknooppunten zodat de eindknooppunten direct verbonden lijken te zijn via een point-to-point link. U kunt deze link gebruiken om twee sites te verbinden.

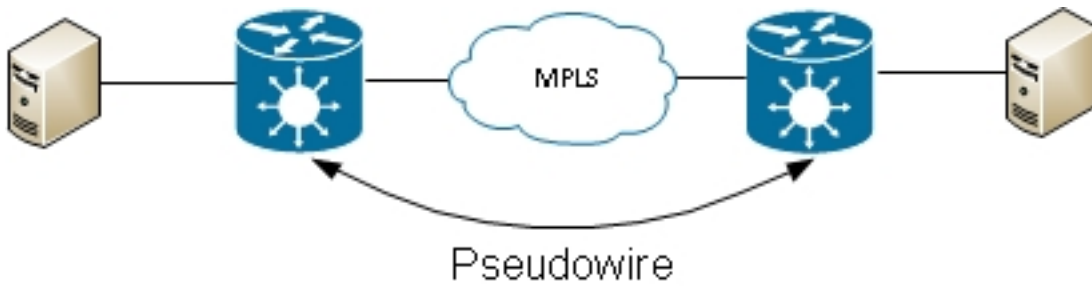


In werkelijkheid kunnen er meerdere routers tussen de twee eindknooppunten zijn en kunnen er meerdere ontwerpen zijn om de point-to-point service te leveren.

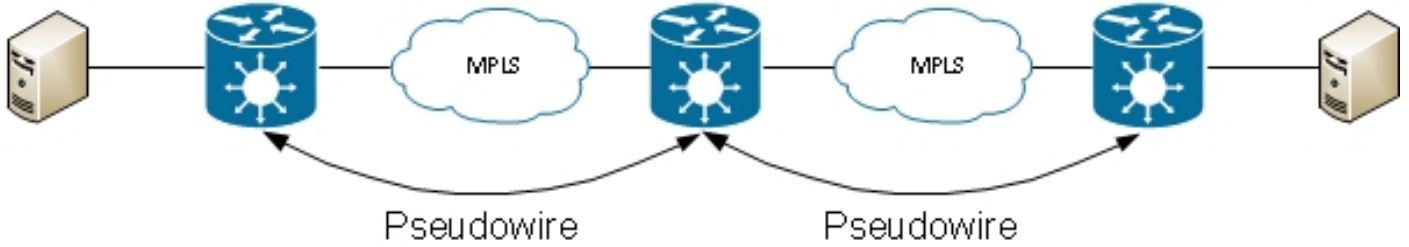
Eén router kan lokale switching tussen twee van zijn interfaces uitvoeren:



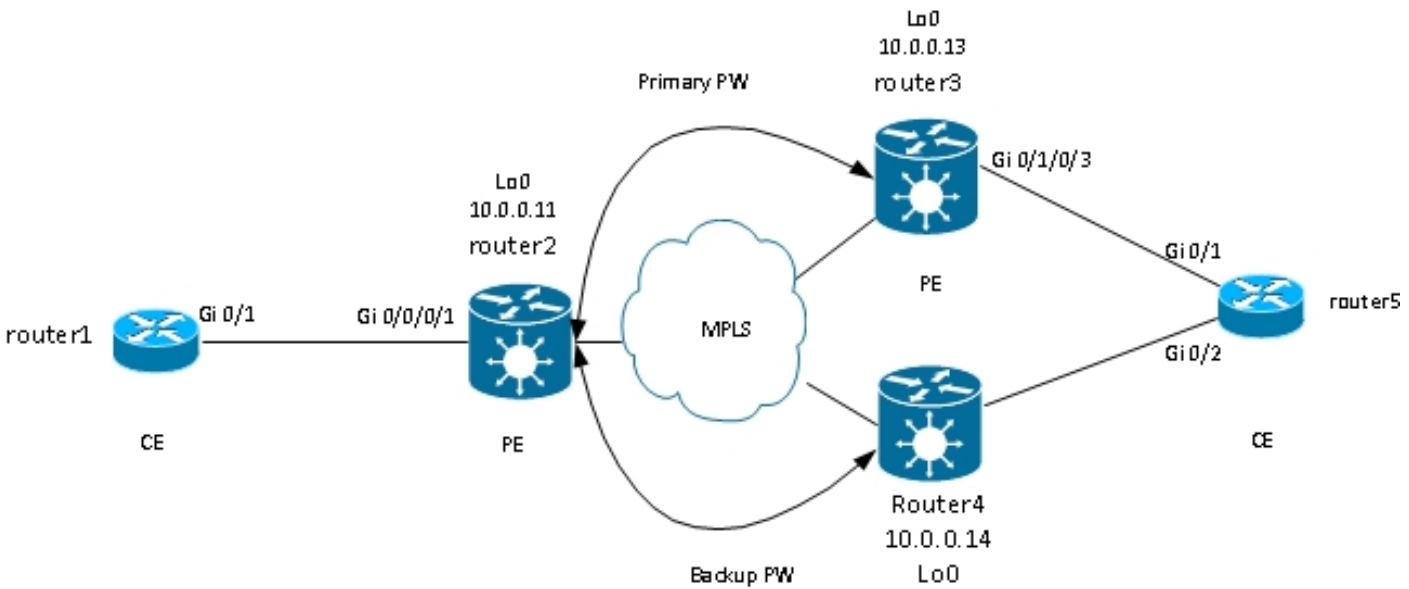
Er kan ook een Multiprotocol Label Switching (MPLS) pseudowire (PW) bestaan tussen twee routers:



Een router kan frames tussen twee PW's switches; in dit geval is dit een multi-segment PW:



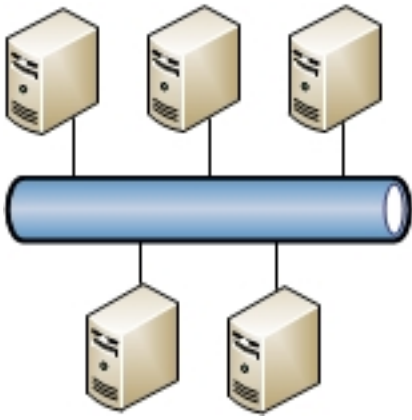
Redundantie is beschikbaar via de PW-redundantiefunctie:



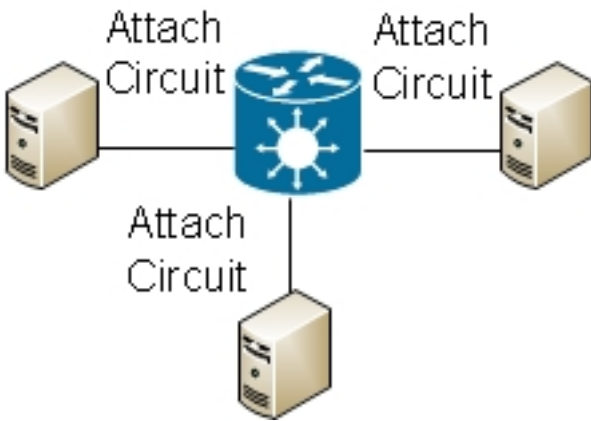
Andere ontwerpen zijn beschikbaar, maar kunnen niet alle hier worden vermeld.

1.2 Multipoint service

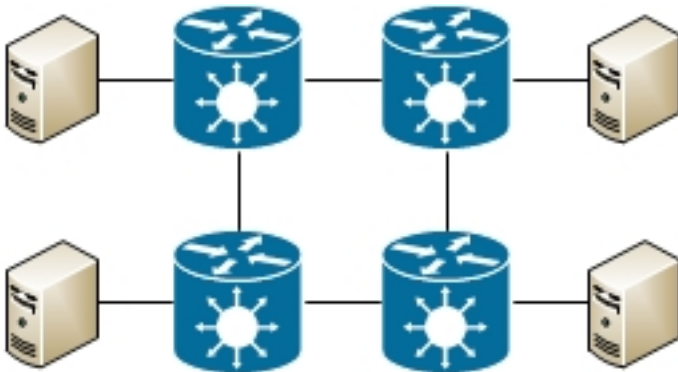
De dienst van Multipoint streeft een uitzendingsdomein na zodat alle die gastheren in dat bridge-domein worden aangesloten logisch gezien met het zelfde segment Ethernet lijken te zijn verbonden:



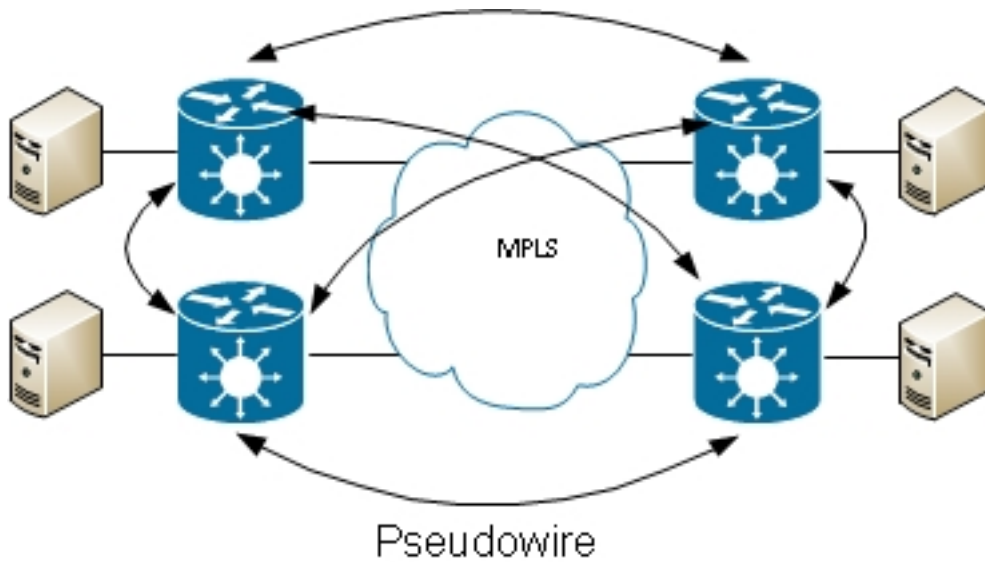
Alle hosts kunnen worden aangesloten op dezelfde router/switch:



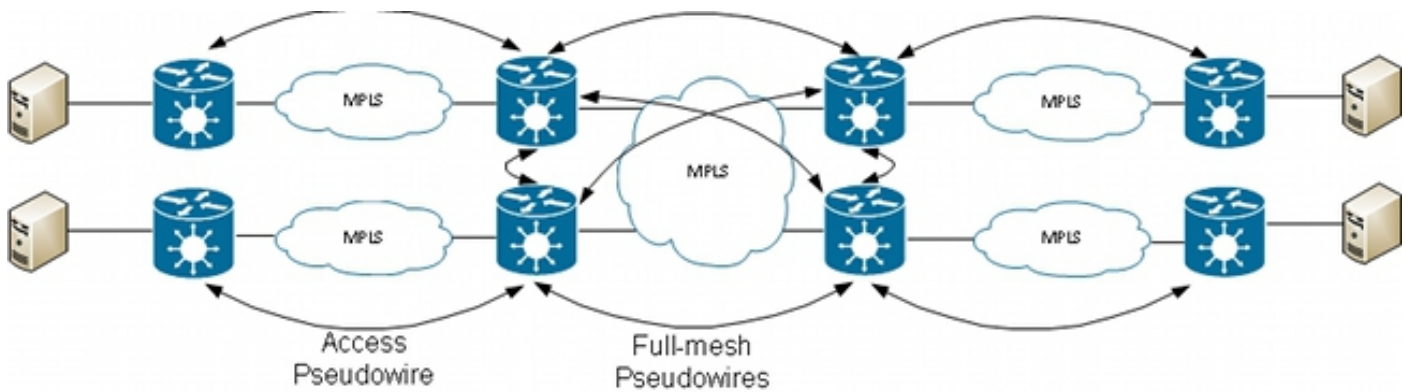
Meervoudige switches kunnen traditionele Ethernet-switching uitvoeren; overspannen - boom moet worden gebruikt om lijnen te breken:



Met Virtual Private LAN Services (VPLS) kunt u het uitzenddomein tussen meerdere sites uitbreiden met MPLS PW's:



Hierarchical VPLS kan worden gebruikt om schaalbaarheid te vergroten:



2. Bijlagecircuits

2.1 ASR 900 Ethernet virtueel circuit

2.1.1 Inkomende interfacematching

Basisregels voor bevestigingscircuits (AC's) omvatten:

- Een pakket moet op een interface worden ontvangen die met het *I2transport* sleutelwoord is geconfigureerd om door de L2VPN-functie te kunnen worden verwerkt.
- Deze interface kan een hoofdinterface zijn, waar het **I2transport** commando is geconfigureerd onder de interface config mode, of een subinterface, waar het *I2transport* sleutelwoord is geconfigureerd na het subinterface nummer.
- Een langste gelijke raadpleging bepaalt de inkomende interface van het pakket. De langste gelijke raadpleging controleert deze voorwaarden in deze orde om het inkomende pakket aan een subinterface aan te passen:

1. Het inkomende frame heeft twee dot1q-tags en komt overeen met een subinterface die geconfigureerd is met dezelfde twee dot1q-tags (802.1Q-tunneling, of QinQ). Dit is de

langst mogelijke match.

2. Het inkomende frame heeft twee dot1q-tags en komt overeen met een subinterface die geconfigureerd is met dezelfde dot1q eerste tag en *elke* tag voor de tweede tag.
 3. Het inkomende frame heeft één dot1q-tag en komt overeen met een subinterface die geconfigureerd is met dezelfde dot1q-tag en het *exacte* trefwoord.
 4. Het inkomende frame heeft een of meer dot1q-tags en komt overeen met een subinterface die geconfigureerd is met een van de dot1q-tags.
 5. Het inkomende frame heeft geen dot1q-tags en past een subinterface aan die is geconfigureerd met de opdracht **Encapsulation Untagged**.
 6. Het inkomende frame komt niet overeen met een andere subinterface, dus het past een subinterface aan die is geconfigureerd met de **inkapselingsstandaardopdracht**.
 7. Het inkomende frame komt niet overeen met een andere subinterface, zodat het overeenkomt met de hoofdinterface die is geconfigureerd voor *I2transport*.
- Op traditionele routers die niet gebruikmaken van het EVC-model (Ethernet Virtual Connection) worden de VLAN-tags die onder de subinterface zijn geconfigureerd, uit het frame verwijderd voordat ze door de L2VPN-functie worden vervoerd.
 - Op een Cisco ASR 9000 Series aggregatieservices router die de EVC-infrastructuur gebruikt, is de standaardactie dat de bestaande tags behouden blijven. Gebruik de opdracht **Herschrijven** om de standaardinstelling te wijzigen.
 - Als er een Bridge Virtual Interface (BVI) in het bridge-domein is, moeten alle inkomende tags worden gekopieerd, omdat de BVI een routed interface is zonder tag. Zie het [BVI-gedeelte](#) voor meer informatie.

Hier zijn verscheidene voorbeelden die deze regels illustreren:

1. Een basisvoorbeeld is wanneer al verkeer dat op een fysieke haven wordt ontvangen moet worden vervoerd, al dan niet het een markering van VLAN heeft. Als u **I2transport** configureert onder de hoofdinterface, wordt al het verkeer dat op die fysieke poort wordt ontvangen getransporteerd door de L2VPN-functie:

```
interface GigabitEthernet0/0/0/2
I2transport
```

Als er subinterfaces van die hoofdinterface zijn, vangt de hoofdinterface elk frame dat niet door een subinterface werd aangepast; dit is de langste matchregel.

2. Bundelinterfaces en subinterfaces kunnen als I2transport worden geconfigureerd:

```
interface Bundle-Ether1
  I2transport
```

3. Gebruik **inkapselingsstandaard** onder een I2transport subinterface om elk gelabeld of niet-gelabeld verkeer aan te passen dat niet is gekoppeld door een andere subinterface met een langste overeenkomst. (Zie voorbeeld 4). Het sleutelwoord *I2transport* wordt geconfigureerd in de subinterfacenaam, niet onder de subinterface zoals op de hoofdinterface:

```
interface GigabitEthernet0/1/0/3.1 I2transport
encapsulation default
```

Insluiting **untagged** configureren als u alleen untagged frames wilt aanpassen.

4. Wanneer er meerdere subinterfaces zijn, voert u de langste matchtest op het inkomende frame uit om de inkomende interface te bepalen:

```
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
```

In deze configuratie, merk op dat:

- Een QinQ-frame met een buitenste VLAN-tag 2 en een binnenste VLAN-tag 3 kan overeenkomen met de subinterfaces .1, .2 of .3, maar het is toegewezen aan de subinterface .3 vanwege de langste matchregel. Twee tags op .3 zijn langer dan één tag op .2 en langer dan geen tags op .1.
- Een QinQ-frame met een buitenste VLAN-tag 2 en een binnenste VLAN-tag 4 wordt toegewezen aan de subinterface .2 omdat **inkapseling dot1q 2** dot1q-frames kan koppelen aan alleen VLAN-tag 2, maar ook QinQ-frames kan koppelen aan een buitenste tag 2. Zie Voorbeeld 5 (het *exacte* trefwoord) als u de QinQ-frames niet wilt aanpassen.
- Een QinQ-frame met een buitenste VLAN-tag 3 komt overeen met de subinterface .1.
- Een dot1q frame met een VLAN-tag 2 komt overeen met de subinterface .2.
- Een dot1q frame met een VLAN-tag 3 komt overeen met de subinterface .1.

5. Om een dot1q kader en niet een kader aan te passen QinQ, gebruik het *nauwkeurige* sleutelwoord:

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

Deze configuratie past geen QinQ-frames aan met een buitenste VLAN-tag 2, omdat deze alleen frames aanpast met precies één VLAN-tag.

6. Gebruik het *niet-gelabelde* trefwoord om alleen niet-gelabelde frames aan te passen zoals Cisco Discovery Protocol (CDP)-pakketten of MST-eenheden (Multiple Spanning Tree Protocol Data Units):

```
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
```

In deze configuratie, merk op dat:

- Dot1q frames met een VLAN tag 3 of QinQ frames met een buitentag 3 komen overeen

met de .3 subinterfaces.

- Alle andere dot1q- of QinQ-frames komen overeen met de subinterface .1.
- Frames zonder VLAN-tag komen overeen met de subinterface .2.

7. Het *willekeurige* trefwoord kan als jokerteken worden gebruikt:

```
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
```

Zowel subinterfaces .4 als .5 konden QinQ frames met tags 4 en 5 aanpassen, maar de frames worden toegewezen aan de .5 subinterfaces omdat het specifieker is. Dit is de langste wedstrijdregel.

8. U kunt verschillende VLAN-tags gebruiken:

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

9. Er kunnen meerdere VLAN-tagwaarden of -bereiken worden weergegeven voor de eerste of tweede dot1q-tag:

```
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
```

U kunt maximaal negen waarden opgeven. Als er meer waarden nodig zijn, moeten deze aan een andere subinterface worden toegewezen. Groepswaarden in een bereik om de lijst te verkorten.

10. De opdracht **inkapselingsdot1q second-dot1q** gebruikt het Ethertype 0x8100 voor de buiten- en binnenste tags omdat dit de Cisco-methode is om QinQ-frames in te kapselen. Volgens IEEE moet echter de Ethertype 0x8100 worden gereserveerd voor 802.1q-frames met één VLAN-tag, en moet een externe tag met Ethertype 0x88a8 worden gebruikt voor QinQ-frames. De buitenste tag met Ethertype 0x88a8 kan worden geconfigureerd met het *dot1ad* sleutelwoord:

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

11. Om de oude Ethertype 0x9100 of 0x9200 voor de QinQ buitenmarkeringen te gebruiken, gebruik het **dot1q tunneling ethertype** bevel onder de belangrijkste interface van de QinQ subinterface:

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



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

De buitenste tag heeft een Ethertype van 0x9100 of 0x9200 en de binnenste tag heeft de dot1q Ethertype 0x8100.

12. Een inkomend kader kan aan een subinterface worden toegewezen, die op het adres bron van MAC wordt gebaseerd:

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

2.1.2 VLAN-manipulatie

Het standaardgedrag van een op EVC gebaseerd platform is om de VLAN-tags op het inkomende frame te behouden.

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

In deze configuratie, houdt een inkomend dot1q kader met een VLAN-tag 3 zijn VLAN-tag 3 wanneer het frame wordt doorgestuurd. Een inkomend QinQ-frame met een buitenste VLAN-tag 3 en een binnenste tag 100 houdt beide tags ongewijzigd wanneer het frame wordt doorgestuurd.

Maar met de EVC-infrastructuur kunt u de tags manipuleren met de opdracht **herschrijven**, zodat u tags kunt pop (verwijderen), vertalen of duwen (toevoegen) naar de inkomende VLAN-tagstack.

Hier zijn verschillende voorbeelden:

- Met het *pop*-sleutelwoord kunt u een QinQ-tag verwijderen uit een inkomend dot1q-frame. In dit voorbeeld wordt de buitenste tag 13 van het inkomende QinQ-frame verwijderd en het frame met de dot1q-tag 100 naar boven doorgestuurd:

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

Het gedrag is altijd symmetrisch, wat betekent dat de buitenste tag 13 in de indringingsrichting wordt gedrukt en in de uitgangsricting wordt geduwd.

- Met het trefwoord *translate* kunt u een of twee inkomende tags vervangen door een of twee nieuwe tags:

```
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
```

Het *symmetrische* trefwoord wordt automatisch toegevoegd omdat het de enige ondersteunde modus is.

- Met het *push*-trefwoord kunt u een QinQ-tag toevoegen aan een inkomend dot1q-frame:

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

Een buitenste QinQ tag 100 wordt toegevoegd aan het inkomende frame met een dot1q tag 4. In de uitgangsrichting wordt de QinQ-tag gekopieerd.

2.2 Gedrag van Cisco IOS XR non-EVC router (CRS en XR12000)

De syntaxis voor VLAN-matching op de niet-EVC-platforms gebruikt niet het sleutelwoord *inkapseling*:

```
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
```

De manipulatie van de VLAN-tags kan niet worden geconfigureerd, omdat het enige mogelijke gedrag is dat alle tags die in de opdrachten **dot1q** of **dot1ad** zijn gespecificeerd, worden gekopieerd. Dit gebeurt standaard, dus er is geen **herschrijfopdracht**.

3. Point-to-Point Service

Opmerkingen:

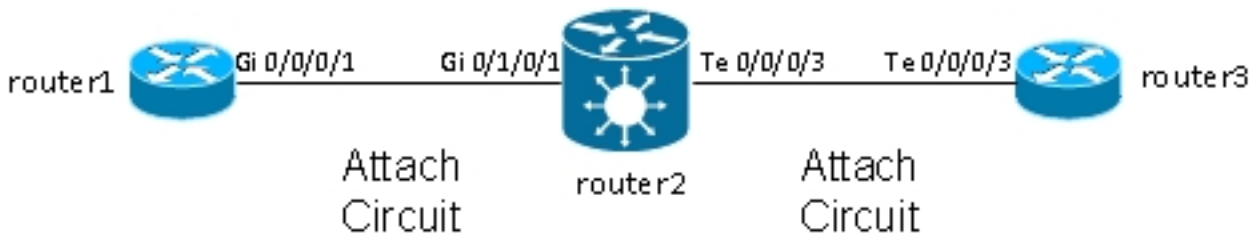
Gebruik de [Command Lookup Tool \(alleen voor geregistreeerde gebruikers\)](#) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

De [Output Interpreter Tool \(alleen voor geregistreeerde klanten\)](#) ondersteunt bepaalde opdrachten met **show**. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show**.

3.1 Lokale switching

3.1.1 Hoofdinterface

De basistopologie is een lokaal kruispunt tussen twee hoofdinterfaces:



Router2 neemt al die verkeer op Gi 0/1/0/1 wordt ontvangen en door:sturen het aan Te 0/0/0/3 en vice versa.

Terwijl router1 en router3 een directe back-to-back kabel in deze topologie lijken te hebben, is dit niet het geval omdat router2 eigenlijk tussen de TienGigE en Gigabit Ethernet interfaces vertaalt. Router2 kan functies op deze twee interfaces uitvoeren; een toegangscontrolelijst (ACL) kan bijvoorbeeld specifieke typen pakketten of een beleidskaart laten vallen om laag prioriteitsverkeer te vormen of te beperken.

Een basis punt-tot-punt kruis wordt gevormd tussen twee belangrijkste interfaces die als l2transport op router2 worden gevormd:

```
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
!
```

Op router1 en router3, worden de belangrijkste interfaces gevormd met CDP en een IPv4 adres:

```
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

```

Router1 ziet router3 als een CDP buur en kan 10.1.1.2 (het interfaceadres van router3) pingelen alsof de twee routers direct werden verbonden.

Omdat er geen subinterface op router2 is geconfigureerd, worden inkomende frames met een VLAN-tag transparant getransporteerd wanneer dot1q-subinterfaces op router1 en router3 zijn geconfigureerd:

```

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

```

Nadat 10.000 van router1 aan router3 pingelt, kunt u de **showinterface** gebruiken en **l2vpn** bevelen **tonen** om ervoor te zorgen dat pingelen verzoeken die door router2 op één AC worden ontvangen op andere AC door:sturen en dat pingelen de antwoorden worden behandeld de zelfde manier in omgekeerde.

```

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

**RP0/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

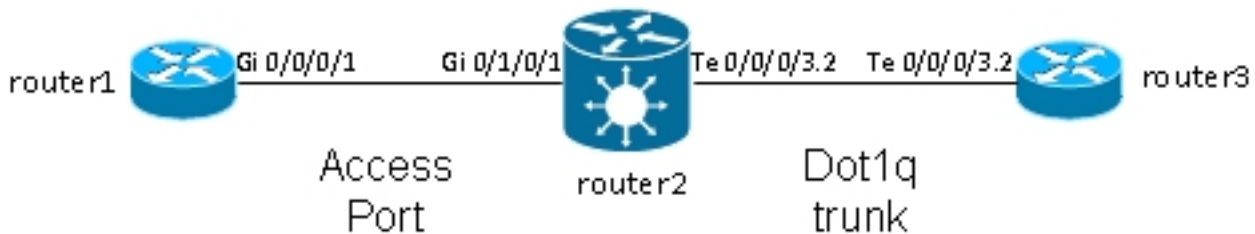
Flags: Learn enable

uIDB Index: 0x0007, LAG pointer: 0x0000

Split Horizon Group: None

3.1.2 Subinterfaces en VLAN-manipulatie

In Cisco IOS[®]-softwareterminologie heeft dit voorbeeld één AC die lijkt op een toegangsinterface voor de switchport-modus en een dot1q-subinterface die lijkt op een trunk:



Meestal gebruikt deze topologie een bridge-domein omdat er meestal meer dan twee poorten in het VLAN zijn, hoewel u een point-to-point cross connect kunt gebruiken als er maar twee poorten zijn. In deze sectie wordt beschreven hoe flexibel herschrijfmogelijkheden u meerdere manieren geven om het VLAN te manipuleren.

3.1.2.1 Hoofdinterface en Dot1q subinterface

In dit voorbeeld staat de hoofdinterface aan de ene kant en de dot1q subinterface aan de andere kant:

Dit is de belangrijkste interface op router1:

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

Dit is de dot1q subinterface op router2:

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

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

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

Er is nu een *l2transport* sleutelwoord in de subinterfacenaam van TenGigE0/0/0/3.2. Router3 stuurt dot1q frames met tag 2, die overeenkomen met de TenGigE0/0/0/3.2 subinterface op router2.

De inkomende tag 2 wordt verwijderd in de ingangsrichting door de **herschrijvingstag pop 1 symmetric** opdracht. Aangezien de tag is verwijderd in de ingangsrichting op de TenGigE0/0/0/3.2, worden de pakketten verzonden untagged in de uitgangsrichting op Gigabit Ethernet0/1/0/1.

Router1 verstuurt niet-gemerkte frames, die overeenkomen met de belangrijkste interface Gigabit

Ethernet0/1/0/1.

Er is geen **herschrijfopdracht** op Gigabit Ethernet0/1/0/1, dus er wordt geen tag weergegeven, gedrukt of vertaald.

Wanneer pakketten moeten worden doorgestuurd vanuit TenGigE0/0/0/3.2, wordt de dot1q tag 2 gedrukt vanwege het *symmetrische* sleutelwoord in de **herschrijvingstag pop 1** opdracht. De opdracht springt één tag in de toegangsrichting, maar drukt symmetrisch één tag in de uitgangsrichting. Dit is een voorbeeld op 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
```

Controleer de subinterfacetellers met de zelfde **showinterface** en **toon l2vpn** bevelen:

```
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
```

Zoals verwacht, komt het aantal pakketten dat op TenGigE0/0/0/3.2 wordt ontvangen overeen met

het aantal pakketten dat op Gigabit Ethernet0/1/0/1 wordt verzonden en vice versa.

3.1.2.2 Subinterface met insluiting

In plaats van de hoofdinterface op Gigabit Ethernet0/1/0/1, kunt u een subinterface met **inkapselingsgebrek** gebruiken om alle frames te vangen of met **inkapseling untagged** om alleen untagged frames aan te passen:

```
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 Ingangsrichting op Gigabit Ethernet0/1/0/1.1

In plaats van pop tag 2 in de toegangsrichting op TenGigE0/0/0/3.2, kunt u tag 2 in de toegangsrichting op Gigabit Ethernet0/1/0/1.1 duwen en niets doen op 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
```

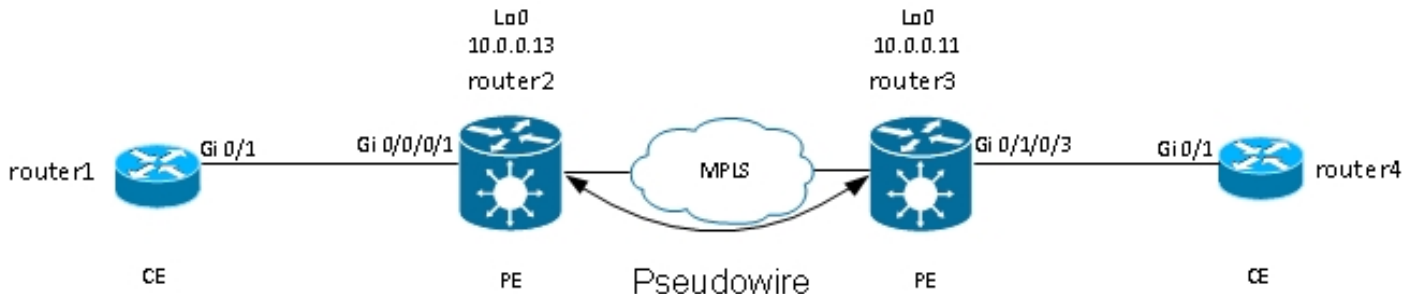
```
RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p3
interface TenGigE0/0/0/3.2
interface GigabitEthernet0/1/0/1.1
```

Aldus, kunt u zien dat het EVC model met de **inkapseling** en **herschrijft** bevelen u grote flexibiliteit geeft om de markeringen van VLAN aan te passen en te manipuleren.

3.2 Virtual Private Wire-services

3.2.1 Overzicht

Met Virtual Private Wire Services (VPWS), ook bekend als Ethernet over MPLS (EoMPLS), kunnen twee L2VPN Provider Edge (PE)-apparaten het L2VPN-verkeer via een MPLS-cloud tunnelen. De twee L2VPN-PE's worden doorgaans op twee verschillende sites met een MPLS-kern onderling verbonden. De twee AC's die bij elke L2VPN-PE zijn aangesloten, zijn via een PW verbonden via het MPLS-netwerk, dat MPLS PW is.



Elke PE moet een MPLS-label hebben om de loopback van de afstandsbediening te bereiken. Dit etiket, dat doorgaans het etiket Interior Gateway Protocol (IGP) wordt genoemd, kan worden geleerd met behulp van het MPLS Label Distribution Protocol (LDP) of MPLS Traffic Engineering (TE).

De twee PW's stellen onderling een gerichte MPLS LDP-sessie in zodat ze de status van de PW kunnen instellen en controleren. Eén PE adverteert met de andere PE met het MPLS-label voor PW-identificatie.

Opmerking: hoewel BGP voor signalering kan worden gebruikt, is dit niet het geval in dit document.

Het verkeer dat door router2 op zijn lokale AC wordt ontvangen is ingekapseld in een MPLS-labelstack:

- Het buiten MPLS etiket is het IGP etiket om de loopback van router3 te bereiken. Dit zou het impliciete-nulllabel kunnen zijn als de labels direct zijn verbonden; dit betekent dat er geen IGP-label zou worden toegevoegd.
- Het binnenste MPLS-label is het PW-label geadverteerd door router3 via de beoogde LDP-sessie.
- Er kan een PW-controlewoord zijn na de MPLS-labels, afhankelijk van de configuratie en het type inkapseling. Het controlewoord wordt niet gebruikt door gebrek op Ethernet interfaces en moet uitdrukkelijk worden gevormd wanneer nodig.
- Het getransporteerde L2 frame volgt in het pakket.
- Sommige VLAN-tags worden over de PW getransporteerd, afhankelijk van de configuratie en het PW-type.

De voorlaatste hop, net voor router3 in de MPLS kern, knalt het IGP-etiket of vervangt het door een expliciet null-etiket. Aldus, is het hoogste zinvolle etiket op het kader dat door router3 wordt ontvangen het PW- etiket dat router3 aan router2 voor PW signaleerde. Zo, router3 weet dat het verkeer dat met dat MPLS- etiket wordt ontvangen aan AC zou moeten worden overgeschakeld die aan router4 wordt aangesloten.

In het [vorige voorbeeld](#) moet u eerst controleren of elke L2VPN een MPLS-label heeft voor de loopback van de externe PE. Dit is een voorbeeld van hoe te om etiketten op router2 te controleren:

```
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
```

De AC-configuratie is nog steeds hetzelfde:

```
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
```

Omdat er geen **herschrijf ingress-pop** opdracht is, wordt de inkomende VLAN-tag 2 over de PW getransporteerd. [Zie Type 4 en 5 PWs](#) voor nadere informatie.

De L2VPN-configuratie specificeert de lokale AC en de externe L2VPN-PE met een PW-id dat aan elke kant moet overeenkomen en uniek moet zijn voor elke buur:

```
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
```

De bijbehorende configuratie op router3 is:

```
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
```

Gebruik de opdracht **show l2vpn xconnect detail** om de details op de cross connect te bekijken:

```
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
```

In deze configuratie, merk op dat:

- De maximale transmissie-eenheid (MTU) van de wisselstroom is 1504 omdat de inkomende tag op de wisselstroom niet wordt ingedrukt. De MTU moet aan elke kant passen, anders komt de PW niet omhoog.
- Er werden 186 pakketten ontvangen op de AC en verzonden op de PW zoals verwacht.
- 38448 pakketten werden ontvangen op de PW en werden op de AC gestuurd zoals verwacht.
- Het lokale etiket op router2 is 16026 en is het etiket dat router3 als binnenetiket gebruikt. De pakketten worden ontvangen op router2 met dat MPLS etiket als hoogste etiket omdat het IGP etiket door de voorlaatste MPLS hop is gekopieerd. Router2 weet dat inkomende frames met dat PW-label naar de AC Gi 0/0/0/1.2 moeten worden geschakeld:

```
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 PW- en AC-gekoppelde status

In een point-to-point cross connect worden de AC en de PW gekoppeld. Dus, als de AC daalt, de L2VPN PE-signalen via LDP naar de externe PE dat de PW-status zou moeten worden verlaagd. Dit leidt tot convergentie wanneer PW-redundantie is geconfigureerd. Zie het gedeelte [Redundantie](#) voor meer informatie.

In dit voorbeeld, is AC neer op router2 en verzendt de "AC Beneden" PW status naar router3:

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

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

PW Status TLV in use

MPLS Local Remote

```
-----
Label 16026 16031
Group ID 0x4000280 0x6000180
Interface GigabitEthernet0/0/0/1.2 GigabitEthernet0/1/0/3.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
-----
```

```
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x6 (AC Down) in Notification message
MIB cpwVcIndex: 3221225476
Create time: 30/04/2013 16:30:58 (1d07h ago)
Last time status changed: 01/05/2013 14:05:07 (09:33:47 ago)
Statistics:
packets: received 38544, sent 186
bytes: received 2620884, sent 12644
```

Router3 weet dat PW neer zou moeten zijn omdat ver AC neer is:

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

```
Group test, XC p2p4, state is down; Interworking none
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1504; XC ID 0xc40003; interworking none
Statistics:
packets: received 38545, sent 186
bytes: received 2620952, sent 12644
drops: illegal VLAN 0, illegal length 0
```

```
PW: neighbor 10.0.0.13, PW ID 222, state is down ( local ready )  
PW class not set, XC ID 0xc0000005  
Encapsulation MPLS, protocol LDP  
Source address 10.0.0.11  
PW type Ethernet, control word disabled, interworking none  
PW backup disable delay 0 sec  
Sequencing not set
```

```
PW Status TLV in use  
MPLS Local Remote
```

```
-----  
Label 16031 16026  
Group ID 0x6000180 0x4000280  
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2  
MTU 1504 1504  
Control word disabled disabled  
PW type Ethernet Ethernet  
VCCV CV type 0x2 0x2  
(LSP ping verification) (LSP ping verification)  
VCCV CC type 0x6 0x6  
(router alert label) (router alert label)  
(TTL expiry) (TTL expiry)  
-----
```

```
Incoming Status (PW Status TLV):  
Status code: 0x6 (AC Down) in Notification message  
Outgoing Status (PW Status TLV):  
Status code: 0x0 (Up) in Notification message  
MIB cpwVcIndex: 3221225477  
Create time: 30/04/2013 16:37:57 (1d07h ago)  
Last time status changed: 01/05/2013 14:11:33 (09:35:50 ago)  
Statistics:  
packets: received 186, sent 38545  
bytes: received 12644, sent 2620952
```

3.2.3 PW's van type 4 en type 5

Er kunnen twee typen PW's worden gebruikt: type 4 en type 5.

- Een type 4 PW is gekend als op VLAN gebaseerde PW. De toegang PE wordt niet verondersteld om de inkomende markeringen van VLAN te verwijderen die over PW moeten worden vervoerd.

Op de op EVC gebaseerde platforms zoals de ASR 9000, is het probleem dat de inkomende AC's een **herschrijfopdracht** kunnen hebben die de inkomende VLAN-tags doorgeeft, zodat er mogelijk geen VLAN-tag over de PW kan worden getransporteerd. Om deze mogelijkheid aan te pakken, plaatsen de EVC-platforms een dummy VLAN-tag 0 bovenop het frame voor type 4 PW's. Type 4 PW's zijn geconfigureerd met de opdracht **transport-mode VLAN**. De externe PE moet op EVC gebaseerd zijn en moet begrijpen dat de bovenste VLAN-tag de te verwijderen dummy-tag is.

Echter, als u een type 4 PW tussen een EVC-platform en een niet-EVC-platform gebruikt, kan dit leiden tot interoperabiliteitsproblemen. Het platform niet-EVC beschouwt de top VLAN-tag niet als de dummy VLAN-tag en stuurt in plaats daarvan het frame met de dummy VLAN-tag 0 door als de buitntag. De EVC-platforms hebben de mogelijkheid om de VLAN-tags te manipuleren die op het inkomende frame worden ontvangen met de opdracht **Herschrijven**. De resultaten van die manipulatie van VLAN worden vervoerd over type 4 PW met de extra

dummy tag 0 bovenop.

Recente Cisco IOS XR-software-releases bieden de mogelijkheid om een type 4 PW te gebruiken zonder gebruik van de dummy-tag 0 met de opdracht **Transport-Mode VLAN-passthrough**. De VLAN-tagmanipulatie op het Ethernet Flow Point (EFP) moet ervoor zorgen dat er ten minste één tag blijft omdat er een VLAN-tag moet worden getransporteerd op een type 4 PW en omdat er in dit geval geen dummy-tag is die aan dat vereiste voldoet. De tags die op het frame blijven na het herschrijven van de inkomende interfacetag worden transparant door de PW getransporteerd.

- Een type 5 PW staat bekend als een Ethernet-poortgebaseerde PW. De toegang PE vervoert frames die worden ontvangen op een hoofdinterface of nadat de subinterface-tags zijn verwijderd wanneer het pakket wordt ontvangen op een subinterface. Er is geen eis om een geëtiketteerd kader over een type 5 PW te verzenden, en geen dummy markering wordt toegevoegd door de op EVC-gebaseerde platforms. De op EVC gebaseerde platforms hebben de mogelijkheid om de VLAN-tags te manipuleren die op het inkomende frame worden ontvangen met de opdracht **Herschrijven**. De resultaten van die manipulatie van VLAN worden vervoerd over type 5 PW, of geëtiketteerd of untagged.

Standaard proberen de L2VPN-PE's een type 5 PW te onderhandelen, zoals in dit voorbeeld te zien is:

```
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
```

Het PW-type Ethernet geeft een type 5 PW aan.

Dit is een snuffelopname van een ARP-verzoek dat door router1 wordt verzonden en door router2 via PW naar router3 wordt ingekapseld:

```
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)
```

De MPLS label 16031 is het PW label geadverteerd door router3. De snuffelopname is genomen tussen de voorlaatste hop en router3, dus er is geen IGP-label.

Het ingekapselde Ethernet-frame wordt onmiddellijk na het PW-label gestart. Er kan een PW controlewoord zijn, maar het wordt niet gevormd in dit voorbeeld.

Zelfs als het een type 5 PW is, wordt de inkomende VLAN-tag 2 die op de AC wordt ontvangen door router2 getransporteerd omdat er geen **herschrijfopdracht** is die op de AC wordt gekopieerd. De resultaten die uit AC na de herschrijfverwerking komen worden vervoerd omdat er geen automatische markering die op EVC-gebaseerde platforms komt knallen. Merk op dat er geen dummy VLAN-tag 0 is met een type 5 PW.

Als u met de **herschrijvingstag pop 1 symmetrische** opdracht vormde, zou er geen VLAN-tag over

de PW worden vervoerd.

Hier is een voorbeeld van een type 4 PW met configuratie van een pw-klasse op router2 en router3.

Opmerking: als u alleen aan één kant een type 4 instelt, blijft de PW ingedrukt en meldt 'Fout: PW-type niet goed afgestemd.'

```
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
!
!
!
!
```

Het PW-type Ethernet VLAN geeft een type 4 PW aan.

```
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
```

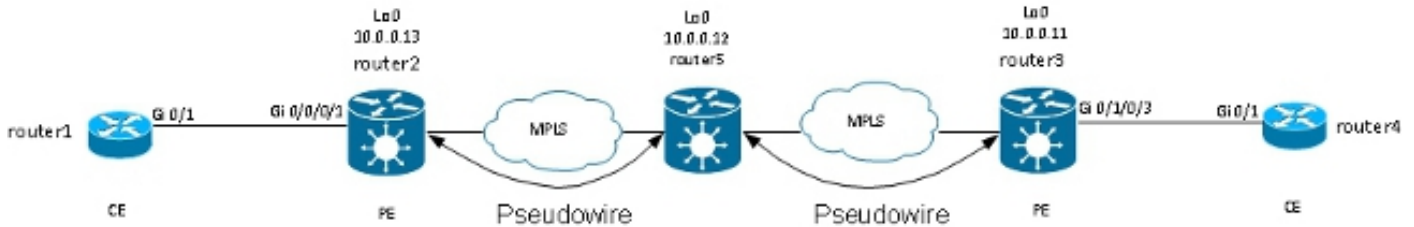
Er is nu een dummy tag 0 geplaatst bovenop het frame dat wordt vervoerd:

```
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)
```

De uitgaande EVC-gebaseerde PE verwijdert de dummy tag en verstuurt het frame met de tag 2 op zijn lokale AC. De uitgaande PE past de lokale tagmanipulatie toe die op zijn AC is ingesteld op het frame dat op de PW wordt ontvangen. Als zijn lokale AC is geconfigureerd als **herschrijf ingress tag pop 1 symmetric**, moet de geconfigureerde tag in de uitgangsrichting worden gedruwd, zodat een nieuwe tag wordt gedrukt bovenop de tag 2 die op de PW wordt ontvangen. De herschrijfopdracht is erg flexibel, maar je moet zorgvuldig evalueren wat je aan elke kant van de PW wilt bereiken.

3.2.4 Multisegment PW

Het is mogelijk om een L2VPN PE die een PW, in plaats van een fysieke interface, als AC heeft te hebben:



Router5 ontvangt pakketten op PW van router2 en switches de pakketten op zijn andere PW aan router3. Router5 is dus schakelen tussen PW's om een multisegment PW tussen router2 en router3 te creëren.

De configuratie op router2 wijst nu op router5 als verre PE:

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

De configuratie op router5 is basis:

```
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
!
```

De **omschrijving** opdracht is optioneel en wordt ingevoegd in een PW-switching Type Length Value (TLV) die wordt verzonden door router5 naar elke externe PE (router2 en router3). De **beschrijving** is nuttig wanneer u een probleem van PW moet oplossen wanneer er een router in het midden is die PW-omschakeling doet.

Voer de opdracht **sh l2vpn xconnect** in om de PW-switching TLV te bekijken:

```
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)

Router5 stuurt een PW-switching TLV naar router3 met de details van zijn PW naar router2 en stuurt een PW-switching TLV naar router2 met de details van zijn PW naar router3.

3.2.5 Redundantie

Een point-to-point PW kan worden gebruikt voor de aansluiting van twee locaties, maar deze twee locaties moeten verbonden blijven in het geval van een PE- of AC-storing.

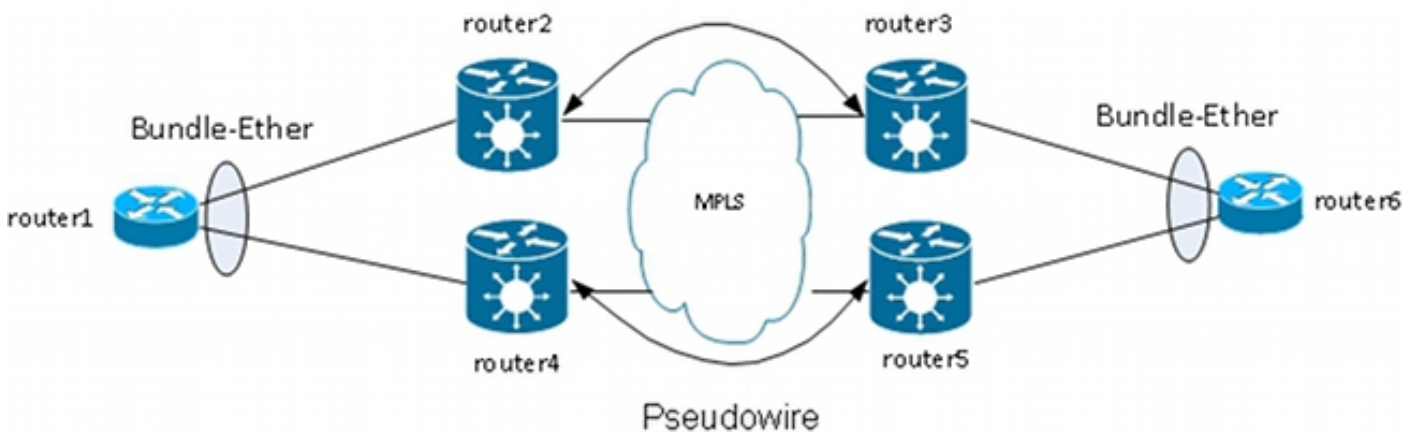
3.2.5.1 Core-redundantie

Als u een topologiewijziging aanbrengt die gevolgen heeft voor de doorgifte in de MPLS-kern, dan erft de MPLS PW onmiddellijk het nieuwe pad.

3.2.5.2 Bundel over PW's

Een Customer Edge (CE)-apparaat kan via een Ethernet-bundel op de PE worden aangesloten om koppelingsredundantie te bieden als er een storing is in de bundellidkoppeling tussen de CE en de PE. De bundel blijft omhoog zelfs als één bundelverbindingslid daalt. Merk op dat dit geen PE overtuiging verstrekt omdat een PE mislukking de volledige bundel neer brengt.

Een methode voor redundantie is om meerdere circuits te laten transporteren door point-to-point PW's. Elk circuit is lid van een Ethernet-bundel tussen twee CE's:



De PE beëindigt de bundel niet en vervoert in plaats daarvan op transparante wijze frames over de PW, met inbegrip van de Link Aggregation Control Protocol (LACP)-frames die CE's onderling uitwisselen.

Met dit ontwerp, het verlies van een AC of een PE veroorzaakt een bundellid daalt, maar de bundel blijft omhoog.

Opmerking: LACP BPDU's zijn niet via L2VPN met de ASR 9000 in releases eerder dan Cisco IOS XR-software release 4.2.1 vervoerd.

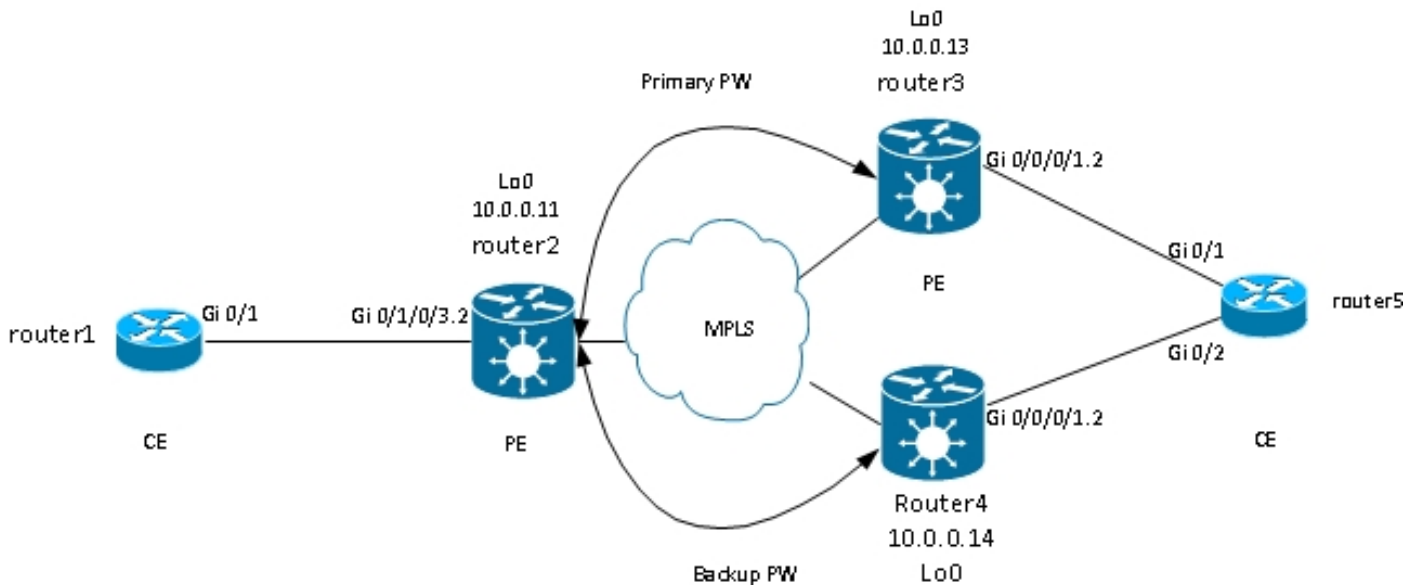
De CE is nog steeds een single point of failure in dit ontwerp. Andere redundantiefuncties die op de CE kunnen worden gebruikt, zijn onder meer:

- Multichassis Link Aggregation Group (MC-LAG)
- ASR 9000 netwerkvirtualisatie (nV)-clustering
- Virtual Switching System (VSS) op Cisco IOS-switches
- Virtual Port Channel (vPC) op Cisco Nexus-Switches

Vanuit het perspectief van de PE is er een eenvoudige point-to-point verbinding tussen een AC en een MPLS PW.

3.2.5.3 PW-redundantie

PEs kan redundantie ook voorzien van een functie die PW Redundantie wordt genoemd.



Router2 heeft een primaire PW naar router3. Het verkeer van router1 naar router6 stroomt over dat primaire PW onder normale omstandigheden. Router2 heeft ook een back-up PW naar router4 in hot stand-by, maar onder normale omstandigheden, geen verkeersstromen over die PW.

Als er een probleem is met de primaire PW, met de externe PE van de primaire PW (router3), of met de AC op de externe PE (router3), activeert router2 onmiddellijk de back-up PW, en het verkeer begint door het te stromen. Wanneer het probleem is opgelost, keert het verkeer terug naar het primaire PW.

De configuratie op router2 is:

```
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
!
```

De standaardconfiguratie op router3 en router4 is:

```

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
!
!
!
!

```

Onder stabiele omstandigheden is de PW naar router3 actief en is de PW naar router4 in een stand-by status:

```

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#

Omdat de AC status en de PW status zijn gekoppeld, router3 "AC neer"aan router2 wanneer AC op router3 daalt. Router2 brengt zijn primaire PW naar beneden en activeert de reserve PW:

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)

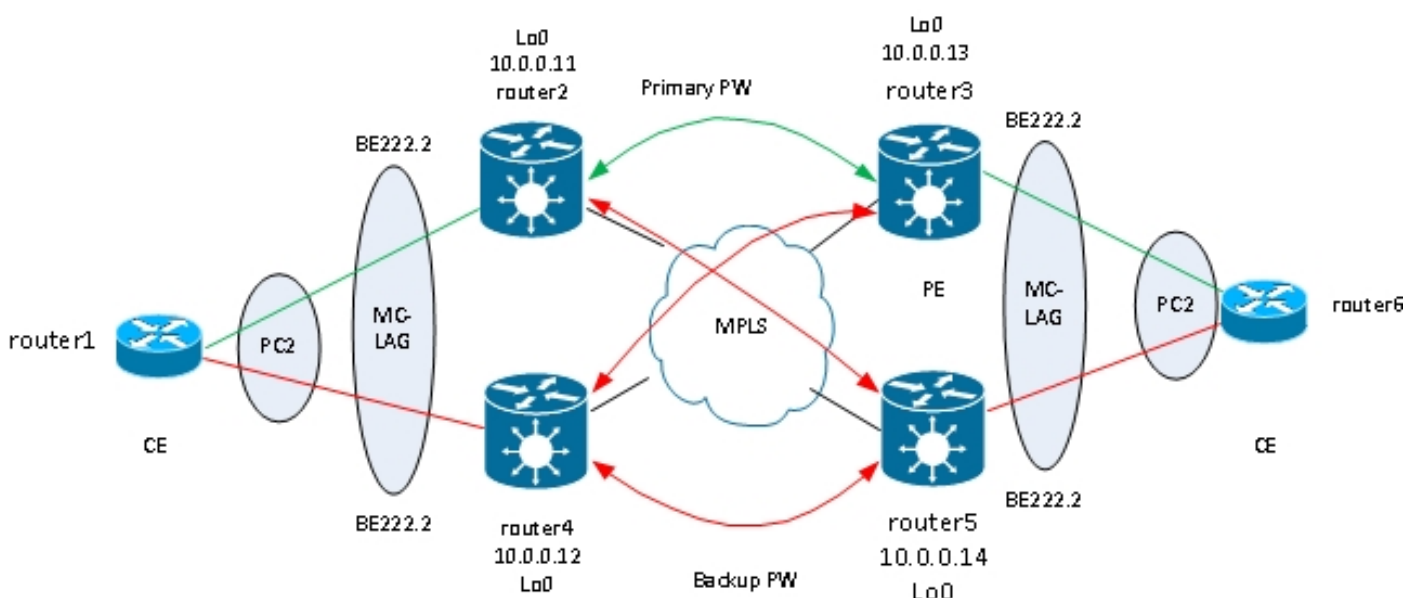
(TTL expiry) (TTL expiry)

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#

Wanneer AC op router3 terug omhoog komt, reactiveert router2 primaire PW aan router3, en PW aan router4 gaat terug naar een standby staat.

De back-up PW wordt ook geactiveerd wanneer router3 uitvalt, en router2 verliest de route aan zijn loopback.

De volgende logische stap is tweevoudige PW-redundantie met twee PE's op elke locatie te introduceren:



Dit volledige netwerk van PW's stuit echter op een probleem wanneer twee PW's tegelijkertijd actief zijn en een lus in het netwerk wordt geïntroduceerd. De lus moet worden gebroken, over het algemeen met behulp van het Spanning Tree Protocol (STP). U wilt echter geen overspannende boominstabiliteit op één site om te verspreiden naar de andere site. Daarom is het beter om geen overspannende boom op deze PW's in werking te stellen en niet de overspannende boom tussen de twee plaatsen samen te voegen. Het is eenvoudiger als er slechts één logisch verband tussen de twee sites is, zodat er geen overspannende boom nodig is.

Een oplossing is om een MC-LAG bundel te gebruiken tussen de twee PE's op één locatie en hun lokale CE. Slechts één van de twee PE's heeft zijn bundelleden actief zodat zijn PW naar de verafgelegen site actief is. De andere PE heeft zijn bundelleden in stand-by status en heeft zijn PW naar de afgelegen site down. Met slechts één PW actief tussen de twee sites, wordt er geen loop geïntroduceerd. De PE met de actieve PW heeft ook een stand-by PW naar de tweede PE op de afgelegen site.

Onder stabiele omstandigheden, zijn de actieve bundelleden op router2 en router3, en actieve PW is tussen hen. Dit is de configuratie op router3:

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

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

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

```
interface Bundle-Ether222
lACP switchover suppress-flaps 100
mlacp iccp-group 2
mlacp switchover type revertive
mlacp switchover recovery-delay 40
mlacp port-priority 1
mac-address 0.0.2
bundle wait-while 0
bundle maximum-active links 1
load-interval 30
!
```

```
RP/0/RSP1/CPU0:router3#sh run l2vpn xconnect group test
```

```
l2vpn
xconnect group test
p2p p2p7
interface Bundle-Ether222.2
neighbor 10.0.0.11 pw-id 222
backup neighbor 10.0.0.12 pw-id 222
!
!
!
!
!
```

```
RP/0/RSP1/CPU0:router3#sh l2vpn xconnect group test
```

```
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed
```

```
XConnect Segment 1 Segment 2
```

```
Group Name ST Description ST Description ST
```

```
-----
test p2p7 UP BE222.2 UP 10.0.0.11 222 UP
```

```
Backup
```

```
10.0.0.12 222 DN
-----
```

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

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

```
Port Device State Port ID B/W, kbps
```

```
-----
Gi0/0/0/1 Local Active 0x8001, 0x9001 1000000
Link is Active
Gi0/0/0/1 10.0.0.14 Standby 0x8002, 0xa002 1000000
Link is marked as Standby by mLACP peer
```

Op router5, zijn het lokale bundellid en primaire PW aan router2 in standby staat, en reserve PW aan router4 is neer:

```
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
```

Op router6, is het bundellid aan router3 actief, terwijl het bundellid aan router5 in standby staat is:

```
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
```


Backup
10.0.0.14 222 UP

Router5 heeft zijn bundellid actief evenals zijn primaire PW aan 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
```

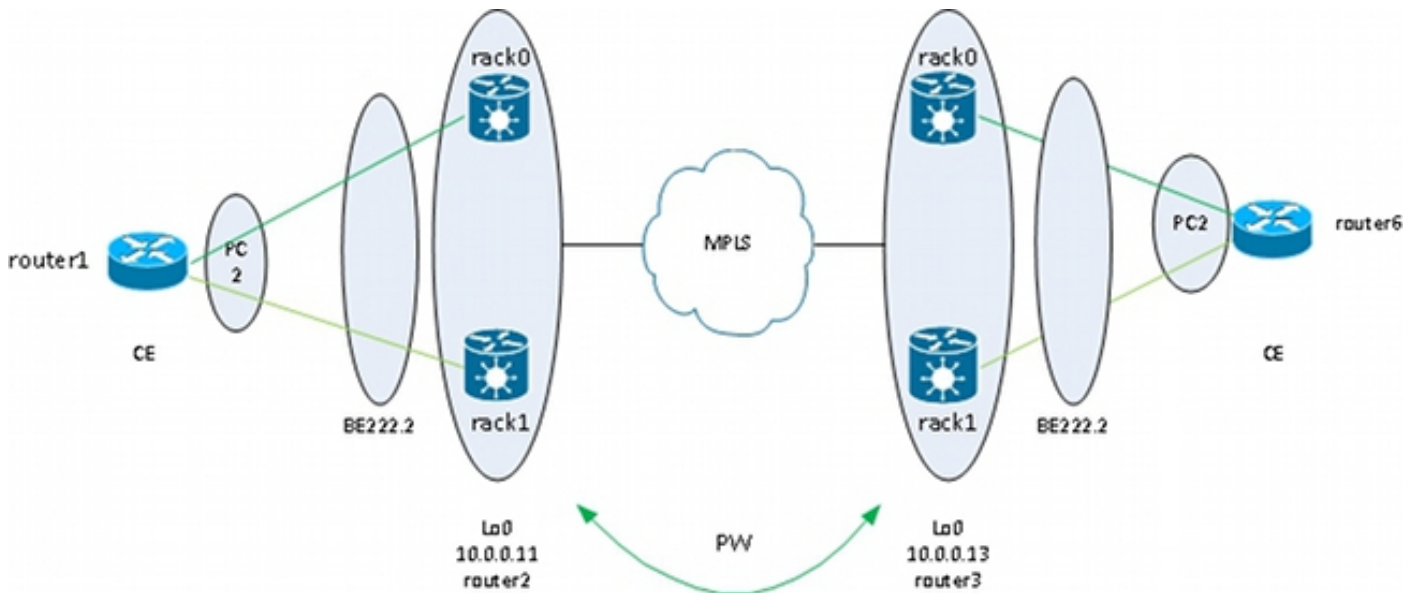
```
XConnect Segment 1 Segment 2
Group Name ST Description ST Description ST
```

```
-----
test p2p7 UP BE222.2 UP 10.0.0.11 222 UP
Backup
10.0.0.12 222 DN
-----
```

3.2.5.4 ASR 9000 nV Edge-cluster

Het [vorige ontwerp](#) op basis van MC-LAG en PW redundantie werkt prima voor redundantie, maar omdat sommige bundelleden in stand-by status zijn, dragen ze geen verkeer onder stabiele omstandigheden.

Als u wilt dat alle bundelleden actief zijn, zelfs onder stabiele omstandigheden, kunt u een ASR 9000 cluster gebruiken met bundelleden van de CE aangesloten op elk rek van de PE:



Dit ontwerp biedt redundantie tegen een bundelkoppelingfout tussen de CE en de PE, een rackstoring en een kernkoppelingfout - zolang het cluster dual is aangesloten op de MPLS-kern en er redundantie in de kern is. De twee racks hoeven niet op dezelfde locatie te worden geplaatst en kunnen zich op verschillende locaties bevinden. Inter-rack links zijn niet in dit diagram weergegeven.

Als u redundantie op de CE wilt, kunt u een multichassis oplossing voor de CE gebruiken:

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

De configuratie op het ASR 9000-cluster is zeer eenvoudig:

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

Cisco raadt u aan een statisch LACP-systeem MAC-adres en een bundel MAC-adres te configureren om te voorkomen dat een MAC-adreswijziging wordt veroorzaakt door een aangewezen shelf controller-overschakeling. Dit voorbeeld toont hoe de adressen te vinden:

```
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
```

Samengevat, dit is bundel-ether 222 met een lid op elk rek (tien 0/0/0/8 op rek 0 en tien 1/0/0/8 op rek 1) en de bundel subinterface die voor een punt-tot-punt dwars wordt gevormd verbindt:

```
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
```

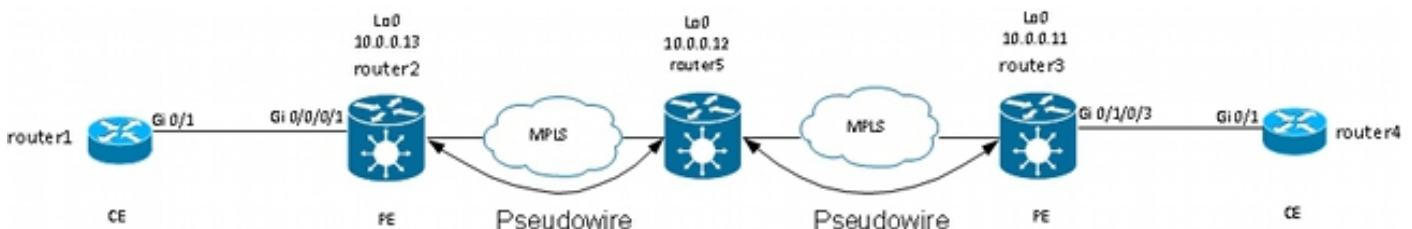
```
Group Name ST Description ST Description ST
```

```
-----
```

```
test p2p8 UP BE222.2 UP 10.0.0.13 8 UP
```

3.3 CDP

Routers en switches van Cisco verzenden CDP-pakketten meestal zonder dot1q-tags. Er zijn meerdere scenario's die bepalen wat er gebeurt met deze CDP-pakketten wanneer deze worden ontvangen door een IOS XR-router die is geconfigureerd voor een kruisschakeling:



In deze topologie, kan router1 zijn lokale PE router2 als buur CDP of de verre router van CDP 4, afhankelijk van de configuratie zien.

3.3.1 CDP niet ingeschakeld op hoofdinterface van L2VPN PE

De CDP-pakketten van de L2VPN CE worden over de cross connect vervoerd. De twee L2VPN CE's zien elkaar (met behulp van de opdracht `show cdp buren`) als de hoofdinterface is geconfigureerd als I2transport of als er een subinterface is die overeenkomt met de niet-gelabelde

CDP-frames.

Dit is een voorbeeld van de hoofdinterface:

```
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
!
!
!
!
```

Dit is een voorbeeld van een ongetagde subinterface:

```
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
!
!
!
!
```

In deze twee voorbeelden, worden de CDP pakketten vervoerd over het kruis verbinden, en CEs zien elkaar als CDP burens. De CE ziet de PE niet als een CDP-buur:

```
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 ingeschakeld op hoofdinterface van L2VPN PE

PE verwerkt de untagged CDP pakketten, en de PE en CE zien elkaar als burens. De CE ziet echter geen externe CE wanneer CDP is ingeschakeld op de hoofdinterface van de L2VPN PE.

Let op:

- U kunt CDP niet configureren op een hoofdinterface die is geconfigureerd als l2transport.
- PE onderschept de CDP pakketten wanneer CDP op de belangrijkste niet-l2transport interface wordt gevormd. Dit gebeurt zelfs als er een l2transport subinterface is geconfigureerd om de untagged CDP pakketten aan te passen (met gebruik van de **inkapseling untagged** of **inkapseling standaard** opdrachten). CDP-pakketten worden in dit

geval niet naar de externe site vervoerd.

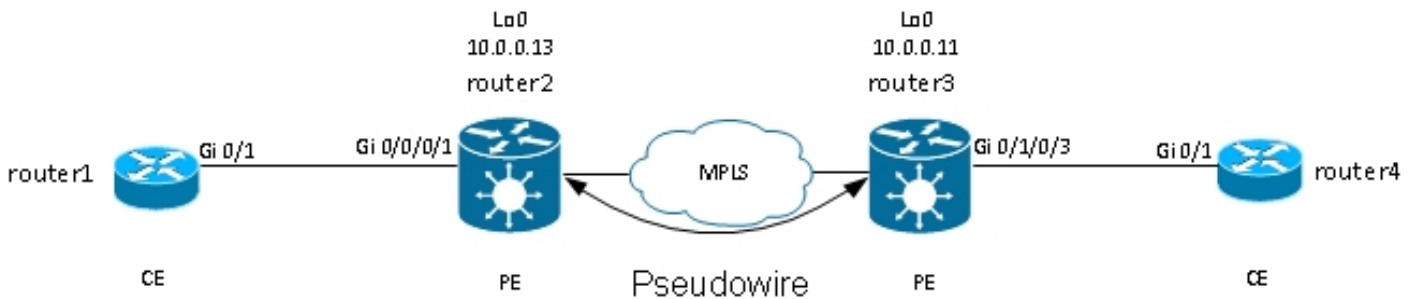
3.4 Spanning Tree

Als de L2VPN CE een Ethernet-switch is en overspannende BPDU's naar de L2VPN PE stuurt, worden deze BPDU's als gewoon verkeer verwerkt en vervoerd volgens de L2VPN-configuratie.

STP of MST BPDUs worden verzonden untagged en door het punt-tot-punt kruis vervoerd verbinden als de belangrijkste interface als l2transport wordt gevormd of als er een l2transport subinterface die met de **inkapseling untagged** of **inkapseling standaard** bevelen wordt gevormd is.

Per VLAN Spanning Tree Plus (PVST+) of Rapid PVST+ (PVRST+) verstuurd gelabelde BPDU's die worden getransporteerd als er een l2transport-subinterface is die overeenkomt met de dot1q-tag van de BPDU's.

Dit is een voorbeeldtopologie:



Router2 en router3 transporteren untagged frames en frames met 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
!
!
!
!
```

Switch 1 ontvangt de niet-gelabelde BPDU's in VLAN 1 en de gelabelde BPDU's in VLAN2 vanaf switch 4; de basispoort bevindt zich op Gi0/1 richting 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

```

Met deze configuratie wordt het overspannen - boombdomein bij plaats A samengevoegd met het overspannen - boombdomein aan kant B. Een potentieel probleem is dat het overspannen - boombdomein bij één plaats aan de andere plaats zou kunnen verspreiden.

Als u er zeker van bent dat één site alleen via één PW met een andere site is verbonden en dat er geen backdoor link is die een fysieke loop kan introduceren, is het een goed idee om geen overspannende boom over de twee sites te gebruiken. Dit houdt de twee overspannende boombdomeinen geïsoleerd. Om dit te doen, vorm een overspannen - boom bpdfilter op CEs, of vorm een ethernetdiensten toegang-lijst op PEs om kaders met het adres van bestemmingsMAC te laten vallen dat door BPDUs wordt gebruikt. Een Ethernet-services toeganglijst op de PoS kan worden gebruikt om frames met de BPDU-doelmap MAC of andere soorten L2-protocollen die u niet via de PW wilt doorsturen, te laten vallen.

Dit is een toeganglijst die u zou kunnen gebruiken onder elke I2transport (sub)interface die wordt vervoerd tussen de twee 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
!
```

De ACL voor Ethernet-services begint de BPDU's te laten vallen:

```
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)
```

Switch 1 ontvangt de BPDU's niet meer van switch 4, dus switch 1 is nu de hoofdmap:

```
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

Het risico van het uitschakelen van het overspannen - boom op een link is dit: als een backdoor verbinding tussen de plaatsen wordt gemaakt, introduceert het een fysieke lijn, en het overspannen - de boom kan de lijn niet breken. Dus als u het overspannen van een boom over een PW uitschakelt, zorg er dan voor dat er geen redundante koppelingen tussen sites zijn en dat de PW de enige verbinding tussen de sites blijft.

Als er meerdere verbindingen tussen locaties zijn, gebruikt u een oplossing zoals VPLS samen met een toegangsgateway versie van de overspannende structuur, zoals MST Access Gateway (MSTAG) of PVST+ Access Gateway (PVSTAG). Zie het gedeelte over [Multipoint Service](#) voor meer informatie.

4. Multipoint service

Opmerkingen:

Gebruik de [Command Lookup Tool \(alleen voor geregistreerde gebruikers\)](#) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

De [Output Interpreter Tool \(alleen voor geregistreerde klanten\)](#) ondersteunt bepaalde opdrachten met **show**. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show**.

Zie [Multipoint Layer 2 Services implementeren](#) voor een volledige beschrijving van de multipoint L2-functies.

Met slechts twee interfaces in een point-to-point cross connect, een L2VPN switch neemt alles ontvangen aan de kant en door te sturen het aan de andere kant.

Wanneer er meer dan twee interfaces in een bridge-domain zijn, moet een Ethernet-switch een switching-besluit nemen om te bepalen waar frames moeten worden doorgestuurd op basis van hun doelmap. De switch doet MAC-leren op basis van het bron-MAC-adres van de frames die het ontvangt en bouwt een mac-adres-tabel.

De switch zendt frames in deze methode door:

- Uitzendframes worden overstroomd naar alle poorten. Gebruik stormcontrole om de uitzending overstromingssnelheid te beperken.
- Multicastframes worden overstroomd naar alle poorten in het bridge-domein, behalve wanneer Internet Group Management Protocol (IGMP) of Multicast Listener Discovery (MLD)-snooping is geconfigureerd. Gebruik stormcontrole om de multicast overstromingssnelheid te beperken.
- Unicast-frames met een MAC-adres van de bestemming dat geen deel uitmaakt van de mac-adrestabel van het bridge-domein (onbekende unicast) worden op alle poorten in het bridge-domein overstroomd. Gebruik stormcontrole om de overstromingssnelheid van onbekende

unicast te beperken.

- Unicast-frames met een MAC-adres van de bestemming dat deel uitmaakt van de mac-adres-tabel van het bridge-domein worden doorgestuurd naar de poort waar het MAC-adres van de bestemming is geleerd.

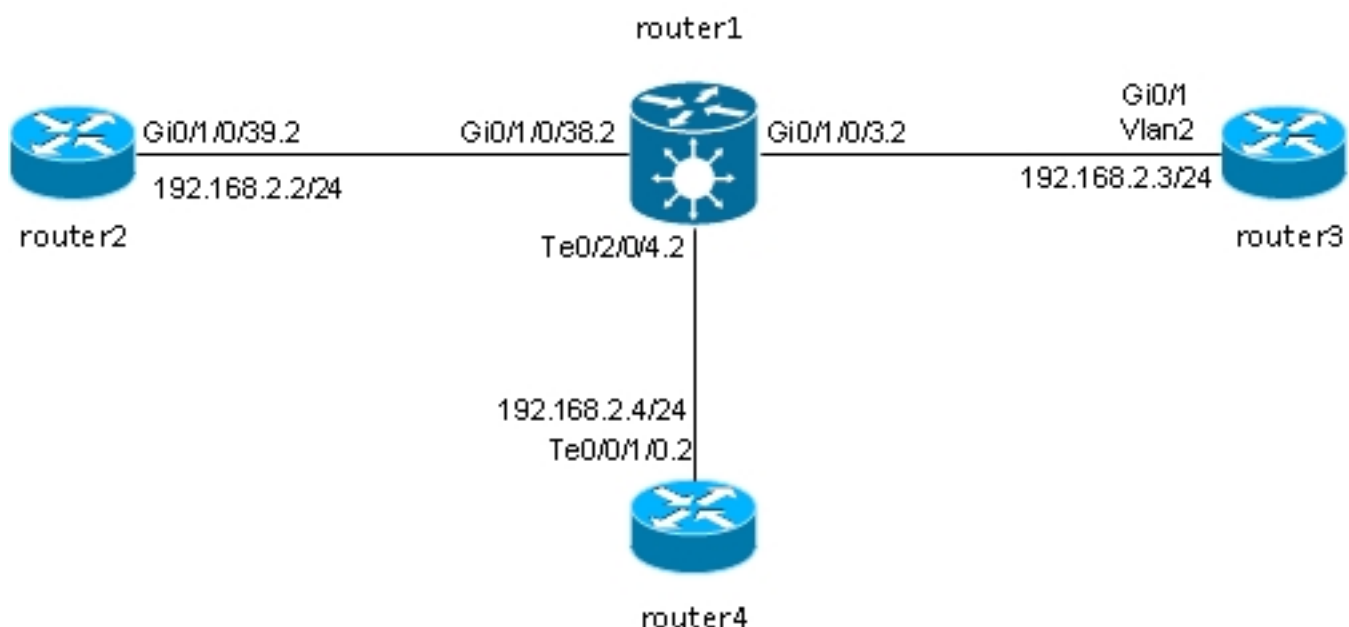
In Cisco IOS XR-software wordt een broadcast-domein of een geëmuleerde LAN een bridge-domein genoemd. Dit is vergelijkbaar met een VLAN in Cisco IOS-softwareterminologie, behalve dat een VLAN in IOS is gekoppeld aan een VLAN-nummer dat wordt gebruikt als de dot1q-tag op de trunks. Een bridge-domein in Cisco IOS XR-software is niet gekoppeld aan een dot1q VLAN-tagnummer. U kunt het EVC-model gebruiken om de dot1q-tags te manipuleren en dot1q subinterfaces met verschillende dot1q VLAN-nummers in hetzelfde bridge-domein te hebben of om untagged interfaces te hebben.

Een bridge-domein is in principe één broadcast-domein waar uitzendingen en multicast frames overstroomd zijn. Eén mac-adres-tabel is gekoppeld aan elk bridge-domein (tenzij MAC-leren handmatig is uitgeschakeld door configuratie, wat zeer zeldzaam is). Dit komt meestal overeen met één IPv4- of IPv6-subnetverbinding waar alle hosts in het bridge-domein direct verbonden zijn.

De brug-domeinen kunnen binnen een bruggroep worden gegroepeerd. Dit is een handige manier om de configuratie te controleren. U kunt één show commando uitvoeren voor een bridge groep in plaats van één show commando voor elk bridge-domein. Een bruggroep heeft geen mac-adres-lijst of andere verenigingen; het wordt enkel gebruikt voor configuratie en toont bevelen.

4.1 Lokale switching

Dit is een heel eenvoudig voorbeeld:



Router2, router3, en router4 worden aangesloten door een ASR 9000, die LAN tussen die drie routers simuleert.

Dit zijn de interfaceconfiguraties op die drie routers:

```
RP/0/RSP0/CPU0:router2#sh run int gig 0/1/0/39.2
interface GigabitEthernet0/1/0/39.2
ipv4 address 192.168.2.2 255.255.255.0
encapsulation dot1q 2
!
```

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

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

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

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

```
router3#
```

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

Pakketten worden ontvangen door router1 met de dot1q tag 2 en worden doorgestuurd naar de andere routers met de dot1q tag 2.

In dit basisscenario zijn er twee opties voor de wisselkoersen:

1. Aangezien alle AC's de dot1q-tag 2 gebruiken, kunt u deze op het frame houden en het frame op de uitgangsinterface doorsturen met dezelfde dot1q-tag als ontvangen op de ingangside. De **herschrijf ingangstag pop 1 symmetric** opdracht is niet vereist.
2. Je kunt de inkomende dot1q tag 2 in de indringingsrichting pop en symmetrisch de dot1q tag 2 in de uitgangsrichting duwen. Hoewel dit niet vereist is in dit basisscenario, is het een goed idee om het bridge-domein op deze manier aan het begin te configureren, omdat het meer flexibiliteit biedt voor de toekomst. Hier zijn twee voorbeelden van veranderingen die na eerste configuratie kunnen optreden:
 - Als een routed BVI-interface later in het bridge-domein wordt geïntroduceerd, moeten pakketten op de BVI zonder tags worden verwerkt. Zie de paragraaf voor meer informatie.
 - Later wordt er een nieuwe AC toegevoegd, die een andere dot1q-tag gebruikt. De dot1q-tag 2 zou in de indringingsrichting worden gedrukt en de andere dot1q-tag zou op de nieuwe interface in de uitgangsrichting worden gedrukt en vice versa. [BVI](#)

Pop de dot1q-tags op elke AC op router1:

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

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

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

Bekijk de configuratie van het bridge-domein met deze drie AC's:

```
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
!
!
!
!
```

Het bridge-domein moet worden geconfigureerd onder een bridgegroep. Als er andere bridge-domeinen van deze klant nodig zijn, kunnen deze worden geconfigureerd onder dezelfde bridge-groep, customer1. Als nieuwe bridge-domeinen tot een andere klant behoren, kunt u een nieuwe bridge-groep maken. Deze voorbeelden gebruiken de klant om bridge-domeinen te groeperen, maar bridge-domeinen kunnen worden gegroepeerd op basis van alle criteria.

Gebruik de **show run l2vpn bridge group customer1 bridge-domain engineering** opdracht om de configuratie van het bridge-domein weer te geven.

Gebruik de opdracht **show run l2vpn bridge group customer1** om de configuratie van alle bridge-domeinen te bekijken.

Gebruik de **show l2vpn bridge-domain bd-name engineering** opdracht of de **show l2vpn bridge-domain group customer1** opdracht om informatie over het bridge-domein weer te geven.

```
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), VFI: 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:
```

Gebruik de **show l2vpn bridge-domain groep customer1 bd-name engineering det** opdracht als u wilt controleren dat pakketten worden ontvangen en verzonden op elke AC.

Voeg het *mac-adres* sleutelwoord toe aan de **show l2vpn doorsturen bridge-domain** opdracht als u de *mac-adres-tabel* wilt controleren:

```
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
```

Het leren van MAC wordt uitgevoerd in hardware door de lijnkaarten telkens als een kader in het bridge-domein wordt ontvangen. Er is ook een software cache van de *mac-adres-tabel*, maar deze software tabel kan niet continu worden bijgewerkt om de hardware-vermeldingen aan te passen. Wanneer het **show** commando is ingevoerd in recente code, probeert het om de software tabel te synchroniseren met de hardware tabel. Na een maximum van 15 seconden, drukt het de huidige staat van de software *mac-adres-tabel* af, zelfs als de resynchronisatie niet volledig is (bijvoorbeeld, als de tabel groot is). Gebruik **l2vpn resynchronize het door:sturen mac-adres-lijst** bevel om de software en hardwaretabellen manueel te resynchroniseren.

```
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
```

Een syslogbericht wijst erop wanneer het resynchronisatieproces volledig is, zodat is het nuttig om **eindmonitor** te hebben toegelaten om het bericht te zien.

De kolom Resync Age toont de laatste keer dat het MAC-adres is gesynchroniseerd van de hardwaretabel.

Het sleutelwoord *location* is de locatie van een inkomende of uitgaande lijnkaart. De MAC-adressen worden in hardware tussen de lijnkaarten uitgewisseld, zodat de MAC-adressen op elke lijnkaart bekend moeten zijn waar een AC of een PW is. Het trefwoord *detail* kan een recentere versie van de softwaretabel bieden:

```
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
```

De gedetailleerde versie van de opdracht geeft het totale aantal MAC-adressen die in het bridge-domein zijn geleerd, en het aantal MAC-adressen dat onder elke AC is geleerd.

Het *hardware* sleutelwoord polls de hardware mac-adres-tabel direct van de ingress of egress voorwaartse motoren:

```
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
```

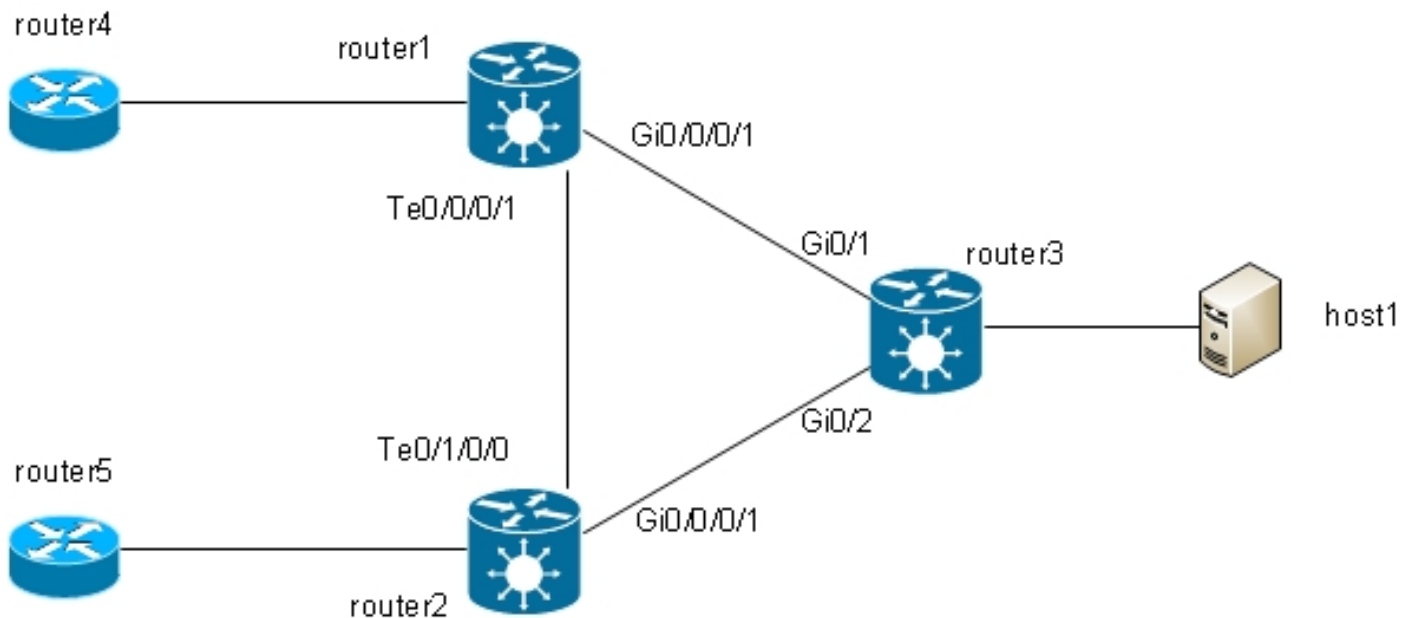
```
Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
```

```
-----
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 Volledig MST

De [eerdere voorbeelden van lokale switching](#) waren eenvoudig omdat alleen routers waren verbonden met het bridge-domein. Zodra u echter L2-switches gaat verbinden, kunt u een lus introduceren en de STP nodig hebben om de lus te doorbreken:



In deze topologie, zijn router1, router2, en router3 elk gevormd met een brug-domein met al hun interfaces in het diagram. Als router4 een uitzending, zoals een ARP verzoek, naar router1, router1 overstroomingen het aan router2 en router3, router2 overstroomingen het aan router3, en router3 vloed het aan router2. Dit resulteert in een lus en een broadcast storm.

Om de lijn te breken, gebruik een STP. Er zijn meerdere typen STP's, maar Cisco IOS XR-software biedt slechts één volledige implementatie, de MST.

Er zijn ook toegangsgatewayversies van de protocollen die in Cisco IOS XR-software worden ondersteund, zoals PVSTAG en MSTAG. Dit zijn statische, beperkte versies van het protocol om in specifieke topologieën te gebruiken, typisch met VPLS, en in de secties [MSTAG](#) en [PVSTAG](#) beschreven. In Cisco IOS XR-software is MST de enige optie als er een topologie met meerdere switches is en als een volledige overspannende-boomimplementatie vereist is.

Twee subinterfaces worden gevormd op elke router en toegevoegd aan een bridge-domein. Voor router1, is de configuratie:

```

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

```

```

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

```

MST is ingesteld op de hoofdinterface. In dit voorbeeld, wordt VLAN 2 toegewezen aan instantie 1, en alle andere VLANs blijven standaardinstantie 0. (Een realistischer configuratie zou VLANs gelijk tussen instanties verdelen.)

De selectie van de root-brug binnen een STP-netwerk wordt bepaald door de ingestelde prioriteit en de ingesloten bridge-id van elk apparaat. Het apparaat met de laagste prioriteit, of met de laagste prioriteit maar de laagste brug-ID, wordt als root-brug gekozen. In dit voorbeeld, router3 wordt gevormd met een lagere prioriteit dan router1 voor instantie 0, zodat is router3 de wortel voor instantie 0. Router1 heeft een lagere prioriteit dan router3 bijvoorbeeld 1, zodat router1 de wortel voor instantie 1 is.

Dit is de configuratie voor router1:

```

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

```

Dit is de configuratie op router3:

```

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

```

De naam, revisie en VLAN-to-instantie-toewijzing moeten op alle switches hetzelfde zijn.

Controleer nu de overspanningsboomstatus op router1:

```

RP/0/RSP1/CPU0:router1#sh spanning-tree mst customer1
Role: ROOT=Root, DSGN=Designated, ALT=Alternate, BKP=Backup, MSTR=Master

```

State: FWD=Forwarding, LRN=Learning, BLK=Blocked, DLY=Bringup Delayed

Operating in dot1q mode

MSTI 0 (CIST):

VLANS Mapped: 1,3-4094

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

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

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

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

MSTI 1:

VLANS Mapped: 2

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

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

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

Router3 is de wortel bijvoorbeeld 0, zodat router1 zijn wortelhaven op Gi0/0/0/1 naar router3 heeft.
Router1 is de wortel bijvoorbeeld 1, zodat router1 de aangewezen brug op alle interfaces voor die instantie is.

Router2 is geblokkeerd, bijvoorbeeld 0 op 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 wordt doorgestuurd terwijl Te0/1/0/0.3 geblokkeerd is. Wanneer de STP geblokkeerde waarde 0x0 is, is de voorwaarde vals, zodat door:sturen de interface; wanneer de STP geblokkeerde waarde 0x1 is, is de voorwaarde waar, zodat wordt de interface geblokkeerd.

Gebruik de opdracht **debietgegevens tonen** om dit te bevestigen en de interfacegegevens weer te geven die in de netwerkprocessor aanwezig zijn:

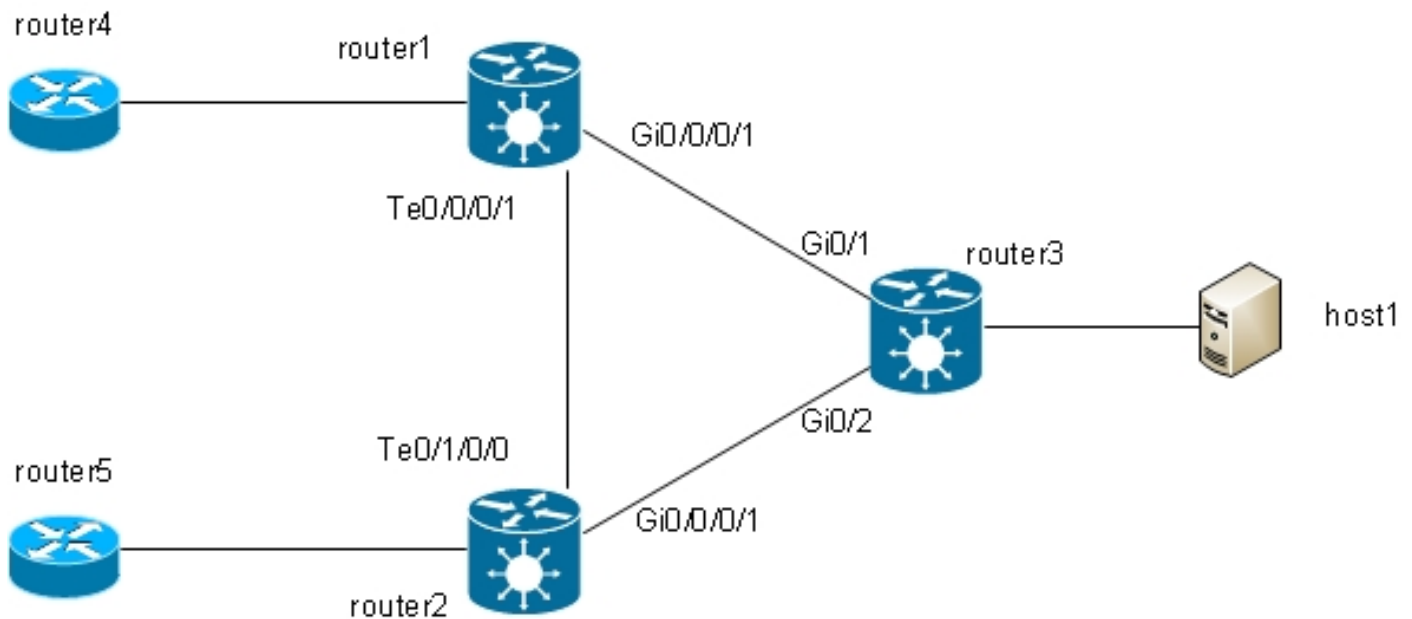

```
RP/0/RSP1/CPU0:router2#sh uidb data location 0/1/CPU0 TenGigE0/1/0/0.2
ingress | i Blocked
STP Blocked                                0x0
RP/0/RSP1/CPU0:router2#sh uidb data location 0/1/CPU0 TenGigE0/1/0/0.3
ingress | i Blocked
STP Blocked                                0x1
```

4,3 BVI

De configuratie van een bridge-domein maakt een L2-domein. Om dat L2 domein te verlaten, sluit L3 routers die tussen hosts binnen het bridge-domein en de buitenwereld routeren aan. In het [vorige diagram](#), kon host1 router4 of router5 gebruiken om lokale Subnet te verlaten en het internet te bereiken.

Router1 en router2 waar de bridge-domeinen zijn geconfigureerd zijn ASR 9000 routers, die IPv4- en IPv6-verkeer kunnen leiden. Deze twee routers zouden het IP-verkeer uit het bridge-domein kunnen halen en naar het internet zelf kunnen leiden, in plaats van te vertrouwen op L3-routers. Om dit te doen, moet u een BVI configureren, wat een L3-interface is die in een bridge-domein steekt om pakketten in en uit het bridge-domein te routeren.

Zo ziet het er logisch uit:



Dit is de configuratie:

```
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
!

```

Een BVI is een niet-gelabelde L3-interface, dus als u het BVI-proces wilt hebben van de pakketten die worden ontvangen op de AC's van het bridge-domein, moeten de AC's worden geconfigureerd om alle inkomende tags te pop. Anders kan de BVI de tag niet begrijpen en laat de pakketten vallen. Er is geen manier om een dot1q subinterface op een BVI te configureren, dus de tags moeten worden ingedrukt op de AC's, zoals is gedaan op Gi0/0/0/1.2 in het [vorige voorbeeld](#).

Aangezien een BVI-interface een virtuele interface is, zijn er enige beperkingen op de functies die kunnen worden ingeschakeld. Deze beperkingen zijn gedocumenteerd in [Configureren van geïntegreerde routing en bridging op de Cisco ASR 9000 Series router: beperkingen voor het configureren van IRB](#). Deze functies worden niet ondersteund op de BVI-interfaces op de ASR 9000:

- Toegangscontrolelijsten (ACL's). L2 ACL's kunnen echter op elke L2-poort van het bridge-domein worden geconfigureerd.
- IP Fast Reroute (FRR)
- NetFlow
- MoFRR (alleen multicast snelle omleiding)
- MPLS-labelswitching
- mVPNv4
- Quality-of-Service (QoS)
- Traffic mirroring
- Ongenummerde interface voor BVI
- Videobewaking (Vidmon)

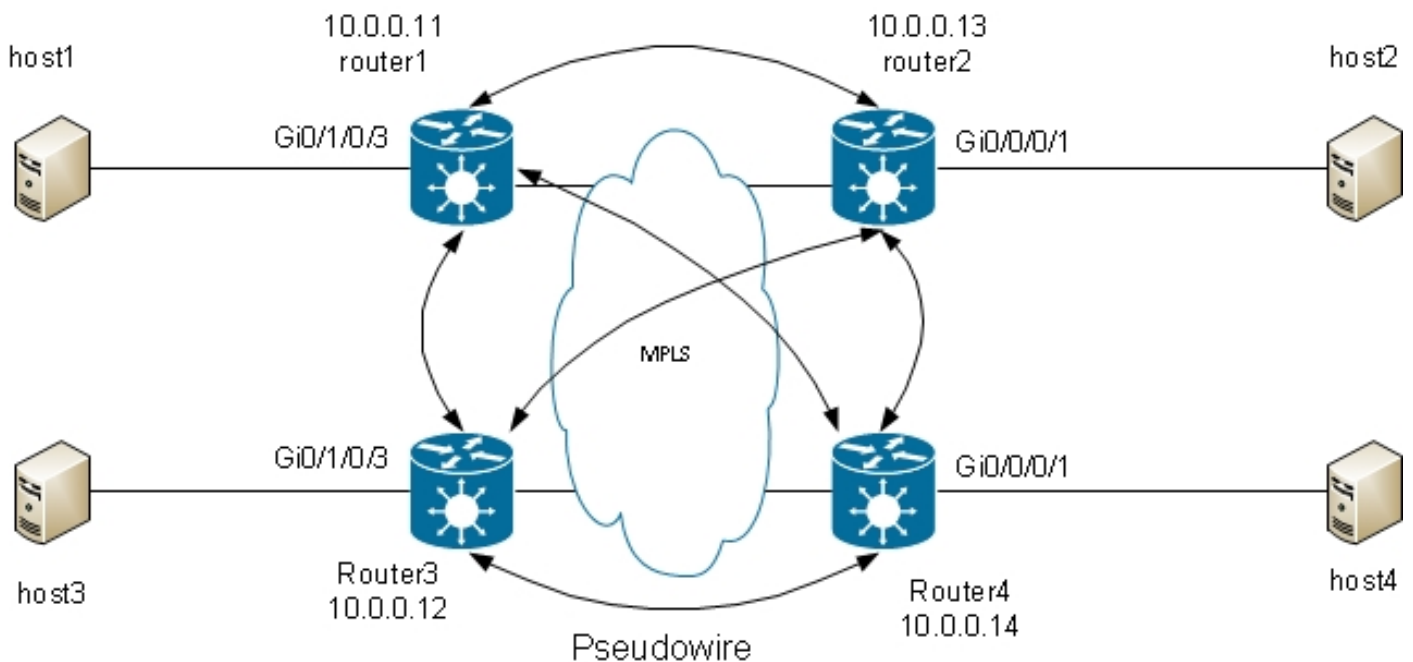
De BVI kan in een Virtual Routing and Forwarding (VRF)-configuratie worden gebruikt, zodat verkeer dat op de BVI wordt ontvangen via MPLS wordt doorgestuurd, maar de *label-toewijzingsmodus per-Vrf* moet worden gebruikt.

Als een van deze beperkte functies vereist is, kunt u geen BVI gebruiken. Een andere oplossing is om een externe loopback kabel tussen twee poorten op de router te gebruiken, waar één poort in het bridge-domein is en één poort is geconfigureerd als een normale routed interface waar alle functies kunnen worden geconfigureerd.

4,4 VPLS

4.4.1 Overzicht

VPLS biedt de mogelijkheid om bridge-domeinen op meerdere locaties te combineren tot één groot bridge-domein via MPLS PW's. Gastheren op de verschillende locaties lijken rechtstreeks verbonden te zijn met hetzelfde L2-segment omdat hun verkeer transparant is ingekapseld over het volledige netwerk van MPLS PW's tussen L2VPN-PE's:



Een volledig netwerk van PW's wordt vereist om ervoor te zorgen dat elke gastheer verkeer van alle andere gastheren kan ontvangen. Het gevolg is dat een L2VPN PE geen frame doorstuurt dat ontvangen is op een VPLS PW via andere VPLS PW's. Er zou een volledige maas van PW's moeten zijn, zodat elke PE het verkeer direct ontvangt en hoeft geen verkeer tussen PW's door:sturen aangezien het door:sturen een lijn zou veroorzaken. Dit wordt de gespleten horizonregel genoemd.

De router voert MAC learning uit. Zodra een MAC-adres in de mac-adres-tabel aanwezig is, verstuurt u alleen het frame voor dat bestemmings-MAC-adres via de PW naar de L2VPN-PE waar dit MAC-adres van is geleerd. Dit voorkomt onnodige duplicatie van verkeer in de kern. Uitzendingen en multicast worden overstromd over alle PW's om ervoor te zorgen dat alle hosts ze kunnen ontvangen. Een functie zoals IGMP-spionage is nuttig omdat het multicast frames alleen naar PE's kan worden verzonden waar er ontvangers of multicast routers zijn. Dit vermindert de hoeveelheid verkeer in de kern, hoewel er nog steeds meerdere kopieën van dezelfde pakketten die naar elke PE moeten worden verzonden wanneer er interesse is voor die groep.

Het volledige netwerk van PW's moet worden geconfigureerd in het kader van een 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
!
!
!
!
!

```

De PW's die onder de VFI zijn ingesteld, zijn die welke volledig zijn ingekapseld in de kern. Ze maken deel uit van dezelfde gesplitste horzongroep (SHG) om ervoor te zorgen dat frames die op een PW worden ontvangen niet naar een andere PW worden doorgestuurd.

Het is mogelijk om toegang PWs te vormen, die als type van AC worden beschouwd en niet onder VFI worden gevormd. Zie de paragraaf voor meer informatie.

De configuratie op router2, router3, en router4 is zeer gelijkaardig, en allen hebben de andere drie routers als burens onder 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 up [H-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
```

Het lokale label voor de PW tot 10.0.0.12 is 16049, wat betekent dat Ethernet-frames worden ontvangen met de 16049. De schakelbeslissing is gebaseerd op dit MPLS-label omdat de voorlaatste MPLS hop het IGP-label zou moeten hebben verlaten. Er kan nog steeds een expliciet null-label zijn, maar het switchingbesluit is gebaseerd op het PW-label:

```
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
```

De **show mpls doorsturen labels** opdracht voor het label geeft het bridge-domein nummer, dat u kunt gebruiken om het doelmac-adres en het PW (buurman en pw-id) te vinden waar het pakket werd ontvangen. U kunt dan ingangen in de mac-adres-lijst tot stand brengen die op die buur richten:

```
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 PW-typen en getransporteerde tags

VPLS PW's worden standaard als type 5 (Ethernet) PW's verwerkt. Wat er ook in de AC komt nadat er gemanipuleerd is met VLAN-tags (wanneer de opdracht **herschrijven** is geconfigureerd), wordt via de PW verzonden.

Met Cisco IOS XR-software release 4.1.0 voor LDP-signalering en release 4.3.1 met BGP kunt u een pw-klasse configureren onder een buur en via **transportmodus een VLAN-passthrough** configureren onder de pw-klasse. Dit bespreekt een PW van het virtuele verbinding (VC) type 4 (Ethernet VLAN), die vervoert wat uit AC na de de markeringsmanipulatie van VLAN komt wanneer het **herschrijfbevel** wordt gevormd.

De manipulatie van VLAN-tags op de EFP zorgt ervoor dat er ten minste één VLAN-tag op het frame achterblijft omdat u een dot1q-tag op het frame nodig hebt als er VC-type 4 PW's zijn. Er wordt geen dummy tag 0 aan het frame toegevoegd wanneer u de **vlan passthrough**-modus voor **transportmodus** gebruikt.

Een combinatie van PW's van type 4 en type 5 onder dezelfde VFI wordt niet ondersteund. Alle PW's moeten van hetzelfde type zijn.

```
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 Automatische detectie en signalering

Deze waren gebaseerd op handmatige configuratie van alle burens onder de VFI. MPLS LDP is gebruikt voor de signalering van PW met de [eerdere voorbeelden](#) buurman.[Previous](#)

Wanneer u een nieuwe PE VPLS aan het netwerk toevoegt, configureer de PE om een PW te hebben voor alle bestaande PE's in elk van zijn lokale bridge-domeinen. Alle bestaande PE's moeten dan worden aangepast om een PW te hebben voor de nieuwe PE, omdat alle PE's volledig moeten worden ingepast. Dit zou een operationele uitdaging kunnen worden naarmate het aantal PE's en bridge-domeinen toeneemt.

Een oplossing is om PE's andere PE's automatisch te laten ontdekken via BGP. Hoewel IBGP ook met volle mazen kan worden opgeheven door het gebruik van routeflectoren. Zo wordt een nieuwe PE typisch gevormd om met een klein aantal route-reflectoren te peer, ontvangen alle andere PEs

zijn updates, en nieuwe PE ontvangt de updates van de andere PEs.

Om andere PE's te ontdekken via BGP, wordt elke PE geconfigureerd voor de *vpls-vpws-adresfamilie* en adverteert in BGP met de bridge-domeinen waaraan ze willen deelnemen. Zodra de andere PE's die deel uitmaken van hetzelfde bridge-domein worden ontdekt, wordt voor elk van hen een PW vastgesteld. BGP is het protocol dat voor deze automatische detectie wordt gebruikt.

Er zijn twee opties voor de signalering van PW aan de automatisch ontdekte PEs: BGP en LDP. In deze voorbeelden converteert u de [vorige topologie](#) naar BGP-automatische detectie met BGP-signalering en LDP-signalering.

4.4.3.1 BGP-automatische detectie en BGP-signalering

Configureer de **adresfamilie l2vpn vpls-vpws** onder router bgp en de burenen, die andere PE's of de routerelectoren zijn:

```
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
!
```

De nieuwe adresfamilie wordt actief met de burenen, maar geen PE heeft zijn deelname aan een brugdomein nog geadverteert:

```
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
```

Configureer **autodiscovery bgp** en **signaleringsprotocol bgp** onder de configuratiemodus voor L2VPN bridge-domein. De configuratie op router1 is:

```
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
!
!
!
!
!
```

De configuratie op router2 is:

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

De VPN-id en het routedoel zijn hetzelfde op de verschillende PE's voor elk bridge-domein, maar elke PE heeft een unieke Virtual Edge Identifier (VE-ID). Elke PE ontdekt de andere PE's in de VPN via BGP en gebruikt BGP om de PW's te signaleren. Het resultaat is een volledige maas van 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

Dit zijn de prefixes geadverteerd door router3 (10.0.0.13) zoals gezien op router1; de prefixes worden ontvangen door de twee route-reflectoren, 10.0.0.3 en 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

Router1 heeft sommige PWs gevestigd:

```
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 BGP-automatische detectie en LDP-signalering

De BGP-configuratie met de opdracht **l2vpn vpls-vpws** voor de **adresfamilie** is precies hetzelfde als met BGP-signalering. De L2VPN-configuratie wordt aangepast om LDP-signalering te gebruiken met de opdracht **Signaling-protocol ldp**.

De zelfde configuratie wordt gebruikt op alle vier 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
!
!
!
!
!
!

```

De vpls-id bestaat uit het BGP Autonomous System (AS)-nummer en de VPN-id.

Drie showbevelen van router1 illustreren dat PWs met ontdekte PEs zijn gevestigd:

```
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 MAC-flushes en -opnames

Doorsturen in VPLS is gebaseerd op de mac-adres-tabel, die dynamisch wordt gebouwd door de bron-MAC-adressen te leren van de frames die worden ontvangen. Als er een topologieverandering in een bridge-domein is, kan een host bereikbaar worden via een andere AC of VPLS buur. Het verkeer voor die host bereikt zijn bestemming mogelijk niet als frames doorgestuurd blijven worden volgens de bestaande MAC-adres-tabel.

Voor een L2VPN PE zijn er meerdere manieren om een topologiewijziging te detecteren:

- Een poort in het bridge-domein gaat omhoog of omlaag.
- Een overspannende boom Topology Change Notification (TCN) BPDU wordt verwerkt wanneer de L2VPN PE de volledige MST-implementatie of een overspannende boom toegangsgateway protocol uitvoert. De falende link is misschien niet lokaal op de PE, maar kan verder weg liggen in de topologie. De PE onderschept het TCN.

Wanneer een L2VPN PE een topologieverandering ontdekt, neemt het twee acties:

1. PE spoelt de mac-adres-lijst van de brug-domeinen die door de topologieverandering worden beïnvloed. Wanneer de PoE is geconfigureerd voor PVSTAG of Per-VLAN Rapid Spanning Tree Access Gateway (PVRSTAG), heeft een TCN BPDU die in één VLAN-subinterface is gedetecteerd, invloed op alle VLAN's en bridge-domeinen op die fysieke interface.
2. De PE signaleert aan de VPLS burens door een MPLS LDP MAC-terugtrekkingsbericht dat zij hun mac-adres-tabel moeten doorspoelen. Alle externe L2VPN-PE's die het MAC-onthoudings LDP-bericht ontvangen, doorspoelen hun mac-adres-tabellen, en het verkeer wordt opnieuw overspoeld. De mac-adres-tabellen worden opnieuw opgebouwd op basis van de nieuwe topologie.

Het standaardgedrag van het MAC-verwijderingsbericht in het geval van een havenflap is in de loop van de tijd gewijzigd:

- Een L2VPN PE verstuurde in Cisco IOS XR-software traditioneel MAC-terugtrekkingsberichten wanneer een AC-netstroom afliep. De bedoeling was om externe PE's hun MAC-adrestabellen te laten doorspoelen voor het getroffen bridge-domein, zodat de MAC-adressen die achter de neergehaalde poort aanwijzen van een andere poort zouden worden geleerd.
- Dit leidde echter tot een interoperabiliteitsprobleem met een aantal externe PE's die RFC

4762 volgen en de MAC-adressen die op alle PE's wijzen verwijderen, behalve de ene die het MAC-onthoudingsbericht verstuurt. RFC 4762 gaat ervan uit dat een PE een MAC onthoudingsbericht zou versturen wanneer een AC omhoog komt, maar niet wanneer een AC omlaag gaat. Na Cisco IOS XR-software release 4.2.1 is het standaardgedrag om LDP-MAC-terugtrekkingsberichten alleen te verzenden wanneer er een bridge-domeinpoort verschijnt om beter aan de RFC te voldoen. Er is een configuratieopdracht toegevoegd om terug te keren naar het oude gedrag.

Dit is een showopdracht met het standaardgedrag na 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:
```

De belangrijke regel is de 'MAC trekkings verzonden op bridge port down,' die nu standaard uitgeschakeld is na Cisco IOS XR-software release 4.2.1. Het commando geeft ook het aantal MAC-terugtrekkingsberichten verzonden en ontvangen in het bridge-domein. Een groot aantal terugtrekkingsberichten duidt op instabiliteit in het brugdomein.

Dit is de configuratie die terugkeert naar het oude gedrag:

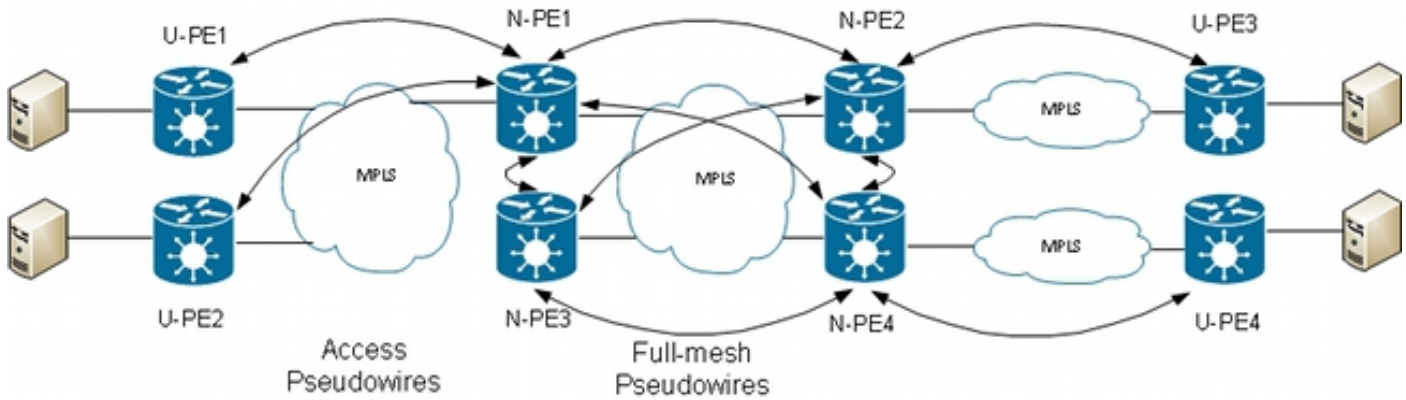
```
l2vpn
bridge group customer1
bridge-domain finance
mac
withdraw state-down
!
!
!
!
```

4.4.5 H-VPLS

VPLS vereist een volledige maas van PWs tussen L2VPN PEs om ervoor te zorgen dat elke PE, in één hop, een gastheer achter een andere PE kan bereiken zonder de behoefte aan één PE om kaders van één PW aan een andere PW te weerspiegelen. Dit is de basis voor de gesplitste horizonregel, die verhindert dat een PE frames doorstuurt van één PW naar een andere PW. Zelfs in speciale gevallen, waar het adres van bestemmingsMAC in de MAC-adres-lijst bij een andere PW punten, wordt het kader gelaten vallen.

Een volledig netwerk van PWs betekent dat het aantal PWs zeer hoog zou kunnen worden aangezien het aantal PEs groeit, zodat dit schaalbaarheidskwesties zou kunnen introduceren.

U kunt het aantal PWs in deze topologie met een hiërarchie van PEs verminderen:



In deze topologie, merk op dat:

- Een U-PE-apparaat (User Provider Edge) heeft AC's voor de CE's.
- Het U-PE apparaat transporteert het CE-verkeer via een MPLS point-to-point PW naar een Network Provider Edge (N-PE) apparaat.
- De N-PE is een kern-VPLS PE die volledig is vernet met andere N-PE's.
- Op de N-PE wordt de PW die uit de U-PE komt beschouwd als een toegang PW net als een AC. De U-PE maakt geen deel uit van het netwerk met de andere N-PE's, zodat de N-PE de toegang PW als een AC en voorwaarts verkeer kan beschouwen van die toegang PW tot de kern-PW's die deel uitmaken van het VPLS volledige netwerk.
- De kern-PW's tussen N-PE's worden geconfigureerd onder een VFI om ervoor te zorgen dat de gesplitste horizonregel wordt toegepast op alle kern-PW's die onder de VFI zijn geconfigureerd.
- Toegang PW's van U-PE's zijn niet geconfigureerd onder een VFI, zodat ze niet tot dezelfde SHG behoren als de VFI PW's. Verkeer kan worden doorgestuurd van een toegangs-PW naar een VFI-PW en vice versa.
- U-PE's kunnen de PW-redundantiefunctie gebruiken om een primaire PW te hebben naar een primaire N-PE en een stand-by PW naar een standby N-PE. De stand-by neemt het over wanneer de primaire PW daalt.

Dit is een voorbeeld waarbij U-PE1 (10.0.0.15) is geconfigureerd met PW-redundantie voor N-PE1 (10.0.0.11) en 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
-----
```

De PW naar 10.0.0.12 staat in de stand-by modus. Op de N-PE1 zijn er een toegang PW tot 10.0.0.15 en een AC die niet onder de VFI vallen.

N-PE1 leert sommige MAC-adressen via de toegang PW en VFI PW's:

```
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
```

Op N-PE2 (10.0.0.12) staat de toegang PW in stand-by:

```
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 Splitsen van horizontale groepen (SHG's)

De gesplitste horizonregel schrijft voor dat een frame dat op een VFI-PW wordt ontvangen, niet over een andere VFI-PW kan worden doorgestuurd. VFI N-PE's moeten volledig worden vermeld.

Deze gespleten horizon wordt afgedwongen door een SHG:

- Leden van de ene SHG kunnen geen frames doorsturen naar elkaar, maar kunnen frames doorsturen naar leden van andere SHG's.
- Alle VFI-PW's worden standaard aan SHG 1 toegewezen. Dit zorgt ervoor dat er geen doorsturen tussen VFI PW's plaatsvindt, zodat de gesplitste horizonregel wordt afgedwongen. Pakketten die worden ontvangen op een VFI-PW kunnen worden doorgestuurd naar AC's en toegang krijgen tot PW's omdat ze geen deel uitmaken van dezelfde SHG.
- Alle AC's en access PW's maken standaard geen deel uit van een SHG-groep, wat betekent

dat pakketten die worden ontvangen op een AC of access PW kunnen worden doorgestuurd naar een andere AC of toegang PW in hetzelfde bridge-domein.

- AC's en toegang PW's kunnen worden toegewezen aan de SHG 2 met het commando **van de split-horizon groep** als het doel is om doorsturen tussen hen te voorkomen.

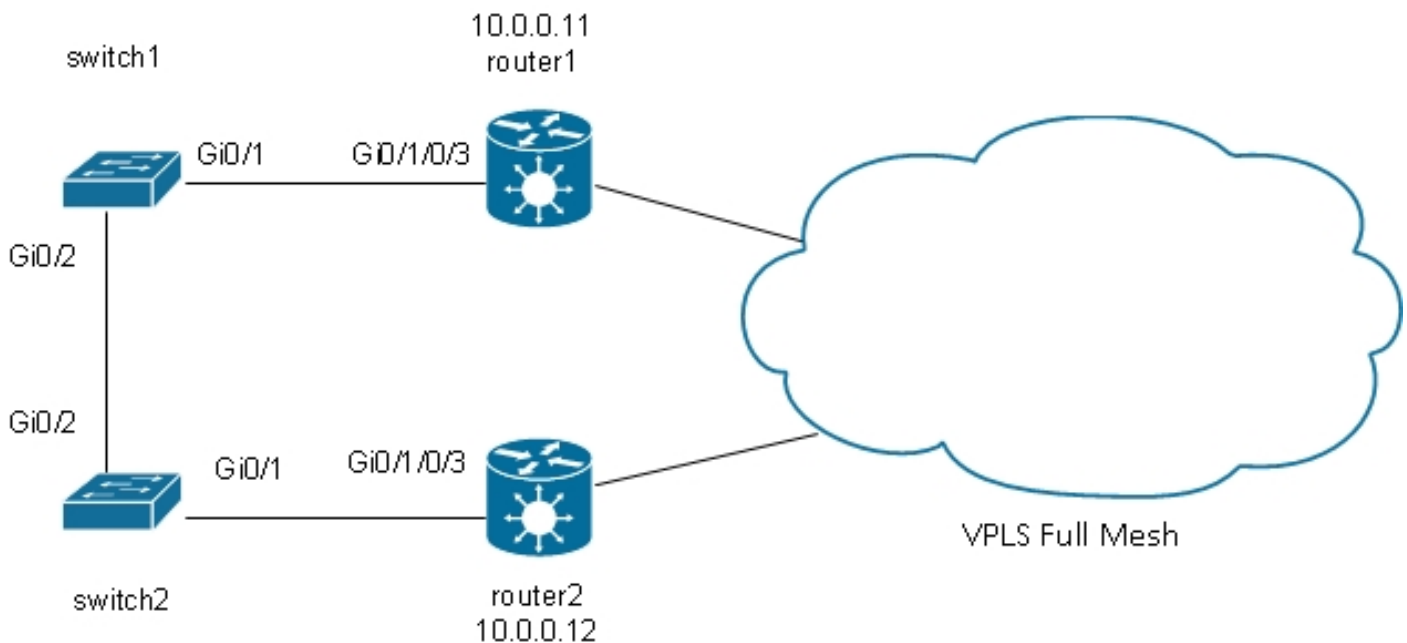
```
RP/0/RSP0/CPU0:N-PE1#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
bridge group customer1
bridge-domain engineering
interface GigabitEthernet0/0/0/1.2
split-horizon group
!
interface GigabitEthernet0/1/0/3.2
split-horizon group
!
neighbor 10.0.0.15 pw-id 15
split-horizon group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

In deze configuratie is er geen doorsturen tussen Gi 0/0/0/1.2 en Gi 0/1/0/3.2, Gi 0/0/0/1.2 en 10.0.0.15, of Gi 0/1/0/3.2 en 10.0.0.15. Maar er kan nog steeds verkeer doorsturen tussen de AC's en de VFI PW's omdat ze deel uitmaken van verschillende SHG's (1 en 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 Redundantie

In een poging om redundantie te introduceren, kunt u een site hebben die dubbel is gekoppeld aan het VPLS-domein:



Als een host die is aangesloten op switch 1 een broadcast verstuurt, stuurt switch 1 deze door naar router1 en switch 2. Router1 heeft een volledig netwerk van PWs, zodat is er PW aan router2, en router1 door:sturen de uitzending over dat PW. Router2 door:sturen de uitzending aan switch 2, die het aan switch 1 door:sturen. Dit resulteert in een fysieke lus.

4.4.7.1 Spanning Tree

De [volledige MST](#)-implementatie werkt niet met VPLS omdat die implementatie MST BPDU's op een hoofdinterface stuurt om de doorsturen status van alle VLAN's op die interface te controleren. Met VPLS zijn er VFI's voor elk bridge-domein, dus u kunt geen BPDU's verzenden op een hoofdinterface voor al die VFI's.

Spanning Tree BPDU's worden standaard over VPLS en point-to-point PW's getransporteerd.

Als switch 1 en switch 2 per-VLAN BPDUs of untagged MST BPDUs verzenden en als de BPDUs gelijke I2transport subinterfaces op router1 en router2, worden de BPDUs vervoerd door VPLS. De switches zien elkaars BPDU's op de Gi 0/1 interfaces, en het overspannen van de boom breekt de lus en blokkeert één poort.

Switch 2 is de basis voor 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)

```

Switch 1 heeft zijn wortelpoort op Gi 0/1 en blokkeert 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

```

Het probleem is dat de BPDU's ook naar externe sites worden getransporteerd, en dat de overspannen-boominstabiliteit in één site zich verspreidt naar alle sites die zijn verbonden met het VPLS-domein. Het is veiliger om elke plaats te isoleren en niet BPDUs over VPLS te vervoeren.

Eén oplossing is het gebruik van een versie van een toegangsgateway van de STP. Dit is een beperkte implementatie van het protocol, waar de L2VPN PEs worden geconfigureerd om wat statische BPDUs te verzenden om te lijken verbonden met de overspannende boomwortel. De L2VPN PE vervoert niet de BPDU's die van de CE's worden ontvangen naar de externe sites, zodat elke site zijn eigen overspannende boomdomein heeft.

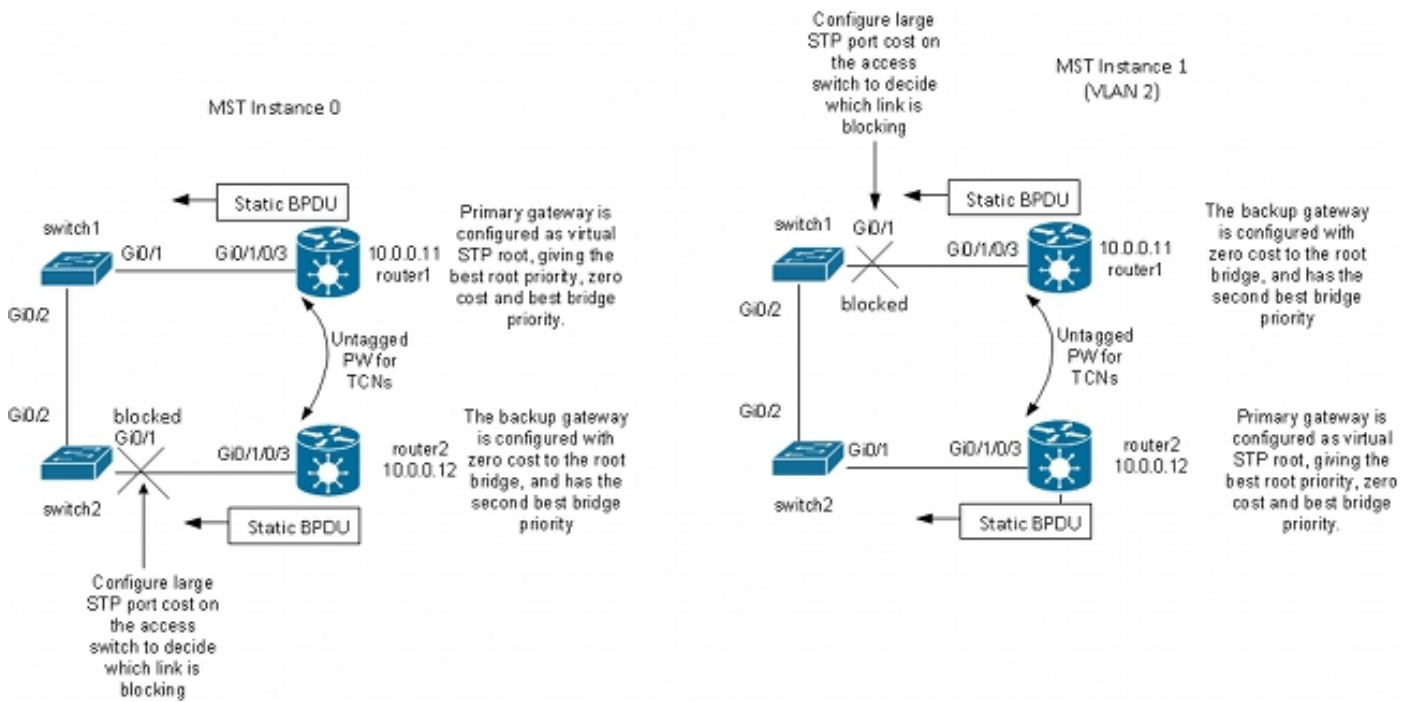
4.4.7.2 MSTAG

Zoals uitgelegd in de sectie [Spanning Tree](#) verstuurt MST niet-gelabelde BPDU's, maar deze BPDU's controleren de doorsturen status van alle VLAN's op de interface.

VLAN's kunnen worden gegroepeerd in meerdere instanties en elke instantie heeft zijn eigen doorsturen status.

VLAN's worden doorgaans gegroepeerd zodat verkeer gelijkmatig tussen meerdere paden kan worden verdeeld. Wanneer er twee paden zijn, behoort de helft van het verkeer tot een instantie die op het eerste pad doorstuurt en op het tweede pad blokkeert. De andere helft van het verkeer behoort tot een instantie die op de eerste weg blokkeert en op de tweede weg doorsturen. Dit maakt lastverdeling tussen de twee paden onder stabiele omstandigheden mogelijk. Anders hebt u één pad dat normaal volledig geblokkeerd is en alleen actief wordt als het primaire pad omlaag is.

Hier is een typische topologie MSTAG:



In dit laboratoriumvoorbeeld, heeft instantie 1 VLAN 2, en instantie 0 heeft andere VLANs. (In een realistischer scenario worden VLAN's verspreid tussen meerdere exemplaren om een goede taakverdeling tussen de exemplaren te realiseren.) Omdat sommige VLAN's veel meer verkeer hebben dan anderen, zijn er niet altijd hetzelfde aantal VLAN's in elke instantie.

Dit is de configuratie voor MST instantie 0:

- Router1 en router2 verzenden sommige statische BPDUs die op de configuratie MSTAG worden gebaseerd. Zij verwerken niet de inkomende BPDUs van het netwerk of proberen een volledige implementatie uit te voeren. Met MSTAG, verzenden de twee L2VPN PEs enkel statische BPDUs die op hun configuratie MSTAG worden gebaseerd.
- Router1 wordt gevormd om verkeer van instantie 0 aan te trekken door de wortel voor die instantie te schijnen te zijn.
- Router2 is geconfigureerd met de op één na beste basisprioriteit, bijvoorbeeld 0, zodat het de nieuwe root wordt in het geval van een router1-fout of AC-fout tussen switch 1 en router1.
- Switch 2 is geconfigureerd met een hoge overspanningskosten op de poort Gi 0/1 tot router2 om ervoor te zorgen dat zijn belangrijkste pad naar de root is op Gig 0/2 via switch 1 en router1.
- Switch 2 selecteert Gi 0/2 als wortelpoort bijvoorbeeld 0 en selecteert Gi 0/1 als een alternatieve poort voor het geval dat de wortel verloren gaat.
- Aldus, bereikt het verkeer van die plaats in VLANs die tot instantie 0 behoren andere plaatsen over VPLS door router1.

Bij de meeste gevallen 1 (VLAN 2) wordt de configuratie omgekeerd:

- Router2 wordt gevormd om verkeer van instantie 1 aan te trekken door de wortel voor die instantie te schijnen te zijn.
- Router1 is geconfigureerd met de op één na beste basisprioriteit, bijvoorbeeld 1, zodat het de nieuwe root wordt in het geval van een router2-storing of AC-storing tussen switch 2 en router2.
- Switch 1 is geconfigureerd met een hoge overspanningskosten op de poort Gi 0/1 tot router1

om ervoor te zorgen dat zijn belangrijkste pad naar de root is op Gig 0/2 via switch 2 en router2.

- Switch 1 selecteert Gi 0/2 als wortelpoort bijvoorbeeld 1 en selecteert Gi 0/1 als een alternatieve poort voor het geval dat de wortel verloren gaat.
- Aldus, bereikt het verkeer van die plaats in VLANs die tot instantie 1 behoren (VLAN 2 in dit voorbeeld) andere plaatsen over VPLS door router2.
- Er moet een subinterface op router1 en router2 zijn om untagged TCNs te vangen en hen door een punt te versturen om PW aan de andere router te richten. Omdat switch 1 en switch 2 hun directe verbindingen kunnen verliezen en van elkaar geïsoleerd kunnen raken, moeten router1 en router2 de TCN's tussen hen door dat punt-naar-punt PW doorsturen.
- De PE's onderscheppen ook de TCN's, spoelen hun mac-adrestabellen, en sturen LDP MAC-terugtrekking naar externe PE's.

Dit is de configuratie op router1:

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

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

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

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

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

In deze configuratie, merk op dat:

- In MST instantie 0, is de root-brug 0000.000.0001, die overbruggingsidentificatie van router1 is.
- In MST instantie 1, is de root-brug 0000.000.0002, die overbruggings-ID van router2 is.
- De overbruggingsprioriteit van router1 is 4096 in instantie 0 (om de wortel te worden) en 8192 in instantie 1 (de op één na beste wortel te worden).
- De overbruggingsprioriteit van router1 is 8192 in instantie 0 (de op één na beste wortel worden) en 4096 in instantie 1 (de wortel worden).
- De point-to-point cross connect op Gigabit Ethernet0/1/0/3.1 brengt de niet-gelabelde MST TCN's naar de andere router.

Op de dot1q subinterfaces is een uitgaande ACL geconfigureerd om per VLAN BPDU's te laten vallen die door een andere site kunnen worden verzonden die nog niet naar MST is gemigreerd. Deze configuratie voorkomt dat de CE-switch verklaart dat de interface inconsistent is wanneer deze een BPDU per VLAN ontvangt op een interface die voor MST is geconfigureerd.

De configuratie op router2 is zeer gelijkaardig:

```
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

Dit is de basisconfiguratie van 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
```

Zodoende wordt verkeer in instantie 0 doorgestuurd via router1 en het verkeer in instantie 1 doorgestuurd via switch 2 en router2.

De configuratie op switch 2 gebruikt dezelfde opdrachten als switch 1:


```

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

```

Switch 2 gaat door switch 1 en router1 bijvoorbeeld0 en door router2 bijvoorbeeld1.

Het verkeer is belastbaar omdat één instantie de site via router1 verlaat en de andere instantie de site via router2 verlaat.

Als het verband tussen router1 en switch 1 neer is, gaan beide instanties door router2.

```

switch1#sh spanning-tree

MST0
Spanning tree enabled protocol mstp
Root ID Priority 4096

```

Address 0000.0000.0001
Cost 0
Port 2 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

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

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

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

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

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

switch2#sh spanning-tree

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

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

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

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

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

```
Interface Role Sts Cost Prio.Nbr Type
```

```
-----  
Gi0/1 Root FWD 20000 128.1 P2p
```

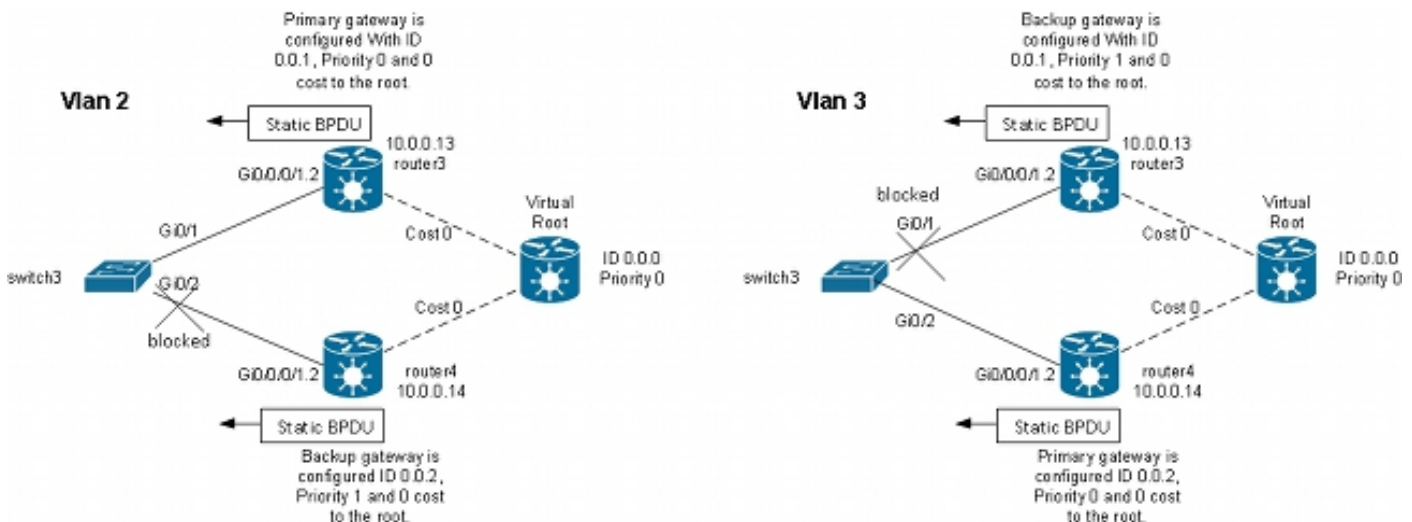
```
Gi0/2 Desg FWD 20000 128.2 P2p
```

Snelle convergentie kan worden bereikt in dit type van mislukking omdat het pad door de op één na beste wortel al was geselecteerd als alternatieve weg. Met MSTAG worden MST BPDU's niet via VPLS getransporteerd, zodat locaties worden geïsoleerd van de instabiliteit in andere locaties.

4.4.7.3 PVSTAG of PVRSTAG

MSTAG is het geprefereerde toegangsgateway protocol voor VPLS omdat het de snelle overspannende boom gebruikt en omdat het schaalbaar is met het gebruik van instanties in plaats van BPDU's op elk VLAN.

Als een site niet kan worden gemigreerd naar MST en de enige oplossing is om PVST+ of PVRST te blijven draaien, kunt u PVSTAG of PVRSTAG gebruiken, maar de implementatie is beperkt tot één specifieke topologie:



In deze topologie is de belangrijkste restrictie dat er slechts één CE-switch kan zijn. Je kunt niet twee switches hebben zoals in de [MSTAG topologie](#). In MSTAG, kunt u een punt-tot-punt PW vormen om het untagged verkeer (met inbegrip van de BPDU TCNs) van één PE aan andere te vervoeren wanneer de plaats in twee delen wordt verdeeld. Met PVST en PVRST worden de TCN's getagd zodat ze overeenkomen met dezelfde subinterface als het gegevensverkeer dat over VPLS moet worden getransporteerd. De router zou de BPDU's moeten identificeren op basis van het MAC-adres en het protocoltype om de TCN's naar de andere kant te kunnen doorsturen. Omdat dit momenteel niet wordt ondersteund, is slechts één CE-apparaat vereist.

Een andere vereiste in releases eerder dan Cisco IOS XR-software release 4.3.0 is dat bundelinterfaces niet als AC's kunnen worden gebruikt. Deze beperking is opgeheven in Cisco IOS XR-software release 4.3.0.

Het principe is ongeveer hetzelfde als bij MSTAG. De PVSTAG router stuurt statische BPDU's zodat de CE lijkt te zijn verbonden met switches die direct zijn verbonden met de (virtuele) root met kosten 0. Om het verkeer in evenwicht te brengen, kunnen sommige VLAN's worden geconfigureerd met de root op router3 en anderen met de root op router4.

Dit is een configuratievoorbeeld op router3:

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

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

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

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

Dit is een configuratievoorbeeld op router4:

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

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

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

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

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

Dit is een configuratievoorbeeld op CE switch 3:

```
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
```

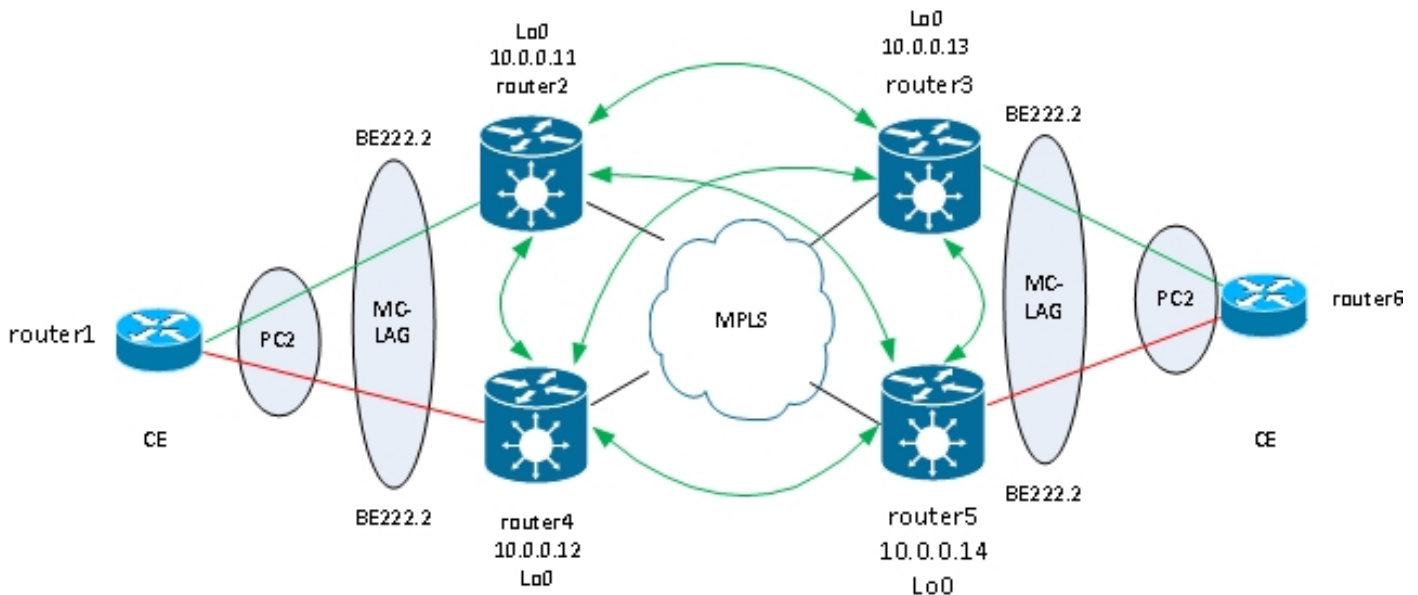
De configuratie voor PVSTAG is zeer vergelijkbaar met MSTAG behalve dat de wortel-prioriteit en de prioriteit van de primaire gateway worden gevormd als 4096 en de prioriteit van de reservegateway wordt gevormd als 8192 in het voorbeeld MSTAG.

Alle andere switches in de domeinen moeten een hogere prioriteit hebben dan die welke in PVSTAG of PVRSTAG zijn geconfigureerd.

U kunt de interfacekosten op de switches van CE afstemmen om te beïnvloeden welke haven de wortelhaven wordt en welke haven wordt geblokkeerd.

4.4.7.4 MC-LAG

De MC-LAG configuratie met VPLS is eenvoudiger dan point-to-point PW's met tweevoudige PW-redundantie. In plaats van één primaire PW en drie stand-by PW's, hebben de PE's alleen een volledige mesh van VPLS PW's nodig, die standaard is bij VPLS:



In deze topologie, merk op dat:

- MC-LAG loopt tussen de twee VPLS PE's aan de linkerkant: router2 en router4.
- Onder normale omstandigheden, zijn de bundelleden actief tussen router1 en router2 en in standby staat tussen router1 en router4.
- Router2 heeft de bundelsubinterfaces die onder VPLS brug-domeinen worden gevormd, zodat router2 het verkeer door:sturen aan verre VPLS PE's. Er zijn twee plaatsen geïllustreerd in het topologiediagram maar er zouden kunnen zijn veel meer.
- De externe PE's leren de MAC-adressen van router1 en apparaten erachter door router2, zodat het PE's voorwaartse verkeer voor deze bestemmingsMAC-adressen door router2.
- Wanneer het verband tussen router1 en router2 daalt of wanneer router2 daalt, wordt het bundellid tussen router1 en router4 actief.
- Net als router 2, heeft router4 zijn bundel subinterfaces geconfigureerd onder VPLS bridge-domeinen.
- Wanneer de bundelsubinterfaces op router4 komen, verstuurt router4 LDP MAC-terugtrekkingsberichten naar de externe VPLS-PE's om hen te laten weten dat er een topologiewijziging is.

Dit is de configuratie op router3:

```
RP/0/RSP1/CPU0:router3#sh run redundancy
redundancy
iccp
group 2
mlacp node 1
mlacp system mac 0200.0000.0002
mlacp system priority 1
mlacp connect timeout 0
member
neighbor 10.0.0.14
!
backbone
interface TenGigE0/0/0/0
interface TenGigE0/0/0/1
!
isolation recovery-delay 300
```



```

RP/0/RSP1/CPU0: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  
!  
!  
!  
!  
!
```

Onder normale omstandigheden, is het bundellid tussen router3 en router6 actief, en het lid tussen router5 en router6 is in standby staat:

```
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#

Verkeer van Ce wordt ontvangen op router3 en door:sturen aan verre PEs:

```
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
```

Het laatste bevel illustreert dat router3 sommige adressen van MAC op zijn bundel leert en de actieve leden op router3 zijn. Op router5, is er geen die adres van MAC over de bundel wordt geleerd aangezien het lokale lid in standby staat is:

```
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
```

Wanneer het bundellid tussen router3 en router6 daalt, wordt het bundellid actief op router5. De MC-LAG VPLS PEs verzenden een LDP MAC onthoudingsbericht zodat de verre PEs hun mac-

adrestabellen zuiveren en het MAC-adres leren door de nieuwe actieve MC-LAG PE router5.

Router2 ontvangt een MAC-terugtrekkingsberichten van router3 en router5 wanneer het actieve MC-LAG bundellid van router3 naar router5 beweegt:

```
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
```

De MAC-adressen op router2 gaan van router3 (10.0.0.13) naar router5 (10.0.0.14):

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

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

```
-----
6c9c.ed3e.e46d dynamic (10.0.0.15, 15) 0/0/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A
001d.4603.1f02 dynamic (10.0.0.14, 2) 0/0/CPU0 0d 0h 0m 0s N/A
001d.4603.1f42 dynamic (10.0.0.14, 2) 0/0/CPU0 0d 0h 0m 0s N/A
```

Met MC-LAG kan een site één bundel gebruiken om via VPLS aan de andere sites te worden gekoppeld. MC-LAG biedt de link en PE redundantie, maar logischerwijs is het nog steeds één bundelinterface om andere sites te bereiken. Spanning Tree is niet nodig op die bundel, en een BPDU-filter kan worden geconfigureerd op de CE om ervoor te zorgen dat BPDU's niet worden uitgewisseld tussen sites via VPLS.

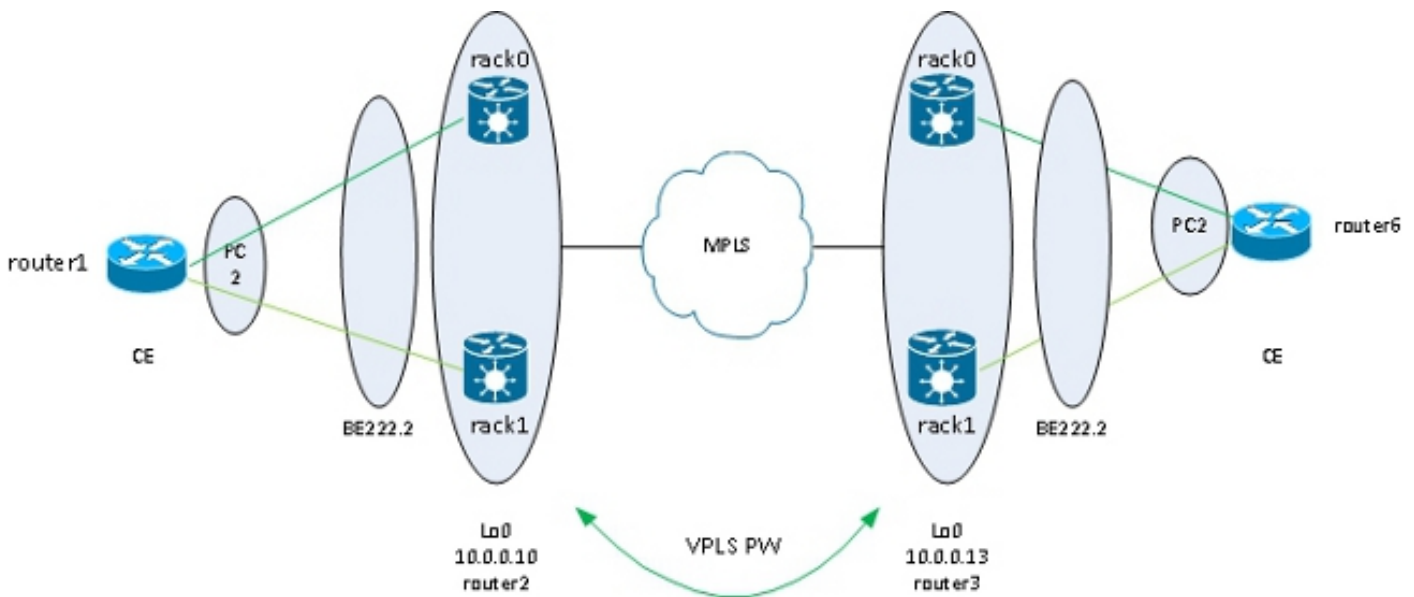
Een andere optie is de configuratie van een Ethernet-services access-list op de AC's in de bundel om de MAC-adressen van de BPDU's te laten vallen, zodat de BPDU's niet tussen sites worden getransporteerd. Als er echter een backdoor link tussen de sites wordt geïntroduceerd, kan het overspannen van de boom de lus niet doorbreken omdat deze niet op de MC-LAG bundel loopt.

Beoordeel dus zorgvuldig of overspannen-tree op de MC-LAG bundel moet worden uitgeschakeld. Als de topologie tussen plaatsen zorgvuldig wordt gehandhaafd, is het fijn om overtuiging door MC-LAG zonder de behoefte aan het overspannen te hebben - boom.

4.4.7.5 ASR 9000 nV Edge-cluster

De [MC-LAG oplossing](#) bood redundantie zonder de noodzaak om Spanning Tree te gebruiken. Eén nadeel is dat de bundelleden van een MC-LAG PE zich in stand-by bevinden, dus het is een active-stand-by oplossing die het linkgebruik niet maximaliseert.

Een andere ontwerpoptie is het gebruik van een ASR 9000 nV Edge-cluster, zodat CE's gebundelde leden kunnen hebben in elk clusterrack die allemaal tegelijk actief zijn:



Een ander voordeel van deze oplossing is dat het aantal PW's wordt verminderd omdat er slechts één PW per cluster voor elk van de clusters op elke plaats is. Wanneer er twee PE's per locatie zijn, moet elke PE een PW hebben voor elk van de twee PE's op elke locatie.

De eenvoud van de configuratie is een ander voordeel. De configuratie ziet eruit als een zeer eenvoudige VPLS-configuratie met een bridge-domein met gebundelde AC's en VFI PW's:

```
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
```

Redundantie wordt geleverd door de bundel AC dual homed naar de twee racks zodat de bundel blijft omhoog in het geval van een storing in het bundellid of een rackstoring.

Wanneer een site slechts via een cluster aan het VPLS-domein is gekoppeld, is de topologie vergelijkbaar met MC-LAG met betrekking tot het overspannen van de boom. Zo wordt het overspannen - boom niet vereist op die bundel, en een filter BPDU op Ce zou kunnen worden gevormd om ervoor te zorgen dat BPDUs niet tussen plaatsen over VPLS worden geruild.

Een andere optie is de configuratie van een Ethernet-services access-list op de AC's in de bundel om de MAC-adressen van de BPDU's te laten vallen, zodat de BPDU's niet tussen sites worden getransporteerd. Als er echter een backdoor link tussen de sites wordt geïntroduceerd, kan het overspannen - boom de lus niet doorbreken omdat het niet op de CE-PE bundel loopt. Zo, evalueer zorgvuldig of om het overspannen uit te schakelen - boom op die bundel CE-PE. Als de topologie tussen sites zorgvuldig wordt onderhouden, is het leuk om redundantie door het cluster te hebben zonder de noodzaak van het overspannen van boom.

4.4.7.6 Op ICCP gebaseerde services voor meervoudig calibreren (ICCP-SM) (PMCLAG (Pseudo MCLAG) en actief/actief)

Er is een nieuwe functie geïntroduceerd in versie 4.3.1 om de beperking van MC-LAG te overwinnen, waarbij sommige bundelkoppelingen ongebruikt blijven omdat ze in stand-by modus blijven staan. In de nieuwe functie, genaamd *Pseudo MCLAG*, zijn alle links van de DHD naar de Punten van Attachments (PoAs) in gebruik, maar de VLAN's zijn verdeeld tussen de verschillende bundels:

ICCP-SM (Pseudo MCLAG)

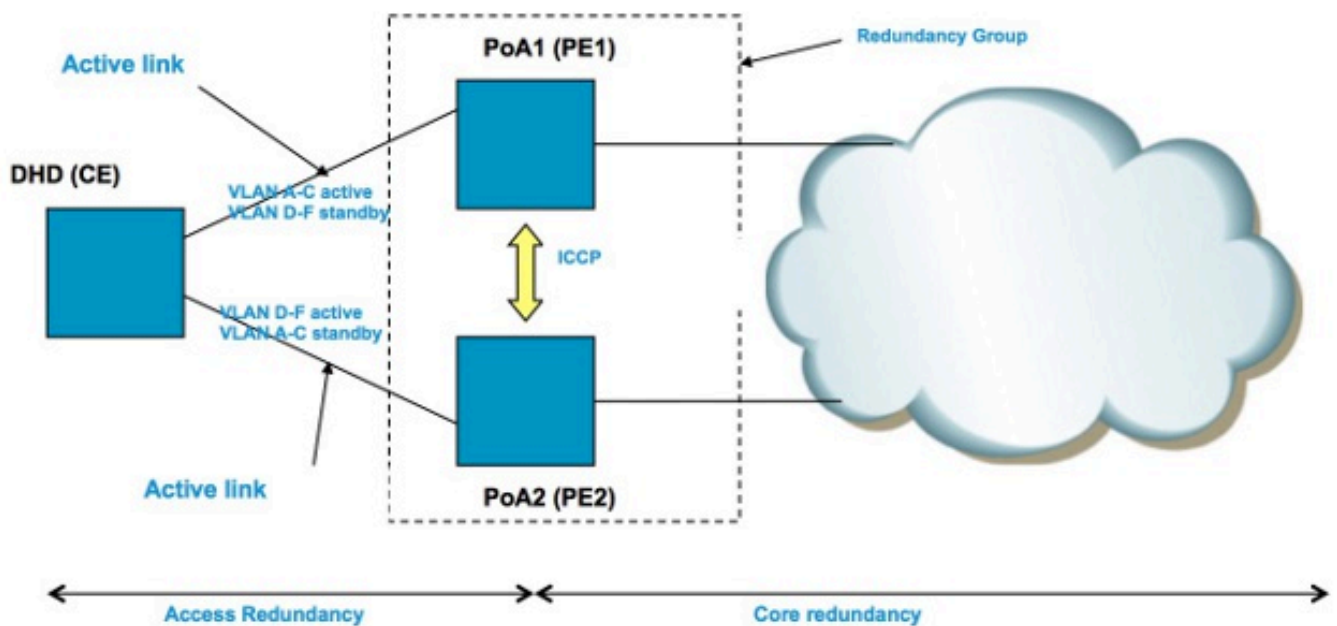


Figure 2 Pseudo MCLAG

DHD has two separate bundles – one to PoA1 and the other to PoA2.
Both bundles are active for some vlans and standby for others.
Active vlans on one bundle = standby vlans for other bundle.
PoAs communicate over ICCP.
Only VPLS is supported in core (first release.)

4.5 Stormcontrole in het verkeer

In een L2 uitzendingsdomein, is er het risico dat een gastheer zich misdraagt en een hoog tarief van uitzending of multicast kaders verzenden die overal in het bridge-domein moeten worden overstroomd. Een ander risico is het creëren van een L2-lus (die niet wordt gebroken door het overspannen van een boom), wat resulteert in uitzendingen en multicast-pakketten van een lus voorzien. Een hoog tarief van uitzendingen en multicast pakketten beïnvloedt de prestaties van de gastheren in de uitzendingsdomeinen.

De prestaties van switchingapparaten in het netwerk kunnen ook worden beïnvloed door de replicatie van één invoerframe (broadcast, multicast of een onbekend unicastframe) naar meerdere uitgaande poorten in het bridge-domein. Het maken van meerdere kopieën van hetzelfde pakket kan arbeidsintensief zijn, afhankelijk van de plaats binnen het apparaat waar het pakket moet worden gerepliceerd. Het repliceren van een uitzending naar meerdere verschillende sleuven is bijvoorbeeld geen probleem vanwege de multicast replicatiemogelijkheden van de stof. De prestaties van een netwerkprocessor kunnen worden beïnvloed wanneer deze meerdere kopieën van hetzelfde pakket moet maken die worden verzonden op enkele poorten die de netwerkprocessor verwerkt.

Om apparaten in het geval van een storm te beschermen, laat de eigenschap van de verkeersonweer u een maximumtarief van uitzendingen, multicast en onbekende unicasts vormen die op een brug-domein AC moeten worden goedgekeurd. Zie [Cisco ASR 9000 Series aggregatieservices routerconfiguratiehandleiding voor systeem security, release 4.3.x: implementatie van verkeersstormcontrole onder een VPLS-brug](#) voor meer informatie.

Traffic storm control wordt niet ondersteund op een bundel AC-interfaces of VFI PW's, maar wordt ondersteund op niet-bundel AC's en toegang PW's. De functie is standaard uitgeschakeld; tenzij u stormcontrole instelt, accepteert u elk tarief van uitzendingen, multicast en onbekende unicasts.

Hier is een voorbeeldconfiguratie:

```
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>
```

De stormcontrole drop-tellers zijn altijd aanwezig in de output van de **show l2vpn bridge-domain detail** opdracht. Omdat de functie standaard is uitgeschakeld, beginnen de tellers alleen te melden wanneer de functie is geconfigureerd.

De ingestelde snelheden kunnen variëren afhankelijk van het verkeerspatroon van het ene netwerk naar het andere. Alvorens een snelheid te configureren raadt Cisco u aan de uitzendsnelheid, multicast of onbekende unicastframes onder normale omstandigheden te begrijpen. Voeg vervolgens een marge toe in de ingestelde snelheid boven de normale snelheid.

4.6 MAC-bewegingen

In het geval van netwerkinstabiliteit zoals een interfaceklap, zou een adres van MAC van een nieuwe interface kunnen worden geleerd. Dit is normale netwerkconvergentie en de mac-adrestabel wordt dynamisch bijgewerkt.

Echter, constante MAC-bewegingen wijzen vaak op netwerkinstabiliteit, zoals ernstige instabiliteit tijdens een L2-lus. Met de functie MAC-adresbeveiliging kunt u MAC-bewegingen melden en corrigerende maatregelen nemen, zoals het afsluiten van een aanstootgevende poort.

Zelfs als een corrigerende actie niet is geconfigureerd, kunt u de **logboekopdracht** configureren zodat u wordt gewaarschuwd voor netwerkinstabiliteit via de MAC-bewegingsberichten:

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

In dit voorbeeld is de actie ingesteld op geen, dus er wordt niets gedaan als er een MAC-verplaatsing wordt gedetecteerd, behalve dat er een syslog-bericht wordt vastgelegd. Dit is een voorbeeldbericht:

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

4.7 IGMP- en MLD-controle

Standaard worden multicast frames overstromd naar alle poorten in een bridge-domein. Wanneer u high speed streams zoals IP-televisie (IPTV) services gebruikt, is er mogelijk een aanzienlijke hoeveelheid verkeer doorgestuurd naar alle poorten en gerepliceerd over meerdere PW's. Als alle tv-stromen via één interface worden doorgestuurd, kunnen poorten hierdoor sterk worden vervormd. De enige optie is configuratie van een functie zoals IGMP of MLD snooping, die multicast controlepakketten onderschept om de ontvangers en multicast routers en voorwaartse stromen op de poorten alleen wanneer van toepassing te volgen.

Raadpleeg de [configuratiehandleiding voor de Cisco ASR 9000 Series aggregatieservices router voor multicast, release 4.3.x](#) voor meer informatie over deze functies.

5. Aanvullende L2VPN-onderwerpen

Opmerkingen:

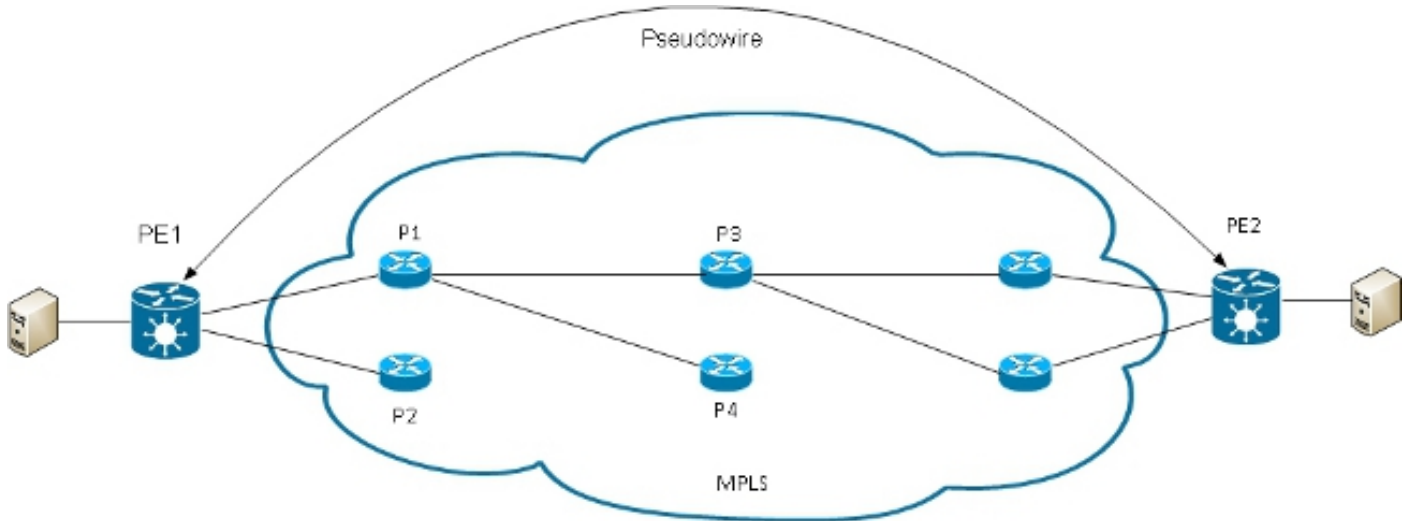
Gebruik de [Command Lookup Tool \(alleen voor geregistreeerde gebruikers\) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.](#)

De [Output Interpreter Tool \(alleen voor geregistreeerde klanten\) ondersteunt bepaalde opdrachten met show](#). Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show**.

5.1 Taakverdeling

Wanneer een L2VPN PE een frame over een MPLS PW moet verzenden, is het Ethernet frame ingekapseld in een MPLS frame met een of meer MPLS labels; er is ten minste één PW label en misschien een IGP label om de externe PE te bereiken.

Het MPLS-frame wordt door het MPLS-netwerk naar de externe L2VPN-PE getransporteerd. Er zijn doorgaans meerdere paden om de bestemmings-PE te bereiken:



Opmerking: niet alle koppelingen worden in dit diagram weergegeven.

PE1 kan kiezen tussen P1 en P2 als de eerste MPLS P router naar PE2. Als P1 is geselecteerd, kiest PE1 dan tussen P3 en P4, enzovoort. De beschikbare paden zijn gebaseerd op IGP-topologie en het MPLS TE-tunnelpad.

MPLS-serviceproviders geven er de voorkeur aan dat alle links even gebruikt worden in plaats van één stremmende link met andere onderbenutte links. Dit doel is niet altijd gemakkelijk te bereiken omdat sommige PW's veel meer verkeer dan anderen dragen en omdat het pad genomen door een PW verkeer afhankelijk is van het hashing algoritme gebruikt in de kern. Meervoudige hoge bandbreedte PWs kunnen worden gehakt op dezelfde koppelingen, wat congestie creëert.

Een zeer belangrijke vereiste is dat alle pakketten van één stroom de zelfde weg zouden moeten volgen. Anders leidt dit tot out-of-order frames, die van invloed kunnen zijn op de kwaliteit of de prestaties van de toepassingen.

Loadbalancing in een MPLS-netwerk op Cisco-routers is doorgaans gebaseerd op de gegevens die op het MPLS-label onder worden vermeld.

- Als de gegevens onmiddellijk nadat het bodemetiket met 0x4 of 0x6 begint, veronderstelt een router MPLS P dat er een IPv4 of IPv6 pakket binnen het pakket MPLS is en probeert om evenwicht te laden gebaseerd op een hash van de bron en bestemming IPv4 of IPv6 adressen die uit het kader worden gehaald. In theorie zou dit niet van toepassing moeten zijn op een Ethernet-frame dat is ingekapseld en getransporteerd over een PW, omdat het doelMAC-adres het onderste label volgt. Maar onlangs zijn sommige MAC-adresbereiken die beginnen met 0x4 en 0x6 toegewezen. De MPLS-IP-router kan er ten onrechte van uitgaan dat de Ethernet-header in feite een IPv4-header is en het frame wordt gehakt op basis van de veronderstelde IPv4-bron- en doeladressen. Ethernet-frames van een PW kunnen over verschillende paden in de MPLS-kern worden gehakt, wat leidt tot niet-sequentiële frames in de PW en problemen met de toepassingskwaliteit. De oplossing is de configuratie van een controlewoord onder een pw-klasse dat kan worden gekoppeld aan een point-to-point of VPLS PW. Het controlewoord wordt ingevoegd onmiddellijk na de MPLS-labels. Het

controlewoord begint niet met 0x4 of 0x6 zodat wordt het probleem vermeden.

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

- Als de gegevens onmiddellijk na de onderkant van de MPLS-labelstack niet beginnen met 0x4 of 0x6, de P-routerlastbalansen op basis van het onderste label. Al het verkeer vanaf één PW volgt hetzelfde pad, dus out-of-order pakketten komen niet voor, maar dit kan leiden tot stremming op sommige koppelingen in het geval van hoge bandbreedte PW's. Met Cisco IOS XR-software release 4.2.1 ondersteunt de ASR 9000 de Flow Aware Transport (FAT) PW-functie. Deze optie werkt op de L2VPN PE's, waar het wordt onderhandeld tussen de twee uiteinden van een point-to-point of VPLS PW. De ingang L2VPN PE detecteert stromen op de AC en de L2VPN configuratie en voegt een nieuw MPLS-stroomlabel in onder het PW MPLS-label onder de MPLS-labelstack. De toegang PE detecteert stromen op basis van de bron- en doelMAC-adressen (standaard) of de bron- en doelIPv4-adressen (configureerbaar). Het gebruik van de MAC-adressen is de standaardinstelling; het gebruik van IPv4-adressen wordt

aanbevolen, maar moet handmatig worden ingesteld.

Met de FAT PW-functie voegt de ingang L2VPN PE één onderste MPLS-etiket per src-dst-mac of per src-dst-ip in. De MPLS P-routers (tussen de PE's) hashframes over de beschikbare paden, bereiken vervolgens de bestemmings-PE op basis van dat FAT PW-stroomlabel onder in de MPLS-stack. Dit biedt over het algemeen een veel beter bandbreedtegebruik in de kern tenzij een PW slechts een klein aantal src-dst-mac of src-dst-ip gesprekken draagt. Cisco raadt u aan een controlewoord te gebruiken, zodat u kunt voorkomen dat u MAC-adressen hebt die direct na het stroomlabel beginnen met 0x4 en 0x6. Dit zorgt ervoor dat de hash correct is gebaseerd op de pseudo IP-adressen en niet op het flow label.

Met deze functie wordt het verkeer van één PW over meerdere paden in de kern, indien beschikbaar, gebalanceerd. Het verkeer van de toepassing lijdt niet aan uit-van-ordepakketten omdat al verkeer van de zelfde bron (MAC of IP) aan de zelfde bestemming (MAC of IP) de zelfde weg volgt.

Hierna volgt een configuratievoorbeeld:

```
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 Vastlegging

Er kunnen verschillende typen logberichten worden geconfigureerd in de L2VPN-configuratiemodus. Configureer l2vpn-logboekregistratie om syslog-waarschuwingen voor L2VPN-gebeurtenissen te ontvangen en stel logboekpseudowire in om te bepalen wanneer een PW-status wijzigt:

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

Als vele PWs worden gevormd, zouden de berichten het logboek kunnen overstromen.

5.3 Ethernet-services toegangslijst

U kunt een Ethernet-services access-lijst gebruiken om verkeer van specifieke hosts te laten vallen of om te verifiëren of een router pakketten van een host op een L2transport interface krijgt:

```
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)
```

De hardware overeenkomsten kunnen slechts met het *hardware* sleutelwoord worden gezien. Gebruik het *inloop*- of *uitgangssleutelwoord* afhankelijk van de richting van de toegangsgroep. De lijnkaartlocatie van de interface waarop de toegangslijst wordt toegepast, wordt ook gespecificeerd.

U kunt ook een IPV4-toegangslijst op een l2transport-interface toepassen als een beveiliging of

probleemoplossing:

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

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

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

5.4 Ethernet uitgaande filter

In de uitgangsrichting van een AC, veronderstel dat er geen **herschrijf ingangstag pop <> symmetrische** opdracht is die de uitgaande VLAN-tags bepaalt. In dat geval is er geen controle om er zeker van te zijn dat het uitgaande frame de juiste VLAN-tags heeft volgens de opdracht **inkapseling**.

Hierna volgt een configuratievoorbeeld:

```
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
!
!
!
!
```

In deze configuratie, merk op dat:

- Een uitzending ontvangen met een dot1q-tag 2 op Gigabit Ethernet0/1/0/39.2 behoudt zijn inkomende tag omdat er geen **herschrijf**-indringingsopdracht is.
- Die uitzending wordt overstromd uit Gigabit Ethernet0/1/0/3.2 met zijn dot1q tag 2, maar dat

veroorzaakt geen probleem omdat Gigabit Ethernet0/1/0/3.2 ook geconfigureerd is met de dot1q tag 2.

- Die uitzending wordt ook overstroomd uit Gigabit Ethernet0/1/0/3.3, die zijn originele markering 2 houdt omdat er geen **herschrijfbevel** op Gigabit Ethernet0/1/0/3.3 is. De opdracht **inkapseling dot1q 3** op Gigabit Ethernet0/1/0/3.3 is niet ingeschakeld in de uitgangsrichting.
- Het resultaat is dat er voor een uitzending ontvangen met tag 2 op Gigabit Ethernet0/1/0/39, twee uitzendingen zijn met tag 2 die uit Gigabit Ethernet0/1/0/3 gaan. Dat gedupliceerde verkeer kan problemen met de toepassing veroorzaken.
- De oplossing is *strikte* configuratie van *ethernetfilter* om ervoor te zorgen dat pakketten de subinterface verlaten met de juiste VLAN-tags. Anders worden de pakketten niet doorgestuurd en gedropt.

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.