IOS XR L2VPN-Services und -Funktionen

Inhalt

Einleitung

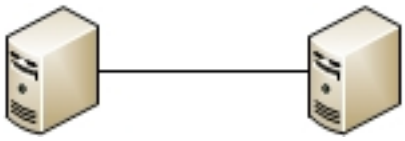
In diesem Dokument werden grundlegende Layer-2 (L2)-VPN-Topologien (L2VPN) beschrieben. Es ist nützlich, grundlegende Beispiele zu präsentieren, um Design, Services, Funktionen und Konfiguration zu demonstrieren. Weitere Informationen finden Sie im Konfigurationshandbuch für Aggregation Services Router der Cisco Serie ASR 9000, L2VPN und Ethernet Services, Version 4.3.x.

1. Point-to-Point- und Multipoint-Services

Die L2VPN-Funktion ermöglicht die Bereitstellung von Point-to-Point- und Multipoint-Services.

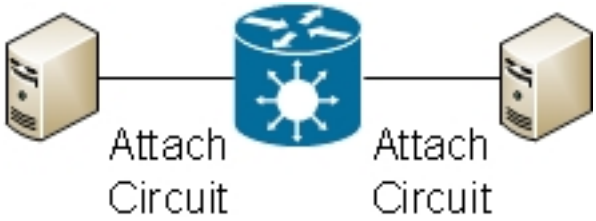
1.1 Punkt-zu-Punkt-Service

Der Punkt-zu-Punkt-Dienst emuliert im Wesentlichen eine Transportschaltung zwischen zwei Endknoten, sodass die Endknoten über eine Punkt-zu-Punkt-Verbindung direkt verbunden zu sein scheinen. Dies kann verwendet werden, um zwei Standorte zu verbinden.

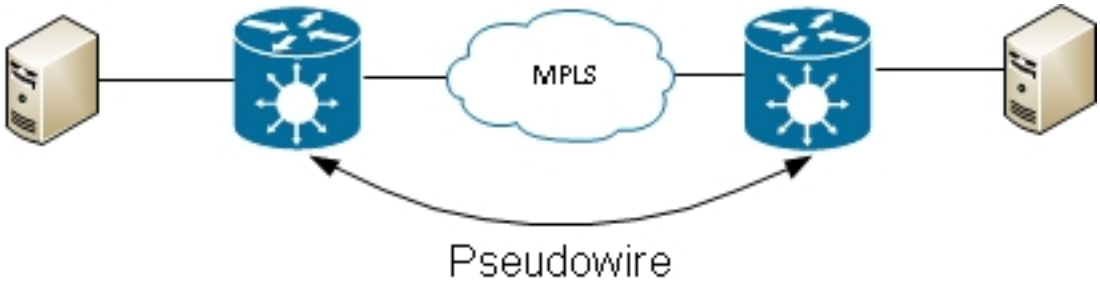


In der Praxis können mehrere Router zwischen den beiden Endknoten vorhanden sein, und es kann mehrere Designs geben, um den Point-to-Point-Service bereitzustellen.

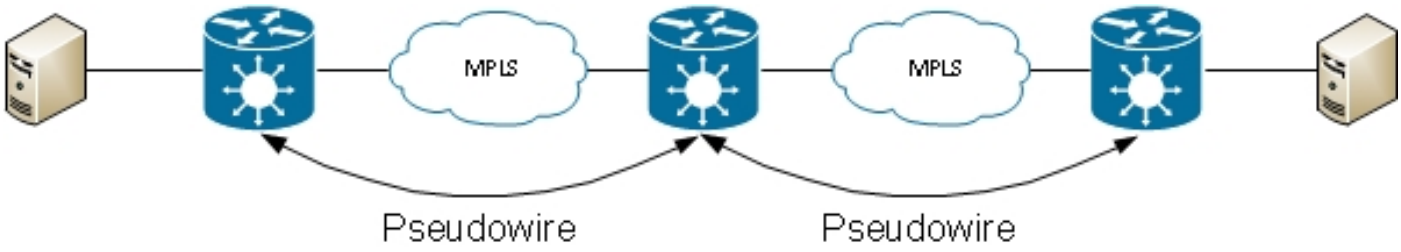
Ein Router kann zwischen zwei seiner Schnittstellen lokal wechseln:



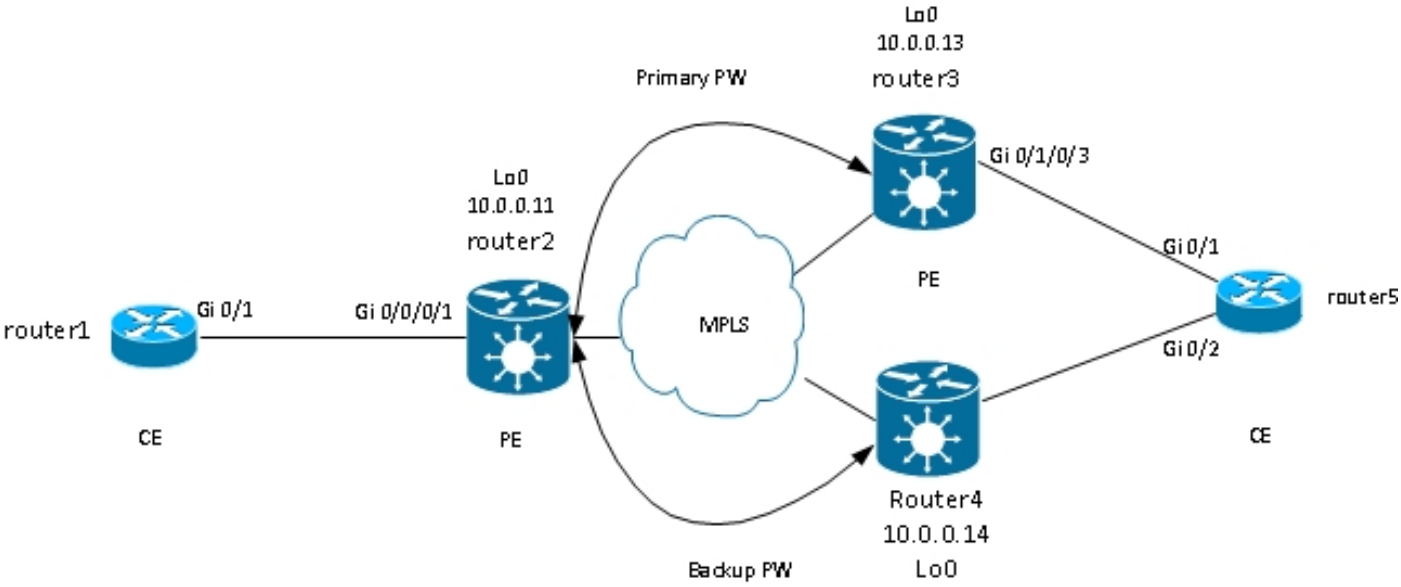
Es kann auch eine MPLS-Pseudowire-Verbindung (Multiprotocol Label Switching) zwischen zwei Routern geben:



Ein Router kann Frames zwischen zwei PWs schalten. In diesem Fall handelt es sich um einen PW mit mehreren Segmenten:



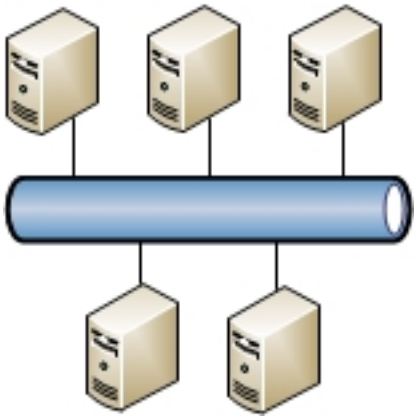
Die Redundanz ist über die PW-Redundanzfunktion verfügbar:



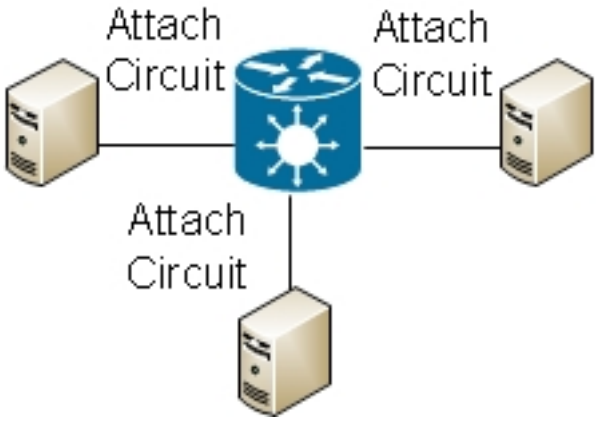
Andere Designs sind verfügbar, können aber nicht alle hier aufgelistet werden.

1.2 Multipoint-Dienst

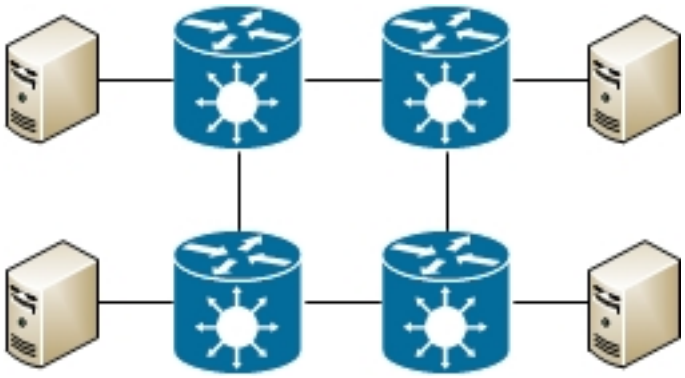
Der Multipoint-Dienst emuliert eine Broadcast-Domäne, sodass alle in dieser Bridge-Domäne verbundenen Hosts logisch mit demselben Ethernet-Segment verbunden zu sein scheinen:



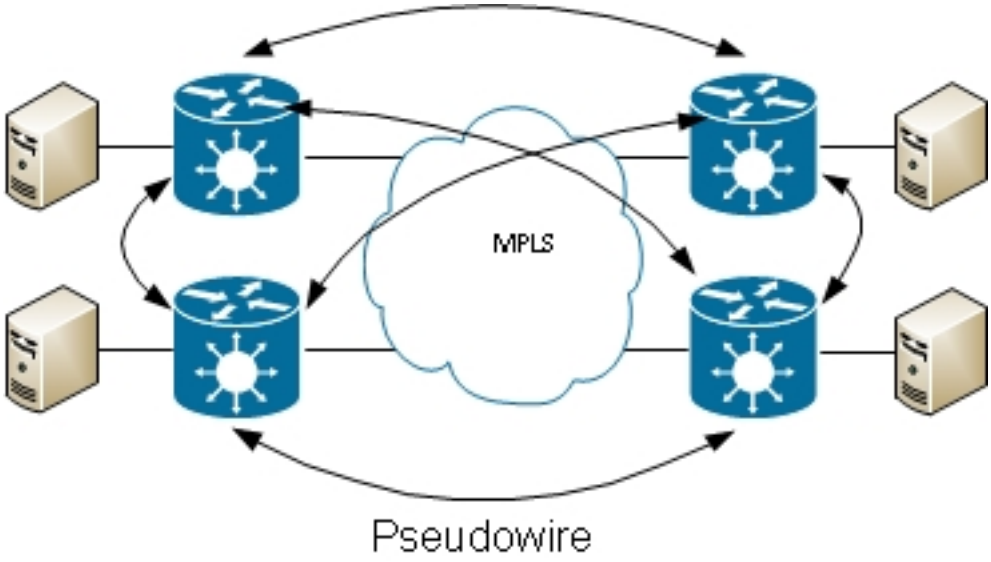
Alle Hosts können mit demselben Router/Switch verbunden werden:



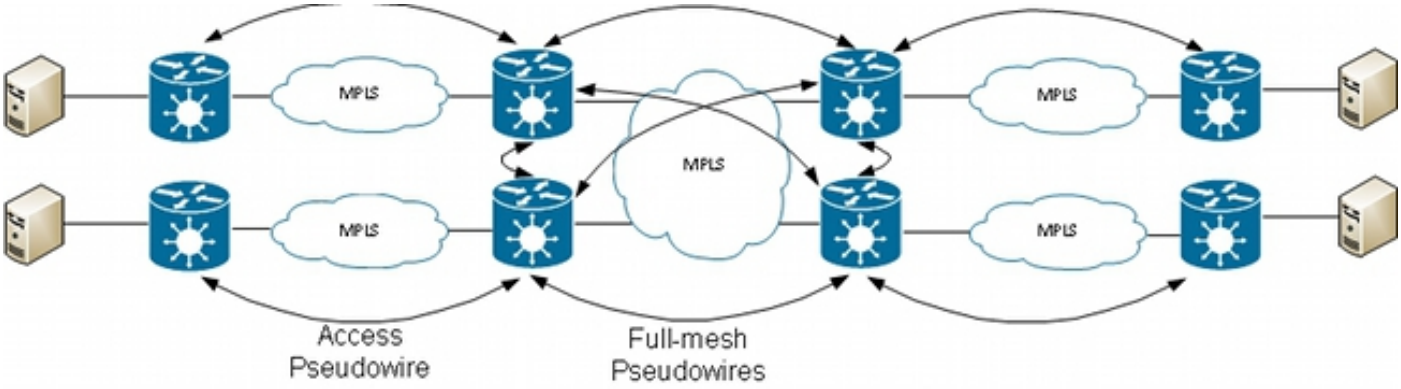
Mehrere Switches können herkömmliches Ethernet-Switching ausführen; Spanning Tree muss verwendet werden, um Schleifen zu unterbrechen:



Mit Virtual Private LAN Services (VPLS) können Sie die Broadcast-Domäne mithilfe von MPLS-PWs zwischen mehreren Standorten erweitern:



Ein hierarchisches VPLS kann verwendet werden, um die Skalierbarkeit zu erhöhen:



2. Anschlussschaltungen

2.1 ASR 9000 Ethernet Virtual Circuit

2.1.1 Eingehende Schnittstellenzuordnung

Grundregeln für Anschlusskreise (ACs) sind:

- Ein Paket muss auf einer Schnittstelle empfangen werden, die mit dem *l2transport*-Schlüsselwort konfiguriert ist, damit es von der L2VPN-Funktion verarbeitet werden kann.
- Bei dieser Schnittstelle kann es sich um eine Hauptschnittstelle handeln, bei der der Befehl **l2transport** im Schnittstellenkonfigurationsmodus konfiguriert wird, oder um eine Subschnittstelle, bei der das Schlüsselwort *l2transport* nach der Subschnittstellennummer konfiguriert wird.
- Eine Suche nach der längsten Übereinstimmung bestimmt die eingehende Schnittstelle des Pakets. Die Suche nach der längsten Übereinstimmung überprüft diese Bedingungen in dieser Reihenfolge, um das eingehende Paket mit einer Subschnittstelle abzugleichen:

    1. Der eingehende Frame hat zwei dot1q-Tags und entspricht einer Subschnittstelle, die mit

denselben zwei dot1q-Tags konfiguriert ist (802.1Q Tunneling oder QinQ). Dies ist die längstmögliche Übereinstimmung.
2. Der eingehende Frame hat zwei dot1q-Tags und stimmt mit einer Subschnittstelle überein, die mit demselben dot1q-ersten Tag und *einem beliebigen* Tag für das zweite Tag konfiguriert wurde.
3. Der eingehende Frame hat ein dot1q-Tag und stimmt mit einer Subschnittstelle überein, die mit demselben dot1q-Tag und dem *genauen* Schlüsselwort konfiguriert wurde.
4. Der eingehende Frame hat ein oder mehrere dot1q-Tags und stimmt mit einer Subschnittstelle überein, die mit einem der dot1q-Tags konfiguriert wurde.
5. Der eingehende Frame hat keine dot1q-Tags und stimmt mit einer Subschnittstelle überein, die mit dem Befehl **encapsulation untagged** konfiguriert wurde.
6. Der eingehende Frame stimmt nicht mit einer anderen Subschnittstelle überein, sodass er mit einer Subschnittstelle übereinstimmt, die mit dem **Standard-**Kapselungsbefehl konfiguriert wurde.
7. Der eingehende Frame stimmt mit keiner anderen Subschnittstelle überein und entspricht daher der Hauptschnittstelle, die für *l2transport* konfiguriert ist.

- Auf herkömmlichen Routern, die nicht das Ethernet Virtual Connection (EVC)-Modell verwenden, werden die unter der Subschnittstelle konfigurierten VLAN-Tags aus dem Frame entfernt (per Popup), bevor sie von der L2VPN-Funktion transportiert werden.
- Auf einem Cisco Aggregation Services Router der Serie ASR 9000, der die EVC-Infrastruktur verwendet, werden die vorhandenen Tags standardmäßig beibehalten. Verwenden Sie den Befehl **rewrite**, um die Standardeinstellung zu ändern.
- Wenn in der Bridge-Domäne eine Bridge Virtual Interface (BVI) vorhanden ist, sollten alle eingehenden Tags geöffnet werden, da es sich bei der BVI um eine geroutete Schnittstelle ohne Tag handelt. Weitere Informationen finden Sie im Abschnitt BVI.

Hier einige Beispiele, die diese Regeln veranschaulichen:

1. Ein einfaches Beispiel ist, wenn der gesamte Datenverkehr, der auf einem physischen Port eingeht, transportiert werden muss, unabhängig davon, ob er über einen VLAN-Tag verfügt oder nicht. Wenn Sie **l2transport** unter der Hauptschnittstelle konfigurieren, wird der gesamte an diesem physischen Port empfangene Datenverkehr durch die L2VPN-Funktion transportiert:

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

   Wenn es Subschnittstellen dieser Hauptschnittstelle gibt, fängt die Hauptschnittstelle jeden Frame ab, der keiner Subschnittstelle entspricht. Dies ist die Regel für die längste Übereinstimmung.

2. Paketschnittstellen und Subschnittstellen können als l2transport konfiguriert werden:

```
interface Bundle-Ether1
l2transport
```

3. Verwenden Sie **den Kapselungsstandard** unter einer l2transport-Subschnittstelle, um jeden markierten oder nicht markierten Datenverkehr abzugleichen, der nicht von einer anderen Subschnittstelle mit der längsten Übereinstimmung abgeglichen wurde. (siehe Beispiel 4). Das Schlüsselwort *l2transport* wird im Namen der Subschnittstelle konfiguriert, nicht unter

der Subschnittstelle wie auf der Hauptschnittstelle:

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

Konfigurieren Sie **die Kapselung unmarkiert**, wenn Sie nur Frames ohne Tagging zuordnen möchten.

4. Wenn mehrere Subschnittstellen vorhanden sind, führen Sie den Test der längsten Übereinstimmung für den eingehenden Frame aus, um die eingehende Schnittstelle zu ermitteln:

```
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
```

Beachten Sie bei dieser Konfiguration Folgendes:

- Ein QinQ-Frame mit einem äußeren VLAN-Tag 2 und einem inneren VLAN-Tag 3 könnte mit den Subschnittstellen .1, .2 oder .3 übereinstimmen, wird jedoch aufgrund der Regel für die längste Übereinstimmung der Subschnittstelle .3 zugewiesen. Zwei Tags auf .3 sind länger als ein Tag auf .2 und länger als keine Tags auf .1.
- Ein QinQ-Frame mit einem äußeren VLAN-Tag 2 und einem inneren VLAN-Tag 4 ist der .2-Subschnittstelle zugeordnet, da **encapsulation dot1q 2** dot1q-Frames nur mit dem VLAN-Tag 2, aber auch QinQ-Frames mit einem äußeren Tag 2 abgleichen kann. Wenn Sie die QinQ-Frames nicht abgleichen wollen, beachten Sie Beispiel 5 (*exaktes* Schlüsselwort).
- Ein QinQ-Frame mit dem äußeren VLAN-Tag 3 entspricht der .1-Subschnittstelle.
- Ein dot1q-Frame mit dem VLAN-Tag 2 entspricht der .2-Subschnittstelle.
- Ein dot1q-Frame mit dem VLAN-Tag 3 entspricht der .1-Subschnittstelle.

5. Um einen dot1q-Frame und keinen QinQ-Frame zu finden, verwenden Sie das *genaue* Schlüsselwort:

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

Diese Konfiguration stimmt nicht mit QinQ-Frames mit einem äußeren VLAN-Tag 2 überein, da sie nur Frames mit genau einem VLAN-Tag entspricht.

6. Verwenden Sie das Schlüsselwort *untagged,* um nur untagged Frames wie CDP-Pakete (Cisco Discovery Protocol) oder MST-BPDUs (Multiple Spanning Tree) zuzuordnen:

```
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
```

Beachten Sie bei dieser Konfiguration Folgendes:

- Dot1q-Frames mit einem VLAN-Tag 3 oder QinQ-Frames mit einem äußeren Tag 3 entsprechen den .3-Subschnittstellen.
- Alle anderen dot1q- oder QinQ-Frames entsprechen der .1-Subschnittstelle.
- Frames ohne VLAN-Tag entsprechen der .2-Subschnittstelle.

7. Das Schlüsselwort *any* kann als Platzhalter verwendet werden:

```
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
```

Beide Subschnittstellen .4 und .5 könnten QinQ-Frames mit den Tags 4 und 5 entsprechen, aber die Frames werden den .5-Subschnittstellen zugewiesen, da sie spezifischer sind. Dies ist die Regel für die längste Übereinstimmung.

8. VLAN-Tags können in verschiedenen Bereichen verwendet werden:

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

9. Für das erste oder zweite dot1q-Tag können mehrere VLAN-Tag-Werte oder -Bereiche aufgelistet werden:

```
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
```

Sie können maximal neun Werte auflisten. Wenn mehr Werte erforderlich sind, müssen diese einer anderen Subschnittstelle zugewiesen werden. Gruppieren Sie Werte in einem Bereich, um die Liste zu verkürzen.

10. Der Befehl **encapsulation dot1q second-dot1q** verwendet den Ethertype 0x8100 für die äußeren und inneren Tags, da dies die Cisco Methode zum Kapseln von QinQ-Frames ist. Gemäß IEEE sollte der Ethertype 0x8100 jedoch für 802.1q-Frames mit einem VLAN-Tag reserviert werden, und ein äußeres Tag mit Ethertype 0x88a8 sollte für QinQ-Frames verwendet werden. Das äußere Tag mit Ethertype 0x88a8 kann mit dem *dot1ad*-Schlüsselwort konfiguriert werden:

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

11. Um den alten Ethertype 0x9100 oder 0x9200 für die QinQ-äußeren Tags zu verwenden,

verwenden Sie den Befehl **dot1q tunneling ethertype** unter der Hauptschnittstelle der QinQ-Subschnittstelle:

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

Das äußere Tag hat den Ethertyp 0x9100 oder 0x9200, und das innere Tag hat den dot1q Ethertyp 0x8100.

12. Ein eingehender Frame kann basierend auf der Quell-MAC-Adresse einer Subschnittstelle zugewiesen werden:

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

2.1.2 VLAN-Manipulation

Das Standardverhalten einer EVC-basierten Plattform besteht darin, die VLAN-Tags auf dem eingehenden Frame beizubehalten.

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

In dieser Konfiguration behält ein eingehender dot1q-Frame mit dem VLAN-Tag 3 sein VLAN-Tag 3 bei, wenn der Frame weitergeleitet wird. Ein eingehender QinQ-Frame mit einem äußeren VLAN-Tag 3 und einem inneren Tag 100 behält beide Tags bei der Weiterleitung des Frames unverändert bei.

Mit der EVC-Infrastruktur können Sie die Tags jedoch mit dem Befehl **rewrite** bearbeiten, sodass Sie Tags in den eingehenden VLAN-Tag-Stack einfügen (entfernen), übersetzen oder verschieben (hinzufügen) können.

Hier einige Beispiele:

- Mit dem *pop*-Schlüsselwort können Sie ein QinQ-Tag aus einem eingehenden dot1q-Frame entfernen. In diesem Beispiel wird das äußere Tag 13 des eingehenden QinQ-Frames entfernt und der Frame mit dem dot1q-Tag 100 weitergeleitet:

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

Das Verhalten ist immer symmetrisch, d.h. der äußere Anhänger 13 wird in Einlaufrichtung gestopft und in Auslaufrichtung geschoben.

- Mit dem *translate*-Schlüsselwort können Sie ein oder zwei eingehende Tags durch ein oder zwei neue Tags ersetzen:

```
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
```

Das *symmetrische* Schlüsselwort wird automatisch hinzugefügt, da es der einzige unterstützte Modus ist.

- Mit dem *push*-Schlüsselwort können Sie einem eingehenden dot1q-Frame ein QinQ-Tag hinzufügen:

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

Dem eingehenden Frame wird ein äußeres QinQ-Tag 100 mit einem dot1q-Tag 4 hinzugefügt. In Egress-Richtung wird das QinQ-Tag eingeblendet.

2.2 Cisco IOS XR Nicht-EVC-Router-Verhalten (CRS und XR12000)

Die Syntax für den VLAN-Abgleich auf Nicht-EVC-Plattformen verwendet nicht das *Kapselungs*-Schlüsselwort:

```
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
```

Die Bearbeitung von VLAN-Tags kann nicht konfiguriert werden, da das einzig mögliche Verhalten darin besteht, alle Tags anzuzeigen, die in den Befehlen **dot1q** oder **dot1ad** angegeben sind. Dies geschieht standardmäßig, sodass es keinen **rewrite**-Befehl gibt.

3. Point-to-Point-Service

Hinweise:

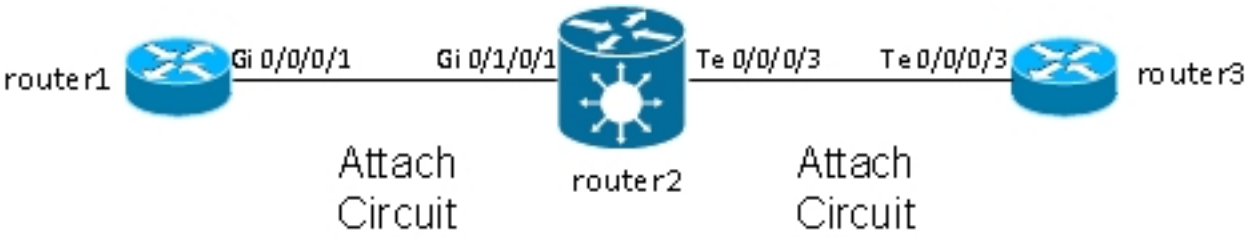
Verwenden Sie das Command Lookup-Tool (Tool für die Suche nach Befehlen) (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Das Output Interpreter-Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter-Tool, um eine Analyse der **show**-Befehlsausgabe anzuzeigen.

3.1 Lokales Switching

3.1.1 Hauptschnittstelle

Die grundlegende Topologie ist eine lokale Verbindung zwischen zwei Hauptschnittstellen:



Router2 nimmt den gesamten von Gi 0/1/0/1 empfangenen Datenverkehr auf und leitet ihn an Te 0/0/0/3 weiter und umgekehrt.

Obwohl Router1 und Router3 in dieser Topologie über ein direktes Back-to-Back-Kabel zu verfügen scheinen, ist dies nicht der Fall, da Router2 tatsächlich zwischen den TenGigE- und GigabitEthernet-Schnittstellen übersetzt. Router2 kann Funktionen auf diesen beiden Schnittstellen ausführen. Eine Zugriffskontrollliste (ACL) kann beispielsweise bestimmte Pakettypen oder eine Richtlinienzuweisung verwerfen, um Datenverkehr mit niedriger Priorität zu steuern oder zu begrenzen.

Eine grundlegende Punkt-zu-Punkt-Verbindung wird zwischen zwei Hauptschnittstellen konfiguriert, die auf Router2 als l2transport konfiguriert sind:

```
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
```

```
!
```

Auf Router 1 und Router 3 werden die Hauptschnittstellen mit CDP und einer IPv4-Adresse konfiguriert:

```
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 betrachtet Router3 als CDP-Nachbarn und kann einen Ping an 10.1.1.2 (die Schnittstellenadresse von Router3) senden, als wären die beiden Router direkt verbunden.

Da auf Router2 keine Subschnittstelle konfiguriert ist, werden eingehende Frames mit einem VLAN-Tag transparent übertragen, wenn auf Router1 und Router3 dot1q-Subschnittstellen konfiguriert sind:

```
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
```

Nach 10.000 Pings von Router1 zu Router3 können Sie die Show-Schnittstelle und die show l2vpn-Befehle verwenden, um sicherzustellen, dass Ping-Anforderungen, die von Router2 auf einer AC empfangen werden, an die andere AC weitergeleitet werden und dass Ping-Antworten auf die gleiche Weise in umgekehrter Richtung verarbeitet werden.

```
RP/0/RSP0/CPU0:router2#sh int gig 0/1/0/1
GigabitEthernet0/1/0/1 is up, line protocol is up
Interface state transitions: 1
Hardware is GigabitEthernet, address is 0024.986c.63f1 (bia 0024.986c.63f1)
Description: static lab connection to acdc 0/0/0/1 - dont change
Layer 2 Transport Mode
MTU 1514 bytes, BW 1000000 Kbit (Max: 1000000 Kbit)
reliability 255/255, txload 0/255, rxload 0/255
Encapsulation ARPA,
Full-duplex, 1000Mb/s, SXFD, link type is force-up
output flow control is off, input flow control is off
loopback not set,
```

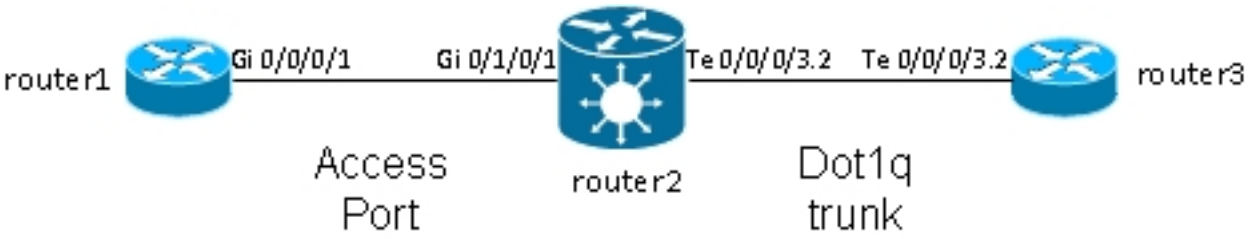
```
Last input 00:00:00, output 00:00:00
Last clearing of "show interface" counters 00:01:07
5 minute input rate 28000 bits/sec, 32 packets/sec
5 minute output rate 28000 bits/sec, 32 packets/sec
10006 packets input, 1140592 bytes, 0 total input drops
0 drops for unrecognized upper-level protocol
Received 0 broadcast packets, 6 multicast packets
0 runts, 0 giants, 0 throttles, 0 parity
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
10007 packets output, 1140832 bytes, 0 total output drops
Output 0 broadcast packets, 7 multicast packets
0 output errors, 0 underruns, 0 applique, 0 resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions


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


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

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

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

```
Type Ethernet
MTU 1500; XC ID 0x1880003; interworking none
Statistics:
packets: received 10006, sent 10008
bytes: received 1140592, sent 1140908

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

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

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

Platform AC context:
Egress AC: Local Switch, State: Bound
Flags: Remote is Simple AC
XID: 0x00000001, SHG: None
Ingress uIDB: 0x0007, Egress uIDB: 0x0007, NP: 0, Port Learn Key: 0
NP0
Egress uIDB:
Flags: L2, Status, Done
Stats ptr: 0x000000
VPLS SHG: None
L2 ACL Format: 0, L2 ACL ID: 0, IPV4 ACL ID: 0, IPV6 ACL ID: 0
```

```
VLAN1: 0, VLAN1 etype: 0x0000, VLAN2: 0, VLAN2 etype: 0x0000
UIDB IF Handle: 0x04000240, Search VLAN Vector: 0
QOS ID: 0, QOS format: 0
Xconnect ID: 0x00000001, NP: 0
Type: AC, Remote type: AC
Flags: Learn enable
uIDB Index: 0x0007, LAG pointer: 0x0000
Split Horizon Group: None
```

3.1.2 Subschnittstellen und VLAN-Manipulation

In der Terminologie der Cisco IOS® Software weist dieses Beispiel einen AC auf, der einer Switch-Port-Modus-Zugriffsschnittstelle ähnelt, und eine dot1q-Subschnittstelle, die einem Trunk ähnelt:



Normalerweise verwendet diese Topologie eine Bridge-Domäne, da das VLAN in der Regel mehr als zwei Ports enthält. Wenn es jedoch nur zwei Ports gibt, können Sie eine Punkt-zu-Punkt-Verbindung verwenden. In diesem Abschnitt wird beschrieben, wie Sie durch flexible Umschreibfunktionen mehrere Möglichkeiten zur Manipulation des VLANs erhalten.

3.1.2.1 Hauptschnittstelle und Dot1q-Subschnittstelle

In diesem Beispiel befindet sich die Hauptschnittstelle auf der einen Seite und die dot1q-Subschnittstelle auf der anderen Seite:

Dies ist die Hauptschnittstelle auf 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
!
```

Dies ist die dot1q-Subschnittstelle auf 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
```

Im Subschnittstellennamen TenGigE0/0/0/3.2 gibt es jetzt das Schlüsselwort *l2transport*. Router3 sendet dot1q-Frames mit Tag 2, die mit der TenGigE0/0/0/3.2-Subschnittstelle auf Router2 übereinstimmen.

Das eingehende Tag 2 wird durch den **symmetrischen** Befehl **rewrite ingress tag pop 1** in Eingangsrichtung entfernt. Da der Tag auf dem TenGigE0/0/0/3.2 in Eingangsrichtung entfernt wurde, werden die Pakete auf GigabitEthernet0/1/0/1 ohne Tags in Ausgangsrichtung gesendet.

Router1 sendet unmarkierte Frames, die der Hauptschnittstelle GigabitEthernet0/1/0/1 entsprechen.

GigabitEthernet0/1/0/1 verfügt über keinen **Rewrite**-Befehl, sodass kein Tag geöffnet, verschoben oder übersetzt wird.

Wenn Pakete aus TenGigE0/0/0/3.2 weitergeleitet werden müssen, wird das dot1q-Tag 2 aufgrund des *symmetrischen* Schlüsselworts im Befehl **rewrite ingress tag pop 1** verschoben. Der Befehl öffnet ein Tag in Eingangsrichtung, schiebt jedoch ein Tag symmetrisch in Ausgangsrichtung. Dies ist ein Beispiel auf 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
```

Überwachen Sie die Subschnittstellen-Zähler mit derselben **show-Schnittstelle** und den **show l2vpn-**Befehlen:

```
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
```

Wie erwartet, entspricht die Anzahl der über TenGigE0/0/0/3.2 empfangenen Pakete der Anzahl der über GigabitEthernet0/1/0/1 gesendeten Pakete und umgekehrt.

3.1.2.2 Subschnittstelle mit Kapselung

Anstelle der Hauptschnittstelle auf GigabitEthernet0/1/0/1 können Sie eine Subschnittstelle mit **Kapselungsstandard** verwenden, um alle Frames abzufangen, oder mit **Kapselung untagged,** um nur untagged Frames zuzuordnen:

```
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 Eingangs-richtung bei GigabitEthernet0/1/0/1.1

Anstatt Tag 2 in Eingangsrichtung auf TenGigE0/0/0/3.2 einzublenden, können Sie Tag 2 in Eingangsrichtung auf GigabitEthernet0/1/0/1.1 schieben und auf TenGigE0/0/0/3.2 nichts tun:

```
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
```

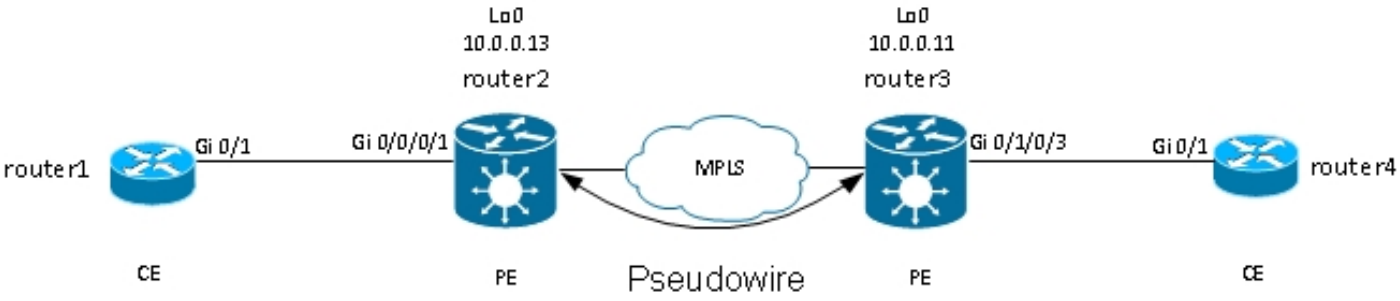
```
encapsulation dot1q 2

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
```

So können Sie sehen, dass das EVC-Modell mit den Befehlen **Kapselung** und **Umschreiben** Ihnen eine große Flexibilität bei der Anpassung und Manipulation von VLAN-Tags bietet.

3.2 Virtuelle Private-Wire-Services

3.2.1 Übersicht

Mit Virtual Private Wire Services (VPWS), auch als Ethernet over MPLS (EoMPLS) bezeichnet, können zwei L2VPN Provider Edge (PE)-Geräte den L2VPN-Datenverkehr über eine MPLS-Cloud tunneln. Die beiden L2VPN-PEs sind in der Regel an zwei verschiedenen Standorten über einen MPLS-Core verbunden. Die beiden an jedem L2VPN-PE angeschlossenen ACs sind über einen PW mit dem MPLS-Netzwerk, dem MPLS-PW, verbunden.



Jeder PE benötigt ein MPLS-Label, um das Loopback des Remote-PEs zu erreichen. Dieses Label, das in der Regel als IGP-Label (Interior Gateway Protocol) bezeichnet wird, kann über das MPLS Label Distribution Protocol (LDP) oder MPLS Traffic Engineering (TE) abgerufen werden.

Die beiden PEs stellen untereinander eine gezielte MPLS-LDP-Sitzung her, um den PW-Status zu ermitteln und zu steuern. Ein PE kündigt dem anderen PE das MPLS-Label zur PW-Identifizierung an.

> **Hinweis**: BGP kann zwar für die Signalisierung verwendet werden, wird in diesem Dokument jedoch nicht behandelt.

Der von Router2 auf seinem lokalen Wechselstrom empfangene Datenverkehr wird in einen MPLS-Label-Stack gekapselt:

- Das äußere MPLS-Label ist das IGP-Label, mit dem der Loopback von Router3 erreicht wird. Hierbei kann es sich um das implizite Null-Label handeln, wenn die Labels direkt verbunden sind. Dies bedeutet, dass kein IGP-Label angehängt wird.
- Das innere MPLS-Label ist das PW-Label, das von Router3 über die anvisierte LDP-Sitzung angekündigt wird.

- Abhängig von der Konfiguration und dem Kapselungstyp kann hinter den MPLS-Labels ein PW-Kontrollwort stehen. Das Kontrollwort wird standardmäßig nicht auf Ethernet-Schnittstellen verwendet und muss bei Bedarf explizit konfiguriert werden.
- Der transportierte L2-Frame wird in das Paket eingefügt.
- Einige VLAN-Tags werden je nach Konfiguration und PW-Typ über den PW transportiert.

Der vorletzte Hop, kurz vor router3 im MPLS-Core, öffnet das IGP-Label oder ersetzt es durch ein explizites Null-Label. Das wichtigste, aussagekräftige Label im Frame, das Router3 empfängt, ist das PW-Label, das Router3 Router2 für den PW signalisiert hat. Router3 weiß also, dass der mit diesem MPLS-Label empfangene Datenverkehr an den mit Router4 verbundenen Wechselstrom weitergeleitet werden muss.

Im vorherigen Beispiel sollten Sie zunächst prüfen, ob jedes L2VPN über ein MPLS-Label für das Loopback des Remote-PE verfügt. Dies ist ein Beispiel dafür, wie Sie die Labels auf Router2 überprüfen:

```
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
```

Die Wechselstromkonfiguration ist nach wie vor identisch:

```
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
```

Da es keinen **Rewrite Ingress Pop**-Befehl gibt, wird der eingehende VLAN-Tag 2 über den PW transportiert. Weitere Informationen finden Sie unter Typ 4 und 5.

Die L2VPN-Konfiguration gibt die lokale AC und den Remote-L2VPN-PE mit einer PW-ID an, die auf jeder Seite übereinstimmen und für jeden Nachbarn eindeutig sein muss:

```
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
```

Die entsprechende Konfiguration auf Router3 ist wie folgt:

```
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
```

Verwenden Sie den Befehl **show l2vpn xconnect detail**, um Details zum Cross-Connect

anzuzeigen:

```
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
```

Beachten Sie bei dieser Konfiguration Folgendes:

- Die Maximum Transmission Unit (MTU) des Wechselstroms beträgt 1504, da der Eingang des Wechselstroms nicht angewählt wird. Die MTU muss auf beiden Seiten übereinstimmen, da die PW andernfalls nicht hochgefahren wird.
- 186 Pakete wurden auf dem AC empfangen und wie erwartet auf dem PW gesendet.
- 38448 Pakete wurden auf der PW empfangen und wie erwartet auf der AC gesendet.
- Das lokale Label auf Router2 ist 16026 und ist das Label, das Router3 als inneres Label verwendet. Die Pakete werden auf Router2 empfangen, wobei das MPLS-Label das oberste Label ist, da das IGP-Label vom vorletzten MPLS-Hop abgerufen wurde. Router2 weiß, dass eingehende Frames mit diesem PW-Label auf AC Gi 0/0/0/1.2 umgeschaltet werden sollten:

```
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- und AC-gekoppelter Status

Bei einem Punkt-zu-Punkt-Crossconnect werden Wechselstrom und PW gekoppelt. Wenn die Wechselstromversorgung ausfällt, signalisiert der L2VPN-PE dem Remote-PE über LDP, dass der PW-Status "ausgefallen" sein sollte. Dies löst bei konfigurierter PW-Redundanz Konvergenz aus. Weitere Informationen finden Sie im Abschnitt zur Redundanz.

In diesem Beispiel ist die Wechselspannung auf Router2 ausgefallen und sendet den PW-Status "Wechselspannung ausgefallen" an 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 weiß, dass der PW ausfallen sollte, da die Remote-Wechselstromversorgung ausgefallen ist:

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

Group test, XC p2p4, state is down; Interworking none
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1504; XC ID 0xc40003; interworking none
Statistics:
packets: received 38545, sent 186
bytes: received 2620952, sent 12644
drops: illegal VLAN 0, illegal length 0
 PW: neighbor 10.0.0.13, PW ID 222, state is down ( local ready )
PW class not set, XC ID 0xc0000005
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

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

3.2.3 PWs vom Typ 4 und Typ 5

Es können zwei Arten von PWs verwendet werden - Typ 4 und Typ 5.

- Ein Typ-4-PW wird als VLAN-basierter PW bezeichnet. Der Eingangs-PE soll die eingehenden VLAN-Tags, die über den PW übertragen werden sollen, nicht entfernen.

  Auf EVC-basierten Plattformen wie dem ASR 9000 besteht das Problem darin, dass die

eingehenden ACs möglicherweise über einen **Rewrite-**Befehl verfügen, der die eingehenden VLAN-Tags öffnet, sodass möglicherweise kein VLAN-Tag über den PW übertragen werden kann. Um diese Möglichkeit zu nutzen, fügen die EVC-Plattformen für Typ-4-PWs einen Dummy-VLAN-Tag 0 oben auf den Frame ein. Typ-4-PWs werden mit dem Befehl **transport-mode vlan** konfiguriert. Der Remote-PE sollte EVC-basiert sein und erkennen, dass das obere VLAN-Tag das zu entfernende Dummy-Tag ist.

Wenn Sie jedoch einen Typ-4-PW zwischen einer EVC-Plattform und einer Nicht-EVC-Plattform verwenden, kann dies zu Interoperabilitätsproblemen führen. Die Nicht-EVC-Plattform betrachtet das obere VLAN-Tag nicht als Dummy-VLAN-Tag, sondern leitet den Frame mit dem Dummy-VLAN-Tag 0 als äußeren Tag weiter. Die EVC-Plattformen können die auf dem eingehenden Frame empfangenen VLAN-Tags mit dem Befehl **rewrite** bearbeiten. Die Ergebnisse dieser VLAN-Manipulation werden über Typ 4 PW übertragen, wobei das zusätzliche Dummy-Tag 0 oben steht.

Kürzlich veröffentlichte Cisco IOS XR-Softwareversionen bieten die Möglichkeit, ein Typ-4-PW ohne Verwendung des Dummy-Tags 0 mit dem Befehl **transport-mode vlan passthrough zu** verwenden. Die VLAN-Tag-Manipulation am Ethernet Flow Point (EFP) muss sicherstellen, dass mindestens ein Tag erhalten bleibt, da ein VLAN-Tag auf einem Typ-4-PW transportiert werden muss und in diesem Fall kein Dummy-Tag vorhanden ist, der diese Anforderung erfüllt. Die Tags, die nach dem Umschreiben der eingehenden Schnittstellentags auf dem Frame verbleiben, werden transparent durch den PW transportiert.

- Ein Typ-5-PW wird als Ethernet-Port-basierter PW bezeichnet. Der Eingangs-PE transportiert Frames, die auf einer Hauptschnittstelle empfangen werden, oder nachdem die Subschnittstellen-Tags entfernt wurden, wenn das Paket auf einer Subschnittstelle empfangen wird. Ein markierter Frame muss nicht über ein Typ-5-PW gesendet werden, und die EVC-basierten Plattformen fügen kein Dummy-Tag hinzu. Die EVC-basierten Plattformen können die auf dem eingehenden Frame empfangenen VLAN-Tags mit dem Befehl **rewrite** bearbeiten. Die Ergebnisse dieser VLAN-Manipulation werden über Typ-5-PW übertragen, unabhängig davon, ob diese mit oder ohne Tags versehen sind.

Standardmäßig versuchen die L2VPN-PEs, einen Typ-5-PW auszuhandeln, wie in diesem Beispiel gezeigt:

```
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
```

Der PW-Typ "Ethernet" gibt einen Typ "5 PW" an.

Dies ist eine Sniffer-Erfassung einer ARP-Anforderung, die von Router 1 gesendet und von Router 2 über den PW an Router 3 gekapselt wurde:

```
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)
```

Das MPLS-Label 16031 ist das von Router3 angekündigte PW-Label. Die Sniffer-Erfassung wurde zwischen dem vorletzten Hop und Router3 durchgeführt, sodass kein IGP-Label vorhanden ist.

Der gekapselte Ethernet-Frame beginnt unmittelbar nach dem PW-Label. Es kann ein PW-Kontrollwort geben, es ist in diesem Beispiel jedoch nicht konfiguriert.

Selbst wenn es sich um einen Typ-5-PW handelt, wird der von Router2 auf dem AC empfangene VLAN-Tag 2 transportiert, da kein **Rewrite-**Befehl vorhanden ist, der ihn auf dem AC öffnet. Die Ergebnisse, die nach der Umschreibverarbeitung vom AC kommen, werden transportiert, da es kein automatisches Tag-Popping auf den EVC-basierten Plattformen gibt. Beachten Sie, dass es keinen Dummy-VLAN-Tag 0 mit einem Typ-5-PW gibt.

Wenn Sie den **symmetrischen** Befehl **rewrite ingress tag pop 1** konfiguriert haben, wird kein VLAN-Tag über den PW übertragen.

Hier ist ein Beispiel für einen Typ-4-PW mit der Konfiguration einer PW-Klasse auf Router2 und Router3.

> **Hinweis**: Wenn Sie einen Typ 4 nur auf einer Seite konfigurieren, bleibt der PW geschlossen und meldet "Fehler: PW-Typ nicht zugeordnet".

```
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
!
!
!
!
```

Der PW-Typ Ethernet VLAN gibt einen Typ 4 PW an.

```
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
```

Auf dem zu transportierenden Rahmen befindet sich nun ein Dummy-Tag 0:

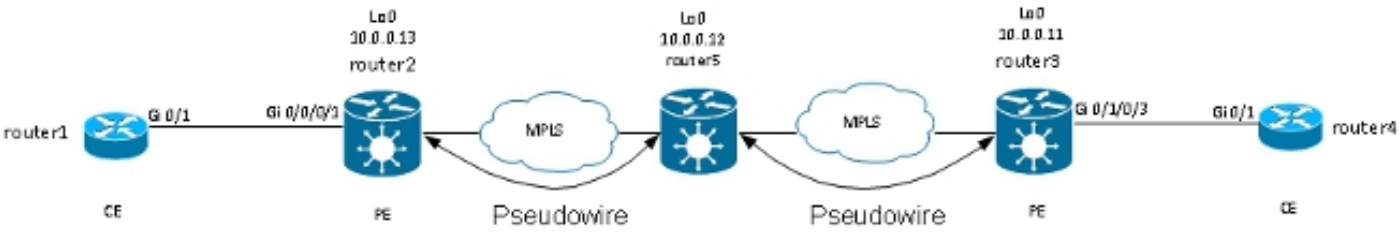
```
Frame 15: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: Cisco_2f:dc:04 (00:0b:60:2f:dc:04), Dst: Cisco_1e:93:50
(00:24:f7:1e:93:50)
MultiProtocol Label Switching Header, Label: 16031, Exp: 0, S: 1, TTL: 251
Ethernet II, Src: Cisco_03:1f:46 (00:1d:46:03:1f:46), Dst: Broadcast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

Der Egress-PE auf EVC-Basis entfernt das Dummy-Tag und leitet den Frame mit dem Tag 2 an

den lokalen AC weiter. Der Egress-PE wendet die auf seinem AC konfigurierte lokale Tag-Manipulation auf den auf dem PW empfangenen Frame an. Wenn der lokale AC als **Rewrite Ingress Tag pop 1 symmetric** konfiguriert ist, muss der konfigurierte Tag in Ausgangsrichtung verschoben werden, sodass ein neuer Tag über den Tag 2 geschoben wird, der auf dem PW empfangen wird. Der Befehl zum Umschreiben ist sehr flexibel. Sie sollten jedoch sorgfältig prüfen, was Sie auf beiden Seiten des PW erreichen möchten.

3.2.4 Multisegment-PW

Es ist möglich, einen L2VPN-PE mit einem PW anstelle einer physischen Schnittstelle als AC zu verwenden:



Router 5 empfängt Pakete auf dem PW von Router 2 und schaltet die Pakete auf dem anderen PW auf Router 3 um. Router5 wechselt also zwischen PWs, um einen Multisegment-PW zwischen Router2 und Router3 zu erstellen.

Die Konfiguration auf Router2 verweist nun auf Router5 als Remote-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
!
!
!
!
```

Die Konfiguration auf Router5 ist grundlegend:

```
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
!
!
!
```

Der Befehl **description** ist optional und wird in einen TLV (Type Length Value) für PW-Switching eingefügt, der von Router5 an jeden Remote-PE-Router (Router2 und Router3) gesendet wird. Die **Beschreibung** ist nützlich, wenn Sie ein PW-Problem beheben müssen, wenn sich in der Mitte ein Router befindet, der PW-Switching betreibt.

Geben Sie den Befehl **sh l2vpn xconnect** ein, um die PW Switching TLV zu überprüfen:

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

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

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------------------
Label 16042 unknown
Group ID 0x4000280 0x0
Interface GigabitEthernet0/0/0/1.2 unknown
MTU 1504 unknown
Control word disabled unknown
PW type Ethernet unknown
VCCV CV type 0x2 0x0
(none)
(LSP ping verification)
VCCV CC type 0x4 0x0
(none)
(TTL expiry)
------------ ------------------------------ ------------------------------
Outgoing PW Switching TLVs (Label Mapping message):
Local IP Address: 10.0.0.12, Remote IP Address: 10.0.0.13, PW ID: 222
Description: R1-R5-R3
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Statistics for MS-PW:
packets: received 0
bytes: received 0
MIB cpwVcIndex: 3221225474
Create time: 02/05/2013 15:37:53 (00:34:43 ago)
Last time status changed: 02/05/2013 16:12:30 (00:00:06 ago)
Last time PW went down: 02/05/2013 16:12:30 (00:00:06 ago)
PW: neighbor 10.0.0.13, PW ID 222, state is up ( established )
PW class not set, XC ID 0xc0000001
Encapsulation MPLS, protocol LDP
Source address 10.0.0.12
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ------------------------------
Label 16043 16056
Group ID 0x6000180 0x4000280
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
MTU 1504 1504
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x4 0x6
```

```
(router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ----------------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Outgoing PW Switching TLVs (Label Mapping message):
Local IP Address: 10.0.0.12, Remote IP Address: 10.0.0.11, PW ID: 223
Description: R2-R5-R3
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
Statistics for MS-PW:
packets: received 0
bytes: received 0
MIB cpwVcIndex: 0
Create time: 02/05/2013 15:37:53 (00:34:43 ago)
Last time status changed: 02/05/2013 16:12:35 (00:00:01 ago)
Last time PW went down: 02/05/2013 16:12:30 (00:00:06 ago)
```

Router5 sendet eine PW-Switching-TLV an Router3 mit den Details seiner PW an Router2 und eine PW-Switching-TLV an Router2 mit den Details seiner PW an Router3.

3.2.5 Redundanz

Ein Point-to-Point-PW kann verwendet werden, um zwei Standorte zu verbinden. Diese beiden Standorte sollten jedoch bei einem PE- oder Wechselstromausfall verbunden bleiben.

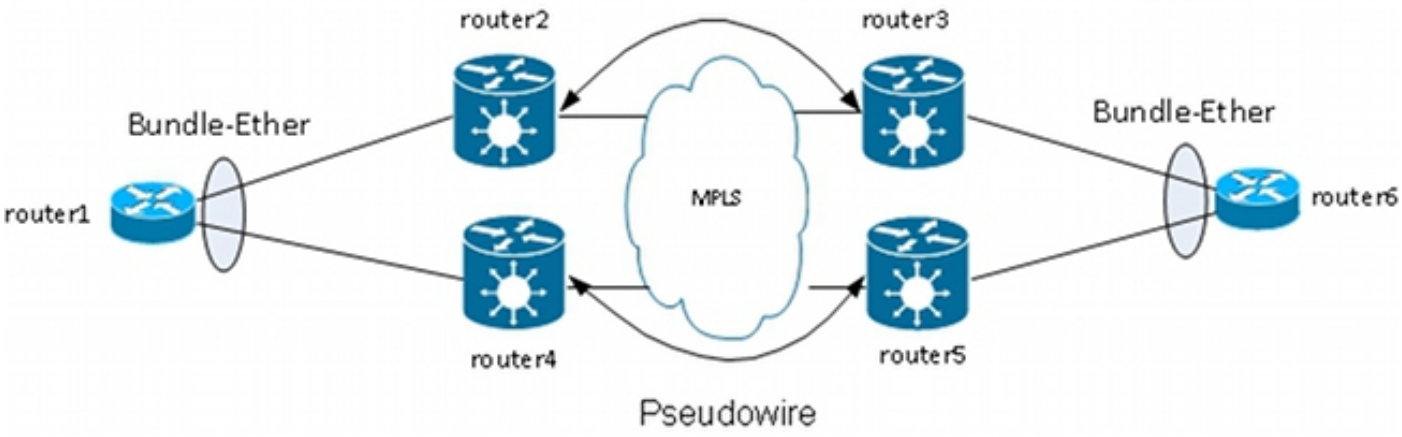
3.2.5.1 Core-Redundanz

Wenn Sie Topologieänderungen vornehmen, die das Rerouting im MPLS-Core beeinträchtigen, übernimmt der MPLS-PW sofort den neuen Pfad.

3.2.5.2 Paket über PWs

Ein Customer Edge (CE)-Gerät kann über ein Ethernet-Paket mit dem PE verbunden werden, um eine Verbindungsredundanz sicherzustellen, wenn ein Verbindungsausfall zwischen dem CE und dem PE bei einem Paketmitglied auftritt. Das Paket bleibt auch dann aktiv, wenn ein Link-Mitglied des Pakets ausfällt. Beachten Sie, dass dies keine PE-Redundanz bietet, da bei einem PE-Ausfall das gesamte Paket ausfällt.

Eine Möglichkeit zur Redundanz besteht darin, mehrere Schaltkreise über Punkt-zu-Punkt-PWs zu übertragen. Jeder Schaltkreis ist Teil eines Ethernet-Bündels zwischen zwei CEs:



Der PE terminiert das Paket nicht und transportiert stattdessen Frames transparent über den PW, einschließlich der LACP-Frames (Link Aggregation Control Protocol), die CEs zwischen ihnen austauschen.

Bei diesem Design fällt beim Verlust eines Wechselstroms oder eines PE das Mitglied des Pakets aus, das Paket bleibt jedoch aktiv.

> **Hinweis:** LACP-BPDUs wurden vom ASR 9000 in früheren Versionen als der Cisco IOS XR Software-Version 4.2.1 nicht über L2VPN transportiert.

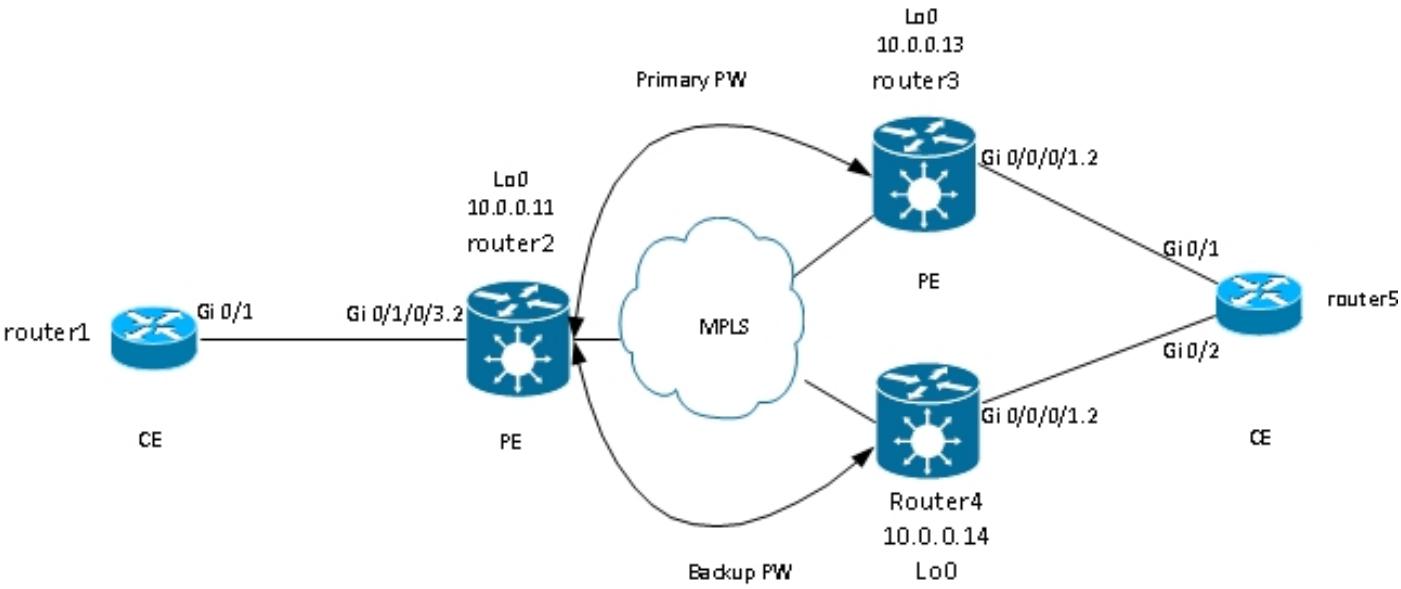
Der CE stellt in diesem Design immer noch einen Single Point of Failure dar. Weitere Redundanzfunktionen, die auf dem CE verwendet werden können:

- Link-Aggregationsgruppe mit mehreren Chassis (MC-LAG)
- ASR 9000 Network Virtualization (nV)-Clustering
- Virtual Switching System (VSS) auf Cisco IOS-Switches
- Virtual Port Channel (vPC) auf Cisco Nexus Switches

Aus PE-Sicht gibt es eine einfache Punkt-zu-Punkt-Verbindung zwischen einem Wechselstrom- und einem MPLS-PW.

3.2.5.3 PW-Redundanz

PEs können außerdem mithilfe der Funktion PW-Redundanz Redundanz bereitstellen.



Router2 hat einen primären PW zu Router3. Der Datenverkehr von Router1 zu Router6 fließt unter normalen Umständen über diesen primären PW. Router2 verfügt auch über einen Backup-PW für Router4 im Hot-Standby-Modus, aber unter normalen Umständen fließt kein Datenverkehr über diesen PW.

Tritt ein Problem mit dem primären PW, mit dem Remote-PE des primären PW (Router3) oder mit dem Wechselstrom auf dem Remote-PE (Router3) auf, aktiviert Router2 sofort den Backup-PW und der Datenverkehr beginnt, diesen zu durchlaufen. Der Datenverkehr wird wieder zum primären PW geleitet, wenn das Problem behoben ist.

Die Konfiguration auf Router 2 ist wie folgt:

```
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
!
!
!
!
!
```

Die Standardkonfiguration auf Router3 und Router4 ist wie folgt:

```
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
!
!
!
!
```

Unter stabilen Bedingungen ist der PW an Router3 aktiv, und der PW an Router4 befindet sich im Standby-Zustand:

```
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#
```

Da der Wechselstromstatus und der PW-Status gekoppelt sind, signalisiert Router3 dem Router2 den Status "AC Down", wenn der Wechselstrom auf Router3 ausfällt. Router 2 schaltet seinen primären PW aus und aktiviert den Backup-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
```

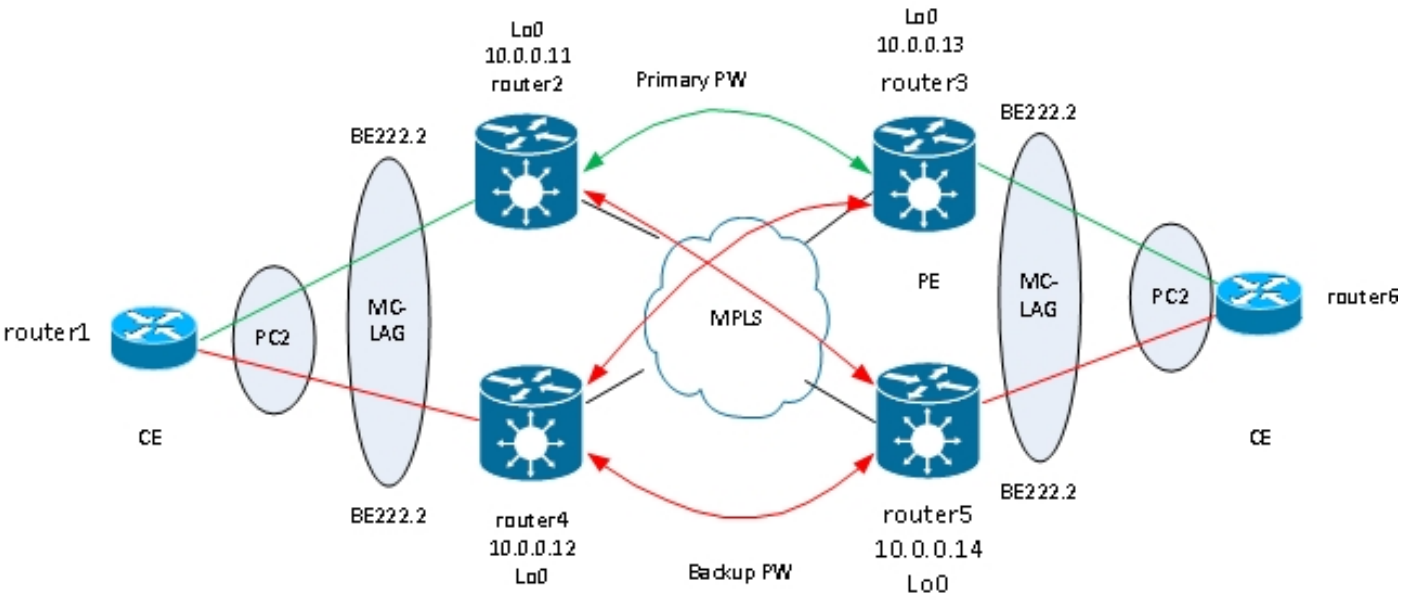
```
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

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#
```

Wenn die Wechselstromversorgung auf Router3 wieder aktiviert wird, aktiviert Router2 die primäre Verbindung zwischen PW und Router3, und die Verbindung zwischen PW und Router4 wechselt in den Standby-Status.

Der Backup-PW wird auch aktiviert, wenn Router3 ausfällt und Router2 die Route zum Loopback verliert.

Der nächste logische Schritt ist die Einführung einer bidirektionalen PW-Redundanz mit zwei PEs an jedem Standort:



Bei diesem Full-Mesh von PWs tritt jedoch ein Problem auf, wenn zwei PWs gleichzeitig aktiv sind und eine Schleife in das Netzwerk eingeführt wird. Der Loop muss unterbrochen werden, in der Regel mithilfe des Spanning Tree Protocol (STP). Die Spanning-Tree-Instabilität an einem Standort soll jedoch nicht auf den anderen übertragen werden. Daher ist es besser, Spanning Tree nicht auf diesen PWs auszuführen und den Spanning Tree nicht zwischen den beiden Standorten zusammenzuführen. Einfacher ist es, wenn nur eine logische Verbindung zwischen den beiden Standorten besteht, sodass Spanning Tree nicht erforderlich ist.

Eine Lösung besteht darin, ein MC-LAG-Paket zwischen den beiden PEs an einem Standort und ihrem lokalen CE zu verwenden. Nur eines der beiden PE-Pakete ist aktiv, sodass die PW-Verbindung zum Remote-Standort aktiv ist. Die anderen PE-Geräte befinden sich im Standby-Zustand und verfügen nicht über eine dezentrale PW. Wenn nur ein PW zwischen den beiden Standorten aktiv ist, wird kein Loop eingeführt. Der PE mit dem aktiven PW verfügt außerdem über einen Standby-PW zum zweiten PE am Remote-Standort.

Unter stabilen Bedingungen befinden sich die aktiven Paketmitglieder auf Router2 und Router3, und der aktive PW befindet sich zwischen ihnen. Dies ist die Konfiguration auf 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
```

Auf Router5 befinden sich das lokale Paketmitglied und der primäre PW an Router2 im Standby-Zustand, und der Backup-PW an Router4 ist ausgefallen:

```
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
```

Auf Router6 ist das Bündelmitglied zu Router3 aktiv, während sich das Bündelmitglied zu Router5 im Standby-Zustand befindet:

```
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)
```

Wenn ein Bündelmitglied auf Router3 ausfällt, hat Router6 sein aktives Mitglied auf Router5:

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

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


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

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

Da der Bundle-Ether222 auf Router5 nicht verfügbar ist, fällt die mit Router2 verbundene PW gleichzeitig aus:

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

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

Router2 erkennt, dass seine PW zu Router3 ausgefallen ist, und aktiviert seine Backup-PW zu Router5:

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

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

Das Paketmitglied von Router 5 ist aktiv, und das primäre PW zu Router 2:

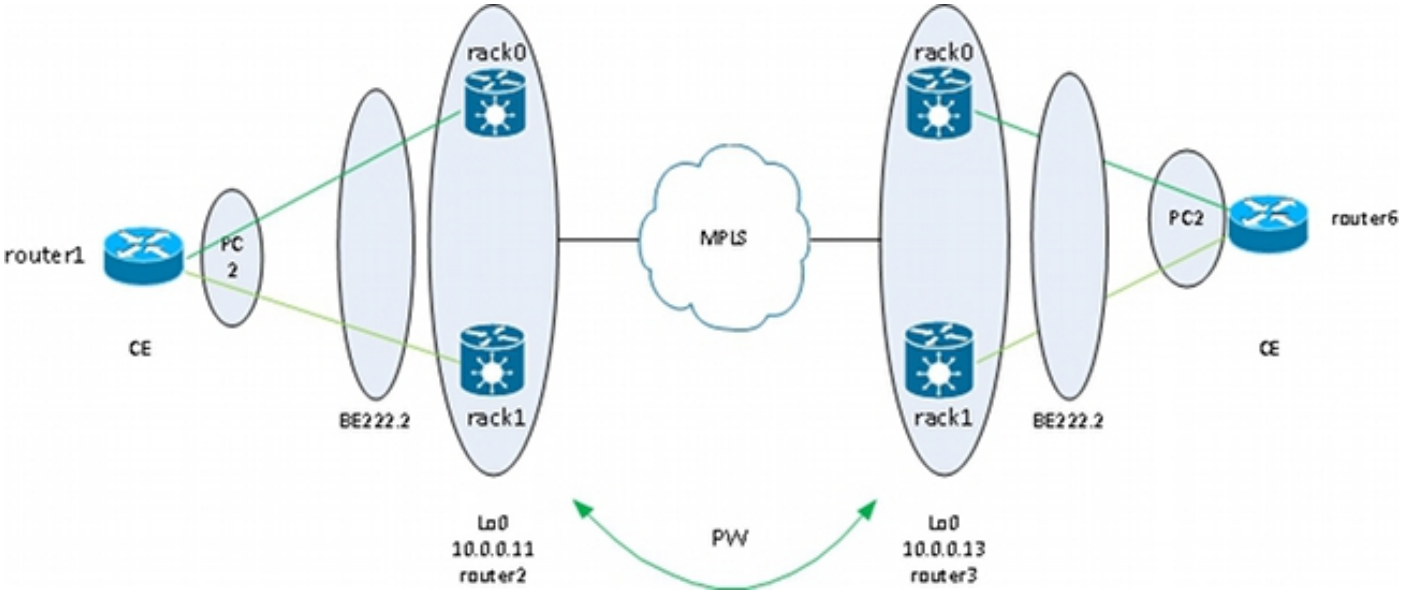
```
RP/0/RSP1/CPU0:router5#sh bundle bundle-ether 222
```

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

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

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

3.2.5.4 ASR 9000 nV Edge-Cluster

Das vorherige Design basiert auf einer MC-LAG- und PW-Redundanz und eignet sich gut für die Redundanz. Da sich einige Paketkomponenten jedoch im Standby-Modus befinden, wird der Datenverkehr nicht unter stabilen Bedingungen übertragen.

Wenn alle Paketmitglieder aktiv sein sollen, auch unter stabilen Bedingungen, können Sie einen ASR 9000-Cluster verwenden, bei dem die Paketmitglieder vom CE mit jedem Rack des PE verbunden sind:



Dieses Design bietet Redundanz bei einem Verbindungsausfall eines Paketmitglieds zwischen dem CE und dem PE, einem Rack- und einem Core-Verbindungsausfall, solange der Cluster doppelt mit dem MPLS-Core verbunden ist und Redundanz im Core vorhanden ist. Die beiden Racks müssen nicht am selben Standort aufgestellt werden, sondern können sich an unterschiedlichen Standorten befinden. Rack-übergreifende Verbindungen sind in diesem Diagramm nicht dargestellt.

Wenn Sie Redundanz auf dem CE wünschen, können Sie eine Multi-Chassis-Lösung für den CE verwenden:

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

Die Konfiguration des ASR 9000-Clusters ist sehr einfach:

```
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 empfiehlt, eine statische LACP-System-MAC-Adresse und eine Paket-MAC-Adresse zu konfigurieren, um eine Änderung der MAC-Adresse zu vermeiden, die durch einen designierten

Gehäuse-Controller-Switchover verursacht wird. Dieses Beispiel zeigt, wie Sie nach den Adressen suchen:

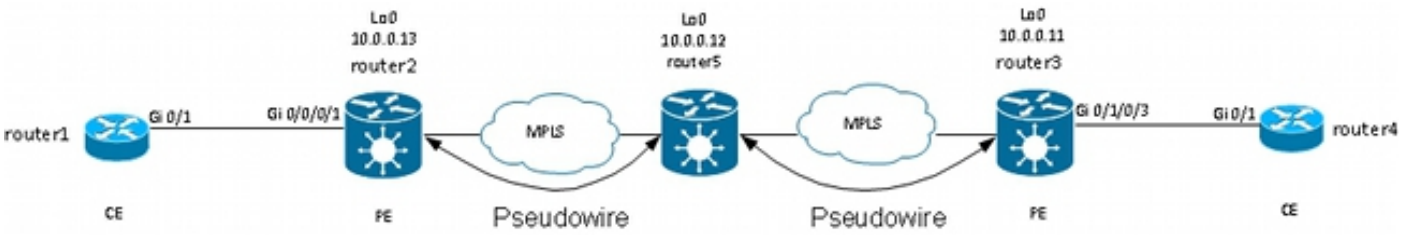
```
RP/1/RSP0/CPU0:router2#sh int bundle-ether 222 | i address is
Hardware is Aggregated Ethernet interface(s), address is 0024.f71e.d309
Internet address is Unknown
RP/1/RSP0/CPU0:router2#
RP/1/RSP0/CPU0:router2#conf
RP/1/RSP0/CPU0:router2(config)#int bundle-ether 222
RP/1/RSP0/CPU0:router2(config-if)#mac-address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

Zusammenfassend handelt es sich hierbei um den Bundle-Ether 222 mit einem Element auf jedem Rack (zehn 0/0/0/8 auf Rack 0 und zehn 1/0/0/8 auf Rack 1) und die für eine Punkt-zu-Punkt-Verbindung konfigurierte Paket-Subschnittstelle:

```
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

Cisco Router und Switches senden in der Regel CDP-Pakete ohne dot1q-Tags. Es gibt mehrere Szenarien, die bestimmen, was mit diesen CDP-Paketen geschieht, wenn sie von einem IOS XR-Router empfangen werden, der für eine Verbindung konfiguriert ist:



In dieser Topologie kann Router1 seinen lokalen PE-Router2 je nach Konfiguration als CDP-Nachbarn oder den Remote-CE-Router4 sehen.

3.3.1 CDP ist auf der Hauptschnittstelle von L2VPN PE nicht aktiviert

Die CDP-Pakete vom L2VPN-CE werden über die Querverbindung transportiert. Die beiden L2VPN-CEs sehen sich gegenseitig (mithilfe des Befehls **show cdp neighbors)**, wenn die Hauptschnittstelle als l2transport konfiguriert ist oder wenn eine Subschnittstelle vorhanden ist, die mit den nicht markierten CDP-Frames übereinstimmt.

Dies ist ein Beispiel für die Hauptschnittstelle:

```
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
!
!
!
!
```

Dies ist ein Beispiel für eine nicht getaggte Subschnittstelle:

```
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 diesen beiden Beispielen werden die CDP-Pakete über den Cross-Connect übertragen, und die CEs sehen einander als CDP-Nachbarn. Der CE sieht den PE nicht als CDP-Nachbarn:

```
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 aktiviert in der Hauptschnittstelle von L2VPN PE

Der PE verarbeitet die nicht getaggten CDP-Pakete, und der PE und der CE sehen einander als Nachbarn. Der CE erkennt den Remote-CE jedoch nicht, wenn CDP an der Hauptschnittstelle des L2VPN-PE aktiviert ist.

Beachten Sie, dass:

- Sie können CDP nicht auf einer Hauptschnittstelle konfigurieren, die als l2transport

konfiguriert ist.
- Der PE fängt die CDP-Pakete ab, wenn CDP an der Hauptschnittstelle (nicht l2transport) konfiguriert ist. Dies geschieht selbst dann, wenn eine l2transport-Subschnittstelle konfiguriert ist, um den nicht markierten CDP-Paketen zu entsprechen (unter Verwendung der **Kapselungsbefehle "untagged"** oder "**encapsulation default"**). CDP-Pakete werden in diesem Fall nicht an den Remote-Standort übertragen.

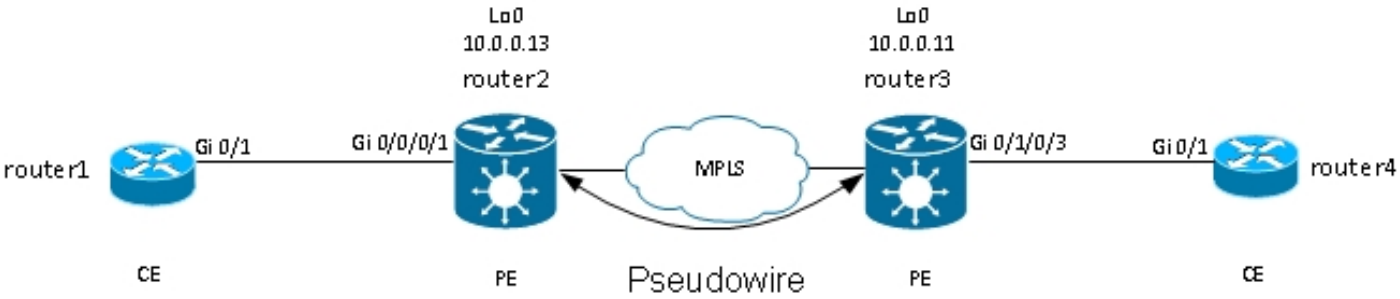
3.4 Spanning Tree

Wenn der L2VPN-CE ein Ethernet-Switch ist und Spanning-Tree-BPDUs an den L2VPN-PE sendet, werden diese BPDUs als regulärer Datenverkehr behandelt und entsprechend der L2VPN-Konfiguration transportiert.

STP- oder MST-BPDUs werden unmarkiert gesendet und über die Point-to-Point-Verbindung transportiert, wenn die Hauptschnittstelle als l2transport konfiguriert ist oder wenn eine l2transport-Subschnittstelle mit den Befehlen **encapsulation untagged** oder **encapsulation default** konfiguriert ist.

Per VLAN Spanning Tree Plus (PVST+) oder Rapid PVST+ (PVRST+) senden markierte BPDUs, die übertragen werden, wenn eine l2transport-Subschnittstelle vorhanden ist, die mit dem dot1q-Tag der BPDUs übereinstimmt.

Dies ist eine Beispieltopologie:



Router2 und Router3 transportieren nicht markierte Frames und Frames mit 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
!
```

```
!
!
!
```

Switch1 empfängt die nicht markierten BPDUs in VLAN 1 und die markierten BPDUs in VLAN2 von Switch4; sein Root-Port befindet sich auf Gi0/1 zu Switch4:

```
switch1#sh spanning-tree vlan 1

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32768
Address 0024.985e.6a00
Cost 8
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

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

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

switch1#sh spanning-tree vlan 2

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

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

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

Bei dieser Konfiguration wird die Spanning Tree-Domäne an Standort A mit der Spanning Tree-Domäne an Seite B zusammengeführt. Ein potenzielles Problem besteht darin, dass sich die Spanning Tree-Instabilität an einem Standort auf den anderen Standort ausbreiten kann.

Wenn Sie sicher sind, dass ein Standort nur über einen PW mit einem anderen Standort verbunden ist und es keine Backdoor-Verbindung gibt, die zu einem physischen Loop führen könnte, sollten Sie Spanning Tree nicht über die beiden Standorte ausführen. Dadurch werden die beiden Spanning-Tree-Domänen isoliert. Konfigurieren Sie dazu auf den CEs einen Spanning-Tree-bpdufilter oder auf den PEs eine Ethernet-Services-Zugriffsliste, um Frames mit der von den BPDUs verwendeten MAC-Zieladresse zu verwerfen. Eine Ethernet-Services-Zugriffsliste auf den PEs kann verwendet werden, um Frames mit der BPDU-Ziel-MAC oder anderen L2-Protokollen zu verwerfen, die nicht über den PW weitergeleitet werden sollen.

Dies ist eine Zugriffsliste, die Sie unter jeder L2Transport-(Sub-)Schnittstelle verwenden können, die zwischen den beiden Standorten übertragen wird:

```
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
!
```

Die Ethernet-Services-ACL beginnt, die BPDUs zu löschen:

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

Switch1 empfängt die BPDUs nicht mehr von Switch4, sodass Switch1 jetzt der Root ist:

```
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
```

Das Risiko, Spanning Tree für eine Verbindung zu deaktivieren, ist folgender: Wenn eine Backdoor-Verbindung zwischen den Standorten hergestellt wird, führt dies zu einer physischen Schleife, und Spanning Tree kann die Schleife nicht unterbrechen. Wenn Sie also Spanning Tree über einen PW deaktivieren, stellen Sie sicher, dass es keine redundanten Verbindungen zwischen den Standorten gibt und dass der PW die einzige Verbindung zwischen den Standorten bleibt.

Wenn mehrere Verbindungen zwischen Standorten bestehen, verwenden Sie eine Lösung wie VPLS zusammen mit einer Access Gateway-Version des Spanning Tree, z. B. MST Access Gateway (MSTAG) oder PVST+ Access Gateway (PVSTAG). Weitere Informationen finden Sie im Abschnitt Multipoint Service.

4. Multipoint-Dienst

> **Hinweise:**
>
> Verwenden Sie das Command Lookup-Tool (Tool für die Suche nach Befehlen) (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.
>
> Das Output Interpreter-Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter-Tool, um eine Analyse der **show**-Befehlsausgabe anzuzeigen.

Eine vollständige Beschreibung der Multipoint-L2-Funktionen finden Sie unter Implementieren von Multipoint-Layer-2-Services.

Mit nur zwei Schnittstellen in einer Punkt-zu-Punkt-Verbindung übernimmt ein L2VPN-Switch alles, was auf der Seite empfangen wird, und leitet es auf der anderen Seite weiter.

Wenn eine Bridge-Domäne mehr als zwei Schnittstellen umfasst, muss ein Ethernet-Switch eine Switching-Entscheidung treffen, um anhand der MAC-Zieladresse zu bestimmen, wohin Frames weitergeleitet werden sollen. Der Switch führt anhand der Quell-MAC-Adresse der empfangenen Frames MAC-Learning-Vorgänge aus und erstellt eine MAC-Adresstabelle.

Der Switch leitet bei dieser Methode Frames weiter:

- Broadcast-Frames werden an alle Ports übertragen. Verwenden Sie die Sturmkontrolle, um

die Broadcast-Überflutungsrate zu begrenzen.
- Multicast-Frames werden an alle Ports in der Bridge-Domäne geleitet, außer wenn Internet Group Management Protocol (IGMP)- oder Multicast Listener Discovery (MLD)-Snooping konfiguriert ist. Verwenden Sie die Sturmkontrolle, um die Multicast-Überflutungsrate zu begrenzen.
- Unicast-Frames mit einer Ziel-MAC-Adresse, die nicht Teil der MAC-Adresstabelle der Bridge-Domäne ist (unbekanntes Unicast), werden auf alle Ports in der Bridge-Domäne verteilt. Verwenden Sie die Sturmkontrolle, um die Unicast-Überflutungsrate zu begrenzen.
- Unicast-Frames mit einer Ziel-MAC-Adresse, die Teil der MAC-Adresstabelle der Bridge-Domäne ist, werden an den Port weitergeleitet, von dem die Ziel-MAC-Adresse abgerufen wurde.

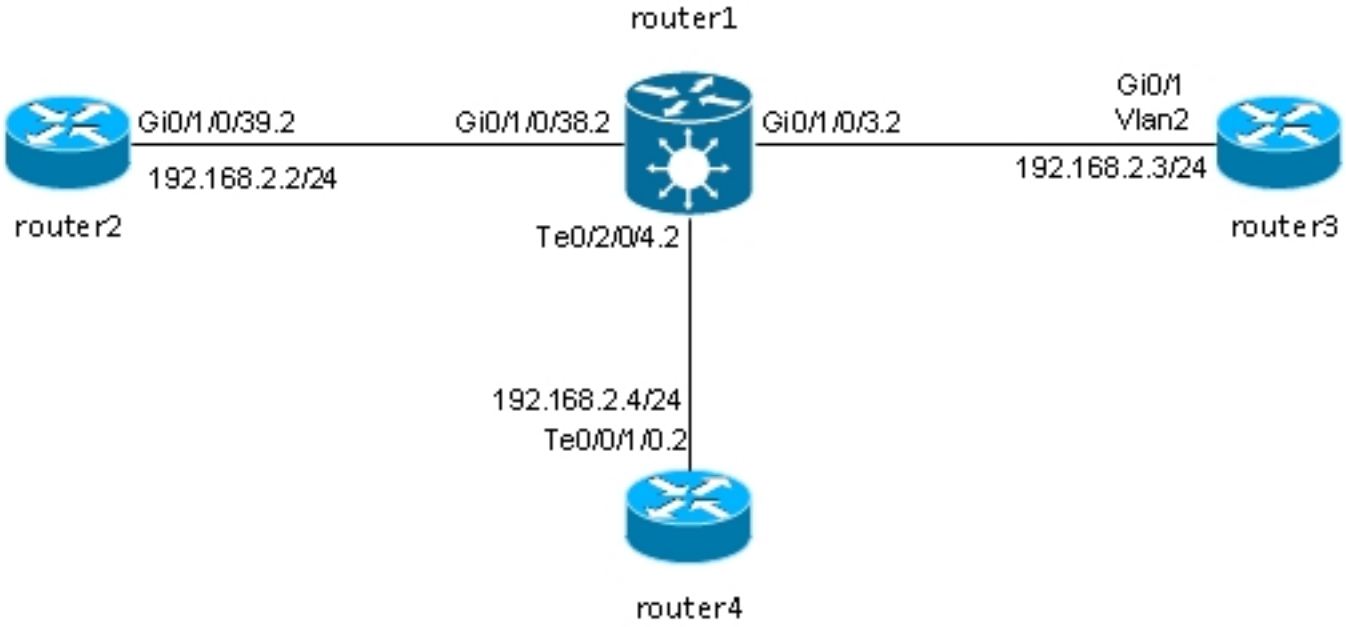
In der Cisco IOS XR-Software wird eine Broadcast-Domäne oder ein emuliertes LAN als Bridge-Domäne bezeichnet. Dies ähnelt einem VLAN in der Terminologie der Cisco IOS-Software, jedoch ist ein VLAN in IOS mit einer VLAN-Nummer verknüpft, die als dot1q-Tag auf den Trunks verwendet wird. Eine Bridge-Domäne in der Cisco IOS XR-Software ist nicht mit einem dot1q VLAN-Tag verknüpft. Sie können das EVC-Modell verwenden, um die dot1q-Tags zu manipulieren und dot1q-Subschnittstellen mit unterschiedlichen dot1q-VLAN-Nummern in derselben Bridge-Domäne einzurichten, oder um nicht getaggte Schnittstellen zu verwenden.

Eine Bridge-Domäne ist im Grunde eine Broadcast-Domäne, in der Broadcasts und Multicast-Frames übertragen werden. Jeder Bridge-Domäne ist eine MAC-Adresstabelle zugeordnet (es sei denn, die MAC-Ermittlung wird manuell durch eine Konfiguration deaktiviert, was sehr selten vorkommt). Dies entspricht in der Regel einem IPv4- oder IPv6-Subnetz, mit dem alle Hosts in der Bridge-Domäne direkt verbunden sind.

Bridge-Domänen können innerhalb einer Bridge-Gruppe gruppiert werden. Dies ist eine bequeme Möglichkeit, die Konfiguration zu überprüfen. Sie können einen show-Befehl für eine Bridge-Gruppe anstelle eines show-Befehls für jede Bridge-Domäne ausführen. Eine Bridge-Gruppe hat keine MAC-Adresstabelle oder andere Zuordnungen; sie wird nur für Konfigurations- und Anzeigebefehle verwendet.

4.1 Lokales Switching

Dies ist ein sehr einfaches Beispiel:



Router2, Router3 und Router4 sind über einen ASR 9000 verbunden, der ein LAN zwischen diesen drei Routern simuliert.

Dies sind die Schnittstellenkonfigurationen für diese drei Router:

```
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
!
```

Pakete werden von Router1 mit dem dot1q-Tag 2 empfangen und an die anderen Router mit dem dot1q-Tag 2 weitergeleitet.

In diesem Basisszenario gibt es zwei Optionen für die ACs:

1. Da alle ACs das dot1q-Tag 2 verwenden, können Sie es auf dem Frame belassen und den Frame auf der Ausgangsschnittstelle mit dem gleichen dot1q-Tag weiterleiten, wie es auf der Eingangsschnittstelle empfangen wurde. Der **symmetrische** Befehl **rewrite ingress tag pop 1** ist nicht erforderlich.

2. Sie können das eingehende dot1q-Tag 2 in die Eingangsrichtung und das dot1q-Tag 2 symmetrisch in die Ausgangsrichtung verschieben. Dies ist in diesem Basisszenario zwar nicht erforderlich, es empfiehlt sich jedoch, die Bridge-Domäne zu Beginn auf diese Weise zu konfigurieren, da dies mehr Flexibilität für die Zukunft bietet. Im Folgenden finden Sie zwei Beispiele für Änderungen, die nach der Erstkonfiguration vorgenommen werden können:

   - Wenn später in der Bridge-Domäne eine geroutete BVI-Schnittstelle eingeführt wird, müssen Pakete auf der BVI ohne Tags verarbeitet werden. Weitere Informationen finden Sie im Abschnitt .
   - Später wird eine neue AC hinzugefügt, die ein anderes dot1q-Tag verwendet. Das dot1q-Tag 2 wird in die Eingangsrichtung und das andere dot1q-Tag auf die neue Schnittstelle in die Ausgangsrichtung und umgekehrt verschoben.BVI

Pop der dot1q-Tags an jedem AC auf 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
!
```

Zeigen Sie die Konfiguration der Bridge-Domäne mit den folgenden drei ACs an:

```
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
!
!
```

```
!
!
```

Die Bridge-Domäne muss unter einer Bridge-Gruppe konfiguriert werden. Wenn andere Bridge-Domänen von diesem Kunden benötigt werden, können sie unter derselben Bridge-Gruppe konfiguriert werden: customer1. Wenn neue Bridge-Domänen einem anderen Kunden angehören, können Sie eine neue Bridge-Gruppe erstellen. In diesen Beispielen wird der Kunde verwendet, um Bridge-Domänen zu gruppieren. Bridge-Domänen können jedoch nach beliebigen Kriterien gruppiert werden.

Verwenden Sie den Befehl **show run l2vpn bridge group customer1 bridge-domain engineering**, um die Konfiguration der Bridge-Domäne anzuzeigen.

Verwenden Sie den Befehl **show run l2vpn bridge group customer1**, um die Konfiguration aller Bridge-Domänen anzuzeigen.

Verwenden Sie den Befehl **show l2vpn bridge-domain bd-name engineering** oder den Befehl **show l2vpn bridge-domain group customer1,** um Informationen über die Bridge-Domain anzuzeigen.

```
RP/0/RSP0/CPU0:router1#show l2vpn bridge-domain group customer1 bd-name
engineering
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 3 (3 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.2, state: up, Static MAC addresses: 0
Gi0/1/0/38.2, state: up, Static MAC addresses: 0
Te0/2/0/4.2, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
RP/0/RSP0/CPU0:router1#show l2vpn bridge-domain group customer1 bd-name
engineering det
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 6
Filter MAC addresses:
Create time: 28/05/2013 17:17:03 (00:18:06 ago)
```

```
No status change since creation
ACs: 3 (3 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40003; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 185066, sent 465
bytes: received 13422918, sent 34974
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
AC: GigabitEthernet0/1/0/38.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40005; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 8, sent 12287
bytes: received 770, sent 892418
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
AC: TenGigE0/2/0/4.2, state is up
```

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

Verwenden Sie den Befehl **show l2vpn bridge-domain group customer1 bd-name engineering det,** wenn Sie überprüfen möchten, ob Pakete von jedem AC empfangen und gesendet werden.

Fügen Sie das *mac-address*-Schlüsselwort zum Befehl **show l2vpn forwarding bridge-domain hinzu,** wenn Sie die mac-address-table überprüfen möchten:

```
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
```

Das MAC Learning wird von den Linecards in der Hardware ausgeführt, sobald ein Frame in der Bridge-Domäne empfangen wird. Es gibt auch einen Software-Cache der MAC-Adresstabelle, aber diese Software-Tabelle kann nicht kontinuierlich aktualisiert werden, um den Hardwareeinträgen zu entsprechen. Wenn der Befehl **show** in den letzten Code eingegeben wird, versucht er, die Softwaretabelle mit der Hardwaretabelle zu resynchronisieren. Nach maximal 15 Sekunden wird der aktuelle Status der Software-MAC-Adresstabelle ausgegeben, auch wenn die Neusynchronisierung nicht abgeschlossen ist (z.B. wenn die Tabelle groß ist). Verwenden Sie den Befehl **l2vpn resynchronize forwarding mac-address-table**, um die Software- und Hardwaretabellen manuell zu resynchronisieren.

```
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
```

Eine Syslog-Meldung gibt an, wann der Resynchronisierungsprozess abgeschlossen ist. Es ist daher sinnvoll, die Terminalüberwachung zu aktivieren, damit die Meldung angezeigt wird.

In der Spalte Re-Synchronisierungsalter wird das letzte Mal angezeigt, dass die MAC-Adresse aus der Hardwaretabelle heraus re-synchronisiert wurde.

Das *location*-Schlüsselwort ist der Speicherort einer eingehenden oder ausgehenden Linecard. Die MAC-Adressen werden in der Hardware zwischen Linecards ausgetauscht. Daher sollten MAC-Adressen auf jeder Linecard bekannt sein, auf der Wechselstrom oder PW vorhanden sind. Das *detail*-Schlüsselwort kann eine aktuellere Version der Softwaretabelle bereitstellen:

```
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
```

Die detaillierte Version des Befehls gibt die Gesamtzahl der in der Bridge-Domäne gelernten MAC-Adressen sowie die Anzahl der unter jedem AC gelernten MAC-Adressen an.

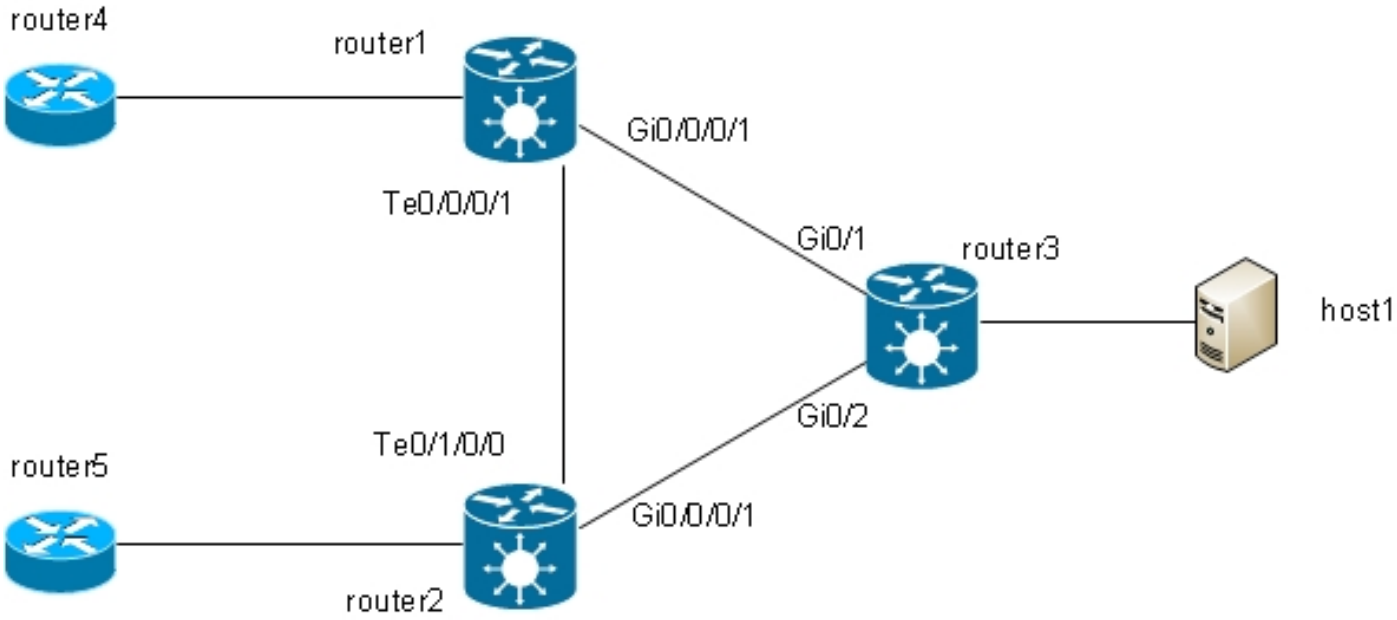
Das *Hardware*-Schlüsselwort fragt die MAC-Adresstabelle der Hardware direkt von den Eingangs- oder Ausgangsweiterleitungs-Engines ab:

```
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 Vollständige MST

Die vorherigen Beispiele für lokales Switching waren einfach, da nur Router mit der Bridge-Domäne verbunden waren. Sobald Sie jedoch mit der Verbindung von L2-Switches beginnen, können Sie eine Schleife einführen und den STP benötigen, um die Schleife zu unterbrechen:



In dieser Topologie sind Router1, Router2 und Router3 jeweils mit einer Bridge-Domäne konfiguriert, deren Schnittstellen im Diagramm enthalten sind. Wenn Router4 eine Broadcast-Nachricht (z. B. eine ARP-Anfrage) an Router1 sendet, wird diese von Router1 an Router2 und Router3 überflutet, von Router2 an Router3 und von Router3 an Router2. Dies führt zu einer Schleife und einem Broadcast-Sturm.

Um die Schleife zu unterbrechen, verwenden Sie ein STP. Es gibt mehrere Arten von STPs, aber die Cisco IOS XR-Software bietet nur eine vollständige Implementierung, die MST.

Es gibt auch Access Gateway-Versionen der Protokolle, die von der Cisco IOS XR-Software unterstützt werden, z. B. PVSTAG und MSTAG. Hierbei handelt es sich um statische, eingeschränkte Versionen des Protokolls, die in bestimmten Topologien, in der Regel mit VPLS, verwendet werden können. Sie werden in den Abschnitten zu MSTAG und PVSTAG beschrieben. In der Cisco IOS XR-Software ist MST die einzige Option, wenn eine Topologie mit mehreren Switches vorhanden ist und eine vollständige Spanning Tree-Implementierung erforderlich ist.

Auf jedem Router werden zwei Subschnittstellen konfiguriert, die einer Bridge-Domäne hinzugefügt werden. Für Router1 lautet die Konfiguration:

```
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 wird auf der Hauptschnittstelle konfiguriert. In diesem Beispiel wird VLAN 2 Instanz 1 zugewiesen, und alle anderen VLANs bleiben die Standardinstanz 0. (Eine realistischere Konfiguration würde VLANs gleichmäßig auf Instanzen aufteilen.)

Die Auswahl der Root-Bridge innerhalb eines STP-Netzwerks wird durch die konfigurierte Priorität und die integrierte Bridge-ID jedes Geräts bestimmt. Das Gerät mit der niedrigsten Priorität oder mit der gleichen niedrigsten Priorität, jedoch der niedrigsten Bridge-ID, wird als Root Bridge ausgewählt. In diesem Beispiel ist Router3 mit einer niedrigeren Priorität als Router1 für Instanz 0 konfiguriert, sodass Router3 der Root für Instanz 0 ist. Router1 hat eine niedrigere Priorität als Router3 für Instanz 1, sodass Router1 der Root für Instanz 1 ist.

Dies ist die Konfiguration für 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
!
!
```

Dies ist die Konfiguration auf 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
```

Der Name, die Revision und die Zuordnung von VLAN zu Instanz müssen auf allen Switches gleich sein.

Überprüfen Sie jetzt den Spanning Tree-Status auf 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 ist der Root für Instanz 0, sodass Router1 seinen Root-Port auf Gi0/0/0/1 zu Router3 hat. Router1 ist der Root für Instanz 1, also ist Router1 die designierte Bridge auf allen Schnittstellen für diese Instanz.

Router2 ist für Beispiel 0 auf Te0/1/0/0 blockiert:

```
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 leitet weiter, während Te0/1/0/0.3 blockiert ist. Wenn der STP Blocked-Wert 0x0 ist, ist die Bedingung false, sodass die Schnittstelle weitergeleitet wird. Wenn der STP Blocked-Wert 0x1 ist, ist die Bedingung true, sodass die Schnittstelle blockiert wird.

Verwenden Sie den Befehl **show uidb data**, um dies zu bestätigen und die Schnittstellendaten anzuzeigen, die im Netzwerkprozessor vorhanden sind:

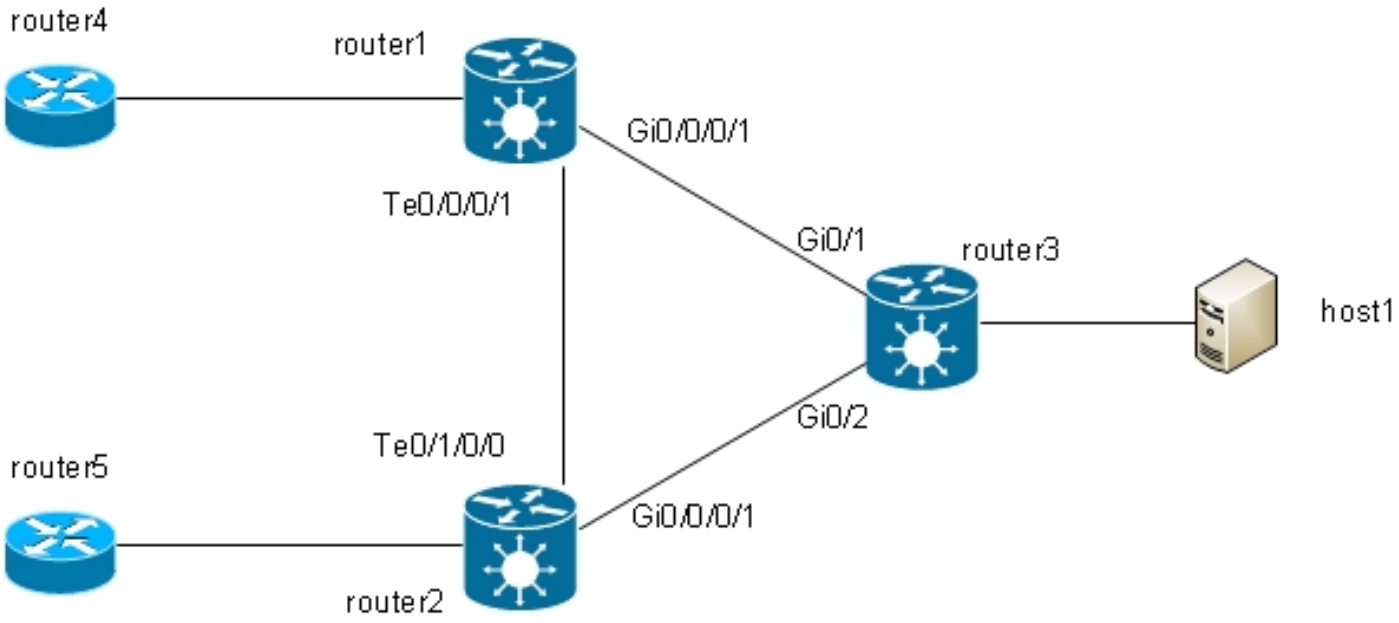
```
RP/0/RSP1/CPU0:router2#sh uidb data location 0/1/CPU0 TenGigE0/1/0/0.2
ingress | i Blocked
STP Blocked                       0x0
RP/0/RSP1/CPU0:router2#sh uidb data location 0/1/CPU0 TenGigE0/1/0/0.3
ingress | i Blocked
STP Blocked                       0x1
```

4,3 BVI

Durch die Konfiguration einer Bridge-Domäne wird eine L2-Domäne erstellt. Um diese L2-Domäne zu verlassen, verbinden Sie L3-Router, die zwischen Hosts innerhalb der Bridge-Domäne und der Außenwelt routen. Im vorherigen Diagramm könnte Host1 Router4 oder Router5 verwenden, um das lokale Subnetz zu verlassen und das Internet zu erreichen.

Router1 und Router2, bei denen die Bridge-Domänen konfiguriert sind, sind ASR 9000-Router, die IPv4- und IPv6-Datenverkehr weiterleiten können. Diese beiden Router könnten den IP-Datenverkehr aus der Bridge-Domäne herausnehmen und selbst an das Internet weiterleiten, anstatt sich auf L3-Router zu verlassen. Hierzu müssen Sie ein BVI konfigurieren. Hierbei handelt es sich um eine L3-Schnittstelle, die an eine Bridge-Domäne angeschlossen wird, um Pakete in die Bridge-Domäne ein- und aus dieser heraus weiterzuleiten.

So sieht es logisch aus:



Dies ist die Konfiguration:

```
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
!
```

Ein BVI ist eine nicht gekennzeichnete L3-Schnittstelle. Wenn das BVI die auf den ACs der Bridge-Domäne empfangenen Pakete verarbeiten soll, müssen die ACs so konfiguriert werden, dass alle eingehenden Tags angezeigt werden. Andernfalls kann die BVI den Tag nicht erkennen

und verwirft die Pakete. Es gibt keine Möglichkeit, eine dot1q-Subschnittstelle auf einem BVI zu konfigurieren, daher müssen die Tags auf den ACs eingepoppt werden, wie im vorherigen Beispiel bei Gi0/0/0/1.2 geschehen.

Da es sich bei einer BVI-Schnittstelle um eine virtuelle Schnittstelle handelt, gibt es einige Einschränkungen für die aktivierbaren Funktionen. Diese Einschränkungen werden unter Configuring Integrated Routing and Bridging auf dem Cisco Router der Serie ASR 9000: Restrictions for Configuring IRB (Konfigurieren von integriertem Routing und Bridging) dokumentiert. Die folgenden Funktionen werden von den BVI-Schnittstellen des ASR 9000 nicht unterstützt:

- Zugriffskontrolllisten (ACLs): L2-ACLs können jedoch auf jedem L2-Port der Bridge-Domäne konfiguriert werden.
- IP Fast Reroute (FRR)
- NetFlow
- MoFRR (nur Multicast Fast Re-Route)
- MPLS-Label-Switching
- mVPNv4
- Quality of Service (QoS)
- Datenverkehrsspiegelung
- Nicht nummerierte Schnittstelle für BVI
- Videoüberwachung (Vidmon)

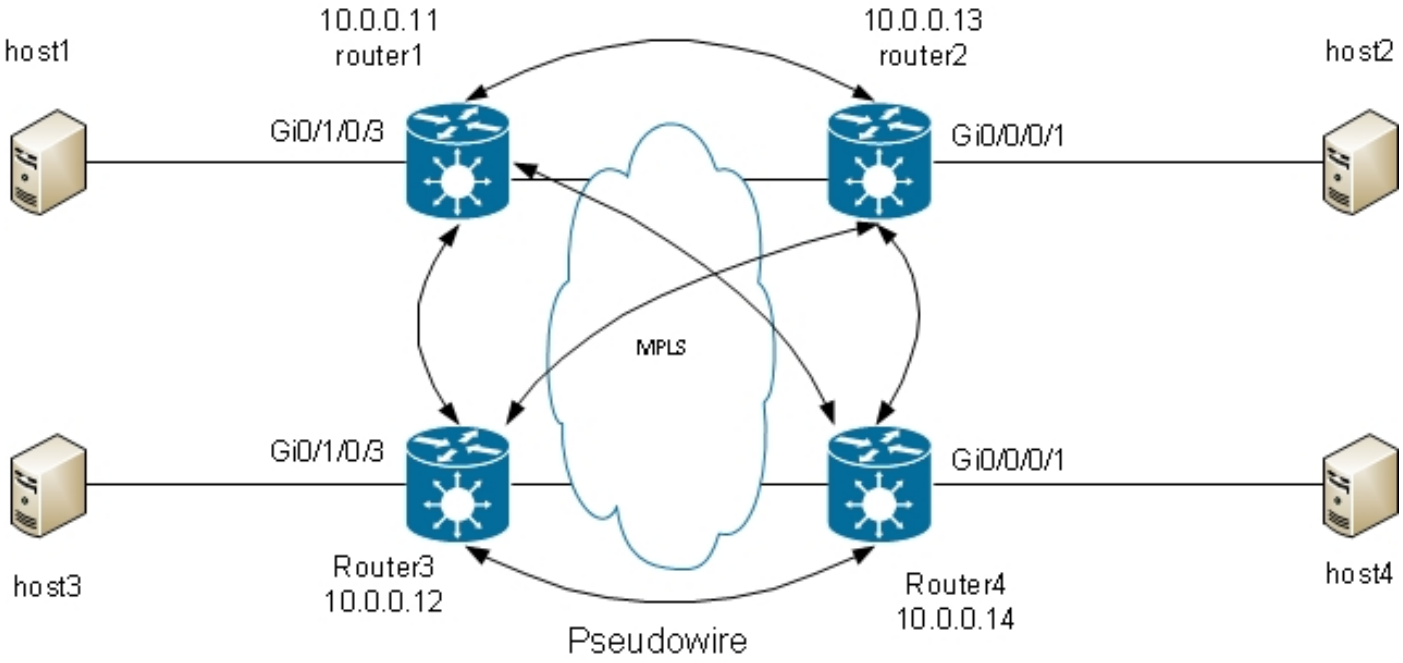
Die BVI kann in einer VRF-Konfiguration (Virtual Routing and Forwarding) konfiguriert werden, sodass der über die BVI empfangene Datenverkehr über MPLS weitergeleitet wird. Es muss jedoch ein *VRF-basierter Labelzuweisungsmodus* verwendet werden.

Wenn eine dieser eingeschränkten Funktionen erforderlich ist, können Sie kein BVI verwenden. Eine andere Lösung besteht darin, ein externes Loopback-Kabel zwischen zwei Ports des Routers zu verwenden, wobei sich ein Port in der Bridge-Domäne befindet und ein Port als normale geroutete Schnittstelle konfiguriert ist, in der alle Funktionen konfiguriert werden können.

4,4 VPLS

4.4.1 Übersicht

VPLS bietet die Möglichkeit, Bridge-Domains an mehreren Standorten über MPLS-PWs zu einer großen Bridge-Domain zu kombinieren. Die Hosts an den verschiedenen Standorten scheinen direkt mit demselben L2-Segment verbunden zu sein, da ihr Datenverkehr transparent über das vollständige Netz von MPLS-PWs zwischen L2VPN-PEs gekapselt wird:



Ein Full-Mesh aus PWs ist erforderlich, um sicherzustellen, dass jeder Host Datenverkehr von allen anderen Hosts empfangen kann. Dies hat zur Folge, dass ein L2VPN-PE einen auf einem VPLS-PW empfangenen Frame nicht über seine anderen VPLS-PWs weiterleitet. Es sollte ein Full-Mesh aus PWs geben, sodass jeder PE-Router den Datenverkehr direkt empfängt und ihn nicht zwischen PWs weiterleiten muss, da die Weiterleitung einen Loop verursachen würde. Dies wird als Split-Horizon-Regel bezeichnet.

Auf dem Router wird MAC Learning ausgeführt. Sobald eine MAC-Adresse in der MAC-Adresstabelle vorhanden ist, leiten Sie nur den Frame für diese MAC-Zieladresse über den PW an den L2VPN-PE weiter, von dem diese MAC-Adresse abgerufen wurde. Dadurch wird unnötiges Duplizieren von Datenverkehr im Core vermieden. Broadcasts und Multicasts werden über alle PWs verteilt, um sicherzustellen, dass alle Hosts sie empfangen können. Eine Funktion wie IGMP-Snooping ist nützlich, da sie das Senden von Multicast-Frames an PEs nur dann ermöglicht, wenn Empfänger oder Multicast-Router vorhanden sind. Dadurch wird der Datenverkehr im Core verringert, obwohl es immer noch mehrere Kopien derselben Pakete gibt, die an jeden PE gesendet werden müssen, wenn Interesse an dieser Gruppe besteht.

Das vollständige Mesh der PWs muss unter einer Virtual Forwarding Instance (VFI) konfiguriert werden:

```
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
!
!
!
!
!
```

Die unter der VFI konfigurierten PWs sind vollständig mit dem Core vermascht. Sie sind Teil derselben Split Horizon Group (SHG), um sicherzustellen, dass auf einem PW empfangene Frames nicht an einen anderen PW weitergeleitet werden.

Es ist möglich, Zugangs-PWs zu konfigurieren, die als Wechselstromtypen gelten und nicht unter der VFI konfiguriert sind. Weitere Informationen finden Sie im Abschnitt .

Die Konfiguration auf den Routern 2, 3 und 4 ist sehr ähnlich, und alle haben die anderen drei Router als Nachbarn unter der VFI.

```
RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain bd-name engineering detail
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 6
Filter MAC addresses:
Create time: 28/05/2013 17:17:03 (23:06:02 ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.2, state is upH-VPLS
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40003; interworking none
MAC learning: enabled
Flooding:
Broadcast & Multicast: enabled
Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
```

```
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 234039, sent 7824
bytes: received 16979396, sent 584608
Storm control drop counters:
packets: broadcast 0, multicast 0, unknown unicast 0
bytes: broadcast 0, multicast 0, unknown unicast 0
Dynamic ARP inspection drop counters:
packets: 0, bytes: 0
IP source guard drop counters:
packets: 0, bytes: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )
PW class not set, XC ID 0xc0000009
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ----------------------
Label 16049 16042
Group ID 0x5 0x1
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ----------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225481
Create time: 29/05/2013 15:36:17 (00:46:49 ago)
Last time status changed: 29/05/2013 15:57:36 (00:25:29 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 555, sent 285
bytes: received 36308, sent 23064
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.13, PW ID 2, state is up ( established )
PW class not set, XC ID 0xc000000a
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
```

```
PW backup disable delay 0 sec
Sequencing not set

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

PW Status TLV in use
MPLS Local Remote
------------ ------------------------------ ----------------------
Label 16051 289974
Group ID 0x5 0x6
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word disabled disabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x6 0x6
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
------------ ------------------------------ ----------------------
Incoming Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225483
Create time: 29/05/2013 15:36:17 (00:46:49 ago)
Last time status changed: 29/05/2013 16:02:38 (00:20:27 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 137
bytes: received 0, sent 12064
DHCPv4 snooping: disabled
```

```
IGMP Snooping profile: none
VFI Statistics:
drops: illegal VLAN 0, illegal length 0
```

Das lokale Label für den PW an 10.0.0.12 ist 16049, was bedeutet, dass Ethernet-Frames mit dem Label 16049 empfangen werden. Die Switching-Entscheidung basiert auf diesem MPLS-Label, da das IGP-Label im vorletzten MPLS-Hop hätte platziert werden müssen. Es kann weiterhin ein explizites Null-Label geben, aber die Switching-Entscheidung basiert auf dem 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
```

Der Befehl **show mpls forwarding labels** für das Label gibt die Bridge-Domain-Nummer an, die Sie verwenden können, um die MAC-Zieladresse und den PW (neighbor und pw-id) zu finden, an dem das Paket empfangen wurde. Anschließend können Sie Einträge in der MAC-Adresstabelle erstellen, die auf diesen Nachbarn zeigen:

```
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 und transportierte Tags

VPLS-PWs werden standardmäßig als Typ-5-PW (Ethernet) ausgehandelt. Alle Inhalte, die nach einer Änderung der VLAN-Tags (bei Konfiguration des **ReWrite-**Befehls) in den AC gelangen, werden über den PW gesendet.

Mit der Cisco IOS XR Software-Version 4.1.0 für die LDP-Signalisierung und Version 4.3.1 mit BGP können Sie eine PW-Klasse unter einem Nachbarn und **VLAN-Passthrough** für den **Transportmodus** unter der PW-Klasse konfigurieren. Hierbei wird ein VC-Typ-4-PW (Ethernet-VLAN) ausgehandelt, der alle Komponenten transportiert, die nach der Änderung der VLAN-Tags bei der Konfiguration des Befehls **rewrite** aus dem AC herauskommen.

Die VLAN-Tag-Manipulation auf dem EFP stellt sicher, dass mindestens ein VLAN-Tag auf dem Frame übrig ist, da Sie ein dot1q-Tag auf dem Frame benötigen, wenn VC-Typ-4-PWs vorhanden sind. Dem Frame wird kein Dummy-Tag 0 hinzugefügt, wenn Sie den **VLAN-Passthrough-**Modus für den **Transportmodus** verwenden.

Eine Kombination aus Typ-4- und Typ-5-PWs unter demselben VFI wird nicht unterstützt. Alle PWs müssen vom gleichen Typ sein.

```
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 Erkennung und Signalisierung

Die basierten auf der manuellen Konfiguration aller Nachbarn unter der VFI. Für die Signalisierung des PW mit dem Nachbarn wurde MPLS LDP verwendet.vorhergehende Beispiele

Wenn Sie dem Netzwerk einen neuen VPLS-PE hinzufügen, konfigurieren Sie den PE so, dass er über einen PW für alle vorhandenen PEs in jeder seiner lokalen Bridge-Domänen verfügt. Alle vorhandenen PEs müssen dann neu konfiguriert werden, damit sie über einen PW für den neuen PE verfügen, da alle PEs vollständig vernetzt sein müssen. Mit zunehmender Anzahl von PEs und Bridge-Domänen kann sich dies zu einer Herausforderung für den Betrieb entwickeln.

Eine Lösung besteht darin, dass PEs andere PEs automatisch über das BGP erkennen. IBGP benötigt zwar auch eine Full-Mesh-Funktion, kann jedoch mithilfe von Routen-Reflektoren deaktiviert werden. Ein neuer PE wird in der Regel so konfiguriert, dass er mit einer kleinen Anzahl von Routen-Reflektoren Peer hat, alle anderen PEs erhalten seine Updates, und der neue PE empfängt die Updates von den anderen PEs.

Um andere PEs über BGP zu erkennen, wird jeder PE für die *vpls-vpws-Adressfamilie* konfiguriert und gibt im BGP die Bridge-Domänen an, an denen er teilnehmen möchte. Sobald die anderen PEs erkannt werden, die Teil derselben Bridge-Domäne sind, wird für jeden von ihnen ein PW eingerichtet. BGP ist das Protokoll für diese automatische Erkennung.

Es gibt zwei Optionen für die Signalisierung des PW an die automatisch erkannten PEs: BGP und LDP. In diesen Beispielen konvertieren Sie die vorherige Topologie mit BGP-Signalisierung und LDP-Signalisierung in BGP Auto Discovery.

4.4.3.1 BGP Autodiscovery und BGP Signaling

Konfigurieren Sie die **Adressengruppe "l2vpn vpls-vpws"** unter "router bgp" und den Nachbarn, bei denen es sich um andere PEs oder die Routen-Reflektoren handelt:

```
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
!
```

Die neue Adressfamilie wird mit den Nachbarn aktiv, aber noch hat kein PE seine Teilnahme an einer Bridge-Domäne angekündigt:

```
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
```

Konfigurieren Sie **autodiscovery bgp** und **signaling-protocol bgp** im L2VPN bridge-domain-Konfigurationsmodus. Die Konfiguration auf Router1 ist wie folgt:

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

Die Konfiguration auf Router 2 ist wie folgt:

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

Die VPN-ID und das Route Target sind in den verschiedenen PEs für die einzelnen Bridge-Domänen identisch, aber jeder PE verfügt über eine eindeutige Virtual Edge Identifier (VE-ID). Jeder PE erkennt über BGP die anderen PEs im VPN und verwendet BGP, um die PWs zu signalisieren. Das Ergebnis ist eine vollständige Vernetzung der 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
```

Dies sind die von Router3 (10.0.0.13) angekündigten Präfixe (siehe Router1). Die Präfixe werden über die beiden Routen-Reflektoren 10.0.0.3 und 10.0.0.10 empfangen:

```
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 hat einige PWs eingerichtet:

```
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-Autodiscovery und LDP-Signalisierung

Die BGP-Konfiguration mit dem **address-family-**Befehl **l2vpn vpls-vpws** entspricht exakt der BGP-Signalisierung. Die L2VPN-Konfiguration wird geändert, um die LDP-Signalisierung mit dem Befehl **signaling-protocol ldp** zu verwenden.

Auf allen vier PEs wird die gleiche Konfiguration verwendet:

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

Die vpls-id besteht aus der BGP Autonomous System (AS)-Nummer und der vpn-id.

Drei Befehle von Router1 zeigen, dass die PWs mit den erkannten PEs eingerichtet wurden:

```
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 und -Entnahmen

Die Weiterleitung in VPLS basiert auf der MAC-Adresstabelle, die dynamisch erstellt wird, indem die Quell-MAC-Adressen der empfangenen Frames abgefragt werden. Wenn sich die Topologie in einer Bridge-Domäne ändert, ist ein Host möglicherweise über einen anderen AC- oder VPLS-Nachbarn erreichbar. Der Datenverkehr für diesen Host erreicht sein Ziel möglicherweise nicht, wenn Frames weiterhin gemäß der vorhandenen MAC-Adresstabelle weitergeleitet werden.

Für einen L2VPN-PE gibt es mehrere Möglichkeiten, eine Topologieänderung zu erkennen:

- Ein Port in der Bridge-Domäne wechselt nach oben oder unten.
- Ein Spanning Tree Topology Change Notification (TCN)-BPDU wird verarbeitet, wenn der L2VPN-PE die vollständige MST-Implementierung oder ein Spanning Tree Access Gateway-Protokoll ausführt. Die fehlerhafte Verbindung ist möglicherweise nicht lokal auf dem PE, aber in der Topologie möglicherweise weiter entfernt. Der PE fängt die TCN ab.

Wenn ein L2VPN-PE eine Topologieänderung erkennt, führt er zwei Schritte aus:

1. Der PE löscht die MAC-Adresstabelle der Bridge-Domänen, die von der Topologieänderung betroffen sind. Wenn der PE für PVSTAG oder Per-VLAN Rapid Spanning Tree Access Gateway (PVRSTAG) konfiguriert ist, wirkt sich eine in einer VLAN-Subschnittstelle erkannte TCN-BPDU auf alle VLANs und Bridge-Domänen auf dieser physischen Schnittstelle aus.
2. Der PE signalisiert den VPLS-Nachbarn über eine MPLS-LDP-MAC-Abbruchmeldung, dass sie ihre MAC-Adresstabelle leeren sollen. Alle Remote-L2VPN-PEs, die die LDP-Nachricht zur MAC-Abmeldung empfangen, leeren ihre MAC-Adresstabellen, und der Datenverkehr wird erneut geflutet. Die MAC-Adresstabellen werden basierend auf der neuen Topologie neu erstellt.

Das Standardverhalten der MAC-Abmeldung bei Port-Flap hat sich im Laufe der Zeit geändert:

- In der Cisco IOS XR-Software hat ein L2VPN-PE-Router üblicherweise MAC-Abmeldungsnachrichten gesendet, wenn die Stromversorgung unterbrochen wurde. Ziel war es, dass Remote-PEs ihre MAC-Adresstabellen für die betroffene Bridge-Domäne leeren, sodass die MAC-Adressen, die hinter dem heruntergefahrenen Port liegen, von einem anderen Port abgerufen werden.
- Dies führte jedoch zu einem Interoperabilitätsproblem mit einigen Remote-PEs, die RFC 4762 folgen und MAC-Adressen löschen, die auf alle PEs mit Ausnahme des PEs verweisen, der die MAC-Entzugsmeldung sendet. RFC 4762 geht davon aus, dass ein PE eine MAC-Abmeldung sendet, wenn eine Wechselstromquelle aktiviert wird, nicht jedoch, wenn eine Wechselstromquelle deaktiviert wird. Nach Version 4.2.1 der Cisco IOS XR-Software werden LDP-MAC-Abbruchmeldungen standardmäßig nur dann gesendet, wenn ein Bridge-Domain-Port aktiviert ist, um die RFC-Vorgaben zu erfüllen. Ein Konfigurationsbefehl wurde hinzugefügt, um zum alten Verhalten zurückzukehren.

Dies ist ein Befehl zum Anzeigen des Standardverhaltens nach Version 4.2.1 der Cisco IOS XR-Software:

```
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:
```

Die wichtige Zeile lautet "MAC Withdraw sent on bridge port down" (MAC-Zurücknahme bei deaktiviertem Bridge-Port gesendet), die nach Version 4.2.1 der Cisco IOS XR-Software jetzt standardmäßig deaktiviert ist. Der Befehl gibt außerdem die Anzahl der in der Bridge-Domäne gesendeten und empfangenen MAC-Abmeldungsnachrichten an. Eine hohe Anzahl von Entzugsmeldungen deutet auf Instabilität im Bridge-Bereich hin.

Dies ist die Konfiguration, die zum alten Verhalten zurückkehrt:

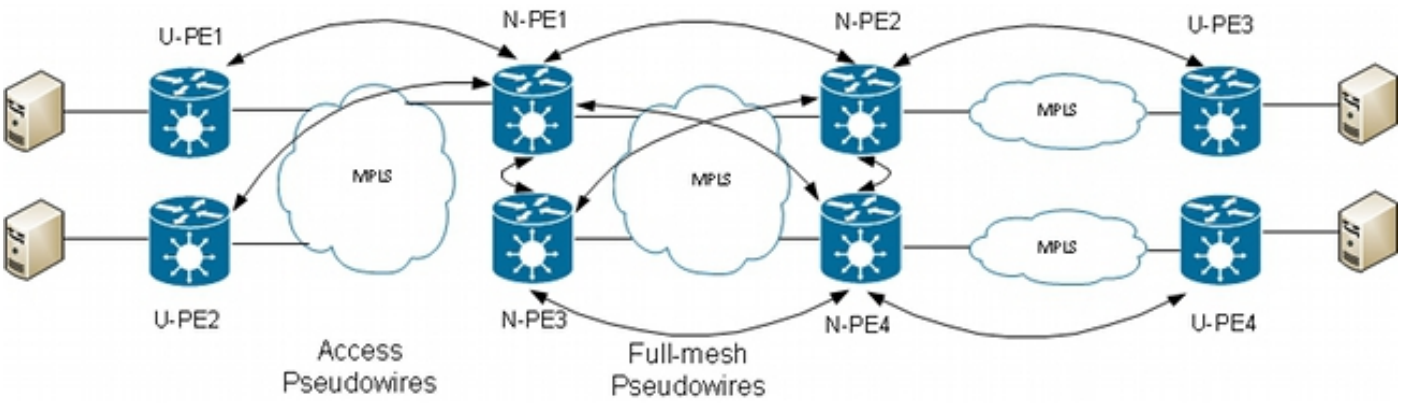
```
l2vpn
bridge group customer1
bridge-domain finance
mac
withdraw state-down
!
!
!
!
```

4.4.5 H-VPLS

VPLS erfordert ein Full-Mesh aus PWs zwischen L2VPN-PEs, um sicherzustellen, dass jeder PE in einem Hop einen Host hinter einem anderen PE erreichen kann, ohne dass ein PE Frames von einem PW zu einem anderen PW reflektieren muss. Dies ist die Grundlage für die Split-Horizon-Regel, die verhindert, dass ein PE Frames von einem PW an ein anderes PW weiterleitet. Selbst in Sonderfällen, in denen die MAC-Zieladresse in der MAC-Adresstabelle auf einen anderen PW zeigt, wird der Frame verworfen.

Ein Full-Mesh der PWs bedeutet, dass die Anzahl der PWs mit wachsender Zahl der PEs sehr hoch werden kann, was zu Problemen bei der Skalierbarkeit führen kann.

Mit einer PE-Hierarchie können Sie die Anzahl der PWs in dieser Topologie reduzieren:



Beachten Sie in dieser Topologie Folgendes:

- Ein Benutzer-PE-Gerät (Provider Edge) verfügt über Wechselstromverbindungen zu den CEs.
- Das U-PE-Gerät transportiert den CE-Datenverkehr über einen MPLS-Punkt-zu-Punkt-PW zu einem Netzwerk-Provider-Edge (N-PE).
- Der N-PE ist ein VPLS-Core-PE, der vollständig mit anderen N-PEs vernetzt ist.
- Auf dem N-PE-Router wird der PW vom U-PE-Router als Access-PW ähnlich wie ein Wechselstrom-Switch betrachtet. Der U-PE ist nicht Teil des Netzes mit den anderen N-PEs, daher kann der N-PE den Access-PW als Wechselstrom betrachten und Datenverkehr von diesem Access-PW an die Core-PWs weiterleiten, die Teil des VPLS Full Mesh sind.
- Die Core-PWs zwischen N-PEs werden unter einem VFI konfiguriert, um sicherzustellen, dass die Split-Horizon-Regel auf alle Core-PWs angewendet wird, die unter dem VFI konfiguriert sind.
- Access-PWs von U-PEs werden nicht unter einem VFI konfiguriert, daher gehören sie nicht zum gleichen SHG wie die VFI-PWs. Datenverkehr kann von einem Zugriffs-PW an einen VFI-PW weitergeleitet werden und umgekehrt.
- U-PEs können die PW-Redundanzfunktion verwenden, um einen primären PW zu einem primären N-PE und einen Standby-PW zu einem Standby-N-PE zu erhalten. Der Standby-Modus übernimmt, wenn der primäre PW ausfällt.

Dies ist ein Beispiel, in dem U-PE1 (10.0.0.15) mit PW-Redundanz für N-PE1 (10.0.0.11) und N-PE2 (10.0.0.12) konfiguriert ist:

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

Der PW zu 10.0.0.12 befindet sich im Standby-Zustand. Auf N-PE1 gibt es einen Zugangs-PW zu 10.0.0.15 und einen AC, die sich nicht unter dem VFI befinden.

N-PE1 erfasst einige MAC-Adressen über den Zugangs-PW und die VFI-PWs:

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

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
------------------------------------------------------------------------------
6c9c.ed3e.e46d dynamic (10.0.0.15, 15) 0/0/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A
0024.985e.6a42 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A
001d.4603.1f42 dynamic (10.0.0.13, 2) 0/0/CPU0 0d 0h 0m 0s N/A
```

Auf N-PE2 (10.0.0.12) befindet sich der Zugangs-PW im Standby-Zustand:

```
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 Split Horizon Groups (SHGs)

Die Split-Horizon-Regel legt fest, dass ein auf einem VFI PW empfangener Frame nicht über einen anderen VFI PW weitergeleitet werden kann. VFI-N-PEs müssen vollständig vernetzt sein.

Dieser Split-Horizon wird durch ein SHG durchgesetzt:

- Mitglieder einer SHG können Frames nicht untereinander, sondern an Mitglieder anderer SHGs weiterleiten.
- Alle VFI-PWs werden standardmäßig SHG 1 zugewiesen. Dadurch wird sichergestellt, dass keine Weiterleitung zwischen VFI-PWs erfolgt, sodass die Split-Horizon-Regel durchgesetzt wird. Pakete, die über einen VFI-PW empfangen werden, können an ACs weitergeleitet werden und auf PWs zugreifen, da sie nicht Teil derselben SHG sind.
- Alle ACs und Zugangs-PWs sind standardmäßig nicht Teil einer SHG-Gruppe, d. h., dass Pakete, die auf einem AC oder Zugangs-PW empfangen werden, an einen anderen AC oder Zugangs-PW in derselben Bridge-Domäne weitergeleitet werden können.
- ACs und Zugangs-PWs können dem SHG 2 mit dem **Split-Horizon-**Gruppenbefehl zugewiesen werden, wenn das Ziel darin besteht, eine Weiterleitung zwischen ihnen zu verhindern.

```
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
!
```

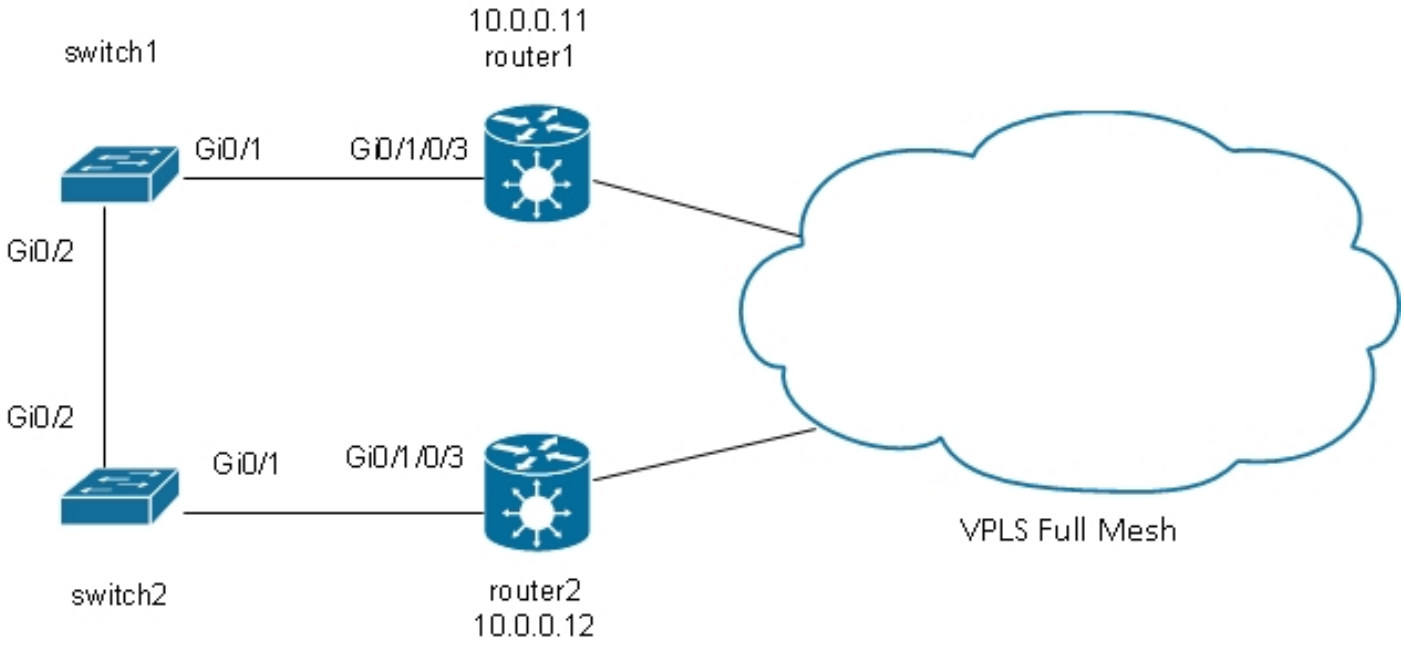
```
interface GigabitEthernet0/1/0/3.2
split-horizon group
!
neighbor 10.0.0.15 pw-id 15
split-horizon group
!
vfi customer1-engineering
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!
```

In dieser Konfiguration findet keine Weiterleitung zwischen Gi 0/0/0/1.2 und Gi 0/1/0/3.2, Gi 0/0/0/1.2 und 10.0.0.15 oder Gi 0/1/0/3.2 und 10.0.0.15 statt. Zwischen den ACs und den VFI-PWs kann jedoch weiterhin Datenverkehr weitergeleitet werden, da sie Teil verschiedener SHGs (1 und 2) sind.

```
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 Redundanz

Um Redundanz zu gewährleisten, kann ein doppelt mit der VPLS-Domäne verbundener Standort vorhanden sein:



Wenn ein mit Switch1 verbundener Host einen Broadcast sendet, leitet Switch1 diesen an Router1 und an Switch2 weiter. Router1 verfügt über ein vollständiges Mesh aus PWs. Daher ist ein PW für Router2 vorhanden, und Router1 leitet den Broadcast über diesen PW weiter. Router2 leitet den Broadcast an Switch2 weiter, der ihn an Switch1 weiterleitet. Daraus ergibt sich eine physikalische Schleife.

4.4.7.1 Spanning Tree

Die vollständige MST-Implementierung funktioniert nicht mit VPLS, da diese Implementierung MST-BPDUs an eine Hauptschnittstelle sendet, um den Weiterleitungsstatus aller VLANs an dieser Schnittstelle zu steuern. Bei VPLS gibt es VFIs für jede Bridge-Domäne. Daher können Sie für alle VFIs keine BPDUs an eine Hauptschnittstelle senden.

Spanning-Tree-BPDUs werden standardmäßig über VPLS und Point-to-Point-PWs übertragen.

Wenn Switch1 und Switch2 Pro-VLAN-BPDUs oder nicht gekennzeichnete MST-BPDUs senden und wenn die BPDUs mit den l2transport-Subschnittstellen auf Router1 und Router2 übereinstimmen, werden die BPDUs über VPLS übertragen. Die Switches sehen die BPDUs der anderen auf den Gi 0/1-Schnittstellen, und Spanning Tree unterbricht die Schleife und blockiert einen Port.

Switch2 ist der Root für 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)
```

Switch1 hat seinen Root-Port an Gi 0/1 und blockiert 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
```

Das Problem besteht darin, dass die BPDUs auch an Remote-Standorte übertragen werden und sich die Spanning-Tree-Instabilität an einem Standort auf alle mit der VPLS-Domäne verbundenen Standorte ausweitet. Es ist sicherer, jeden Standort zu isolieren und BPDUs nicht über VPLS zu transportieren.

Eine Lösung ist die Verwendung einer Access Gateway-Version des STP. Dies ist eine begrenzte Implementierung des Protokolls, bei der die L2VPN-PEs so konfiguriert sind, dass sie einige statische BPDUs senden, damit sie mit dem Spanning-Tree-Root verbunden erscheinen. Der L2VPN-PE transportiert die von den CEs empfangenen BPDUs nicht zu den Remote-Standorten, sodass jeder Standort über eine eigene Spanning-Tree-Domäne verfügt.

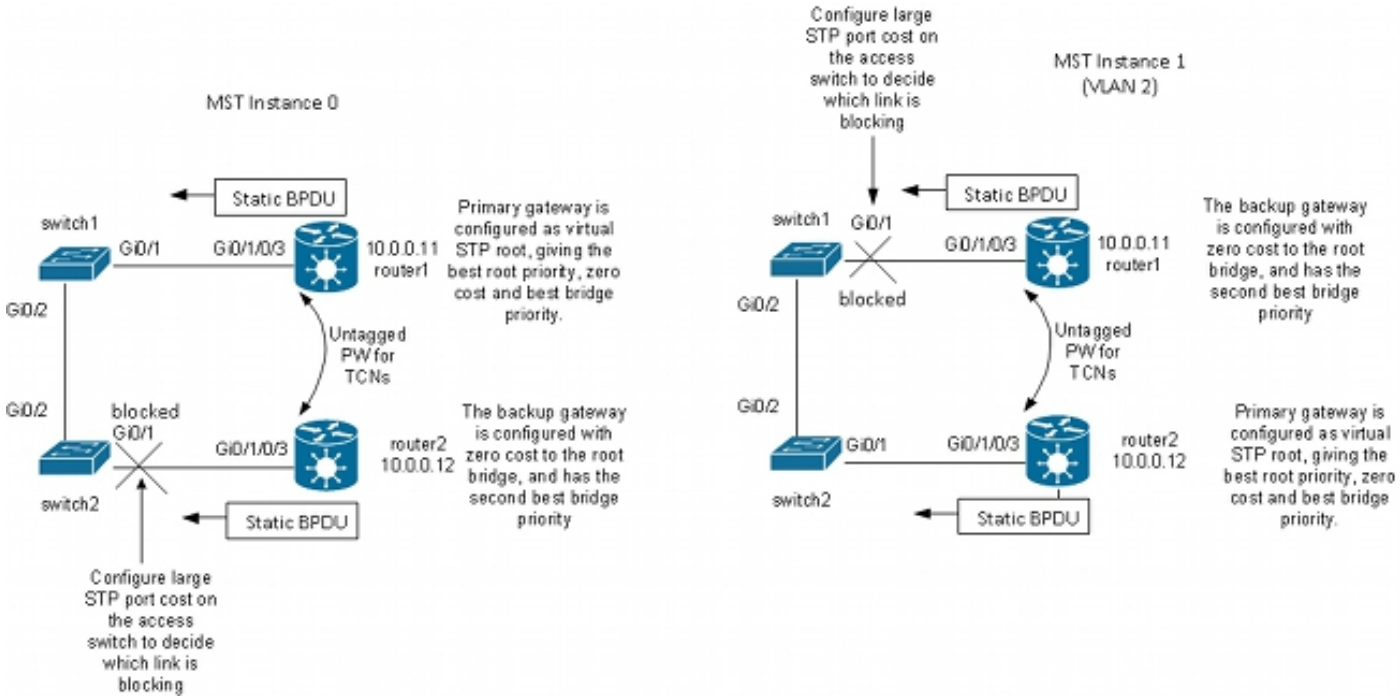
4.4.7.2 MSTAG

Wie im Abschnitt Spanning Tree erläutert, sendet MST nicht markierte BPDUs, diese BPDUs steuern jedoch den Weiterleitungsstatus aller VLANs an der Schnittstelle.

VLANs können in mehrere Instanzen gruppiert werden, und jede Instanz verfügt über einen eigenen Weiterleitungsstatus.

VLANs werden in der Regel so gruppiert, dass der Datenverkehr gleichmäßig über mehrere Pfade verteilt werden kann. Wenn zwei Pfade vorhanden sind, gehört die Hälfte des Datenverkehrs zu einer Instanz, die den ersten Pfad weiterleitet und den zweiten Pfad blockiert. Die andere Hälfte des Datenverkehrs gehört zu einer Instanz, die den ersten Pfad blockiert und den Datenverkehr über den zweiten Pfad weiterleitet. Dies ermöglicht einen Lastausgleich zwischen den beiden Pfaden unter stabilen Bedingungen. Andernfalls haben Sie einen Pfad, der normalerweise vollständig blockiert ist und nur dann aktiv wird, wenn der primäre Pfad nicht verfügbar ist.

Nachfolgend finden Sie eine typische MSTAG-Topologie:



In diesem Beispiel hat Instanz 1 VLAN 2 und Instanz 0 die anderen VLANs. (In einem realistischeren Szenario werden VLANs auf mehrere Instanzen aufgeteilt, um ein gutes Load Balancing des Datenverkehrs zwischen den Instanzen zu erreichen.) Da einige VLANs viel mehr Datenverkehr haben als andere, gibt es nicht immer dieselbe Anzahl von VLANs in jeder Instanz.

Dies ist die Konfiguration für MST-Instanz 0:

- Router1 und Router2 senden einige statische BPDUs, basierend auf der MSTAG-Konfiguration. Die eingehenden BPDUs aus dem Netzwerk werden nicht verarbeitet, und es wird nicht versucht, eine vollständige Implementierung durchzuführen. Mit MSTAG senden die beiden L2VPN-PEs lediglich statische BPDUs, basierend auf ihrer MSTAG-Konfiguration.
- Router1 wird so konfiguriert, dass er Datenverkehr von Instanz 0 anzieht, indem er als Root für diese Instanz angezeigt wird.
- Router2 wird mit der zweitbesten Root-Priorität für Instanz 0 konfiguriert, sodass sie bei einem Ausfall von Router1 oder bei einem Ausfall der Wechselspannung zwischen Switch1 und Router1 zur neuen Root wird.
- Switch2 wird mit hohen Spanning Tree-Kosten auf dem Port Gi 0/1 zu Router2 konfiguriert, um sicherzustellen, dass sein primärer Pfad zum Root auf Gig 0/2 über Switch1 und Router1 verläuft.
- Switch2 wählt Gi 0/2 als Root-Port für Instance0 und Gi 0/1 als alternativen Port für den Fall, dass der Root verloren geht.
- Der Datenverkehr von diesem Standort in den VLANs, die zu Instanz 0 gehören, gelangt daher über VPLS über Router1 zu anderen Standorten.

Für MST-Instanz 1 (VLAN 2) wird die Konfiguration umgekehrt:

- Router2 wird so konfiguriert, dass er Datenverkehr von Instanz 1 anzieht, indem er als Root für diese Instanz angezeigt wird.
- Router1 wird mit der zweitbesten Root-Priorität für Instanz 1 konfiguriert, sodass er bei einem Ausfall von Router2 oder bei einem Ausfall der Wechselspannung zwischen Switch2 und Router2 zur neuen Root wird.

- Switch1 wird mit hohen Spanning Tree-Kosten auf dem Port Gi 0/1 zu Router1 konfiguriert, um sicherzustellen, dass sein primärer Pfad zum Root auf Gig 0/2 über Switch2 und Router2 verläuft.
- Switch1 wählt Gi 0/2 als Root-Port für Instanz 1 und Gi 0/1 als alternativen Port für den Fall, dass der Root verloren geht.
- Der Datenverkehr von diesem Standort in den VLANs, die zu Instanz 1 (in diesem Beispiel VLAN 2) gehören, gelangt daher über Router2 über VPLS zu anderen Standorten.
- Es muss eine Subschnittstelle auf Router1 und Router2 vorhanden sein, damit die nicht gekennzeichneten TCNs abgefangen und über einen Point-to-Point-PW an den anderen Router weitergeleitet werden können. Da die direkten Verbindungen zwischen Switch1 und Switch2 verloren gehen und die Verbindungen voneinander isoliert werden können, müssen Router1 und Router2 die TCNs zwischen ihnen über diesen Punkt-zu-Punkt-PW weiterleiten.
- Die PEs fangen auch die TCNs ab, leeren ihre MAC-Adresstabellen und senden die LDP-MAC-Abmeldung an die Remote-PEs.

Dies ist die Konfiguration auf 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
```

Beachten Sie bei dieser Konfiguration Folgendes:

- In MST-Instanz 0 ist die Root-Bridge 0000.0000.0001, was der Bridge-ID von Router1 entspricht.
- In MST-Instanz 1 ist die Root-Bridge 0000.0000.0002, was der Bridge-ID von router2 entspricht.
- Die Bridge-Priorität von Router1 ist 4096 in Instanz 0 (wird zum Root) und 8192 in Instanz 1 (wird zum zweitbesten Root).
- Die Bridge-Priorität von Router1 ist 8192 in Instanz 0 (wird zweitbester Root) und 4096 in Instanz 1 (wird Root).
- Über die Punkt-zu-Punkt-Verbindung auf GigabitEthernet0/1/0/3.1 werden die nicht gekennzeichneten MST-TCNs an den anderen Router übertragen.

Für die dot1q-Subschnittstellen wurde eine Ausgangs-ACL konfiguriert, um VLAN-spezifische BPDUs zu verwerfen, die möglicherweise von einem anderen Standort gesendet werden, der noch nicht zum MST migriert wurde. Diese Konfiguration verhindert, dass der CE-Switch die Schnittstelle als inkonsistent deklariert, wenn er eine Per-VLAN-BPDU auf einer für MST konfigurierten Schnittstelle empfängt.

Die Konfiguration auf Router 2 ist sehr ähnlich:

```
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
```

Dies ist die Basiskonfiguration für 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
```

Daher wird der Datenverkehr in Instanz 0 über Router1 und der Datenverkehr in Instanz 1 über Switch2 und Router2 weitergeleitet.

Für die Konfiguration auf Switch2 werden die gleichen Befehle wie für Switch1 verwendet:

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

switch2#sh spanning-tree

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

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

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



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

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

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

Switch2 durchläuft Switch1 und Router1 für Instanz0 und Router2 für Instanz1.

Für den Datenverkehr wird ein Lastenausgleich durchgeführt, da eine Instanz den Standort über Router1 und die andere Instanz den Standort über Router2 verlässt.

Wenn die Verbindung zwischen Router1 und Switch1 unterbrochen ist, durchlaufen beide Instanzen 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)
```

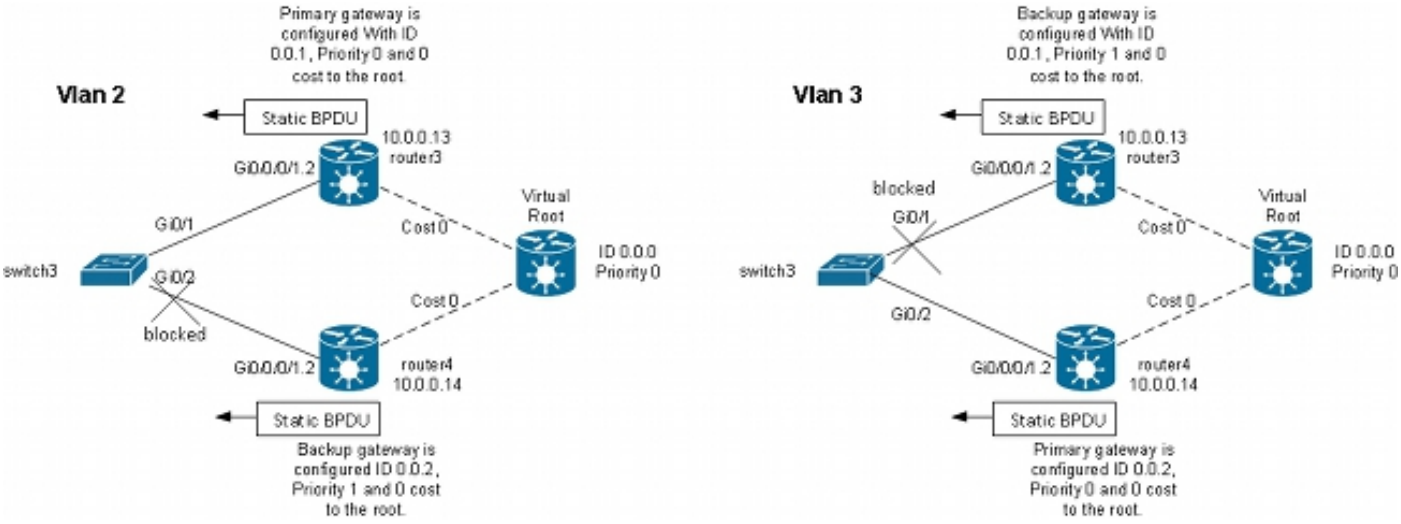
```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

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
```

Bei diesem Fehlertyp kann eine schnelle Konvergenz erreicht werden, da der Pfad durch den zweitbesten Stamm bereits als alternativer Pfad ausgewählt wurde. Bei MSTAG werden MST-BPDUs nicht über VPLS transportiert, sodass Standorte von der Instabilität an anderen Standorten isoliert werden.

4.4.7.3 PVSTAG oder PVRSTAG

MSTAG ist das bevorzugte Zugriffs-Gateway-Protokoll für VPLS, da es den schnellen Spanning Tree verwendet und skalierbar ist, da Instanzen anstelle von BPDUs in jedem VLAN verwendet werden.

Wenn ein Standort nicht auf MST migriert werden kann und die einzige Lösung darin besteht, weiterhin PVST+ oder PVRST auszuführen, können Sie PVSTAG oder PVRSTAG verwenden. Die Implementierung ist jedoch auf eine bestimmte Topologie beschränkt:



Die wichtigste Einschränkung bei dieser Topologie ist, dass es nur einen CE-Switch geben kann. Es können nicht zwei Switches wie in der MSTAG-Topologie verwendet werden. In MSTAG können Sie einen Punkt-zu-Punkt-PW konfigurieren, um den nicht gekennzeichneten Datenverkehr (einschließlich der BPDU-TCNs) von einem PE zum anderen zu transportieren, wenn der Standort in zwei Teile aufgeteilt wird. Mit PVST und PVRST werden die TCNs mit Tags gesendet, sodass sie derselben Subschnittstelle entsprechen wie der Datenverkehr, der über VPLS transportiert wird. Der Router muss die BPDUs anhand der MAC-Adresse und des Protokolltyps identifizieren, um die TCNs an die andere Seite weiterzuleiten. Da dies derzeit nicht unterstützt wird, ist nur ein CE-Gerät erforderlich.

Eine weitere Anforderung in früheren Versionen als Cisco IOS XR Software Version 4.3.0 ist, dass Paketschnittstellen nicht als ACs verwendet werden können. Diese Einschränkung wurde in Version 4.3.0 der Cisco IOS XR-Software aufgehoben.

Das Prinzip ist das gleiche wie bei MSTAG. Der PVSTAG-Router sendet statische BPDUs, sodass der CE mit Switches verbunden zu sein scheint, die direkt mit dem (virtuellen) Root verbunden sind, wobei die Kosten 0 betragen. Um einen Lastausgleich für den Datenverkehr zu erreichen, können einige VLANs mit dem Root auf Router3 und andere mit dem Root auf Router4 konfiguriert werden.

Dies ist ein Konfigurationsbeispiel für Router 3:

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

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

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

```
root-cost 0
priority 1
bridge-id 0000.0000.0001
!
!
!

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

Dies ist ein Konfigurationsbeispiel für Router 4:

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

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

```
neighbor 10.0.0.13 pw-id 3
!
!
!
bridge-domain engineering
interface GigabitEthernet0/0/0/1.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
!
!
!
!

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

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

```
Bridge ID: 0000.0000.0002
Port Priority: 128
Port ID 1
Hello Time: 2
Active: Yes
BPDUs sent: 202799
Topology Changes: 0
```

Dies ist ein Konfigurationsbeispiel für den CE-Switch3:

```
switch3#sh spanning-tree vlan 2

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

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

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

switch3#sh spanning-tree vlan 3

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

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

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

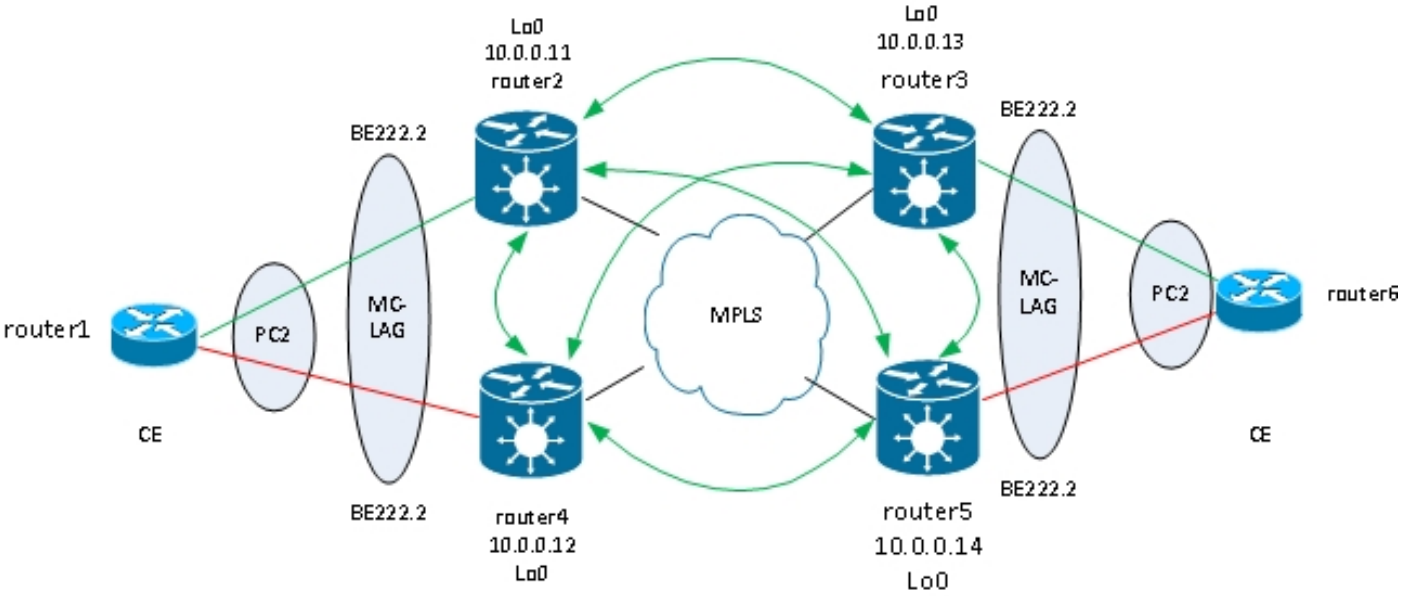
Die Konfiguration für PVSTAG ähnelt stark dem MSTAG, mit der Ausnahme, dass die Root-Priorität und die Priorität des primären Gateways als 4096 und die Priorität des Backup-Gateways im MSTAG-Beispiel als 8192 konfiguriert sind.

Alle anderen Switches in den Domänen sollten höhere Prioritäten als die in PVSTAG oder PVRSTAG konfigurierten haben.

Sie können die Schnittstellenkosten auf den CE-Switches anpassen, um zu beeinflussen, welcher Port zum Root-Port wird und welcher Port blockiert wird.

4.4.7.4 MC-LAG

Die MC-LAG-Konfiguration mit VPLS ist einfacher als Point-to-Point-PWs mit bidirektionaler PW-Redundanz. Anstelle von einem primären PW und drei Standby-PWs benötigen die PEs nur ein Full-Mesh-VPLS-PWs, was bei VPLS standardmäßig der Fall ist:



Beachten Sie in dieser Topologie Folgendes:

- Die MC-LAG wird zwischen den beiden VPLS-PEs auf der linken Seite ausgeführt: Router2 und Router4.
- Unter normalen Bedingungen sind die Paketmitglieder zwischen Router1 und Router2 und im Standby-Zustand zwischen Router1 und Router4 aktiv.
- Router2 hat die Paket-Subschnittstellen, die unter VPLS Bridge-Domains konfiguriert sind, sodass Router2 den Datenverkehr an Remote-VPLS-PEs weiterleitet. Im Topologiediagramm sind zwei Standorte abgebildet. Es können jedoch noch viele weitere Standorte hinzukommen.
- Die Remote-PEs beziehen die MAC-Adressen von Router1 und den Geräten hinter Router2, sodass die PEs den Datenverkehr für diese Ziel-MAC-Adressen über Router2 weiterleiten.
- Wenn die Verbindung zwischen Router1 und Router2 ausfällt oder Router2 ausfällt, wird das Paketmitglied zwischen Router1 und Router4 aktiviert.
- Wie bei Router 2 sind die Subschnittstellen des Routers 4 unter VPLS-Bridge-Domains konfiguriert.
- Wenn die Paket-Subschnittstellen auf Router4 verfügbar sind, sendet Router4 LDP-MAC-Abmeldungsnachrichten an die Remote-VPLS-PEs, um sie über eine Topologieänderung zu informieren.

Dies ist die Konfiguration auf Router3:

```
RP/0/RSP1/CPU0:router3#sh run redundancy
redundancy
iccp
group 2
mlacp node 1
mlacp system mac 0200.0000.0002
```

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

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

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

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

```
!
!
```

Sobald das MC-LAG-Paket konfiguriert ist, fügen Sie es wie jedes andere AC unter der VPLS-Konfiguration hinzu.

Dies ist die entsprechende Konfiguration auf Router5:

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

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

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

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

```
!
!
!
bridge-domain engineering
interface Bundle-Ether222.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
!
!
!
!
```

Unter normalen Umständen ist das Bündelelement zwischen Router3 und Router6 aktiv, und das Element zwischen Router5 und Router6 befindet sich im Standby-Zustand:

```
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#
```

Datenverkehr vom CE wird auf Router3 empfangen und an Remote-PEs weitergeleitet:

```
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
```

Der letzte Befehl zeigt an, dass Router3 einige MAC-Adressen in seinem Paket erfasst und die aktiven Mitglieder in Router3. Bei Router5 wird keine MAC-Adresse über das Paket abgefragt, da sich das lokale Mitglied im Standby-Status befindet:

```
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
```

Wenn das Paketmitglied zwischen Router3 und Router6 ausfällt, wird es auf Router5 aktiviert. Die MC-LAG-VPLS-PEs senden eine LDP-MAC-Abmeldung, sodass Remote-PEs ihre MAC-Adresstabellen löschen und die MAC-Adresse über den neuen aktiven MC-LAG-PE-Router 5 abrufen können.

Router2 erhält eine MAC-Abmeldung von Router3 und Router5, wenn das aktive MC-LAG-Paketmitglied von Router3 zu Router5 wechselt:

```
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
```

Die MAC-Adressen auf Router2 werden von Router3 (10.0.0.13) zu Router5 (10.0.0.14) verschoben:

```
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
```

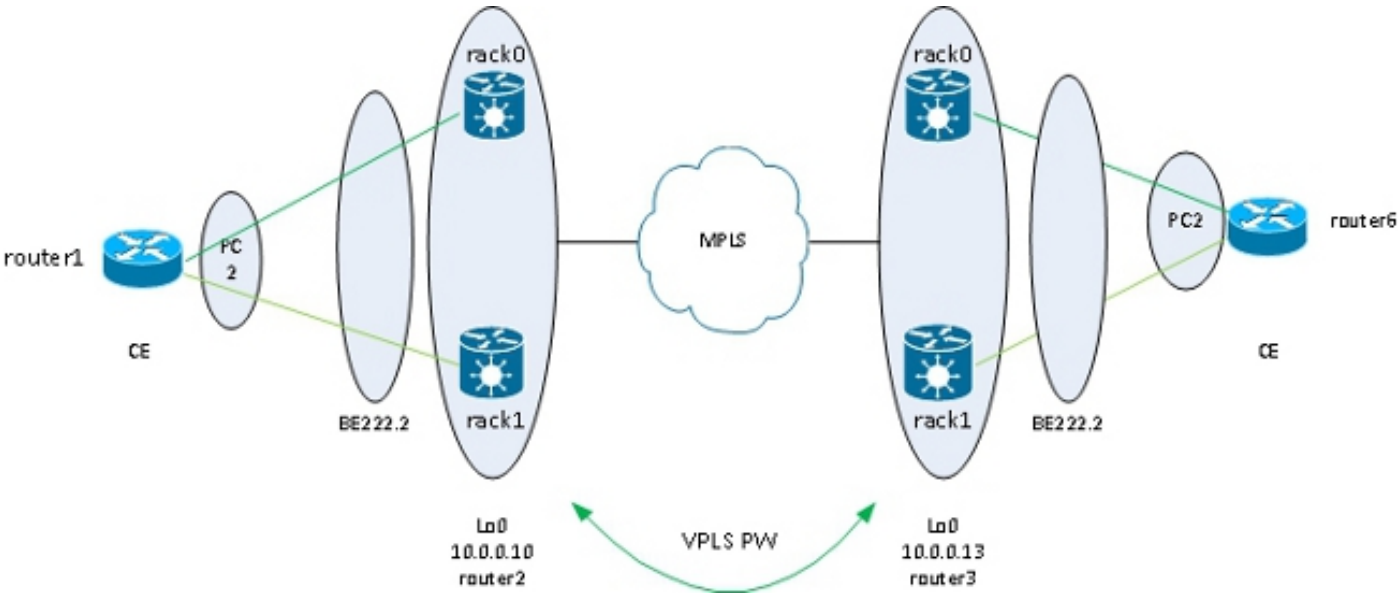
Mit der MC-LAG kann ein Standort ein einzelnes Paket nutzen, das über VPLS mit den anderen Standorten verbunden wird. MC-LAG bietet die Redundanz von Verbindungen und PE, ist jedoch logischerweise immer noch eine Paketschnittstelle, um andere Standorte zu erreichen. Spanning Tree ist für dieses Paket nicht erforderlich, und auf dem CE könnte ein BPDU-Filter konfiguriert werden, um sicherzustellen, dass BPDUs nicht zwischen Standorten über VPLS ausgetauscht werden.

Eine weitere Option ist die Konfiguration einer Ethernet-Services-Zugriffsliste auf den ACs des Pakets, um die Ziel-MAC-Adressen der BPDUs zu löschen, sodass die BPDUs nicht zwischen Standorten übertragen werden. Wenn jedoch eine Backdoor-Verbindung zwischen den Standorten eingeführt wird, kann Spanning Tree die Schleife nicht unterbrechen, da sie nicht auf dem MC-LAG-Paket ausgeführt wird. Prüfen Sie daher sorgfältig, ob Spanning Tree im MC-LAG-Paket deaktiviert werden soll. Wenn die Topologie zwischen den Standorten sorgfältig gepflegt wird, ist eine Redundanz über die MC-LAG ohne Spanning Tree möglich.

4.4.7.5 ASR 9000 nV Edge-Cluster

Die MC-LAG-Lösung bot Redundanz, ohne dass Spanning Tree verwendet werden musste. Ein Nachteil ist, dass sich die Paketmitglieder eines MC-LAG PE im Standby-Zustand befinden, sodass es sich um eine Aktiv/Standby-Lösung handelt, die die Verbindungsnutzung nicht maximiert.

Eine weitere Designoption ist die Verwendung eines ASR 9000 nV Edge-Clusters, sodass CEs Paketmitglieder zu jedem Cluster-Rack haben können, die alle gleichzeitig aktiv sind:



Ein weiterer Vorteil dieser Lösung besteht darin, dass die Anzahl der PWs reduziert wird, da es für jeden Cluster an jedem Standort nur eine PW pro Cluster gibt. Wenn es zwei PEs pro Standort gibt, muss jeder PE über einen PW für jeden der beiden PEs an jedem Standort verfügen.

Die einfache Konfiguration ist ein weiterer Vorteil. Die Konfiguration ähnelt einer sehr einfachen VPLS-Konfiguration mit einer Bridge-Domäne mit Paket-ACs und VFI-PWs:

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

Bundle-Ether222
```

```
Status: Up
Local links : 2 / 0 / 2
Local bandwidth : 20000000 (20000000) kbps
MAC address (source): 0024.f71e.d309 (Configured)
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
Maximum active links: 64
Wait while timer: 2000 ms
Load balancing: Default
LACP: Not operational
Flap suppression timer: Off
Cisco extensions: Disabled
mLACP: Not configured
IPv4 BFD: Not configured

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

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

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

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

```
!
!
!

RP/1/RSP0/CPU0:router2#sh l2vpn bridge-domain group customer1
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 4 (4 up), PBBs: 0 (0 up)
List of ACs:
BE222.3, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-finance (up)
Neighbor 10.0.0.11 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.12 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 3, state: up, Static MAC addresses: 0
Bridge group: customer1, bridge-domain: engineering, id: 4, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 4 (4 up), PBBs: 0 (0 up)
List of ACs:
BE222.2, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.11 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0
```

Die Redundanz wird durch das AC-Paket bereitgestellt, das dual-homed mit den beiden Racks ist, sodass das Paket bei einem Ausfall der Paketmitglieder oder des Racks verfügbar bleibt.

Wenn ein Standort nur über einen Cluster mit der VPLS-Domäne verbunden ist, ähnelt die Topologie in Bezug auf Spanning Tree der MC-LAG. Spanning Tree ist für dieses Paket nicht erforderlich, und ein BPDU-Filter könnte auf dem CE konfiguriert werden, um sicherzustellen, dass BPDUs nicht zwischen Standorten über VPLS ausgetauscht werden.

Eine weitere Option ist die Konfiguration einer Ethernet-Services-Zugriffsliste auf den ACs des Pakets, um die Ziel-MAC-Adressen der BPDUs zu löschen, sodass die BPDUs nicht zwischen Standorten übertragen werden. Wenn jedoch eine Backdoor-Verbindung zwischen den Standorten eingeführt wird, kann Spanning Tree die Schleife nicht unterbrechen, da sie nicht auf dem CE-PE-Bündel ausgeführt wird. Prüfen Sie daher sorgfältig, ob Spanning Tree für dieses CE-PE-Paket deaktiviert werden soll. Wenn die Topologie zwischen den Standorten sorgfältig gepflegt wird, ist eine Redundanz über den Cluster ohne Spanning Tree sinnvoll.

4.4.7.6 ICCP-Based Service Multi-Homing (ICCP-SM) (PMCLAG (Pseudo MCLAG) und Active/Active)

In Version 4.3.1 wurde eine neue Funktion eingeführt, um die Einschränkungen der MC-LAG zu umgehen, bei der einige Paketverbindungen nicht verwendet werden, da sie im Standby-Modus verbleiben. Bei der neuen Funktion *Pseudo-MCLAG* werden alle Verbindungen vom DHD zu den Points of Attachments (PoAs) verwendet. Die VLANs sind jedoch auf die verschiedenen Pakete verteilt:

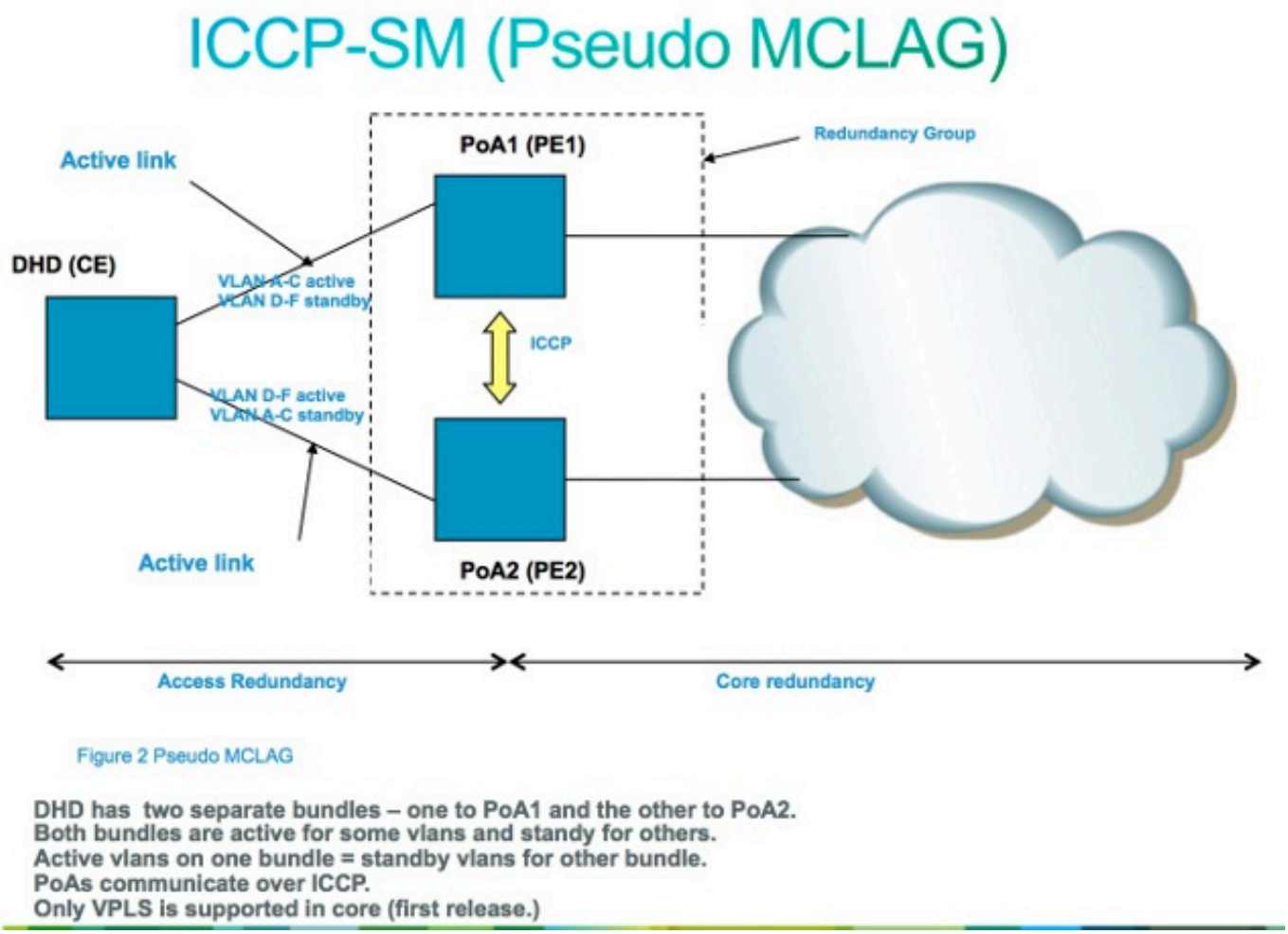


Figure 2 Pseudo MCLAG

4.5 Traffic Storm Control

In einer L2-Broadcast-Domäne besteht das Risiko, dass sich ein Host falsch verhält und eine hohe Rate von Broadcast- oder Multicast-Frames sendet, die überall in der Bridge-Domäne übertragen werden müssen. Ein weiteres Risiko besteht in der Schaffung einer L2-Schleife (die nicht durch Spanning Tree unterbrochen wird), was zu Schleifen bei Broadcast- und Multicast-Paketen führt. Eine hohe Rate von Broadcast- und Multicast-Paketen beeinträchtigt die Leistung der Hosts in den Broadcast-Domänen.

Die Leistung der Switching-Geräte im Netzwerk kann auch durch die Replikation eines Eingangs-Frames (Broadcast, Multicast oder ein unbekannter Unicast-Frame) auf mehrere Ausgangs-Ports in der Bridge-Domäne beeinträchtigt werden. Das Erstellen mehrerer Kopien desselben Pakets kann ressourcenintensiv sein, je nachdem, wo im Gerät das Paket repliziert werden muss. So stellt beispielsweise die Replikation eines Broadcasts auf mehrere verschiedene Slots aufgrund der Multicast-Replikationsfunktionen der Fabric kein Problem dar. Die Leistung eines Netzwerkprozessors kann beeinträchtigt werden, wenn er mehrere Kopien desselben Pakets erstellen muss, um an einige Ports gesendet zu werden, die der Netzwerkprozessor verarbeitet.

Um Geräte im Fall eines Gewitters zu schützen, können Sie mit der Traffic Storm Control-Funktion eine maximale Rate von Broadcasts, Multicast und unbekannten Unicasts konfigurieren, die von einem Bridge-Domain-AC akzeptiert werden. Weitere Informationen finden Sie im Konfigurationshandbuch zur Systemsicherheit für Aggregation Services Router der Cisco Serie ASR 9000, Version 4.3.x: Implementing Traffic Storm Control under a VPLS Bridge.

Traffic Storm Control wird für Bundle-AC-Schnittstellen oder VFI-PWs nicht unterstützt, jedoch für Nicht-Bundle-ACs und Access-PWs. Die Funktion ist standardmäßig deaktiviert. Wenn Sie keine Sturmkontrolle einrichten, akzeptieren Sie Broadcast-, Multicast- und unbekannte Unicast-Raten.

Nachfolgend finden Sie ein Beispiel für eine Konfiguration:

```
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>
```

Die Zähler für Sturmkontrolle werden immer in der Ausgabe des Befehls **show l2vpn bridge-domain detail** angezeigt. Da die Funktion standardmäßig deaktiviert ist, wird der Bericht der Zähler erst nach der Konfiguration der Funktion gelöscht.

Die konfigurierten Tarife können je nach Verkehrsmuster von einem Netzwerk zum anderen variieren. Bevor Sie eine Übertragungsrate konfigurieren, empfiehlt Cisco, die Übertragungsrate von Broadcast-, Multicast- oder unbekannten Unicast-Frames unter normalen Umständen zu kennen. Fügen Sie dann eine Marge in der konfigurierten Rate über der normalen Rate hinzu.

4.6 MAC-Verschiebungen

Bei einer Instabilität des Netzwerks, z. B. durch einen Schnittstellen-Flapping, kann eine MAC-Adresse von einer neuen Schnittstelle abgerufen werden. Dies ist eine normale Netzwerkkonvergenz, und die MAC-Adresstabelle wird dynamisch aktualisiert.

Konstante MAC-Verschiebungen weisen jedoch häufig auf eine Instabilität des Netzwerks hin, z. B. eine schwere Instabilität während einer L2-Schleife. Mit der Sicherheitsfunktion für MAC-Adressen können Sie MAC-Verschiebungen melden und Korrekturmaßnahmen ergreifen, z. B. das Herunterfahren eines beanstandeten Ports.

Selbst wenn keine Korrekturmaßnahme konfiguriert ist, können Sie den Befehl **logging**

konfigurieren, sodass Sie durch die MAC-Verschiebungsmeldungen über Netzwerkinstabilität informiert werden:

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

In diesem Beispiel ist die Aktion auf none (keine) konfiguriert. Wenn eine MAC-Verschiebung erkannt wird, wird also nichts unternommen, außer dass eine Syslog-Meldung protokolliert wird. Dies ist eine Beispielmeldung:

```
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- und MLD-Snooping

Standardmäßig werden Multicast-Frames an alle Ports in einer Bridge-Domäne weitergeleitet. Wenn Sie Streams mit hohen Übertragungsraten wie IP-TV (IPTV) verwenden, wird möglicherweise ein Großteil des Datenverkehrs an alle Ports weitergeleitet und über mehrere PWs repliziert. Wenn alle TV-Streams über eine Schnittstelle weitergeleitet werden, kann dies zu einer Überlastung der Ports führen. Die einzige Option ist die Konfiguration einer Funktion wie IGMP oder MLD-Snooping, die Multicast-Steuerungspakete abfängt, um die Empfänger und Multicast-Router zu verfolgen und Streams nur dann an die Ports weiterzuleiten, wenn dies erforderlich ist.

Weitere Informationen zu diesen Funktionen finden Sie im Konfigurationshandbuch für Aggregation Services Router Multicast der Cisco Serie ASR 9000, Version 4.3.x.

5. Zusätzliche L2VPN-Themen

Hinweise:

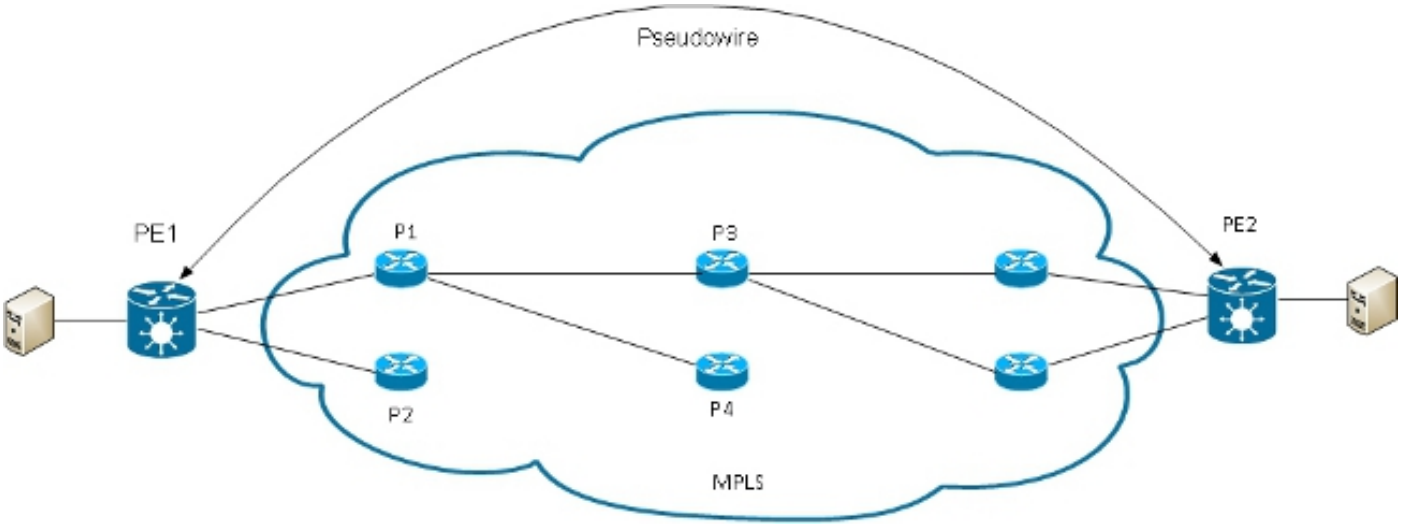
Verwenden Sie das Command Lookup-Tool (Tool für die Suche nach Befehlen) (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Das Output Interpreter-Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter-Tool, um eine Analyse der **show**-Befehlsausgabe anzuzeigen.

5.1 Lastenausgleich

Wenn ein L2VPN-PE einen Frame über einen MPLS-PW senden muss, wird der Ethernet-Frame in einen MPLS-Frame mit einem oder mehreren MPLS-Labels gekapselt. Es gibt mindestens ein PW-Label und möglicherweise ein IGP-Label, um den Remote-PE zu erreichen.

Der MPLS-Frame wird vom MPLS-Netzwerk zum Remote-L2VPN-PE transportiert. Es gibt in der Regel mehrere Pfade, um den Ziel-PE zu erreichen:



Hinweis: Nicht alle Links sind in diesem Diagramm dargestellt.

PE1 kann zwischen P1 und P2 als erster MPLS-P-Router zum PE2 wählen. Wenn P1 ausgewählt ist, wählt PE1 dann P3 oder P4 usw. aus. Die verfügbaren Pfade basieren auf der IGP-Topologie und dem MPLS-TE-Tunnelpfad.

MPLS-Service-Provider ziehen es vor, alle Verbindungen gleich zu nutzen, anstatt nur eine überlastete Verbindung mit anderen nicht ausgelasteten Verbindungen zu verwenden. Dieses Ziel ist nicht immer leicht zu erreichen, da einige PWs viel mehr Datenverkehr übertragen als andere und der Pfad, den ein PW-Datenverkehr nimmt, vom Hash-Algorithmus im Core abhängt. Mehrere PWs mit hoher Bandbreite können auf dieselben Verbindungen gehasht werden, was zu Überlastungen führt.

Eine sehr wichtige Anforderung besteht darin, dass alle Pakete eines Datenflusses dem gleichen Pfad folgen müssen. Andernfalls kann es zu ungeordneten Frames kommen, was sich auf die Qualität oder die Leistung der Anwendungen auswirken kann.

Der Lastenausgleich in einem MPLS-Netzwerk auf Cisco Routern basiert in der Regel auf den Daten, die dem unteren MPLS-Label folgen.

- Wenn die Daten unmittelbar nach dem unteren Label mit 0x4 oder 0x6 beginnen, geht ein MPLS-P-Router davon aus, dass sich ein IPv4- oder IPv6-Paket im MPLS-Paket befindet, und versucht, ein Load Balancing basierend auf einem Hash der Quell- und Ziel-IPv4- oder -IPv6-Adressen durchzuführen, die aus dem Frame extrahiert wurden. Theoretisch sollte dies nicht für einen Ethernet-Frame gelten, der gekapselt und über einen PW übertragen wird, da die Ziel-MAC-Adresse dem unteren Label folgt. Kürzlich wurden jedoch einige MAC-Adressbereiche zugewiesen, die mit 0x4 und 0x6 beginnen. Der MPLS-P-Router könnte fälschlicherweise davon ausgehen, dass der Ethernet-Header tatsächlich ein IPv4-Header ist, und den Frame hash, basierend auf der Annahme, dass es sich um die IPv4-Quell- und

Zieladresse handelt. Ethernet-Frames von einem PW können über verschiedene Pfade im MPLS-Core gehasht werden, was zu Out-of-Sequence-Frames im PW und Problemen mit der Anwendungsqualität führt. Die Lösung besteht in der Konfiguration eines Kontrollworts unter einer PW-Klasse, die an einen Punkt-zu-Punkt- oder VPLS-PW angeschlossen werden kann. Das Kontrollwort wird unmittelbar nach den MPLS-Labels eingefügt. Das Kontrollwort beginnt nicht mit 0x4 oder 0x6, sodass das Problem vermieden wird.

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

- Wenn die Daten unmittelbar nach dem Ende des MPLS-Label-Stacks nicht mit 0x4 oder 0x6 beginnen, erfolgt der Lastausgleich für den P-Router auf Basis des unteren Labels. Der gesamte Datenverkehr von einem PW folgt demselben Pfad, sodass keine Pakete außerhalb der Reihenfolge auftreten. Dies kann jedoch bei PWs mit hoher Bandbreite zu Überlastungen auf einigen Verbindungen führen. Mit Version 4.2.1 der Cisco IOS XR Software unterstützt die ASR Serie 9000 die Flow Aware Transport (FAT) PW-Funktion. Diese Funktion wird auf den

L2VPN-PEs ausgeführt, wo sie zwischen den beiden Enden eines Punkt-zu-Punkt- oder VPLS-PWs ausgehandelt wird. Der Eingangs-L2VPN-PE erkennt Datenflüsse in der AC- und der L2VPN-Konfiguration und fügt ein neues MPLS-Flow-Label unter dem PW-MPLS-Label unten im MPLS-Label-Stack ein. Der Eingangs-PE erkennt Datenflüsse anhand der Quell- und Ziel-MAC-Adressen (Standard) oder der Quell- und Ziel-IPv4-Adressen (konfigurierbar). Standardmäßig werden MAC-Adressen verwendet. Die Verwendung von IPv4-Adressen wird empfohlen, muss jedoch manuell konfiguriert werden.

Bei Verwendung der FAT-PW-Funktion fügt der Eingangs-L2VPN-PE ein unteres MPLS-Label pro src-dst-mac oder pro src-dst-ip ein. Die MPLS-P-Router (zwischen den PEs) übertragen Frames über die verfügbaren Pfade und erreichen dann den Ziel-PE auf Basis des FAT-PW-Flow-Labels am unteren Rand des MPLS-Stacks. Dadurch wird die Bandbreitennutzung im Core im Allgemeinen deutlich verbessert, es sei denn, ein PW überträgt nur eine geringe Anzahl von src-dst-mac- oder src-dst-ip-Gesprächen. Cisco empfiehlt die Verwendung eines Kontrollworts, damit MAC-Adressen, die mit 0x4 und 0x6 beginnen, nicht unmittelbar nach dem Flow-Label stehen. Dadurch wird sichergestellt, dass der Hash auf den Pseudo-IP-Adressen und nicht auf dem Flow-Label richtig basiert.

Mit dieser Funktion wird für den Datenverkehr von einem PW ein Lastausgleich über mehrere Pfade im Core vorgenommen, wenn diese verfügbar sind. Anwendungsdatenverkehr weist keine Probleme mit ungeordneten Paketen auf, da der gesamte Datenverkehr von derselben Quelle (MAC oder IP) zum selben Ziel (MAC oder IP) dem gleichen Pfad folgt.

Unten sehen Sie eine Beispielkonfiguration:

```
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 Protokollierung

Im L2VPN-Konfigurationsmodus können verschiedene Arten von Protokollmeldungen konfiguriert werden. Konfigurieren Sie die l2vpn-Protokollierung, um Syslog-Warnungen für L2VPN-Ereignisse zu erhalten, und konfigurieren Sie die Protokoll-Pseudowire-Funktion, um zu bestimmen, wann sich der PW-Status ändert:

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

Wenn viele PWs konfiguriert sind, können Meldungen das Protokoll überfluten.

5.3 Zugriffsliste für Ethernet-Services

Sie können eine Ethernet-Services-Zugriffsliste verwenden, um Datenverkehr von bestimmten Hosts zu verwerfen oder um zu überprüfen, ob ein Router Pakete von einem Host auf einer l2transport-Schnittstelle empfängt:

```
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)
```

Die Hardwareübereinstimmungen können nur mit dem *Hardware*-Schlüsselwort angezeigt werden. Verwenden Sie je nach Richtung der Zugriffsgruppe das Schlüsselwort *ingress* oder *egress*. Der Linecard-Speicherort der Schnittstelle, auf die die Zugriffsliste angewendet wird, wird ebenfalls angegeben.

Sie können eine ipv4-Zugriffsliste auch auf eine l2transport-Schnittstelle als Sicherheits- oder Fehlerbehebungsfunktion anwenden:

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

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

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

5.4 Ethernet-Egress-Filter

Nehmen Sie an, es gibt keinen **symmetrischen** Befehl **rewrite ingress tag pop <>, der** die Egress-VLAN-Tags bestimmt. In diesem Fall wird nicht überprüft, ob der ausgehende Frame die richtigen VLAN-Tags gemäß dem **Kapselungsbefehl** aufweist.

Unten sehen Sie eine Beispielkonfiguration:

```
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
!
!
!
!
```

Beachten Sie bei dieser Konfiguration Folgendes:

- Ein Broadcast, der mit einem dot1q-Tag 2 auf GigabitEthernet0/1/0/39.2 empfangen wird, behält den eingehenden Tag bei, da kein **rewrite ingress-**Befehl vorhanden ist.
- Dieser Broadcast wird von GigabitEthernet0/1/0/3.2 mit dem dot1q-Tag 2 geflutet, was jedoch kein Problem verursacht, da GigabitEthernet0/1/0/3.2 ebenfalls mit dem dot1q-Tag 2 konfiguriert ist.
- Dieser Broadcast wird auch aus GigabitEthernet0/1/0/3.3 geflutet, das sein ursprüngliches Tag 2 beibehält, da es keinen **Rewrite-**Befehl auf GigabitEthernet0/1/0/3.3 gibt. Der Befehl **encapsulation dot1q 3** auf GigabitEthernet0/1/0/3.3 wird nicht in Ausgangsrichtung überprüft.
- Das Ergebnis ist, dass für eine Sendung, die mit dem Tag 2 auf GigabitEthernet0/1/0/39 empfangen wird, zwei Sendungen mit dem Tag 2 aus GigabitEthernet0/1/0/3 ausgehen. Dieser duplizierte Datenverkehr kann einige Anwendungsprobleme verursachen.
- Die Lösung besteht in der Konfiguration des *EtherNet-Egress-Filters "strict"*, um sicherzustellen, dass Pakete die Subschnittstelle mit den richtigen VLAN-Tags verlassen. Andernfalls werden die Pakete nicht weitergeleitet und verworfen.

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.