

# ASR 9000 - VPLS LSM begrijpen en configureren

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[VPLS Label Switched Multicast \(LSM\) - Overzicht](#)

[Nadelen van ingress replicatie](#)

[VPLS LSM-functies](#)

[VPLS LSM-beperkingen](#)

[Media Access Control \(MAC\) learning](#)

[Ondersteuning van Internet Group Management Protocol Snooping \(IGMP\)](#)

[Schaal ondersteunde producten](#)

[Configuratie VPLS LSM](#)

[Configuratie van P2MP Auto Tunnel](#)

[Configuratie MPLS TE Fast Reroute \(FRR\)](#)

[L2VPN-configuratie](#)

[Monstertopologie en -configuratie](#)

[PE1-configuratie](#)

[IP-configuratie](#)

[PE2-configuratie](#)

[PE3-configuratie](#)

[Verifiëren - Opdrachten weergeven](#)

[Probleemoplossing voor VPLS LSM](#)

[Veelvoorkomende configuratieproblemen](#)

[L2VPN en L2FIB tonen opdrachten en probleemoplossing](#)

## Inleiding

Dit document beschrijft Virtual Private LAN Service (VPLS) Label Switched Multicast (LSM) voor de Aggregation Services Router (ASR) 9000 Series waarop Cisco IOS<sup>®</sup> XR-software wordt uitgevoerd.

## Voorwaarden

## Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

## Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

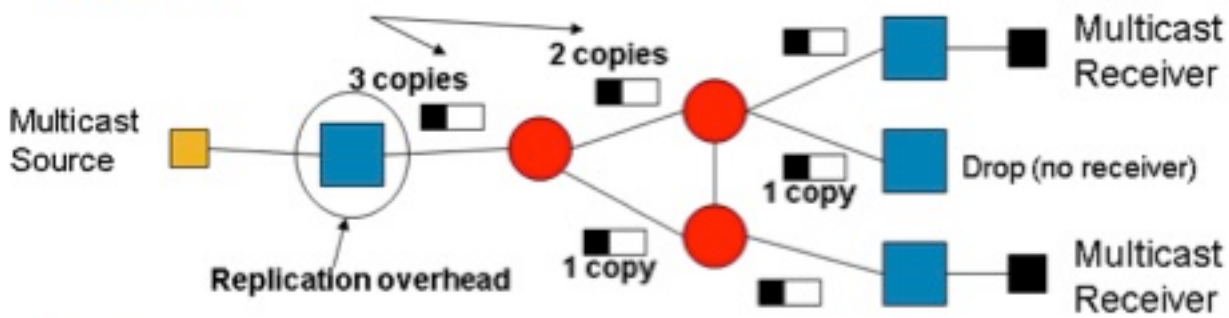
## VPLS Label Switched Multicast (LSM) - Overzicht

VPLS emuleert LAN-services over een Multiprotocol Label Switching (MPLS) kern. Er is een volledig netwerk van point-to-point (P2P) pseudowires (PW's) ingesteld tussen alle routers van Provider Edge (PE) die deelnemen aan een VPLS-domein om VPLS-emulatie te bieden. De uitzending, multicast, en het onbekende unicastverkeer worden overstromd in een domein VPLS aan alle PEs. Ingress-replicatie wordt gebruikt om dat overstromde verkeer via elk P2P-PW naar alle externe PE-routers te sturen die deel uitmaken van hetzelfde VPLS-domein.

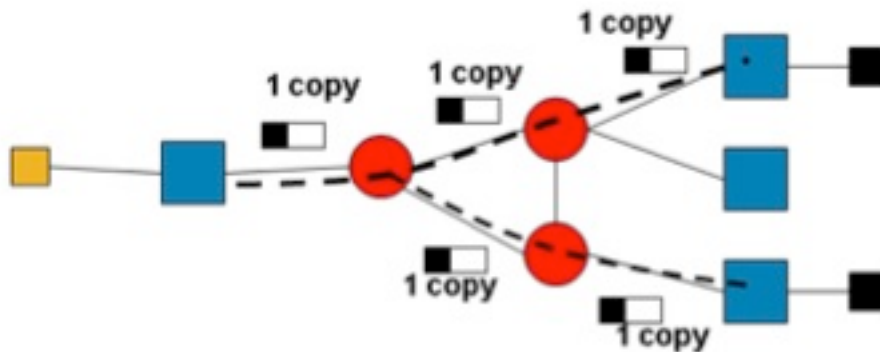
## Nadelen van ingress replicatie

- Ingress-replicatie is een inefficiënte bandbreedte omdat hetzelfde pakket meerdere keren over dezelfde link verzonden kan worden voor elke P2P PW.
- Ingress-replicatie kan resulteren in aanzienlijk verspilde linkbandbreedte wanneer er veel uitzending en multicast VPLS-verkeer is.
- Ingress-replicatie is ook zeer arbeidsintensief omdat de IP-toegangsrouter de volledige last van de replicatie draagt.

## Problems



## Solution



## VPLS LSM-functies

VPLS is een breed geïmplementeerde serviceprovider L2VPN-technologie die ook wordt gebruikt voor multicast transport. Hoewel L2 technologie het mogelijk maakt om snuffelen te gebruiken om replicatie van multicast verkeer naar L2 pseudowires te optimaliseren, blijft de kern onafhankelijk van multicast verkeer. Als resultaat hiervan, meerdere kopieën van dezelfde flow traverse core netwerken. Om deze inefficiëntie te verminderen, koppel LSM met VPLS om LSM multicast bomen over de kern te introduceren. In Cisco IOS-XR-software release 5.1.0 implementeert Cisco ASR 9000 Series VPLS LSM met point-to-multipoint traffic engineering (P2MP-TE) inclusieve bomen. VPLS-eindpunten worden automatisch gedetecteerd en P2MP-TE-bomen worden ingesteld met behulp van Resource Reservation Protocol Traffic Engineering (RSVP-TE) zonder operationele interventie.

- VPLS LSM overbrugt de nadelen van toegangsreplicatie.
- De VPLS LSM-oplossing maakt gebruik van P2MP LSP's in de MPLS-kern om broadcast-, multicast- en onbekend unicastverkeer voor een VPLS-domein te transporteren.
- P2MP LSP's maken replicatie in het MPLS-netwerk mogelijk bij de meest optimale knooppunt en minimaliseren de hoeveelheid pakketrelicatie in het netwerk.
- De VPLS LSM-oplossing verstuurt alleen overstroomd VPLS-verkeer via P2MP LSP's.
- Unicast VPLS-verkeer wordt nog steeds verzonden via P2P-PW's. Verkeer dat via Access-PW's wordt verzonden, wordt nog steeds met toegangsreplicatie verzonden.
- P2MP-PW's zijn unidirectioneel tegenover P2P-PW's, die bidirectioneel zijn.

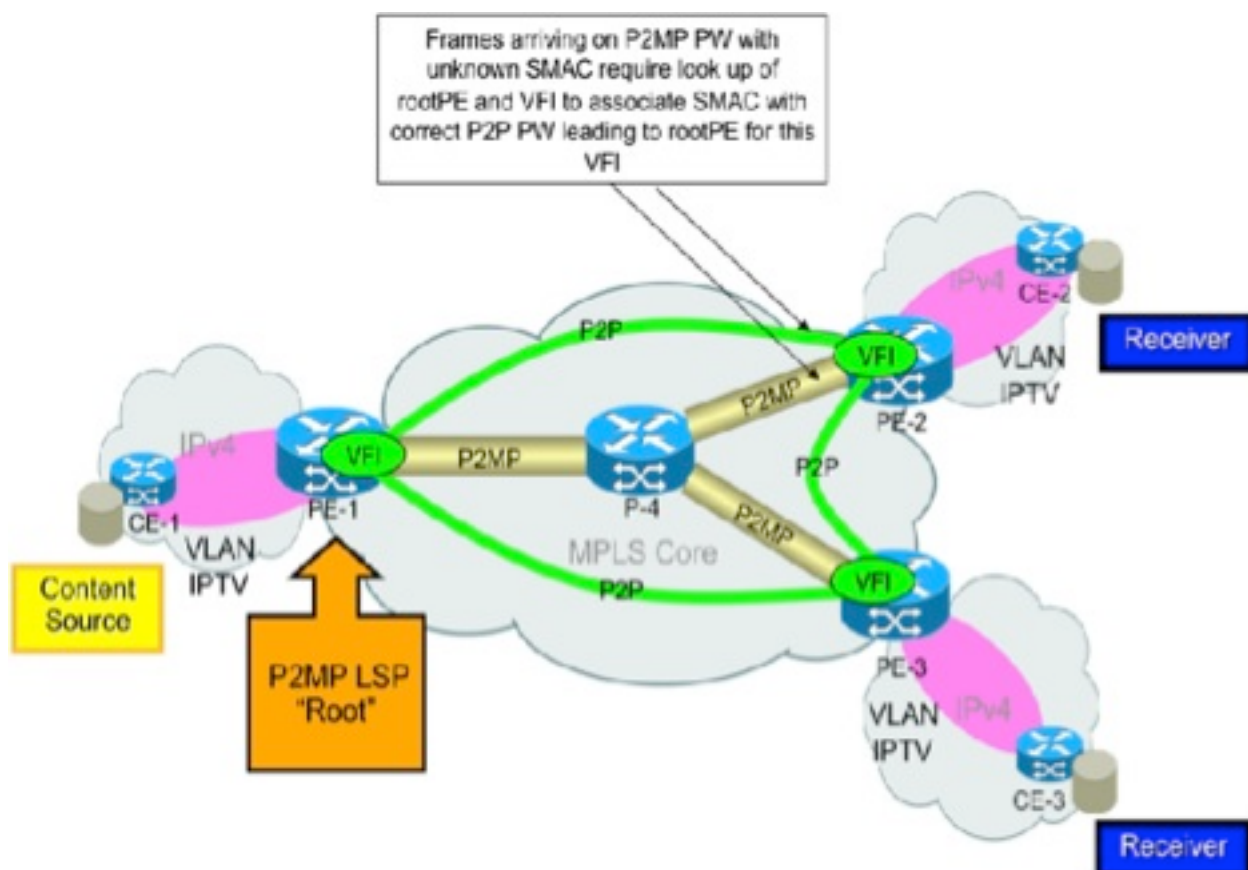
- De VPLS LSM-oplossing omvat de creatie van een P2MP PW per VPLS-domein om een VPLS P2MP-service voor kern-PW's in het VPLS-domein na te bootsen.
- VPLS LSM wordt ondersteund in Cisco IOS XR release 5.1.0 en hoger.

## VPLS LSM-beperkingen

- Cisco IOS-XR release 5.1.0 VPLS LSM-functionaliteit ondersteunt alleen MPLS Traffic Engineering P2MP-TE-bomen die met RSVP-TE zijn geïnstalleerd.
- Een P2MP-PW kan alleen met het BGP-protocol worden gesignaleerd in Cisco IOS-XR release 5.1.0. In deze eerste fase worden de externe PE's die deelnemen aan het VPLS-domein automatisch ontdekt met BGP Auto-Discovery (BGP-AD).
- Statische LDP-signalering wordt niet ondersteund in Cisco IOS XR release 5.1.0.

## Media Access Control (MAC) learning

MAC leren op het blad PE voor een frame dat aankomt op P2MP PW wordt gedaan alsof het frame wordt ontvangen op de P2P PW leidend tot de root PE voor die P2MP PW. In dit beeld wordt MAC Learning op PE-2 voor frames die aankomen op de P2MP PW LSP geworteld in PE-1 gedaan alsof het frame aankwam op de P2P PW tussen PE-1 en PE-2. Het L2VPN-besturingsplane is verantwoordelijk voor het programmeren van de VPLS-dispositie-informatie met P2P PW-informatie voor MAC-leren over de P2MP LSP-dispositie.



# Ondersteuning van Internet Group Management Protocol Snooping (IGMP)

IGMP-snooping (Internet Group Management Protocol) wordt ondersteund op zowel de kop als de staart van de P2MP-structuur in een brugdomein dat deelneemt aan VPLS LSM. Hierdoor kan IGMP/SN multicast-verkeer via een VFI-PW (Virtual Forwarding Instance) profiteren van de optimalisatie van resources die door P2MP-LSP's wordt geboden. Als IGMP/SN is ingeschakeld in een brugdomein met een of meer VFI-PW's die deelnemen aan VPLS LSM, wordt al het Layer 2 (L2) multicast-verkeer over het P2MP P-boomhoofd verzonden dat is gekoppeld aan het brugdomein. L2 multicast routes worden gebruikt om verkeer door te sturen naar lokale ontvangers, Ethernet Flow Points (EFP's), toegang tot PW's en VFI-PW's die niet deelnemen aan VPLS LSM.

Wanneer IGMP/SN is ingeschakeld in een brugdomein dat een P2MP LSP-staart is, wordt geoptimaliseerde verwerking van L2 multicast-verkeer dat op de P2MP LSP wordt ontvangen, uitgevoerd voor lokale ontvangers (dat wil zeggen, Attachment Circuit (AC) Bridge Ports (BP's) en toegang tot PW BP's).

**Opmerking:** multicast Label Distribution Protocol (MLDP)-signalering wordt niet ondersteund in Cisco IOS XR release 5.1.0.

## Schaal ondersteunde producten

Cisco IOS XR-release 5.1.0 ondersteunt maximaal **1000** P2MP-tunnels of **1000** P2MP PW's per head/tail-router.

## Configuratie VPLS LSM

### Configuratie van P2MP Auto Tunnel

```
mpls traffic-eng
interface GigabitEthernet0/1/1/0
!
interface GigabitEthernet0/1/1/1
!
auto-tunnel p2mp
tunnel-id min 100 max 200
```

### Configuratie MPLS TE Fast Reroute (FRR)

```
mpls traffic-eng
interface GigabitEthernet0/1/1/0
auto-tunnel backup
nhop-only
!
```

```

!
interface GigabitEthernet0/1/1/1
auto-tunnel backup
  nhop-only
!
!
auto-tunnel p2mp
tunnel-id min 100 max 200
!
auto-tunnel backup
tunnel-id min 1000 max 1500
!
attribute-set p2mp-te set1
bandwidth 10000
fast-reroute
record-route
!

```

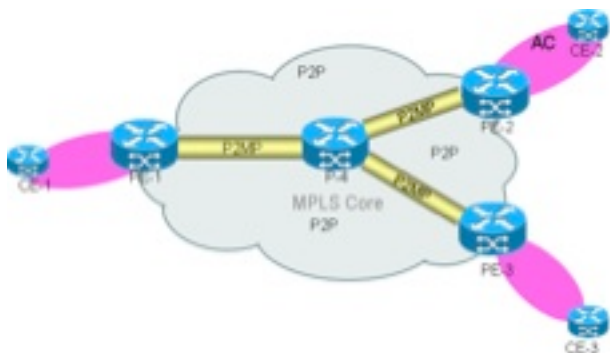
## L2VPN-configuratie

```

l2vpn
bridge group bg1
bridge-domain bg1_bd1
interface GigabitEthernet0/1/1/10.1
!
vfi bg1_bd1_vfi
vpn-id 1
autodiscovery bgp
rd auto
route-target 209.165.201.1:1
signaling-protocol bgp
ve-id 100
!
!
multicast p2mp
signaling-protocol bgp
!
transport rsvp-te
attribute-set p2mp-te set1
!

```

## Monstertopologie en -configuratie



De P2MP-tunnels zijn automatisch ontdekte tunnels. Statische P2MP-tunnels worden **niet** ondersteund.

Statische tunnelconfiguraties worden niet gebruikt. De automatische P2MP-tunnelconfiguratie

moet worden ingeschakeld op alle PE-routers en ook op een P-router als deze fungeert als knooppunt. Een bud knooppunt is een middelpunt en een tailend router tegelijkertijd.

Een steekproeftopologie met configuratie wordt hier getoond. In deze topologie worden P2MP-PW's gecreëerd tussen de drie PE's en een P-router die fungeert als knooppunt. Alle drie PE-routers fungeren als head (voor toegangsverkeer) en Tail (voor uitgaand verkeer).

## PE1-configuratie

```
RP/0/RSP0/CPU0:PE1#show run
hostname PE1
!
ipv4 unnumbered mpls traffic-eng Loopback0
!
interface Loopback0
  ipv4 address 209.165.200.225 255.255.255.255
!
interface GigabitEthernet0/1/1/0
  description connected P router
  ipv4 address 209.165.201.1 255.255.255.224
!
interface GigabitEthernet0/1/1/1
  description connected to P router
  ipv4 address 209.165.201.151 255.255.255.224
  transceiver permit pid all
!
interface GigabitEthernet0/1/1/10
  transceiver permit pid all
!
interface GigabitEthernet0/1/1/10.1 l2transport
  encapsulation dot1q 1
!
router ospf 100
  router-id 209.165.200.225
  area 0
  mpls traffic-eng
  interface Loopback0
  !
  interface GigabitEthernet0/1/1/0
  !
  interface GigabitEthernet0/1/1/1
  !
  !
  mpls traffic-eng router-id 209.165.200.225
!
router bgp 100
  nsr
  bgp router-id 209.165.200.225
  bgp graceful-restart
  address-family l2vpn vpls-vpws
  !
  neighbor 209.165.200.226
  remote-as 100
  update-source Loopback0
  address-family l2vpn vpls-vpws
  !
  !
  neighbor 209.165.200.227
  remote-as 100
```

```

update-source Loopback0
address-family l2vpn vpls-vpws
!
!
neighbor 209.165.200.228
remote-as 100
update-source Loopback0
address-family l2vpn vpls-vpws
!
!
!
l2vpn
bridge group bg1
bridge-domain bg1_bd1
interface GigabitEthernet0/1/1/10.1
!
vfi bg1_bd1_vfi
vpn-id 1
autodiscovery bgp
rd auto
route-target 209.165.201.1:1
signaling-protocol bgp
ve-id 100
!
!
multicast p2mp
signaling-protocol bgp
!
transport rsvp-te
attribute-set p2mp-te set1
!
!
!
!
!
!
!
!
rsvp
interface GigabitEthernet0/1/1/0
bandwidth 100000
!
interface GigabitEthernet0/1/1/1
bandwidth 100000
!
!
mpls traffic-eng
interface GigabitEthernet0/1/1/0
auto-tunnel backup
nhop-only
!
!
interface GigabitEthernet0/1/1/1
auto-tunnel backup
nhop-only
!
!
auto-tunnel p2mp
tunnel-id min 100 max 200
!
auto-tunnel backup
tunnel-id min 1000 max 1500
!
attribute-set p2mp-te set1
bandwidth 10000
fast-reroute

```



```

record-route
!
!
mpls ldp
nsr
graceful-restart
router-id 209.165.200.225
interface GigabitEthernet0/1/1/0
!
interface GigabitEthernet0/1/1/1
!
!
end

```

RP/0/RSP0/CPU0:PE1#

## IP-configuratie

```

RP/0/RSP0/CPU0:P#show run
hostname P
ipv4 unnumbered mpls traffic-eng Loopback0
interface Loopback0
  ipv4 address 209.165.200.226 255.255.255.255
!
interface GigabitEthernet0/1/1/0
  description connected to PE1 router
  ipv4 address 209.165.201.2 255.255.255.224
  transceiver permit pid all
!
interface GigabitEthernet0/1/1/1
  description connected to PE1 router
  ipv4 address 209.165.201.152 255.255.255.224
  transceiver permit pid all
!
interface GigabitEthernet0/1/1/3
  description connected to PE2 router
  ipv4 address 209.165.201.61 255.255.255.224
!
interface GigabitEthernet0/1/1/4
  transceiver permit pid all
!
interface GigabitEthernet0/1/1/4.1 l2transport
  encapsulation dot1q 1
!
interface GigabitEthernet0/1/1/8
  description connected to PE3 router
  ipv4 address 209.165.201.101 255.255.255.224
!
router ospf 100
nsr
nsf cisco
area 0
mpls traffic-eng
interface Loopback0
!
interface GigabitEthernet0/1/1/0
!
interface GigabitEthernet0/1/1/1
!
interface GigabitEthernet0/1/1/3
!

```



```

!
interface GigabitEthernet0/1/1/8
bandwidth 100000
!
!
mpls traffic-eng
interface GigabitEthernet0/1/1/0
auto-tunnel backup
nhop-only
!
!
interface GigabitEthernet0/1/1/1
auto-tunnel backup
nhop-only
!
!
interface GigabitEthernet0/1/1/3
!
interface GigabitEthernet0/1/1/8
!
auto-tunnel p2mp
tunnel-id min 100 max 200
!
auto-tunnel backup
tunnel-id min 1000 max 1500
!
attribute-set p2mp-te set1
bandwidth 10000
fast-reroute
record-route
!
!
mpls ldp
nsr
graceful-restart
router-id 209.165.200.226
interface GigabitEthernet0/1/1/0
!
interface GigabitEthernet0/1/1/1
!
interface GigabitEthernet0/1/1/3
!
interface GigabitEthernet0/1/1/8
!
!
end

```

RP/0/RSP0/CPU0:P#

## PE2-configuratie

```

RP/0/RSP0/CPU0:PE2#show run
hostname PE2
ipv4 unnumbered mpls traffic-eng Loopback0
interface Loopback0
ipv4 address 209.165.200.227 255.255.255.255
!
interface GigabitEthernet0/3/0/2.1 l2transport
encapsulation dot1q 1
!
interface GigabitEthernet0/3/0/3

```

```
description connected to P router
ipv4 address 209.165.201.62 255.255.255.224
transceiver permit pid all
!
router ospf 100
nsr
router-id 209.165.200.227
nsf cisco
area 0
mpls traffic-eng
interface Loopback0
!
interface GigabitEthernet0/3/0/3
!
!
mpls traffic-eng router-id 209.165.200.227
!
router bgp 100
nsr
bgp router-id 209.165.200.227
bgp graceful-restart
address-family l2vpn vpls-vpws
!
neighbor 209.165.200.225
remote-as 100
update-source Loopback0
address-family l2vpn vpls-vpws
!
!
neighbor 209.165.200.226
remote-as 100
update-source Loopback0
address-family l2vpn vpls-vpws
!
!
neighbor 209.165.200.228
remote-as 100
update-source Loopback0
address-family l2vpn vpls-vpws
!
!
!
l2vpn
bridge group bg1
bridge-domain bg1_bd1
interface GigabitEthernet0/3/0/2.1
!
vfi bg1_bd1_vfi
vpn-id 1
autodiscovery bgp
rd auto
route-target 209.165.201.1:1
signaling-protocol bgp
ve-id 300
!
!
multicast p2mp
signaling-protocol bgp
!
transport rsvp-te
attribute-set p2mp-te set1
!
!
!
```

```

!
!
!
rsvp
 interface GigabitEthernet0/3/0/3
 bandwidth 100000
!
!
mpls traffic-eng
 interface GigabitEthernet0/3/0/3
!
 auto-tunnel p2mp
 tunnel-id min 100 max 200
!
 auto-tunnel backup
 tunnel-id min 1000 max 1500
!
 attribute-set p2mp-te set1
 bandwidth 10000
 fast-reroute
 record-route
!
!
mpls ldp
 nsr
 graceful-restart
 router-id 209.165.200.227
 interface GigabitEthernet0/3/0/3
!
!
end

```

RP/0/RSP0/CPU0:PE2#

## PE3-configuratie

```

RP/0/RSP0/CPU0:PE3#show run
hostname PE3
ipv4 unnumbered mpls traffic-eng Loopback0

interface Loopback0
 ipv4 address 209.165.200.228 255.255.255.255
!
interface GigabitEthernet0/2/1/8
 description connected to P router
 ipv4 address 209.165.201.102 255.255.255.224
 transceiver permit pid all
!
interface GigabitEthernet0/2/1/11
 transceiver permit pid all
!
interface GigabitEthernet0/2/1/11.1 l2transport
 encapsulation dot1q 1
!
router ospf 100
 nsr
 router-id 209.165.200.228
 nsf cisco
 area 0
 mpls traffic-eng
 interface Loopback0

```

```
!  
interface GigabitEthernet0/2/1/8  
!  
!  
mpls traffic-eng router-id 209.165.200.228  
!  
router bgp 100  
  nsr  
  bgp router-id 209.165.200.228  
  bgp graceful-restart  
  address-family l2vpn vpls-vpws  
  !  
  neighbor 209.165.200.225  
  remote-as 100  
  update-source Loopback0  
  address-family l2vpn vpls-vpws  
  !  
  !  
  neighbor 209.165.200.226  
  remote-as 100  
  update-source Loopback0  
  address-family l2vpn vpls-vpws  
  !  
  !  
  neighbor 209.165.200.227  
  remote-as 100  
  update-source Loopback0  
  address-family l2vpn vpls-vpws  
  !  
  !  
!  
l2vpn  
  bridge group bg1  
  bridge-domain bg1_bd1  
  interface GigabitEthernet0/2/1/11.1  
  !  
  vfi bg1_bd1_vfi  
  vpn-id 1  
  autodiscovery bgp  
  rd auto  
  route-target 209.165.201.1:1  
  signaling-protocol bgp  
  ve-id 400  
  !  
  !  
  multicast p2mp  
  signaling-protocol bgp  
  !  
  transport rsvp-te  
  attribute-set p2mp-te set1  
  !  
  !  
  !  
  !  
!  
rsvp  
  interface GigabitEthernet0/2/1/8  
  bandwidth 1000000  
  !  
!  
mpls traffic-eng  
  interface GigabitEthernet0/2/1/8  
  !
```

```

auto-tunnel p2mp
tunnel-id min 100 max 200
!
auto-tunnel backup
tunnel-id min 1000 max 1500
!
attribute-set p2mp-te set1
bandwidth 10000
fast-reroute
record-route
!
!
mpls ldp
nsr
graceful-restart
router-id 209.165.200.228
interface GigabitEthernet0/2/1/8
!
!
end

```

RP/0/RSP0/CPU0:PE3#

## Verifiëren - Opdrachten weergeven

Deze showopdrachten zijn handig om de status van de P2MP PW- en P2MP MPLS TE-tunnels te debuggen en te verifiëren.

- **het l2vpn bridge-domein weergeven**
- **details van l2vpn bridge-domein weergeven**
- **toon mpls traffic-eng tunnels p2mp**
- **tonen mpls door:sturen labels <label> detail**
- **toon mpls traffic-eng tunnels p2mp tabulair**

Hier volgen enkele voorbeelden:

### **show l2vpn bridge-domain**

```

RP/0/RSP0/CPU0:PE1#show l2vpn bridge-domain
Legend: pp = Partially Programmed.
Bridge group: bg1, bridge-domain: bg1_bd1, id: 0, 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:
  GigabitEthernet0/1/1/10.1, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
  VFI bg1_bd1_vfi (up)
    P2MP: RSVP-TE, BGP, 1, Tunnel Up
    Neighbor 209.165.200.226 pw-id 1, state: up, Static MAC addresses: 0
    Neighbor 209.165.200.227 pw-id 1, state: up, Static MAC addresses: 0
    Neighbor 209.165.200.228 pw-id 1, state: up, Static MAC addresses: 0
RP/0/RSP0/CPU0:PE1#

```

### **show l2vpn bridge-domain detail**

```

RP/0/RSP0/CPU0:PE1#show l2vpn bridge-domain detail

```

Legend: pp = Partially Programmed.

Bridge group: bgl, bridge-domain: bgl\_bd1, id: 0, 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 up

MAC withdraw relaying (access to access): 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: enabled

IGMP Snooping profile: none

MLD Snooping profile: none

Storm Control: disabled

Bridge MTU: 1500

MIB cvplsConfigIndex: 1

Filter MAC addresses:

P2MP PW: enabled

Create time: 18/02/2014 03:47:59 (00:41:54 ago)

No status change since creation

ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)

List of ACs:

AC: GigabitEthernet0/1/1/10.1, state is up

Type VLAN; Num Ranges: 1

VLAN ranges: [1, 1]

MTU 1504; XC ID 0x8802a7; 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: enabled

IGMP Snooping profile: none

MLD Snooping profile: none

Storm Control: disabled

Static MAC addresses:

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



List of Access PWs:

List of VFIs:

VFI bg1\_bdl\_vfi (up)

**P2MP:**

**Type RSVP-TE, BGP signaling, PTree ID 1**

**P2MP Status: Tunnel Up**

**P2MP-TE attribute-set: set1**

**Tunnel tunnel-mte100, Local Label: 289994**

**VPN-ID: 1, Auto Discovery: BGP, state is Provisioned (Service Connected)**

**Route Distinguisher: (auto) 209.165.200.225:32768**

Import Route Targets:

209.165.201.1:1

Export Route Targets:

209.165.201.1:1

Signaling protocol: BGP

Local VE-ID: 100 , Advertised Local VE-ID : 100

VE-Range: 10

PW: neighbor 209.165.200.226, PW ID 1, state is up ( established )

PW class not set, XC ID 0xc0000001

Encapsulation MPLS, Auto-discovered (BGP), protocol BGP

Source address 209.165.200.225

PW type VPLS, control word disabled, interworking none

Sequencing not set

MPLS	Local	Remote
-----	-----	-----
Label	289959	16030
MTU	1500	1500
Control word disabled		disabled
PW type	VPLS	VPLS
VE-ID	100	200
-----	-----	-----

MIB cpwVcIndex: 3221225473

Create time: 18/02/2014 03:58:31 (00:31:23 ago)

Last time status changed: 18/02/2014 03:58:31 (00:31:23 ago)

MAC withdraw messages: sent 0, received 0

Static MAC addresses:

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

DHCPv4 snooping: disabled

IGMP Snooping profile: none

MLD Snooping profile: none

P2MP-PW:

FEC	Local	Remote
-----	-----	-----
Label	NULL (inclusive tree)	NULL (inclusive tree)
P2MP ID	100	100
Flags	0x00	0x00
PTree Type	RSVP-TE	RSVP-TE
Tunnel ID	100	100
Ext. Tunnel ID	209.165.200.225	209.165.200.226

Statistics:

packets: received 0

bytes: received 0

PW: neighbor 209.165.200.227, PW ID 1, state is up ( established )

PW class not set, XC ID 0xc0000002

Encapsulation MPLS, Auto-discovered (BGP), protocol BGP

Source address 209.165.200.225

PW type VPLS, control word disabled, interworking none

Sequencing not set

MPLS	Local	Remote
Label	289944	16030
MTU	1500	1500
Control word	disabled	disabled
PW type	VPLS	VPLS
VE-ID	100	300

MIB cpwVcIndex: 3221225474

Create time: 18/02/2014 04:05:25 (00:24:29 ago)

Last time status changed: 18/02/2014 04:05:25 (00:24:29 ago)

MAC withdraw messages: sent 0, received 0

Static MAC addresses:

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

DHCPv4 snooping: disabled

IGMP Snooping profile: none

MLD Snooping profile: none

P2MP-PW:

FEC	Local	Remote
Label	NULL (inclusive tree)	NULL (inclusive tree)
P2MP ID	100	100
Flags	0x00	0x00
PTree Type	RSVP-TE	RSVP-TE
Tunnel ID	100	100
Ext. Tunnel ID	209.165.200.225	209.165.200.227

Statistics:

packets: received 0

bytes: received 0

PW: neighbor 209.165.200.228, PW ID 1, state is up ( established )

PW class not set, XC ID 0xc0000003

Encapsulation MPLS, Auto-discovered (BGP), protocol BGP

Source address 209.165.200.225

PW type VPLS, control word disabled, interworking none

Sequencing not set

MPLS	Local	Remote
Label	289929	16045
MTU	1500	1500
Control word	disabled	disabled
PW type	VPLS	VPLS
VE-ID	100	400

MIB cpwVcIndex: 3221225475

Create time: 18/02/2014 04:08:11 (00:21:43 ago)

Last time status changed: 18/02/2014 04:08:11 (00:21:43 ago)

MAC withdraw messages: sent 0, received 0

Static MAC addresses:

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

DHCPv4 snooping: disabled

IGMP Snooping profile: none

MLD Snooping profile: none

```

P2MP-PW:
  FEC          Local          Remote
  -----
  Label        NULL (inclusive tree)  NULL (inclusive tree)
  P2MP ID      100                          100
  Flags        0x00                          0x00
  PTree Type   RSVP-TE                      RSVP-TE
  Tunnel ID    100                          100
  Ext. Tunnel ID 209.165.200.225      209.165.200.228
  Statistics:
    packets: received 0
    bytes: received 0
  VFI Statistics:
    drops: illegal VLAN 0, illegal length 0
RP/0/RSP0/CPU0:PE1#

```

**show mpls traffic-eng tunnels p2mp**

RP/0/RSP0/CPU0:PE1#**show mpls traffic-eng tunnels p2mp**

```

Name: tunnel-mt100 (auto-tunnel for VPLS (l2vpn))
  Signalled-Name: auto_PE1_mt100
  Status:
    Admin: up  Oper: up (Up for 00:32:35)

  Config Parameters:
    Bandwidth: 0 kbps (CT0) Priority: 7 7 Affinity: 0x0/0xffff
    Interface Bandwidth: 10000 kbps
    Metric Type: TE (default)
    Fast Reroute: Enabled, Protection Desired: Any
    Record Route: Enabled
    Reoptimization after affinity failure: Enabled

  Attribute-set: set1 (type p2mp-te)
  Destination summary: (3 up, 0 down, 0 disabled) Affinity: 0x0/0xffff
  Auto-bw: disabled
  Destination: 209.165.200.226
    State: Up for 00:32:35
    Path options:
      path-option 10 dynamic      [active]
  Destination: 209.165.200.227
    State: Up for 00:25:41
    Path options:
      path-option 10 dynamic      [active]
  Destination: 209.165.200.228
    State: Up for 00:22:55
    Path options:
      path-option 10 dynamic      [active]

  Current LSP:
    lsp-id: 10004 p2mp-id: 100 tun-id: 100 src: 209.165.200.225 extid:
    209.165.200.225
    LSP up for: 00:32:35 (since Tue Feb 18 03:58:31 UTC 2014)
    Reroute Pending: No
    Inuse Bandwidth: 0 kbps (CT0)
    Number of S2Ls: 3 connected, 0 signaling proceeding, 0 down

  S2L Sub LSP: Destination 209.165.200.226 Signaling Status: connected
    S2L up for: 00:32:35 (since Tue Feb 18 03:58:31 UTC 2014)
    Sub Group ID: 1 Sub Group Originator ID: 209.165.200.225
    Path option path-option 10 dynamic      (path weight 1)
    Path info (OSPF 100 area 0)

```

209.165.201.2  
209.165.200.226

S2L Sub LSP: Destination 209.165.200.227 Signaling Status: connected  
S2L up for: 00:25:41 (since Tue Feb 18 04:05:25 UTC 2014)  
Sub Group ID: 2 Sub Group Originator ID: 209.165.200.225  
Path option path-option 10 dynamic (path weight 2)  
Path info (OSPF 100 area 0)  
209.165.201.2  
209.165.201.61  
209.165.201.62  
209.165.200.227

S2L Sub LSP: Destination 209.165.200.228 Signaling Status: connected  
S2L up for: 00:22:55 (since Tue Feb 18 04:08:11 UTC 2014)  
Sub Group ID: 4 Sub Group Originator ID: 209.165.200.225  
Path option path-option 10 dynamic (path weight 2)  
Path info (OSPF 100 area 0)  
209.165.201.2  
209.165.201.101  
209.165.201.102  
209.165.200.228

Reoptimized LSP (Install Timer Remaining 0 Seconds):  
None  
Cleaned LSP (Cleanup Timer Remaining 0 Seconds):  
None

LSP Tunnel 209.165.200.226 100 [10005] is signalled, connection is up  
Tunnel Name: auto\_P\_mt100 **Tunnel Role: Tail**  
InLabel: GigabitEthernet0/1/1/0, 289995  
Signalling Info:  
Src 209.165.200.226 Dst 209.165.200.225, Tun ID 100, Tun Inst 10005, Ext ID  
209.165.200.226  
Router-IDs: upstream 209.165.200.226  
                  local 209.165.200.225  
Bandwidth: 0 kbps (CT0) Priority: 7 7 DSTE-class: 0  
Soft Preemption: None  
Path Info:  
Incoming Address: 209.165.201.1  
Incoming:  
Explicit Route:  
  Strict, 209.165.201.1  
  Strict, 209.165.200.225  
Record Route:  
  IPv4 209.165.201.2, flags 0x0  
Tspec: avg rate=0 kbits, burst=1000 bytes, peak rate=0 kbits  
Session Attributes: Local Prot: Set, Node Prot: Not Set, BW Prot: Not Set  
                  Soft Preemption Desired: Not Set  
Resv Info: None  
Record Route: Empty  
Resv Info:  
Record Route: Empty  
Fspec: avg rate=0 kbits, burst=1000 bytes, peak rate=0 kbits

LSP Tunnel 209.165.200.227 100 [10003] is signalled, connection is up  
Tunnel Name: auto\_PE2\_mt100 **Tunnel Role: Tail**  
InLabel: GigabitEthernet0/1/1/0, 289998  
Signalling Info:  
Src 209.165.200.227 Dst 209.165.200.225, Tun ID 100, Tun Inst 10003, Ext ID  
209.165.200.227  
Router-IDs: upstream 209.165.200.226  
                  local 209.165.200.225  
Bandwidth: 0 kbps (CT0) Priority: 7 7 DSTE-class: 0

Soft Preemption: None

Path Info:

Incoming Address: 209.165.201.1

Incoming:

Explicit Route:

Strict, 209.165.201.1

Strict, 209.165.200.225

Record Route:

IPv4 209.165.201.2, flags 0x0

IPv4 209.165.201.62, flags 0x0

Tspec: avg rate=0 kbits, burst=1000 bytes, peak rate=0 kbits

Session Attributes: Local Prot: Set, Node Prot: Not Set, BW Prot: Not Set

Soft Preemption Desired: Not Set

Resv Info: None

Record Route: Empty

Resv Info:

Record Route: Empty

Fspec: avg rate=0 kbits, burst=1000 bytes, peak rate=0 kbits

LSP Tunnel 209.165.200.228 100 [10004] is signalled, connection is up

Tunnel Name: auto\_PE3\_mt100 **Tunnel Role: Tail**

InLabel: GigabitEthernet0/1/1/0, 289970

Signalling Info:

Src 209.165.200.228 Dst 209.165.200.225, Tun ID 100, Tun Inst 10004, Ext ID

209.165.200.228

Router-IDs: upstream 209.165.200.226

local 209.165.200.225

Bandwidth: 0 kbps (CT0) Priority: 7 7 DSTE-class: 0

Soft Preemption: None

Path Info:

Incoming Address: 209.165.201.1

Incoming:

Explicit Route:

Strict, 209.165.201.1

Strict, 209.165.200.225

Record Route:

IPv4 209.165.201.2, flags 0x0

IPv4 209.165.201.102, flags 0x0

Tspec: avg rate=0 kbits, burst=1000 bytes, peak rate=0 kbits

Session Attributes: Local Prot: Set, Node Prot: Not Set, BW Prot: Not Set

Soft Preemption Desired: Not Set

Resv Info: None

Record Route: Empty

Resv Info:

Record Route: Empty

Fspec: avg rate=0 kbits, burst=1000 bytes, peak rate=0 kbits

Displayed 1 (of 2) heads, 0 (of 0) midpoints, 3 (of 4) tails

Displayed 1 up, 0 down, 0 recovering, 0 recovered heads

RP/0/RSP0/CPU0:PE1#

**show mpls forwarding labels detail**

RP/0/RSP0/CPU0:PE1#**show mpls forwarding labels 289994 detail**

Local Label	Outgoing Label	Prefix or ID	Outgoing Interface	Next Hop	Bytes Switched
289994		P2MP TE: 100			
Updated Feb 18 03:58:32.360					
TE Tunnel Head, tunnel ID: 100, tunnel ifh: 0x8000e20					
IPv4 Tableid: 0xe0000000, IPv6 Tableid: 0xe0800000					
Flags:IP Lookup:not-set, Expnnullv4:not-set, Expnnullv6:set					
Payload Type v4:set, Payload Type v6:not-set, l2vpn:set					

```
Head:set, Tail:not-set, Bud:not-set, Peek:not-set, inclusive:set
Ingress Drop:not-set, Egress Drop:not-set
Platform Data: {0x2000000, 0x2000000, 0x0, 0x0}, RPF-ID:0x80003
VPLS Disposition: Bridge ID: 0, SHG ID: 0, PW Xconnect ID: 0x0
```

```
mpls paths: 1, local mpls paths: 0, protected mpls paths: 1
```

```
16005      P2MP TE: 100      Gi0/1/1/0      209.165.201.2    0
Updated Feb 18 03:58:32.360
```

```
My Nodeid:65, Interface Nodeid:2065, Backup Interface Nodeid:2065
```

```
Packets Switched: 0
```

```
RP/0/RSP0/CPU0:PE1#
```

```
show mpls traffic-eng tunnels p2mp tabular
```

```
RP/0/RSP0/CPU0:PE1#show mpls traffic-eng tunnels p2mp tabular
```

Tunnel Name	LSP ID	Destination Address	Source Address	State	FRR State	LSP Role	Path Prot
^tunnel-mte100	10004	209.165.200.226	209.165.200.225	up	Ready	Head	
^tunnel-mte100	10004	209.165.200.227	209.165.200.225	up	Ready	Head	
^tunnel-mte100	10004	209.165.200.228	209.165.200.225	up	Ready	Head	
auto_P_mt100	10005	209.165.200.225	209.165.200.226	up	Inact	Tail	
auto_PE2_mt100	10003	209.165.200.225	209.165.200.227	up	Inact	Tail	
auto_PE3_mt100	10004	209.165.200.225	209.165.200.228	up	Inact	Tail	

```
* = automatically created backup tunnel
```

```
^ = automatically created P2MP tunnel
```

```
RP/0/RSP0/CPU0:PE1#
```

## Probleemoplossing voor VPLS LSM

### Veelvoorkomende configuratieproblemen

De meest voorkomende oorzaken voor P2MP problemen in L2VPN worden hier getoond.

- De BGP-configuratie voor LSM is precies hetzelfde als die voor BGP-AD. Zorg ervoor dat u L2vpn vpls-vpws adresfamilieroutes exporteert/importeert door **adresfamilie l2vpn vpls-vpws te** configureren voor BGP-buren.
- Er zijn MPLS- en multicast-configuratiefouten.

MPLS Traffic Engineering moet zijn ingeschakeld op de interfaces waar de P2MP-PW's passeren.

```
mpls traffic-eng
interface gigabit <>
```

```
auto-tunnel p2mp
tunnel-id min 100 max 200
```

Enable multicast-routing for interfaces.

```
multicast-routing
address-family ipv4
interface all enable
```

- De L2VPN-configuratie voor LSM in Cisco IOS XR-release 5.1.0 vereist dat u:

De VPN-id-configuratie voor de VFI configurerenConfigureer multicast P2MP voor de VFI. Configuratie van het transportprotocol en het signaleringsprotocol, zoals in deze voorbeeldconfiguratie:

```
l2vpn
bridge group bg
  bridge-domain bd1
  vfi vf1
    vpn-id 1
    autodiscovery bgp
    rd auto
    route-target 209.165.201.7:1
    signaling-protocol bgp
    ve-id 1
  multicast p2mp
    signaling-protocol bgp
    transport rsvp-te
```

- De LSM-kop/taart moet correct worden ingesteld. In Cisco IOS XR-release 5.1.0 is elke LSM-taart ook een LSM-kop en vice versa. Omdat er geen expliciete LSM-vermogensuitwisseling tussen routers is, moeten alle routers in een LSM-enabled brugdomein aan LSM deelnemen.

## L2VPN en L2FIB tonen opdrachten en probleemoplossing

- Het L2VPN-beheerproces (l2vpn\_mgr) communiceert met het MPLS Traffic Engineering (TE) controleproces (te\_control) en vraagt de tunnelcreatie. Zorg ervoor dat de te\_control en l2vpn\_mgr processen in de lopende staat zijn met deze opdrachten:  
**proces tonen l2vpn\_mgrtoon proces te\_control**
- Controleer of het l2vpn\_mgr-proces om de tunnelcreatie heeft gevraagd. Een ingang voor de tunnel zou in dit showbevel moeten zijn:

```
RP/0/RSP0/CPU0:PE1#show l2vpn atom-db preferred-path
Tunnel          BW Tot/Avail/Resv    Peer ID          VC ID
-----
tunnel-mte1 0/0/0                209.165.200.226  1
                                     209.165.200.227  1
                                     209.165.200.228  1
```

- L2VPN moet de tunnelinformatie van het te\_control proces ontvangen. Controleer dat dit showcommando niet-nul details heeft zoals tunnel-id, Ext.tunnel-id, tunnel-ifh en p2mp-id:

```
RP/0/RSP0/CPU0:PE1#show l2vpn atom-db preferred-path private
Tunnel tunnel-mte1 0/0/0:
Peer ID: 209.165.200.226, VC-ID 1
Peer ID: 209.165.200.227, VC-ID 1
Peer ID: 209.165.200.228, VC-ID 1
MTE details:
  tunnel-ifh: 0x08000e20
  local-label: 289994
  p2mp-id: 100
  tunnel-id: 100
  Ext.tunnel-id: 209.165.200.225
```

- L2VPN moet de Provider Multicast Service Instance (PMSI) adverteren naar alle andere PE routers. Controleer of l2vpn\_mgr de PMSI voor de geconfigureerde VFI heeft verzonden. Het evenement **LSM Head: stuur PMSI** moet aanwezig zijn in de geschiedenis van het evenement voor de VFI.

```
RP/0/0/CPU0:one#show l2vpn bridge-domain p2mp private
[...]
Object: VFI
Base info: version=0x0, flags=0x0, type=0, reserved=0
VFI event trace history [Num events: 5]
-----
Time          Event          Flags          Flags
====          =====          =====          =====
Dec  3 08:52:37.504 LSM Head: P2MP Provision 00000001, 00000000 - -
Dec  3 08:52:37.504 BD VPN Add          00000000, 00000000 M -
Dec  3 08:55:56.672 LSM Head: MTE updated  00000001, 00000000 - -
Dec  3 08:55:56.672 LSM Head: send PMSI 00000480, 00002710 - -
-----
[...]
```

- L2VPN op de andere routers moet de PMSI ontvangen die zojuist is verzonden. Zorg ervoor dat **LSM Tail: PMSI ontvangen** wordt getoond in de gebeurtenisgeschiedenis aan de ontvangende kant:

```
RP/0/0/CPU0:two#show l2vpn bridge-domain p2mp private
[...]
VFI event trace history [Num events: 7]
-----
Time          Event          Flags          Flags
====          =====          =====          =====
Dec  3 08:42:49.216 LSM Head: P2MP Provision 00000001, 00000000 - -
Dec  3 08:42:50.240 LSM Head: MTE updated  00000001, 00000070 - -
Dec  3 08:42:50.240 LSM Head: send PMSI 00000480, 00002710 - -
Dec  3 08:43:51.680 BD VPN Add          00000000, 00000000 - -
Dec  3 08:44:59.776 LSM Tail: PMSI received 0100a8c0, 00002710 - -
Dec  3 08:45:00.288 LSM Head: MTE updated  00000001, 00000000 - -
-----
[...]
```

- Elke router is zowel een LSM-hoofd als een staart en moet de PMSI versturen en PMSI's



ontvangen van elk van de andere routers. De eerste gecontroleerde router moet PMSI's van elk van de andere knooppunten ontvangen.

- Layer 2 Forwarding Information Base (L2FIB) moet de HEAD-informatie van L2VPN ontvangen en deze naar de lijnkaart downloaden.

```
RP/0/RSP0/CPU0:PE1#show l2vpn forwarding bridge-domain detail location 0/1/CPU0
```

```
Bridge-domain name: bg1:bg1_bd1, id: 0, 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
  MLD snooping: disabled, flooding: disabled
  Storm control: disabled
P2MP PW: enabled
Ptree type: RSVP-TE, TE i/f: tunnel-mte100,
nhop valid: TRUE, Status: Bound, Label: 289994
  Bridge MTU: 1500 bytes
  Number of bridge ports: 4
  Number of MAC addresses: 0
  Multi-spanning tree instance: 0
```

- L2FIB moet de TAIL-informatie van L2VPN voor elke PW ontvangen en moet deze naar het platform downloaden.

```
RP/0/RSP0/CPU0:PE1#show l2vpn forwarding bridge-domain hardware ingress detail location 0/1/CPU0
```

```
Bridge-domain name: bg1:bg1_bd1, id: 0, 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
  MLD snooping: disabled, flooding: disabled
  Storm control: disabled
  P2MP PW: enabled
  Ptree type: RSVP-TE, TE i/f: tunnel-mte100,
```

nhop valid: TRUE, Status: Bound, Label: 289994  
Bridge MTU: 1500 bytes  
Number of bridge ports: 4  
Number of MAC addresses: 0  
Multi-spanning tree instance: 0

Platform Bridge context:

Last notification sent at: 02/18/2014 21:58:55  
Ingress Bridge Domain: 0, State: Created  
static MACs: 0, port level static MACs: 0, MAC limit: 4000, current MAC limit:  
4000, MTU: 1500, MAC limit action: 0  
Rack 0 FGIDs:shg0: 0x00000000, shg1: 0x00000002, shg2: 0x00000002  
Rack 1 FGIDs:shg0: 0x00000000, shg1: 0x00000000, shg2: 0x00000000  
Flags: Virtual Table ID Disable, P2MP Enable, CorePW Attach  
P2MP Head-end Info: Head end bound  
Tunnel ifhandle: 0x08000e20, Internal Label: 289994, Local LC NP mask: 0x0,  
Head-end Local LC NP mask: 0x0, All L2 Mcast routes local LC NP mask: 0x0  
Rack: 0, Physical slot: 1, shg 0 members: 1, shg 1 members: 0, shg 2 members: 0

Platform Bridge HAL context:

Number of NPs: 4, NP mask: 0x0008, mgid index: 513, learn key: 0  
NP: 3, shg 0 members: 1, shg 1 members: 0, shg 2 members: 0  
MAC limit counter index: 0x00ecl60

Platform Bridge Domain Hardware Information:

Bridge Domain: 0 NP 0  
Flags: Virtual Table, Learn Enable, P2MP Tree Enabled  
Head-end P-Tree Int Label: 289994  
Num Members: 0, Learn Key: 0x00, Half Age: 5  
fgid shg0: 0x0000, fgid shg1: 0x0002, fgid shg2: 0x0002, mgid index: 513  
BD learn cntr: 0x00ecl60

Bridge Domain: 0 NP 1  
Flags: Virtual Table, Learn Enable, P2MP Tree Enabled  
Head-end P-Tree Int Label: 289994  
Num Members: 0, Learn Key: 0x00, Half Age: 5  
fgid shg0: 0x0000, fgid shg1: 0x0002, fgid shg2: 0x0002, mgid index: 513  
BD learn cntr: 0x00ecl60

Bridge Domain: 0 NP 2  
Flags: Virtual Table, Learn Enable, P2MP Tree Enabled  
Head-end P-Tree Int Label: 289994  
Num Members: 0, Learn Key: 0x00, Half Age: 5  
fgid shg0: 0x0000, fgid shg1: 0x0002, fgid shg2: 0x0002, mgid index: 513  
BD learn cntr: 0x00ecl60

Bridge Domain: 0 NP 3  
Flags: Virtual Table, Learn Enable, P2MP Tree Enabled  
Head-end P-Tree Int Label: 289994  
Num Members: 1, Learn Key: 0x00, Half Age: 5  
fgid shg0: 0x0000, fgid shg1: 0x0002, fgid shg2: 0x0002, mgid index: 513  
BD learn cntr: 0x00ecl60

Bridge Member 0, copy 0  
Flags: Active, XID: 0x06c002a7  
Bridge Member 0, copy 1  
Flags: Active, XID: 0x06c002a7

GigabitEthernet0/1/1/10.1, state: oper up

Number of MAC: 0

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  
Platform Bridge Port context:  
Last notification sent at: 02/18/2014 21:58:56  
Ingress State: Bound  
 Flags: None

Platform AC context:  
Ingress AC: VPLS, State: Bound  
 Flags: Port Level MAC Limit  
XID: 0x06c002a7, SHG: None  
uIDB: 0x001a, NP: 3, Port Learn Key: 0  
Slot flood mask rack 0: 0x200000 rack 1: 0x0 NP flood mask: 0x0008  
NP3

Ingress uIDB:  
 Flags: L2, Status, Racetrack Eligible, VPLS  
 Stats Ptr: 0x5302c9, uIDB index: 0x001a, Wire Exp Tag: 1  
 BVI Bridge Domain: 0, BVI Source XID: 0x00000000  
 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: 0x06c002a7  
 UIDB IF Handle: 0x02001042, Source Port: 0, Num VLANs: 0  
Xconnect ID: 0x06c002a7, NP: 3  
 Type: AC  
 Flags: Learn enable, VPLS  
 uIDB Index: 0x001a  
 Bridge Domain ID: 0, Stats Pointer: 0xec1e62  
 Split Horizon Group: None  
Bridge Port : Bridge 0 Port 0  
 Flags: Active Member  
 XID: 0x06c002a7  
Bridge Port Virt: Bridge 0 Port 0  
 Flags: Active Member  
 XID: 0x06c002a7  
Storm Control not enabled

Nbor 209.165.200.226 pw-id 1  
Number of MAC: 0  
Statistics:  
 packets: received 0, sent 2  
 bytes: received 0, sent 192  
Storm control drop counters:  
 packets: broadcast 2, multicast 0, unknown unicast 0  
 bytes: broadcast 192, multicast 0, unknown unicast 0  
Dynamic arp inspection drop counters:  
 packets: 0, bytes: 0  
IP source guard drop counters:  
 packets: 0, bytes: 0  
Statistics P2MP:  
 packets: received 0  
 bytes: received 0

Platform Bridge Port context:  
Last notification sent at: 02/18/2014 21:58:55  
Ingress State: Bound  
 Flags: None  
 **P2MP PW enabled, P2MP Role: tail**  
**Platform PW context:**  
**Ingress PW: VPLS, State: Bound**  
XID: 0xc0008000, bridge: 0, MAC limit: 4000, l2vpn ldi index: 0x0001, vc label:  
16030, nr\_ldi\_hash: 0xab, r\_ldi\_hash: 0xbd, lag\_hash: 0x17, SHG: VFI Enabled

Flags: MAC Limit Port Level  
Port Learn Key: 0  
Trident Layer Flags: None  
Slot flood mask rack 0: 0x0 rack 1: 0x0 NP flood mask: 0x0000  
Primary L3 path: ifhandle: 0x02000100, sfp\_or\_lagid: 0x00d2  
Backup L3 path: Not set  
NP0

Xconnect ID: 0xc0008000, NP: 0  
Type: Pseudowire (no control word)  
Flags: Learn enable, Type 5, Local replication, VPLS  
VC label hash, nR-LDI Hash: 0xab, R-LDI Hash: 0xb7, LAG Hash: 0x17,  
VC output label: 0x03e9e (16030), LDI: 0x0001, stats ptr: 0x00530258  
Bridge Domain ID: 0, Stats Pointer: 0xec1e62  
Split Horizon Group: VFI Enabled

NP1

Xconnect ID: 0xc0008000, NP: 1  
Type: Pseudowire (no control word)  
Flags: Learn enable, Type 5, Local replication, VPLS  
VC label hash, nR-LDI Hash: 0xab, R-LDI Hash: 0xb7, LAG Hash: 0x17,  
VC output label: 0x03e9e (16030), LDI: 0x0001, stats ptr: 0x00530258  
Bridge Domain ID: 0, Stats Pointer: 0xec1e62  
Split Horizon Group: VFI Enabled

NP2

Xconnect ID: 0xc0008000, NP: 2  
Type: Pseudowire (no control word)  
Flags: Learn enable, Type 5, Local replication, VPLS  
VC label hash, nR-LDI Hash: 0xab, R-LDI Hash: 0xb7, LAG Hash: 0x17,  
VC output label: 0x03e9e (16030), LDI: 0x0001, stats ptr: 0x00530300  
Bridge Domain ID: 0, Stats Pointer: 0xec1e62  
Split Horizon Group: VFI Enabled

NP3

Xconnect ID: 0xc0008000, NP: 3  
Type: Pseudowire (no control word)  
Flags: Learn enable, Type 5, Local replication, VPLS  
VC label hash, nR-LDI Hash: 0xab, R-LDI Hash: 0xb7, LAG Hash: 0x17,  
VC output label: 0x03e9e (16030), LDI: 0x0001, stats ptr: 0x00530488  
Bridge Domain ID: 0, Stats Pointer: 0xec1e64  
Split Horizon Group: VFI Enabled

Nbor 209.165.200.227 pw-id 1

Number of MAC: 0

Statistics:

packets: received 0, sent 1  
bytes: received 0, sent 96

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

Statistics P2MP:

packets: received 0  
bytes: received 0

Platform Bridge Port context:

Last notification sent at: 02/18/2014 21:58:55

Ingress State: Bound

Flags: None

**P2MP PW enabled, P2MP Role: tail**

**Platform PW context:**

**Ingress PW: VPLS, State: Bound**

XID: 0xc0008001, bridge: 0, MAC limit: 4000, l2vpn ldi index: 0x0002, vc label:  
16030, nr\_ldi\_hash: 0xab, r\_ldi\_hash: 0xbd, lag\_hash: 0x17, SHG: VFI Enabled

Flags: MAC Limit Port Level  
Port Learn Key: 0  
Trident Layer Flags: None  
Slot flood mask rack 0: 0x0 rack 1: 0x0 NP flood mask: 0x0000  
Primary L3 path: ifhandle: 0x02000100, sfp\_or\_lagid: 0x00d2  
Backup L3 path: Not set  
NP0

Xconnect ID: 0xc0008001, NP: 0  
Type: Pseudowire (no control word)  
Flags: Learn enable, Type 5, Local replication, VPLS  
VC label hash, nR-LDI Hash: 0xab, R-LDI Hash: 0xb7, LAG Hash: 0x17,  
VC output label: 0x03e9e (16030), LDI: 0x0002, stats ptr: 0x0053025e  
Bridge Domain ID: 0, Stats Pointer: 0xec1e64  
Split Horizon Group: VFI Enabled

NP1

Xconnect ID: 0xc0008001, NP: 1  
Type: Pseudowire (no control word)  
Flags: Learn enable, Type 5, Local replication, VPLS  
VC label hash, nR-LDI Hash: 0xab, R-LDI Hash: 0xb7, LAG Hash: 0x17,  
VC output label: 0x03e9e (16030), LDI: 0x0002, stats ptr: 0x0053025e  
Bridge Domain ID: 0, Stats Pointer: 0xec1e64  
Split Horizon Group: VFI Enabled

NP2

Xconnect ID: 0xc0008001, NP: 2  
Type: Pseudowire (no control word)  
Flags: Learn enable, Type 5, Local replication, VPLS  
VC label hash, nR-LDI Hash: 0xab, R-LDI Hash: 0xb7, LAG Hash: 0x17,  
VC output label: 0x03e9e (16030), LDI: 0x0002, stats ptr: 0x00530306  
Bridge Domain ID: 0, Stats Pointer: 0xec1e64  
Split Horizon Group: VFI Enabled

NP3

Xconnect ID: 0xc0008001, NP: 3  
Type: Pseudowire (no control word)  
Flags: Learn enable, Type 5, Local replication, VPLS  
VC label hash, nR-LDI Hash: 0xab, R-LDI Hash: 0xb7, LAG Hash: 0x17,  
VC output label: 0x03e9e (16030), LDI: 0x0002, stats ptr: 0x0053048e  
Bridge Domain ID: 0, Stats Pointer: 0xec1e66  
Split Horizon Group: VFI Enabled

Nbor 209.165.200.228 pw-id 1

Number of MAC: 0

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

Statistics P2MP:

packets: received 0

bytes: received 0

Platform Bridge Port context:

Last notification sent at: 02/18/2014 21:58:55

Ingress State: Bound

Flags: None

**P2MP PW enabled, P2MP Role: tail**

**Platform PW context:**

**Ingress PW: VPLS, State: Bound**

XID: 0xc0008002, bridge: 0, MAC limit: 4000, l2vpn ldi index: 0x0003, vc label:  
16045, nr\_ldi\_hash: 0x7b, r\_ldi\_hash: 0xb3, lag\_hash: 0xa8, SHG: VFI Enabled

Flags: MAC Limit Port Level  
Port Learn Key: 0  
Trident Layer Flags: None  
Slot flood mask rack 0: 0x0 rack 1: 0x0 NP flood mask: 0x0000  
Primary L3 path: ifhandle: 0x02000100, sfp\_or\_lagid: 0x00d2  
Backup L3 path: Not set  
NP0

Xconnect ID: 0xc0008002, NP: 0  
Type: Pseudowire (no control word)  
Flags: Learn enable, Type 5, Local replication, VPLS  
VC label hash, nR-LDI Hash: 0x7b, R-LDI Hash: 0xd6, LAG Hash: 0xa8,  
VC output label: 0x03ead (16045), LDI: 0x0003, stats ptr: 0x00530264  
Bridge Domain ID: 0, Stats Pointer: 0xec1e66  
Split Horizon Group: VFI Enabled

NP1

Xconnect ID: 0xc0008002, NP: 1  
Type: Pseudowire (no control word)  
Flags: Learn enable, Type 5, Local replication, VPLS  
VC label hash, nR-LDI Hash: 0x7b, R-LDI Hash: 0xd6, LAG Hash: 0xa8,  
VC output label: 0x03ead (16045), LDI: 0x0003, stats ptr: 0x00530264  
Bridge Domain ID: 0, Stats Pointer: 0xec1e66  
Split Horizon Group: VFI Enabled

NP2

Xconnect ID: 0xc0008002, NP: 2  
Type: Pseudowire (no control word)  
Flags: Learn enable, Type 5, Local replication, VPLS  
VC label hash, nR-LDI Hash: 0x7b, R-LDI Hash: 0xd6, LAG Hash: 0xa8,  
VC output label: 0x03ead (16045), LDI: 0x0003, stats ptr: 0x0053030c  
Bridge Domain ID: 0, Stats Pointer: 0xec1e66  
Split Horizon Group: VFI Enabled

NP3

Xconnect ID: 0xc0008002, NP: 3  
Type: Pseudowire (no control word)  
Flags: Learn enable, Type 5, Local replication, VPLS  
VC label hash, nR-LDI Hash: 0x7b, R-LDI Hash: 0xd6, LAG Hash: 0xa8,  
VC output label: 0x03ead (16045), LDI: 0x0003, stats ptr: 0x00530494  
Bridge Domain ID: 0, Stats Pointer: 0xec1e68  
Split Horizon Group: VFI Enabled

RP/0/RSP0/CPU0:PE1#

## Over deze vertaling

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