ASR 9000 - Comprensione e configurazione di VPLS LSM

Sommario

Introduzione

In questo documento viene descritto il servizio VPLS (Virtual Private LAN Service) Label Switched Multicast (LSM) per il router ASR (Aggregation Services Router) serie 9000 con software Cisco IOS® XR.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

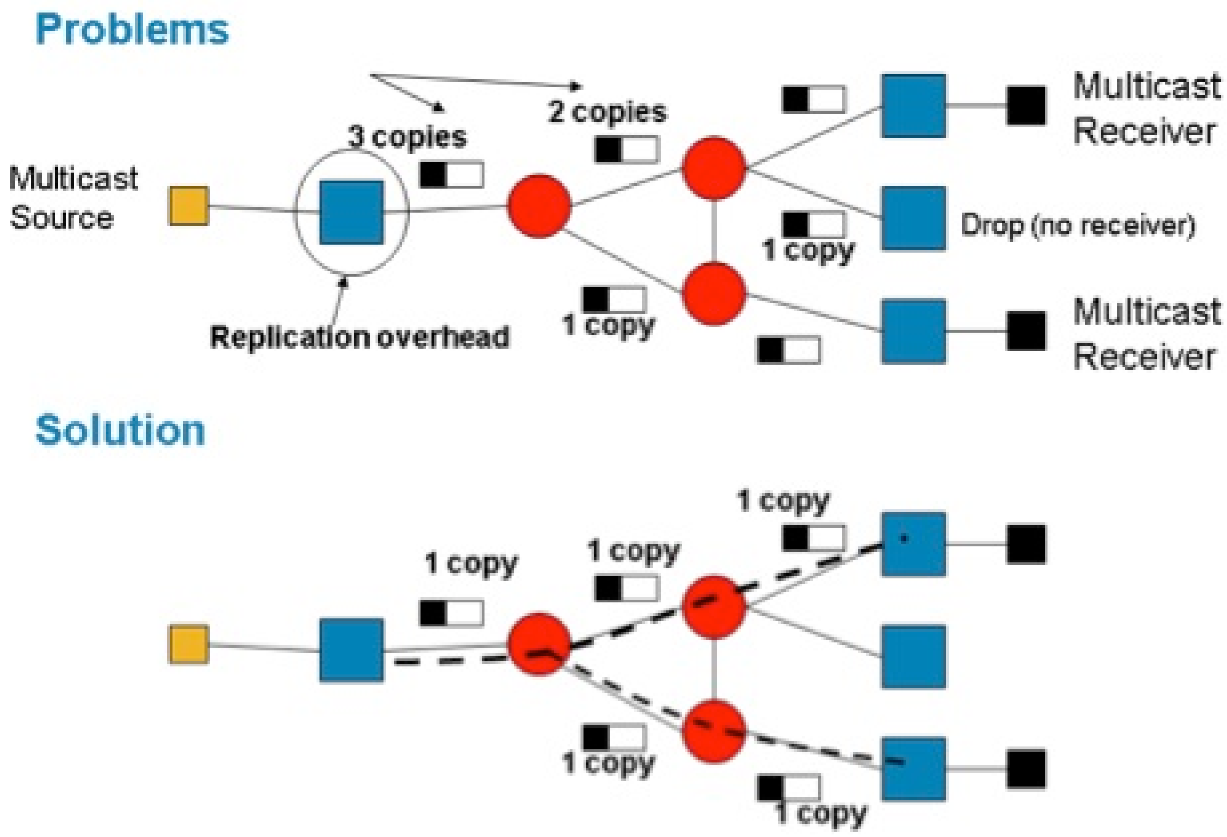
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica di VPLS Label Switched Multicast (LSM)

VPLS emula i servizi LAN su un core Multiprotocol Label Switching (MPLS). Tra tutti i router Provider Edge (PE) che partecipano a un dominio VPLS viene configurata una rete completa di pseudofili (PW) point-to-point (P2P) per fornire l'emulazione VPLS. Il traffico broadcast, multicast e unicast sconosciuto viene inondato in un dominio VPLS a tutti i PE. La replica in ingresso viene utilizzata per inviare il traffico di flooded su ogni PW P2P a tutti i router PE remoti che fanno parte dello stesso dominio VPLS.

Svantaggi della replica in ingresso

- La replica in ingresso non è efficiente a livello di larghezza di banda, in quanto lo stesso pacchetto potrebbe essere inviato più volte sullo stesso collegamento per ogni PW P2P.
- La replica in ingresso può comportare uno spreco significativo della larghezza di banda del collegamento in caso di traffico broadcast e multicast VPLS elevato.
- Anche la replica in ingresso richiede un uso intensivo delle risorse, in quanto il router PE in entrata sopporta l'intero carico della replica.



Funzioni VPLS LSM

VPLS è una tecnologia L2VPN ampiamente implementata dal provider di servizi che viene utilizzata anche per il trasporto multicast. Sebbene la tecnologia L2 consenta l'utilizzo dello snooping per ottimizzare la replica del traffico multicast negli alimentatori L2, il core rimane indipendente dal traffico multicast. Di conseguenza, più copie dello stesso flusso attraversano le reti principali. Per ridurre questa inefficienza, abbinare LSM a VPLS in modo da introdurre gli alberi multicast LSM nel core. Nel software Cisco IOS-XR versione 5.1.0, Cisco ASR serie 9000 implementa VPLS LSM con alberi inclusivi di progettazione del traffico point-to-multipoint (P2MP-TE). Gli endpoint VPLS vengono rilevati automaticamente e gli alberi P2MP-TE vengono impostati con l'utilizzo di Resource Reservation Protocol Traffic Engineering (RSVP-TE) senza alcun intervento operativo.

- VPLS LSM consente di superare gli inconvenienti della replica in entrata.
- La soluzione LSM VPLS impiega LSP P2MP nel core MPLS per trasportare il traffico broadcast, multicast e unicast sconosciuto per un dominio VPLS.
- I provider di servizi di traduzione P2MP consentono la replica nella rete MPLS al nodo ottimale e riducono al minimo la quantità di replica dei pacchetti nella rete.
- La soluzione VPLS LSM invia solo il traffico VPLS in modalità flooded sugli LSP P2MP.
- Il traffico VPLS unicast viene ancora inviato sui PW P2P. Il traffico inviato tramite i PW di accesso continua a essere inviato con la replica in entrata.
- I PW P2MP sono unidirezionali rispetto ai PW P2P, che sono bidirezionali.

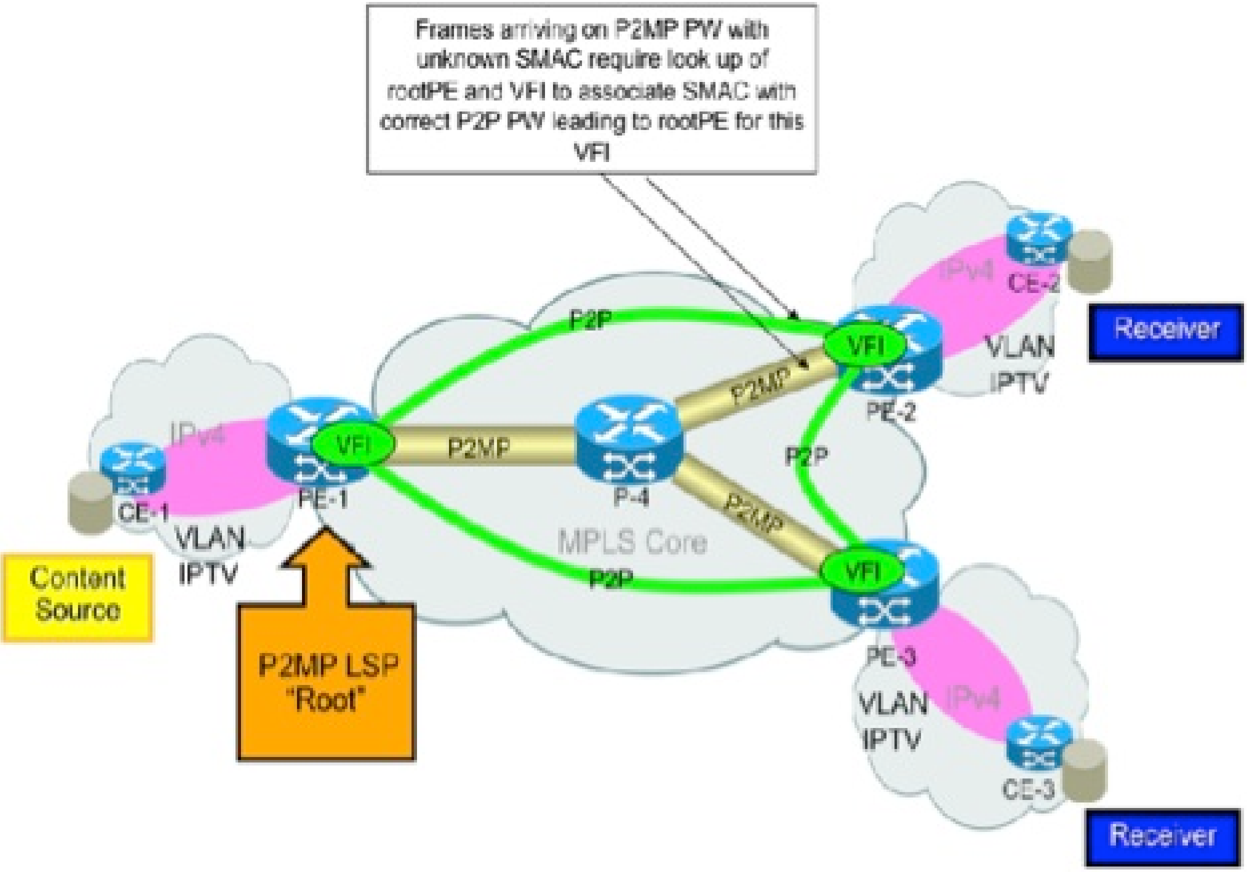
- La soluzione VPLS LSM implica la creazione di una PW P2MP per dominio VPLS al fine di emulare un servizio P2MP VPLS per i PW di base nel dominio VPLS.
- VPLS LSM è supportato in Cisco IOS XR versione 5.1.0 e successive.

Restrizioni VPLS LSM

- Cisco IOS-XR release 5.1.0 VPLS LSM supporta solo alberi P2MP-TE di progettazione del traffico MPLS configurati con RSVP-TE.
- Una PW P2MP può essere segnalata con il protocollo BGP solo in Cisco IOS-XR release 5.1.0. In questa prima fase, i PE remoti che partecipano al dominio VPLS vengono rilevati automaticamente con BGP Auto-Discovery (BGP-AD).
- La segnalazione LDP statica non è supportata in Cisco IOS XR versione 5.1.0.

Apprendimento MAC (Media Access Control)

L'apprendimento MAC sul PW foglia per un frame che arriva sul PW P2MP viene eseguito come se il frame fosse ricevuto sul PW P2P che porta al PW radice per quel PW P2MP. In questa immagine, MAC Learning su PE-2 per i frame che arrivano su P2MP PW LSP con radice in PE-1 viene eseguito come se il frame arrivasse su P2P PW tra PE-1 e PE-2. Il control plane L2VPN è responsabile della programmazione delle informazioni di disposizione VPLS con informazioni PW P2P per l'apprendimento MAC sulla disposizione LSP P2MP.


Frames arriving on P2MP PW with unknown SMAC require look up of rootPE and VFI to associate SMAC with correct P2P PW leading to rootPE for this VFI
IPv4
CE-2
Receiver
VLAN
IPTV
P2P
VFI
P2MP
PE-2
IPv4
VFI
P2MP
CE-1
PE-1
P-4
P2P
VLAN
IPTV
MPLS Core
P2MP
Content Source
P2P
VFI
P2MP LSP "Root"
PE-3
VLAN
IPTV
IPv4
CE-3
Receiver

Supporto IGMPSN (Internet Group Management Protocol Snooping)

Lo snooping IGMP (Internet Group Management Protocol) (IGMPSN) è supportato sia sulla parte iniziale che finale dell'albero P2MP in un dominio bridge che partecipa a VPLS LSM. In questo modo, il traffico multicast IGMPSN su PW di un'istanza di inoltro virtuale (VFI) può trarre vantaggio dall'ottimizzazione delle risorse fornita dai PSP P2MP. Se IGMPSN è abilitato in un dominio bridge con una o più PW VFI che partecipano a VPLS LSM, tutto il traffico multicast di livello due (L2) viene inviato sulla testa P2MP dell'albero associato al dominio bridge. Le route multicast L2 vengono utilizzate per inoltrare il traffico ai ricevitori locali, ai punti di flusso Ethernet (EFP), ai PW di accesso e ai PW VFI che non partecipano al modulo LSM VPLS.

Quando IGMPSN è abilitato in un dominio bridge che è una coda LSP P2MP, la disposizione ottimizzata del traffico multicast L2 ricevuto sull'LSP P2MP viene effettuata per i ricevitori locali (cioè, porte Bridge (BP) del circuito di collegamento (AC) e accesso ai BP del PW).

> **Nota**: lo snooping MLDP (Multicast Label Distribution Protocol) non è supportato in Cisco IOS XR release 5.1.0.

Scala supportata

Cisco IOS XR release 5.1.0 supporta un massimo di **1000** tunnel P2MP o **1000** PW P2MP per router head/tail.

Configurazione VPLS LSM

Configurazione automatica tunnel P2MP

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

Configurazione MPLS TE Fast Reroute (FRR)

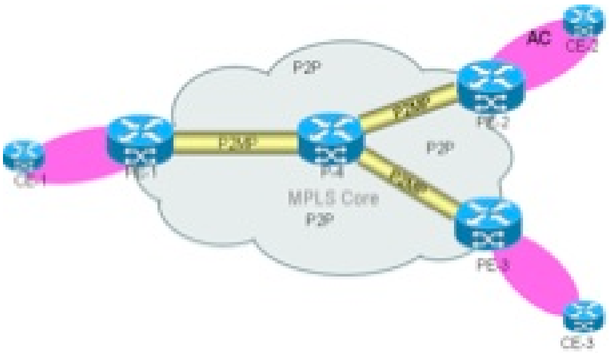
```
mpls traffic-eng
 interface GigabitEthernet0/1/1/0
 auto-tunnel backup
  nhop-only
 !
 !
 interface GigabitEthernet0/1/1/1
 auto-tunnel backup
```

```
  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
 !
```

Configurazione L2VPN

```
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
    !
```

Topologia e configurazione di esempio



I tunnel P2MP sono tunnel rilevati automaticamente. I tunnel P2MP statici **non** sono supportati.

Non vengono utilizzate configurazioni di tunnel statici. La configurazione automatica del tunnel P2MP deve essere abilitata su tutti i router PE e anche su un router IP se funge da nodo bud. Un nodo build è un router intermedio e allo stesso tempo un router terminale.

Di seguito è riportato un esempio di topologia con configurazione. In questa topologia, i PW P2MP vengono creati tra i tre PE e un router IP che funge da nodo bud. I tre router PE fungono da testa (per il traffico in entrata) e coda (per il traffico in uscita).

Configurazione PE1

```
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#
```

P Configurazione

```
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
 !
 !
 mpls traffic-eng router-id 209.165.200.226
```

```
!
router bgp 100
 nsr
 bgp router-id 209.165.200.226
 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 209.165.200.227
 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 GigabitEthernet0/1/1/4.1
  !
  vfi bg1_bd1_vfi
   vpn-id 1
   autodiscovery bgp
    rd auto
    route-target 209.165.201.1:1
    signaling-protocol bgp
     ve-id 200
    !
   !
   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
 !
 interface GigabitEthernet0/1/1/3
 bandwidth 100000
 !
 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#
```

Configurazione PE2

```
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#
```

Configurazione PE3

```
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#
```

Verifica - Mostra comandi

Questi comandi show sono utili per eseguire il debug e verificare lo stato dei tunnel P2MP PW e P2MP MPLS TE.

- **show l2vpn bridge-domain**
- **show l2vpn bridge-domain detail**
- **show mpls traffic-eng tunnels p2mp**
- **mostra dettagli <label> etichette di inoltro mpls**
- **show mpls traffic-eng tunnels p2mp tabulare**

Seguono alcuni esempi:

```
 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: bg1, bridge-domain: bg1_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_bd1_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-mte100 (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  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    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, Expnullv4:not-set, Expnullv6: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&colon;{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   LSP     Destination          Source          FRR  LSP  Path
            Name    ID         Address         Address  State  State Role  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#
```

Risoluzione dei problemi di VPLS LSM

Problemi comuni di configurazione

Di seguito sono indicate le cause più comuni dei problemi P2MP in L2VPN.

- La configurazione BGP per LSM è esattamente la stessa di BGP-AD. Accertarsi di esportare/importare le route della famiglia di indirizzi l2vpn vpls-vpws configurando le route della famiglia di indirizzi **l2vpn vpls-vpws** per i router adiacenti BGP.

- Errori di configurazione MPLS e multicast.

  MPLS Traffic Engineering deve essere abilitato sulle interfacce su cui passano i PW P2MP.

  ```
  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
  ```

- La configurazione L2VPN per LSM in Cisco IOS XR release 5.1.0 richiede quanto segue:

  Configurare la configurazione dell'ID VPN per la VFIConfigurare il protocollo IP2MP multicast per la VFI. Configurare il protocollo di trasporto e il protocollo di segnalazione, come nell'esempio seguente:

```
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
```

- La testa/coda dell'LSM deve essere impostata correttamente. In Cisco IOS XR release 5.1.0, ogni coda LSM è anche una testa LSM e viceversa. Poiché non vi è scambio esplicito di **funzionalità LSM** tra i router, tutti i router di un dominio bridge abilitato a LSM devono partecipare a LSM.

Comandi L2VPN e L2FIB Show e risoluzione dei problemi

- Il processo di gestione L2VPN (l2vpn_mgr) comunica con il processo di controllo MPLS Traffic Engineering (TE) (te_control) e richiede la creazione del tunnel. Verificare che i processi te_control e l2vpn_mgr siano in esecuzione con i seguenti comandi:
  show process l2vpn_mgrshow process te_control

- Verificare che il processo l2vpn_mgr abbia richiesto la creazione del tunnel. Una voce per il tunnel deve essere in questo comando show:

```
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 deve ricevere le informazioni sul tunnel dal processo te_control. Verificare che il comando show abbia dettagli diversi da zero, ad esempio tunnel-id, Ext.tunnel-id, tunnel-ifh e 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 deve annunciare l'istanza del servizio multicast del provider (PMSI) a tutti gli altri router PE. Verificare che l2vpn_mgr abbia inviato il PMSI per la VFI configurata. L'**intestazione LSM dell'**evento**: invio PMSI** deve essere presente nella cronologia degli eventi per la 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 sugli altri router deve ricevere il PMSI appena inviato. Verificare che **coda LSM: il PMSI ricevuto** venga visualizzato nella cronologia eventi sul lato ricevente:

```
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 -  -
  ----------------------------------------------------------------------------
[...]
```

- Ciascun router è sia testa che coda LSM e deve inviare il PMSI e ricevere i PMSI da ciascuno degli altri router. Il primo router controllato deve ricevere i PMSI da ciascuno degli altri nodi.

- L2FIB (Layer Two Forwarding Information Base) deve ricevere le informazioni HEAD da L2VPN e scaricarle nella scheda di linea.

```
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 deve ricevere le informazioni TAIL da L2VPN per ogni PW e deve scaricarle sulla piattaforma.

```
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: 0x00ec1e60

    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: 0x00ec1e60
      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: 0x00ec1e60
      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: 0x00ec1e60
      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: 0x00ec1e60
        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#
```