Exemple d'aperçu et de configuration de la Multidiffusion commuté par étiquette ASR 9000 VPLS (LSM)

Contenu

Introduction

Ce document décrit la Multidiffusion commutée par étiquette privée virtuelle du service réseau local (VPLS) (LSM) pour la gamme 9000 du routeur de services d'agrégation (ASR) qui exécutent le logiciel du Cisco IOS® XR.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Aperçu de la Multidiffusion commuté par étiquette VPLS (LSM)

VPLS émule des services de RÉSEAU LOCAL à travers un noyau de Commutation multiprotocole par étiquette (MPLS). Un maillage complet des pseudowires point par point (de P2P) (PWs) est installé entre tous les Routeurs de Provider Edge (PE) qui participent à un domaine VPLS afin de fournir l'émulation VPLS. L'émission, la Multidiffusion, et le trafic unicast inconnu est inondée dans un domaine VPLS à tout le siège potentiel d'explosion. La réplication d'entrée est utilisée afin d'envoyer ce trafic propagé au-dessus de chaque P2P PWs à tous les Routeurs distants de PE qui font partie du même domaine VPLS.

Inconvénients de réplication d'entrée

- La réplication d'entrée est bande passante inefficace parce que le même paquet pourrait être envoyé de plusieurs périodes au-dessus du même lien pour chaque P2P picowatt.
- La réplication d'entrée peut avoir comme conséquence la bande passante gaspillée significative de lien quand il y a du trafic lourd d'émission et de Multidiffusion VPLS.
- La réplication d'entrée est également ressource-intensive parce que le routeur PE d'entrée soutient la pleine charge de la réplication.

Caractéristiques VPLS LSM

VPLS est une technologie large-déployée de L2VPN de fournisseur de services qui est également utilisée pour le transport de Multidiffusion. Bien que la technologie L2 permette piller à utiliser afin d'optimiser la réplication du trafic de multidiffusion dans les pseudowires L2, le noyau demeure agnostique au trafic de multidiffusion. En conséquence, les plusieurs copies de la même traversée d'écoulement creusent des réseaux. Afin d'atténuer cette inefficacité, paires LSM avec VPLS afin d'introduire des arbres de multicast LSM au-dessus du noyau. Dans le Logiciel Cisco IOS XR libérez 5.1.0, la mise en place de gamme 9000 de Cisco ASR VPLS LSM avec les arborescences incluses point-à-multipoint de l'ingénierie de trafic (P2MP-TE). Des points d'extrémité VPLS sont automatiquement découverts et des arborescences P2MP-TE sont installées avec l'utilisation de l'ingénierie du trafic de protocole de RSVP (RSVP-TE) sans intervention opérationnelle.

- VPLS LSM surmonte les inconvénients de la réplication d'entrée.
- La solution VPLS LSM utilise P2MP LSP dans le noyau MPLS afin de porter l'émission, la Multidiffusion, et le trafic unicast inconnu pour un domaine VPLS.
- P2MP LSP permettent la réplication dans le noeud optimal de réseau MPLS tout au plus et réduisent la quantité de réplication de paquet dans le réseau.
- La solution VPLS LSM envoie seulement le trafic inondé VPLS au-dessus de P2MP LSP.
- Le trafic d'Unicast VPLS est encore envoyé au-dessus du P2P PWs. Le trafic envoyé au-dessus d'Access PWs continue à être envoyé avec la réplication d'entrée.
- P2MP PWs sont unidirectionnels par opposition au P2P PWs, qui sont bidirectionnels.
- La solution VPLS LSM comporte la création d'un P2MP picowatt par domaine VPLS afin d'émuler un service VPLS P2MP pour principal PWs dans le domaine VPLS.
- VPLS LSM est pris en charge dans la version 5.1.0 et ultérieures de Cisco IOS XR.

Restrictions VPLS LSM

- La fonctionnalité de la version 5.1.0 VPLS LSM de Cisco IOS XR prend en charge seulement des arborescences de l'Ingénierie de trafic MPLS P2MP-TE installées avec RSVP-TE.
- UN P2MP picowatt peut être signalé avec le protocole BGP seulement dans la version 5.1.0 de Cisco IOS XR. Dans cette première phase, le siège potentiel d'explosion distant qui participent au domaine VPLS automatique-sont découverts avec la détection automatique BGP (BGP-AD).
- La signalisation statique LDP n'est pas prise en charge dans la version 5.1.0 de Cisco IOS XR.

Apprendre de Contrôle d'accès au support (MAC)

Le MAC apprenant sur le PE de feuille d'une trame qui arrive sur P2MP picowatt est fait comme si la trame est reçue sur le P2P picowatt menant au PE de racine pour cela P2MP picowatt. Dans cette image, le MAC apprenant sur PE-2 des trames qui arrivent sur le P2MP LE picowatt LSP enraciné à PE-1 est fait comme si la trame est arrivée sur le P2P picowatt entre PE-1 et PE-2. L'avion de contrôle de L2VPN est responsable de programmer les informations de disposition VPLS avec les informations picowatt de P2P pour le MAC apprenant sur la disposition P2MP LSP.

Support pillant de protocole de gestion de groupes Internet (IGMP) (IGMPSN)

Le Protocole IGMP (Internet Group Management Protocol) pillant (IGMPSN) est pris en charge sur

chacun des deux la circulaire de la P-arborescence P2MP dans un domaine de passerelle qui participe à VPLS LSM. Ceci permet au trafic de multidiffusion IGMPSN au-dessus d'une instance de transfert virtuelle (VFI) PWs pour tirer bénéfice de l'optimisation de ressource fournie par P2MP LSP. S'IGMPSN est activé dans un domaine de passerelle avec un ou plusieurs VFI PWs participant à VPLS LSM, tout les trafic de multidiffusion de la couche deux (L2) est envoyé au-dessus de la tête de P-arborescence P2MP associée avec le domaine de passerelle. Les routes multicasts L2 sont utilisées afin d'expédier le trafic aux récepteurs locaux, des Ethernets circulent les points (EFP), l'accès PWs, et les VFI PWs qui ne participent pas à VPLS LSM.

Quand IGMPSN est activé dans un domaine de passerelle qui est une queue P2MP LSP, la disposition optimisée du trafic de multidiffusion L2 reçue sur le P2MP LSP est faite pour les récepteurs locaux (c'est-à-dire, ports de passerelle de circuit de connexion (courant alternatif) (bps) et l'accès picowatt bps).

> Remarque: Le protocole de distribution d'étiquette de Multidiffusion (MLDP) pillant n'est pas pris en charge dans la version 5.1.0 de Cisco IOS XR.

Échelle prise en charge

La version 5.1.0 de Cisco IOS XR prend en charge un maximum de 1000 tunnels ou de 1000 P2MP PWs P2MP par personne/routeur de queue.

Configuration VPLS LSM

Configuration automatique de tunnel P2MP

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

MPLS TE rapide reroutent la configuration (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
 !
```

Configuration de 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
    !
```

Exemple de topologie et configuration

Les tunnels P2MP sont les tunnels automatique-découverts. Des tunnels statiques P2MP ne sont pas pris en charge.

Des configurations statiques de tunnel ne sont pas utilisées. La configuration de tunnel de l'automatique P2MP doit être activée sur tous les Routeurs de PE et également sur un routeur P si elle agit en tant que noeud de bourgeon. Un noeud de bourgeon est un routeur de point médian et de tailend en même temps.

Un exemple de topologie avec la configuration est affiché ici. Dans cette topologie, P2MP PWs sont créés entre le siège potentiel d'explosion trois et un routeur P qui agit en tant que noeud de bourgeon. Chacun des trois Routeurs de PE agit en tant que tête (pour le trafic entrant) et queue (pour le trafic en sortie).

Configuration 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#
```

Configuration P

```
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#
```

Configuration 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#
```

Configuration 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#
```

Vérifiez - Commandes show

Ces commandes show sont utiles afin de mettre au point et vérifier l'état des tunnels P2MP picowatt et P2MP MPLS TE.

- affichez le bridge-domain de l2vpn
- affichez le détail de bridge-domain de l2vpn
- show mpls traffic-eng tunnels p2mp
- le show mpls forwarding étiquette le détail de <label>
- show mpls traffic-eng tunnels p2mp tabulaire

Voici quelques exemples :

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 <label> 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#
```

Dépannez VPLS LSM

Questions communes de configuration

Les la plupart des causes classiques pour des problèmes P2MP dans le L2VPN sont affichées ici.

- La configuration BGP pour LSM est exactement identique que celle pour BGP-AD. Veillez à exporter/des artères de famille d'adresse de vpls-vpws l2vpn d'importation en configurant des **vpls-vpws d'address-family l2vpn** pour des voisins BGP.

- Il y a MPLS et erreurs de configuration de Multidiffusion.

  L'Ingénierie de trafic MPLS doit être activée sur les interfaces où le P2MP PWs passe.

  ```
  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 configuration de L2VPN pour LSM dans la version 5.1.0 de Cisco IOS XR exige que vous :

  Configurez la configuration de VPN ID pour le VFIConfigurez la Multidiffusion P2MP pour le VFI. Confgure le protocole de transport et le protocole de signalisation, configuration de comme indiqué dans cet exemple :`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 tête/queue LSM doit être placée correctement. Dans le Cisco IOS XR libérez 5.1.0, chaque queue LSM est également une tête LSM et vice-versa. Puisqu'il n'y a aucun échange explicite de **capacité LSM** parmi des Routeurs, tous les Routeurs dans un domaine de passerelle activé par LSM doivent participer à LSM.

Les commandes show de L2VPN et L2FIB et dépannent

- Le processus maître de L2VPN (l2vpn_mgr) communique avec le processus de contrôle de l'Ingénierie de trafic MPLS (TE) (te_control) et demande la création de tunnel. Assurez-vous que le te_control et les processus l2vpn_mgr sont dans l'état courant avec ces commandes : **affichez l2vpn_mgr de processusaffichez le te_control de processus**

- Vérifiez que le processus l2vpn_mgr a demandé la création de tunnel. Une entrée pour le tunnel devrait être dans cette commande 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
```

- Le L2VPN doit recevoir les informations de tunnel du processus de te_control. Vérifiez que cette commande show a les détails différents de zéro tels que le tunnel-id, l'Ext.tunnel-id, le tunnel-ifh, et le 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
```

- Le L2VPN doit annoncer le service instance de Multidiffusion de fournisseur (PMSI) à tous autres Routeurs de PE. Vérifiez que l2vpn_mgr a envoyé le PMSI pour le VFI configuré. **La tête de l'**événement **LSM : envoyez PMSI** devrait être en cas l'historique actuel pour le 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 -  -
  ------------------------------------------------------------------------
[...]
```

- Le L2VPN sur les autres Routeurs devrait recevoir le PMSI qui a été juste envoyé. Assurez-vous que **queue LSM : PMSI reçu** est affiché en cas l'historique du côté réception :

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

- Chaque routeur est une circulaire LSM et devrait envoyer le PMSI et recevoir PMSIs de chacun des autres Routeurs. Le premier routeur vérifié devrait recevoir PMSIs de chacun des autres Noeuds.

- Le Forwarding Information Base de la couche deux (L2FIB) doit recevoir les informations PRINCIPALES du L2VPN et doit les télécharger au linecard.

```
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 doit recevoir les informations de QUEUE du L2VPN pour chaque picowatt et doit les télécharger à la plate-forme.

```
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#
```