

ASR 9000 - Entender e configurar VPLS LSM

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Visão geral do VPLS Label Switched Multicast \(LSM\)](#)

[Desvantagens da replicação de entrada](#)

[Recursos de VPLS LSM](#)

[Restrições de VPLS LSM](#)

[Aprendizado de Controle de Acesso ao Meio \(MAC - Media Access Control\)](#)

[Suporte a Internet Group Management Protocol Snooping \(IGMPSN\)](#)

[Escala suportada](#)

[Configuração de VPLS LSM](#)

[Configuração de túnel automático P2MP](#)

[Configuração de redirecionamento rápido \(FRR - Fast Reroute\) MPLS TE](#)

[Configuração de L2VPN](#)

[Exemplo de topologia e configuração](#)

[Configuração de PE1](#)

[Configuração P](#)

[Configuração do PE2](#)

[Configuração de PE3](#)

[Verificar - Comandos show](#)

[Identificar e Solucionar Problemas do LSM do VPLS](#)

[Problemas comuns de configuração](#)

[Comandos Show e Troubleshooting de L2VPN e L2FIB](#)

Introduction

Este documento descreve o Virtual Private LAN Service (VPLS) Label Switched Multicast (LSM) para o Aggregation Services Router (ASR) 9000 Series que executa o software Cisco IOS[®] XR.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

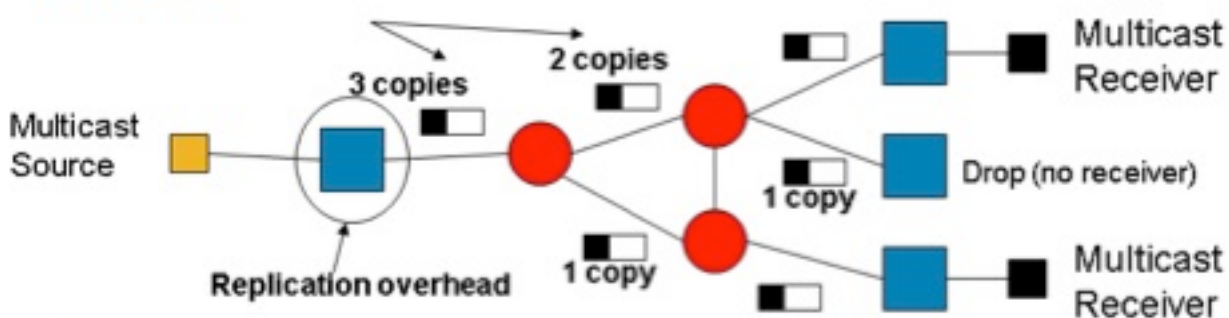
Visão geral do VPLS Label Switched Multicast (LSM)

O VPLS emula serviços de LAN através de um núcleo de Multiprotocol Label Switching (MPLS). Uma malha completa de pseudofios (PWs) ponto-a-ponto (P2P) é configurada entre todos os roteadores da Borda do Provedor (PE) que participam de um domínio VPLS para fornecer emulação de VPLS. O tráfego de broadcast, multicast e unicast desconhecido é enviado em um domínio VPLS para todos os PEs. A replicação de entrada é usada para enviar esse tráfego inundado em cada PWs P2P para todos os roteadores PE remotos que fazem parte do mesmo domínio VPLS.

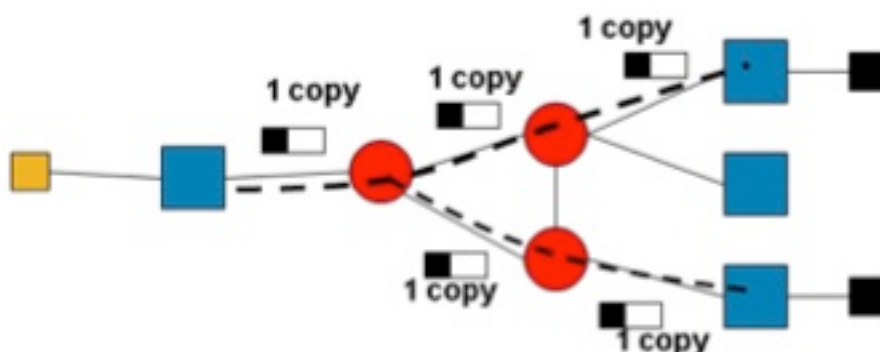
Desvantagens da replicação de entrada

- A replicação de entrada é ineficiente em termos de largura de banda porque o mesmo pacote pode ser enviado várias vezes sobre o mesmo link para cada PW P2P.
- A replicação de ingresso pode resultar em um desperdício significativo da largura de banda do link quando há tráfego pesado de VPLS de broadcast e multicast.
- A replicação de entrada também exige muitos recursos, pois o roteador PE de entrada suporta toda a carga da replicação.

Problems



Solution



Recursos de VPLS LSM

O VPLS é uma tecnologia L2VPN de provedor de serviços amplamente implantada que também é usada para transporte multicast. Embora a tecnologia L2 permita que o snooping seja usado para otimizar a replicação do tráfego multicast em pseudofios L2, o núcleo permanece independente do tráfego multicast. Como resultado, várias cópias do mesmo fluxo passam pelas redes centrais. Para atenuar essa ineficiência, emparelhe o LSM com o VPLS para introduzir árvores multicast LSM sobre o núcleo. No Cisco IOS-XR Software Release 5.1.0, o Cisco ASR 9000 Series implementa VPLS LSM com árvores inclusivas de P2MP-TE (Point-to-Multipoint Traffic Engineering). Terminais VPLS são automaticamente descobertos e árvores P2MP-TE são configuradas com o uso de Resource Reservation Protocol Traffic Engineering (RSVP-TE) sem intervenção operacional.

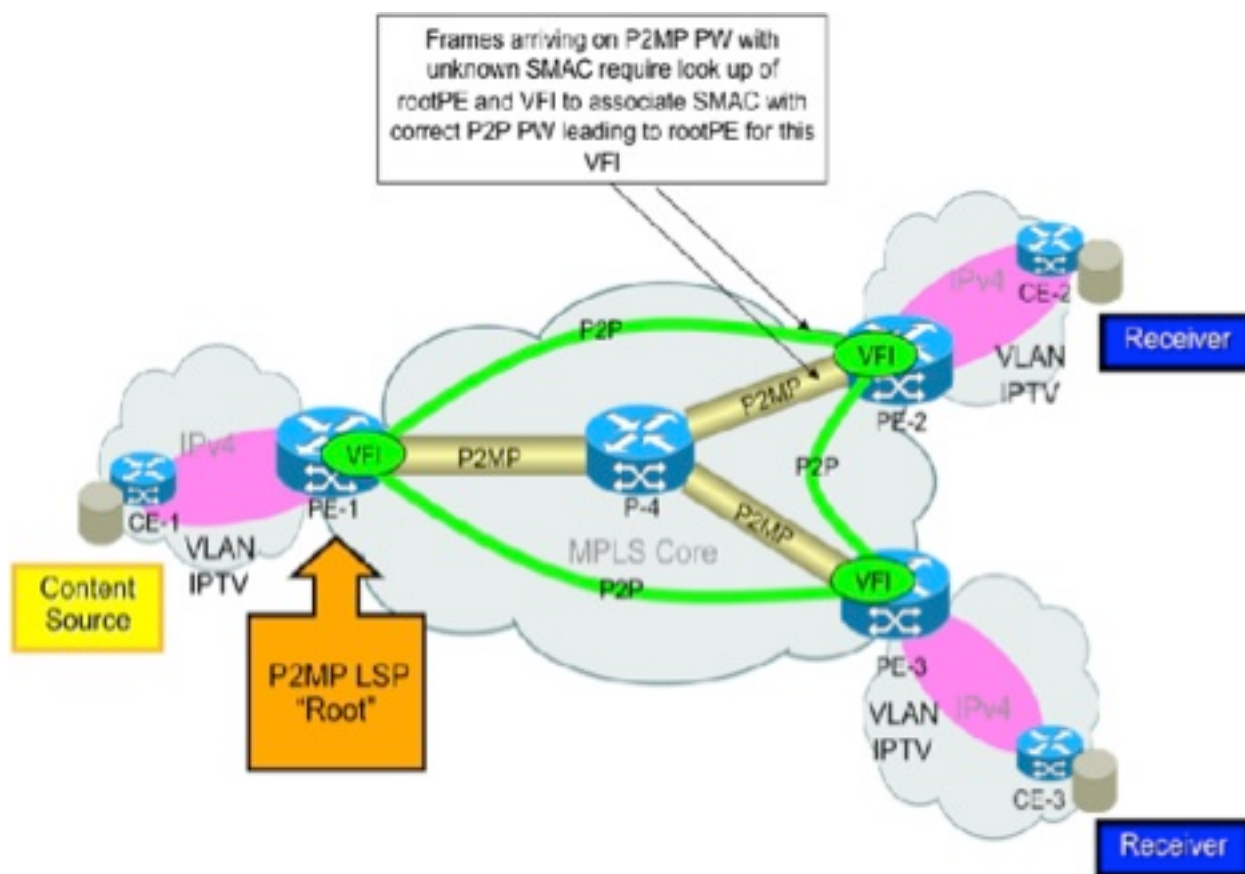
- O LSM do VPLS supera as desvantagens da replicação de entrada.
- A solução LSM VPLS emprega LSPs P2MP no núcleo MPLS para transportar tráfego de broadcast, multicast e unicast desconhecido para um domínio VPLS.
- Os LSPs P2MP permitem a replicação na rede MPLS no nó ideal e minimizam a quantidade de replicação de pacotes na rede.
- A solução LSM VPLS envia apenas tráfego VPLS inundado sobre LSPs P2MP.
- O tráfego VPLS unicast ainda é enviado sobre PWs P2P. O tráfego enviado por PWs de acesso continua a ser enviado com replicação de entrada.
- Os PWs P2MP são unidirecionais, ao contrário dos PWs P2P, que são bidirecionais.
- A solução VPLS LSM envolve a criação de um PW P2MP por domínio VPLS para emular um serviço P2MP VPLS para PWs centrais no domínio VPLS.
- O VPLS LSM é suportado no Cisco IOS XR Release 5.1.0 e posterior.

Restrições de VPLS LSM

- A funcionalidade do Cisco IOS-XR Release 5.1.0 VPLS LSM suporta apenas árvores P2MP-TE de Engenharia de Tráfego MPLS configuradas com RSVP-TE.
- Um PW P2MP pode ser sinalizado com o protocolo BGP somente no Cisco IOS-XR Release 5.1.0. Nesta primeira fase, os PEs remotos que participam do domínio VPLS são descobertos automaticamente com a Descoberta Automática BGP (BGP-AD).
- A sinalização LDP estática não é suportada no Cisco IOS XR Release 5.1.0.

Aprendizado de Controle de Acesso ao Meio (MAC - Media Access Control)

O aprendizado de MAC no PE de folha para um quadro que chega no PW P2MP é feito como se o quadro fosse recebido no PW P2P levando ao PE de raiz para esse PW P2MP. Nesta imagem, o MAC Learning em PE-2 para quadros que chegam ao P2MP PW LSP enraizado em PE-1 é feito como se o quadro chegasse ao P2P PW entre PE-1 e PE-2. O plano de controle L2VPN é responsável por programar as informações de disposição do VPLS com informações P2P PW para aprendizagem MAC na disposição P2MP LSP.



Suporte a Internet Group Management Protocol Snooping (IGMPSN)

O Internet Group Management Protocol (IGMP) Snooping (IGMPSN) é suportado no início e no fim da árvore P2MP em um domínio de bridge que participa do LSM VPLS. Isso permite que o tráfego multicast IGMPSN em um PWs de instância de encaminhamento virtual (VFI) se beneficie da otimização de recursos fornecida por LSPs P2MP. Se o IGMPSN estiver habilitado em um domínio de bridge com um ou mais PWs de VFI participando do LSM do VPLS, todo o tráfego multicast da camada dois (L2) será enviado pelo P2MP P-tree Head associado ao domínio de bridge. As rotas multicast L2 são usadas para encaminhar o tráfego para receptores locais, pontos de fluxo Ethernet (EFPs), PWs de acesso e PWs de VFI que não participam do LSM do VPLS.

Quando o IGMPSN é habilitado em um domínio de bridge que é uma extremidade LSP P2MP, a disposição otimizada do tráfego multicast L2 recebido no LSP P2MP é feita para receptores locais (ou seja, Portas de Bridge (BPs) de Circuito de Conexão (AC) e BPs de PW de acesso).

Observação: o Snooping Multicast Label Distribution Protocol (MLDP) não é suportado no Cisco IOS XR Release 5.1.0.

Escala suportada

O Cisco IOS XR Release 5.1.0 suporta um máximo de **1000** Túneis P2MP ou **1000** PWs P2MP por roteador Head/Tail.

Configuração de VPLS LSM

Configuração de túnel automático P2MP

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

Configuração de redirecionamento rápido (FRR - Fast Reroute) MPLS TE

```
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
 !
```

Configuração de L2VPN

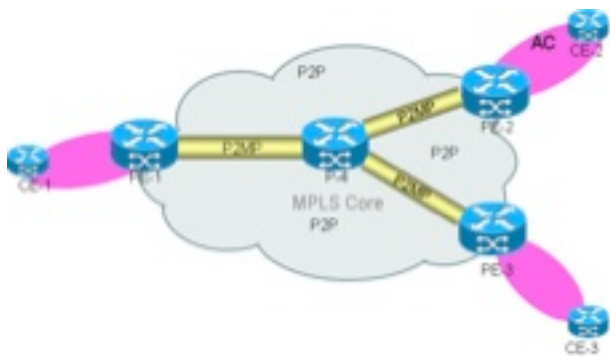
```
l2vpn
 bridge group bg1
 bridge-domain bg1_bd1
 interface GigabitEthernet0/1/1/10.1
 !
 vfi bg1_bd1_vfi
```

```

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
!

```

Exemplo de topologia e configuração



Os túneis P2MP são autodescobertos. Túneis P2MP estáticos **não** são suportados.

Configurações de túnel estático não são usadas. A configuração automática do túnel P2MP deve ser ativada em todos os roteadores PE e também em um roteador P se ele atuar como um nó de geração. Um nó bud é um roteador de ponto médio e de extremidade traseira ao mesmo tempo.

Um exemplo de topologia com configuração é mostrado aqui. Nessa topologia, os PWs P2MP são criados entre os três PEs e um roteador P que atua como um nó de geração. Todos os três roteadores PE atuam como Head (para tráfego de entrada) e Tail (para tráfego de saída).

Configuração de 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#

Configuração 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#

Configuração do 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

```


end

RP/0/RSP0/CPU0:PE2#

Configuração de 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
  !
  !
```


- **show l2vpn bridge-domain**
- **show l2vpn bridge-domain detail**
- **show mpls traffic-eng tunnels p2mp**
- **show mpls forwarding labels <label> detail**
- **show mpls traffic-eng tunnels p2mp tabular**

Aqui estão alguns exemplos:

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 Label	Outgoing Label	Prefix or ID	Outgoing Interface	Next Hop	Bytes Switched
289994		P2MP TE: 100			
Updated Feb 18 03:58:32.360					
TE Tunnel Head, tunnel ID: 100, tunnel ifh: 0x8000e20					
IPv4 Tableid: 0xe0000000, IPv6 Tableid: 0xe0800000					
Flags:IP Lookup:not-set, Expnulv4:not-set, Expnulv6:set					
Payload Type v4:set, Payload Type v6:not-set, l2vpn:set					
Head:set, Tail:not-set, Bud:not-set, Peek:not-set, inclusive:set					
Ingress Drop:not-set, Egress Drop:not-set					
Platform Data: {0x2000000, 0x2000000, 0x0, 0x0}, RPF-ID:0x80003					
VPLS Disposition: Bridge ID: 0, SHG ID: 0, PW Xconnect ID: 0x0					
mpls paths: 1, local mpls paths: 0, protected mpls paths: 1					
16005		P2MP TE: 100	Gi0/1/1/0	209.165.201.2	0
Updated Feb 18 03:58:32.360					
My Nodeid:65, Interface Nodeid:2065, Backup Interface Nodeid:2065					
Packets Switched: 0					

RP/0/RSP0/CPU0:PE1#

show mpls traffic-eng tunnels p2mp tabular

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

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

* = automatically created backup tunnel
^ = automatically created P2MP tunnel

Identificar e Solucionar Problemas do LSM do VPLS

Problemas comuns de configuração

As causas mais comuns de problemas P2MP no L2VPN são mostradas aqui.

- A configuração de BGP para LSM é exatamente a mesma que para BGP-AD. Certifique-se de exportar/importar rotas da família de endereços l2vpn vpls-vpws configurando **address-family l2vpn vpls-vpws** para vizinhos BGP.
- Há erros de configuração de MPLS e multicast.

A Engenharia de tráfego MPLS deve ser habilitada nas interfaces em que os PWs P2MP passam.

```
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
```

- A configuração L2VPN para LSM no Cisco IOS XR Release 5.1.0 requer que você:

Configurar a ID de VPN para o VFIConfigure o P2MP multicast para o VFI. Configure o protocolo de transporte e o protocolo de sinalização, como neste exemplo de configuração:

```
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
```

- A LSM Head/Tail deve ser ajustada corretamente. No Cisco IOS XR Release 5.1.0, cada extremidade de LSM também é um Cabeçalho de LSM e vice-versa. Como não há **intercâmbio de capacidade LSM** explícito entre os roteadores, todos os roteadores em um

domínio de bridge habilitado para LSM devem participar do LSM.

Comandos Show e Troubleshooting de L2VPN e L2FIB

- O processo do gerenciador L2VPN (l2vpn_mgr) comunica-se com o processo de controle de Engenharia de Tráfego (TE) de MPLS (te_control) e solicita a criação do túnel. Certifique-se de que os processos te_control e l2vpn_mgr estejam no estado de execução com estes comandos:

```
show process l2vpn_mgr
show process te_control
```

- verifique se o processo l2vpn_mgr solicitou a criação do túnel. Uma entrada para o túnel deve estar neste 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
```

- O L2VPN precisa receber as informações de túnel do processo te_control. Verifique se este comando show tem detalhes diferentes de zero, como 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
```

- O L2VPN deve anunciar a PMSI (Provider Multicast Service Instance) a todos os outros roteadores PE. Verifique se l2vpn_mgr enviou o PMSI para o VFI configurado. O evento **LSM Head: send PMSI** deve estar presente no histórico de eventos do 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 - -
-----

```

[...]

- O L2VPN nos outros roteadores deve receber o PMSI que acabou de ser enviado. Certifique-se de que **LSM Tail: PMSI received** seja mostrado no histórico de eventos no lado receptor:

```
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 - -
-----

```

[...]

- Cada roteador é um LSM Head e Tail e deve enviar o PMSI e receber PMSIs de cada um dos outros roteadores. O primeiro roteador verificado deve receber PMSIs de cada um dos outros nós.
- A Base de Informações de Encaminhamento da Camada Dois (L2FIB) deve receber as informações HEAD do L2VPN e deve baixá-las para a placa de linha.

```
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

- O L2FIB deve receber as informações TAIL do L2VPN para cada PW e deve baixá-las para a plataforma.

```
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
  EVI Bridge Domain: 0, EVI 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#

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.