# マルチポイント レイヤ 2 サービス実装の前提条件

マルチポイント レイヤ2サービスを設定する前に、次の作業を確認し、条件が満たされていることを確認してください。

- 適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。このコマンド リファレンスには、各コマンドに必要なタスク ID が含まれます。

  ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。

- プロバイダー エッジ（PE）ルータが IP によって相互に到達できるように、コアに IP ルーティングを設定します。

- レイヤ2 トラフィックを開始して終了するようにループバック インターフェイスを設定します。PE ルータが他のルータのループバック インターフェイスにアクセスできるようにします。

（注） ループバック インターフェイスは、すべてのケースで必要というわけではありません。たとえば、マルチポイント レイヤ2 サービスが TE トンネルに直接マッピングされている場合、トンネル選択ではループバック インターフェイスは必要ありません。


- マルチポイント レイヤ 2 サービスの実装に関する情報 （2 ページ）
- マルチポイント レイヤ 2 サービスの実装方法 （13 ページ）
- MAC アドレス取り消し （39 ページ）
- マルチポイント レイヤ 2 サービスの設定例 （42 ページ）
- LDP ベースの VPLS および VPWS FAT 擬似回線 （52 ページ）

# マルチポイント レイヤ 2 サービスの実装に関する情報

マルチポイント レイヤ 2 サービスを実装するには、次の概念を理解する必要があります。

## マルチポイント レイヤ 2 サービスの概要

マルチポイント レイヤ 2 サービスを使用すると、地理的に離れたローカル エリア ネットワーク（LAN）セグメントを MPLS ネットワーク経由で単一ブリッジ ドメインとして相互接続できます。MAC アドレス ラーニング、エージング、およびスイッチングなどの従来の LAN の機能はすべて、単一のブリッジ ドメインに属する、リモート接続されたすべての LAN セグメント全体でエミュレートされます。サービス プロバイダーは、カスタマーごとに別のブリッジ ドメインを定義することで、MPLS ネットワーク上で複数のカスタマーに VPLS サービスを提供できます。あるブリッジ ドメインからのパケットが別のブリッジ ドメインには伝送または配信されることはないため、LAN サービスのプライバシーが確保されます。

（注） VPLS PW は、BGP マルチパスではサポートされていません。

以降の各項では、マルチポイント レイヤ 2 サービス ネットワークのいくつかのコンポーネントについて説明します。

（注） マルチポイント レイヤ 2 サービスは、仮想プライベート LAN サービスとも呼ばれます。

### ブリッジ ドメイン

ネイティブ ブリッジ ドメインは、一連の物理ポートまたは仮想ポート（VFI を含む）から構成されるレイヤ 2 のブロードキャスト ドメインです。データ フレームは、宛先 MAC アドレスに基づいてブリッジ ドメイン内でスイッチングされます。マルチキャスト、ブロードキャスト、不明な宛先ユニキャスト フレームは、ブリッジ ドメイン内でフラッディングされます。また、送信元 MAC アドレス ラーニングは、ブリッジ ドメインのすべての着信フレームで行われます。学習されたアドレスは期限切れになります。着信フレームは、入力ポート、または入力ポートと MAC ヘッダー フィールドの両方の組み合わせのいずれかに基づいてブリッジ ドメインにマッピングされます。

### ブリッジ ドメインと BVI スケール

ブリッジ ドメイン（BD）の数は、BD ごとに設定された接続回線（AC）の数に依存し、ブリッジグループ仮想インターフェイス（BVI）が設定されているかどうかによって異なります。サポートされている論理インターフェイス（LIF）の数は、4000 未満です。

次の表に、BD ごとに 2 つの AC が設定されている場合に必要な論理インターフェイス（LIF）数の計算方法の例を示します。

| ブリッジ ドメイン | ブリッジの数 | AC | 必要な LIF の合計 |
|---|---|---|---|
| BVI のある BD | 625 | 2 | 3750 |
| BVI のない BD | 125 | 2 | 250 |
| BD の合計 | 750 | - | - |

必要な LIF の数は、

a * 3 + b として計算されます。ここで、a は BVI のある AC の数、b は BVI のない AC の数で、4,000 を超えることはできません。

## 疑似回線

疑似回線は、PE ルータのペア間のポイントツーポイント接続です。その主な機能は、共通 MPLS 形式にカプセル化することによって、基礎となるコア MPLS ネットワーク経由でイーサネットなどのサービスをエミュレートすることです。共通 MPLS 形式へのサービスのカプセル化によって、疑似回線では、通信事業者は MPLS ネットワークにサービスを統合できます。

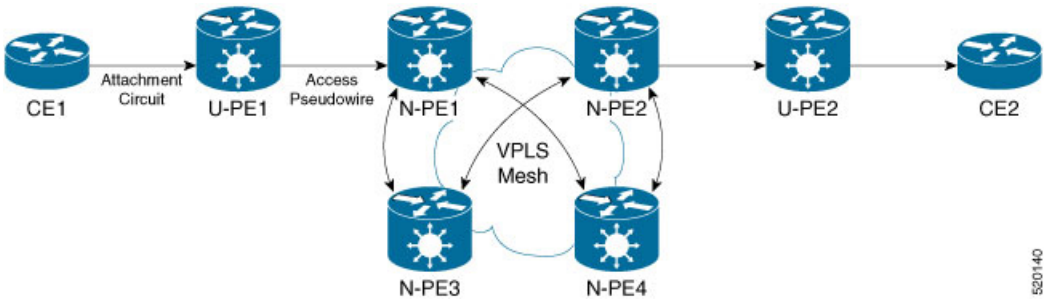
## アクセス疑似回線

アクセス擬似回線機能を使用すると、ネットワーク プロバイダー エッジ（N-PE）デバイス間の疑似回線（PW）の数を減らせます。ユーザプロバイダーエッジ（U-PE）デバイスは、アクセス擬似回線（PW）を使用して N-PE デバイスに接続します。この機能により、シグナリングのオーバーヘッドとパケットの複製が防止されます。

PW が物理ポートまたは論理ポートで終端する従来の VPLS とは異なり、アクセス PW は N-PE デバイスで終端します。VPLS サービスごとに、U-PE と N-PE の間にアクセス PW を作成します。

VPLS では、VPLS サービスに参加する L2VPN PE 間で疑似回線（PW）のフルメッシュが必要です。各 VPLS サービスに対して、PE 間で PW を設定する必要があります。PW のフルメッシュでは、PE の数が増えるとスケーラビリティの問題が発生するため、PW の数が増加します。PE の階層を使用して、PW の数を減らせます。

**図 *1*：アクセス疑似回線**




このトポロジでは、ユーザプロバイダーエッジ（U-PE）デバイスが CE への AC を備えています。U-PE デバイスは、アクセス PW を介して CE トラフィックをネットワーク プロバイダー

エッジ（N-PE）デバイスに転送します。N-PE は、VPLS メッシュ内の他の N-PE に接続されたコア VPLS PE です。N-PE では、U-PE からのアクセス PW は AC とほぼ同じです。U-PE は、他の N-PE とのメッシュの一部ではありません。したがって、N-PE はアクセス PW を AC と見なします。N-PE は、そのアクセス PW からのトラフィックを VPLS フルメッシュの一部であるコア PW に転送します。VFI で、N-PE 間のコア PW を設定します。スプリットホライズンルールを、VFI で設定されたすべてのコア PW に適用します。U-PE からのアクセス PW は、VFI では設定されていないため、VFI PW と同じスプリットホライズングループ（SHG）には属していません。トラフィックはアクセス PW から VFI PW、また逆方向に転送されます。

## アクセス疑似回線の設定

アクセス疑似配線を設定するには、次のタスクを実行します。

```
/* Configure U-PE1 */
Router#configure
Router(config)# iinterface TenGigE0/1/0/5.2 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 2
Router(config-l2vpn-subif)# rewrite ingress tag pop 1 symmetric
Router(config-l2vpn-subif)# exit
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group XCON1
Router(config-l2vpn-xc)# p2p xc1
Router(config-l2vpn-xc-p2p)# interface TenGigE0/1/0/5.2 l2transport
Router(config-l2vpn-xc-p2p)# neighbor 172.16.0.1 pw-id 1
Router(config-l2vpn-xc-p2p-pw)# commit

/* Configure N-PE1 */
Router#configure
Router(config)l2vpn
Router(config-l2vpn)#router-id 172.16.0.1
Router(config-l2vpn)#pw-class class1
Router(config-l2vpn-pwc)#encapsulation mpls
Router(config-l2vpn-pwc-mpls)#transport-mode ethernet
Router(config-l2vpn-pwc-mpls)#exit
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group bg1
Router(config-l2vpn-bg)# bridge-domain bd1
Router(config-l2vpn-bg-bd)# interface GigabitEthernet0/1/0/3.2
Router(config-bg-bd-ac)# split-horizon group
Router(config-l2vpn-bg-bd-ac)#exit
Router(config-l2vpn-bg-bd)#vfi vfi1
Router(config-l2vpn-bg-bd-vfi)#neighbor 10.0.0.1 pw-id 2
Router(config-l2vpn-bg-bd-vfi-pw)#pw-class class1
Router(config-l2vpn-bg-bd-vfi-pw-pwc)#commit
```

### 実行コンフィギュレーション

この項では、アクセス疑似回線の実行コンフィギュレーションを示します。

```
/* On U-PE1 */
configure
 interface TenGigE0/1/0/5.2 l2transport
  encapsulation dot1q 2
  rewrite ingress tag pop 1 symmetric
!
l2vpn
 xconnect group XCON1
```

```
  p2p xc1
   interface TenGigE0/1/0/5.2 l2transport
   neighbor 172.16.0.1 pw-id 1
   !
!
------------------------------------------------------------------------
/* On N-PE1 */
l2vpn
 router-id 172.16.0.1
 pw-class class1
 encapsulation mpls
 transport-mode ethernet
 !
!
l2vpn
 bridge group bg1
  bridge-domain bd1
   interface GigabitEthernet0/1/0/3.2
    split-horizon group
   !
 !
!
vfi vf1
 neighbor 10.0.0.1 pw-id 2
  pw-class class1
  !
!
```

## 確認

アクセス擬似回線の設定を確認します。

```
Router:U-PE1#show l2vpn xconnect group XCON1
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
        SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect                    Segment 1                       Segment 2
Group      Name       ST    Description            ST       Description      ST
-----------------   ----- --------------   ------------------------------   ------
XCON_1     xc1        UP    Te0/1/0/5.2            UP       172.16.0.1   1   UP
------------------------------------------------------------------------------------
```

```
Router:N-PE1#show l2vpn bridge-domain bd1
PW: neighbor 10.0.0.1, PW ID 2, state is up ( established )
      PW class mpls, XC ID 0xc0000008
      Encapsulation MPLS, protocol LDP
      Source address 172.16.0.1
      PW type Ethernet, control word disabled, interworking none
      PW backup disable delay 0 sec
      Sequencing not set
      LSP : Up

      PW Status TLV in use
        MPLS         Local                          Remote
        ------------ ------------------------------ ------------------------------
        Label        24752                          24752
        Group ID     0x2                            0x2
        Interface    Access PW                      Access PW
        MTU          1500                           1500
        Control word disabled                       disabled
```

```
PW type      Ethernet                       Ethernet
VCCV CV type 0x2                            0x2
             (LSP ping verification)        (LSP ping verification)
VCCV CC type 0x6                            0x6
             (router alert label)           (router alert label)
             (TTL expiry)                   (TTL expiry)
------------ ------------------------------ --------------------------
```

### 関連項目

- アクセス疑似回線 （3 ページ）

### 関連コマンド

- show l2vpn xconnect group
- show l2vpn bridge-domain

## 仮想転送インスタンス

VPLS は、仮想転送インスタンス（VFI）の特性に基づいています。VFI は、宛先 MAC アドレス、送信元 MAC アドレス ラーニングとエージングなどに基づいて、転送などのネイティブ ブリッジング機能を実行できる仮想ブリッジ ポートです。

VFI は、VPLS インスタンスごとに PE ルータ上に作成されます。PE ルータでは、特定の VPLS インスタンスの VFI を検索して、パケットの転送先が決定されます。VFI は、特定の VPLS インスタンスの仮想ブリッジのように動作します。VFI には、特定の VPLS に属する複数の接続回線を接続できます。PE ルータは、その VPLS インスタンス内にあるすべての他の PE ルータに対するエミュレート VC を構築し、これらのエミュレート VC を VFI に接続します。パケット転送決定は、VFI で保持されるデータ構造に基づきます。

# MPLS ベースのプロバイダー コアの VPLS

VPLS はマルチポイント レイヤ 2 VPN テクノロジーであり、ブリッジング技法によって複数のカスタマー デバイスを接続します。Multipoint Bridging のビルディング ブロックのブリッジ ドメインは、各 PE ルータに存在します。PE ルータのブリッジ ドメインへのアクセス接続は、接続回線と呼ばれます。接続回線は、一連の物理ポート、仮想ポート、またはネットワーク内の各 PE デバイスのブリッジに接続されている両方ポートです。

接続回線をプロビジョニングした後、この特定のインスタンスの MPLS ネットワークを介したネイバー関係が、エンド PE を識別する一連の手動コマンドによって確立されます。ネイバー アソシエーションが完了すると、MPLS コアとカスタマー ドメイン間のゲートウェイである疑似回線のフル メッシュがネットワーク側プロバイダー エッジ デバイス間で確立されています。

MPLS/IP プロバイダー コアは、1 つのブロードキャスト ドメインを構成するために、各 PE デバイス上の複数の接続回線を接続する仮想ブリッジをシミュレートします。また、これらの間でエミュレート仮想回線（VC）を構成するために、VPLS インスタンスに参加しているすべての PE ルータも必要です。

次に、サービス プロバイダー ネットワークは、宛先 MAC アドレスを調べてカスタマーに固有のブリッジ ドメイン内でパケットの交換を開始します。不明、ブロードキャスト、マルチキャストの宛先 MAC アドレスを持つすべてのトラフィックは、サービス プロバイダー ネットワークに接続するすべての接続済み CE カスタマー エッジ デバイスにフラッディングされます。ネットワーク側プロバイダー エッジ デバイスは、パケットがフラッディングされると送信元 MAC アドレスを学習します。トラフィックは、学習されたすべての MAC アドレスのカスタマー エッジ デバイスにユニキャストされます。

# レイヤ 2 スイッチングの VPLS

VPLS テクノロジーには、レイヤ 2 ブリッジングを実行するようにルータを設定する機能が含まれます。このモードではルータは、他のシスコ スイッチのように動作するように設定できます。

（注） ストーム制御の設定はメインインターフェイスの 1 つのサブインターフェイスでのみサポートされますが、システムでは複数のサブインターフェイスでストーム制御を設定することができます。ただし、実行コンフィギュレーションにはコミットされたすべてのストーム制御設定が表示されますが、有効になるのはメインインターフェイス配下の最初のストーム制御設定だけです。リロード後は、設定の順序に関係なく、どのストーム制御設定も有効になる可能性があります。

次の機能がサポートされています。

- ブリッジング IOS XR トランク インターフェイス
- EFP でのブリッジング

# VPLS LDP シグナリングにおける Cisco IOS XR と Cisco IOS 間の相互運用性

Cisco IOS ソフトウェアは、BGP アップデート メッセージ内で、最初のバイト内の NLRI の長さをビット型式でエンコードします。ただし、Cisco IOS XR ソフトウェアは、NLRI の長さを 2 バイトで解釈します。したがって、VPLS-VPWS アドレス ファミリを使用する BGP ネイバーが IOS と IOS XR 間に設定されている場合、NLRI の不一致が発生し、ネイバー間のフラッピングの原因になります。この競合を避けるために、IOS は **prefix-length-size 2** コマンドをサポートしています。IOS が IOS XR とともに動作するようにするには、このコマンドをイネーブルにする必要があります。IOS で **prefix-length-size 2** コマンドが設定されている場合、NLRI の長さはバイト単位でエンコードされます。この設定は、IOS を IOS XR とともに動作させるために必要です。

次に、**prefix-length-size 2** コマンドを使用した IOS の設定の例を示します。

```
router bgp 1
 address-family l2vpn vpls
```

```
 neighbor 5.5.5.2 activate
 neighbor 5.5.5.2 prefix-length-size 2 --------> NLRI length = 2 bytes
exit-address-family
```

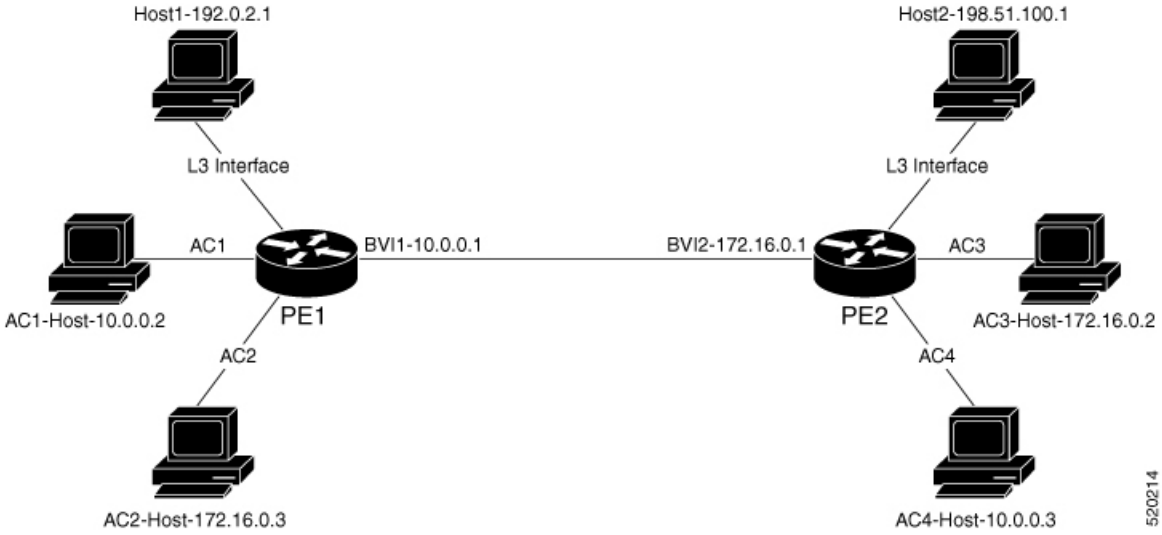
# ルーテッドインターフェイスとして BVI を使用した VPLS VFI

BVI をルーテッドインターフェイスとして VPLS VFI を使用すると、BVI インターフェイスを介して VPLS PW トラフィックを動的にルーティングできます。

Integrated Routing and Bridging（IRB）機能により、ブリッジグループ仮想インターフェイス（BVI）を使用して、ブリッジグループやルーテッドインターフェイス上のホストから受信したパケットをルーティングできます。BVI はルータ上で設定される仮想インターフェイスです。コアネットワークへのゲートウェイ ルーテッド インターフェイスとして機能します。

単一ブリッジドメインで設定する BVI は、ルータ上のドメインのブリッジングとルーティング間のリンクを表します。ルーテッドインターフェイスを宛先とするブリッジされたインターフェイスからパケットを受信するには、BVI を設定する際にブリッジドメイン内のホストと同じサブネット内にある適切な IP アドレスを指定します。

**図 *2:* ルーテッドインターフェイスとして *BVI* を使用した *VPLS VFI***




このトポロジは、次の 2 種類のトラフィックフローを示しています。

- ルーティングされたローカルトラフィック：AC1 ホストから Host1 へのトラフィックフローについて考えます。AC1 ホストが BVI1 にトラフィックを送信します。AC1 ホストと BVI1 を PE1 の同じブリッジドメインに接続します。PE1 は、BVI1 を介してトラフィックをルーティングしてから、Host1 にそのトラフィックを送信します。L3 インターフェイスが、Host1 と PE1 に接続します。
- ルーティングされたリモートトラフィック：AC2 ホストから Host2 へのトラフィックフローについて考えます。AC2 ホストは、PE1 のブリッジドメインにトラフィックを送信します。PE1 は BVI2 にトラフィックを送信します。AC2 ホストは BVI2 サブネットの一部です。PW は、PE2 のブリッジドメインにトラフィックを送信します。PE1 は、BVI2 を介

してトラフィックをルーティングしてから、Host2 にそのトラフィックを送信します。L3 インターフェイスが Host2 と PE2 に接続します。

次のプロトコルは、ブリッジドメインが PW と BVI の両方（DHCP、ERPS、CDP、IGMP スヌーピング、CDP、VRRP、CFM、LACP、BFDoBVI）を使用して接続されている場合はサポートされません。

## ルーテッドインターフェイスとして BVI を使用した VPLS VFI の設定

BVI インターフェイスを介して VPLS PW トラフィックを動的にルーティングするには、次のタスクを実行します。

### 設定例

```
/* PE1 Configuration */
Router#configure
Router(config)#l2vpn
Router(config-l2vpn)#bridge group bg1
Router(config-l2vpn-bg)#bridge-domain bd1
Router(config-l2vpn-bg-bd)#interface TenGigE0/0/0/0.1 -> AC1-L2 Sub-Interface (AC)
Router(config-l2vpn-bg-bd-ac)#exit
Router(config-l2vpn-bg-bd)#vfi core
Router(config-l2vpn-bg-bd-vfi)#neighbor 209.165.200.225 pw-id 1 -> VPLS Core-PW
Router(config-l2vpn-bg-bd-vfi-pw)#exit
Router(config-l2vpn-bg-bd-vfi)#exit
Router(config-l2vpn-bg-bd)#routed interface BVI1 -> BVI-1 Interface
Router(config-l2vpn-bg-bd-bvi)#exit
Router(config-l2vpn-bg-bd)#interface BVI1
Router(config-if)#ipv4 address 10.0.0.1 255.0.0.0
Router(config-if)#commit


/* PE2 Configuration */
Router#configure
Router(config)#l2vpn
Router(config-l2vpn)#bridge group bg1
Router(config-l2vpn-bg)#bridge-domain bd1
Router(config-l2vpn-bg-bd)#interface TenGigE0/0/0/1.1 -> AC3 L2 subinterface(AC)
Router(config-l2vpn-bg-bd-ac)#exit
Router(config-l2vpn-bg-bd)#vfi core
Router(config-l2vpn-bg-bd-vfi)#neighbor 209.165.200.226 pw-id 1 -> VPLS Core-PW
Router(config-l2vpn-bg-bd-vfi-pw)#exit
Router(config-l2vpn-bg-bd-vfi)#exit
Router(config-l2vpn-bg-bd)#routed interface BVI2 -> BVI-2 Interface
Router(config-l2vpn-bg-bd-bvi)#exit
Router(config-l2vpn-bg-bd)#interface BVI2
Router(config-if)#ipv4 address 172.16.0.1 255.240.0.0
Router(config-if)#commit
```

### 実行コンフィギュレーション

この項では、ルーテッドインターフェイスのコンフィギュレーションとして、BVIを使用したVPLS VFI を示します。

```
/* PE1 Configuration */
configure
```

```
 l2vpn
  bridge group bg1
   bridge-domain bd1
    interface TenGigE0/0/0/0.1 -> AC1-L2 Sub-Interface (AC)
    !
    vfi core
     neighbor 209.165.200.225 pw-id 1 -> VPLS Core-PW
     !
    !
    routed interface BVI1 -> BVI-1 Interface
    !
  !
interface BVI1
 ipv4 address 10.0.0.1 255.0.0.0


/* PE2 Configuration */
configure
 l2vpn
  bridge group bg1
   bridge-domain bd2
    interface TenGigE0/0/0/1.1 -> AC3 L2 Sub-Interface (AC)
    !
    vfi core
     neighbor 209.165.200.226 pw-id 1 -> VPLS Core-PW
     !
    !
    routed interface BVI2 -> BVI2 Interface
    !
  !
interface BVI2
 ipv4 address 172.16.0.1 255.240.0.0
```

### 確認

BVI を使用した VPLS VFI が、ルーテッドインターフェイス機能として正しく設定されていることを確認します。

```
Router-PE1#show l2vpn bridge-domain neighbor 209.165.200.225 detail
Legend: pp = Partially Programmed.
Bridge group: 1, bridge-domain: 1, id: 0, state: up, ShgId: 0, MSTi: 0
  VINE state: BVI Resolved
  MAC learning: enabled
  MAC withdraw: enabled
  Flooding:
    Broadcast & Multicast: enabled
    Unknown unicast: enabled
  MAC aging time: 300 s, Type: inactivity
  Create time: 10/01/2020 04:18:29 (00:14:06 ago)
  ACs: 2 (2 up), VFIs: 1, PWs: 1 (1 up), PBBs: 0 (0 up), VNIs: 0 (0 up)
  List of Access PWs:
  List of VFIs:
    VFI 1 (up)
      PW: neighbor 209.165.200.225, PW ID 1, state is up ( established )
        PW class mpls, XC ID 0xc0000002
        Encapsulation MPLS, protocol LDP
        Source address 209.165.200.226
        PW type Ethernet, control word disabled, interworking none
        Sequencing not set
        LSP : Up

        PW Status TLV in use
```

```
MPLS         Local                          Remote
------------ ------------------------------ --------------------------
Label        24006                          24002
Group ID     0x0                            0x0
Interface    1                              1
MTU          1500                           1500
Control word disabled                       disabled

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

### 関連項目

- ルーテッドインターフェイスとして BVI を使用した VPLS VFI （8 ページ）

### 関連コマンド

- show l2vpn bridge-domain detail

# MAC アドレス関連パラメータ

MAC アドレス テーブルには、既知の MAC アドレスおよび転送情報のリストが含まれます。現在の VPLS の仕様では、MAC アドレス テーブルとその管理がルート プロセッサ（RP）カードで維持されます。

次のトピックでは、MAC アドレス関連パラメータについて説明します。

## MAC アドレス フラッディング

イーサネット サービスでは、ブロードキャスト アドレスおよび不明な宛先アドレスに送信されるフレームをすべてのポートにフラッディングする必要があります。VPLS ブロードキャスト モデル内のフラッディングを取得するために、すべての不明ユニキャスト、ブロードキャスト、およびマルチキャスト フレームが、対応する疑似回線およびすべての接続回線にフラッディングされます。したがって、PE は、接続回線および疑似回線の両方にパケットを複製する必要があります。

## MAC アドレスベース転送

フレームを転送するには、PEは、宛先MACアドレスを疑似回線または接続回線に関連付ける必要があります。このタイプのアソシエーションは、各 PE で静的設定によって行われるか、すべてのブリッジ ポートにフラッディングされるダイナミック学習によって行われます。

## MAC アドレスの送信元ベースの学習

フレームがブリッジ ポート（たとえば、疑似回線または接続回路）に到達し、受信側 PE ルータが送信元 MAC アドレスを認識していない場合、送信元 MAC アドレスは、疑似回線または接続回線に関連付けられます。MAC アドレスへの送信フレームは、適切な疑似回線または接続回線に転送されます。

MAC アドレスの送信元ベースの学習は、ハードウェア転送パスで学習される MAC アドレス情報を使用します。更新された MAC テーブルはルータのハードウェアに伝達され、それによってルータのハードウェアがプログラミングされます。

（注） スタティック MAC 移動は、1 つのポート、インターフェイス、または AC から別のポート、インターフェイス、または AC に対してはサポートされていません。たとえば、スタティック MAC が AC1（ポート 1）で設定されていて、AC2（ポート 2）の送信元 MAC と同じ MAC を持つパケットを送信しようとした場合、その MAC をダイナミック MAC として AC2 に接続することはできません。したがって、MAC を持つパケットは、設定したどのスタティック MAC アドレスとしても送信しないでください。

学習される MAC アドレスの数は、設定可能なポート単位およびブリッジ ドメイン単位の MAC アドレス制限によって制限されます。

## MAC アドレス エージング

MAC テーブルの MAC アドレスは、MAC アドレス エージング タイムの間だけ有効と見なされます。期限切れになると、関連する MAC エントリが再度読み込まれます。MAC エージング タイムをブリッジ ドメインだけで設定すると、ブリッジ ドメインのすべての疑似回線と接続回線において、設定したその MAC エージング タイムが使用されます。

ブリッジは、ブリッジテーブルに基づいてパケットの転送、フラッディング、ドロップを行います。ブリッジ テーブルは、スタティック エントリとダイナミック エントリの両方を保持します。スタティック エントリは、ネットワーク マネージャまたはブリッジ自体によって入力されます。ダイナミック エントリはブリッジ学習プロセスによって入力されます。ダイナミック エントリは、エントリが作成された時点か最後に更新された時点から、「エージング タイム」と呼ばれる指定された期間が経過すると、自動的に削除されます。

ブリッジ型ネットワークのホストが移動する可能性が高い場合、ブリッジが変更に迅速に適応できるようにエージング タイムを小さくします。ホストが連続して送信しない場合は、より長い時間ダイナミック エントリを記録するようにエージング タイムを長くして、ホストが再度送信する場合よりフラッディングの可能性を低減できます。

MAC アドレスのエージング タイムの範囲は 300 ～ 3 万秒です。すべてのブリッジ間の MAC アドレスの最大エージング タイムで経過時間の計算は考慮されます。各 AC または PW インターフェイスで MAC アドレスのエージング タイムを設定することはできません。ブリッジ ドメイン コンフィギュレーション モードで MAC アドレスのエージング タイムを設定します。MAC アドレスの最大エージングタイムを表示する show コマンドはありません。

## MAC アドレス制限

MAC アドレス制限は、学習される MAC アドレスの数を制限するために使用されます。MAC アドレス制限のデフォルト値は、Cisco NCS 5501 および Cisco NCS 5502 の場合、64000 です。

制限を超えると、これらの通知を行うようシステムが設定されています。

- syslog（デフォルト）

- 簡易ネットワーク管理プロトコル（SNMP）トラップ
- syslog および SNMP トラップ
- なし（通知なし）

syslog メッセージおよび SNMP トラップ通知を生成するには、L2VPN ブリッジドメイン コンフィギュレーション モードで **mac limit notification both** コマンドを使用します。

MAC アドレス制限のアクションは、ローカル MAC アドレスの数が設定された制限を超えた場合にのみ適用されます。設定された MAC 制限しきい値に達するまで、ソフトウェアは MAC アドレスを学習解除します。後で、ルータは新しい MAC アドレスの学習を再開します。MAC 制限しきい値が設定されていない場合、デフォルトのしきい値は、設定された MAC アドレス制限の 75% です。

## MAC アドレス取り消し

高速な VPLS コンバージェンスでは、ダイナミックに学習された MAC アドレスを削除または学習解除できます。ラベル配布プロトコル（LDP）アドレス取り消しメッセージが MAC アドレスのリストと一緒に送信されます。これらのアドレスは、対応する VPLS サービスに参加する他のすべての PE で取り消す必要があります。

Cisco IOS XR VPLS の実装では、ダイナミックに学習された MAC アドレスの部分は、デフォルトで MAC アドレス エージング メカニズムを使用してクリアされます。MAC アドレス取り消し機能は、LDP アドレス取り消しメッセージによって追加されます。MAC アドレス取り消し機能をイネーブルにするには、l2vpn ブリッジ グループ ブリッジ ドメイン MAC コンフィギュレーション モードで **withdrawal** コマンドを使用します。MAC アドレス取り消しがイネーブルであることを確認するには、**detail** キーワードとともに **show l2vpn bridge-domain** コマンドを使用します。

（注） デフォルトでは、Cisco IOS XR で LDP MAC 取り消し機能がイネーブルになっています。

LDP MAC 取り消し機能は、次のイベントが原因で生成されます。

- 接続回線がダウンした。CLI から接続回線を削除または追加できます。
- MAC 取り消しメッセージを VFI 擬似回線経由で受信した。RFC 4762 では、ワイルドカード（空のタイプ、長さ、および値（TLV）による方法）と、特定の MAC アドレス取り消しの両方が規定されています。Cisco IOS XR ソフトウェアは、ワイルドカードによる MAC アドレス取り消しだけをサポートしています。

# マルチポイント レイヤ 2 サービスの実装方法

ここでは、マルチポイント レイヤ 2 サービスの実装に必要なタスクについて説明します。

# ブリッジ ドメインの設定

次のトピックでは、ブリッジ ドメインの設定方法について説明します。

## ブリッジ ドメインの作成

ブリッジ ドメインを作成するには、次の作業を実行します。

**手順**

**ステップ 1** **configure**

**例**：

```
RP/0/RP0/cpu 0: router# configure
```

XR コンフィギュレーション モードを開始します。

**ステップ 2** **l2vpn**

**例**：

```
RP/0/RP0/cpu 0: router(config)# l2vpn
RP/0/RP0/cpu 0: router(config-l2vpn)#
```

L2VPN コンフィギュレーション モードを開始します。

**ステップ 3** **bridge group** *bridge-group-name*

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn)# bridge group csco
RP/0/RP0/cpu 0: router(config-l2vpn-bg)#
```

ブリッジ ドメインを含めることができるブリッジ グループを作成し、ブリッジ ドメインにネットワーク インターフェイスを割り当てます。

**ステップ 4** **bridge-domain** *bridge-domain-name*

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)#
```

ブリッジ ドメインを確立し、L2VPN ブリッジ グループ ブリッジ ドメイン コンフィギュレーション モードを開始します。

**ステップ 5** **commit** コマンドまたは **end** コマンドを使用します。

**commit** ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

**end** ：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーション セッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーション セッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーション モードに留まります。

## メンバのブリッジ ドメインへの関連付け

ブリッジ ドメインの作成後、ブリッジ ドメインにインターフェイスを割り当てるには、この作業を実行します。次のタイプのブリッジ ポートは、ブリッジ ドメインに関連付けられています。

- イーサネットおよび VLAN
- VFI

### 手順

**ステップ 1** **configure**

例：

```
RP/0/RP0/cpu 0: router# configure
```

XR コンフィギュレーション モードを開始します。

**ステップ 2** **l2vpn**

例：

```
RP/0/RP0/cpu 0: router(config)# l2vpn
```

L2VPN コンフィギュレーション モードを開始します。

**ステップ 3** **bridge group** *bridge group name*

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn)# bridge group csco
RP/0/RP0/cpu 0: router(config-l2vpn-bg)#
```

ブリッジ ドメインを包含できるようにブリッジ グループを作成し、ブリッジ ドメインにネットワーク インターフェイスを割り当てます。

**ステップ 4** **bridge-domain** *bridge-domain name*

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)#
```

ブリッジ ドメインを確立し、L2VPN ブリッジ グループ ブリッジ ドメイン コンフィギュレーション モードを開始します。

**ステップ 5** **interface** *type interface-path-id*

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)# interface GigabitEthernet 0/4/0/0
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-ac)#
```

インターフェイス コンフィギュレーション モードを開始し、同じブリッジ ドメインに属する他のインターフェイスからパケットを転送および受信できるブリッジ ドメインにインターフェイスを追加します。

**ステップ 6** （任意）**static-mac-address** { *MAC-address* }

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-ac)# static-mac-address 1.1.1
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-ac)# exit
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)#
```

スタティック MAC アドレスを設定してリモート MAC アドレスを疑似回線またはその他のブリッジ インターフェイスに関連付けます。

**ステップ 7** **commit** コマンドまたは **end** コマンドを使用します。

**commit** ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

**end** ：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーション セッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーション セッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーション モードに留まります。

## ブリッジ ドメイン パラメータの設定

ブリッジ ドメイン パラメータを設定するには、ブリッジ ドメインに次のパラメータを関連付けます。

- Maximum transmission unit (MTU)：ブリッジ ドメインのすべてのメンバーに同じ MTU があることを指定します。MTU サイズが異なるブリッジ ドメイン メンバーは、まだブリッジ ドメインに関連付けられている場合でもブリッジ ドメインによって使用されません。
- フラッディング：フラッディングは常に有効になります。

手順

**ステップ 1** **configure**

例：

```
RP/0/RP0/cpu 0: router# configure
```

XR コンフィギュレーション モードを開始します。

**ステップ 2** **l2vpn**

例：

```
RP/0/RP0/cpu 0: router(config)# l2vpn
RP/0/RP0/cpu 0: router(config-l2vpn)#
```

l2vpn コンフィギュレーション モードを開始します。

**ステップ 3** **bridge group** *bridge-group-name*

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn)# bridge group csco
RP/0/RP0/cpu 0: router(config-l2vpn-bg)#
```

ブリッジ ドメインを包含できるようにブリッジ グループを作成し、ブリッジ ドメインにネットワーク インターフェイスを割り当てます。

**ステップ 4** **bridge-domain** *bridge-domain-name*

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)#
```

ブリッジ ドメインを確立し、l2vpn ブリッジ グループ ブリッジ ドメイン コンフィギュレーション モードを開始します。

**ステップ 5** **flooding disable**

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)# flooding disable
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)#
```

フラッディングを無効にします。

**ステップ 6** **mtu** *bytes*

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)# mtu 1000
```

ブリッジ ドメインの最大パケット サイズまたは最大伝送単位（MTU）サイズを調整します。

- バイト単位で MTU サイズを指定するには、*bytes* 引数を使用します。範囲は 64 ～ 65535 です。

**ステップ 7** **commit** コマンドまたは **end** コマンドを使用します。

**commit** ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

**end** ：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーション セッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーション セッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーション モードに留まります。

## ブリッジ ドメインのディセーブル化

ブリッジ ドメインをディセーブルにするには、次の作業を実行します。ブリッジ ドメインをディセーブルにすると、ブリッジ ドメインに関連付けられているすべての VFI がディセーブルになります。引き続き、ブリッジ ドメインに関連付けられたブリッジ ドメインと VFI にメンバーを接続するか、または取り外すことができます。

**手順**

**ステップ 1** **configure**

**例**：

```
RP/0/RP0/cpu 0: router# configure
```

XR コンフィギュレーション モードを開始します。

**ステップ 2** **l2vpn**

**例**：

```
RP/0/RP0/cpu 0: router(config)# l2vpn
RP/0/RP0/cpu 0: router(config-l2vpn)#
```

L2VPN コンフィギュレーション モードを開始します。

**ステップ 3** **bridge group** *bridge group name*

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn)# bridge group csco
RP/0/RP0/cpu 0: router(config-l2vpn-bg)#
```

ブリッジ ドメインを包含できるようにブリッジ グループを作成し、ブリッジ ドメインにネットワーク インターフェイスを割り当てます。

**ステップ 4** **bridge-domain** *bridge-domain name*

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)#
```

ブリッジ ドメインを確立し、l2vpn ブリッジ グループ ブリッジ ドメイン コンフィギュレーション モードを開始します。

**ステップ 5** **shutdown**

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)#
```

ブリッジ ドメインをシャットダウンし、ブリッジと、ブリッジ下のすべての接続回線と疑似回線を管理ダウン状態に戻します。

**ステップ 6** **commit** コマンドまたは **end** コマンドを使用します。

**commit** ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

**end** ：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーション セッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーション セッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーション モードに留まります。

# フラッディングの無効化

フラッディング無効化機能は、ブリッジドメインでのブロードキャスト、未知のユニキャスト、およびマルチキャスト（BUM）トラフィックの転送を防止します。ブリッジレベルまたはインターフェイスレベルで BUM トラフィックのフラッディングを無効にできます。ブリッジレベルでフラッディングを無効にすることで、接続回線（AC）、疑似回線（PW）、および EVPN LIF で BUM トラフィックが転送されるのを防ぐことができます。

未知のユニキャストトラフィックのみをブリッジレベルまたはインターフェイスレベルで無効にすることもできます。ブリッジレベルで未知のユニキャストトラフィックのフラッディングを無効にすることで、接続回線（AC）、疑似回線（PW）、および EVPN LIF で未知のユニキャストトラフィックが転送されるのを防ぐことができます。

インターフェイスレベルで未知のユニキャストトラフィックのフラッディングを無効にすると、AC でのみ未知のユニキャストトラフィックの転送を防ぐことができます。

# フラッディング無効化の設定

フラッディング無効化機能を設定するには、次のタスクを実行します。

次のフラッディングを無効にできます。

- ブリッジレベルの BUM トラフィック
- ブリッジレベルの未知のユニキャストトラフィック
- インターフェイスレベルの未知のユニキャストトラフィック

ただし、未知のユニキャストトラフィックのフラッディングをブリッジレベルで無効化できるのは、**flooding disable** コマンドがブリッジレベルで BUM トラフィックに対して設定されていない場合に限られます。

また、未知のユニキャストトラフィックのフラッディングをインターフェイスレベルで無効化できるのは、**flooding disable** および **flooding unknown-unicast disable** コマンドがブリッジレベルで設定されていない場合に限られます。

### 設定例

```
/* Configuration to disable flooding of BUM traffic at the bridge level */
Router# configure
Router(config)#l2vpn
Router(config-l2vpn)#bridge group bg1
Router(config-l2vpn-bg)#bridge-domain bd1
Router(config-l2vpn-bg-bd)#flooding disable\
Router(config-l2vpn-bg-bd)#commit

/* Configuration to disable flooding of unknown-unicast traffic at the bridge level */
Router# configure
Router(config)#l2vpn
Router(config-l2vpn)#bridge group bg1
Router(config-l2vpn-bg)#bridge-domain bd1
Router(config-l2vpn-bg-bd)#flooding unknown-unicast disable
Router(config-l2vpn-bg-bd)#commit

/* Configuration to disable flooding of unknown-unicast traffic at the interface level
*/
Router(config-l2vpn)#bridge group bg1
Router(config-l2vpn-bg)#bridge-domain bd1
Router(config-l2vpn-bg-bd)#interface TenGigE0/0/0/0.2
Router(config-l2vpn-bg-bd-ac)#flooding unknown-unicast disable
Router(config-l2vpn-bg-bd-ac)#commit
```

### 実行コンフィギュレーション

ここでは、フラッディング無効化の実行コンフィギュレーションを示します。

```
/* Configuration to disable flooding of BUM traffic at the bridge level */
configure
 l2vpn
  bridge group bg1
   bridge-domain bd1
    flooding disable
    flooding unknown-unicast disable
```

```
    interface TenGigE0/0/0/0.2
      flooding unknown-unicast disable
   !

/* Configuration to disable flooding of unknown-unicast traffic at the bridge level */
configure
 l2vpn
  bridge group bg1
   bridge-domain bd1
    flooding unknown-unicast disable
    !
  !


/* Configuration to disable flooding of unknown-unicast traffic at the interface level
*/
configure
 l2vpn
  bridge group bg1
   bridge-domain bd1
    interface TenGigE0/0/0/0.2
      flooding unknown-unicast disable
     !
   !
 !
```

### 関連コマンド

- flooding disable
- flooding unknown-unicast disable

# レイヤ 2 仮想転送インスタンスの設定

次のトピックでは、レイヤ 2 仮想転送インスタンス（VFI）の設定方法について説明します。

## 仮想転送インスタンスの作成

ブリッジ ドメインのすべてのプロバイダー エッジ（PE）デバイスでレイヤ 2 仮想転送インスタンス（VFI）を作成するには、次の作業を実行します。

### 手順

**ステップ 1** **configure**

**例**：

```
RP/0/RP0/cpu 0: router# configure
```

XR コンフィギュレーション モードを開始します。

**ステップ 2** **l2vpn**

**例**：

```
RP/0/RP0/cpu 0: router(config)# l2vpn
RP/0/RP0/cpu 0: router(config-l2vpn)#
```

L2VPN コンフィギュレーション モードを開始します。

**ステップ 3** **bridge group** *bridge group name*

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn)# bridge group csco
RP/0/RP0/cpu 0: router(config-l2vpn-bg)#
```

ブリッジ ドメインを包含できるようにブリッジ グループを作成し、ブリッジ ドメインにネットワーク インターフェイスを割り当てます。

**ステップ 4** **bridge-domain** *bridge-domain name*

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)#
```

ブリッジ ドメインを確立し、L2VPN ブリッジ グループ ブリッジ ドメイン コンフィギュレーション モードを開始します。

**ステップ 5** **vfi** {*vfi-name*}

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)# vfi v1
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-vfi)#
```

仮想転送インターフェイス（VFI）パラメータを設定し、L2VPN ブリッジ グループ ブリッジ ドメイン VFI コンフィギュレーション モードを開始します。

**ステップ 6** **commit** コマンドまたは **end** コマンドを使用します。

**commit** ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

**end** ：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーション セッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーション セッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーション モードに留まります。

## 疑似回線の仮想転送インスタンスへの関連付け

VFI を作成したら、1 つ以上の疑似回線を VFI に関連付けるには、次の作業を実行します。

手順

**ステップ 1** **configure**

例：

```
RP/0/RP0/cpu 0: router# configure
```

XR コンフィギュレーション モードを開始します。

**ステップ 2** **l2vpn**

例：

```
RP/0/RP0/cpu 0: router(config)# l2vpn
RP/0/RP0/cpu 0: router(config-l2vpn)#
```

L2VPN コンフィギュレーション モードを開始します。

**ステップ 3** **bridge group** *bridge-group-name*

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn)# bridge group csco
RP/0/RP0/cpu 0: router(config-l2vpn-bg)#
```

ブリッジ ドメインを包含できるようにブリッジ グループを作成し、ブリッジ ドメインにネットワーク インターフェイスを割り当てます。

**ステップ 4** **bridge-domain** *bridge-domain-name*

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)#
```

ブリッジ ドメインを確立し、L2VPN ブリッジ グループ ブリッジ ドメイン コンフィギュレーション モードを開始します。

**ステップ 5** **vfi** { *vfi name* }

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)# vfi v1
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-vfi)#
```

仮想転送インターフェイス（VFI）パラメータを設定し、L2VPN ブリッジ グループ ブリッジ ドメイン VFI コンフィギュレーション モードを開始します。

**ステップ 6** **neighbor** { *A.B.C.D* } { **pw-id** *value* }

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-vfi-pw)#
```

疑似回線ポートをブリッジ ドメインに追加するか、または疑似回線を仮想転送インターフェイス（VFI）に追加します。

- 相互接続ピアの IP アドレスを指定するには、*A.B.C.D* 引数を使用します。
- 疑似回線 ID および ID 値を設定するには、**pw-id** キーワードを使用します。指定できる範囲は 1 ～ 4294967295 です。

**ステップ 7** **commit** コマンドまたは **end** コマンドを使用します。

**commit** ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

**end** ：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーション セッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーション セッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーション モードに留まります。

## ブリッジ ドメインへの仮想転送インスタンスの関連付け

VFI をブリッジ ドメインのメンバーになるように関連付けるには、次の作業を実行します。

**手順**

**ステップ 1** **configure**

**例**：

```
RP/0/RP0/cpu 0: router# configure
```

XR コンフィギュレーション モードを開始します。

**ステップ 2** **l2vpn**

**例**：

```
RP/0/RP0/cpu 0: router(config)# l2vpn
RP/0/RP0/cpu 0: router(config-l2vpn)#
```

L2VPN コンフィギュレーション モードを開始します。

**ステップ 3** **bridge group** *bridge group name*

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn)# bridge group csco
```

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg)#
```

ブリッジ ドメインを包含できるようにブリッジ グループを作成し、ブリッジ ドメインにネットワーク インターフェイスを割り当てます。

**ステップ 4** **bridge-domain** *bridge-domain name*

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)#
```

ブリッジ ドメインを確立し、L2VPN ブリッジ グループ ブリッジ ドメイン コンフィギュレーション モードを開始します。

**ステップ 5** **vfi** { *vfi name* }

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)# vfi v1
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-vfi)#
```

仮想転送インターフェイス（VFI）パラメータを設定し、L2VPN ブリッジ グループ ブリッジ ドメイン VFI コンフィギュレーション モードを開始します。

**ステップ 6** **neighbor** { *A.B.C.D* } { **pw-id** *value* }

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-vfi-pw)#
```

疑似回線ポートをブリッジ ドメインに追加するか、または疑似回線を仮想転送インターフェイス（VFI）に追加します。

- 相互接続ピアの IP アドレスを指定するには、*A.B.C.D* 引数を使用します。
- 疑似回線 ID および ID 値を設定するには、**pw-id** キーワードを使用します。指定できる範囲は 1 ～ 4294967295 です。

**ステップ 7** **static-mac-address** { *MAC-address* }

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-vfi-pw)# static-mac-address 1.1.1
```

スタティック MAC アドレスを設定してリモート MAC アドレスを疑似回線またはその他のブリッジ インターフェイスに関連付けます。

**ステップ 8** **commit** コマンドまたは **end** コマンドを使用します。

**commit** ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

**end** ：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーション セッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーション セッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーション モードに留まります。

## 疑似回線への疑似回線クラスの接続

疑似回線に疑似回線クラスを接続するには、次の作業を実行します。

**手順**

**ステップ 1** **configure**

**例**：

```
RP/0/RP0/cpu 0: router# configure
```

XR コンフィギュレーション モードを開始します。

**ステップ 2** **l2vpn**

**例**：

```
RP/0/RP0/cpu 0: router(config)# l2vpn
RP/0/RP0/cpu 0: router(config-l2vpn)#
```

L2VPN コンフィギュレーション モードを開始します。

**ステップ 3** **bridge group** *bridge group name*

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn)# bridge group csco
RP/0/RP0/cpu 0: router(config-l2vpn-bg)#
```

ブリッジ ドメインを包含できるようにブリッジ グループを作成し、ブリッジ ドメインにネットワーク インターフェイスを割り当てます。

**ステップ 4** **bridge-domain** *bridge-domain name*

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)#
```

ブリッジ ドメインを確立し、L2VPN ブリッジ グループ ブリッジ ドメイン コンフィギュレーション モードを開始します。

**ステップ 5** **vfi** { *vfi-name* }

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)# vfi v1
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-vfi)#
```

仮想転送インターフェイス（VFI）パラメータを設定し、L2VPN ブリッジ グループ ブリッジ ドメイン VFI コンフィギュレーション モードを開始します。

**ステップ 6** **neighbor** { *A.B.C.D* } { **pw-id** *value* }

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-vfi-pw)#
```

疑似回線ポートをブリッジ ドメインに追加するか、または疑似回線を仮想転送インターフェイス（VFI）に追加します。

- 相互接続ピアの IP アドレスを指定するには、*A.B.C.D* 引数を使用します。
- 疑似回線 ID および ID 値を設定するには、 **pw-id** キーワードを使用します。指定できる範囲は 1 ～ 4294967295 です。

**ステップ 7** **pw-class** { *class-name* }

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-vfi-pw)# pw-class canada
```

疑似回線に使用する疑似回線クラス テンプレート名を設定します。

**ステップ 8** **commit** コマンドまたは **end** コマンドを使用します。

**commit** ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

**end** ：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーション セッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーション セッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーション モードに留まります。

## スタティック ラベルを使用した擬似回線の設定

スタティック ラベルを使用して Any Transport over Multiprotocol（AToM）疑似回線を設定するには、次の作業を実行します。疑似回線は、ローカルとリモートに MPLS スタティック ラベルを設定することでスタティック AToM 疑似回線になります。

手順

**ステップ 1** **configure**

例：

```
RP/0/RP0/cpu 0: router# configure
```

XR コンフィギュレーション モードを開始します。

**ステップ 2** **l2vpn**

例：

```
RP/0/RP0/cpu 0: router(config)# l2vpn
RP/0/RP0/cpu 0: router(config-l2vpn)#
```

L2VPN コンフィギュレーション モードを開始します。

**ステップ 3** **bridge group** *bridge-group-name*

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn)# bridge group csco
RP/0/RP0/cpu 0: router(config-l2vpn-bg)#
```

ブリッジ ドメインを包含できるようにブリッジ グループを作成し、ブリッジ ドメインにネットワーク インターフェイスを割り当てます。

**ステップ 4** **bridge-domain** *bridge-domain-name*

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)#
```

ブリッジ ドメインを確立し、L2VPN ブリッジ グループ ブリッジ ドメイン コンフィギュレーション モードを開始します。

**ステップ 5** **vfi** { *vfi-name* }

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)# vfi v1
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-vfi)#
```

仮想転送インターフェイス（VFI）パラメータを設定し、L2VPN ブリッジ グループ ブリッジ ドメイン VFI コンフィギュレーション モードを開始します。

**ステップ 6** **neighbor** { *A.B.C.D* } { **pw-id** *value* }

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-vfi-pw)#
```

疑似回線ポートをブリッジ ドメインに追加するか、または疑似回線を仮想転送インターフェイス（VFI）に追加します。

- 相互接続ピアの IP アドレスを指定するには、*A.B.C.D* 引数を使用します。
- 疑似回線 ID および ID 値を設定するには、 **pw-id** キーワードを使用します。指定できる範囲は 1 ～ 4294967295 です。

**ステップ 7** **mpls static label** { **local** *value* } { **remote** *value* }

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-vfi-pw)# mpls static label local 800 remote
500
```

MPLS スタティック ラベルおよび疑似回線コンフィギュレーションのスタティック ラベルを設定します。ローカルおよびリモートの疑似回線ラベルを設定できます。

**ステップ 8** **commit** コマンドまたは **end** コマンドを使用します。

**commit** ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

**end** ：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーション セッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーション セッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーション モードに留まります。

## 仮想転送インスタンスのディセーブル化

VFI をディセーブルにするには、次の作業を実行します。VFI がディセーブルの場合、VFI に関連付けられた、以前に確立された疑似回線はすべて切断されます。LDP アドバタイズメントは、VFI に関連付けられた MAC アドレスを回収するために送信されます。ただし、シャットダウン後にも引き続き接続回線を VFI に接続したり切断したりできます。

**手順**

**ステップ 1** **configure**

**例**：

```
RP/0/RP0/cpu 0: router# configure
```

XR コンフィギュレーション モードを開始します。

**ステップ 2** **l2vpn**

例：

```
RP/0/RP0/cpu 0: router(config)# l2vpn
RP/0/RP0/cpu 0: router(config-l2vpn)#
```

L2VPN コンフィギュレーション モードを開始します。

**ステップ 3** **bridge group** *bridge group name*

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn)# bridge group csco
RP/0/RP0/cpu 0: router(config-l2vpn-bg)#
```

ブリッジ ドメインを包含できるようにブリッジ グループを作成し、ブリッジ ドメインにネットワーク インターフェイスを割り当てます。

**ステップ 4** **bridge-domain** *bridge-domain name*

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)#
```

ブリッジ ドメインを確立し、L2VPN ブリッジ グループ ブリッジ ドメイン コンフィギュレーション モードを開始します。

**ステップ 5** **vfi** { *vfi-name* }

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)# vfi v1
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-vfi)#
```

仮想転送インターフェイス（VFI）パラメータを設定し、L2VPN ブリッジ グループ ブリッジ ドメイン VFI コンフィギュレーション モードを開始します。

**ステップ 6** **shutdown**

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-vfi)# shutdown
```

仮想転送インターフェイス（VFI）をディセーブルにします。

**ステップ 7** **commit** コマンドまたは **end** コマンドを使用します。

**commit** ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

**end** ：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーション セッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーション セッションを終了します。

• [Cancel]：設定変更をコミットせずに、コンフィギュレーション モードに留まります。

**ステップ 8** **show l2vpn bridge-domain** [ **detail** ]

例：

```
RP/0/RP0/cpu 0: router# show l2vpn bridge-domain detail
```

VFI の状態を表示します。たとえば、VFI をシャットダウンすると、VFI はブリッジ ドメインでシャットダウンされていると示されています。

# MAC アドレス関連パラメータの設定

次のトピックでは、MAC アドレス関連パラメータの設定方法について説明します。

MAC テーブル属性は、ブリッジ ドメインについて設定されます。

（注） **show l2vpn forwarding bridge-domain BRIDGE_GROUP:BRIDGE_DOMAIN mac-address location R/S/I** コマンドを実行しても、MAC アドレスのハードウェア情報は自動的にはダンプされません。show の出力情報が最新ではない可能性があります。**show l2vpn forwarding bridge-domain BRIDGE_GROUP:BRIDGE_DOMAIN mac-address location R/S/I** コマンドを実行する前に、次のいずれかの操作を実行します。

- **l2vpn resynchronize forwarding mac-address location R/S/I** コマンドを実行して、MAC アドレスのエントリを再同期します。
- **show l2vpn forwarding bridge-domain mac-address location R/S/I** コマンドを実行して、MAC アドレス テーブルをダンプします。

## MAC アドレスの送信元ベースの学習の設定

MAC アドレスの送信元ベースの学習を設定するには、次の作業を実行します。

手順

**ステップ 1** **configure**

例：

```
RP/0/RP0/cpu 0: router# configure
```

XR コンフィギュレーション モードを開始します。

**ステップ 2** **l2vpn**

例：

```
RP/0/RP0/cpu 0: router(config)# l2vpn
RP/0/RP0/cpu 0: router(config-l2vpn)#
```

L2VPN コンフィギュレーション モードを開始します。

**ステップ 3** **bridge group** *bridge group name*

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn)# bridge group csco
RP/0/RP0/cpu 0: router(config-l2vpn-bg)#
```

ブリッジ ドメインを包含できるようにブリッジ グループを作成し、ブリッジ ドメインにネットワーク インターフェイスを割り当てます。

**ステップ 4** **bridge-domain** *bridge-domain-name*

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)#
```

ブリッジ ドメインを確立し、L2VPN ブリッジ グループ ブリッジ ドメイン コンフィギュレーション モードを開始します。

**ステップ 5** **mac**

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)# mac
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-mac)#
```

L2VPN ブリッジ グループ ブリッジ ドメイン MAC コンフィギュレーション モードを開始します。

**ステップ 6** **learning disable**

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-mac)# learning disable
```

**ステップ 7** **commit** コマンドまたは **end** コマンドを使用します。

**commit** ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

**end** ：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーション セッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーション セッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーション モードに留まります。

**ステップ 8** **show l2vpn bridge-domain** [ **detail** ]

例：

```
RP/0/RP0/cpu 0: router# show l2vpn bridge-domain detail
```

MAC アドレスの送信元ベースの学習がブリッジでディセーブルになったことの詳細が表示されます。

## MAC アドレス制限の設定

MAC アドレス制限のパラメータを設定するには、次の作業を実行します。

手順

**ステップ 1** **configure**

例：

```
RP/0/RP0/cpu 0: router# configure
```

XR コンフィギュレーション モードを開始します。

**ステップ 2** **l2vpn**

例：

```
RP/0/RP0/cpu 0: router(config)# l2vpn
RP/0/RP0/cpu 0: router(config-l2vpn)#
```

L2VPN コンフィギュレーション モードを開始します。

**ステップ 3** **bridge group** *bridge group name*

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn)# bridge group csco
RP/0/RP0/cpu 0: router(config-l2vpn-bg)#
```

ブリッジ ドメインを包含できるようにブリッジ グループを作成し、ブリッジ ドメインにネットワーク インターフェイスを割り当てます。

**ステップ 4** **bridge-domain** *bridge-domain name*

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)#
```

ブリッジ ドメインを確立し、L2VPN ブリッジ グループ ブリッジ ドメイン コンフィギュレーション モードを開始します。

**ステップ 5** （任意） **interface** *type interface_id*

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)# interface gigabitEthernet 0/2/0/1
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-ac)#
```

指定したインターフェイスのインターフェイス コンフィギュレーション モードを開始し、このインターフェイスをブリッジ ドメイン メンバー インターフェイスとして追加します。

（注） 特定のインターフェイスに対してのみ MAC アドレス制限を設定する場合は、この手順を実行します。以降の手順では、MAC アドレス制限をブリッジ ドメイン レベルで設定するためのルータ プロンプトを示します。ルータ プロンプトはこの手順をスキップした場合に表示されます。

**ステップ 6** **mac**

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)# mac
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-mac)#
```

L2VPN ブリッジ グループ ブリッジ ドメイン MAC コンフィギュレーション モードを開始します。

**ステップ 7** **limit**

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-mac)# limit
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-mac-limit)#
```

アクション、最大、通知の MAC アドレス制限を設定し、L2VPN ブリッジ グループ ブリッジ ドメイン MAC 制限コンフィギュレーション モードを開始します。

**ステップ 8** **maximum** { *value* }

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-mac-limit)# maximum 5000
```

ブリッジで学習される MAC アドレスの数が制限に到達したときの特定のアクションを設定します。

**ステップ 9** **action** { **flood** | **no-flood** | **shutdown** }

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-mac-limit)# action flood
```

学習される MAC アドレスの数が設定された MAC 制限を超えたときのブリッジの動作を設定します。

**ステップ 10** **notification** { **both** | **none** | **trap** }

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-mac-limit)# notification both
```

学習される MAC アドレスの数が設定された制限を超えたときに送信される通知のタイプを指定します。

**ステップ 11** **mac limit threshold** *80*

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn)# mac limit threshold 80
```

MAC 制限のしきい値を設定します。デフォルトは、ステップ 8 で設定した MAC アドレス制限の 75% です。

**ステップ 12** **commit** コマンドまたは **end** コマンドを使用します。

**commit** ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

**end** ：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーション セッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーション セッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーション モードに留まります。

**ステップ 13** **show l2vpn bridge-domain** [ **detail** ]

**例**：

```
RP/0/RP0/cpu 0: router# show l2vpn bridge-domain detail
```

MAC アドレス制限の詳細が表示されます。

## MAC アドレス エージングの設定

MAC アドレス エージングのパラメータを設定するには、次の作業を実行します。

手順

**ステップ 1** **configure**

例：

```
RP/0/RP0/cpu 0: router# configure
```

XR コンフィギュレーション モードを開始します。

**ステップ 2** **l2vpn**

例：

```
RP/0/RP0/cpu 0: router(config)# l2vpn
RP/0/RP0/cpu 0: router(config-l2vpn)#
```

L2VPN コンフィギュレーション モードを開始します。

**ステップ 3** **bridge group** *bridge-group-name*

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn)# bridge group csco
RP/0/RP0/cpu 0: router(config-l2vpn-bg)#
```

ブリッジ ドメインを包含できるようにブリッジ グループを作成し、ブリッジ ドメインにネットワーク インターフェイスを割り当てます。

**ステップ 4** **bridge-domain** *bridge-domain-name*

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)#
```

ブリッジ ドメインを確立し、L2VPN ブリッジ グループ ブリッジ ドメイン コンフィギュレーション モードを開始します。

**ステップ 5** **mac**

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)# mac
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-mac)#
```

L2VPN ブリッジ グループ ブリッジ ドメイン MAC コンフィギュレーション モードを開始します。

**ステップ 6** **aging**

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-mac)# aging
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-mac-aging)#
```

MAC エージング コンフィギュレーション サブモードを開始し、時間やタイプなどのエージング パラメータを設定します。

**ステップ 7** **time** { *seconds* }

**例**：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-mac-aging)# time 300
```

最大エージング タイムを設定します。

- MAC アドレス テーブル エントリの最大経過時間を指定するには、*seconds* 引数を使用します。エージング タイムは最後にスイッチが MAC アドレスを検出した時点からカウントされます。MAC アドレスのエージング タイムの範囲は 300 ～ 3 万秒です。デフォルト値は 300 秒です。

**ステップ 8** **commit** コマンドまたは **end** コマンドを使用します。

**commit** ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

**end** ：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーション セッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーション セッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーション モードに留まります。

**ステップ 9** **show l2vpn bridge-domain** [ **detail** ]

**例**：

```
RP/0/RP0/cpu 0: router# show l2vpn bridge-domain detail
```

エージング フィールドに関する詳細を表示します。

## ブリッジ ポート レベルでの MAC フラッシュのディセーブル化

ブリッジ ドメイン レベルで MAC フラッシュをディセーブルにするには、次の作業を実行します。

ブリッジ ドメインまたはブリッジ ポート レベルで MAC フラッシュをディセーブルにできます。デフォルトでは、そのポートが機能しなくなると、特定のポートで学習される MAC はただちにフラッシュされます。

手順

**ステップ 1** **configure**

例：

```
RP/0/RP0/cpu 0: router# configure
```

XR コンフィギュレーション モードを開始します。

**ステップ 2** **l2vpn**

例：

```
RP/0/RP0/cpu 0: router(config)# l2vpn
RP/0/RP0/cpu 0: router(config-l2vpn)#
```

L2VPN コンフィギュレーション モードを開始します。

**ステップ 3** **bridge group** *bridge-group-name*

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn)# bridge group csco
RP/0/RP0/cpu 0: router(config-l2vpn-bg)#
```

ブリッジ ドメインを包含できるようにブリッジ グループを作成し、ブリッジ ドメインにネットワーク インターフェイスを割り当てます。

**ステップ 4** **bridge-domain** *bridge-domain-name*

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)#
```

ブリッジ ドメインを確立し、l2vpn ブリッジ グループ ブリッジ ドメイン コンフィギュレーション モードを開始します。

**ステップ 5** **mac**

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd)# mac
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-mac)#
```

l2vpn ブリッジ グループ ブリッジ ドメイン MAC コンフィギュレーション モードを開始します。

**ステップ 6** **port-down flush disable**

例：

```
RP/0/RP0/cpu 0: router(config-l2vpn-bg-bd-mac)#
port-down flush disable
```

ブリッジ ポートが機能しなくなったら、MAC フラッシュをディセーブルにします。

**ステップ 7** **commit** コマンドまたは **end** コマンドを使用します。

**commit** ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

**end** ：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーション セッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーション セッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーション モードに留まります。

# MAC アドレス取り消し

VMAC アドレス取り消し機能により、ダイナミックに学習された MAC アドレスが削除され、コンバージェンスが高速になります。この機能では、ラベル配布プロトコル（LDP）ベースの MAC アドレス取り消しメッセージが使用されます。MAC リストのタイプ/長さ/値（TLV）は、MAC アドレス取り消しメッセージの一部です。

この機能は、MAC アドレス取り消しの最適化もサポートしています。最適化により、PE は、アクセス側を介して CE デバイスから学習した MAC アドレスを保持できます。ピア PE から学習された MAC アドレスのみがフラッシュ アウトされます。これにより、接続回線（AC）側への不要な MAC フラッシュが回避され、帯域幅とリソースの使用率が向上します。

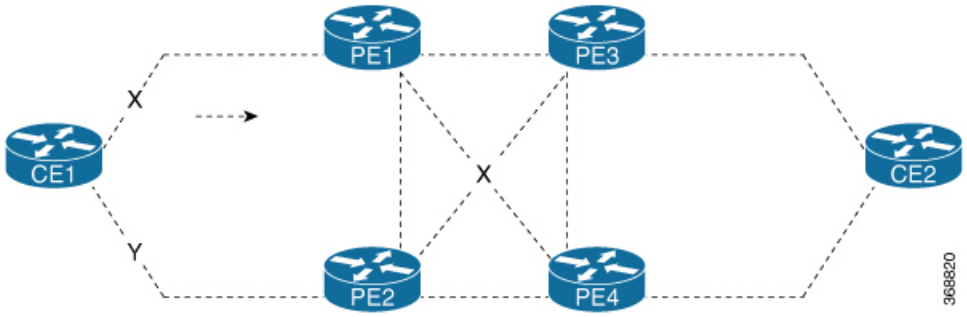
MAC アドレス取り消し機能はデフォルトでイネーブルになっています。MAC アドレス取り消し機能をディセーブルにするには、**mac withdraw disable** コマンドを使用します。

### トポロジ

CE1 が PE1 と PE2 にデュアルホーム接続されている次のトポロジを考えてみます。リンク X は VPLS にアクティブに参加しています。一方、Y は冗長リンクです。初期状態では、PE1、PE2、PE3、および PE4 は、トラフィック プロファイルに基づく各自の MAC 転送テーブルを学習し、トラフィックは既知のユニキャストになります。MAC アドレス取り消し機能がすべての PE でイネーブルになっている場合、PE は、MAC アドレス取り消しメッセージを受信したときに MAC エントリを削除します。次に、リンクのステータスに基づいた MAC アドレス取り消しメッセージを示します。

- シナリオ 1：PE1 の AC であるリンク X がダウンすると、PE1 は、LDP MAC 取り消し TLV メッセージ「FLUSH ALL MAC FROM ME」をネイバー PE に送信します。ピア PE は、PE1 からのみ学習した MAC アドレスを削除します。PE2、PE3、および PE4 は、PE1 から学習した MAC アドレスのみをフラッシュします。PE1 は、自身のアクセス側の AC がダウンしたときに MAC フラッシュを開始します。
- シナリオ 2：PE2 の AC であるリンク Y がアップ状態になると、PE2 は、LDP MAC 取り消し TLV メッセージ「FLUSH ALL MAC BUT ME」をネイバー PE に送信します。ピア PE は、要求を受信した PE からの MAC アドレスを除くすべての MAC アドレスをフラッシュします。

図 *3: MAC* アドレス取り消し




### 制約事項

MAC アドレス取り消しを設定する場合、次の制限事項が適用されます。

- この機能は、アクセス PW ではサポートされていません。
- この機能は、H-VPLS ネットワークではサポートされていません。
- この機能は、BGP シグナリングおよびディスカバリではサポートされていません。
- MAC 取り消しリレーはサポートされていません。

# MAC アドレス取り消しの設定

### 設定例

MAC アドレス取り消しを設定するには、次の作業を実行します。

```
/* Configure MAC address withdrawal on PE1. This configuration is required for scenario
 1 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group bg1
Router(config-l2vpn-bg)# bridge-domain bd1
Router(config-l2vpn-bg-bd)# mac
Router(config-l2vpn-bg-bd-mac)# withdraw state-down
Router(config-l2vpn-bg-bd-mac)# exit
Router(config-l2vpn-bg-bd)# interface tenGigE0/0/0/0
Router(config-l2vpn-bg-bd-ac)# exit
Router(config-l2vpn-bg-bd)# vfi vf1
Router(config-l2vpn-bg-bd-vfi)# neighbor 192.0.2.1 pw-id 1
Router(config-l2vpn-bg-bd-vfi-pw)# commit

/* Configure optimization of MAC address withdrawal on PE1. This configuration is required
 for scenario 1  */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group bg1
Router(config-l2vpn-bg)# bridge-domain bd1
Router(config-l2vpn-bg-bd)# mac
Router(config-l2vpn-bg-bd-mac)# withdraw optimize
Router(config-l2vpn-bg-bd-mac)# exit
Router(config-l2vpn-bg-bd)# neighbor 192.0.2.1 pw-id 1234
```

```
Router(config-l2vpn-bg-bd-pw)# exit
Router(config-l2vpn-bg-bd)# vfi vf1
Router(config-l2vpn-bg-bd-vfi)# neighbor 192.0.2.2 pw-id 1
Router(config-l2vpn-bg-bd-vfi-pw)# exit
Router(config-l2vpn-bg-bd-vfi)# neighbor 192.0.2.3 pw-id 2
Router(config-l2vpn-bg-bd-vfi-pw)# commit

/* MAC address withdrawal is enabled by default when AC comes up. Use the following
configuration if you want to disable MAC address withdrawal. This configuration is
required for scenario 2 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group bg1
Router(config-l2vpn-bg)# bridge-domain bd1
Router(config-l2vpn-bg-bd)# mac
Router(config-l2vpn-bg-bd-mac)# withdraw disable
Router(config-l2vpn-bg-bd-mac)# commit
```

### 実行コンフィギュレーション

ここでは、MAC アドレス取り消しの実行コンフィギュレーションを示します。

```
/* Configure MAC address withdrawal on PE1 */
l2vpn
 bridge group bg1
  bridge-domain bd1
   mac
    withdraw state-down
   !
   interface tengige 0/0/0/0
   !
   vfi vf1
    neighbor 192.0.2.1 pw-id 1
    !

/* Configure optimization of MAC address withdrawal on PE1 */
l2vpn
 bridge group bg1
  bridge-domain bd1
   mac
    withdraw optimize
   !
   neighbor neighbor 192.0.2.1 pw-id 1234
   !
   vfi vf1
    neighbor neighbor 192.0.2.2 pw-id 1
    !
    neighbor neighbor 192.0.2.3 pw-id 2


/* Disable MAC address widhrawal on PE2 */
l2vpn
 bridge group bg1
  bridge-domain bd1
   mac
    withdraw disable
   !
```

### 確認

MAC アドレス取り消しの設定を確認します。

```
/* Verify if MAC address widhrawal is configured on PE1 */
Router:PE1# show l2vpn bridge-domain detail
MAC learning: enabled
  MAC withdraw: enabled
    MAC withdraw sent on: bridge port down

/* Verify if optimization of MAC address withdrawal is configured on PE1 */
Router:PE1# show l2vpn bridge-domain detail
MAC learning: enabled
  MAC withdraw: enabled
    MAC withdraw sent on: bridge port down (optimization)
```

### 関連項目

- MAC アドレス取り消し （39 ページ）

### 関連コマンド

- mac withdraw
- show l2vpn bridge-domain detail

# マルチポイント レイヤ 2 サービスの設定例

ここで示す設定例は、次のとおりです。

## プロバイダーエッジ間のマルチポイント レイヤ2サービスの設定：例

これらの設定は、参加しているマルチポイント レイヤ2サービスのプロバイダーエッジ（PE）ノードのフル メッシュでレイヤ 2 VFI を作成する例を示しています。

この設定は、PE 1 を設定する例を示しています。

```
configure
 l2vpn
  bridge group 1
   bridge-domain PE1-VPLS-A
    interface TenGigE0/0/0/0
    vfi 1
     neighbor 10.2.2.2 pw-id 1
     neighbor 10.3.3.3 pw-id 1
     !
   !
 interface loopback 0
  ipv4 address 10.1.1.1 255.255.255.25
```

この設定は、PE 2 を設定する例を示しています。

```
configure
 l2vpn
  bridge group 1
   bridge-domain PE2-VPLS-A
    interface TenGigE0/0/0/1

    vfi 1
```

```
    neighbor 10.1.1.1 pw-id 1
    neighbor 10.3.3.3 pw-id 1
    !
  !
 interface loopback 0
  ipv4 address 10.2.2.2 255.255.255.25
```

この設定は、PE 3 を設定する例を示しています。

```
configure
 l2vpn
  bridge group 1
   bridge-domain PE3-VPLS-A
    interface TenGigE0/0/0/2
    vfi 1
     neighbor 10.1.1.1 pw-id 1
     neighbor 10.2.2.2 pw-id 1
     !
   !
 interface loopback 0
  ipv4 address 10.3.3.3 255.255.255.25
```

# プロバイダー エッジとカスタマー エッジ間のマルチポイント レイヤ 2 サービスの設定：例

この設定は、PE-to-CE ノードのマルチポイント レイヤ 2 サービスの設定方法を示しています。

```
configure
 interface TenGigE0/0/0/0
  l2transport---AC interface

  no ipv4 address
  no ipv4 directed-broadcast
  negotiation auto
  no cdp enable
```

# MAC アドレス取り消しフィールドの表示：例

この出力は、MAC アドレス取り消しフィールドの例を示しています。

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

Legend: pp = Partially Programmed.
Bridge group: 222, bridge-domain: 222, id: 0, state: up, ShgId: 0, MSTi: 0
  Coupled state: disabled
  MAC learning: enabled
  MAC withdraw: 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: disabled
Create time: 01/03/2017 11:01:11 (00:21:33 ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 1 (1 up), PBBs: 0 (0 up)
List of ACs:
  AC: TenGigE0/2/0/1.7, state is up
    Type VLAN; Num Ranges: 1
    Outer Tag: 21
    VLAN ranges: [22, 22]
    MTU 1508; XC ID 0x208000b; 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: bridge-domain policer
    Static MAC addresses:
    Statistics:
     packets: received 714472608 (multicast 0, broadcast 0, unknown unicast 0, unicast
0), sent 97708776
      bytes: received 88594603392 (multicast 0, broadcast 0, unknown unicast 0, unicast
0), sent 12115888224
      MAC move: 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 VFIs:
  VFI 222 (up)
    PW: neighbor 1.1.1.1, PW ID 222, state is up ( established )
      PW class not set, XC ID 0xc000000a
      Encapsulation MPLS, protocol LDP
      Source address 21.21.21.21
      PW type Ethernet, control word disabled, interworking none
      Sequencing not set

      PW Status TLV in use
        MPLS         Local                          Remote
        ------------ ------------------------------ ------------------------
        Label        24017                          24010
```

```
    Group ID     0x0                            0x0
    Interface    222                            222
    MTU          1500                           1500
    Control word disabled                       disabled
    PW type      Ethernet                       Ethernet
    VCCV CV type 0x2                            0x2
                 (LSP ping verification)        (LSP ping verification)
    VCCV CC type 0x6                            0x6
                 (router alert label)           (router alert label)
                 (TTL expiry)                   (TTL expiry)
    ------------ ------------------------------ ------------------------
  Incoming Status (PW Status TLV):
    Status code: 0x0 (Up) in Notification message
  MIB cpwVcIndex: 3221225482
  Create time: 01/03/2017 11:01:11 (00:21:33 ago)
  Last time status changed: 01/03/2017 11:21:01 (00:01:43 ago)
  Last time PW went down: 01/03/2017 11:15:21 (00:07:23 ago)
  MAC withdraw messages: sent 0, received 0
  Forward-class: 0
  Static MAC addresses:
  Statistics:
    packets: received 95320440 (unicast 0), sent 425092569
    bytes: received 11819734560 (unicast 0), sent 52711478556
    MAC move: 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
VFI Statistics:
  drops: illegal VLAN 0, illegal length 0
```

# IOS XR トランク インターフェイスでのブリッジング：例

次に、を単純な L2 スイッチとして設定する例を示します。

**特記事項**：

4 本の接続回線（AC）があるブリッジ ドメインを作成します。各 AC は、IOS XR トランク インターフェイスです（つまり、サブインターフェイス/EFP ではありません）。

- 次の例では、実行コンフィギュレーションが空であり、すべてのコンポーネントが作成されていると想定します。
- この例では、インターフェイス間のスイッチングを実行するようにを設定するために必要なすべての手順を示しています。ただし、no shut、negotiation auto などのインターフェイスを準備するためのコマンドは除外されています。
- ブリッジ ドメインは、作成直後に no shut 状態になります。
- この例ではトランク（つまりメイン）インターフェイスだけが使用されます。
- トランク インターフェイスは、タグ付き（IEEE 802.1Q）またはタグなし（つまり VLAN ヘッダーなし）フレームを処理できます。
- ブリッジ ドメインは、MAC アドレスに基づいて学習、フラッディング、および転送を行います。この機能は、タグの設定に関係なくフレームで動作します。

- ブリッジ ドメイン エンティティはシステム全体にわたります。単一の LC にすべてのブリッジ ドメイン AC を配置する必要はありません。これは、ブリッジ ドメインの設定に適用されます。
- ルータが予期したとおりに設定されていること、およびコマンドによあって新しい設定ステータスが表示されることを確認するには、show bundle および show l2vpn bridge-domain コマンドを使用します。
- 次の例の AC では、管理ダウン状態になっているインターフェイスを使用します。

設定例

```
RP/0/RSP0/CPU0:router#config
RP/0/RSP0/CPU0:router(config)#interface Bundle-ether10
RP/0/RSP0/CPU0:router(config-if)#l2transport
RP/0/RSP0/CPU0:router(config-if-l2)#interface GigabitEthernet0/2/0/5
RP/0/RSP0/CPU0:router(config-if)#bundle id 10 mode active
RP/0/RSP0/CPU0:router(config-if)#interface GigabitEthernet0/2/0/6
RP/0/RSP0/CPU0:router(config-if)#bundle id 10 mode active
RP/0/RSP0/CPU0:router(config-if)#interface GigabitEthernet0/2/0/0
RP/0/RSP0/CPU0:router(config-if)#l2transport
RP/0/RSP0/CPU0:router(config-if-l2)#interface GigabitEthernet0/2/0/1
RP/0/RSP0/CPU0:router(config-if)#l2transport
RP/0/RSP0/CPU0:router(config-if-l2)#interface TenGigE0/1/0/2
RP/0/RSP0/CPU0:router(config-if)#l2transport
RP/0/RSP0/CPU0:router(config-if-l2)#l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)#bridge group examples
RP/0/RSP0/CPU0:router(config-l2vpn-bg)#bridge-domain test-switch
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)#interface Bundle-ether10
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)#exit
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)#interface GigabitEthernet0/2/0/0
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)#exit
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)#interface GigabitEthernet0/2/0/1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)#exit
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)#interface TenGigE0/1/0/2
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)#commit
RP/0/RSP0/CPU0:Jul 26 10:48:21.320 EDT: config[65751]: %MGBL-CONFIG-6-DB_COMMIT :
Configuration committed by user 'lab'. Use 'show configuration commit changes 1000000973'
 to view the changes.
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)#end
RP/0/RSP0/CPU0:Jul 26 10:48:21.342 EDT: config[65751]: %MGBL-SYS-5-CONFIG_I : Configured
 from console by lab
RP/0/RSP0/CPU0:router#show bundle Bundle-ether10

Bundle-Ether10
  Status:                                  Down
  Local links <active/standby/configured>:   0 / 0 / 2
  Local bandwidth <effective/available>:     0 (0) kbps
  MAC address (source):                    0024.f71e.22eb (Chassis pool)
  Minimum active links / bandwidth:        1 / 1 kbps
  Maximum active links:                    64
  Wait while timer:                        2000 ms
  LACP:                                    Operational
    Flap suppression timer:                Off
  mLACP:                                   Not configured
  IPv4 BFD:                                Not configured

  Port                Device           State        Port ID         B/W, kbps
  ------------------  ---------------  -----------  --------------  ----------
  Gi0/2/0/5           Local            Configured   0x8000, 0x0001     1000000
      Link is down
```

```
  Gi0/2/0/6             Local            Configured   0x8000, 0x0002     1000000
      Link is down

RP/0/RSP0/CPU0:router#
RP/0/RSP0/CPU0:router#show l2vpn bridge-domain group examples
Bridge group: examples, bridge-domain: test-switch, id: 2000, state: up, ShgId: 0, MSTi:
 0
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 4 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up)
  List of ACs:
    BE10, state: down, Static MAC addresses: 0
    Gi0/2/0/0, state: up, Static MAC addresses: 0
    Gi0/2/0/1, state: down, Static MAC addresses: 0
    Te0/5/0/1, state: down, Static MAC addresses: 0
  List of VFIs:
RP/0/RSP0/CPU0:router#
```

次の表に、設定手順（アクション）およびこの例の対応する目的を示します。

### 手順

**ステップ 1** **configure**

グローバル コンフィギュレーション モードを開始します。

**ステップ 2** **interface Bundle-ether10**

新しいバンドル トランク インターフェイスを作成します。

**ステップ 3** **l2transport**

Bundle-ether10 を L3 インターフェイスから L2 インターフェイスに変更します。

**ステップ 4** **interface GigabitEthernet0/2/0/5**

インターフェイス設定モードを開始します。GigabitEthernet0/2/0/5 で機能するようコンフィギュレーション モードを変更します。

**ステップ 5** **bundle id 10 mode active**

GigabitEthernet0/2/0/5 を Bundle-ether10 のメンバーとして設定します。**mode active** キーワードは、LACP プロトコルを指定します。

**ステップ 6** **interface GigabitEthernet0/2/0/6**

インターフェイス設定モードを開始します。GigabitEthernet0/2/0/6 で機能するようコンフィギュレーション モードを変更します。

**ステップ 7** **bundle id 10 mode active**

GigabitEthernet0/2/0/6 を Bundle-ether10 のメンバーとして設定します。**mode active** キーワードは、LACP プロトコルを指定します。

**ステップ 8** **interface GigabitEthernet0/2/0/0**

インターフェイス設定モードを開始します。GigabitEthernet0/2/0/0 で機能するようコンフィギュレーション モードを変更します。

**ステップ 9** **l2transport**

GigabitEthernet0/2/0/0 を L3 インターフェイスから L2 インターフェイスに変更します。

**ステップ 10** **interface GigabitEthernet0/2/0/1**

インターフェイス設定モードを開始します。GigabitEthernet0/2/0/1 で機能するようコンフィギュレーション モードを変更します。

**ステップ 11** **l2transport**

GigabitEthernet0/2/0/1 を L3 インターフェイスから L2 インターフェイスに変更します。

**ステップ 12** **interface TenGigE0/1/0/2**

インターフェイス設定モードを開始します。TenGigE0/1/0/2 で機能するようコンフィギュレーション モードを変更します。

**ステップ 13** **l2transport**

TenGigE0/1/0/2 を L3 インターフェイスから L2 インターフェイスに変更します。

**ステップ 14** **l2vpn**

L2VPN コンフィギュレーション モードを開始します。

**ステップ 15** **bridge group examples**

ブリッジ グループ **examples** を作成します。

**ステップ 16** **bridge-domain test-switch**

ブリッジ ドメイン **test-switch** を作成します。これは、ブリッジ グループ **examples** のメンバーです。

**ステップ 17** **interface Bundle-ether10**

Bundle-ether10 をブリッジ ドメイン test-switch の AC として設定します。

**ステップ 18** **exit**

ブリッジ ドメイン AC コンフィギュレーション サブモードを終了し、次の AC を設定できるようにします。

**ステップ 19** **interface GigabitEthernet0/2/0/0**

GigabitEthernet0/2/0/0 をブリッジ ドメイン **test-switch** の AC として設定します。

**ステップ 20** **exit**

ブリッジ ドメイン AC コンフィギュレーション サブモードを終了し、次の AC を設定できるようにします。

**ステップ 21** **interface GigabitEthernet0/2/0/1**

GigabitEthernet0/2/0/1 をブリッジ ドメイン **test-switch** の AC として設定します。

**ステップ 22** **exit**

ブリッジ ドメイン AC コンフィギュレーション サブモードを終了し、次の AC を設定できるようにします。

**ステップ 23** **interface TenGigE0/1/0/2**

インターフェイス TenGigE0/1/0/2 をブリッジ ドメイン **test-switch** の AC として設定します。

**ステップ 24** **commit** コマンドまたは **end** コマンドを使用します。

**commit** ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

**end** ：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーション セッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーション セッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーション モードに留まります。

# イーサネット フロー ポイントでのブリッジング：例

次に、イーサネットフローポイント（EFP）を通過するトラフィックでレイヤ2スイッチングを実行するように を設定する例を示します。EFP トラフィックには通常、1 つ以上の VLAN ヘッダーがあります。IOS XR トランクと IOS-XR EFP の両方をブリッジ ドメインで接続回線として結合できますが、この例では EFP だけを使用します。

**特記事項**：

- EFPは、レイヤ2サブインターフェイスです。これは常に、トランク インターフェイスの下で作成されます。トランク インターフェイスは、EFPを作成する前に存在している必要があります。
- 空の設定では、バンドル インターフェイス トランクは存在しませんが、物理トランク インターフェイスは自動的に設定されます。したがって、バンドル トランクだけが作成されます。
- この例では、サブインターフェイス番号および VLAN ID は同じですが、これは便利ではなく、必要性はありません。同じ値である必要はありません。
- ブリッジ ドメイン test-efp には、3 本の接続回線（AC）があります。AC はすべて EFP です。
- VLAN ID が 999 のフレームだけが EFP に入ります。これによって、このブリッジ ドメインのすべてのトラフィックで同じ VLAN カプセル化を確保できます。

- 次の例の AC では、管理ダウン状態（「未解決」状態）になっているインターフェイスを使用します。AC として存在しないインターフェイスを使用するブリッジ ドメインは正常であり、このような設定のコミットは失敗しません。この場合、ブリッジ ドメインのステータスは、欠落しているインターフェイスを設定するまで **unresolved** と表示されます。

設定例

```
RP/0/RSP1/CPU0:router#configure
RP/0/RSP1/CPU0:router(config)#interface Bundle-ether10
RP/0/RSP1/CPU0:router(config-if)#interface Bundle-ether10.999 l2transport
RP/0/RSP1/CPU0:router(config-subif)#encapsulation dot1q 999
RP/0/RSP1/CPU0:router(config-subif)#interface GigabitEthernet0/6/0/5
RP/0/RSP1/CPU0:router(config-if)#bundle id 10 mode active
RP/0/RSP1/CPU0:router(config-if)#interface GigabitEthernet0/6/0/6
RP/0/RSP1/CPU0:router(config-if)#bundle id 10 mode active
RP/0/RSP1/CPU0:router(config-if)#interface GigabitEthernet0/6/0/7.999 l2transport
RP/0/RSP1/CPU0:router(config-subif)#encapsulation dot1q 999
RP/0/RSP1/CPU0:router(config-subif)#interface TenGigE0/1/0/2.999 l2transport
RP/0/RSP1/CPU0:router(config-subif)#encapsulation dot1q 999
RP/0/RSP1/CPU0:router(config-subif)#l2vpn
RP/0/RSP1/CPU0:router(config-l2vpn)#bridge group examples
RP/0/RSP1/CPU0:router(config-l2vpn-bg)#bridge-domain test-efp
RP/0/RSP1/CPU0:router(config-l2vpn-bg-bd)#interface Bundle-ether10.999
RP/0/RSP1/CPU0:router(config-l2vpn-bg-bd-ac)#exit
RP/0/RSP1/CPU0:router(config-l2vpn-bg-bd)#interface GigabitEthernet0/6/0/7.999
RP/0/RSP1/CPU0:router(config-l2vpn-bg-bd-ac)#exit
RP/0/RSP1/CPU0:router(config-l2vpn-bg-bd)#interface TenGigE0/1/0/2.999
RP/0/RSP1/CPU0:router(config-l2vpn-bg-bd-ac)#commit
RP/0/RSP1/CPU0:router(config-l2vpn-bg-bd-ac)#end
RP/0/RSP1/CPU0:router#
RP/0/RSP1/CPU0:router#show l2vpn bridge group examples
Fri Jul 23 21:56:34.473 UTC Bridge group: examples, bridge-domain: test-efp, id: 0,
state: up, ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 3 (0 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up)
  List of ACs:
    BE10.999, state: down, Static MAC addresses: 0
    Gi0/6/0/7.999, state: unresolved, Static MAC addresses: 0
    Te0/1/0/2.999, state: down, Static MAC addresses: 0
  List of VFIs:
RP/0/RSP1/CPU0:router#
```

次の表に、設定手順（アクション）およびこの例の対応する目的を示します。

**手順**

**ステップ 1** **configure**

グローバル コンフィギュレーション モードを開始します。

**ステップ 2** **interface Bundle-ether10**

新しいバンドル トランク インターフェイスを作成します。

**ステップ 3** **interface Bundle-ether10.999 l2transport**

新しいバンドル トランクに EFP を作成します。

**ステップ 4** **encapsulation dot1q 999**

この EFP に VLAN ID 999 を割り当てます。

**ステップ 5** **interface GigabitEthernet0/6/0/5**

インターフェイス設定モードを開始します。GigabitEthernet0/6/0/5 で機能するようコンフィギュレーション モードを変更します。

**ステップ 6** **bundle id 10 mode active**

GigabitEthernet0/6/0/5 を Bundle-ether10 のメンバーとして設定します。**mode active** キーワードは、LACP プロトコルを指定します。

**ステップ 7** **interface GigabitEthernet0/6/0/6**

インターフェイス設定モードを開始します。GigabitEthernet0/6/0/6 で機能するようコンフィギュレーション モードを変更します。

**ステップ 8** **bundle id 10 mode active**

GigabitEthernet0/6/0/6 を Bundle-ether10 のメンバーとして設定します。**mode active** キーワードは、LACP プロトコルを指定します。

**ステップ 9** **interface GigabitEthernet0/6/0/7.999 l2transport**

GigabitEthernet0/6/0/7 に EFP を作成します。

**ステップ 10** **encapsulation dot1q 999**

この EFP に VLAN ID 999 を割り当てます。

**ステップ 11** **interface TenGigE0/1/0/2.999 l2transport**

TenGigE0/1/0/2 に EFP を作成します。

**ステップ 12** **encapsulation dot1q 999**

この EFP に VLAN ID 999 を割り当てます。

**ステップ 13** **l2vpn**

L2VPN コンフィギュレーション モードを開始します。

**ステップ 14** **bridge group examples**

**examples** という名前のブリッジ グループを作成します。

**ステップ 15** **bridge-domain test-efp**

**test-efp** という名前のブリッジ ドメインを作成します。これは、ブリッジ グループ **examples** のメンバーです。

**ステップ 16** **interface Bundle-ether10.999**

Bundle-ether10.999 を **test-efp** という名前のブリッジ ドメインの AC として設定します。

**ステップ 17** **exit**

ブリッジ ドメイン AC コンフィギュレーション サブモードを終了し、次の AC を設定できるようにします。

**ステップ 18** **interface GigabitEthernet0/6/0/7.999**

GigabitEthernet0/6/0/7.999 を **test-efp** という名前のブリッジ ドメインの AC として設定します。

**ステップ 19** **exit**

ブリッジ ドメイン AC コンフィギュレーション サブモードを終了し、次の AC を設定できるようにします。

**ステップ 20** **interface TenGigE0/1/0/2.999**

インターフェイス TenGigE0/1/0/2.999 を **test-efp** という名前のブリッジ ドメインの AC として設定します。

**ステップ 21** **commit** コマンドまたは **end** コマンドを使用します。

**commit** ：設定の変更を保存し、コンフィギュレーション セッションに留まります。

**end** ：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーション セッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーション セッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーション モードに留まります。

# LDP ベースの VPLS および VPWS FAT 擬似回線

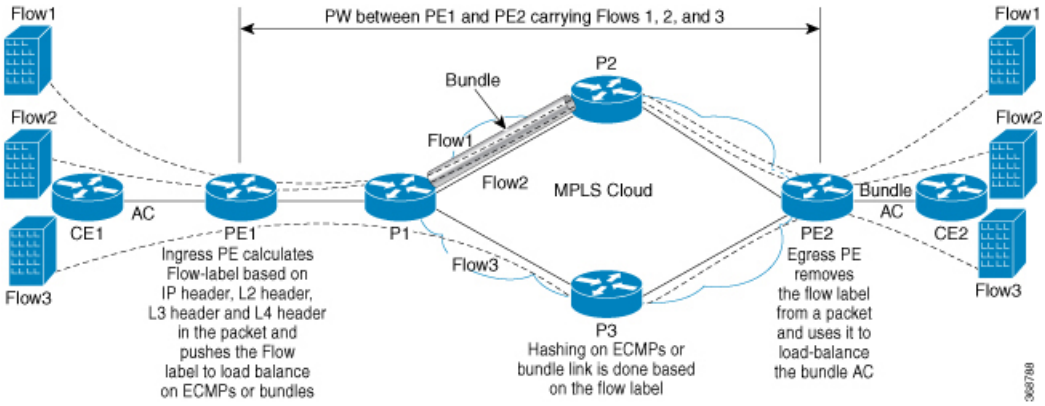
LDP ベースの VPLS および VPWS FAT 擬似回線機能を使用すると、プロバイダー（P）のルータでフローベースのロード バランシングを使用してプロバイダー エッジ（PE）デバイス間でトラフィックを転送できます。この機能は、MPLS パケット スイッチド ネットワーク上で疑似回線（PW）のフロー認識型転送（FAT）を使用して、仮想プライベート LAN サービス（VPLS）およびバーチャル プライベート ワイヤ サービス（VPWS）の LDP ベースのシグナリング擬似回線間でトラフィックのロードバランシングを行います。

FAT PW は、PW 内の個々のフローを識別する機能を提供します。また、ルータに対してこれらのフローを使用してトラフィックをロードバランスする機能を提供します。等価コストマルチパス（ECMP）が使用されている場合は、FAT PW はコア内のトラフィックのロード バランスに使用されます。インポジション PE に流入する不可分のパケット フローに基づいて、フロー ラベルが作成されます。このフロー ラベルは、パケットの一番下のラベルとして挿入されます。P ルータは、フロー ラベルをロードバランシングに使用し、コア内の ECMP パスに全体わたって、またはリンクがバンドルされたパス全体にわたって、より適切にトラフィック

を分配します。フローは、トラフィックの送信元/宛先 IP アドレスとトラフィックのレイヤ 4 送信元/宛先ポートによって識別されるか、またはトラフィックの送信元/宛先 MAC アドレスによって識別されます。

次の図に、FAT PW と、ECMP およびバンドルされたリンクに分配される 2 つのフローの例を示します。

**図 *4 : FAT PW* と *ECMP* およびバンドルされたリンクに分配される *2* つのフロー**




フロー ラベルと呼ばれるラベルがさらにスタックに追加されます。このラベルは、PE 上の一意の着信フローごとに生成されます。フロー ラベルは、PW 内のフローを区別する一意の ID で、送信元/宛先 MAC アドレスと送信元/宛先 IP アドレスから取得されます。フロー ラベルには、ラベルスタック終端（EOS）ビットセットが含まれています。フロー ラベルは、VC ラベルの後ろ、およびコントロール ワード（存在する場合）の前に挿入されます。入力 PE は、フロー ラベルを計算し、転送します。FAT PW コンフィギュレーションは、フロー ラベルをイネーブルにします。出力 PE は、決定が行われないように、フロー ラベルを廃棄します。

すべてのコア ルータが、FAT PW でフロー ラベルに基づいてロード バランシングを実行します。これにより、ECMP とリンク バンドルへのフローの分配が可能になります。

このトポロジでは、インポジション ルータ（PE1）によってトラフィックにフロー ラベルが追加されます。ディスポジション ルータ（PE2）では、フロー ラベルを持つトラフィックとフロー ラベルを持たないトラフィックの混合タイプが許可されます。P ルータはフロー ラベルを使用して、PE 間でトラフィックのロード バランシングを行います。PE2 は、トラフィックのフローラベルを無視し、すべてのユニキャスト トラフィックで 1 つのラベルを使用します。

# LDP ベースの VPLS および VPWS FAT 擬似回線の設定

この機能は、VPLS および VPWS サービスの BGP シグナリング擬似回線間のトラフィックではサポートされていません。

### 設定例

PE1 と PE2 の両方で VPLS および VPWS FAT 擬似回線を設定するには、次の作業を実行します。

```
/* Configure LDP-based VPLS FAT Pseudowire */
Router# configure
```

```
Router(config)# l2vpn
Router(config-l2vpn)# pw-class vpls
Router(config-l2vpn-pwc)# encapsulation mpls
Router(config-l2vpn-pwc-mpls)# load-balancing
Router(config-l2vpn-pwc-mpls-load-bal)# flow-label both
Router(config-l2vpn-pwc-mpls-load-bal)# exit
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group bg0
Router(config-l2vpn-bg)# bridge-domain bd1
Router(config-l2vpn-bg-bd)#
Router(config-l2vpn-bg-bd-ac)# exit
Router(config-l2vpn-bg-bd)# vfi 2001
Router(config-l2vpn-bg-bd-vfi)# neighbor 192.0.2.1 pw-id 1
Router(config-l2vpn-bg-bd-vfi-pw)# pw-class vpls
Router(config-l2vpn-bg-bd-vfi-pw)# commit

/* Configure LDP-based VPWS FAT Pseudowire */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# pw-class vpws
Router(config-l2vpn-pwc)# encapsulation mpls
Router(config-l2vpn-pwc-mpls)# load-balancing
Router(config-l2vpn-pwc-mpls-load-bal)# flow-label both
Router(config-l2vpn-pwc-mpls-load-bal)# exit
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group vpws
Router(config-l2vpn-xc)# p2p 1001
Router(config-l2vpn-xc-p2p)#
Router(config-l2vpn-xc-p2p)# neighbor ipv4 192.0.2.1 pw-id 1001
Router(config-l2vpn-xc-p2p-pw)# pw-class vpws
Router(config-l2vpn-xc-p2p-pw)# commit
```

### 実行コンフィギュレーション

ここでは、VPLS および VPWS FAT 擬似回線の実行コンフィギュレーションを示します。

```
/* Configure LDP-based VPLS FAT Pseudowire */
l2vpn
pw-class vpls
  encapsulation mpls
   load-balancing
    flow-label both
   !
  !
bridge group bg0
  bridge-domain bd1

   !
   vfi 2001
    neighbor 192.0.2.1 pw-id 1
     pw-class vpls
    !
    !

/* Configure LDP-based VPWS FAT Pseudowire */
l2vpn
pw-class vpws
  encapsulation mpls
   load-balancing
    flow-label both
```

```
   !
  !
!
l2vpn
 xconnect group vpws
  p2p 1001

   neighbor ipv4 192.0.2.1 pw-id 1001
    pw-class vpws
   !
  !
```

### 確認

LDP ベースの VPLS および VPWS FAT 擬似回線機能を正常に設定したことを確認します。

```
/* Verify the LDP-based VPLS FAT Pseudowire configuration */
Router# show l2vpn bridge-domain group bg0 bd-name bd1 detail
Fri May 17 06:00:45.745 UTC
  List of VFIs:
    VFI 1 (up)
      PW: neighbor 192.0.2.1, PW ID 1, state is up ( established )
        PW class vpws, XC ID 0xc0000001
        Encapsulation MPLS, protocol LDP
        Source address 192.0.2.5
        PW type Ethernet, control word disabled, interworking none
        Sequencing not set
        LSP : Up
        Flow Label flags configured (Tx=1,Rx=1), negotiated (Tx=1,Rx=1)

        PW Status TLV in use
          MPLS         Local                          Remote
          ------------ ------------------------------ ------------------------
          Label        24000                          24000
          Group ID     0x0                            0x0
          Interface    1                              1
          MTU          1500                           1500
          Control word disabled                       disabled
          PW type      Ethernet                       Ethernet
          VCCV CV type 0x2                            0x2
                       (LSP ping verification)        (LSP ping verification)
          VCCV CC type 0x6                            0x6
                       (router alert label)           (router alert label)
                       (TTL expiry)                   (TTL expiry)
          ------------ ------------------------------ ------------------------
        Incoming Status (PW Status TLV):
          Status code: 0x0 (Up) in Notification message
        MIB cpwVcIndex: 3221225473
        Create time: 12/05/2019 11:17:59 (4d18h ago)
        Last time status changed: 12/05/2019 11:24:03 (4d18h ago)
        MAC withdraw messages: sent 7, received 9
        Forward-class: 0
        Static MAC addresses:
        Statistics:
          packets: received 0 (unicast 0), sent 0
          bytes: received 0 (unicast 0), sent 0
          MAC move: 0
        Storm control drop counters:
          packets: broadcast 0, multicast 0, unknown unicast 0
          bytes: broadcast 0, multicast 0, unknown unicast 0
      MAC learning: enabled
      Flooding:
        Broadcast & Multicast: enabled
```

```
        Unknown unicast: enabled
      MAC aging time: 900 s, Type: inactivity
      MAC limit: 32000, Action: none, Notification: syslog
      MAC limit reached: no, threshold: 75%
      MAC port down flush: enabled
      MAC Secure: disabled, Logging: disabled
      Split Horizon Group: none
      E-Tree: Root
      DHCPv4 Snooping: disabled
      DHCPv4 Snooping profile: none
      IGMP Snooping: disabled
      IGMP Snooping profile: none
      MLD Snooping profile: none
      Storm Control: bridge-domain policer
      DHCPv4 Snooping: disabled
      DHCPv4 Snooping profile: none
      IGMP Snooping: disabled
      IGMP Snooping profile: none
      MLD Snooping profile: none

/* Verify the LDP-based VPWS FAT Pseudowire configuration */
Router# show l2vpn xconnect group vpws detail
Group vpws, XC 1001, state is up; Interworking none
  AC: , state is up
    Type VLAN; Num Ranges: 1
    Rewrite Tags: []
    VLAN ranges: [1001, 1001]
    MTU 1504; XC ID 0x47f; interworking none
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0
      drops: illegal VLAN 0, illegal length 0
  PW: neighbor 192.0.2.1, PW ID 1001, state is up ( established )
    PW class vpws, XC ID 0xc0000548
    Encapsulation MPLS, protocol LDP
    Source address 192.0.2.2
    PW type Ethernet, control word disabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set
    LSP : Up
    Flow Label flags configured (Tx=1,Rx=1), negotiated (Tx=1,Rx=1)

    PW Status TLV in use
      MPLS         Local                          Remote
      ------------ ------------------------------ ------------------------------
      Label        25011                          25010
      Group ID     0xf000190                      0x228
      Interface
      MTU          1504                           1504
      Control word disabled                       disabled
      PW type      Ethernet                       Ethernet
      VCCV CV type 0x2                            0x2
                   (LSP ping verification)        (LSP ping verification)
      VCCV CC type 0x6                            0x6
                   (router alert label)           (router alert label)
                   (TTL expiry)                   (TTL expiry)
      ------------ ------------------------------ ------------------------------
    Incoming Status (PW Status TLV):
      Status code: 0x0 (Up) in Notification message
    Outgoing Status (PW Status TLV):
      Status code: 0x0 (Up) in Notification message
    MIB cpwVcIndex: 3221226824
    Create time: 17/05/2019 05:52:59 (00:05:22 ago)
    Last time status changed: 17/05/2019 05:53:11 (00:05:10 ago)
```

```
Statistics:
  packets: received 0, sent 0
 bytes: received 0, sent 0
```

## 関連項目

- LDP ベースの VPLS および VPWS FAT 擬似回線 （52 ページ）

## 関連コマンド

- show l2vpn xconnect detail