

# IOS XR L2VPN サービスと機能

## 目次

### 概要

1. [ポイントツーポイント サービスとマルチポイント サービス](#)
  - 1.1 [ポイントツーポイント サービス](#)
  - 1.2 [マルチポイント サービス](#)
2. [接続回線](#)
  - 2.1 [ASR 9000 のイーサネット仮想回線](#)
    - 2.1.1 [着信インターフェイスの照合](#)
    - 2.1.2 [VLAN の操作](#)
  - 2.2 [Cisco IOS XR 非 EVC ルータの動作 \( CRS および XR12000 \)](#)
3. [ポイントツーポイント サービス](#)
  - 3.1 [ローカル スイッチング](#)
    - 3.1.1 [メイン インターフェイス](#)
    - 3.1.2 [サブインターフェイスと VLAN 操作](#)
  - 3.2 [Virtual Private Wire Service](#)
    - 3.2.1 [概要](#)
    - 3.2.2 [PW と AC のペアのステータス](#)
    - 3.2.3 [タイプ 4 とタイプ 5 の PW](#)
    - 3.2.4 [マルチセグメント PW](#)
    - 3.2.5 [冗長性](#)
  - 3.3 [CDP](#)
    - 3.3.1 [L2VPN PE のメイン インターフェイスの CDP が無効の場合](#)
    - 3.3.2 [L2VPN PE のメイン インターフェイスの CDP が有効の場合](#)
  - 3.4 [スパニング ツリー](#)
4. [マルチポイント サービス](#)
  - 4.1 [ローカル スイッチング](#)
  - 4.2 [フル MST](#)
  - 4.3 [BVI](#)
  - 4.4 [VPLS](#)
    - 4.4.1 [概要](#)
    - 4.4.2 [PW のタイプと転送されるタグ](#)
    - 4.4.3 [自動検出とシグナリング](#)
    - 4.4.4 [MAC の消去と回収](#)
    - 4.4.5 [H-VPLS](#)
    - 4.4.6 [スプリット ホライズン グループ \( SHG \)](#)
    - 4.4.7 [冗長性](#)
  - 4.5 [トラフィック ストーム制御](#)
  - 4.6 [MAC 移動](#)

## [4.7 IGMP と MLD スヌーピング](#)

## [5. その他の L2VPN のトピック](#)

### [5.1 ロードバランシング](#)

### [5.2 ログイン](#)

### [5.3 イーサネットサービス アクセスリスト](#)

### [5.4 イーサネット出力フィルタ](#)

## 概要

このドキュメントでは、基本的なレイヤ 2 ( L2 ) VPN ( L2VPN ) トポロジについて説明します。設計、サービス、機能、および設定について説明するために、基本的な例を使用します。詳細については、『[Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ L2VPN およびイーサネット サービス構成ガイド、リリース 4.3.x](#)』を参照してください。

## 1. ポイントツーポイント サービスとマルチポイント サービス

L2VPN 機能は、ポイントツーポイント サービスとマルチポイント サービスを実現するための機能を提供します。

### 1.1 ポイントツーポイント サービス

ポイントツーポイント サービスは、基本的に 2 つのエンド ノード間のトランスポート回路をエミュレートして、これらのエンド ノードがポイントツーポイント リンク上に直接接続されているかのようにします。このサービスを使用すると、2 つのサイトを接続することができます。

実際には、2 つのエンド ノードの間に複数のルータを置くことができるので、ポイントツーポイント サービスを提供する設計は複数通りあります。

1 台のルータの 2 つのインターフェイスの間で、ローカル スイッチングを実行できます。

2 台のルータ間でマルチプロトコル ラベル スイッチング ( MPLS ) の疑似回線 ( PW ) を使用することもできます。

ルータで、2 つの PW の間でフレームをスイッチングできます。この例では、これはマルチセグメント PW です。

PW の冗長性機能によって冗長性を実現できます。

他の設計も可能ですが、すべてをここに記載することはできません。

### 1.2 マルチポイント サービス

マルチポイント サービスは、ブリッジドメインに接続されているすべてのホストが論理的に同じ

イーサネット セグメントに接続されているかのように、ブロードキャスト ドメインをエミュレートします。

すべてのホストを同じルータやスイッチに接続できます。

複数のスイッチで、従来のイーサネット スイッチングを実行できます。ループを避けるためにスパニング ツリーを使用する必要があります。

仮想プライベート LAN サービス (VPLS) を用いると、MPLS PW を使用して複数サイト間にブロードキャスト ドメインを拡大できます。

階層型 VPLS を使用すると、拡張性を向上させることができます。

## 2. 接続回線

### 2.1 ASR 9000 のイーサネット仮想回線

#### 2.1.1 着信インターフェイスの照合

接続回線 (AC) の基本的なルールには次のようなものがあります。

- パケットを L2VPN 機能によって処理するためには、*I2transport* キーワードが設定されたインターフェイスでそのパケットが受信される必要があります。
- このインターフェイスには、インターフェイス コンフィギュレーション モードで *I2transport* コマンドが設定されたメイン インターフェイス、またはサブインターフェイス番号の後に *I2transport* キーワードが設定されたサブインターフェイスを使用できます。
- 最長一致によってパケットの着信インターフェイスを決定します。最長一致では、着信パケットをサブインターフェイスに対応させるために、次の順序で条件を確認します。
  1. 着信フレームに 2 つの dot1q タグが含まれており、同じ 2 つの dot1q タグ (802.1Q トンネリングまたは QinQ) が設定されたサブインターフェイスと一致する。これが、考えられる最長の一致です。
  2. 着信フレームには 2 つの dot1q タグが含まれており、dot1q の最初のタグが同じで 2 番目のタグが *any* に設定されたサブインターフェイスと一致する。
  3. 着信フレームに 1 つの dot1q タグが含まれており、同じ dot1q タグと *exact* キーワードが設定されたサブインターフェイスと一致する。
  4. 着信フレームに 1 つ以上の dot1q タグが含まれており、それらの dot1q タグのうち 1 つが設定されたサブインターフェイスと一致する。
  5. 着信フレームに dot1q タグが含まれておらず、*encapsulation untagged* コマンドが設定されたサブインターフェイスと一致する。
  6. 着信フレームは他のどのサブインターフェイスとも一致しないため、*encapsulation default* コマンドが設定されたサブインターフェイスと一致する。
  7. 着信フレームはどのサブインターフェイスとも一致しないため、*I2transport* が設定されたメイン インターフェイスと一致する。
- イーサネット仮想接続 (EVC) モデルを使用しない従来のルータでは、サブインターフェイス

すでに設定された VLAN タグは、L2VPN 機能によって転送される前にフレームから削除 (ポップ) されます。

- EVC インフラストラクチャを使用する Cisco ASR 9000 シリーズ アグリゲーション サービス ルータのデフォルトのアクションでは、既存のタグは維持されます。デフォルトを変更するには **rewrite** コマンドを使用します。
- ブリッジドメインにブリッジ仮想インターフェイス (BVI) がある場合、BVI はタグを持たないルーティング インターフェイスであるため、すべての着信タグをポップする必要があります。詳細については、「[BVI](#)」の項を参照してください。

これらのルールについて説明するいくつかの例を次に示します。

1. 基本的な例は、VLAN タグが含まれているかどうかにかかわらず、物理ポートで受信したすべてのトラフィックを転送する必要がある場合です。メイン インターフェイスで **I2transport** を設定した場合、その物理ポートで受信されたすべてのトラフィックは、L2VPN 機能によって転送されます。

```
interface GigabitEthernet0/0/0/2
```

**I2transport** このメイン インターフェイスにサブインターフェイスがある場合、どのサブインターフェイスにも一致しなかったフレームはすべてメイン インターフェイスによってキャッチされます。これが最長一致ルールです。

2. バンドル インターフェイスおよびサブインターフェイスを **I2transport** として設定できます。

```
interface Bundle-Ether1
  I2transport
```

3. 最長一致では他のサブインターフェイスに一致しなかったすべてのタグ付きまたはタグなしのトラフィックを一致させるには、**I2transport** サブインターフェイスで **encapsulation default** を使用します。(例 4 を参照)。**I2transport** キーワードは、メイン インターフェイスのサブインターフェイスの下ではなく、サブインターフェイス名の中で設定します。

```
interface GigabitEthernet0/1/0/3.1 I2transport
```

**encapsulation default** タグなしフレームだけを一致させるには、**encapsulation untagged** を設定します。

4. 複数のサブインターフェイスがある場合、着信インターフェイスを判断するために、着信フレームの最長一致テストを実行します。

```
interface GigabitEthernet0/1/0/3.1 I2transport
  encapsulation default
```

```
!
interface GigabitEthernet0/1/0/3.2 I2transport
  encapsulation dot1q 2
```

```
!
interface GigabitEthernet0/1/0/3.3 I2transport
```

**encapsulation dot1q 2 second-dot1q 3** この設定では、次の点に注意してください。

- 外部 VLAN タグ 2 と内部 VLAN タグ 3 を持つ QinQ フレームは、.1、.2、.3 の各サブインターフェイスに一致する可能性があります。最長一致ルールによって .3 サブインターフェイスに割り当てられます。これは、.3 の 2 つのタグが、.2 の 1 つのタグやタグがない .1 よりも長いからです。

- 外部 VLAN タグ 2 と内部 VLAN タグ 4 を持つ QinQ フレームは、.2 サブインターフェイスに割り当てられます。encapsulation dot1q 2 は VLAN タグ 2 のみを持つ dot1q フレームと一致するだけでなく、外部タグ 2 を持つ QinQ フレームとも一致するからです。QinQ フレームと一致させないようにするには、例 5 ( exact キーワード ) を参照してください。
- 外部 VLAN タグ 3 を持つ QinQ フレームは、.1 サブインターフェイスに一致します。
- VLAN タグ 2 を持つ dot1q フレームは、.2 サブインターフェイスに一致します。
- VLAN タグ 3 を持つ dot1q フレームは、.1 サブインターフェイスに一致します。

5. dot1q フレームに一致させ、QinQ フレームには一致させないようにするには、exact キーワードを使用します。

```
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2 exact
```

この設定は、ただ 1 つの VLAN タグを持つフレームにのみ一致するため、外部 VLAN タグ 2 を持つ QinQ フレームには一致しません。

6. Cisco Discovery Protocol ( CDP ) パケットやマルチ スパニング ツリー ( MST ) ブリッジ プロトコル データ ユニット ( BPDU ) などのタグなしフレームにのみ一致させるには、untagged キーワードを使用します。

```
interface GigabitEthernet0/1/0/3.1 l2transport
encapsulation default
!
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation untagged
!
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
```

この設定では、次の点に注意してください。

- VLAN タグ 3 を持つ dot1q フレームや外部タグ 3 を持つ QinQ フレームは、.3 サブインターフェイスに一致します。
- その他の dot1q フレームまたは QinQ フレームはすべて、.1 サブインターフェイスに一致します。
- VLAN タグのないフレームは、.2 サブインターフェイスに一致します。

7. any キーワードは、ワイルドカードとして使用できます。

```
interface GigabitEthernet0/1/0/3.4 l2transport
encapsulation dot1q 4 second-dot1q any
!
interface GigabitEthernet0/1/0/3.5 l2transport
encapsulation dot1q 4 second-dot1q 5
```

サブインターフェイス .4 と .5 の両方がタグ 4 と 5 を持つ QinQ フレームと一致する可能性があります。このフレームはより具体的な .5 サブインターフェイスに割り当てられます。これが最長一致ルールです。

8. VLAN タグの範囲を使用できます。

```
interface GigabitEthernet0/1/0/3.6 l2transport
encapsulation dot1q 6-10
```

9. 最初または 2 番目の dot1q タグには、複数の VLAN タグの値または範囲をリストできます。

```
interface GigabitEthernet0/1/0/3.7 l2transport
encapsulation dot1q 6 , 7 , 8-10
!
```

```
interface GigabitEthernet0/1/0/3.11 l2transport
encapsulation dot1q 11 second-dot1q 1 , 2 , 3 , 4-6 , 10
```

リストできる値は最大で 9 個です。さらに値が必要な場合は、別のサブインターフェイスに割り当てる必要があります。リストを短くするために値を範囲にまとめてください。

10. シスコの QinQ フレームのカプセル化方法として、**encapsulation dot1q second-dot1q** コマンドは、外部タグと内部タグに EtherType 0x8100 を使用します。ただし、IEEE では EtherType 0x8100 は 1 つの VLAN タグを持つ 802.1q フレーム用に予約されているため、QinQ フレームについては EtherType 0x88a8 の外部タグを使用する必要があります。EtherType 0x88a8 の外部タグは、*dot1ad* キーワードで設定できます。

```
interface GigabitEthernet0/1/0/3.12 l2transport
encapsulation dot1ad 12 dot1q 100
```

11. QinQ の外部タグに古い EtherType 0x9100 または 0x9200 を使用するには、QinQ サブインターフェイスのメイン インターフェイスで **dot1q tunneling ethertype** コマンドを使用します。

```
interface GigabitEthernet0/1/0/3
dot1q tunneling ethertype [0x9100|0x9200]
!
```

```
interface GigabitEthernet0/1/0/3.13 l2transport
encapsulation dot1q 13 second-dot1q 100
```

外部タグは EtherType 0x9100 または 0x9200 を持ち、内部タグは dot1q の EtherType 0x8100 を持ちます。

12. 送信元の MAC アドレスに基づいて、着信フレームをサブインターフェイスに割り当てることができます。

```
interface GigabitEthernet0/1/0/3.14 l2transport
encapsulation dot1q 14 ingress source-mac 1.1.1
```

## 2.1.2 VLAN の操作

EVC ベースのプラットフォームのデフォルトの動作では、着信フレームの VLAN タグは維持されません。

```
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
```

この設定では、VLAN タグ 3 を持つ dot1q の着信フレームは、転送されるときに VLAN タグ 3 を維持します。外部 VLAN タグ 3 と内部タグ 100 を持つ QinQ の着信フレームは、転送されるときに両方のタグが変更されずに維持されます。

ただし、EVC インフラストラクチャでは **rewrite** コマンドによってタグを操作できるため、着信した VLAN タグのスタックからタグのポップ ( 削除 )、変換、またはプッシュ ( 追加 ) を行うことができます。

以下にいくつかの例を示します。

- *pop* キーワードは、着信した dot1q フレームから QinQ タグを削除します。この例では、着

信した QinQ フレームの外部タグ 13 を削除し、dot1q タグ 100 を先頭にしてこのフレームを転送します。

```
interface GigabitEthernet0/1/0/3.13 l2transport
encapsulation dot1q 13 second-dot1q 100
rewrite ingress tag pop 1 symmetric
```

この動作は常に対称です。つまり、外部タグ 13 は入力方向ではポップされ、出力方向ではプッシュされます。

- *translate* キーワードは、1 つまたは 2 つの着信タグを 1 つまたは 2 つの新しいタグで置換します。

```
RP/0/RSP0/CPU0:router2(config-subif)#interface GigabitEthernet0/1/0/3.3
l2transport
RP/0/RSP0/CPU0:router2(config-subif)# encapsulation dot1q 3
RP/0/RSP0/CPU0:router2(config-subif)#rewrite ingress tag translate ?
1-to-1 Replace the outermost tag with another tag
1-to-2 Replace the outermost tag with two tags
2-to-1 Replace the outermost two tags with one tag
2-to-2 Replace the outermost two tags with two other tags
RP/0/RSP0/CPU0:router2(config-subif)#rewrite ingress tag translate 1-to-1 ?
dot1ad Push a Dot1ad tag
dot1q Push a Dot1Q tag
RP/0/RSP0/CPU0:router2(config-subif)#rewrite ingress tag translate 1-to-1
dot1q 4
RP/0/RSP0/CPU0:router2(config-subif)#show config
Building configuration...
!! IOS XR Configuration 4.3.0
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
rewrite ingress tag translate 1-to-1 dot1q 4 symmetric
!
end
```

*symmetric* キーワードが自動的に追加されます。これが唯一サポートされているモードだからです。

- *push* キーワードは、着信した dot1q フレームに QinQ タグを 1 つ追加します。

```
interface GigabitEthernet0/1/0/3.4 l2transport
encapsulation dot1q 4
rewrite ingress tag push dot1q 100 symmetric
```

外部 QinQ タグ 100 が、dot1q タグ 4 を持つ着信フレームに追加されます。出力方向では QinQ タグはポップされます。

## 2.2 Cisco IOS XR 非 EVC ルータの動作 ( CRS および XR12000 )

非 EVC プラットフォーム上の VLAN 照合のシンタックスでは、*encapsulation* キーワードは使用されません。

```
RP/0/RP0/CPU0:router1#config
RP/0/RP0/CPU0:router1(config)#int gig 0/0/0/2.3 l2transport
RP/0/RP0/CPU0:router1(config-subif)#dot1q ?
vlan Configure a VLAN ID on the subinterface
RP/0/RP0/CPU0:router1(config-subif)#dot1q vlan ?
<1-4094> Configure first (outer) VLAN ID on the subinterface
RP/0/RP0/CPU0:router1(config-subif)#dot1q vlan 3 ?
<1-4094> Configure second (inner 802.1Q) VLAN ID on the subinterface
```

any Match frames with any second 802.1Q VLAN ID

```
RP/0/RP0/CPU0:router1(config-subif)#dot1q vlan 3 100
```

可能な動作は `dot1q` コマンドまたは `dot1ad` コマンドで指定されたすべてのタグのポップのみであるため、VLAN タグの操作は設定できません。この動作はデフォルトで行われるため、`rewrite` コマンドはありません。

## 3. ポイントツーポイント サービス

注：

このセクションで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ( [登録ユーザ専用](#) ) を使用してください。

特定の show コマンドが [アウトプット インタープリタ ツール](#) ( [登録ユーザ専用](#) ) でサポートされています。show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

### 3.1 ローカル スイッチング

#### 3.1.1 メイン インターフェイス

基本的なトポロジは、2 つのメイン インターフェイス間のローカル クロス コネクトです。

router2 は Gi 0/1/0/1 で受信するすべてのトラフィックを受け取り、Te 0/0/0/3 に転送します。その逆も同様です。

このトポロジでは router1 と router3 が直接ケーブルで接続されているようですが、そうではありません。実際は、router2 が TenGigE インターフェイスと GigabitEthernet インターフェイスの間で変換を行っています。router2 では、これら 2 つのインターフェイス上で複数の機能を実行できます。たとえば、アクセス コントロール リスト ( ACL ) によって特定の種類のパケットやポリシーマップをドロップして、優先度の低いトラフィックのシェーピングやレート制限を行うことができます。

次の例では、基本的なポイントツーポイント クロス コネクトが、l2transport として設定された router2 の 2 つのメイン インターフェイスの間で設定されています。

```
interface GigabitEthernet0/1/0/1
l2transport
!
!
interface TenGigE0/0/0/3
l2transport
!
!
l2vpn
xconnect group test
p2p p2p1
interface TenGigE0/0/0/3
```



```
interface GigabitEthernet0/1/0/1
!
```

router1 と router3 のメイン インターフェイスには、CDP および IPv4 アドレスが設定されています。

```
RP/0/RP0/CPU0:router1#sh run int Gi 0/0/0/1
interface GigabitEthernet0/0/0/1
 cdp
 ipv4 address 10.1.1.1 255.255.255.0
!
```

```
RP/0/RP0/CPU0:router1#
RP/0/RP0/CPU0:router1#sh cdp nei Gi 0/0/0/1
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater
```

```
Device ID Local Intrfce Holdtme Capability Platform Port ID
router3.cisco.c Gi0/0/0/1 132 R ASR9K Ser Te0/0/0/3
RP/0/RP0/CPU0:router1#ping 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/8/32 ms
```

router1 は router3 を CDP ネイバーとして認識し、これら 2 台のルータが直接接続されているかのように 10.1.1.2 ( router3 のインターフェイスアドレス ) に ping できます。

router2 に設定されているサブインターフェイスはないため、router1 および router3 で dot1q のサブインターフェイスが設定されている場合、VLAN タグ付きの着信フレームは透過的に転送されます。

```
RP/0/RP0/CPU0:router1#sh run int gig 0/0/0/1.2
interface GigabitEthernet0/0/0/1.2
 ipv4 address 10.1.2.1 255.255.255.0
 dot1q vlan 2
!
```

```
RP/0/RP0/CPU0:router1#ping 10.1.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/5 ms
```

router1 から router3 へ 10,000 回の ping を行った後で、**show interface** コマンドおよび **show l2vpn** コマンドを使用すると、ある AC 上で router2 によって受信された ping 要求が別の AC に転送されていること、および逆方向でも ping 応答が同様に処理されていることを確認できます。

```
RP/0/RSP0/CPU0:router2#sh int gig 0/1/0/1
GigabitEthernet0/1/0/1 is up, line protocol is up
Interface state transitions: 1
Hardware is GigabitEthernet, address is 0024.986c.63f1 (bia 0024.986c.63f1)
Description: static lab connection to acdc 0/0/0/1 - dont change
Layer 2 Transport Mode
MTU 1514 bytes, BW 1000000 Kbit (Max: 1000000 Kbit)
reliability 255/255, txload 0/255, rxload 0/255
Encapsulation ARPA,
Full-duplex, 1000Mb/s, SXFD, link type is force-up
output flow control is off, input flow control is off
loopback not set,
Last input 00:00:00, output 00:00:00
Last clearing of "show interface" counters 00:01:07
5 minute input rate 28000 bits/sec, 32 packets/sec
```

```
5 minute output rate 28000 bits/sec, 32 packets/sec
10006 packets input, 1140592 bytes, 0 total input drops
0 drops for unrecognized upper-level protocol
Received 0 broadcast packets, 6 multicast packets
0 runts, 0 giants, 0 throttles, 0 parity
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
10007 packets output, 1140832 bytes, 0 total output drops
Output 0 broadcast packets, 7 multicast packets
0 output errors, 0 underruns, 0 applique, 0 resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
```

```
RP/0/RSP0/CPU0:router2#sh int ten 0/0/0/3
TenGigE0/0/0/3 is up, line protocol is up
Interface state transitions: 3
Hardware is TenGigE, address is 0024.98ea.038b (bia 0024.98ea.038b)
Layer 1 Transport Mode is LAN
Description: static lab connection to putin 0/0/0/3 - dont change
Layer 2 Transport Mode
MTU 1514 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
reliability 255/255, txload 0/255, rxload 0/255
Encapsulation ARPA,
Full-duplex, 10000Mb/s, LR, link type is force-up
output flow control is off, input flow control is off
loopback not set,
Last input 00:00:00, output 00:00:06
Last clearing of "show interface" counters 00:01:15
5 minute input rate 27000 bits/sec, 30 packets/sec
5 minute output rate 27000 bits/sec, 30 packets/sec
10008 packets input, 1140908 bytes, 0 total input drops
0 drops for unrecognized upper-level protocol
Received 0 broadcast packets, 8 multicast packets
0 runts, 0 giants, 0 throttles, 0 parity
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
10006 packets output, 1140592 bytes, 0 total output drops
Output 0 broadcast packets, 6 multicast packets
0 output errors, 0 underruns, 0 applique, 0 resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
```

```
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test
```

```
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
```

```
-----
test p2p1 UP Te0/0/0/3 UP Gi0/1/0/1 UP
-----
```

```
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test det
```

```
Group test, XC p2p1, state is up; Interworking none
```

```
AC: TenGigE0/0/0/3, state is up
```

```
Type Ethernet
```

```
MTU 1500; XC ID 0x1080001; interworking none
```

```
Statistics:
```

```
packets: received 10008, sent 10006
```

```
bytes: received 1140908, sent 1140592
```

```
AC: GigabitEthernet0/1/0/1, state is up
```

```
Type Ethernet
```

```
MTU 1500; XC ID 0x1880003; interworking none
```

```
Statistics:
```

packets: received 10006, sent 10008  
bytes: received 1140592, sent 1140908

RP/0/RSP0/CPU0:router2#sh l2vpn forwarding interface gigabitEthernet 0/1/0/1  
hardware ingress detail location 0/1/CPU0

Local interface: GigabitEthernet0/1/0/1, Xconnect id: 0x1880003, Status: up  
Segment 1

AC, GigabitEthernet0/1/0/1, Ethernet port mode, status: Bound

Statistics:

packets: received 10022, sent 10023  
bytes: received 1142216, sent 1142489  
packets dropped: PLU 0, tail 0  
bytes dropped: PLU 0, tail 0

Segment 2

AC, TenGigE0/0/0/3, Ethernet port mode, status: Bound

Platform AC context:

Ingress AC: Local Switch, State: Bound

Flags: Remote is Simple AC

XID: 0x00580003, SHG: None

Ingress uIDB: 0x0003, Egress uIDB: 0x0003, NP: 3, Port Learn Key: 0  
NP3

Ingress uIDB:

Flags: L2, Status

Stats Ptr: 0x0d842c, uIDB index: 0x0003, Wire Exp Tag: 0

BVI Bridge Domain: 0, BVI Source XID: 0x01000000

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: 0x00000001

UIDB IF Handle: 0x00000000, Source Port: 1, Num VLANs: 0

Xconnect ID: 0x00580003, NP: 3

Type: AC, Remote type: AC

Flags: Learn enable

uIDB Index: 0x0003, LAG pointer: 0x0000

Split Horizon Group: None

RP/0/RSP0/CPU0:router2#sh l2vpn forwarding interface Te 0/0/0/3 hardware egress  
detail location 0/0/CPU0

Local interface: TenGigE0/0/0/3, Xconnect id: 0x1080001, Status: up  
Segment 1

AC, TenGigE0/0/0/3, Ethernet port mode, status: Bound

Statistics:

packets: received 10028, sent 10027  
bytes: received 1143016, sent 1142732  
packets dropped: PLU 0, tail 0  
bytes dropped: PLU 0, tail 0

Segment 2

AC, GigabitEthernet0/1/0/1, Ethernet port mode, status: Bound

Platform AC context:

Egress AC: Local Switch, State: Bound

Flags: Remote is Simple AC

XID: 0x00000001, SHG: None

Ingress uIDB: 0x0007, Egress uIDB: 0x0007, NP: 0, Port Learn Key: 0  
NP0

Egress uIDB:

Flags: L2, Status, Done

Stats ptr: 0x000000

VPLS SHG: None

L2 ACL Format: 0, L2 ACL ID: 0, IPV4 ACL ID: 0, IPV6 ACL ID: 0

VLAN1: 0, VLAN1 etype: 0x0000, VLAN2: 0, VLAN2 etype: 0x0000

UIDB IF Handle: 0x04000240, Search VLAN Vector: 0

QOS ID: 0, QOS format: 0

```
Xconnect ID: 0x00000001, NP: 0
Type: AC, Remote type: AC
Flags: Learn enable
uIDB Index: 0x0007, LAG pointer: 0x0000
Split Horizon Group: None
```

### 3.1.2 サブインターフェイスと VLAN 操作

次の例には、Cisco IOS<sup>®</sup> ソフトウェアの用語で言えば、スイッチポート モード アクセス インターフェイスのような 1 つの AC と、トランクのような 1 つの dot1q サブインターフェイスがあります。

このトポロジでは、一般に 3 つ以上の VLAN のポートがあるため、通常はブリッジドメインを使用しますが、2 つのポートしかない場合にはポイントツーポイント クロス コネクトを使用できます。この項では、さまざまな VLAN の操作方法を可能にする書き換え機能の柔軟性について説明します。

#### 3.1.2.1 メイン インターフェイスと dot1q サブインターフェイス

この例では、片側にメイン インターフェイスがあり、もう一方の側には dot1q サブインターフェイスがあります。

router1 のメイン インターフェイスは次のとおりです。

```
RP/0/RP0/CPU0:router1#sh run int gig 0/0/0/1
interface GigabitEthernet0/0/0/1
description static lab connection to router2 0/1/0/1
cdp
ipv4 address 10.1.1.1 255.255.255.0
!
```

router2 の dot1q サブインターフェイスは次のとおりです。

```
RP/0/RSP0/CPU0:router2#sh run int gig 0/1/0/1
interface GigabitEthernet0/1/0/1
description static lab connection to router1 0/0/0/1
l2transport
```

```
RP/0/RSP0/CPU0:router2#sh run int ten 0/0/0/3.2
interface TenGigE0/0/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
```

```
RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p2
interface TenGigE0/0/0/3.2
interface GigabitEthernet0/1/0/1
```

TenGigE0/0/0/3.2 のサブインターフェイスの名前には、*l2transport* キーワードがあります。router3 がタグ 2 を持つ dot1q フレームを送信すると、このフレームが router2 の TenGigE0/0/0/3.2 サブインターフェイスに一致します。

着信したタグ 2 は、入力方向では、**rewrite ingress tag pop 1 symmetric** コマンドによって削除されます。タグが TenGigE0/0/0/3.2 の入力方向で削除されたため、GigabitEthernet0/1/0/1 の出力

方向ではパケットはタグなしで送信されます。

router1 がタグなしフレームを送信すると、このフレームがメイン インターフェイス GigabitEthernet0/1/0/1 に一致します。

GigabitEthernet0/1/0/1 には **rewrite** コマンドがないため、タグのポップ、プッシュ、変換は行われません。

パケットが TenGigE0/0/0/3.2 から外に転送されるときは、*symmetric* キーワードが **rewrite ingress tag pop 1** コマンドにあるため、dot1q のタグ 2 がプッシュされます。このコマンドは、入力方向では 1 つのタグをポップし、出力方向では対称的に 1 つのタグをプッシュします。router3 の例を次に示します。

```
RP/0/RSP0/CPU0:router3#sh run int ten 0/0/0/3.2
interface TenGigE0/0/0/3.2
ipv4 address 10.1.1.2 255.255.255.0
encapsulation dot1q 2
```

同じ **show interface** コマンドと **show l2vpn** コマンドを使用して、サブインターフェイスのカウンタをモニタします。

```
RP/0/RSP0/CPU0:router2#clear counters
Clear "show interface" counters on all interfaces [confirm]
RP/0/RSP0/CPU0:router2#clear l2vpn forwarding counters
RP/0/RSP0/CPU0:router2#
RP/0/RSP0/CPU0:router2#
RP/0/RSP0/CPU0:router2#sh int TenGigE0/0/0/3.2
TenGigE0/0/0/3.2 is up, line protocol is up
Interface state transitions: 1
Hardware is VLAN sub-interface(s), address is 0024.98ea.038b
Layer 2 Transport Mode
MTU 1518 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
reliability Unknown, txload Unknown, rxload Unknown
Encapsulation 802.1Q Virtual LAN,
Outer Match: Dot1Q VLAN 2
Ethertype Any, MAC Match src any, dest any
loopback not set,
Last input 00:00:00, output 00:00:00
Last clearing of "show interface" counters 00:00:27
1000 packets input, 122000 bytes
0 input drops, 0 queue drops, 0 input errors
1002 packets output, 122326 bytes
0 output drops, 0 queue drops, 0 output errors
```

```
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect detail
```

```
Group test, XC p2p2, state is up; Interworking none
AC: TenGigE0/0/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0x1080001; interworking none
Statistics:
packets: received 1001, sent 1002
bytes: received 118080, sent 118318
drops: illegal VLAN 0, illegal length 0
AC: GigabitEthernet0/1/0/1, state is up
Type Ethernet
MTU 1500; XC ID 0x1880003; interworking none
Statistics:
packets: received 1002, sent 1001
```

bytes: received 114310, sent 114076

予想通り、TenGigE0/0/0/3.2 で受信したパケット数は、GigabitEthernet0/1/0/1 で送信したパケット数と一致し、その逆も同じです。

### 3.1.2.2 カプセル化を設定したサブインターフェイス

GigabitEthernet0/1/0/1 のメイン インターフェイスの代わりに **encapsulation default** を設定したサブインターフェイスを使用すると、すべてのフレームをキャッチできます。また、**encapsulation untagged** を設定したサブインターフェイスを使用すると、タグなしフレームのみを一致させることができます。

```
RP/0/RSP0/CPU0:router2#sh run interface GigabitEthernet0/1/0/1.1
interface GigabitEthernet0/1/0/1.1 l2transport
encapsulation untagged
```

```
RP/0/RSP0/CPU0:router2#sh run int TenGigE0/0/0/3.2
interface TenGigE0/0/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
```

```
RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p3
interface TenGigE0/0/0/3.2
interface GigabitEthernet0/1/0/1.1
```

### 3.1.2.3 GigabitEthernet0/1/0/1.1 の入力方向

TenGigE0/0/0/3.2 の入力方向で tag 2 をポップする代わりに、GigabitEthernet0/1/0/1.1 の入力方向でタグ 2 をプッシュし、TenGigE0/0/0/3.2 では何もしないようにすることもできます。

```
RP/0/RSP0/CPU0:router2#sh run int TenGigE0/0/0/3.2
interface TenGigE0/0/0/3.2 l2transport
encapsulation dot1q 2
```

```
RP/0/RSP0/CPU0:router2#sh run interface GigabitEthernet0/1/0/1.1
interface GigabitEthernet0/1/0/1.1 l2transport
encapsulation untagged
rewrite ingress tag push dot1q 2 symmetric
```

```
RP/0/RSP0/CPU0:router2#sh run int TenGigE0/0/0/3.2
interface TenGigE0/0/0/3.2 l2transport
encapsulation dot1q 2
```

```
RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p3
interface TenGigE0/0/0/3.2
interface GigabitEthernet0/1/0/1.1
```

このように、**encapsulation** コマンドと **rewrite** コマンドを備えた EVC モデルによって、VLAN タグの照合と操作の柔軟性が非常に高くなります。

## 3.2 Virtual Private Wire Service

### 3.2.1 概要

Virtual Private Wire Service ( VPWS ) は、Ethernet over MPLS ( EoMPLS ) と呼ばれ、2 台の L2VPN プロバイダー エッジ ( PE ) デバイスが L2VPN トラフィックを MPLS クラウド上でトンネリングできるようにします。2 つの L2VPN PE は通常異なる 2 つのサイトに接続されており、MPLS コアがあります。各 L2VPN PE に接続された 2 つの AC は、MPLS ネットワーク上の PW ( MPLS PW ) によってリンクされます。

各 PE がリモート PE のループバックに到達するためには、MPLS ラベルが必要です。このラベルは、通常、内部ゲートウェイ プロトコル ( IGP ) ラベルと呼ばれ、MPLS ラベル配布プロトコル ( LDP ) または MPLS トラフィック エンジニアリング ( TE ) を通じて学習できます。

2 つの PE の間にターゲットの MPLS LDP セッションが確立し、これによって PW のステータスを確立して制御することができます。PE は、PW を識別する MPLS ラベルを他の PE にアドバタイズします。

**注:** BGP をシグナリングに使用できますが、このドキュメントでは説明しません。

router2 がローカルの AC で受信したトラフィックは、MPLS のラベル スタックにカプセル化されます。

- 外部 MPLS ラベルは、router3 のループバックに到達するための IGP ラベルです。ラベルが直接接続される場合、このラベルは暗黙のヌル ラベルになる場合があります。つまり、IGP ラベルは追加されません。
- 内部 MPLS ラベルは、ターゲット LDP セッションを介して router3 によってアドバタイズされる PW ラベルです。
- 設定およびカプセル化の種類によっては、MPLS ラベルの後に PW のコントロールワードが付く場合があります。コントロールワードはデフォルトではイーサネット インターフェイス上で使用されないため、必要な場合は明示的に設定する必要があります。
- パケット内では、転送された L2 フレームが続きます。
- 設定および PW の種類によっては、一部の VLAN タグが PW 上で転送されます。

最後から 2 番目のホップ ( MPLS コア内の router3 の直前 ) では、IGP ラベルはポップされるか、明示的なヌル ラベルに置き換えられます。したがって、router3 で受信されたフレームの先頭の有効なラベルは、router3 が PW のために router2 にシグナリングした PW ラベルです。これにより router3 は、この MPLS ラベルが付いた受信トラフィックを、router4 に接続された AC にスイッチングする必要があると認識します。

**前の例**では、各 L2VPN にリモート PE のループバック用の MPLS ラベルがあるかどうかを最初に確認する必要がありました。router2 のラベルを確認する方法の例を次に示します。

```
RP/0/RSP1/CPU0:router2#sh mpls forwarding prefix 10.0.0.11/32
Local Outgoing Prefix Outgoing Next Hop Bytes
Label Label or ID Interface Switched
```

```
-----
16008 16009 10.0.0.11/32 Te0/0/0/1 10.0.23.2 681260
```

AC の設定は変わっていません。

```
RP/0/RSP1/CPU0:router2#sh run int gig 0/0/0/1.2
Wed May 1 13:56:07.668 CEST
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
```

rewrite ingress pop コマンドがないため、着信した VLAN タグ 2 は PW 上を転送されます。詳細については、「[タイプ 4 とタイプ 5 の PW](#)」を参照してください。

L2VPN の設定では、ローカル AC と、PW ID を持つリモート L2VPN PE を指定します。PW ID は両側で一致し、ネイバーごとに一意である必要があります。

```
RP/0/RSP1/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p4
interface GigabitEthernet0/0/0/1.2
neighbor 10.0.0.11 pw-id 222
```

router3 の対応する設定を次に示します。

```
RP/0/RSP0/CPU0:router3#sh run int gig 0/1/0/3.2
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
!
```

```
RP/0/RSP0/CPU0:router3#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p4
interface GigabitEthernet0/1/0/3.2
neighbor 10.0.0.13 pw-id 222
```

クロスコネクトの詳細を表示するには、**show l2vpn xconnect detail** コマンドを使用します。

```
RP/0/RSP1/CPU0:router2#sh l2vpn xconnect group test xc-name p2p4 detail
```

```
Group test, XC p2p4, state is up; Interworking none
AC: GigabitEthernet0/0/0/1.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1504; XC ID 0x840006; interworking none
Statistics:
packets: received 186, sent 38448
bytes: received 12644, sent 2614356
drops: illegal VLAN 0, illegal length 0
PW: neighbor 10.0.0.11, PW ID 222, state is up ( established )
PW class not set, XC ID 0xc0000004
Encapsulation MPLS, protocol LDP
Source address 10.0.0.13
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set
```

```
PW Status TLV in use
MPLS Local Remote
```

```
-----
Label 16026 16031
Group ID 0x4000280 0x6000180
Interface GigabitEthernet0/0/0/1.2 GigabitEthernet0/1/0/3.2
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: 3221225476
Create time: 30/04/2013 16:30:58 (21:31:00 ago)
Last time status changed: 30/04/2013 16:36:42 (21:25:16 ago)
Statistics:
packets: received 38448, sent 186
bytes: received 2614356, sent 12644
```

この設定では、次の点に注意してください。

- AC 上の着信タグはポップされないため、AC の最大伝送ユニット ( MTU ) は 1504 です。MTU は両側で一致する必要があります。一致しない場合、PW は有効になりません。
- AC 上で 186 個のパケットが受信され、予期したとおりに PW 上で送信されました。
- PW 上で 38448 個のパケットが受信され、予期したとおりに AC 上で送信されました。
- router2 のローカル ラベルは 16026 であり、これは router3 が内部ラベルとして使用するラベルです。パケットは、router2 で受信されたときにこの MPLS ラベルを先頭のラベルとして持っています。これは、最後から 2 番目の MPLS ホップで IGP ラベルがポップされたからです。router2 は、この PW ラベルを持つ着信フレームを AC Gi 0/0/0/1.2 にスイッチングする必要があると認識します。

```
RP/0/RSP1/CPU0:router2#sh mpls forwarding labels 16026
Local Outgoing Prefix Outgoing Next Hop Bytes
Label Label or ID Interface Switched
-----
16026 Pop PW(10.0.0.11:222) Gi0/0/0/1.2 point2point 2620952
```

### 3.2.2 PW と AC のペアのステータス

ポイントツーポイント クロス コネクトでは、AC と PW はペアになります。したがって、AC がダウンすると、L2VPN PE は、PW のステータスをダウンにする必要があることを LDP によってリモート PE にシグナリングします。PW 冗長性が設定されている場合、これによってコンバージェンスがトリガーされます。詳細については、「[冗長性](#)」の項を参照してください。

次の例では、router2 の AC がダウンし、「AC がダウン」の PW ステータスを router3 へ送信しています。

```
RP/0/RSP1/CPU0:router2#sh l2vpn xconnect group test xc-name p2p4 detail
Wed May 1 23:38:55.542 CEST

Group test, XC p2p4, state is down; Interworking none
AC: GigabitEthernet0/0/0/1.2, state is down
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1504; XC ID 0x840006; interworking none
Statistics:
packets: received 186, sent 38544
bytes: received 12644, sent 2620884
drops: illegal VLAN 0, illegal length 0
PW: neighbor 10.0.0.11, PW ID 222, state is down ( remote standby )
PW class not set, XC ID 0xc0000004
Encapsulation MPLS, protocol LDP
Source address 10.0.0.13
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set
```

```

PW Status TLV in use
MPLS Local Remote
-----
Label 16026 16031
Group ID 0x4000280 0x6000180
Interface GigabitEthernet0/0/0/1.2 GigabitEthernet0/1/0/3.2
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: 0x6 (AC Down) in Notification message
MIB cpwVcIndex: 3221225476
Create time: 30/04/2013 16:30:58 (1d07h ago)
Last time status changed: 01/05/2013 14:05:07 (09:33:47 ago)
Statistics:
packets: received 38544, sent 186
bytes: received 2620884, sent 12644

```

router3 は、リモートの AC がダウンしたため PW をダウンさせる必要があることを認識します。

```

RP/0/RSP0/CPU0:router3#sh l2vpn xconnect group test xc-name p2p4 detail

```

```

Group test, XC p2p4, state is down; Interworking none
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1504; XC ID 0xc40003; interworking none
Statistics:
packets: received 38545, sent 186
bytes: received 2620952, sent 12644
drops: illegal VLAN 0, illegal length 0
PW: neighbor 10.0.0.13, PW ID 222, state is down ( local ready )
PW class not set, XC ID 0xc0000005
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

```

```

PW Status TLV in use
MPLS Local Remote
-----
Label 16031 16026
Group ID 0x6000180 0x4000280
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
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: 0x6 (AC Down) in Notification message  
Outgoing Status (PW Status TLV):  
Status code: 0x0 (Up) in Notification message  
MIB cpwVcIndex: 3221225477  
Create time: 30/04/2013 16:37:57 (1d07h ago)  
Last time status changed: 01/05/2013 14:11:33 (09:35:50 ago)  
Statistics:  
packets: received 186, sent 38545  
bytes: received 12644, sent 2620952

### 3.2.3 タイプ 4 とタイプ 5 の PW

タイプ 4 とタイプ 5 の 2 種類の PW を使用できます。

- タイプ 4 の PW は、VLAN ベースの PW と呼ばれます。入力側の PE では着信した VLAN タグを削除しないことになっているため、タグは PW 上を転送されます。

ASR 9000 などの EVC ベースのプラットフォームでは、着信した VLAN タグをポップする **rewrite** コマンドが着信した AC に設定されている可能性があるため、PW 上を転送される VLAN タグが存在しなくなる場合があります。この可能性に対応するために、EVC プラットフォームでは、タイプ 4 の PW についてはフレームの先頭にダミーの VLAN タグ 0 を挿入します。タイプ 4 の PW は、**transport-mode vlan** コマンドで設定します。リモート PE は EVC ベースであり、先頭の VLAN タグは削除が必要なダミー タグであることを認識している必要があります。

ただし、EVC プラットフォームと非 EVC プラットフォームの間でタイプ 4 の PW を使用する場合、これによって相互運用性の問題が発生する可能性があります。非 EVC プラットフォームは、先頭の VLAN タグがダミーの VLAN タグであることを考慮せずに、ダミーの VLAN タグ 0 を外部タグとして含むフレームを転送します。EVC プラットフォームでは、着信フレームで取得した VLAN タグを **rewrite** コマンドを使用して操作することができます。VLAN 操作の結果は、追加のダミー タグ 0 を先頭に含めてタイプ 4 の PW 上で転送されます。

Cisco IOS XR ソフトウェアの最近のリリースでは、**transport-mode vlan passthrough** コマンドを使用することで、ダミー タグ 0 を使用せずにタイプ 4 の PW を使用する機能が提供されています。イーサネット フロー ポイント (EFP) 上の VLAN タグの操作では、少なくとも 1 つのタグを残す必要があります。タイプ 4 の PW 上では VLAN タグが転送される必要がありますが、この場合にはこうした要件を満たすダミー タグが存在しないためです。着信インターフェイスのタグを書き換えた後でフレームに残ったタグは、PW を介して透過的に転送されます。

- タイプ 5 の PW は、イーサネット ポートベース PW と呼ばれます。メイン インターフェイスで受信したフレームは、入力 PE によって転送されます。パケットがサブインターフェイスで受信された場合は、サブインターフェイスのタグが削除された後で転送されます。タイプ 5 の PW 上でタグ付きフレームを送信する要件はないため、EVC ベースのプラットフォームによってダミーのタグが追加されることはありません。EVC ベースのプラットフォームでは、着信フレームで取得した VLAN タグを **rewrite** コマンドを使用して操作することができます。VLAN 操作の結果は、タグの有無にかかわらずタイプ 5 の PW 上で転送されます。

デフォルトでは、L2VPN の PE は、次の例に示すようにタイプ 5 の PW のネゴシエーションを試みます。

```
RP/0/RSP1/CPU0:router2#sh l2vpn xconnect group test det | i " PW type"
```

```
PW type Ethernet, control word disabled, interworking none
```

```
PW type Ethernet Ethernet
```

"PW type Ethernet" は、タイプ 5 の PW を示します。

これは router1 によって送信され、router2 でカプセル化されて PW 上を router3 に送信された ARP 要求のスニファ キャプチャです。

```
Frame 38: 82 bytes on wire (656 bits), 82 bytes captured (656 bits)
```

```
Ethernet II, Src: Cisco_2f:dc:04 (00:0b:60:2f:dc:04), Dst: Cisco_le:93:50  
(00:24:f7:1e:93:50)
```

```
MultiProtocol Label Switching Header, Label: 16031, Exp: 0, S: 1, TTL: 251
```

```
Ethernet II, Src: Cisco_03:1f:46 (00:1d:46:03:1f:46), Dst: Broadcast  
(ff:ff:ff:ff:ff:ff)
```

```
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 2
```

```
Address Resolution Protocol (request)
```

MPLS ラベル 16031 は、router3 によってアドバタイズされた PW ラベルです。スニファ キャプチャは最後から 2 番目のホップと router3 の間で取られたため、IGP ラベルはありません。

カプセル化されたイーサネット フレームが、PW ラベルの直後から始まっています。PW のコントロールワードが含まれる場合もありますが、この例では設定されていません。

AC には VLAN タグをポップする **rewrite** コマンドがないため、タイプ 5 の PW の場合でも、router2 が AC で受信した着信 VLAN タグ 2 は転送されます。EVC ベースのプラットフォームでは自動的なタグのポップは行われないため、書き換え処理の後で AC から送られた結果が転送されます。タイプ 5 の PW にはダミーの VLAN タグ 0 はないことに注意してください。

**rewrite ingress tag pop 1 symmetric** コマンドを設定した場合、PW 上を転送される VLAN タグは存在しなくなります。

router2 と router3 に pw-class が設定されたタイプ 4 の PW の例を次に示します。

注: 片側だけにタイプ 4 を設定した場合、PW はダウンしたままになり、「Error: PW type mismatched」が報告されます。

```
l2vpn
```

```
pw-class VLAN
```

```
encapsulation mpls
```

```
transport-mode vlan
```

```
!
```

```
!
```

```
xconnect group test
```

```
p2p p2p4
```

```
neighbor 10.0.0.11 pw-id 222
```

```
pw-class VLAN
```

```
!
```

```
!
```

```
!
```

```
!
```

"PW type "Ethernet VLAN" は、タイプ 4 の PW を示します。

```
RP/0/RSP1/CPU0:router2#sh l2vpn xconnect group test det | i " PW type"
```

```
PW type Ethernet VLAN, control word disabled, interworking none
```

```
PW type Ethernet VLAN Ethernet VLAN
```

今回は、転送されるフレームの先頭にダミーのタグ 0 が挿入されています。

```
Frame 15: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
```

```
Ethernet II, Src: Cisco_2f:dc:04 (00:0b:60:2f:dc:04), Dst: Cisco_1e:93:50
(00:24:f7:1e:93:50)
MultiProtocol Label Switching Header, Label: 16031, Exp: 0, S: 1, TTL: 251
Ethernet II, Src: Cisco_03:1f:46 (00:1d:46:03:1f:46), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 0
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 2
Address Resolution Protocol (request)
```

出力側の EVCベースの PE はダミーのタグを削除し、タグ 2 を含むフレームをローカルの AC に転送します。出力側の PE は、PW で受信したフレームに対して、AC 上で設定されたローカルのタグ操作を適用します。ローカルの AC で **rewrite ingress tag pop 1 symmetric** のように設定されている場合、出力方向では設定されたタグをプッシュする必要があるため、PW で受信された先頭タグ 2 の前に新しいタグがプッシュされます。rewrite コマンドは柔軟性が高いですが、それぞれの PW で実施する内容について慎重に評価する必要があります。

### 3.2.4 マルチセグメント PW

AC のような物理インターフェイスではなく、PW を持つ L2VPN PE も使用できます。

router5 は router2 から PW のパケットを受信し、そのパケットを他の PW 上で router3 に向けてスイッチングします。つまり、router2 と router3 の間のマルチセグメント PW を構築するために、router5 は PW の間でスイッチングを行います。

この場合、router2 の設定ではリモート PE として router5 をポイントします。

```
RP/0/RSP1/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p5
interface GigabitEthernet0/0/0/1.2
neighbor 10.0.0.12 pw-id 222
!
!
!
!
```

router5 の設定は簡単です。

```
RP/0/RSP0/CPU0:router5#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p5
neighbor 10.0.0.11 pw-id 223
!
neighbor 10.0.0.13 pw-id 222
!
description R2-R5-R3
!
!
!
```

**description** コマンドはオプションです。router5 から各リモート PE ( router2 および router3 ) に送信される PW スイッチング TLV ( タイプ/長さ/値 ) に挿入します。**description** は、PW スイッチングを行うルータが間にあるという PW の問題をトラブルシューティングする必要があるときに役立ちます。

PW スイッチング TLV をレビューするには、**sh l2vpn xconnect** コマンドを入力します。

RP/0/RSP0/CPU0:router5#sh l2vpn xconnect group test det

Group test, XC p2p5, state is down; Interworking none  
Description: R2-R5-R3  
PW: neighbor 10.0.0.11, PW ID 223, state is down ( provisioned )  
PW class not set, XC ID 0xc0000002  
Encapsulation MPLS, protocol LDP  
Source address 10.0.0.12  
PW type Ethernet, control word disabled, interworking none  
PW backup disable delay 0 sec  
Sequencing not set

PW Status TLV in use  
MPLS Local Remote

-----  
Label 16042 unknown  
Group ID 0x4000280 0x0  
Interface GigabitEthernet0/0/0/1.2 unknown  
MTU 1504 unknown  
Control word disabled unknown  
PW type Ethernet unknown  
VCCV CV type 0x2 0x0  
(none)  
(LSP ping verification)  
VCCV CC type 0x4 0x0  
(none)  
(TTL expiry)

-----  
Outgoing PW Switching TLVs (Label Mapping message):  
Local IP Address: 10.0.0.12, Remote IP Address: 10.0.0.13, PW ID: 222

**Description: R1-R5-R3**

Outgoing Status (PW Status TLV):  
Status code: 0x0 (Up) in Notification message  
Statistics for MS-PW:  
packets: received 0  
bytes: received 0  
MIB cpwVcIndex: 3221225474  
Create time: 02/05/2013 15:37:53 (00:34:43 ago)  
Last time status changed: 02/05/2013 16:12:30 (00:00:06 ago)  
Last time PW went down: 02/05/2013 16:12:30 (00:00:06 ago)  
PW: neighbor 10.0.0.13, PW ID 222, state is up ( established )  
PW class not set, XC ID 0xc0000001  
Encapsulation MPLS, protocol LDP  
Source address 10.0.0.12  
PW type Ethernet, control word disabled, interworking none  
PW backup disable delay 0 sec  
Sequencing not set

PW Status TLV in use  
MPLS Local Remote

-----  
Label 16043 16056  
Group ID 0x6000180 0x4000280  
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2  
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 0x4 0x6  
(router alert label)  
(TTL expiry) (TTL expiry)

-----  
Incoming Status (PW Status TLV):

Status code: 0x0 (Up) in Notification message  
Outgoing PW Switching TLVs (Label Mapping message):  
Local IP Address: 10.0.0.12, Remote IP Address: 10.0.0.11, PW ID: 223

**Description: R2-R5-R3**

Outgoing Status (PW Status TLV):  
Status code: 0x0 (Up) in Notification message  
Statistics for MS-PW:  
packets: received 0  
bytes: received 0  
MIB cpwVcIndex: 0  
Create time: 02/05/2013 15:37:53 (00:34:43 ago)  
Last time status changed: 02/05/2013 16:12:35 (00:00:01 ago)  
Last time PW went down: 02/05/2013 16:12:30 (00:00:06 ago)

router5 は router2 への PW の詳細を含んだ PW スイッチング TLV を router3 へ送信し、router3 への PW の詳細を含んだ PW スイッチング TLV を router2 へ送信しています。

### 3.2.5 冗長性

2つのサイトを接続するためにポイントツーポイント PW を使用できますが、これら 2つのサイトは PE または AC の障害時にも接続されたままである必要があります。

#### 3.2.5.1 コアの冗長性

MPLS コアの再ルーティングに影響するトポロジ変更を行うと、MPLS PW は直ちに新しいパスを継承します。

#### 3.2.5.2 PW 上のバンドル

CE と PE の間でバンドル メンバーのリンク障害があった場合にリンクの冗長性を得るために、イーサネット バンドルを介してカスタマー エッジ ( CE ) デバイスを PE に接続できます。1つのバンドル リンク メンバーがダウンしても、バンドルはアップのままになります。この方法では PE の障害によってバンドル全体がダウンするため、PE の冗長性は提供されないことに注意してください。

冗長性を実現する 1つの方法は、ポイントツーポイント PW によって転送される複数の回線を設けることです。各回線は、2つの CE 間のイーサネット バンドルのメンバーです。

PE はバンドルを終端するのではなく、PW 上でフレームを透過的に転送します。これには、CE の間で交換される Link Aggregation Control Protocol ( LACP ) のフレームも含まれます。

この設計では、AC または PE が失われるとバンドル メンバーはダウンしますが、バンドルはアップしたままになります。

**注:** Cisco IOS XR ソフトウェア リリース 4.2.1 より前のリリースでは、ASR 9000 は LACP BPDU を L2VPN 上で転送しません。

この設計でも、CE はシングル ポイント障害になります。CE で使用可能なその他の冗長機能には次のものがあります。

- マルチシャーシ リンク アグリゲーション グループ ( MC-LAG )

- ASR 9000 のネットワーク仮想化 ( nV ) クラスタリング
- Cisco IOS スイッチの仮想スイッチング システム ( VSS )
- Cisco Nexus スイッチの仮想 PortChannel ( vPC )

PE の視点では、AC と MPLS PW の間に単純なポイントツーポイント接続があるだけです。

### 3.2.5.3 PW の冗長性

PE は、PW 冗長性と呼ばれる機能によって冗長性を提供することもできます。

router2 には router3 へのプライマリ PW があります。 router1 から router6 へのトラフィックは、通常の状況ではこのプライマリ PW 上を流れます。 router2 には、ホットスタンバイの router4 へのバックアップ PW もありますが、通常の状況ではこの PW 上をトラフィックは流れません。

プライマリ PW、プライマリ PW のリモート PE ( router3 )、またはリモート PE ( router3 ) の AC に問題が生じた場合、router2 はすぐにバックアップ PW をアクティブにし、トラフィックはこの PW を流れ始めます。 問題が解決されると、トラフィックはプライマリ PW に戻ります。

router2 の設定は次のとおりです。

```
RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p6
interface GigabitEthernet0/1/0/3.2
neighbor 10.0.0.13 pw-id 222
backup neighbor 10.0.0.14 pw-id 222
!
!
!
!
!
```

router3 および router4 の標準設定は次のとおりです。

```
RP/0/RSP1/CPU0:router3#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p6
interface GigabitEthernet0/0/0/1.2
neighbor 10.0.0.11 pw-id 222
!
!
!
!
```

安定した状態では、router3 への PW はアクティブで、router4 への PW はスタンバイ状態です。

```
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test
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
-----
test p2p6 UP Gi0/1/0/3.2 UP 10.0.0.13 222 UP
Backup
10.0.0.14 222 SB
```



-----  
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test det

Group test, XC p2p6, state is up; Interworking none  
AC: GigabitEthernet0/1/0/3.2, state is up  
Type VLAN; Num Ranges: 1  
VLAN ranges: [2, 2]  
MTU 1504; XC ID 0xc40003; interworking none  
Statistics:  
packets: received 51412, sent 25628  
bytes: received 3729012, sent 1742974  
drops: illegal VLAN 0, illegal length 0  
PW: neighbor 10.0.0.13, PW ID 222, state is up ( established )  
PW class not set, XC ID 0xc0000005  
Encapsulation MPLS, protocol LDP  
Source address 10.0.0.11  
PW type Ethernet, control word disabled, interworking none  
PW backup disable delay 0 sec  
Sequencing not set

PW Status TLV in use  
MPLS Local Remote

-----  
Label 16049 16059  
Group ID 0x6000180 0x4000280  
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2  
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: 3221225477  
Create time: 03/05/2013 15:04:03 (00:21:26 ago)  
Last time status changed: 03/05/2013 15:17:34 (00:07:55 ago)  
MAC withdraw message: send 0 receive 0  
Statistics:  
packets: received 25628, sent 51412  
bytes: received 1742974, sent 3729012

Backup PW:  
PW: neighbor 10.0.0.14, PW ID 222, state is standby ( all ready )  
Backup for neighbor 10.0.0.13 PW ID 222 ( inactive )  
PW class not set, XC ID 0xc0000006  
Encapsulation MPLS, protocol LDP  
Source address 10.0.0.11  
PW type Ethernet, control word disabled, interworking none  
Sequencing not set

PW Status TLV in use  
MPLS Local Remote

-----  
Label 16050 289971  
Group ID 0x6000180 0x4000100  
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2  
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: 0x20 (Standby) in Notification message
MIB cpwVcIndex: 3221225478
Create time: 03/05/2013 15:04:03 (00:21:26 ago)
Last time status changed: 03/05/2013 15:17:34 (00:07:55 ago)
MAC withdraw message: send 0 receive 0
RP/0/RSP0/CPU0:router2#
```

AC のステータスと PW のステータスはペアであるため、router3 の AC がダウンした場合、router3 は「AC のダウン」を router2 にシグナリングします。router2 はプライマリ PW をダウンさせ、バックアップ PW をアクティブにします。

```
RP/0/RSP0/CPU0:May  3 15:34:08.772 : l2vpn_mgr[1121]: %L2-L2VPN_PW-3-UPDOWN :
Pseudowire with address 10.0.0.13, id 222, state is Down
RP/0/RSP0/CPU0:May  3 15:34:08.772 : l2vpn_mgr[1121]: %L2-L2VPN_PW-3-UPDOWN :
Pseudowire with address 10.0.0.14, id 222, state is Up
```

```
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test
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
-----
test p2p6 UP Gi0/1/0/3.2 UP 10.0.0.13 222 DN
Backup
10.0.0.14 222 UP
-----
```

```
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect group test det

Group test, XC p2p6, state is up; Interworking none
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1504; XC ID 0xc40003; interworking none
Statistics:
packets: received 51735, sent 25632
bytes: received 3752406, sent 1743230
drops: illegal VLAN 0, illegal length 0
PW: neighbor 10.0.0.13, PW ID 222, state is down ( local ready )
PW class not set, XC ID 0xc0000005
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set
```

```
PW Status TLV in use
MPLS Local Remote
```

```
-----
Label 16049 16059
Group ID 0x6000180 0x4000280
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
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: 0x6 (AC Down) in Notification message
Outgoing Status (PW Status TLV):
Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225477
Create time: 03/05/2013 15:04:03 (00:30:14 ago)
Last time status changed: 03/05/2013 15:34:08 (00:00:09 ago)
MAC withdraw message: send 0 receive 0

Backup PW:
PW: neighbor 10.0.0.14, PW ID 222, state is up ( established )
Backup for neighbor 10.0.0.13 PW ID 222 ( active )
PW class not set, XC ID 0xc0000006
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
Sequencing not set

PW Status TLV in use
MPLS Local Remote
-----
```

```
Label 16050 289971
Group ID 0x6000180 0x4000100
Interface GigabitEthernet0/1/0/3.2 GigabitEthernet0/0/0/1.2
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: 3221225478
Create time: 03/05/2013 15:04:03 (00:30:14 ago)
Last time status changed: 03/05/2013 15:34:08 (00:00:09 ago)
MAC withdraw message: send 0 receive 0
Statistics:
packets: received 25632, sent 51735
bytes: received 1743230, sent 3752406
RP/0/RSP0/CPU0:router2#
```

router3 の AC が復旧すると、router2 は router3 へのプライマリ PW を再びアクティブにし、router4 への PW はスタンバイ状態に戻ります。

router3 がダウンして router2 からループバックへのルートが失われた場合にも、バックアップ PW がアクティブになります。

次の論理的なステップは、各サイトに 2 つの PE を備えた双方向の PW 冗長性を導入することです。

しかし、このフルメッシュのPWでは、2つのPWが同時にアクティブになったときにネットワークにループが発生するという問題があります。ループはなくす必要があります、一般的には、このためにスパニングツリープロトコル(STP)が使用されます。ただし、1つのサイトのスパニングツリーの不安定さが他のサイトに伝播することは望ましくありません。このため、これらのPWでスパニングツリーを実行したり、2つのサイト間でスパニングツリーをマージしたりすることは推奨されません。2つのサイト間に1つの論理リンクしかなく、スパニングツリーが不要であるならば簡単になります。

解決策の1つは、1つのサイトの2つのPEとローカルCEの間でMC-LAGバンドルを使用することです。2つのPEの内の1つだけがアクティブなバンドルメンバーを持つので、そのPEのリモートサイトへのPWがアクティブになります。もう片方のPEはスタンバイ状態のバンドルメンバーを持ち、リモートサイトへのPWはダウンします。2つのサイト間で1つのPWのみがアクティブになるため、ループは発生しません。アクティブなPWを持つPEには、リモートサイトの2番目のPEへのスタンバイPWもあります。

安定した状態では、アクティブなバンドルメンバーはrouter2およびrouter3にあり、アクティブなPWはその間にあります。router3の設定を次に示します。

```
RP/0/RSP1/CPU0:router3#sh run redundancy
redundancy
iccp
group 2
mlacp node 1
mlacp system mac 0200.0000.0002
mlacp system priority 1
mlacp connect timeout 0
member
neighbor 10.0.0.14
!
backbone
interface TenGigE0/0/0/0
interface TenGigE0/0/0/1
!
isolation recovery-delay 300
!
!
!
```

```
RP/0/RSP1/CPU0:router3#sh run int bundle-ether 222
interface Bundle-Ether222
lacp switchover suppress-flaps 100
mlacp iccp-group 2
mlacp switchover type revertive
mlacp switchover recovery-delay 40
mlacp port-priority 1
mac-address 0.0.2
bundle wait-while 0
bundle maximum-active links 1
load-interval 30
!
```

```
RP/0/RSP1/CPU0:router3#sh run l2vpn xconnect group test
l2vpn
xconnect group test
p2p p2p7
interface Bundle-Ether222.2
neighbor 10.0.0.11 pw-id 222
backup neighbor 10.0.0.12 pw-id 222
!
!
```

```
!  
!  
!  
RP/0/RSP1/CPU0:router3#sh l2vpn xconnect group test  
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  
-----  
test p2p7 UP BE222.2 UP 10.0.0.11 222 UP  
Backup  
10.0.0.12 222 DN  
-----
```

```
RP/0/RSP1/CPU0:router3#sh bundle bundle-ether 222
```

```
Bundle-Ether222  
Status: Up  
Local links : 1 / 0 / 1  
Local bandwidth : 1000000 (1000000) kbps  
MAC address (source): 0000.0000.0002 (Configured)  
Inter-chassis link: No  
Minimum active links / bandwidth: 1 / 1 kbps  
Maximum active links: 1  
Wait while timer: Off  
Load balancing: Default  
LACP: Operational  
Flap suppression timer: 100 ms  
Cisco extensions: Disabled  
mLACP: Operational  
ICCP Group: 2  
Role: Active  
Foreign links : 0 / 1  
Switchover type: Revertive  
Recovery delay: 40 s  
Maximize threshold: 1 link  
IPv4 BFD: Not configured
```

```
Port Device State Port ID B/W, kbps  
-----  
Gi0/0/0/1 Local Active 0x8001, 0x9001 1000000  
Link is Active  
Gi0/0/0/1 10.0.0.14 Standby 0x8002, 0xa002 1000000  
Link is marked as Standby by mLACP peer
```

router5 では、ローカル バンドル メンバーと router2 へのプライマリ PW はスタンバイ状態にあり、router4 へのバックアップ PW はダウンしています。

```
RP/0/RSP1/CPU0:router5#sh run redundancy  
redundancy  
iccp  
group 2  
mlacp node 2  
mlacp system mac 0200.0000.0002  
mlacp system priority 1  
mlacp connect timeout 0  
member  
neighbor 10.0.0.13  
!  
backbone  
interface TenGigE0/1/0/0  
interface TenGigE0/1/0/1  
!
```

```
isolation recovery-delay 300
!  
!  
!
```

```
RP/0/RSP1/CPU0:router5#sh run int bundle-ether 222  
interface Bundle-Ether222  
lACP switchover suppress-flaps 100  
mlACP icCP-group 2  
mlACP switchover type revertive  
mlACP switchover recovery-delay 40  
mac-address 0.0.2  
bundle wait-while 0  
bundle maximum-active links 1  
load-interval 30  
!
```

```
RP/0/RSP1/CPU0:router5#sh run l2vpn xconnect group test  
l2vpn  
xconnect group test  
p2p p2p7  
interface Bundle-Ether222.2  
neighbor 10.0.0.11 pw-id 222  
backup neighbor 10.0.0.12 pw-id 222  
!  
!  
!  
!  
!
```

```
RP/0/RSP1/CPU0:router5#sh l2vpn xconnect group test  
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  
-----  
test p2p7 DN BE222.2 UP 10.0.0.11 222 SB  
Backup  
10.0.0.12 222 DN  
-----
```

```
RP/0/RSP1/CPU0:router5#sh bundle bundle-ether 222
```

```
Bundle-Ether222  
Status: mLACP hot standby  
Local links : 0 / 1 / 1  
Local bandwidth : 0 (0) kbps  
MAC address (source): 0000.0000.0002 (Configured)  
Inter-chassis link: No  
Minimum active links / bandwidth: 1 / 1 kbps  
Maximum active links: 1  
Wait while timer: Off  
Load balancing: Default  
LACP: Operational  
Flap suppression timer: 100 ms  
Cisco extensions: Disabled  
mLACP: Operational  
ICCP Group: 2  
Role: Standby  
Foreign links : 1 / 1  
Switchover type: Revertive  
Recovery delay: 40 s  
Maximize threshold: 1 link  
IPv4 BFD: Not configured
```

```
Port Device State Port ID B/W, kbps
-----
Gi0/0/0/1 Local Standby 0x8002, 0xa002 1000000
mLACP peer is active
Gi0/0/0/1 10.0.0.13 Active 0x8001, 0x9001 1000000
Link is Active
```

router6 では、router3 へのバンドル メンバーはアクティブであり、router5 へのバンドル メンバーはスタンバイ状態です。

```
router6#sh etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
```

```
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
```

```
Number of channel-groups in use: 1
Number of aggregators: 1
```

```
Group Port-channel Protocol Ports
-----+-----+-----+-----
2 Po2(SU) LACP Gi0/1(P) Gi0/2(w)
```

router3 のバンドル メンバーがダウンした場合、router6 には router5 へのアクティブ メンバーがあります。

```
router6#sh etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
```

```
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
```

```
Number of channel-groups in use: 1
Number of aggregators: 1
```

```
Group Port-channel Protocol Ports
-----+-----+-----+-----
2 Po2(SU) LACP Gi0/1(D) Gi0/2(P)
```

router5 で bundle-ether222 がダウンしているため、ペアになっている router2 への PW は同時にダウンします。

```
RP/0/RSP1/CPU0:router3#sh l2vpn xconnect group test
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
-----
```

```
test p2p7 DN BE222.2 DN 10.0.0.11 222 DN
Backup
10.0.0.12 222 DN
```

-----

router2 は、router3 への PW がダウンしたことを検出し、router5 へのバックアップ PW をアクティブにします。

```
RP/0/RSP0/CPU0:router2#sh l2vpn xconnect
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
```

```
-----
test p2p7 UP BE222.2 UP 10.0.0.13 222 DN
Backup
10.0.0.14 222 UP
```

-----

router5 はそのバンドル メンバーと router2 へのプライマリ PW をアクティブにします。

```
RP/0/RSP1/CPU0:router5#sh bundle bundle-ether 222
```

```
Bundle-Ether222
Status: Up
Local links : 1 / 0 / 1
Local bandwidth : 1000000 (1000000) kbps
MAC address (source): 0000.0000.0002 (Configured)
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
Maximum active links: 1
Wait while timer: Off
Load balancing: Default
LACP: Operational
Flap suppression timer: 100 ms
Cisco extensions: Disabled
mLACP: Operational
ICCP Group: 2
Role: Active
Foreign links : 0 / 1
Switchover type: Revertive
Recovery delay: 40 s
Maximize threshold: 1 link
IPv4 BFD: Not configured
```

```
Port Device State Port ID B/W, kbps
```

```
-----
Gi0/0/0/1 Local Active 0x8002, 0xa002 1000000
Link is Active
Gi0/0/0/1 10.0.0.13 Configured 0x8003, 0x9001 1000000
Link is down
```

```
RP/0/RSP1/CPU0:router5#sh l2vpn xconnect group test
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
```

```
-----
test p2p7 UP BE222.2 UP 10.0.0.11 222 UP
Backup
10.0.0.12 222 DN
```



### 3.2.5.4 ASR 9000 nV エッジ クラスタ

MC-LAG と PW の冗長性に基づく[前の設計](#)は、冗長性については十分機能しますが、一部のバンドル メンバーはスタンバイ状態であるため、安定した状態ではトラフィックを伝送しません。

安定した状態であってもすべてのバンドル メンバーをアクティブにするために、PE の各ラックに接続された CE からのバンドル メンバーを備えた ASR 9000 クラスタを使用できます。

この設計は、CE と PE の間のバンドル メンバーのリンク障害、ラックの障害、およびコア リンク障害に対して冗長性があります。また、クラスタが MPLS コアに二重で接続されていれば、コアの冗長性もあります。2 つのラックは同じ場所に配置する必要はなく、異なる場所に配置できます。ラック間のリンクはこの図では示されていません。

CE の冗長性が必要な場合は、次のような CE 用マルチシャーシ ソリューションを使用できます。

- MC-LAG
- ASR 9000 nV クラスタリング
- VSS
- vPC

ASR 9000 クラスタの設定はとても基本的です。

```
interface TenGigE0/0/0/8
bundle id 222 mode on
!
interface TenGigE1/0/0/8
bundle id 222 mode on
!
interface Bundle-Ether222
!
interface Bundle-Ether222.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
l2vpn
xconnect group test
p2p p2p8
interface Bundle-Ether222.2
neighbor 10.0.0.13 pw-id 8
!
!
!
!
```

指定シェルフ コントローラのスイッチオーバーによる MAC アドレスの変更を避けるために、スタティックな LACP システムの MAC アドレスとバンドル MAC アドレスを設定することを推奨します。次の例に、アドレスの検出方法を示します。

```
RP/1/RSP0/CPU0:router2#sh int bundle-ether 222 | i address is
Hardware is Aggregated Ethernet interface(s), address is 0024.f71e.d309
Internet address is Unknown
RP/1/RSP0/CPU0:router2#
RP/1/RSP0/CPU0:router2#conf
RP/1/RSP0/CPU0:router2(config)#int bundle-ether 222
RP/1/RSP0/CPU0:router2(config-if)#mac-address 0024.f71e.d309
RP/1/RSP0/CPU0:router2(config-if)#commit
RP/1/RSP0/CPU0:router2(config-if)#end
RP/1/RSP0/CPU0:router2#
```

```
RP/1/RSP0/CPU0:router2#sh lacp system-id
```

```
Priority MAC Address
```

```
-----
```

```
0x8000 00-24-f7-1e-d3-05
```

```
RP/1/RSP0/CPU0:router2#
```

```
RP/1/RSP0/CPU0:router2#conf
```

```
RP/1/RSP0/CPU0:router2(config)#lacp system mac 0024.f71e.d305
```

```
RP/1/RSP0/CPU0:router2(config)#commit
```

```
RP/1/RSP0/CPU0:router2(config)#end
```

要約すると、これは各ラックのメンバー (ラック 0 の 10 の 0/0/0/8 とラック 1 の 10 の 1/0/0/8) を含んだ bundle-ether 222 と、ポイントツーポイント クロス コネクト用に設定されたバンドル サブインターフェイスです。

```
RP/1/RSP0/CPU0:router2#sh l2vpn xconnect group test
```

```
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
```

```
-----
```

```
test p2p8 UP BE222.2 UP 10.0.0.13 8 UP
```

```
-----
```

### 3.3 CDP

シスコのルータとスイッチは、通常、dot1q タグのない CDP パケットを送信します。クロス コネクトが設定された IOS XR ルータで CDP パケットが受信されたときに、これらのパケットの処理を決定するシナリオは複数あります。

このトポロジでは、router1 は、設定に応じて、ローカル PE である router2 またはリモート CE である router4 を CDP ネイバーとして認識します。

#### 3.3.1 L2VPN PE のメイン インターフェイスの CDP が無効の場合

L2VPN CE からの CDP パケットはクロス コネクト上を転送されます。メイン インターフェイスで l2transport が設定されている場合、またはタグなし CDP フレームと一致するサブインターフェイスがある場合、2 つの L2VPN CE はお互いを認識します ( show cdp neighbors コマンドを使用します )。

メイン インターフェイスの例を次に示します。

```
interface GigabitEthernet0/0/0/1
l2transport
!
!
l2vpn
xconnect group test
p2p p2p8
interface GigabitEthernet0/0/0/1
neighbor 10.0.0.11 pw-id 8
!
!
!
!
```

タグなしのサブインターフェイスの例を次に示します。

```
interface GigabitEthernet0/0/0/1.1 l2transport
encapsulation untagged
!
l2vpn
xconnect group test
p2p p2p8
interface GigabitEthernet0/0/0/1.1
neighbor 10.0.0.11 pw-id 8
!
!
!
!
```

これら 2 つの例では、CDP パケットはクロス コネクト上で転送され、CE はお互いを CDP ネイバーとして認識します。CE は PE を CDP ネイバーとして認識しません。

```
router1#sh cdp nei gigabitEthernet 0/1
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
D - Remote, C - CVTA, M - Two-port Mac Relay
```

```
Device ID Local Intrfce Holdtme Capability Platform Port ID
router4 Gig 0/1 168 R S ME-3400G- Gig 0/1
```

### 3.3.2 L2VPN PE のメイン インターフェイスの CDP が有効の場合

PE はタグなし CDP パケットを処理し、PE と CE はお互いをネイバーとして認識します。ただし、L2VPN PE のメイン インターフェイスで CDP が有効な場合、CE はリモート CE を認識しません。

次の注意してください。

- l2transport が設定されたメイン インターフェイスでは、CDP を設定できません。
- l2transport ではないメイン インターフェイスで CDP が設定されている場合、PE が CDP パケットを受信します。これはタグなし CDP パケットと一致するように設定された ( **encapsulation untagged** コマンドまたは **encapsulation default** コマンドを使用 ) l2transport サブインターフェイスがある場合でも起こります。この場合、CDP パケットはリモート サイトに転送されません。

## 3.4 スパニング ツリー

L2VPN CE がイーサネット スイッチで、L2VPN PE にスパニングツリー BPDU を送信する場合、これらの BPDU は通常のトラフィックとして処理され、L2VPN の設定に従って転送されます。

メイン インターフェイスに l2transport が設定されている場合、または **encapsulation untagged** コマンドか **encapsulation default** コマンドが設定された l2transport サブインターフェイスがある場合、STP または MST BPDU はタグなしで送信され、ポイントツーポイント クロス コネクトを介して転送されます。

BPDU の dot1q タグと一致する l2transport サブインターフェイスがある場合、転送されたタグ付き BPDU は Per VLAN Spanning Tree Plus ( PVST+ ) または Rapid PVST+ ( PVRST+ ) によって送信されます。

次にトポロジの例を示します。

router2 と router3 は、タグなしフレームと、dot1q タグ 2 の付いたフレームを転送します。

```
interface GigabitEthernet0/0/0/1.1 l2transport
encapsulation untagged
!
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
l2vpn
xconnect group test
p2p p2p8
interface GigabitEthernet0/0/0/1.2
neighbor 10.0.0.11 pw-id 8
!
!
p2p p2p9
interface GigabitEthernet0/0/0/1.1
neighbor 10.0.0.11 pw-id 9
!
!
!
!
```

switch1 は、switch4 から、VLAN 1のタグなしの BPDU と VLAN2 のタグ付きの BPDU を受信します。 そのルート ポートは Gi0/1 上にあり、switch4 の方を向いています。

```
switch1#sh spanning-tree vlan 1
```

```
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32768
Address 0024.985e.6a00
Cost 8
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
```

```
Interface Role Sts Cost Prio.Nbr Type
```

```
-----
Gi0/1 Root FWD 4 128.1 P2p
```

```
switch1#sh spanning-tree vlan 2
```

```
VLAN0002
Spanning tree enabled protocol ieee
Root ID Priority 32770
Address 0019.552b.b580
Cost 4
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32770 (priority 32768 sys-id-ext 2)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 15
```

```
Interface Role Sts Cost Prio.Nbr Type
```

-----  
Gi0/1 Root FWD 4 128.1 P2p

この設定によって、サイト A のスパニング ツリー ドメインは、B 側のスパニング ツリー ドメインとマージされます。考えられる問題として、1 つのサイトのスパニング ツリーの不安定さが他のサイトに伝播する恐れがあります。

1 つのサイトが 1 つの PW のみを介して他のサイトと接続されており、物理的なループを生じる可能性があるバックドア リンクはないという確信がある場合は、2 つのサイト間でスパニング ツリーを実行しないことを推奨します。これによって、2 つのスパニング ツリー ドメインが分離された状態を維持できます。このためには、CE でスパニング ツリーの bpdudfilter を設定するか、BPDU で使用される宛先 MAC アドレスを持つフレームをドロップするように、PE でイーサネットサービス アクセスリストを設定します。PE 上のイーサネットサービス アクセスリストを使用すると、BPDU の宛先 MAC を持つフレームや、PW 上での転送が望ましくない他の種類の L2 プロトコルを持つフレームをドロップできます。

2 つのサイト間で転送される各 l2transport (サブ) インターフェイスで使用可能なアクセスリストを次に示します。

```
ethernet-services access-list block-invalid-frames
10 deny any 0180.c200.0000 0000.0000.000f
20 deny any host 0180.c200.0010
30 deny any host 0100.0c00.0000
40 deny any host 0100.0ccc.cccc
50 deny any host 0100.0ccc.cccd
60 deny any host 0100.0ccd.cdce
70 permit any any
!
```

```
RP/0/RSP1/CPU0:router2#sh run int GigabitEthernet0/0/0/1.1
interface GigabitEthernet0/0/0/1.1 l2transport
encapsulation untagged
ethernet-services access-group block-invalid-frames ingress
ethernet-services access-group block-invalid-frames egress
!
```

```
RP/0/RSP1/CPU0:router2#sh run int GigabitEthernet0/0/0/1.2
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
ethernet-services access-group block-invalid-frames ingress
ethernet-services access-group block-invalid-frames egress
!
```

イーサネットサービス ACL は、BPDU のドロップを開始します。

```
RP/0/RSP1/CPU0:router2#sh access-lists ethernet-services block-invalid-frames
hardware ingress location 0/0/CPU0
ethernet-services access-list block-invalid-frames
10 deny any 0180.c200.0000 0000.0000.000f (41 hw matches)
20 deny any host 0180.c200.0010
30 deny any host 0100.0c00.0000
40 deny any host 0100.0ccc.cccc
50 deny any host 0100.0ccc.cccd (63 hw matches)
60 deny any host 0100.0ccd.cdce
70 permit any any (8 hw matches)
```

switch1 は switch4 から BPDU を受信しなくなるため、switch1 がルートになります。

```
switch1#sh spanning-tree vlan 1
VLAN0001
```

```
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 001d.4603.1f00
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 15
```

```
Interface Role Sts Cost Prio.Nbr Type
-----
Gi0/1 Desg FWD 4 128.1 P2p
```

```
switch1#sh spanning-tree vlan 2
```

```
VLAN0002
Spanning tree enabled protocol ieee
Root ID Priority 32770
Address 001d.4603.1f00
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 32770 (priority 32768 sys-id-ext 2)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 15
```

```
Interface Role Sts Cost Prio.Nbr Type
-----
Gi0/1 Desg FWD 4 128.1 P2p
```

リンクのスパニング ツリーを無効化するリスクは次のとおりです。 サイト間でバックドア接続が生じた場合、物理的なループが構築され、スパニング ツリーによってループを切断することができません。 このため、PW 上のスパニング ツリーを無効にする場合は、サイトに冗長リンクが存在しないこと、および PW が常にサイト間の唯一の接続であることを確認してください。

サイトに複数の接続がある場合は、MST アクセス ゲートウェイ (MSTAG) や PVST+ アクセス ゲートウェイ (PVSTAG) などのアクセス ゲートウェイ バージョンのスパニング ツリーとともに、VPLS などのソリューションを使用します。 詳細については、「[マルチポイント サービス](#)」の項を参照してください。

## 4. マルチポイント サービス

注：

このセクションで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ( [登録ユーザ専用](#) ) を使用してください。

特定の show コマンドが [アウトプット インタープリタ ツール](#) ( [登録ユーザ専用](#) ) でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

マルチポイント L2 機能全体の説明については、「[マルチポイント レイヤ 2 サービスの実装](#)」を参照してください。

インターフェイスが 2 つだけのポイントツーポイント クロス コネクトでは、L2VPN スイッチは一方の側で受信したすべてをもう一方の側に転送します。

ブリッジドメインに 3 つ以上のインターフェイスがある場合、イーサネット スイッチは、宛先 MAC アドレスに基づいてフレームの転送先を決定するためにスイッチングの判断を行う必要があります。スイッチは、受信したフレームの送信元 MAC アドレスに基づいて MAC ラーニングを実行し、MAC アドレステーブルを作成します。

スイッチは次の方法でフレームを転送します。

- ブロードキャスト フレームはすべてのポートにフラッディングされます。ブロードキャストのフラッディング レートを制限するために、ストーム制御を使用します。
- Internet Group Management Protocol ( IGMP ) またはマルチキャスト リスナー検出 ( MLD ) スヌーピングが設定されている場合を除き、マルチキャスト フレームはブリッジドメインのすべてのポートにフラッディングされます。マルチキャストのフラッディング レートを制限するために、ストーム制御を使用します。
- 宛先 MAC アドレスがブリッジドメインの MAC アドレステーブルにないユニキャスト フレーム ( 不明なユニキャスト ) は、ブリッジドメインのすべてのポートにフラッディングされます。不明なユニキャストのフラッディング レートを制限するために、ストーム制御を使用します。
- 宛先 MAC アドレスがブリッジドメインの MAC アドレステーブル内にあるユニキャスト フレームは、この宛先 MAC アドレスを学習したポートに転送されます。

Cisco IOS XR ソフトウェアでは、ブロードキャスト ドメインまたはエミュレート LAN は、ブリッジドメインと呼ばれます。これは、Cisco IOS ソフトウェアの用語の VLAN に似ていますが、IOS の VLAN は、トランクで dot1q タグとして使用される VLAN 番号にリンクされている点異なります。Cisco IOS XR ソフトウェアのブリッジドメインは、dot1q の VLAN タグ番号にリンクされません。EVC モデルを使用すると、dot1q タグを操作して、dot1q サブインターフェイスに同じブリッジドメイン内で異なる dot1q VLAN 番号を設定したり、タグなしのインターフェイスを設定したりすることができます。

ブリッジドメインは、基本的に、ブロードキャスト フレームおよびマルチキャスト フレームがフラッディングされる 1 つのブロードキャスト ドメインです。それぞれのブリッジドメインには、1 つの MAC アドレステーブルが関連付けられます ( 設定によって手動で MAC ラーニングが無効にされている非常に稀な場合を除く )。これは通常、ブリッジドメイン内のすべてのホストが直接接続される IPv4 または IPv6 の 1 つのサブネットに対応します。

ブリッジドメインはブリッジ グループ内でグループ化できます。これは設定を確認するのに便利です。ブリッジドメインごとに 1 つの show コマンドを実行する代わりに、ブリッジ グループに対して 1 つの show コマンドを実行できます。ブリッジ グループには、MAC アドレステーブルなどの関連付けはありません。設定や show コマンドで使用されるだけです。

## 4.1 ローカル スイッチング

非常に基本的な例を次に示します。

router2、router3、および router4 は、それら 3 台のルータ間の LAN をシミュレートする ASR 9000 を介して接続されています。

これら 3 台のルータのインターフェイス設定を次に示します。

```
RP/0/RSP0/CPU0:router2#sh run int gig 0/1/0/39.2
interface GigabitEthernet0/1/0/39.2
ipv4 address 192.168.2.2 255.255.255.0
encapsulation dot1q 2
!
```

```
router3#sh run int gig 0/1
Building configuration...
```

```
Current configuration : 203 bytes
!
interface GigabitEthernet0/1
port-type nni
switchport access vlan 2
switchport trunk allowed vlan 1,2
switchport mode trunk
end
```

```
router3#sh run int vlan 2
Building configuration...
```

```
Current configuration : 61 bytes
!
interface Vlan2
ip address 192.168.2.3 255.255.255.0
end
```

```
router3#
```

```
RP/0/RSP0/CPU0:router4#sh run int ten 0/0/1/0.2
interface TenGigE0/0/1/0.2
ipv4 address 192.168.2.4 255.255.255.0
encapsulation dot1q 2
!
```

router1 で受信された dot1q タグ 2 を持つパケットは、dot1q タグ 2 を持つ他のルータに転送されます。

この基本的なシナリオでは、AC について 2 つのオプションがあります。

1. すべての AC が dot1q タグ 2 を使用するため、フレームのタグを保持し、入力インターフェイスで受信されたのと同じ dot1q タグを持つフレームを出力インターフェイスで転送できます。 `rewrite ingress tag pop 1 symmetric` コマンドは必要ありません。
2. 入力方向で着信した dot1q タグ 2 をポップし、対称的に出力方向で dot1q タグ 2 をプッシュできます。この基本的なシナリオでは必要ありませんが、将来的に高い柔軟性が得られるので、最初からブリッジドメインをこのように設定するのも良い方法です。初期設定後に行う可能性がある 2 つの変更の例を次に示します。
  - 後でブリッジドメインにルーテッド BVI インターフェイスが導入する場合、パケットはタグなしで BVI で処理する必要があります。詳細については、該当する項を参照してください。
  - 別の dot1q タグを使用する新しい AC が後で追加される場合があります。入力方向で dot1q タグ 2 をポップし、出力方向の新しいインターフェイスで他の dot1q タグをプッシュします。逆も同様です。 [BVI](#)

router1 の各 AC で dot1q タグをポップします。

```
RP/0/RSP0/CPU0:router1#sh run int GigabitEthernet0/1/0/3.2
```



```
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
```

```
RP/0/RSP0/CPU0:router1#sh run int GigabitEthernet0/1/0/38.2
interface GigabitEthernet0/1/0/38.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
```

```
RP/0/RSP0/CPU0:router1#sh run int TenGigE0/2/0/4.2
interface TenGigE0/2/0/4.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
```

これら 3 つの AC を含むブリッジドメインの設定を次に示します。

```
RP/0/RSP0/CPU0:router1#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain engineering
interface TenGigE0/2/0/4.2
!
interface GigabitEthernet0/1/0/3.2
!
interface GigabitEthernet0/1/0/38.2
!
!
!
!
```

ブリッジドメインはブリッジグループで設定する必要があります。この顧客が他のブリッジドメインを必要とする場合、同じブリッジグループ customer1 にそれらのドメインを設定できます。新しいブリッジドメインが他の顧客に属する場合は、新しいブリッジグループを作成できます。この例ではブリッジドメインのグループ化に顧客を使用していますが、ブリッジドメインは任意の条件でグループ化できます。

このブリッジドメインの設定を表示するには、**show run l2vpn bridge group customer1 bridge-domain engineering** コマンドを使用します。

すべてのブリッジドメインの設定を表示するには、**show run l2vpn bridge group customer1** コマンドを使用します。

ブリッジドメインについての情報を表示するには、**show l2vpn bridge-domain bd-name engineering** コマンドまたは **show l2vpn bridge-domain group customer1** コマンドを使用します。

```
RP/0/RSP0/CPU0:router1#show l2vpn bridge-domain group customer1 bd-name
engineering
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,
ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 3 (3 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.2, state: up, Static MAC addresses: 0
Gi0/1/0/38.2, state: up, Static MAC addresses: 0
Te0/2/0/4.2, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
```

```
RP/0/RSP0/CPU0:router1#show l2vpn bridge-domain group customer1 bd-name
engineering det
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 5, 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 down: 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 profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 6
Filter MAC addresses:
Create time: 28/05/2013 17:17:03 (00:18:06 ago)
No status change since creation
ACs: 3 (3 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40003; 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 profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 185066, sent 465
bytes: received 13422918, sent 34974
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
AC: GigabitEthernet0/1/0/38.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40005; 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 profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 8, sent 12287
bytes: received 770, sent 892418
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
AC: TenGigE0/2/0/4.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0x1040001; 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 profile: none
Storm Control: disabled
Static MAC addresses:
Statistics:
packets: received 463, sent 11839
bytes: received 35110, sent 859028
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:
```

各 AC 上でパケットが受信および送信されたことを確認する場合は、**show l2vpn bridge-domain group customer1 bd-name engineering det** コマンドを使用します。

MAC アドレステーブルを確認する場合は、*mac-address* キーワードを **show l2vpn forwarding bridge-domain** コマンドに追加します。

```
RP/0/RSP0/CPU0:router1#show l2vpn forwarding bridge-domain customer1:
engineering mac-address location 0/1/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location
```

```
Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
-----
0019.552b.b581 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0024.986c.6417 dynamic Gi0/1/0/38.2 0/1/CPU0 0d 0h 0m 0s N/A
6c9c.ed3e.e484 dynamic Te0/2/0/4.2 0/2/CPU0 0d 0h 0m 0s N/A
```

MAC ラーニングは、ブリッジ ドメインでフレームが受信されるたびにラインカードによってハードウェアで実行されます。MAC アドレステーブルにはソフトウェアのキャッシュもありますが、ハードウェアのエントリと一致させるためにこのソフトウェアのテーブルを継続的に更新することはできません。最新のコードで **show** コマンドが入力されたときに、ハードウェア テーブルとソフトウェア テーブルの再同期が試みられます。(テーブルが大きい場合など)再同期が完了していなくても、最大 15 秒後にソフトウェアの MAC アドレステーブルの現在の状態が表示されます。ソフトウェアとハードウェアのテーブルを手動で再同期するには、**l2vpn resynchronize forwarding mac-address-table** コマンドを使用します。

```
RP/0/RSP0/CPU0:router1#term mon
RP/0/RSP0/CPU0:router1#l2vpn resynchronize forwarding mac-address-table
location 0/1/CPU0
RP/0/RSP0/CPU0:router1#LC/0/1/CPU0:May 28 18:25:35.734 : vkg_l2fib_mac_cache[357]
%PLATFORM-
PLAT_L2FIB_MAC_CACHE-6-RESYNC_COMPLETE : The resynchronization of the MAC
address table is complete
0/1/CPU0
```

```
RP/0/RSP0/CPU0:router1#show l2vpn forwarding bridge-domain customer1:engineering
mac-address location 0/1/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location
```

```
Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
-----
0019.552b.b581 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
6c9c.ed3e.e484 dynamic Te0/2/0/4.2 0/2/CPU0 0d 0h 0m 0s N/A
```

Syslog メッセージで再同期プロセスの完了が通知されるので、このメッセージを表示するように **terminal monitor** を有効にしておくくと便利です。

"Resync Age" 列には、MAC アドレスを前回ハードウェア テーブルから再同期した時間が表示されます。

*location* キーワードは、着信または送信ラインカードの場所です。MAC アドレスは、ハードウェアのラインカードの間で交換されるため、MAC アドレスは、AC または PW があるそれぞれのラインカードで記憶されます。*detail* キーワードによって、ソフトウェア テーブルのより新しいバージョンが提供される場合があります。

```
RP/0/RSP0/CPU0:router1#show l2vpn forwarding bridge-domain customer1:
engineering mac-address detail location 0/1/CPU0
```

```
Bridge-domain name: customer1:engineering, id: 5, 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  
Bridge MTU: 1500 bytes  
Number of bridge ports: 3  
Number of MAC addresses: 4  
Multi-spanning tree instance: 0  
To Resynchronize MAC table from the Network Processors, use the command...  
l2vpn resynchronize forwarding mac-address-table location

GigabitEthernet0/1/0/3.2, state: oper up  
Number of MAC: 2  
Statistics:  
packets: received 187106, sent 757  
bytes: received 13571342, sent 57446  
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

Mac Address: 0019.552b.b581, LC learned: 0/1/CPU0  
**Resync Age:** 0d 0h 0m 0s, Flag: local

Mac Address: 0019.552b.b5c3, LC learned: 0/1/CPU0  
**Resync Age:** 0d 0h 0m 0s, Flag: local

GigabitEthernet0/1/0/38.2, state: oper up  
Number of MAC: 1  
Statistics:  
packets: received 18, sent 14607  
bytes: received 1950, sent 1061882  
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

Mac Address: 0024.986c.6417, LC learned: 0/1/CPU0  
**Resync Age:** 0d 0h 0m 0s, Flag: local

TenGigE0/2/0/4.2, state: oper up  
Number of MAC: 1  
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
```

```
Mac Address: 6c9c.ed3e.e484, LC learned: 0/2/CPU0
```

```
Resync Age: 0d 0h 0m 0s, Flag: remote
```

詳細バージョンのコマンドでは、ブリッジドメインで学習された MAC アドレスの総数と、各 AC で学習された MAC アドレスの数が表示されます。

*hardware* キーワードは、ハードウェアの MAC アドレステーブルを入力または出力フォワーディング エンジンから直接取得します。

```
RP/0/RSP0/CPU0:router1#show l2vpn forwarding bridge-domain customer1:
engineering mac-address hardware ingress location 0/1/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location
```

```
Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
```

```
-----
0019.552b.b581 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A
0024.986c.6417 dynamic Gi0/1/0/38.2 0/1/CPU0 0d 0h 0m 0s N/A
6c9c.ed3e.e484 dynamic Te0/2/0/4.2 0/2/CPU0 0d 0h 0m 0s N/A
```

```
RP/0/RSP0/CPU0:router1#show l2vpn forwarding bridge-domain customer1:
engineering mac-address hardware egress location 0/2/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location
```

```
Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
```

```
-----
0019.552b.b581 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 14s N/A
0019.552b.b5c3 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 1s N/A
0024.986c.6417 dynamic Gi0/1/0/38.2 0/1/CPU0 0d 0h 0m 10s N/A
6c9c.ed3e.e484 dynamic Te0/2/0/4.2 0/2/CPU0 0d 0h 0m 13s N/A
```

```
RP/0/RSP0/CPU0:router1#
```

## 4.2 フル MST

[前のローカルスイッチングの例](#)は、ルータのみがブリッジドメインに接続されている基本的な例でした。L2 スイッチを接続し始めると、ループが構築される可能性があり、ループを解消するために STP が必要になります。

このトポロジの router1、router2、および router3 には、図に示すすべてのインターフェイスでブリッジドメインがそれぞれ設定されています。router4 が ARP 要求などのブロードキャストを router1 に送信すると、router1 は router2 と router3 にフラッディングし、router2 は router3 にフラッディングし、router3 は router2 にフラッディングします。これによってループおよびブロードキャストストームが発生します。

ループを解消するには STP を使用します。STP には複数の種類がありますが、Cisco IOS XR ソフトウェアでは完全実装の MST のみを提供しています。

Cisco IOS XR ソフトウェアでは、PVSTAG や MSTAG などのアクセス ゲートウェイ バージョンのプロトコルもサポートしています。これらは (一般的に VPLS と共に) 特定のトポロジで使用されるスタティックな限定されたバージョンのプロトコルであり、「[MSTAG](#)」の項および「[PVSTAG](#)」の項で説明します。Cisco IOS XR ソフトウェアでは、複数のスイッチを含むトポロジで完全なスパニング ツリーの実装が必要な場合は、MST が唯一のオプションです。

各ルータには 2 つのサブインターフェイスが設定され、ブリッジドメインに追加されています。

router1 の設定は次のとおりです。

```
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface GigabitEthernet0/0/0/1.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!
interface TenGigE0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface TenGigE0/0/0/1.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!
l2vpn
bridge group customer1
bridge-domain finance
interface TenGigE0/0/0/1.3
!
interface GigabitEthernet0/0/0/1.3
!
!
bridge-domain engineering
interface TenGigE0/0/0/1.2
!
interface GigabitEthernet0/0/0/1.2
!
!
!
!
```

MST はメイン インターフェイスで設定します。この例では、VLAN 2 はインスタンス 1 に割り当てられ、他のすべての VLAN はデフォルトのインスタンス 0 のままです（より現実的な設定では、VLAN をインスタンス間に均等に分配します）。

STP ネットワーク内のルートブリッジの選択は、各デバイスの設定されたプライオリティおよび組み込みブリッジ ID によって決まります。プライオリティが最低であるか、または等しく最低のプライオリティであるが最小ブリッジ ID を持つデバイスが、ルートブリッジとして選択されます。この例では、インスタンス 0 について、router3 に router1 より低いプライオリティが設定されているため、router3 がインスタンス 0 のルートになります。インスタンス 1 については、router1 が router3 より低いプライオリティを持つため、router1 がインスタンス 1 のルートになります。

router1 の設定を次に示します。

```
spanning-tree mst customer1
name customer1
revision 1
instance 0
priority 28672
!
instance 1
vlan-ids 2
priority 24576
!
interface TenGigE0/0/0/1
!
```

```
interface GigabitEthernet0/0/0/1
```

```
!  
!
```

router3 の設定を次に示します。

```
spanning-tree mode mst  
spanning-tree extend system-id  
!  
spanning-tree mst configuration  
name customer1  
revision 1  
instance 1 vlan 2  
!
```

```
spanning-tree mst 0 priority 24576  
spanning-tree mst 1 priority 28672
```

名前、リビジョン、および VLAN とインスタンスのマッピングは、すべてのスイッチで同じにする必要があります。

次に、router1 でスパニング ツリーの状態を確認します。

```
RP/0/RSP1/CPU0:router1#sh spanning-tree mst customer1  
Role: ROOT=Root, DSGN=Designated, ALT=Alternate, BKP=Backup, MSTR=Master  
State: FWD=Forwarding, LRN=Learning, BLK=Blocked, DLY=Bringup Delayed
```

```
Operating in dot1q mode
```

```
MSTI 0 (CIST):
```

```
VLANS Mapped: 1,3-4094
```

```
CIST Root Priority 24576  
Address 001d.4603.1f00  
Ext Cost 0
```

```
Root ID Priority 24576  
Address 001d.4603.1f00  
Int Cost 20000  
Max Age 20 sec, Forward Delay 15 sec
```

```
Bridge ID Priority 28672 (priority 28672 sys-id-ext 0)  
Address 4055.3912.f1e6  
Max Age 20 sec, Forward Delay 15 sec  
Max Hops 20, Transmit Hold count 6
```

```
Interface Port ID Role State Designated Port ID  
Pri.Nbr Cost Bridge ID Pri.Nbr  
-----  
Gi0/0/0/1 128.2 20000 ROOT FWD 24576 001d.4603.1f00 128.1  
Te0/0/0/1 128.1 2000 DSGN FWD 28672 4055.3912.f1e6 128.1
```

```
MSTI 1:
```

```
VLANS Mapped: 2
```

```
Root ID Priority 24576  
Address 4055.3912.f1e6  
This bridge is the root  
Int Cost 0
```



Max Age 20 sec, Forward Delay 15 sec

Bridge ID Priority 24576 (priority 24576 sys-id-ext 0)  
Address 4055.3912.f1e6  
Max Age 20 sec, Forward Delay 15 sec  
Max Hops 20, Transmit Hold count 6

```
Interface Port ID Role State Designated Port ID
Pri.Nbr Cost Bridge ID Pri.Nbr
-----
Gi0/0/0/1 128.2 20000 DSGN FWD 24576 4055.3912.f1e6 128.2
Te0/0/0/1 128.1 2000 DSGN FWD 24576 4055.3912.f1e6 128.1
```

router3 がインスタンス 0 のルートであるため、router1 は router3 へのルート ポートを Gi0/0/0/1 に持ちます。router1 はインスタンス 1 のルートであるため、router1 はすべてのインターフェイスにおいてこのインスタンスの代表ブリッジです。

router2、はインスタンス 0 について Te0/1/0/0 でブロックされています。

```
RP/0/RSP1/CPU0:router2#sh spanning-tree mst customer1
Role: ROOT=Root, DSGN=Designated, ALT=Alternate, BKP=Backup, MSTR=Master
State: FWD=Forwarding, LRN=Learning, BLK=Blocked, DLY=Bringup Delayed
```

Operating in dot1q mode

MSTI 0 (CIST):

VLANS Mapped: 1,3-4094

CIST Root Priority 24576  
Address 001d.4603.1f00  
Ext Cost 0

Root ID Priority 24576  
Address 001d.4603.1f00  
Int Cost 20000  
Max Age 20 sec, Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)  
Address f025.72a7.b13e  
Max Age 20 sec, Forward Delay 15 sec  
Max Hops 20, Transmit Hold count 6

```
Interface Port ID Role State Designated Port ID
Pri.Nbr Cost Bridge ID Pri.Nbr
-----
Gi0/0/0/1 128.2 20000 ROOT FWD 24576 001d.4603.1f00 128.2
Te0/1/0/0 128.1 2000 ALT BLK 28672 4055.3912.f1e6 128.1
```

MSTI 1:

VLANS Mapped: 2

Root ID Priority 24576  
Address 4055.3912.f1e6  
Int Cost 2000  
Max Age 20 sec, Forward Delay 15 sec

```
Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address f025.72a7.b13e
Max Age 20 sec, Forward Delay 15 sec
Max Hops 20, Transmit Hold count 6
```

```
Interface Port ID Role State Designated Port ID
Pri.Nbr Cost Bridge ID Pri.Nbr
-----
Gi0/0/0/1 128.2 20000 DSGN FWD 32768 f025.72a7.b13e 128.2
Te0/1/0/0 128.1 2000 ROOT FWD 24576 4055.3912.f1e6 128.1
RP/0/RSP1/CPU0:router2#
```

Te0/1/0/0.2 は転送を行っていますが、Te0/1/0/0.3 はブロックされています。STP Blocked の値が 0x0 のときは、この条件は false であり、インターフェイスは転送を行っています。STP Blocked の値が 0x1 のときは、この条件は true であり、インターフェイスはブロックされていません。

この確認や、ネットワークプロセッサにあるインターフェイス データを表示するためには、**show uidb data** コマンドを使用します。

```
RP/0/RSP1/CPU0:router2#sh uidb data location 0/1/CPU0 TenGigE0/1/0/0.2
ingress | i Blocked
STP Blocked 0x0
RP/0/RSP1/CPU0:router2#sh uidb data location 0/1/CPU0 TenGigE0/1/0/0.3
ingress | i Blocked
STP Blocked 0x1
```

## 4.3 BVI

ブリッジドメインの設定によって L2 ドメインが作成されます。この L2 ドメインから外に出るには、ブリッジドメイン内のホストと外の世界の間でルーティングを行う L3 ルータを接続します。[前の図](#)では、host1 は router4 または router5 を使用して、ローカル サブネットから抜け出してインターネットに到達することができます。

ブリッジドメインが設定されている router1 および router2 は、IPv4 および IPv6 トラフィックをルーティング可能な ASR 9000 ルータです。このため、これら 2 台のルータは、ブリッジドメインから IP トラフィックを取得し、L3 ルータでリレーすることなく自分でインターネットにルーティングできます。これを行うためには BVI を設定する必要があります。BVI は、ブリッジドメインと相互にパケットのルーティングを行うためにブリッジドメインに接続される L3 インターフェイスです。

これが論理的にどのように見えるかを次に示します。

次に設定例を示します。

```
RP/0/RSP1/CPU0:router1#sh run int bvi 2
interface BVI2
ipv4 address 192.168.2.1 255.255.255.0
!
```

```
RP/0/RSP1/CPU0:router1#sh run int bvi 3
interface BVI3
ipv4 address 192.168.3.1 255.255.255.0
!
```

```
RP/0/RSP1/CPU0:router1#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface TenGigE0/0/0/1.3
!
interface GigabitEthernet0/0/0/1.3
!
routed interface BVI3
!
bridge-domain engineering
interface TenGigE0/0/0/1.2
!
interface GigabitEthernet0/0/0/1.2
!
routed interface BVI2
!
!
!
RP/0/RSP1/CPU0:router1#sh run int gig 0/0/0/1.2
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
```

BVI はタグなし L3 インターフェイスであるため、ブリッジドメインの AC で受信したパケットを BVI で処理するためには、すべての着信タグをポップするように AC を設定する必要があります。この設定を行わない場合、BVI はタグを理解できずにパケットをドロップします。BVI 上で dot1q サブインターフェイスを設定する方法はないため、[前の例](#)の Gi0/0/0/1.2 で行ったように、AC の入力タグをポップする必要があります。

BVI インターフェイスは仮想インターフェイスであるため、有効にできる機能にはいくつかの制限があります。これらの制限については、「[Cisco ASR 9000 シリーズ ルータでの Integrated Routing and Bridging の設定](#)」の「[IRB の設定に関する制約事項](#)」に記載されています。次の機能は、ASR 9000 の BVI インターフェイスではサポートされていません。

- アクセスコントロール リスト ( ACL )。ただし、L2 ACL をブリッジドメインの各 L2 ポートで設定できます。
- IP Fast Reroute ( FRR )
- NetFlow
- MoFRR ( マルチキャスト専用高速再ルーティング )
- MPLS ラベルスイッチング
- mVPNv4
- Quality of Service ( QoS )
- トラフィック ミラーリング
- BVI のアンナンバード インターフェイス
- ビデオ モニタリング ( Vidmon )

BVI を Virtual Routing and Forwarding ( VRF ) の設定に含めて、BVI で受信したトラフィックが MPLS 上で転送されるようにできますが、*per-vrf label-allocation-mode* を使用する必要があります。

上記の制限された機能のいずれかが必要な場合、BVI は使用できません。他の解決策としては、ルータの 2 つのポート間で外部ループバック ケーブルを使用して、1 つのポートをブリッジドメインにし、もう 1 つのポートをすべての機能が設定可能な通常のルーテッド インターフェイスとして設定します。

## 4.4 VPLS

### 4.4.1 概要

VPLS は、複数サイトのブリッジドメインを MPLS PW を通じて 1 つの大きなブリッジドメインに結合する機能を提供します。トラフィックは L2VPN PE 間のフル メッシュの MPLS PW 上で透過的にカプセル化されるため、異なるサイトのホストが同じ L2 セグメントに直接接続されているように見えます。

各ホストが他のすべてのホストからのトラフィックを確実に受信できるようにするためには、フル メッシュの PW が必要になります。結果として、L2VPN PE は、VPLS PW で受信したフレームを他の VPLS PW に転送しません。転送によりループが発生する恐れがあるため、それぞれの PE がトラフィックを直接受信でき、PW 間でトラフィックを転送する必要がなくなるように、フル メッシュの PW を設ける必要があります。これは、スプリット ホライズン ルールと呼ばれています。

ルータは MAC ラーニングを実行しています。MAC アドレスが MAC アドレステーブルにある場合、その宛先 MAC アドレスのフレームのみを、PW を介してこの MAC アドレスの学習元である L2VPN PE へ転送します。こうすることで、コアでの不要なトラフィックの重複を回避できます。ブロードキャストとマルチキャストは、すべてのホストで確実に受信されるようにするために、すべての PW でフラッディングされます。受信者またはマルチキャスト ルータが存在する PE にのみマルチキャスト フレームを送信できる、IGMP スヌーピングのような機能が役に立ちます。これによってコアのトラフィック量を削減できますが、そのグループに関係がある場合、同一パケットの複数のコピーを各 PE に送信する必要があります。

フル メッシュの PW は、仮想転送インスタンス (VFI) の下で設定する必要があります。

```
RP/0/RSP0/CPU0:router1#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/1/0/3.3
!
vfi customer1-finance
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
vfi customer1-engineering
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
```

!  
!  
!

VFIで設定するPWは、コア内のフルメッシュ構造のPWです。あるPWで受信したフレームが別のPWに転送されないようにするために、これらのPWは同じスプリットホライズングループ(SHG)にします。

アクセスPWを設定することができますが、これはACの一種と見なされるので、VFIの下では設定しません。詳細については、該当する項を参照してください。

router2、router3、router4の設定はよく似ており、どのルータでも他の3台のルータがネイバーとしてVFIの下で設定されています。

```
RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain bd-name engineering detail
```

```
Legend: pp = Partially Programmed.
```

```
Bridge group: customer1, bridge-domain: engineering, id: 5, 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 down: 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 profile: none
```

```
Bridge MTU: 1500
```

```
MIB cvplsConfigIndex: 6
```

```
Filter MAC addresses:
```

```
Create time: 28/05/2013 17:17:03 (23:06:02 ago)
```

```
No status change since creation
```

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

```
List of ACs:
```

```
AC: GigabitEthernet0/1/0/3.2, state is up H-VPLS
```

```
Type VLAN; Num Ranges: 1
```

```
VLAN ranges: [2, 2]
```

```
MTU 1500; XC ID 0xc40003; 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 profile: none
```

```
Storm Control: disabled
```

```
Static MAC addresses:
```

Statistics:

packets: received 234039, sent 7824

bytes: received 16979396, sent 584608

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 customer1-engineering (up)

PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )

PW class not set, XC ID 0xc0000009

Encapsulation MPLS, protocol LDP

Source address 10.0.0.11

PW type Ethernet, control word disabled, interworking none

PW backup disable delay 0 sec

Sequencing not set

PW Status TLV in use

MPLS Local Remote

-----  
Label 16049 16042

Group ID 0x5 0x1

Interface customer1-engineering customer1-engineering

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: 3221225481

Create time: 29/05/2013 15:36:17 (00:46:49 ago)

Last time status changed: 29/05/2013 15:57:36 (00:25:29 ago)

MAC withdraw message: send 0 receive 0

Static MAC addresses:

Statistics:

packets: received 555, sent 285

bytes: received 36308, sent 23064

DHCPv4 snooping: disabled

IGMP Snooping profile: none

PW: neighbor 10.0.0.13, PW ID 2, state is up ( established )

PW class not set, XC ID 0xc000000a

Encapsulation MPLS, protocol LDP

Source address 10.0.0.11

PW type Ethernet, control word disabled, interworking none

PW backup disable delay 0 sec

Sequencing not set

PW Status TLV in use

MPLS Local Remote

-----  
Label 16050 16040

Group ID 0x5 0x3

Interface customer1-engineering customer1-engineering

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: 29/05/2013 15:36:17 (00:46:49 ago)
Last time status changed: 29/05/2013 16:00:56 (00:22:09 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 184, sent 158
bytes: received 12198, sent 14144
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
PW class not set, XC ID 0xc000000b
Encapsulation MPLS, protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set
```

```
PW Status TLV in use
MPLS Local Remote
```

```
-----
Label 16051 289974
Group ID 0x5 0x6
Interface customer1-engineering customer1-engineering
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: 3221225483
Create time: 29/05/2013 15:36:17 (00:46:49 ago)
Last time status changed: 29/05/2013 16:02:38 (00:20:27 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 137
bytes: received 0, sent 12064
DHCPv4 snooping: disabled
IGMP Snooping profile: none
VFI Statistics:
drops: illegal VLAN 0, illegal length 0
```

10.0.0.12 への PW のローカル ラベルは 16049 であり、イーサネット フレームがラベル 16049 で受信されたことを意味します。最後から 2 番目の MPLS ホップが IGP ラベルをポップするため、スイッチングの判断はこの MPLS ラベルに基づいて行われます。明示的なヌル ラベルがまだ含まれている可能性があります、スイッチングの判断は PW ラベルに基づいて行われます。

```
RP/0/RSP0/CPU0:router1#sh mpls forwarding labels 16049
Local Outgoing Prefix Outgoing Next Hop Bytes
```

```
Label Label or ID Interface Switched
```

```
-----  
16049 Pop PW(10.0.0.12:2) BD=5 point2point 58226
```

ラベルに対する **show mpls forwarding labels** コマンドによって、宛先 MAC アドレスや、パケットを受信した PW ( ネイバーおよび pw-id ) を見つけるために使用できるブリッジドメイン番号が表示されます。見つけた後で、そのネイバーを指すエントリを MAC アドレステーブルに作成できます。

```
RP/0/RSP0/CPU0:router1#sh l2vpn forwarding bridge-domain customer1:  
engineering mac-address location 0/1/CPU0  
To Resynchronize MAC table from the Network Processors, use the command...  
l2vpn resynchronize forwarding mac-address-table location
```

```
Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
```

```
-----  
0019.552b.b5c3 dynamic Gi0/1/0/3.2 0/1/CPU0 0d 0h 0m 0s N/A  
0024.985e.6a01 dynamic (10.0.0.12, 2) 0/1/CPU0 0d 0h 0m 0s N/A  
0024.985e.6a42 dynamic (10.0.0.12, 2) 0/1/CPU0 0d 0h 0m 0s N/A  
001d.4603.1f42 dynamic (10.0.0.13, 2) 0/1/CPU0 0d 0h 0m 0s N/A
```

#### 4.4.2 PW のタイプと転送されるタグ

VPLS PW は、デフォルトではタイプ 5 ( イーサネット ) PW としてネゴシエートされます。VLAN タグ操作 ( **rewrite** コマンドが設定されている場合 ) の後で、AC に入力されるものすべてが PW に送信されます。

LDP シグナリング対応の Cisco IOS XR ソフトウェア リリース 4.1.0 および BGP を備えたリリース 4.3.1 では、ネイバーの下で pw-class を設定し、pw-class の下で **transport mode vlan passthrough** を設定できます。このようにすると、仮想接続 ( VC ) タイプ 4 ( イーサネット VLAN ) PW をネゴシエートします。このタイプでは、**rewrite** コマンドが設定されている場合、VLAN タグ操作の後で AC から送信されるものすべてが転送されます。

VC タイプ 4 PW がある場合、フレームには dot1q タグが必要なため、EFP の VLAN タグ操作では少なくとも 1 つの VLAN タグがフレームに残るようにします。 **transport mode vlan passthrough** モードを使用する場合、フレームにダミー タグ 0 は追加されません。

同じ VFI でのタイプ 4 とタイプ 5 の PW の混在はサポートされていません。すべての PW は同じタイプにする必要があります。

```
RP/0/RSP0/CPU0:router1#sh run l2vpn bridge group customer1 bridge-domain  
engineering  
l2vpn  
bridge group customer1  
bridge-domain engineering  
interface GigabitEthernet0/1/0/3.2  
!  
vfi customer1-engineering  
neighbor 10.0.0.12 pw-id 2  
pw-class VC4-PT  
!  
neighbor 10.0.0.13 pw-id 2  
pw-class VC4-PT  
!  
neighbor 10.0.0.14 pw-id 2  
pw-class VC4-PT  
!  
!  
!
```



```

!
!
RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain bd-name engineering detail |
i "PW:|PW type"
MAC withdraw for Access PW: enabled
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )
PW type Ethernet VLAN, control word disabled, interworking none
PW type Ethernet VLAN Ethernet VLAN
PW: neighbor 10.0.0.13, PW ID 2, state is up ( established )
PW type Ethernet VLAN, control word disabled, interworking none
PW type Ethernet VLAN Ethernet VLAN
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
PW type Ethernet VLAN, control word disabled, interworking none
PW type Ethernet VLAN Ethernet VLAN

```

### 4.4.3 自動検出とシグナリング

前の例では、VFI の下のすべてのネイバーの手動設定を前提にしていました。ネイバーとの PW のシグナリングに MPLS LDP が使用されていました。[前の例](#)

ネットワークに新しい VPLS PE を追加するときは、それぞれのローカルブリッジドメインで、既存のすべての PE への PW が存在するように PE を設定します。すべての PE をフルメッシュ構造にする必要があるため、新しい PE への PW があるように既存のすべての PE を再設定する必要があります。PE やブリッジドメインの数が増えるにつれて、これは運用上の課題になる可能性があります。

解決策の 1 つは、BGP を使用して PE に他の PE を自動的に検出させる方法です。IBGP にはフルメッシュの要件もありますが、ルートリフレクタを使用することで対応できます。つまり、通常、新しい PE は少数のルートリフレクタとのピアに設定し、他のすべての PE が更新を受信し、新しい PE は他の PE から更新を受信します。

BGP を使用して他の PE を検出するには、各 PE で *vpls-vpws address-family* を設定し、参加させるブリッジドメインを BGP でアドバタイズします。同じブリッジドメインに属している他の PE を検出すると、PW がそれぞれに対して確立されます。この検出に使用されるプロトコルは BGP です。

自動検出された PE に PW のシグナリングを行う 2 つの方法があります。BGP と LDP です。次の例では、[前のトポロジ](#)を、BGP シグナリングおよび LDP シグナリングを使用して BGP 自動検出を行うように変換します。

#### 4.4.3.1 BGP 自動検出と BGP シグナリング

router bgp とネイバー ( 他の PE またはルートリフレクタ ) の下で、**address-family l2vpn vpls-vpws** を設定します。

```

router bgp 65000
address-family l2vpn vpls-vpws
!
neighbor-group IOX-LAB-RR
address-family l2vpn vpls-vpws
!
neighbor 10.0.0.3
use neighbor-group IOX-LAB-RR
!

```

```
neighbor 10.0.0.10
use neighbor-group IOX-LAB-RR
!
```

新しいアドレスファミリはネイバーとアクティブになりますが、どの PE も、ブリッジドメインに参加していることをまだアドバタイズしていません。

```
RP/0/RSP0/CPU0:router1#sh bgp neighbor 10.0.0.3 | i Address family L2VPN
Address family L2VPN VPLS: advertised and received
```

```
P/0/RSP0/CPU0:router1#sh bgp l2vpn vpls summary
BGP router identifier 10.0.0.11, local AS number 65000
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0 RD version: 3890838096
BGP main routing table version 77
BGP scan interval 60 secs
```

BGP is operating in STANDALONE mode.

```
Process RcvTblVer bRIB/RIB LabelVer ImportVer SendTblVer StandbyVer
Speaker 77 77 77 77 77 77
```

```
Neighbor Spk AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down St/PfxRcd
10.0.0.3 0 65000 252950 53252 77 0 0 1w0d 0
10.0.0.10 0 65000 941101 47439 77 0 0 00:10:18 0
```

L2VPN ブリッジドメイン設定モードで、**autodiscovery bgp** と **signaling-protocol bgp** を設定します。router1 の設定は次のとおりです。

```
RP/0/RSP0/CPU0:router1#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/1/0/3.3
!
vfi customer1-finance
vpn-id 3
autodiscovery bgp
rd auto
route-target 0.0.0.1:3
signaling-protocol bgp
ve-id 11
!
!
!
!
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
vfi customer1-engineering
vpn-id 2
autodiscovery bgp
rd auto
route-target 0.0.0.1:2
signaling-protocol bgp
ve-id 11
!
!
!
!
!
```

router2 の設定は次のとおりです。

```
RP/0/RSP1/CPU0:router2#sh run l2vpn bridge group customer1
Thu May 30 15:25:55.638 CEST
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/0/0/1.3
!
vfi customer1-finance
vpn-id 3
autodiscovery bgp
rd auto
route-target 0.0.0.1:3
signaling-protocol bgp
ve-id 13
!
!
!
!
bridge-domain engineering
interface GigabitEthernet0/0/0/1.2
!
vfi customer1-engineering
vpn-id 2
autodiscovery bgp
rd auto
route-target 0.0.0.1:2
signaling-protocol bgp
ve-id 13
!
!
!
!
!
```

vpn-id と route-target は、それぞれのブリッジドメインの他の PE と同じですが、各 PE は一意の仮想エッジ識別子 ( VE-ID ) を持ちます。各 PE は BGP を通じて VPN の他の PE を検出し、BGP を使用して PW をシグナリングします。この結果、フルメッシュの PW になります。

```
RP/0/RSP0/CPU0:router1#sh bgp l2vpn vpls summary
BGP router identifier 10.0.0.11, local AS number 65000
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0x0 RD version: 3890838096
BGP main routing table version 103
BGP scan interval 60 secs
```

BGP is operating in STANDALONE mode.

```
Process RcvTblVer bRIB/RIB LabelVer ImportVer SendTblVer StandbyVer
Speaker 103 103 103 103 103 103
```

```
Neighbor Spk AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down St/PfxRcd
10.0.0.3 0 65000 254944 53346 103 0 0 1w0d 6
10.0.0.10 0 65000 944859 47532 103 0 0 01:40:22 6
```

```
RP/0/RSP0/CPU0:router1#sh bgp l2vpn vpls
BGP router identifier 10.0.0.11, local AS number 65000
BGP generic scan interval 60 secs
BGP table state: Active
```

Table ID: 0x0 RD version: 3890838096  
BGP main routing table version 103  
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, \* valid, > best  
i - internal, r RIB-failure, S stale  
Origin codes: i - IGP, e - EGP, ? - incomplete  
Network Next Hop Rcvd Label Local Label  
Route Distinguisher: 10.0.0.11:32769 (default for vrf customer1:finance)  
\*> 11:10/32 0.0.0.0 nolabel 16060  
\*>i12:10/32 10.0.0.12 16060 nolabel  
\*>i13:10/32 10.0.0.13 16060 nolabel  
\*>i14:10/32 10.0.0.14 289959 nolabel  
Route Distinguisher: 10.0.0.11:32770 (default for vrf customer1:engineering)  
\*> 11:10/32 0.0.0.0 nolabel 16075  
\*>i12:10/32 10.0.0.12 16075 nolabel  
\*>i13:10/32 10.0.0.13 16075 nolabel  
\*>i14:10/32 10.0.0.14 289944 nolabel  
Route Distinguisher: 10.0.0.12:32768  
\*>i12:10/32 10.0.0.12 16060 nolabel  
\* i 10.0.0.12 16060 nolabel  
Route Distinguisher: 10.0.0.12:32769  
\*>i12:10/32 10.0.0.12 16075 nolabel  
\* i 10.0.0.12 16075 nolabel  
Route Distinguisher: 10.0.0.13:32769  
\*>i13:10/32 10.0.0.13 16060 nolabel  
\* i 10.0.0.13 16060 nolabel  
Route Distinguisher: 10.0.0.13:32770  
\*>i13:10/32 10.0.0.13 16075 nolabel  
\* i 10.0.0.13 16075 nolabel  
Route Distinguisher: 10.0.0.14:32768  
\*>i14:10/32 10.0.0.14 289959 nolabel  
\* i 10.0.0.14 289959 nolabel  
Route Distinguisher: 10.0.0.14:32769  
\*>i14:10/32 10.0.0.14 289944 nolabel  
\* i 10.0.0.14 289944 nolabel

Processed 14 prefixes, 20 paths

次に示すのは、router1 で表示される router3 ( 10.0.0.13 ) によってアドバタイズされたプレフィックスです。プレフィックスは、10.0.0.3 と 10.0.0.10 の 2 つのルートリフレクタを介して受信されています。

```
RP/0/RSP0/CPU0:router1#sh bgp l2vpn vpls rd 10.0.0.13:32770 13:10/32
BGP routing table entry for 13:10/32, Route Distinguisher: 10.0.0.13:32770
Versions:
Process bRIB/RIB SendTblVer
Speaker 92 92
Last Modified: May 30 15:10:44.100 for 01:23:38
Paths: (2 available, best #1)
Not advertised to any peer
Path #1: Received by speaker 0
Not advertised to any peer
Local
10.0.0.13 (metric 5) from 10.0.0.3 (10.0.0.13)
Received Label 16075
Origin IGP, localpref 100, valid, internal, best, group-best,
import-candidate, not-in-vrf, import suspect
Received Path ID 0, Local Path ID 1, version 92
Extended community: RT:0.0.0.1:2 L2VPN:19:0:1500
Originator: 10.0.0.13, Cluster list: 10.0.0.3
Block Size:10
Path #2: Received by speaker 0
Not advertised to any peer
```

```

Local
10.0.0.13 (metric 5) from 10.0.0.10 (10.0.0.13)
Received Label 16075
Origin IGP, localpref 100, valid, internal, not-in-vrf, import suspect
Received Path ID 0, Local Path ID 0, version 0
Extended community: RT:0.0.0.1:2 L2VPN:19:0:1500
Originator: 10.0.0.13, Cluster list: 10.0.0.10
Block Size:10
RP/0/RSP0/CPU0:router1#sh bgp l2vpn vpls rd 10.0.0.13:32769 13:10/32
BGP routing table entry for 13:10/32, Route Distinguisher: 10.0.0.13:32769
Versions:
Process bRIB/RIB SendTblVer
Speaker 93 93
Last Modified: May 30 15:10:44.100 for 01:25:02
Paths: (2 available, best #1)
Not advertised to any peer
Path #1: Received by speaker 0
Not advertised to any peer
Local
10.0.0.13 (metric 5) from 10.0.0.3 (10.0.0.13)
Received Label 16060
Origin IGP, localpref 100, valid, internal, best, group-best,
import-candidate, not-in-vrf, import suspect
Received Path ID 0, Local Path ID 1, version 93
Extended community: RT:0.0.0.1:3 L2VPN:19:0:1500
Originator: 10.0.0.13, Cluster list: 10.0.0.3
Block Size:10
Path #2: Received by speaker 0
Not advertised to any peer
Local
10.0.0.13 (metric 5) from 10.0.0.10 (10.0.0.13)
Received Label 16060
Origin IGP, localpref 100, valid, internal, not-in-vrf, import suspect
Received Path ID 0, Local Path ID 0, version 0
Extended community: RT:0.0.0.1:3 L2VPN:19:0:1500
Originator: 10.0.0.13, Cluster list: 10.0.0.10
Block Size:10

```

**router1 は複数の PW を確立しています。**

```
RP/0/RSP0/CPU0:router1#sh l2vpn discovery bridge-domain
```

```

Service Type: VPLS, Connected
List of VPNs (2 VPNs):
Bridge group: customer1, bridge-domain: finance, id: 3, signaling
protocol: BGP
List of Local Edges (1 Edges):
Local Edge ID: 11, Label Blocks (1 Blocks)
Label base Offset Size Time Created
-----
16060 10 10 05/30/2013 15:07:39
List of Remote Edges (3 Edges):
Remote Edge ID: 12, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created
-----
16060 10 10 10.0.0.12 05/30/2013 15:09:53
Remote Edge ID: 13, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created
-----
16060 10 10 10.0.0.13 05/30/2013 15:10:43
Remote Edge ID: 14, NLRIs (1 NLRIs)
Label base Offset Size Peer ID Time Created
-----
289959 10 10 10.0.0.14 05/30/2013 15:11:22

```

Bridge group: customer1, bridge-domain: engineering, id: 5, signaling protocol: BGP

List of Local Edges (1 Edges):

Local Edge ID: 11, Label Blocks (1 Blocks)

Label base Offset Size Time Created

-----  
16075 10 10 05/30/2013 15:08:54

List of Remote Edges (3 Edges):

Remote Edge ID: 12, NLRIs (1 NLRIs)

Label base Offset Size Peer ID Time Created

-----  
16075 10 10 10.0.0.12 05/30/2013 15:09:53

Remote Edge ID: 13, NLRIs (1 NLRIs)

Label base Offset Size Peer ID Time Created

-----  
16075 10 10 10.0.0.13 05/30/2013 15:10:43

Remote Edge ID: 14, NLRIs (1 NLRIs)

Label base Offset Size Peer ID Time Created

-----  
289944 10 10 10.0.0.14 05/30/2013 15:11:22

RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain autodiscovery bgp

Legend: pp = Partially Programmed.

Bridge group: customer1, bridge-domain: finance, id: 3, 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 VFIs:

VFI customer1-finance (up)

Neighbor 10.0.0.12 pw-id 3, state: up, Static MAC addresses: 0

Neighbor 10.0.0.13 pw-id 3, state: up, Static MAC addresses: 0

Neighbor 10.0.0.14 pw-id 3, state: up, Static MAC addresses: 0

Bridge group: customer1, bridge-domain: engineering, id: 5, 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 VFIs:

VFI customer1-engineering (up)

Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0

Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0

Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0

RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain group customer1

Legend: pp = Partially Programmed.

Bridge group: customer1, bridge-domain: finance, id: 3, 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:

Gi0/1/0/3.3, state: up, Static MAC addresses: 0

List of Access PWs:

List of VFIs:

VFI customer1-finance (up)

Neighbor 10.0.0.12 pw-id 3, state: up, Static MAC addresses: 0

Neighbor 10.0.0.13 pw-id 3, state: up, Static MAC addresses: 0

Neighbor 10.0.0.14 pw-id 3, state: up, Static MAC addresses: 0

Bridge group: customer1, bridge-domain: engineering, id: 5, 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:

Gi0/1/0/3.2, state: up, Static MAC addresses: 0

List of Access PWs:

List of VFIs:

VFI customer1-engineering (up)

Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0

Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0

Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0

RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain group customer1 detail

Legend: pp = Partially Programmed.

Bridge group: customer1, bridge-domain: finance, id: 3, 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 down: 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 profile: none

Bridge MTU: 1500

MIB cvplsConfigIndex: 4

Filter MAC addresses:

Create time: 29/05/2013 15:36:17 (1d01h ago)

No status change since creation

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

List of ACs:

AC: GigabitEthernet0/1/0/3.3, state is up

Type VLAN; Num Ranges: 1

VLAN ranges: [3, 3]

MTU 1500; XC ID 0xc40006; 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 profile: none

Storm Control: disabled

Static MAC addresses:

Statistics:

packets: received 10120, sent 43948

bytes: received 933682, sent 2989896

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 customer1-finance (up)  
VPN-ID: 3, Auto Discovery: BGP, state is Provisioned  
(Service Connected)  
Route Distinguisher: (auto) 10.0.0.11:32769  
Import Route Targets:  
0.0.0.1:3  
Export Route Targets:  
0.0.0.1:3  
Signaling protocol: BGP  
Local VE-ID: 11 , Advertised Local VE-ID : 11  
VE-Range: 10  
PW: neighbor 10.0.0.12, PW ID 3, state is up ( established )  
PW class not set, XC ID 0xc000000c  
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP  
Source address 10.0.0.11  
PW type VPLS, control word disabled, interworking none  
PW backup disable delay 0 sec  
Sequencing not set

MPLS Local Remote

-----  
Label 16062 16061  
MTU 1500 1500  
Control word disabled disabled  
PW type VPLS VPLS  
VE-ID 11 12  
-----

MIB cpwVcIndex: 3221225484  
Create time: 30/05/2013 15:09:52 (01:29:44 ago)  
Last time status changed: 30/05/2013 15:09:52 (01:29:44 ago)  
MAC withdraw message: send 0 receive 0  
Static MAC addresses:  
Statistics:  
packets: received 2679, sent 575  
bytes: received 171698, sent 51784  
DHCPv4 snooping: disabled  
IGMP Snooping profile: none  
PW: neighbor 10.0.0.13, PW ID 3, state is up ( established )  
PW class not set, XC ID 0xc000000e  
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP  
Source address 10.0.0.11  
PW type VPLS, control word disabled, interworking none  
PW backup disable delay 0 sec  
Sequencing not set

MPLS Local Remote

-----  
Label 16063 16061  
MTU 1500 1500  
Control word disabled disabled  
PW type VPLS VPLS  
VE-ID 11 13  
-----

MIB cpwVcIndex: 3221225486  
Create time: 30/05/2013 15:10:43 (01:28:54 ago)  
Last time status changed: 30/05/2013 15:10:43 (01:28:54 ago)  
MAC withdraw message: send 0 receive 0



Static MAC addresses:

Statistics:

packets: received 11, sent 574

bytes: received 1200, sent 51840

DHCPv4 snooping: disabled

IGMP Snooping profile: none

PW: neighbor 10.0.0.14, PW ID 3, state is up ( established )

PW class not set, XC ID 0xc0000010

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

Source address 10.0.0.11

PW type VPLS, control word disabled, interworking none

PW backup disable delay 0 sec

Sequencing not set

MPLS Local Remote

-----  
Label 16064 289960

MTU 1500 1500

Control word disabled disabled

PW type VPLS VPLS

VE-ID 11 14  
-----

MIB cpwVcIndex: 3221225488

Create time: 30/05/2013 15:11:22 (01:28:15 ago)

Last time status changed: 30/05/2013 15:11:22 (01:28:15 ago)

MAC withdraw message: send 0 receive 0

Static MAC addresses:

Statistics:

packets: received 0, sent 561

bytes: received 0, sent 50454

DHCPv4 snooping: disabled

IGMP Snooping profile: none

VFI Statistics:

drops: illegal VLAN 0, illegal length 0

Bridge group: customer1, bridge-domain: engineering, id: 5, 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 down: 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 profile: none

Bridge MTU: 1500

MIB cvplsConfigIndex: 6

Filter MAC addresses:

Create time: 28/05/2013 17:17:03 (1d23h ago)

No status change since creation

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

List of ACs:

AC: GigabitEthernet0/1/0/3.2, state is up

Type VLAN; Num Ranges: 1

VLAN ranges: [2, 2]

MTU 1500; XC ID 0xc40007; 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 profile: none  
Storm Control: disabled  
Static MAC addresses:  
Statistics:  
packets: received 243532, sent 51089  
bytes: received 17865888, sent 3528732  
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 customer1-engineering (up)  
VPN-ID: 2, Auto Discovery: BGP, state is Provisioned  
(Service Connected)  
Route Distinguisher: (auto) 10.0.0.11:32770  
Import Route Targets:  
0.0.0.1:2  
Export Route Targets:  
0.0.0.1:2  
Signaling protocol: BGP  
Local VE-ID: 11 , Advertised Local VE-ID : 11  
VE-Range: 10  
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )  
PW class not set, XC ID 0xc000000d  
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP  
Source address 10.0.0.11  
PW type VPLS, control word disabled, interworking none  
PW backup disable delay 0 sec  
Sequencing not set

MPLS Local Remote

-----  
Label 16077 16076  
MTU 1500 1500  
Control word disabled disabled  
PW type VPLS VPLS  
VE-ID 11 12  
-----

MIB cpwVcIndex: 3221225485  
Create time: 30/05/2013 15:09:52 (01:29:45 ago)  
Last time status changed: 30/05/2013 15:09:52 (01:29:45 ago)  
MAC withdraw message: send 0 receive 0  
Static MAC addresses:  
Statistics:  
packets: received 2677, sent 574  
bytes: received 171524, sent 51670

```
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.13, PW ID 2, state is up ( established )
PW class not set, XC ID 0xc000000f
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP
Source address 10.0.0.11
PW type VPLS, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set
```

MPLS Local Remote

```
-----
Label 16078 16076
MTU 1500 1500
Control word disabled disabled
PW type VPLS VPLS
VE-ID 11 13
-----
```

```
MIB cpwVcIndex: 3221225487
Create time: 30/05/2013 15:10:43 (01:28:54 ago)
Last time status changed: 30/05/2013 15:10:43 (01:28:54 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 17, sent 572
bytes: received 1560, sent 51636
DHCPv4 snooping: disabled
IGMP Snooping profile: none
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
PW class not set, XC ID 0xc0000011
Encapsulation MPLS, Auto-discovered (BGP), protocol BGP
Source address 10.0.0.11
PW type VPLS, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set
```

MPLS Local Remote

```
-----
Label 16079 289945
MTU 1500 1500
Control word disabled disabled
PW type VPLS VPLS
VE-ID 11 14
-----
```

```
MIB cpwVcIndex: 3221225489
Create time: 30/05/2013 15:11:22 (01:28:16 ago)
Last time status changed: 30/05/2013 15:11:22 (01:28:16 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 559
bytes: received 0, sent 50250
DHCPv4 snooping: disabled
IGMP Snooping profile: none
VFI Statistics:
drops: illegal VLAN 0, illegal length 0
```

#### 4.4.3.2 BGP 自動検出と LDP シグナリング

**address-family l2vpn vpls-vpws** コマンドによる BGP の設定は、BGP シグナリングとまったく同じです。LDP シグナリングを使用するため、L2VPN の設定は **signaling-protocol ldp** コマンドに変更されています。

次の同じ設定が 4 つすべての PE で使用されます。

```
router bgp 65000
address-family l2vpn vpls-vpws
!
neighbor-group IOX-LAB-RR
address-family l2vpn vpls-vpws
!
neighbor 10.0.0.3
use neighbor-group IOX-LAB-RR
!
neighbor 10.0.0.10
use neighbor-group IOX-LAB-RR
!
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/1/0/3.3
!
vfi customer1-finance
vpn-id 3
autodiscovery bgp
rd auto
route-target 0.0.0.1:3
signaling-protocol ldp
vpls-id 65000:3
!
!
!
!
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
vfi customer1-engineering
vpn-id 2
autodiscovery bgp
rd auto
route-target 0.0.0.1:2
signaling-protocol ldp
vpls-id 65000:2
!
!
!
!
!
```

vpls-id は、BGP 自律システム ( AS ) の番号と vpn-id で構成されています。

router1 の次の 3 つの show コマンドでは、検出された PE との間で PW が確立されたことがわかります。

```
RP/0/RSP0/CPU0:router1#sh l2vpn discovery
```

```
Service Type: VPLS, Connected
List of VPNs (2 VPNs):
Bridge group: customer1, bridge-domain: finance, id: 3,
signaling protocol: LDP
VPLS-ID: 65000:3
Local L2 router id: 10.0.0.11
List of Remote NLRI (3 NLRIs):
Local Addr Remote Addr Remote L2 RID Time Created
-----
```

```
10.0.0.11 10.0.0.12 10.0.0.12 05/30/2013 17:10:18
10.0.0.11 10.0.0.13 10.0.0.13 05/30/2013 17:10:18
10.0.0.11 10.0.0.14 10.0.0.14 05/30/2013 17:11:46
```

```
Bridge group: customer1, bridge-domain: engineering, id: 5,
signaling protocol: LDP
VPLS-ID: 65000:2
```

```
Local L2 router id: 10.0.0.11
```

```
List of Remote NLRI (3 NLRIs):
```

```
Local Addr Remote Addr Remote L2 RID Time Created
```

```
-----
10.0.0.11 10.0.0.12 10.0.0.12 05/30/2013 17:10:18
10.0.0.11 10.0.0.13 10.0.0.13 05/30/2013 17:10:18
10.0.0.11 10.0.0.14 10.0.0.14 05/30/2013 17:11:46
```

```
RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain group customer1
```

```
Legend: pp = Partially Programmed.
```

```
Bridge group: customer1, bridge-domain: finance, id: 3, 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:
```

```
Gi0/1/0/3.3, state: up, Static MAC addresses: 0
```

```
List of Access PWs:
```

```
List of VFIs:
```

```
VFI customer1-finance (up)
```

```
Neighbor 10.0.0.12 pw-id 65000:3, state: up, Static MAC addresses: 0
```

```
Neighbor 10.0.0.13 pw-id 65000:3, state: up, Static MAC addresses: 0
```

```
Neighbor 10.0.0.14 pw-id 65000:3, state: up, Static MAC addresses: 0
```

```
Bridge group: customer1, bridge-domain: engineering, id: 5, 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:
```

```
Gi0/1/0/3.2, state: up, Static MAC addresses: 0
```

```
List of Access PWs:
```

```
List of VFIs:
```

```
VFI customer1-engineering (up)
```

```
Neighbor 10.0.0.12 pw-id 65000:2, state: up, Static MAC addresses: 0
```

```
Neighbor 10.0.0.13 pw-id 65000:2, state: up, Static MAC addresses: 0
```

```
Neighbor 10.0.0.14 pw-id 65000:2, state: up, Static MAC addresses: 0
```

```
RP/0/RSP0/CPU0:router1#sh l2vpn bridge-domain group customer1 det
```

```
Legend: pp = Partially Programmed.
```

```
Bridge group: customer1, bridge-domain: finance, id: 3, 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 down: 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 profile: none  
Bridge MTU: 1500  
MIB cvplsConfigIndex: 4  
Filter MAC addresses:  
Create time: 29/05/2013 15:36:17 (1d01h ago)  
No status change since creation  
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)  
List of ACs:  
AC: GigabitEthernet0/1/0/3.3, state is up  
Type VLAN; Num Ranges: 1  
VLAN ranges: [3, 3]  
MTU 1500; XC ID 0xc40006; 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 profile: none  
Storm Control: disabled  
Static MAC addresses:  
Statistics:  
packets: received 10362, sent 45038  
bytes: received 956240, sent 3064016  
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 customer1-finance (up)  
VPN-ID: 3, Auto Discovery: BGP, state is Provisioned  
(Service Connected)  
Route Distinguisher: (auto) 10.0.0.11:32769  
Import Route Targets:  
0.0.0.1:3  
Export Route Targets:  
0.0.0.1:3  
Signaling protocol: LDP  
AS Number: 65000  
VPLS-ID: 65000:3  
L2VPN Router ID: 10.0.0.11  
PW: neighbor 10.0.0.12, PW ID 65000:3, state is up ( established )  
PW class not set, XC ID 0xc0000003  
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP  
Source address 10.0.0.11  
PW type Ethernet, control word disabled, interworking none  
PW backup disable delay 0 sec  
Sequencing not set  
  
PW Status TLV in use  
MPLS Local Remote  
-----

Label 16006 16033  
BGP Peer ID 10.0.0.11 10.0.0.12  
LDP ID 10.0.0.11 10.0.0.12  
AII 10.0.0.11 10.0.0.12  
AGI 65000:3 65000:3  
Group ID 0x3 0x0  
Interface customer1-finance customer1-finance  
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: 3221225475  
Create time: 30/05/2013 17:10:18 (00:06:32 ago)  
Last time status changed: 30/05/2013 17:10:24 (00:06:25 ago)  
MAC withdraw message: send 0 receive 0  
Static MAC addresses:  
Statistics:  
packets: received 190, sent 40  
bytes: received 12160, sent 3600  
DHCPv4 snooping: disabled  
IGMP Snooping profile: none  
PW: neighbor 10.0.0.13, PW ID 65000:3, state is up ( established )  
PW class not set, XC ID 0xc0000004  
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP  
Source address 10.0.0.11  
PW type Ethernet, control word disabled, interworking none  
PW backup disable delay 0 sec  
Sequencing not set

PW Status TLV in use  
MPLS Local Remote

-----  
Label 16016 16020  
BGP Peer ID 10.0.0.11 10.0.0.13  
LDP ID 10.0.0.11 10.0.0.13  
AII 10.0.0.11 10.0.0.13  
AGI 65000:3 65000:3  
Group ID 0x3 0x4  
Interface customer1-finance customer1-finance  
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: 3221225476  
Create time: 30/05/2013 17:10:18 (00:06:32 ago)  
Last time status changed: 30/05/2013 17:10:27 (00:06:22 ago)  
MAC withdraw message: send 0 receive 0  
Static MAC addresses:  
Statistics:  
packets: received 0, sent 40

bytes: received 0, sent 3600  
DHCPv4 snooping: disabled  
IGMP Snooping profile: none  
PW: neighbor 10.0.0.14, PW ID 65000:3, state is up ( established )  
PW class not set, XC ID 0xc0000009  
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP  
Source address 10.0.0.11  
PW type Ethernet, control word disabled, interworking none  
PW backup disable delay 0 sec  
Sequencing not set

PW Status TLV in use

MPLS Local Remote

-----  
Label 16049 289970  
BGP Peer ID 10.0.0.11 10.0.0.14  
LDP ID 10.0.0.11 10.0.0.14  
AII 10.0.0.11 10.0.0.14  
AGI 65000:3 65000:3  
Group ID 0x3 0x4  
Interface customer1-finance customer1-finance  
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: 3221225481  
Create time: 30/05/2013 17:11:46 (00:05:04 ago)  
Last time status changed: 30/05/2013 17:11:51 (00:04:59 ago)  
MAC withdraw message: send 0 receive 0  
Static MAC addresses:  
Statistics:  
packets: received 0, sent 31  
bytes: received 0, sent 2790  
DHCPv4 snooping: disabled  
IGMP Snooping profile: none  
VFI Statistics:  
drops: illegal VLAN 0, illegal length 0  
Bridge group: customer1, bridge-domain: engineering, id: 5, 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 down: 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 profile: none



Bridge MTU: 1500  
MIB cvplsConfigIndex: 6  
Filter MAC addresses:  
Create time: 28/05/2013 17:17:03 (1d23h ago)  
No status change since creation  
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)  
List of ACs:  
AC: GigabitEthernet0/1/0/3.2, state is up  
Type VLAN; Num Ranges: 1  
VLAN ranges: [2, 2]  
MTU 1500; XC ID 0xc40007; 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 profile: none  
Storm Control: disabled  
Static MAC addresses:  
Statistics:  
packets: received 243774, sent 52179  
bytes: received 17888446, sent 3602852  
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 customer1-engineering (up)  
VPN-ID: 2, Auto Discovery: BGP, state is Provisioned (Service Connected)  
Route Distinguisher: (auto) 10.0.0.11:32770  
Import Route Targets:  
0.0.0.1:2  
Export Route Targets:  
0.0.0.1:2  
Signaling protocol: LDP  
AS Number: 65000  
VPLS-ID: 65000:2  
L2VPN Router ID: 10.0.0.11  
PW: neighbor 10.0.0.12, PW ID 65000:2, state is up ( established )  
PW class not set, XC ID 0xc0000005  
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP  
Source address 10.0.0.11  
PW type Ethernet, control word disabled, interworking none  
PW backup disable delay 0 sec  
Sequencing not set  
  
PW Status TLV in use  
MPLS Local Remote  
-----  
Label 16027 16042  
BGP Peer ID 10.0.0.11 10.0.0.12  
LDP ID 10.0.0.11 10.0.0.12

AII 10.0.0.11 10.0.0.12  
AGI 65000:2 65000:2  
Group ID 0x5 0x1  
Interface customer1-engineering customer1-engineering  
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: 0  
Create time: 30/05/2013 17:10:18 (00:06:33 ago)  
Last time status changed: 30/05/2013 17:10:24 (00:06:26 ago)  
MAC withdraw message: send 0 receive 0  
Static MAC addresses:  
Statistics:  
packets: received 190, sent 41  
bytes: received 12160, sent 3690  
DHCPv4 snooping: disabled  
IGMP Snooping profile: none  
PW: neighbor 10.0.0.13, PW ID 65000:2, state is up ( established )  
PW class not set, XC ID 0xc0000006  
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP  
Source address 10.0.0.11  
PW type Ethernet, control word disabled, interworking none  
PW backup disable delay 0 sec  
Sequencing not set

PW Status TLV in use  
MPLS Local Remote  
-----

Label 16043 16021  
BGP Peer ID 10.0.0.11 10.0.0.13  
LDP ID 10.0.0.11 10.0.0.13  
AII 10.0.0.11 10.0.0.13  
AGI 65000:2 65000:2  
Group ID 0x5 0x3  
Interface customer1-engineering customer1-engineering  
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: 0  
Create time: 30/05/2013 17:10:18 (00:06:33 ago)  
Last time status changed: 30/05/2013 17:10:27 (00:06:23 ago)  
MAC withdraw message: send 0 receive 0  
Static MAC addresses:  
Statistics:  
packets: received 0, sent 40  
bytes: received 0, sent 3600  
DHCPv4 snooping: disabled  
IGMP Snooping profile: none

```
PW: neighbor 10.0.0.14, PW ID 65000:2, state is up ( established )
PW class not set, XC ID 0xc000000a
Encapsulation MPLS, Auto-discovered (BGP), protocol LDP
Source address 10.0.0.11
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set
```

```
PW Status TLV in use
MPLS Local Remote
```

```
-----
Label 16050 289974
BGP Peer ID 10.0.0.11 10.0.0.14
LDP ID 10.0.0.11 10.0.0.14
AII 10.0.0.11 10.0.0.14
AGI 65000:2 65000:2
Group ID 0x5 0x6
Interface customer1-engineering customer1-engineering
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: 30/05/2013 17:11:46 (00:05:05 ago)
Last time status changed: 30/05/2013 17:11:51 (00:05:00 ago)
MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
packets: received 0, sent 31
bytes: received 0, sent 2790
DHCPv4 snooping: disabled
IGMP Snooping profile: none
VFI Statistics:
drops: illegal VLAN 0, illegal length 0
```

#### 4.4.4 MAC の消去と回収

VPLS の転送は、MAC アドレステーブルに基づいて行われます。このテーブルは、受信したフレームの送信元 MAC アドレスを学習することによって動的に構築されます。ブリッジドメイン内でトポロジの変更があった場合、別の AC または VPLS ネイバーを介してホストに到達できるようになる場合があります。既存の MAC アドレステーブルに従ってフレームを転送し続けた場合、そのホストへのトラフィックは宛先に到達しない可能性があります。

L2VPN PE には、トポロジの変更を検出する複数の方法があります。

- ブリッジドメイン内のポートがアップまたはダウンする。
- L2VPN PE がフル MST 実装またはスパニング ツリー アクセス ゲートウェイ プロトコルを実行している場合、スパニング ツリーのトポロジ変更通知 (TCN) BPDU が処理されます。障害リンクは PE ローカルではなく、このトポロジから遠く離れている場合もあります。PE は TCN を傍受します。

L2VPN PE は、トポロジの変更を検出すると次の 2 つの動作を行います。

1. PE は、トポロジ変更の影響を受けるブリッジドメインの MAC アドレステーブルを消去します。PE で PVSTAG または Per-VLAN Rapid Spanning Tree Access Gateway ( PVRSTAG ) が設定されている場合、1 つの VLAN サブインターフェイスで検出された TCN BPDU は、その物理インターフェイスのすべての VLAN とブリッジドメインに影響します。
2. PE は、MAC アドレステーブルを消去する必要があることを、MPLS LDP MAC 回収メッセージによって VPLS ネイバーに伝えます。MAC 回収 LDP メッセージを受信したすべてのリモート L2VPN PE は自身の MAC アドレステーブルを消去し、トラフィックは再びフラッピングされます。MAC アドレステーブルは新しいトポロジに基づいて再構築されます。

ポートフラップの場合の MAC 回収メッセージのデフォルトの動作は、時間と共に次のように変化します。

- 従来の Cisco IOS XR ソフトウェアでは、L2VPN PE は、AC がダウンしたときに MAC 回収メッセージを送信していました。これは、リモートの PE が影響を受けるブリッジドメインの MAC アドレステーブルを消去し、ダウンしたポートの背後をポイントしている MAC アドレスを別のポートから学習できるようにすることを目的としています。
- しかし、これにより、MAC 回収メッセージを送信している PE を除くすべての PE をポイントしている MAC アドレスを RFC 4762 に従い消去する一部のリモート PE と、相互運用性の問題が生じました。RFC 4762 では、AC がダウンしたときではなく、AC がアップしたときに PE が MAC 回収メッセージを送信することを前提としています。Cisco IOS XR ソフトウェア リリース 4.2.1 以降のデフォルトの動作では、より RFC に準拠するために、ブリッジドメインのポートがアップした場合にのみ LDP MAC 回収メッセージを送信します。以前の動作に戻すためのコンフィギュレーション コマンドが追加されています。

Cisco IOS XR ソフトウェア リリース 4.2.1 以降のデフォルトの動作での show コマンドを次に示します。

```
RP/0/RSP1/CPU0:router3#sh l2vpn bridge-domain bd-name engineering det |
i "PW:|VFI|neighbor|MAC w"
MAC withdraw: enabled
MAC withdraw for Access PW: enabled
MAC withdraw sent on bridge port down: disabled
ACs: 1 (1 up), VFIs: 1, PWs: 3 (3 up), PBBs: 0 (0 up)
List of VFIs:
VFI customer1-engineering (up)
PW: neighbor 10.0.0.11, PW ID 2, state is up ( established )
MAC withdraw message: send 0 receive 0
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )
MAC withdraw message: send 0 receive 4
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
MAC withdraw message: send 0 receive 2
VFI Statistics:
```

重要な行は "MAC withdraw sent on bridge port down" です。Cisco IOS XR ソフトウェア リリース 4.2.1 以降では、デフォルトでこの設定は無効になっています。このコマンドは、ブリッジドメイン内で送受信された MAC 回収メッセージの数も表示します。回収メッセージの数が多い場合、ブリッジドメインが不安定であることを示しています。

以前の動作に戻す設定を次に示します。

```
l2vpn
bridge group customer1
bridge-domain finance
mac
withdraw state-down
!
```

!  
!  
!

#### 4.4.5 H-VPLS

すべての PE が、ある PW から別の PW へフレームを転送することなく他の任意の PE の背後にあるホストに 1 ホップで到達できるようにするためには、VPLS では L2VPN PE 間にフル メッシュの PW が必要です。これがスプリット ホライズン ルールの基本です。これにより、PE によって 1 つの PW から別の PW にフレームが転送されるのを防ぐことができます。MAC アドレス テーブルの宛先 MAC アドレスが別の PW を指している特殊な場合でも、フレームはドロップされます。

フル メッシュの PW では、PE の数が増えるに従って PW の数が非常に多くなる可能性があるため、拡張性の問題が生じる場合があります。

このトポロジでは、PE 階層によって PW の数を削減できます。

このトポロジでは、次の点に注意してください。

- ユーザ プロバイダー エッジ ( U-PE ) デバイスには CE への AC があります。
- U-PE デバイスは、CE のトラフィックを、MPLS ポイントツーポイント PW を介してネットワーク プロバイダー エッジ ( N-PE ) デバイスに転送します。
- N-PE は、他の N-PE とのフル メッシュ構造を持つコア VPLS PE です。
- N-PE では、U-PE から来ている PW は AC と同様のアクセス PW であると見なされます。U-PE は他の N-PE とのメッシュの一部ではないため、N-PE はこのアクセス PW を AC と見なし、そのアクセス PW からのトラフィックを VPLS のフル メッシュの一部であるコア PW に転送できます。
- VFI の下で設定されるすべてのコア PW にスプリット ホライズン ルールを確実に適用するために、N-PE 間のコア PW は VFI の下で設定します。
- U-PE からのアクセス PW は VFI の下で設定されていないため、VFI PW と同じ SHG には含まれません。トラフィックはアクセス PW から VFI PW へ、およびその逆方向に転送できます。
- U-PE は PW の冗長機能を使用して、プライマリ N-PE へのプライマリ PW と、スタンバイ N-PE へのスタンバイ PW を持つことができます。プライマリ PW がダウンすると、スタンバイが引き継ぎます。

次の例では、U-PE1 ( 10.0.0.15 ) には N-PE1 ( 10.0.0.11 ) および N-PE2 ( 10.0.0.12 ) への PW 冗長性が設定されています。

```
RP/0/RP0/CPU0:U-PE1#sh run int ten 0/1/0/5.2
interface TenGigE0/1/0/5.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
```

```
RP/0/RP0/CPU0:U-PE1#sh run l2vpn xconnect group customer1
l2vpn
xconnect group customer1
p2p engineering-0-1-0-5
interface TenGigE0/1/0/5.2
neighbor 10.0.0.11 pw-id 15
backup neighbor 10.0.0.12 pw-id 15
!
```

!  
!  
!  
!

```
RP/0/RP0/CPU0:U-PE1#sh l2vpn xconnect group customer1
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
-----
customer1 engineering-0-1-0-5
UP Te0/1/0/5.2 UP 10.0.0.11 15 UP
Backup
10.0.0.12 15 SB
-----
```

10.0.0.12 への PW はスタンバイ状態です。 N-PE1 には、10.0.0.15 へのアクセス PW と、VFI に含まれない AC があります。

N-PE1 は、アクセス PW と VFI PW 上でいくつかの MAC アドレスを学習しています。

```
RP/0/RSP0/CPU0:N-PE1#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
bridge group customer1
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
!
neighbor 10.0.0.15 pw-id 15
!
vfi customer1-engineering
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!
```

```
RP/0/RSP0/CPU0:N-PE1#sh l2vpn bridge-domain bd-name engineering
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 5, 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: 4 (4 up), PBBs: 0 (0 up)
List of ACs:
Gi0/1/0/3.2, state: up, Static MAC addresses: 0
List of Access PWs:
Neighbor 10.0.0.15 pw-id 15, state: up, Static MAC addresses: 0
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0
RP/0/RSP0/CPU0:N-PE1#sh l2vpn forwarding bridge-domain customer1:engineering
mac-address location 0/0/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location
```

Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to

```
-----  
6c9c.ed3e.e46d dynamic (10.0.0.15, 15) 0/0/CPU0 0d 0h 0m 0s N/A  
0019.552b.b5c3 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A  
0024.985e.6a42 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A  
001d.4603.1f42 dynamic (10.0.0.13, 2) 0/0/CPU0 0d 0h 0m 0s N/A
```

N-PE2 ( 10.0.0.12 ) では、アクセス PW はスタンバイ状態です。

```
RP/0/RSP0/CPU0:N-PE2#sh run l2vpn bridge group customer1 bridge-domain  
engineering  
l2vpn  
bridge group customer1  
bridge-domain engineering  
interface GigabitEthernet0/1/0/3.2  
!  
neighbor 10.0.0.15 pw-id 15  
!  
vfi customer1-engineering  
neighbor 10.0.0.11 pw-id 2  
!  
neighbor 10.0.0.13 pw-id 2  
!  
neighbor 10.0.0.14 pw-id 2  
!  
!  
!  
!  
RP/0/RSP0/CPU0:N-PE2#sh l2vpn bridge-domain bd-name engineering  
Legend: pp = Partially Programmed.  
Bridge group: customer1, bridge-domain: engineering, id: 1, 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: 4 (3 up), PBBs: 0 (0 up)  
List of ACs:  
Gi0/1/0/3.2, state: up, Static MAC addresses: 0  
List of Access PWs:  
Neighbor 10.0.0.15 pw-id 15, state: standby, Static MAC addresses: 0  
List of VFIs:  
VFI customer1-engineering (up)  
Neighbor 10.0.0.11 pw-id 2, state: up, Static MAC addresses: 0  
Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0  
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0
```

#### 4.4.6 スプリット ホライズン グループ ( SHG )

スプリット ホライズン ルールによって、ある VFI PW で受信したフレームを別の VFI PW に転送できないことが規定されます。VFI N-PE はフル メッシュ構造にする必要があります。

このスプリット ホライズンは、SHG を通じて次のように適用されます。

- 1 つの SHG に属するメンバーは相互にフレームを転送できませんが、フレームを他の SHG のメンバーに転送することはできます。
- デフォルトでは、すべての VFI PW が SHG 1 に割り当てられます。これにより、VFI PW 間での転送をなくすことができ、スプリット ホライズン ルールが適用されます。VFI PW で受信したパケットは、AC およびアクセス PW に転送できます。これらは同じ SHG に属していないためです。
- デフォルトではすべての AC およびアクセス PW は SHG グループに属していません。これ

は、AC またはアクセス PW で受信したパケットを、同じブリッジドメインの別の AC またはアクセス PW に転送できることを意味します。

- AC およびアクセス PW の間での転送を防ぐことが目的の場合、**split-horizon group** コマンドによってこれらを SHG 2 に割り当てることができます。

```
RP/0/RSP0/CPU0:N-PE1#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
bridge group customer1
bridge-domain engineering
interface GigabitEthernet0/0/0/1.2
split-horizon group
!
interface GigabitEthernet0/1/0/3.2
split-horizon group
!
neighbor 10.0.0.15 pw-id 15
split-horizon group
!
vfi customer1-engineering
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
```

この設定では、Gi 0/0/0/1.2 と Gi 0/1/0/3.2 の間、Gi 0/0/0/1.2 と 10.0.0.15 の間、または Gi 0/1/0/3.2 と 10.0.0.15 の間の転送は行われません。AC と VFI PW は別の SHG ( 1 と 2 ) に属しているため、この場合でもこれらの間でトラフィックの転送は可能です。

```
RP/0/RSP0/CPU0:N-PE1#sh l2vpn bridge-domain bd-name engineering detail |
i "state is|List of|VFI|Split"
Split Horizon Group: none
ACs: 2 (1 up), VFIs: 1, PWs: 4 (4 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/0/0/1.2, state is unresolved
Split Horizon Group: enabled
AC: GigabitEthernet0/1/0/3.2, state is up
Split Horizon Group: enabled
List of Access PWs:
PW: neighbor 10.0.0.15, PW ID 15, state is up ( established )
Split Horizon Group: enabled
List of VFIs:
VFI customer1-engineering (up)
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )
PW: neighbor 10.0.0.13, PW ID 2, state is up ( established )
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
VFI Statistics:
```

#### 4.4.7 冗長性

冗長性を導入する際に、VPLS ドメインに二重接続されたサイトがある場合があります。

switch1 に接続されたホストがブロードキャストを送信する場合、switch1 はそれを router1 と



switch2 に転送します。router1 にはフル メッシュの PW があるため、router2 への PW が存在し、router1 はブロードキャストをその PW に転送します。router2 はブロードキャストを switch2 に転送し、switch2 はそれを switch1 に転送します。この結果、物理的なループが生じます。

#### 4.4.7.1 スパニング ツリー

**フル MST** 実装は VPLS では機能しません。この実装では、インターフェイス上のすべての VLAN のフォワーディング ステートを制御するために、メイン インターフェイスで MST BPDU を送信するからです。VPLS では、各ブリッジドメイン用の VFI があるため、メイン インターフェイスでこれらすべての VFI に BPDU を送信することはできません。

デフォルトでは、スパニング ツリー BPDU は、VPLS とポイントツーポイント PW 上で転送されます。

switch1 および switch2 が Per-VLAN BPDU またはタグなし MST BPDU を送信し、BPDU が router1 および router2 の I2transport サブインターフェイスに一致する場合、BPDU は VPLS を介して転送されます。スイッチは Gi 0/1 インターフェイスでお互いの BPDU を確認し、スパニング ツリーによってループを解消して 1 つのポートをブロックします。

switch2 は VLAN 2 のルートです。

```
switch2#sh spanning-tree vlan 2

MST0
Spanning tree enabled protocol mstp
Root ID Priority 32768
Address 0024.985e.6a00
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address 0024.985e.6a00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
-----
```

```
Gi0/1 Desg FWD 20000 128.1 P2p Bound(PVST)
Gi0/2 Desg FWD 20000 128.2 P2p Bound(PVST)
```

switch1 は Gi 0/1 にルート ポートがあり、Gi 0/2 をブロックしています。

```
switch1#sh spanning-tree vlan 2

VLAN0002
Spanning tree enabled protocol ieee
Root ID Priority 32768
Address 0024.985e.6a00
Cost 4
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32770 (priority 32768 sys-id-ext 2)
Address 0019.552b.b580
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300 sec

Interface Role Sts Cost Prio.Nbr Type
-----
```

Gi0/1 Root FWD 4 128.1 P2p

Gi0/2 Altn BLK 4 128.2 P2p

問題は、BPDU はリモート サイトにも転送されるので、1 つのサイトのスパニング ツリーの不安定さが VPLS ドメインに接続されているすべてのサイトに伝播することです。各サイトを分離し、VPLS 上で BPDU を転送しない方が安全です。

解決策の 1 つは、アクセス ゲートウェイ バージョンの STP を使用することです。これは、このプロトコルの制限された実装であり、L2VPN PE はスパニング ツリー ルートに接続されているふりをするために、ある静的な BPDU を送信するように設定されます。L2VPN PE は CE から受信した BPDU をリモート サイトに転送しないため、各サイトには独自のスパニング ツリー ドメインがあります。

#### 4.4.7.2 MSTAG

「[スパニング ツリー](#)」の項で説明したように、MST はタグなし BPDU を送信しますが、これらの BPDU はインターフェイス上のすべての VLAN のフォワーディング ステートを制御します。

VLAN は、複数のインスタンスにグループ化することができ、各インスタンスには独自のフォワーディング ステートがあります。

通常、VLAN はトラフィックが複数のパス間で均等に分散するようにグループ化されます。2 つのパスがある場合、トラフィックの半分は、最初のパスで転送を行い 2 番目のパスをブロックするインスタンスに含まれます。トラフィックの残りの半分は、最初のパスをブロックして 2 番目のパスで転送を行うインスタンスに含まれます。安定した状態では、これによって 2 つのパス間でロード バランシングが実現します。別の方法では、通常時には 1 つのパスを完全にブロックし、プライマリ パスがダウンした場合にのみこのパスをアクティブにします。

一般的な MSTAG のトポロジを次に示します。

このラボの例では、インスタンス 1 には VLAN 2 が、インスタンス 0 にはその他の VLAN が含まれています（より現実的なシナリオでは、インスタンス間でより良好なトラフィックのロード バランシングを実現するために、VLAN を複数のインスタンス間に分散させます）。一部の VLAN には他よりも多くのトラフィックが存在するため、各インスタンスに常に同じ数の VLAN があるとは限りません。

MST のインスタンス 0 の設定は次のとおりです。

- router1 と router2 は MSTAG の設定に基づいて、ある静的な BPDU を送信します。これらは、ネットワークから着信する BPDU を処理したり、完全な実装の実行を試みたりはしません。MSTAG では、2 つの L2VPN PE は、MSTAG の設定に基づいて静的な BPDU を送信するだけです。
- router1 は、インスタンス 0 のルートであるふりをすることによって、インスタンス 0 のトラフィックを引き寄せるように設定されています。
- router2 は、インスタンス 0 の 2 番目のルート プライオリティを持つように設定され、router1 の障害時または switch1 と router1 の間の AC の障害時に新しいルートになります。
- switch2 では、ポート Gi 0/1 に router2 への高いスパニング ツリー コストが設定されています。これは、ルートへのプライマリ パスを Gig 0/2 にして、switch1 および router1 を経由するようにするためです。
- switch2 はインスタンス 0 のルート ポートとして Gi 0/2 を選択し、このルートが失われた場

合に Gi 0/1 を代替ポートとして選択します。

- したがって、VLAN のこのサイトからのトラフィックはインスタンス 0 に属し、他のサイトには router1 を介して VPLS で到達します。

MST のインスタンス 1 ( VLAN 2 ) では、設定は逆になります。

- router2 は、インスタンス 1 のルートであるふりをすることによって、インスタンス 1 のトラフィックを引き寄せるように設定されています。
- router1 は、インスタンス 1 の 2 番目のルート プライオリティを持つように設定され、router2 の障害時または switch2 と router2 の間の AC の障害時に新しいルートになります。
- switch1 では、ポート Gi 0/1 に router1 への高いスパニング ツリー コストが設定されています。これは、ルートへのプライマリ パスを Gig 0/2 にして、switch2 および router2 を経由するようにするためです。
- switch1 はインスタンス 1 のルート ポートとして Gi 0/2 を選択し、このルートが失われた場合に Gi 0/1 を代替ポートとして選択します。
- したがって、VLAN のこのサイトからのトラフィックはインスタンス 1 ( この例では VLAN 2 ) に属し、他のサイトには router2 を介して VPLS で到達します。
- タグなしの TCN をキャッチしてポイントツーポイント PW で他のルータに転送するために、router1 と router2 にはサブインターフェイスが必要です。switch1 と switch2 は、それらの直接リンクが失われてお互いから分離される可能性があるため、router1 と router2 はそのポイントツーポイント PW を介してお互いの中で TCN を転送する必要があります。
- また、PE は TCN を受信し、自身の MAC アドレス テーブルを消去して、LDP MAC 回収をリモート PE に送信します。

router1 の設定を次に示します。

```
RP/0/RSP0/CPU0:router1#sh run int gigabitEthernet 0/1/0/3.*
interface GigabitEthernet0/1/0/3.1 l2transport
encapsulation untagged
!
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
ethernet-services access-group filter-stp egress
!
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
ethernet-services access-group filter-stp egress
!

RP/0/RSP0/CPU0:router1#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/1/0/3.3
!
vfi customer1-finance
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
```

```
!  
vfi customer1-engineering  
neighbor 10.0.0.12 pw-id 2  
!  
neighbor 10.0.0.13 pw-id 2  
!  
neighbor 10.0.0.14 pw-id 2  
!  
!  
!  
!  
!
```

```
RP/0/RSP0/CPU0:router1#sh run l2vpn xconnect group customer1  
l2vpn  
xconnect group customer1  
p2p mstag-gi-0-1-0-3  
interface GigabitEthernet0/1/0/3.1  
neighbor 10.0.0.13 pw-id 103  
!  
!  
!  
!
```

```
RP/0/RSP0/CPU0:router1#sh run spanning-tree mstag customer1-0-1-0-3  
spanning-tree mstag customer1-0-1-0-3  
interface GigabitEthernet0/1/0/3.1  
name customer1  
revision 1  
bridge-id 0000.0000.0001  
instance 0  
root-id 0000.0000.0001  
priority 4096  
root-priority 4096  
!  
instance 1  
vlan-ids 2  
root-id 0000.0000.0002  
priority 8192  
root-priority 4096  
!  
!  
!
```

```
RP/0/RSP0/CPU0:router1#sh spanning-tree mstag customer1-0-1-0-3  
GigabitEthernet0/1/0/3.1  
Pre-empt delay is disabled  
Name: customer1  
Revision: 1  
Max Age: 20  
Provider Bridge: no  
Bridge ID: 0000.0000.0001  
Port ID: 1  
External Cost: 0  
Hello Time: 2  
Active: yes  
BPDUs sent: 3048  
MSTI 0 (CIST):  
VLAN IDs: 1,3-4094  
Role: Designated  
Bridge Priority: 4096  
Port Priority: 128  
Cost: 0  
Root Bridge: 0000.0000.0001
```

```
Root Priority: 4096
Topology Changes: 369
MSTI 1
VLAN IDs: 2
Role: Designated
Bridge Priority: 8192
Port Priority: 128
Cost: 0
Root Bridge: 0000.0000.0002
Root Priority: 4096
Topology Changes: 322
```

この設定では、次の点に注意してください。

- MST インスタンス 0 では、ルートブリッジは 0000.0000.0001 ( router1 のブリッジ ID ) です。
- MST インスタンス 1 では、ルートブリッジは 0000.0000.0002 ( router2 のブリッジ ID ) です。
- router1 のブリッジプライオリティは、インスタンス 0 では 4096 ( ルートになる )、インスタンス 1 では 8192 ( 2 番目にルートになる ) です。
- router1 のブリッジプライオリティは、インスタンス 0 では 8192 ( 2 番目にルートになる )、インスタンス 1 では 4096 ( ルートになる ) です。
- GigabitEthernet0/1/0/3.1 のポイントツーポイント クロス コネクトは、タグなし MST TCN を他のルータに送信します。

MST にまだ移行していない他のサイトから送信される可能性がある Per-VLAN BPDU をドロップするために、dot1q サブインターフェイスでは出力 ACL が設定されています。この設定により、MST が設定されたインターフェイス上 Per-VLAN BPDU を受信したときに、CE スイッチが矛盾したインターフェイスを宣言することを防ぎます。

router2 の設定は非常によく似ています。

```
RP/0/RSP0/CPU0:router2#sh run int gig 0/1/0/3.*
interface GigabitEthernet0/1/0/3.1 l2transport
encapsulation untagged
!
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
ethernet-services access-group filter-stp egress
!
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
ethernet-services access-group filter-stp egress
!

RP/0/RSP0/CPU0:router2#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/1/0/3.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
```

```
!  
!  
bridge-domain engineering  
interface GigabitEthernet0/1/0/3.2  
!  
vfi customer1-engineering  
neighbor 10.0.0.11 pw-id 2  
!  
neighbor 10.0.0.13 pw-id 2  
!  
neighbor 10.0.0.14 pw-id 2  
!  
!  
!  
!  
!
```

```
RP/0/RSP0/CPU0:router2#sh run l2vpn xconnect group customer1  
l2vpn  
xconnect group customer1  
p2p mstag-gi-0-1-0-3  
interface GigabitEthernet0/1/0/3.1  
neighbor 10.0.0.13 pw-id 103  
!  
!  
!  
!
```

```
RP/0/RSP0/CPU0:router2#sh run spanning-tree mstag customer1-0-1-0-3  
spanning-tree mstag customer1-0-1-0-3  
interface GigabitEthernet0/1/0/3.1  
name customer1  
revision 1  
bridge-id 0000.0000.0002  
instance 0  
root-id 0000.0000.0001  
priority 8192  
root-priority 4096  
!  
instance 1  
vlan-ids 2  
root-id 0000.0000.0002  
priority 4096  
root-priority 4096  
!  
!  
!
```

```
RP/0/RSP0/CPU0:router2#sh spanning-tree mstag customer1-0-1-0-3  
GigabitEthernet0/1/0/3.1  
Pre-empt delay is disabled  
Name: customer1  
Revision: 1  
Max Age: 20  
Provider Bridge: no  
Bridge ID: 0000.0000.0002  
Port ID: 1  
External Cost: 0  
Hello Time: 2  
Active: yes  
BPDUs sent: 3186  
MSTI 0 (CIST):  
VLAN IDs: 1,3-4094  
Role: Designated
```

Bridge Priority: 8192  
Port Priority: 128  
Cost: 0  
Root Bridge: 0000.0000.0001  
Root Priority: 4096  
Topology Changes: 365  
MSTI 1  
VLAN IDs: 2  
Role: Designated  
Bridge Priority: 4096  
Port Priority: 128  
Cost: 0  
Root Bridge: 0000.0000.0002  
Root Priority: 4096  
Topology Changes: 177

スイッチ 1 の基本設定を次に示します。

```
switch1#sh run | b spanning-tree
spanning-tree mode mst
spanning-tree extend system-id
!
spanning-tree mst configuration
name customer1
revision 1
instance 1 vlan 2
!
switch1#sh run int gig 0/1 | i spanning
spanning-tree mst 1 cost 100000

switch1#sh spanning-tree

MST0
Spanning tree enabled protocol mstp
Root ID Priority 4096
Address 0000.0000.0001
Cost 0
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address 0019.552b.b580
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
-----
Gi0/1 Root FWD 20000 128.1 P2p
Gi0/2 Desg FWD 20000 128.2 P2p

MST1
Spanning tree enabled protocol mstp
Root ID Priority 4097
Address 0000.0000.0002
Cost 40000
Port 2 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0019.552b.b580
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface Role Sts Cost Prio.Nbr Type
```

```
-----  
Gi0/1 Altn BLK 100000 128.1 P2p
```

```
Gi0/2 Root FWD 20000 128.2 P2p
```

このように、インスタンス 0 のトラフィックは router1 経由で転送され、インスタンス 1 のトラフィックは switch2 と router2 を経由して転送されます。

switch2 の設定では、switch1 と同じコマンドを使用します。

```
switch2#sh run | b spanning
```

```
spanning-tree mode mst
```

```
spanning-tree extend system-id
```

```
!
```

```
spanning-tree mst configuration
```

```
name customer1
```

```
revision 1
```

```
instance 1 vlan 2
```

```
!
```

```
switch2#sh run int gig 0/1 | i spanning
```

```
spanning-tree mst 0 cost 100000
```

```
switch2#sh spanning-tree
```

```
MST0
```

```
Spanning tree enabled protocol mstp
```

```
Root ID Priority 4096
```

```
Address 0000.0000.0001
```

```
Cost 0
```

```
Port 2 (GigabitEthernet0/2)
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
```

```
Address 0024.985e.6a00
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Interface Role Sts Cost Prio.Nbr Type
```

```
-----  
Gi0/1 Altn BLK 100000 128.1 P2p
```

```
Gi0/2 Root FWD 20000 128.2 P2p
```

```
MST1
```

```
Spanning tree enabled protocol mstp
```

```
Root ID Priority 4097
```

```
Address 0000.0000.0002
```

```
Cost 20000
```

```
Port 1 (GigabitEthernet0/1)
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
```

```
Address 0024.985e.6a00
```

```
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Interface Role Sts Cost Prio.Nbr Type
```

```
-----  
Gi0/1 Root FWD 20000 128.1 P2p
```

```
Gi0/2 Desg FWD 20000 128.2 P2p
```

switch2 は、インスタンス 0 については switch1 と router1 を経由して、インスタンス 1 については router2 を経由して送信を行います。

一方のインスタンスでは router1 経由でサイトから外に出て、もう一方のインスタンスでは



router2 経由でサイトから外にでるため、トラフィックはロードバランスされます。

router1 と switch1 の間のリンクがダウンした場合、両方のインスタンスが router2 経由で転送されます。

```
switch1#sh spanning-tree
```

```
MST0
Spanning tree enabled protocol mstp
Root ID Priority 4096
Address 0000.0000.0001
Cost 0
Port 2 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address 0019.552b.b580
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Interface Role Sts Cost Prio.Nbr Type
-----
Gi0/2 Root FWD 20000 128.2 P2p
```

```
MST1
Spanning tree enabled protocol mstp
Root ID Priority 4097
Address 0000.0000.0002
Cost 40000
Port 2 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0019.552b.b580
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Interface Role Sts Cost Prio.Nbr Type
-----
Gi0/2 Root FWD 20000 128.2 P2p
```

```
switch2#sh spanning-tree
```

```
MST0
Spanning tree enabled protocol mstp
Root ID Priority 4096
Address 0000.0000.0001
Cost 0
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 0)
Address 0024.985e.6a00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Interface Role Sts Cost Prio.Nbr Type
-----
Gi0/1 Root FWD 100000 128.1 P2p
Gi0/2 Desg FWD 20000 128.2 P2p
```

```
MST1
Spanning tree enabled protocol mstp
Root ID Priority 4097
Address 0000.0000.0002
Cost 20000
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0024.985e.6a00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Interface Role Sts Cost Prio.Nbr Type
```

```
-----
Gi0/1 Root FWD 20000 128.1 P2p
Gi0/2 Desg FWD 20000 128.2 P2p
```

2番目のルートを通るパスは代替パスとしてすでに選択されているため、この種の障害では高速コンバージェンスを実現できません。MSTAGではMST BPDUはVPLS上を転送されないため、サイトは他のサイトの不安定さから分離されます。

#### 4.4.7.3 PVSTAG または PVRSTAG

MSTAGは、高速スパンニング ツリー プロトコルを使用することに加えて、各 VLAN 上の BPDUではなくインスタンスを使用して拡張可能であるので、VPLSの推奨されるアクセスゲートウェイプロトコルです。

サイトをMSTに移行できず、PVST+ または PVRST を実行し続けることが唯一の解決策である場合、PVSTAG または PVRSTAG を使用できますが、その実装は特定の1つのトポロジに限定されます。

このトポロジで最も重要な制限は、存在できるCEスイッチは1つだけだということです。「[MSTAG トポロジ](#)」のように2つのスイッチを使用することはできません。MSTAGでは、サイトが2つの部分に分かれている場合、(BPDU TCNを含む)タグなしトラフィックをあるPEから他へ転送するために、ポイントツーポイントPWを設定できます。PVSTおよびPVRSTの場合、TCNはタグ付きで送信されるため、VPLS上を転送されるデータトラフィックと同じサブインターフェイスに一致します。TCNを他のサイトに転送するためには、ルータはMACアドレスとプロトコルタイプに基づいてBPDUを特定する必要があります。これは現在サポートされていないため、CEデバイスは1つのみという要件が存在します。

Cisco IOS XR ソフトウェア リリース 4.3.0 より前のリリースの別の要件として、バンドル インターフェイスをACとして使用できないことがあります。この制限は、Cisco IOS XR ソフトウェア リリース 4.3.0 で解除されました。

この原理はMSTAGとほぼ同じです。PVSTAG ルータは静的なBPDUを送信するため、(仮想)ルートとコスト0で直接接続されているスイッチにCEが接続されているように見えます。トラフィックをロードバランスするためには、一部のVLANではrouter3をルートとして設定し、それ以外についてはrouter4をルートとして設定します。

router3 の設定例を次に示します。

```
RP/0/RSP1/CPU0:router3#sh run int gigabitEthernet 0/0/0/1.*
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
```

```
!  
interface GigabitEthernet0/0/0/1.3 l2transport  
encapsulation dot1q 3  
rewrite ingress tag pop 1 symmetric  
!
```

```
RP/0/RSP1/CPU0:router3#sh run l2vpn bridge group customer1  
l2vpn
```

```
bridge group customer1  
bridge-domain finance  
interface GigabitEthernet0/0/0/1.3
```

```
!  
vfi customer1-finance  
neighbor 10.0.0.11 pw-id 3  
!  
neighbor 10.0.0.12 pw-id 3  
!  
neighbor 10.0.0.14 pw-id 3
```

```
!  
!  
!  
bridge-domain engineering  
interface GigabitEthernet0/0/0/1.2
```

```
!  
vfi customer1-engineering  
neighbor 10.0.0.11 pw-id 2  
!  
neighbor 10.0.0.12 pw-id 2  
!  
neighbor 10.0.0.14 pw-id 2
```

```
!  
!  
!  
!  
!
```

```
RP/0/RSP1/CPU0:router3#sh run spanning-tree pvstag customer1-0-0-0-1
```

```
spanning-tree pvstag customer1-0-0-0-1  
interface GigabitEthernet0/0/0/1
```

```
vlan 2  
root-priority 0  
root-id 0000.0000.0000  
root-cost 0  
priority 0  
bridge-id 0000.0000.0001
```

```
!  
vlan 3  
root-priority 0  
root-id 0000.0000.0000  
root-cost 0  
priority 1  
bridge-id 0000.0000.0001
```

```
!  
!  
!
```

```
RP/0/RSP1/CPU0:router3#sh spanning-tree pvstag customer1-0-0-0-1
```

```
GigabitEthernet0/0/0/1  
VLAN 2  
Pre-empt delay is disabled  
Sub-interface: GigabitEthernet0/0/0/1.2 (Up)  
Max Age: 20  
Root Priority: 0  
Root Bridge: 0000.0000.0000
```

```
Cost: 0
Bridge Priority: 0
Bridge ID: 0000.0000.0001
Port Priority: 128
Port ID 1
Hello Time: 2
Active: Yes
BPDUs sent: 202821
Topology Changes: 0
VLAN 3
Pre-empt delay is disabled
Sub-interface: GigabitEthernet0/0/0/1.3 (Up)
Max Age: 20
Root Priority: 0
Root Bridge: 0000.0000.0000
Cost: 0
Bridge Priority: 1
Bridge ID: 0000.0000.0001
Port Priority: 128
Port ID 1
Hello Time: 2
Active: Yes
BPDUs sent: 202821
Topology Changes: 0
```

**router4 の設定例を次に示します。**

```
RP/0/RSP1/CPU0:router4#sh run int gig 0/0/0/1.*
interface GigabitEthernet0/0/0/1.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface GigabitEthernet0/0/0/1.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!
```

```
RP/0/RSP1/CPU0:router4#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface GigabitEthernet0/0/0/1.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
!
!
bridge-domain engineering
interface GigabitEthernet0/0/0/1.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
!
!
```

```
!  
!  
RP/0/RSP1/CPU0:router4#sh run spanning-tree pvstag customer1-0-0-0-1  
spanning-tree pvstag customer1-0-0-0-1  
interface GigabitEthernet0/0/0/1  
vlan 2  
root-priority 0  
root-id 0000.0000.0000  
root-cost 0  
priority 1  
bridge-id 0000.0000.0002  
!  
vlan 3  
root-priority 0  
root-id 0000.0000.0000  
root-cost 0  
priority 0  
bridge-id 0000.0000.0002  
!  
!  
!
```

```
RP/0/RSP1/CPU0:router4#sh spanning-tree pvstag customer1-0-0-0-1  
GigabitEthernet0/0/0/1  
VLAN 2  
Pre-empt delay is disabled  
Sub-interface: GigabitEthernet0/0/0/1.2 (Up)  
Max Age: 20  
Root Priority: 0  
Root Bridge: 0000.0000.0000  
Cost: 0  
Bridge Priority: 1  
Bridge ID: 0000.0000.0002  
Port Priority: 128  
Port ID 1  
Hello Time: 2  
Active: Yes  
BPDUs sent: 202799  
Topology Changes: 0  
VLAN 3  
Pre-empt delay is disabled  
Sub-interface: GigabitEthernet0/0/0/1.3 (Up)  
Max Age: 20  
Root Priority: 0  
Root Bridge: 0000.0000.0000  
Cost: 0  
Bridge Priority: 0  
Bridge ID: 0000.0000.0002  
Port Priority: 128  
Port ID 1  
Hello Time: 2  
Active: Yes  
BPDUs sent: 202799  
Topology Changes: 0
```

CE switch3 の設定例を次に示します。

```
switch3#sh spanning-tree vlan 2  
  
VLAN0002  
Spanning tree enabled protocol ieee  
Root ID Priority 0  
Address 0000.0000.0000
```

```
Cost 4
Port 1 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32770 (priority 32768 sys-id-ext 2)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
```

```
Interface Role Sts Cost Prio.Nbr Type
-----
```

```
Gi0/1 Root FWD 4 128.1 P2p
Gi0/2 Altn BLK 4 128.2 P2p
```

```
switch3#sh spanning-tree vlan 3
```

```
VLAN0003
Spanning tree enabled protocol ieee
Root ID Priority 0
Address 0000.0000.0000
Cost 4
Port 2 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32771 (priority 32768 sys-id-ext 3)
Address 001d.4603.1f00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
```

```
Interface Role Sts Cost Prio.Nbr Type
-----
```

```
Gi0/1 Altn BLK 4 128.1 P2p
Gi0/2 Root FWD 4 128.2 P2p
```

PVSTAG の設定は MSTAG とよく似ていますが、MSTAG の例ではルートプライオリティとプライマリ ゲートウェイのプライオリティが 4096 に設定され、バックアップ ゲートウェイのプライオリティが 8192 に設定されている点が異なります。

ドメイン内にある他のすべてのスイッチのプライオリティは、PVSTAG または PVRSTAG で設定されているものよりも大きくする必要があります。

CE スwitchのインターフェイス コストを調整することで、どのポートがルート ポートになり、どのポートがブロックされるのかを変更できます。

#### 4.4.7.4 MC-LAG

VPLS を伴う MC-LAG の設定は、双方向の PW 冗長性を備えたポイントツーポイント PW よりも簡単です。PE は、1 つのプライマリ PW と 3 つのスタンバイ PW の代わりに、フル メッシュの VPLS PW ( VPLS の標準 ) のみを必要とします。

このトポロジでは、次の点に注意してください。

- 左側の 2 つの VPLS PE の間で MC-LAG が実行されます ( router2 と router4 ) 。
- 通常の状態では、バンドル メンバーは router1 と router2 の間はアクティブで、router1 と router4 の間はスタンバイ状態です。
- router2 には VPLS ブリッジドメインで設定されたバンドル サブインターフェイスがあるた

め、router2 はトラフィックをリモートの VPLS PE に転送します。トポロジ図には 2 つのサイトが描かれていますが、もっと多い場合もあります。

- リモート PE は router1 や、router2 の背後のデバイスから MAC アドレスを学習するため、PE はこれらの宛先 MAC アドレスのトラフィックを router2 経由で転送します。
- router1 と router2 の間のリンクがダウンした場合、または router2 がダウンした場合、router1 と router4 の間のバンドル メンバーがアクティブになります。
- router2 と同様に、router4 にも VPLS ブリッジドメインで設定されたバンドル サブインターフェイスがあります。
- バンドル サブインターフェイスが router4 で起動すると、トポロジの変更があることを通知するために、router4 はリモートの VPLS PE に LDP MAC 回収メッセージを送信します。

router3 の設定を次に示します。

```
RP/0/RSP1/CPU0:router3#sh run redundancy
```

```
redundancy
iccp
group 2
mlacp node 1
mlacp system mac 0200.0000.0002
mlacp system priority 1
mlacp connect timeout 0
member
neighbor 10.0.0.14
!
backbone
interface TenGigE0/0/0/0
interface TenGigE0/0/0/1
!
isolation recovery-delay 300
!
!
!
```

```
RP/0/RSP1/CPU0:router3#sh run int bundle-ether 222
```

```
interface Bundle-Ether222
lacp switchover suppress-flaps 100
mlacp iccp-group 2
mlacp switchover type revertive
mlacp switchover recovery-delay 40
mlacp port-priority 1
mac-address 0.0.2
bundle wait-while 0
bundle maximum-active links 1
load-interval 30
!
```

```
RP/0/RSP1/CPU0:router3#sh run int bundle-ether 222.*
```

```
interface Bundle-Ether222.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
interface Bundle-Ether222.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!
```

```
RP/0/RSP1/CPU0:router3#sh run l2vpn bridge group customer1
```

```
l2vpn
bridge group customer1
bridge-domain finance
interface Bundle-Ether222.3
```

```

!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface Bundle-Ether222.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!

```

MC-LAG バンドルを設定したら、他の AC と同様にそれを VPLS 設定の下に追加します。

router5 の対応する設定を次に示します。

```

RP/0/RSP1/CPU0:router5#sh run redundancy
redundancy
iccp
group 2
mlacp node 2
mlacp system mac 0200.0000.0002
mlacp system priority 1
mlacp connect timeout 0
member
neighbor 10.0.0.13
!
backbone
interface TenGigE0/1/0/0
interface TenGigE0/1/0/1
!
isolation recovery-delay 300
!
!
!

```

```

RP/0/RSP1/CPU0:router5#sh run int bundle-ether 222
interface Bundle-Ether222
lACP switchover suppress-flaps 100
mlacp iccp-group 2
mlacp switchover type revertive
mlacp switchover recovery-delay 40
mac-address 0.0.2
bundle wait-while 0
bundle maximum-active links 1
load-interval 30
!

```

```

RP/0/RSP1/CPU0:router5#sh run int bundle-ether 222.*
interface Bundle-Ether222.2 l2transport
encapsulation dot1q 2

```



```
rewrite ingress tag pop 1 symmetric
!  
interface Bundle-Ether222.3 l2transport  
encapsulation dot1q 3  
rewrite ingress tag pop 1 symmetric  
!
```

```
RP/0/RSP1/CPU0:router5#sh run l2vpn bridge group customer1  
l2vpn  
bridge group customer1  
bridge-domain finance  
interface Bundle-Ether222.3  
!  
vfi customer1-finance  
neighbor 10.0.0.11 pw-id 3  
!  
neighbor 10.0.0.12 pw-id 3  
!  
neighbor 10.0.0.13 pw-id 3  
!  
!  
!  
bridge-domain engineering  
interface Bundle-Ether222.2  
!  
vfi customer1-engineering  
neighbor 10.0.0.11 pw-id 2  
!  
neighbor 10.0.0.12 pw-id 2  
!  
neighbor 10.0.0.13 pw-id 2  
!  
!  
!  
!  
!
```

通常の状態では、router3 と router6 の間のバンドル メンバーはアクティブで、router5 と router6 の間のメンバーはスタンバイ状態です。

```
RP/0/RSP1/CPU0:router3#sh bundle bundle-ether 222
```

```
Bundle-Ether222  
Status: Up  
Local links : 1 / 0 / 1  
Local bandwidth : 1000000 (1000000) kbps  
MAC address (source): 0000.0000.0002 (Configured)  
Inter-chassis link: No  
Minimum active links / bandwidth: 1 / 1 kbps  
Maximum active links: 1  
Wait while timer: Off  
Load balancing: Default  
LACP: Operational  
Flap suppression timer: 100 ms  
Cisco extensions: Disabled  
mLACP: Operational  
ICCP Group: 2  
Role: Active  
Foreign links : 0 / 1  
Switchover type: Revertive  
Recovery delay: 40 s  
Maximize threshold: 1 link  
IPv4 BFD: Not configured
```

```
Port Device State Port ID B/W, kbps
-----
Gi0/0/0/1 Local Active 0x0001, 0x9001 1000000
Link is Active
Gi0/0/0/1 10.0.0.14 Standby 0x8000, 0xa002 1000000
Link is marked as Standby by mLACP peer
RP/0/RSP1/CPU0:router3#
```

```
router6#sh etherchannel summary
Flags: D - down P - bundled in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
```

```
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
```

```
Number of channel-groups in use: 1
Number of aggregators: 1
```

```
Group Port-channel Protocol Ports
-----+-----+-----+-----
2 Po2(SU) LACP Gi0/1(P) Gi0/2(w)
```

```
router6#
```

**CEからのトラフィックは router3 で受信され、リモート PE に転送されます。**

```
RP/0/RSP1/CPU0:router3#sh l2vpn bridge-domain group customer1
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: finance, id: 4, 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:
BE222.3, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-finance (up)
Neighbor 10.0.0.11 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.12 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 3, state: up, Static MAC addresses: 0
Bridge group: customer1, bridge-domain: engineering, id: 3, 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:
BE222.2, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.11 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0
```

```
RP/0/RSP1/CPU0:router3#sh l2vpn forwarding bridge-domain customer1:
engineering mac location 0/0/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
```

```
l2vpn resynchronize forwarding mac-address-table location
```

```
Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
```

```
-----  
001d.4603.1f01 dynamic BE222.2 0/0/CPU0 0d 0h 0m 0s N/A  
001d.4603.1f42 dynamic BE222.2 0/0/CPU0 0d 0h 0m 0s N/A  
6c9c.ed3e.e46d dynamic (10.0.0.11, 2) 0/0/CPU0 0d 0h 0m 0s N/A  
0019.552b.b5c3 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A
```

最後のコマンドは、router3 がバンドル上で MAC アドレスをいくつか学習しており、アクティブなメンバーが router3 にあることを示しています。router5 では、ローカル メンバーはスタンバイ状態にあるため、バンドル上で学習された MAC アドレスはありません。

```
RP/0/RSP1/CPU0:router5#sh l2vpn forwarding bridge-domain customer1:engineering  
mac location 0/0/CPU0
```

```
To Resynchronize MAC table from the Network Processors, use the command...
```

```
l2vpn resynchronize forwarding mac-address-table location
```

```
Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
```

```
-----  
6c9c.ed3e.e46d dynamic (10.0.0.11, 2) 0/0/CPU0 0d 0h 0m 0s N/A  
0019.552b.b5c3 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A  
001d.4603.1f01 dynamic (10.0.0.13, 2) 0/0/CPU0 0d 0h 0m 0s N/A
```

router3 と router6 の間のバンドル メンバーがダウンした場合、router5 のバンドル メンバーがアクティブになります。リモート PE が自身の MAC アドレス テーブルを消去し、新しいアクティブな MC-LAG PE である router5 経由で MAC アドレスを学習するように、MC-LAG VPLS PE は LDP MAC 回収メッセージを送信します。

アクティブな MC-LAG バンドル メンバーが router3 から router5 に移動したときに、router2 は MAC 回収メッセージを router3 と router5 から受信します。

```
RP/0/RSP0/CPU0:router2#sh l2vpn bridge-domain group customer1 detail |
```

```
i "state is|withd|bridge-domain"
```

```
Bridge group: customer1, bridge-domain: finance, id: 3, state: up,  
ShgId: 0, MSTi: 0
```

```
MAC withdraw: enabled
```

```
MAC withdraw for Access PW: enabled
```

```
MAC withdraw sent on bridge port down: disabled
```

```
AC: GigabitEthernet0/1/0/3.3, state is up
```

```
PW: neighbor 10.0.0.12, PW ID 3, state is up ( established )
```

```
MAC withdraw message: send 0 receive 0
```

```
PW: neighbor 10.0.0.13, PW ID 3, state is up ( established )
```

```
MAC withdraw message: send 0 receive 1
```

```
PW: neighbor 10.0.0.14, PW ID 3, state is up ( established )
```

```
MAC withdraw message: send 0 receive 1
```

```
Bridge group: customer1, bridge-domain: engineering, id: 5, state: up,  
ShgId: 0, MSTi: 0
```

```
MAC withdraw: enabled
```

```
MAC withdraw for Access PW: enabled
```

```
MAC withdraw sent on bridge port down: disabled
```

```
AC: GigabitEthernet0/0/0/1.2, state is unresolved
```

```
AC: GigabitEthernet0/1/0/3.2, state is up
```

```
PW: neighbor 10.0.0.15, PW ID 15, state is up ( established )
```

```
MAC withdraw message: send 2 receive 0
```

```
PW: neighbor 10.0.0.12, PW ID 2, state is up ( established )
```

```
MAC withdraw message: send 0 receive 0
```

```
PW: neighbor 10.0.0.13, PW ID 2, state is up ( established )
```

```
MAC withdraw message: send 0 receive 1
```

```
PW: neighbor 10.0.0.14, PW ID 2, state is up ( established )
```

```
MAC withdraw message: send 0 receive 1
```

router2 の MAC アドレスは router3 ( 10.0.0.13 ) から router5 ( 10.0.0.14 ) に移動します。

```
RP/0/RSP0/CPU0:router2#sh l2vpn forwarding bridge-domain customer1:
engineering mac-address location 0/0/CPU0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location
```

```
Mac Address Type Learned from/Filtered on LC learned Resync Age Mapped to
```

```
-----
6c9c.ed3e.e46d dynamic (10.0.0.15, 15) 0/0/CPU0 0d 0h 0m 0s N/A
0019.552b.b5c3 dynamic (10.0.0.12, 2) 0/0/CPU0 0d 0h 0m 0s N/A
001d.4603.1f02 dynamic (10.0.0.14, 2) 0/0/CPU0 0d 0h 0m 0s N/A
001d.4603.1f42 dynamic (10.0.0.14, 2) 0/0/CPU0 0d 0h 0m 0s N/A
```

MC-LAG では、VPLS を介して他のサイトに接続される単一のバンドルをサイトで使用できます。MC-LAG ではリンクと PE の冗長性が提供されますが、論理的には、他のサイトに到達する 1 つのバンドル インターフェイスのままです。このバンドル上ではスパニング ツリーは必要なく、BPDU が VPLS 経由でサイト間で交換されないように、CE 上で BPDU フィルタを設定できます。

他のオプションとしては、BPDU の宛先 MAC アドレスをドロップして BPDU がサイト間で転送されないようにするために、バンドル上の AC でイーサネットサービスのアクセスリストを設定します。ただし、サイト間にバックドア リンクが導入された場合、スパニング ツリーは MC-LAG バンドル上で実行されないためループを解消することはできません。このため、MC-LAG バンドル上でスパニング ツリーを無効にするかどうか慎重に評価してください。サイト間のトポロジが注意深く維持されている場合は、スパニング ツリーが不要な MC-LAG によって冗長性を実現することをお勧めします。

#### 4.4.7.5 ASR 9000 nV エッジ クラスタ

[MC-LAG ソリューション](#)は、スパニング ツリーを必要とせずに冗長性を実現します。欠点の 1 つは、1 つの MC-LAG PE へのバンドル メンバーがスタンバイ状態になるため、これはアクティブ/スタンバイ ソリューションであり、リンクの使用が最大化されないことです。

別の設計オプションとしては、ASR 9000 nV エッジ クラスタを使用して、すべてが同時にアクティブである、各クラスタ ラックへのバンドル メンバーを CE が持つようにします。

このソリューションのもう 1 つの利点は、各サイトのクラスタについてクラスタごとに PW は 1 つだけであるため、PW の数を削減できることです。サイトごとに PE が 2 つある場合、各 PE には各サイトの 2 つの PE それぞれへの PW が必要です。

設定の簡素化も利点の 1 つです。設定は、バンドル AC と VFI PW を備えたブリッジドメインを使用する非常に基本的な VPLS の設定と似ています。

```
RP/1/RSP0/CPU0:router2#sh bundle bundle-ether 222
```

```
Bundle-Ether222
Status: Up
Local links : 2 / 0 / 2
Local bandwidth : 20000000 (20000000) kbps
MAC address (source): 0024.f71e.d309 (Configured)
Inter-chassis link: No
Minimum active links / bandwidth: 1 / 1 kbps
Maximum active links: 64
Wait while timer: 2000 ms
Load balancing: Default
LACP: Not operational
Flap suppression timer: Off
Cisco extensions: Disabled
```

mLACP: Not configured  
IPv4 BFD: Not configured

Port Device State Port ID B/W, kbps

-----  
Te0/0/0/8 Local Active 0x8000, 0x0005 10000000  
Link is Active  
Tel/0/0/8 Local Active 0x8000, 0x0001 10000000  
Link is Active

```
RP/1/RSP0/CPU0:router2#sh run int bundle-ether 222.2
interface Bundle-Ether222.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
!
```

```
RP/1/RSP0/CPU0:router2#sh run int bundle-ether 222.3
interface Bundle-Ether222.3 l2transport
encapsulation dot1q 3
rewrite ingress tag pop 1 symmetric
!
```

```
RP/1/RSP0/CPU0:router2#sh run l2vpn bridge group customer1
l2vpn
bridge group customer1
bridge-domain finance
interface Bundle-Ether222.3
!
vfi customer1-finance
neighbor 10.0.0.11 pw-id 3
!
neighbor 10.0.0.12 pw-id 3
!
neighbor 10.0.0.13 pw-id 3
!
neighbor 10.0.0.14 pw-id 3
!
!
!
bridge-domain engineering
interface Bundle-Ether222.2
!
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
```

```
RP/1/RSP0/CPU0:router2#sh l2vpn bridge-domain group customer1
```

Legend: pp = Partially Programmed.

Bridge group: customer1, bridge-domain: finance, id: 3, 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: 4 (4 up), PBBs: 0 (0 up)

List of ACs:

```
BE222.3, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-finance (up)
Neighbor 10.0.0.11 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.12 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 3, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 3, state: up, Static MAC addresses: 0
Bridge group: customer1, bridge-domain: engineering, id: 4, 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: 4 (4 up), PBBs: 0 (0 up)
List of ACs:
BE222.2, state: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI customer1-engineering (up)
Neighbor 10.0.0.11 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.12 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.13 pw-id 2, state: up, Static MAC addresses: 0
Neighbor 10.0.0.14 pw-id 2, state: up, Static MAC addresses: 0
```

冗長性は、2つのラックへのバンドル AC のデュアルホームによって実現されるため、バンドルメンバーの障害時またはラックの障害時にバンドルはアップしたままになります。

サイトがクラスタを介してのみ VPLS ドメインに接続されている場合、トポロジはスパニング ツリーに関して MC-LAG に似ています。つまり、バンドル上でスパニング ツリーは必要なく、BPDU が VPLS 経由でサイト間で交換されないように、CE 上で BPDU フィルタを設定できます。

他のオプションとしては、BPDU の宛先 MAC アドレスをドロップして BPDU がサイト間で転送されないようにするために、バンドル上の AC でイーサネットサービスのアクセスリストを設定します。ただし、サイト間にバックドア リンクが導入された場合、スパニング ツリーは CE-PE バンドル上で実行されないためループを解消することはできません。このため、CE-PE バンドル上でスパニング ツリーを無効にするかどうか慎重に評価してください。サイト間のトポロジが注意深く維持されている場合は、スパニング ツリーが不要なクラスタによって冗長性を実現することをお勧めします。

#### 4.4.7.6 ICCP ベース サービス マルチホームिंग (ICCP-SM) (PMCLAG (擬似 MCLAG) とアクティブ/アクティブ)

一部のバンドル リンクが使用されずにスタンバイ モードのままになる MC-LAG の制限を解決するために、バージョン 4.3.1 で導入された新しい機能があります。擬似 MCLAG と呼ばれるこの新機能では、DHD から接続ポイント (PoA) へのすべてのリンクが使用される一方で、VLAN は異なるバンドル間に分散されます。

## 4.5 トラフィック ストーム制御

L2 ブロードキャスト ドメインでは、ホストが誤作動してブロードキャストまたはマルチキャスト フレームを高レートで送信するリスクがあり、これらのフレームはブリッジドメイン全体にフラッディングされます。別のリスクとして L2 ループ (スパニング ツリーによって解消されない) が作られる可能性があり、この場合はブロードキャスト パケットやマルチキャスト パケットがループします。高レートのブロードキャスト パケットやマルチキャスト パケットは、ブロードキャスト ドメインのホストのパフォーマンスに影響します。

ネットワークのスイッチング デバイスのパフォーマンスも、1つの入力フレーム (ブロードキャスト、マルチキャスト、または不明なユニキャスト フレーム) がブリッジドメインの複数の出力ポートに複製されることで、影響を受ける可能性があります。同じパケットのコピーを複数作成すると、パケットを複製するデバイス内の場所によっては、リソースを大量に消費する可能性があります。たとえば、ブロードキャストの複数の異なるスロットへの複製は、ファブリックのマルチキャストレプリケーション機能があるので問題ではありません。ネットワークプロセッサが、処理対象の一部のポートで送信するために同じパケットの複数のコピーを作成する必要がある場合、ネットワークプロセッサのパフォーマンスは影響を受ける可能性があります。

ストームの発生時にデバイスを保護するために、トラフィック ストーム制御機能では、ブリッジドメイン AC で受け入れるブロードキャスト、マルチキャスト、および不明なユニキャストの最大レートを設定できます。詳細については、『[Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ システム セキュリティ コンフィギュレーション ガイド、リリース 4.3.x](#)』の「[VPLS ブリッジでのトラフィック ストーム制御の実装](#)」を参照してください。

トラフィック ストーム制御は、バンドル AC インターフェイスまたは VFI PW ではサポートされませんが、非バンドルの AC およびアクセス PW ではサポートされます。この機能はデフォルトで無効に設定されています。ストーム制御を設定しない場合、任意のレート of ブロードキャスト、マルチキャスト、および不明なユニキャストを受け入れることになります。

次に設定例を示します。

```
RP/0/RSP0/CPU0:router2#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
bridge group customer1
bridge-domain engineering
interface GigabitEthernet0/1/0/3.2
storm-control unknown-unicast pps 10000
storm-control multicast pps 10000
storm-control broadcast pps 1000
!
neighbor 10.0.0.15 pw-id 15
storm-control unknown-unicast pps 10000
storm-control multicast pps 10000
storm-control broadcast pps 1000
!
vfi customer1-engineering
neighbor 10.0.0.10 pw-id 2
!
neighbor 10.0.0.12 pw-id 2
!
neighbor 10.0.0.13 pw-id 2
!
neighbor 10.0.0.14 pw-id 2
!
!
!
!
!
```

```
RP/0/RSP0/CPU0:router2#sh l2vpn bridge-domain bd-name engineering det
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 5, 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 down: 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 profile: none
Bridge MTU: 1500
MIB cvplsConfigIndex: 6
Filter MAC addresses:
Create time: 28/05/2013 17:17:03 (1w1d ago)
No status change since creation
ACs: 1 (1 up), VFI: 1, PWs: 5 (5 up), PBBs: 0 (0 up)
List of ACs:
AC: GigabitEthernet0/1/0/3.2, state is up
Type VLAN; Num Ranges: 1
VLAN ranges: [2, 2]
MTU 1500; XC ID 0xc40007; 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 profile: none
Storm Control:
  Broadcast: enabled(1000)
  Multicast: enabled(10000)
  Unknown unicast: enabled(10000)
Static MAC addresses:
Statistics:
packets: received 251295, sent 3555258
bytes: received 18590814, sent 317984884
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
<snip>
```

ストーム制御のドロップカウンタは、**show l2vpn bridge-domain detail** コマンドの出力に常に表示されます。この機能はデフォルトで無効になっているため、この機能が設定された場合にのみ、カウンタはドロップの報告を開始します。

設定するレートは、1つのネットワークから別のネットワークへのトラフィックパターンによって異なる場合があります。レートを設定する前に、通常の状態でのブロードキャスト、マルチキャスト、または不明なユニキャストフレームのレートについて理解しておくことを推奨します。



その後、通常のレートに、設定するレートのマージンを追加します。

## 4.6 MAC の移動

インターフェイス フラップなど、ネットワークが不安定な場合、MAC アドレスが新しいインターフェイスから学習されることがあります。これは正常なネットワーク収束であり、MAC アドレス テーブルは動的に更新されます。

ただし、絶え間ない MAC 移動は、多くの場合、L2 ループ中の重大な不安定性などのネットワークの不安定さを示しています。MAC アドレスのセキュリティ機能を使用すると、MAC 移動の報告と、問題のあるポートのシャットダウンなどの修正措置を行うことができます。

修正措置を設定しない場合でも、**logging** コマンドを設定することで、MAC 移動メッセージを介してネットワーク不安定性に関するアラートを受け取ることができます。

```
l2vpn
bridge group customer1
bridge-domain engineering
mac
secure
action none
logging
!
```

この例では、アクションが none に設定されているため、MAC 移動が検出されても、Syslog メッセージの記録以外は何も実行されません。メッセージの例を次に示します。

```
LC/0/0/CPU0:Dec 13 13:38:23.396 : l2fib[239]:
%L2-L2FIB-5-SECURITY_MAC_SECURE_VIOLATION_AC : MAC secure in AC
GigabitEthernet0_0_0_4.1310 detected violated packet - source MAC:
0000.0000.0001, destination MAC: 0000.0001.0001; action: none
```

## 4.7 IGMP と MLD スヌーピング

デフォルトでは、マルチキャスト フレームはブリッジドメインのすべてのポートにフラッディングされます。IP テレビ (IPTV) サービスなどの高レートのストリームを使用している場合、大量のトラフィックが全ポートに転送され、複数の PW に複製される可能性があります。すべての TV ストリームが 1 つのインターフェイス上で転送されると、ポートが輻輳する可能性があります。唯一のオプションは、IGMP や MLD スヌーピングなどの機能を設定することです。これらは、受信者やマルチキャスト ルータを追跡したり、適切な場合にのみポートでストリームを転送したりするために、マルチキャスト制御パケットを受信します。

これらの機能の詳細については、『[Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ マルチキャスト コンフィギュレーション ガイド、リリース 4.3.x](#)』を参照してください。

## 5. その他の L2VPN のトピック

注：

このセクションで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ( [登録ユーザ専用](#) ) を使用してください。

特定の show コマンドが [アウトプット インタープリタ ツール \(登録ユーザ専用\)](#) でサポートされています。show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

## 5.1 ロードバランシング

L2VPN PE が MPLS PW 上でフレームを送信する必要がある場合、イーサネット フレームは、1 つ以上の MPLS ラベルの付いた MPLS フレームにカプセル化されます。リモート PE に到達するために、少なくとも 1 つの PW ラベルと、場合によっては IGP ラベルが付けられます。

MPLS フレームは、リモート L2VPN PE に MPLS ネットワークで転送されます。通常、宛先 PE に到達するパスは複数あります。

注: この図では、すべてのリンクを表してはいません。

PE1 は、PE2 への最初の MPLS P ルータとして P1 または P2 を選択できます。P1 を選択した場合、PE1 は次に P3 または P4 を選択し、その後も同様です。使用可能なパスは、IGP トポロジと MPLS TE トンネル パスに基づきます。

MPLS サービス プロバイダーでは、1 つのリンクを混雑させて他のリンクを活用しないことよりも、すべてのリンクが均等に使用されることが望まれます。この目標は常に簡単に達成できるとは限りません。一部の PW は他よりもはるかに多くのトラフィックを伝送し、PW のトラフィックによって使用されるパスは、コアで使用されるハッシュ アルゴリズムに依存するためです。高帯域幅の複数の PW が同じリンクにハッシュされる可能性があり、これによって輻輳が発生します。

非常に重要な要件は、1 つのフローのすべてのパケットが同じパスを通るようにすることです。そうしない場合、順序が不正なフレームが発生し、これによってアプリケーションの品質やパフォーマンスに影響が生じる可能性があります。

シスコ ルータの MPLS ネットワークのロード バランシングは、一般的に、最後の MPLS ラベルに続くデータに基づいて行われます。

- 最後のラベルの直後のデータが 0x4 または 0x6 で始まる場合、MPLS P ルータは、MPLS パケットの内部には IPv4 または IPv6 のパケットがあると判断し、このフレームから抽出した送信元と宛先の IPv4 または IPv6 アドレスのハッシュに基づいてロードバランシングを試みます。理論的には、PW 上でカプセル化されて転送されるイーサネット フレームの場合、最後のラベルの後には宛先 MAC アドレスが続くので、これは適用されません。しかし最近では、0x4 および 0x6 で始まるいくつかの MAC アドレスの範囲が割り当てられています。MPLS P ルータは、イーサネット ヘッダーを実際は IPv4 ヘッダーであると誤って認識し、IPv4 の送信元アドレスと宛先アドレスであると想定されるデータに基づいてフレームをハッシュする可能性があります。PW のイーサネット フレームは MPLS コア内のさまざまなパスにハッシュされる可能性があり、これは PW フレームの順序不正やアプリケーションの品質の問題につながります。解決策は、ポイントツーポイントまたは VPLS PW に追加可能なコントロールワードを pw-class の下で設定することです。コントロールワードは、MPLS ラベルの直後に挿入されます。コントロールワードは 0x4 または 0x6 で始まらないため、上記の問題を回避できます。

```

RP/1/RSP0/CPU0:router#sh run l2vpn bridge group customer1 bridge-domain
engineering
l2vpn
pw-class control-word
encapsulation mpls
control-word
!
!
bridge group customer1
bridge-domain engineering
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
pw-class control-word
!
<snip>
RP/1/RSP0/CPU0:router#sh l2vpn bridge-domain bd-name engineering det
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 4, state: up,
ShgId: 0, MSTi: 0
<snip>
List of VFIs:
VFI customer1-engineering (up)
PW: neighbor 10.0.0.11, PW ID 2, state is up ( established )
PW class control-word, XC ID 0xc000000a
Encapsulation MPLS, protocol LDP
Source address 10.0.0.10
PW type Ethernet, control word enabled, interworking none
Sequencing not set

```

```

PW Status TLV in use
MPLS Local Remote

```

```

-----
Label 281708 16043
Group ID 0x4 0x5
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word enabled enabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x7 0x7
(control word) (control word)
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
-----

```

- 最後の MPLS ラベル スタック直後のデータが 0x4 または 0x6 で始まっていない場合、P ルータは最後のラベルに基づいてロードバランシングを行います。1つのPWからのすべてのトラフィックは同じパスを使うため、順序が不正なパケットは発生しませんが、高帯域幅のPWの場合は一部のリンクがこれによって輻輳する可能性があります。Cisco IOS XR ソフトウェア リリース 4.2.1 を搭載する ASR 9000 は、Flow Aware Transport ( FAT ) PW 機能をサポートします。この機能は L2VPN PE で実行され、ポイントツーポイントまたは VPLS PW の 2 つの端の間でネゴシエートします。入力側の L2VPN PE は、AC 上のフローと L2VPN の設定を検出すると、MPLS ラベル スタックの最後の PW MPLS ラベルの下に新しい MPLS フロー ラベルを挿入します。入力側の PE は、送信元と宛先の MAC アドレス ( デフォルト ) または送信元と宛先の IPv4 アドレス ( 設定可能 ) に基づいてフローを検出します。MAC アドレスの使用がデフォルトです。IPv4 アドレスの使用が推奨されますが、手動で設定する必要があります。

入力側の L2VPN PE は、FAT PW 機能を使用して、src-dst-mac ごとまたは src-dst-ip ごとに 1 つの MPLS ラベルを最後に挿入します。( PE の間の ) MPLS P ルータは、使用可能なパス上でフレームをハッシュし、MPLS スタックの最後の FAT PW フロー ラベルに基づいて宛先 PE に到達します。これは一般的に、少数の src-dst-mac または src-dst-ip のメッセージ交換のみを PW が伝送する場合を除き、コアにおいて非常に優れた帯域幅利用を実現します。フロー ラベルの直後の 0x4 および 0x6 で始まる MAC アドレスを回避できるように、コントロールワードを使用することが推奨されます。これにより、ハッシュが擬似 IP アドレスに正しく基づくようにし、フロー ラベルには基づかないようにできます。

この機能により、1 つの PW からのトラフィックは、可能な場合はコア内の複数のパスの間でロードバランシングされます。同じ送信元 ( MAC または IP ) から同じ宛先 ( MAC または IP ) へのすべてのトラフィックは同じパスを通るため、アプリケーショントラフィックは、順序が不正なパケットの影響を受けません。

次に設定例を示します。

```
l2vpn
pw-class fat-pw
encapsulation mpls
control-word
load-balancing
flow-label both
!
!
!
bridge group customer1
bridge-domain engineering
vfi customer1-engineering
neighbor 10.0.0.11 pw-id 2
pw-class fat-pw
```

```
RP/1/RSP0/CPU0:router#sh l2vpn bridge-domain bd-name engineering det
Legend: pp = Partially Programmed.
Bridge group: customer1, bridge-domain: engineering, id: 4, state: up,
ShgId: 0, MSTi: 0
<snip>
List of VFIs:
VFI customer1-engineering (up)
PW: neighbor 10.0.0.11, PW ID 2, state is up ( established )
PW class fat-pw, XC ID 0xc000000a
Encapsulation MPLS, protocol LDP
Source address 10.0.0.10
PW type Ethernet, control word enabled, interworking none
Sequencing not set
Load Balance Hashing: src-dst-ip
Flow Label flags configured (Tx=1,Rx=1), negotiated (Tx=1,Rx=1)

PW Status TLV in use
MPLS Local Remote
-----
Label 281708 16043
Group ID 0x4 0x5
Interface customer1-engineering customer1-engineering
MTU 1500 1500
Control word enabled enabled
PW type Ethernet Ethernet
VCCV CV type 0x2 0x2
(LSP ping verification) (LSP ping verification)
VCCV CC type 0x7 0x7
```

```
(control word) (control word)
(router alert label) (router alert label)
(TTL expiry) (TTL expiry)
-----
```

## 5.2 ログイング

L2VPN コンフィギュレーション モードでは、さまざまな種類のログイング メッセージを設定できます。L2VPN イベントの Syslog アラートを受信するための l2vpn ログイングの設定と、PW のステータスがいつ変わったのかを知るための擬似回線のログイングの設定を行います。

```
l2vpn
logging
bridge-domain
pseudowire
nsr
!
```

多くの PW が設定されている場合、ログにメッセージがあふれる可能性があります。

## 5.3 イーサネットサービス アクセスリスト

特定のホストからのトラフィックをドロップしたり、ホストからのパケットをルータが l2transport インターフェイスで取得していることを検証したりするために、イーサネットサービス アクセスリストを使用できます。

```
RP/0/RSP0/CPU0:router#sh run ethernet-services access-list count-packets
ethernet-services access-list count-packets
10 permit host 001d.4603.1f42 host 0019.552b.b5c3
20 permit any any
!
```

```
RP/0/RSP0/CPU0:router#sh run int gig 0/1/0/3.2
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
ethernet-services access-group count-packets egress
!
```

```
RP/0/RSP0/CPU0:router#sh access-lists ethernet-services count-packets
hardware egress location 0/1/CPU0
ethernet-services access-list count-packets
10 permit host 001d.4603.1f42 host 0019.552b.b5c3 (5 hw matches)
20 permit any any (30 hw matches)
```

ハードウェアの一致は *hardware* キーワードでのみ確認することができます。アクセスグループの方向によって、*ingress* キーワードまたは *egress* キーワードを使用します。アクセスリストが適用されるインターフェイスのラインカードの場所も指定します。

セキュリティまたはトラブルシューティングの機能として、l2transport インターフェイスに IPv4 アクセスリストを適用することもできます。

```
RP/0/RSP0/CPU0:router#sh run ipv4 access-list count-pings
ipv4 access-list count-pings
10 permit icmp host 192.168.2.1 host 192.168.2.2
20 permit ipv4 any any
!
```

```
RP/0/RSP0/CPU0:router#sh run int gig 0/1/0/3.2
```

```
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
rewrite ingress tag pop 1 symmetric
ipv4 access-group count-pings ingress
!
```

```
RP/0/RSP0/CPU0:router#sh access-lists ipv4 count-pings hardware ingress
location 0/1/CPU0
ipv4 access-list count-pings
10 permit icmp host 192.168.2.1 host 192.168.2.2 (5 hw matches)
20 permit ipv4 any any (6 hw matches)
```

## 5.4 イーサネット出力フィルタ

AC の出力方向において、出力 VLAN タグを決定する `rewrite ingress tag pop <> symmetric` コマンドがないと仮定します。この場合、出力されるフレームが `encapsulation` コマンドに従って正しい VLAN タグを持っていることを確認するチェックは行われません。

次に設定例を示します。

```
interface GigabitEthernet0/1/0/3.2 l2transport
encapsulation dot1q 2
!
interface GigabitEthernet0/1/0/3.3 l2transport
encapsulation dot1q 3
!
interface GigabitEthernet0/1/0/39.2 l2transport
encapsulation dot1q 2
!
l2vpn
bridge group customer2
bridge-domain test
interface GigabitEthernet0/1/0/3.2
!
interface GigabitEthernet0/1/0/3.3
!
interface GigabitEthernet0/1/0/39.2
!
!
!
!
```

この設定では、次の点に注意してください。

- `rewrite ingress` コマンドがないため、GigabitEthernet0/1/0/39.2 で dot1q タグ 2 を伴って受信されたブロードキャストは、着信タグを維持します。
- このブロードキャストは、dot1q タグ 2 を伴って GigabitEthernet0/1/0/3.2 からフラッディングされますが、GigabitEthernet0/1/0/3.2 には dot1q タグ 2 が設定されているため、これによって問題が生じることはありません。
- このブロードキャストは GigabitEthernet0/1/0/3.3 からフラッディングされますが、GigabitEthernet0/1/0/3.3 には `rewrite` コマンドがないため、元のタグ 2 が維持されます。GigabitEthernet0/1/0/3.3 の `encapsulation dot1q 3` コマンドは、出力方向ではチェックされません。
- 結果として、GigabitEthernet0/1/0/39 でタグ 2 を伴って受信された 1 つのブロードキャストについて、GigabitEthernet0/1/0/3 から出力されるタグ 2 を持つ 2 つのブロードキャストが生じます。この重複するトラフィックによって、アプリケーションの問題が発生する可能性があります。

- 解決策は、サブインターフェイスから離れるパケットが正しい VLAN タグを持つように、*ethernet egress-filter strict* を設定することです。 そうしない場合、パケットは転送されず、ドロップされます。

```
interface GigabitEthernet0/1/0/3.2 l2transport
ethernet egress-filter strict
!
interface GigabitEthernet0/1/0/3.3 l2transport
ethernet egress-filter strict
!
```