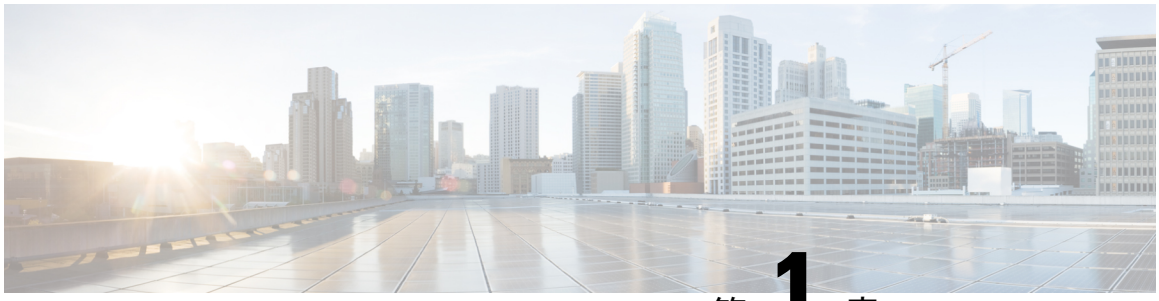
Cisco NCS 560 シリーズ ルータ（IOS XR リリース 7.1.x）L2VPN およびイーサネット サービス コンフィギュレーション ガイド

初版：2020 年 1 月 29 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

レイヤ 2 仮想プライベート ネットワークの概要

レイヤ 2 仮想プライベート ネットワーク（VPN）は、2 つのポイント間にプライベート接続を作成することによって IP ネットワークまたは MPLS ネットワーク内で物理サブネットワークをエミュレートします。L2VPN ネットワークを構築するには、サービス プロバイダーとカスタマー間での調整が必要です。サービス プロバイダーがレイヤ 2 接続を確立します。カスタマーは、サービス プロバイダーから取得したデータ リンク リソースを使用することによってネットワークを構築します。L2VPN サービスでは、サービス プロバイダーはカスタマーのネットワーク トポロジに関する情報やその他の情報を必要としません。これにより、サービス プロバイダーのリソースを使用してネットワークを確立する際にカスタマーのプライバシーが維持されます。

サービス プロバイダーには、次の機能を持つプロバイダー エッジ（PE）ルータが必要です。

- レイヤ 3（L3）パケット内への L2 プロトコル データ ユニット（PDU）のカプセル化。
- any-to-any L2 転送のインターコネクト。
- MPLS トンネリング メカニズムのサポート。
- 回線およびそれらの接続に関連するすべての情報を含むプロセス データベース。

この項では、レイヤ 2 仮想プライベート ネットワーク（VPN）と対応するギガビット イーサネット サービスの概要を示します。

ギガビット イーサネット インターフェイス上のレイヤ 2 VPN の概要

L2VPN ネットワークによって、サービス プロバイダー（SP）は地理的に離れたカスタマー サイトにも L2 サービスを提供できます。通常、SP はアクセス ネットワークを使用して、カスタマーをコア ネットワークに接続します。このアクセス ネットワークでは、イーサネット、フレーム リレーなどの L2 テクノロジーが併用される場合があります。カスタマー サイトと近接した SP エッジルータ間の接続は、接続回線（AC）と呼ばれます。カスタマーからのトラフィックは、このリンク上で SP コア ネットワークのエッジへ伝送されます。次に、SP コア ネットワーク上の疑似接続のトンネルを介して、別のエッジルータへ伝送されます。このトラフィックはエッジ ルータによって別の AC へと伝送され、そこからカスタマーのリモート サイトへ伝送されます。

L2VPN の機能によって、異なる種類の L2 接続回線と疑似回線間の接続が可能になります。その結果、ユーザはさまざまなエンドツーエンド サービスを実装できるようになります。

（注） 任意のタイプの疑似回線を介した BOOTP トラフィック（dst UDP 68）はサポートされていません。

Cisco IOS XR ソフトウェアは、2 つのイーサネット回線が接続されている、ポイントツーポイントおよびエンドツーエンド サービスをサポートしています。L2VPN イーサネット ポートは、次の 2 モードのいずれかで動作します。

- ポート モード：このモードでは、ポートに到達するすべてのパケットは、パケットに指定されている VLAN タグに関係なく、疑似回線上で送信されます。VLAN モードでは、l2transport コンフィギュレーション モードで設定が実行されます。
- VLAN モード：CE（カスタマー エッジ）の各 VLAN または PE（プロバイダー エッジ）リンクへのアクセス ネットワークは個別の L2VPN 接続として設定できます（VC タイプ 4 または VC タイプ 5 を使用する）。VLAN 上で L2VPN を設定する方法については、このマニュアルで後述する「キャリア イーサネット モデル」の章を参照してください。VLAN モードでは、個別のサブインターフェイスで設定を実行します。

スイッチングは次の方法で実行できます。

- AC-to-PW：PE に到達したトラフィックは PW（疑似回線）を介してトンネリングされます（反対に、PW を介して到達したトラフィックは AC を介して送信されます）。これが最も一般的なシナリオです。
- ローカルの切り替え - 1 つの AC 上で到達するトラフィックは、疑似接続を介さずに別の AC へ送出されます。
- PW 切り替え - PW に到達するトラフィックは AC へ送信されませんが、別の PW 上でコアに返信されます。

（注）

- ネットワークの要件として、パケットを透過的に伝送することが必須の場合は、サービスプロバイダー（SP）ネットワークのエッジにおいてパケットの宛先 MAC（メディア アクセス コントロール）アドレスを変更することが必要になる可能性があります。こうすることで、SP ネットワークのデバイスによるパケットの消費が回避されます。
- **encapsulation dot1ad** *vlan-id* コマンドと **encapsulation dot1ad** *vlan-id* **dot1q any** コマンドは、同じ物理インターフェイスまたはバンドルインターフェイス上に共存させることはできません。同様に、**encapsulation dot1q** *vlan-id* コマンドと **encap dot1q** *vlan-id* **second-dot1q any** コマンドも、同じ物理インターフェイスまたはバンドルインターフェイス上に共存させることはできません。共存の必要が生じた場合は、単一タグのカプセル化で exact キーワードを使用することをお勧めします。たとえば、**encap dot1ad** *vlan-id* **exact**、**encap dot1q** *vlan-id* **exact** などとします。
- すでに QinQ が設定されているインターフェイスでは、QRangeinQ の外部 VLAN 範囲が QinQ の外部 VLAN と重複する QRangeinQ サブインターフェイスを設定することはできません。この設定を行おうとすると、既存の QinQ および QinQRange インターフェイスが分割されます。ただし、最近設定した QinQRange インターフェイスを削除すればシステムを回復できます。
- すでに QinQRange 設定があるインターフェイスでは、QRangeinQ の外部 VLAN 範囲が QinQRange の内部 VLAN と重複する QRangeinQ サブインターフェイスを設定することはできません。この設定を行おうとすると、既存の QinQ および QinQRange インターフェイスが分割されます。ただし、最近設定した QinQRange インターフェイスを削除すればシステムを回復できます。
- 設定されたサブインターフェイスの内部 VLAN 範囲は、重複する値を持つことはできません。内部 VLAN 範囲ｶﾞ重複する場合、Cisco IOS XR リリース 6.5.x で LC をリロードすると、システムを回復できます。

AC と疑似回線情報を表示するには、**show interfaces** コマンドを使用します。

レイヤ2転送のギガビットイーサネットインターフェイスの設定

この項では、レイヤ 2 転送にギガビット イーサネット インターフェイスを設定する方法について説明します。

設定例

```
/* Enter the interface configuration mode */
Router# configure
Router(config)# interface TenGigE 0/0/0/10
```

```
/* Configure the ethertype for the 802.1q encapsulation (optional) */
/* For VLANs, the default ethertype is 0x8100. In this example, we configure a value of
 0x9100.
/* The other assignable value is 0x9200 */
/* When ethertype is configured on a physical interface, it is applied to all
sub-interfaces created on this interface */

Router(config-if)# dot1q tunneling ethertype 0x9100

/* Configure Layer 2 transport on the interface, and commit your configuration */
Router(config-if)# l2transport
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# commit
```

実行コンフィギュレーション

```
configure
 interface TenGigE 0/0/0/10
  dot1q tunneling ethertype 0x9100
  l2transport
 !
```

確認

10 ギガビット イーサネット インターフェイスが起動しており、動作できる状態であることを確認します。

```
router# show interfaces TenGigE 0/0/0/10

...
TenGigE0/0/0/10 is up, line protocol is up
  Interface state transitions: 1
  Hardware is TenGigE, address is 0011.1aac.a05a (bia 0011.1aac.a05a)
  Layer 1 Transport Mode is LAN
  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, link type is force-up
  output flow control is off, input flow control is off
  Carrier delay (up) is 10 msec
  loopback not set,
  ...
```

関連コマンド

- l2transport（イーサネット）

イーサネット データ プレーン ループバック

イーサネット データ プレーン ループバック機能は、イーサネット ポートのスループットをリモートでテストするための手段を提供します。フレーム損失なしでフレーム転送の最大速度を確認できます。この機能では、双方向または単方向のスループット測定、およびオンデマンドまたはサービス ターンアップ時のアウトオブサービス（割り込み）動作が可能です。この機能は、2 つのタイプのイーサネット ループバックをサポートしています。

- 外部ループバック：入力インターフェイスでトラフィック ループバックが実行されます。トラフィックはループバック用のルータにフローしません。
- 内部ループバック：出力インターフェイスでトラフィック ループバックが実行されます。トラフィック ループバックはトラフィックが別のインターフェイスへのルータにフローした後で実行されます。

イーサネット データ トラフィックはポートごとにループバックできます。この機能は、システムごとに最大 100 の同時イーサネット データ プレーン ルックバック セッションをサポートしています。フレーム ヘッダーに基づくフィルタを使用してループバック セッションを開始できます。これにより、インターフェイス上で受信されるトラフィックのサブセットのみがループバックされます。送信元 MAC、宛先 MAC、および VLAN 優先順位（COS ビット）をフィルタとして使用できます。

内部イーサネット データ プレーン ループバック機能はサポートされていません。

- N540-28Z4C-SYS-A
- N540-28Z4C-SYS-D
- N540X-16Z4G8Q2C-A
- N540X-16Z4G8Q2C-D
- N540-12Z20G-SYS-A
- N540-12Z20G-SYS-D
- N540X-12Z16G-SYS-A
- N540X-12Z16G-SYS-D

イーサネット データ プレーン ループバック設定の制限事項

イーサネット データプレーン ループバックでは、次の制約事項が設定に適用されます。

- イーサネット データ プレーン ループバックは、L3 インターフェイス上または L3 サブインターフェイス上ではサポートされていません。
- 次のフィルタはサポートされていません。
  - 外部 VLAN または外部 VLAN の範囲
  - 内部 VLAN または内部 VLAN の範囲

- イーサネット タイプ

- 外部ループバックでは、次のフィルタの組み合わせのみがサポートされています。
  - 送信元 MAC
  - 送信元 MAC と宛先 MAC
  - 送信元 MAC、宛先 MAC、および VLAN 優先順位
  - 宛先 MAC
  - 宛先 MAC と VLAN 優先順位

- ループバック トラフィックの書き換え変更はサポートされていません。

（注） サブインターフェイスでリライトを設定する必要がないことを確認します。

- イーサネット データ プレーン ループバックは、ブロードキャスト MAC アドレスとしての宛先アドレスを持つパケット上ではサポートされていません。
- イーサネット データ プレーン ループバックは、BVI インターフェイス上ではサポートされていません。
- イーサネット データ プレーン ループバックは、Cisco IOS XR リリース 6.3.2 のブリッジドメイン インターフェイスではサポートされていません。

  レイヤ 2 VPN ブリッジドメインの内部ループバックはサポートされていません。
- 所定のインスタンスでアクティブにできるイーサネット ループバック セッションは内部または外部のいずれか 1 つのみです。
- この機能は、すべてのセッション上の内部ループバックで最大 10 gbps のスループットをサポートします。外部ループバックの場合はスループットの制限はありません。
- 非ループバック方向で受信したパケットのドロップはサポートされていません。
- イーサネット データ プレーン ループバックは、マルチキャストおよびブロードキャスト MAC アドレスとしての宛先があるパケット上ではサポートされていません。
- 外部および内部イーサネット データ プレーン ループバックは、ブリッジ ドメイン経由ではサポートされていません。
- Cisco NCS 560 シリーズ ルータは、レイヤ 2 VPN ブリッジドメイン上のイーサネット ループバック（外部および内部）をサポートしていません。

イーサネット データ プレーン ループバックの設定

この項では、物理インターフェイスとサブインターフェイス上にイーサネット データ プレーン ループバックを設定する方法について説明します。イーサネット データ プレーン ループバックの設定には、次のステップを実行します。

- イーサネット データ プレーン外部ループバックの設定
- イーサネット データ プレーン ループバック セッションの開始

設定例

```
/* Configuring Ethernet Data Plane External Loopback */

/* On physical interface */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tenGigE 0/0/0/0 l2transport
RP/0/RSP0/CPU0:router(config-subif)# ethernet loopback permit external

/* Starting an Ethernet Data Plane Loopback Session  */

RP/0/RSP0/CPU0:router# ethernet loopback start local interface tenGigE 0/0/0/0 external
 source mac-address 0000.0000.0001 destination mac-address 0000.0000.0002 cos 5 timeout
 none


/* On physical sub-interface */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tenGigE 0/2/0/0/0.1 l2transport
RP/0/RSP0/CPU0:router(config-subif)# encapsulation dot1q 100
RP/0/RSP0/CPU0:router(config-subif)# ethernet loopback permit external

/* Starting an Ethernet Data Plane Loopback Session  */

RP/0/RSP0/CPU0:router# ethernet loopback start local interface tenGigE 0/2/0/0/0.1
external source mac-address 0000.0000.0001 destination mac-address 0000.0000.0002 cos 5
 timeout none

/* Configuring Ethernet Data Plane Internal Loopback */

/* On physical interface

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tenGigE 0/0/0/1 l2transport
RP/0/RSP0/CPU0:router(config-subif)#  ethernet loopback permit internal

/* Starting an Ethernet Data Plane Loopback Session  */

RP/0/RSP0/CPU0:router# ethernet loopback start local interface tenGigE 0/0/0/1 internal
 source mac-address 0000.0000.0002 destination mac-address 0000.0000.0003 cos 5 timeout
 none


/* On physical sub-interface */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tenGigE 0/2/0/0/0.1 l2transport
RP/0/RSP0/CPU0:router(config-subif)# encapsulation dot1q 100
```

```
RP/0/RSP0/CPU0:router(config-subif)# ethernet loopback permit internal

/* Starting an Ethernet Data Plane Loopback Session  */

RP/0/RSP0/CPU0:router# ethernet loopback start local interface tenGigE 0/2/0/0/0.1
internal source mac-address 0000.0000.0002 destination mac-address 0000.0000.0003 cos 5
 timeout none



/* Stopping an Ethernet Data Plane Loopback Session */

RP/0/RSP0/CPU0:router# ethernet loopback stop local interface tenGigE 0/0/0/0 id 1
RP/0/RSP0/CPU0:router# ethernet loopback stop local interface tenGigE 0/0/0/1 id 2
RP/0/RSP0/CPU0:router# ethernet loopback stop local interface tenGigE 0/2/0/0/0.1 id 1
```

同様に、バンドル インターフェイスとバンドル サブインターフェイスにイーサネット データ プレーン ループバック セッションを設定できます。

イーサネット ループバックは、SSO の後でも動作します。

実行コンフィギュレーション

この項では、イーサネット データ プレーン ループバックの実行コンフィギュレーションを示します。

```
/* External Loopback */

/* On physical interface */

configure
 interface interface tenGigE 0/0/0/0 l2transport
  ethernet loopback permit external
 !

/* On physical sub-interface */

configure
 interface interface tenGigE 0/2/0/0/0.1 l2transport
  encapsulation dot1q 100
  ethernet loopback permit external
 !



/* Internal Loopback */

/* On physical interface */

configure
 interface interface tenGigE 0/0/0/1 l2transport
  ethernet loopback permit internal
 !

/* On physical sub-interface */

configure
 interface interface tenGigE 0/2/0/0/0.1 l2transport
  encapsulation dot1q 100
  ethernet loopback permit internal
```

```
!
```

確認

次に、インターフェイスごとのループバック機能の例を示します。次の出力には、内部ループバックは 10 ギガビット イーサネット 0/0/0/1 インターフェイス上で、外部ループアックは 10 ギガビットイーサネット0/0/0/0インターフェイス上で許可されていることが示されています。

```
RP/0/RSP0/CPU0:router# show ethernet loopback permitted

--------------------------------------------------------------------------------
Interface                                 Dot1q(s)                      Direction
--------------------------------------------------------------------------------
tenGigE 0/0/0/1.1                          100                            Internal
tenGigE 0/0/0/0.1                          100                            External
--------------------------------------------------------------------------------


/* This example shows all active sessions on the router */

RP/0/RSP0/CPU0:router# show ethernet loopback active
Thu Jul 20 11:00:57.864 UTC
Local: TenGigE0/0/0/0.1, ID 1
============================================
Direction:                           External
Time out:                                None
Time left:                                  -
Status:                               Active
Filters:
  Dot1Q:                                 Any
  Second-dot1Q:                          Any
  Source MAC Address:                    Any
  Destination MAC Address:               Any
  Class of Service:                      Any
Local: TenGigE0/0/0/0.1, ID 2
============================================
Direction:                           External
Time out:                                None
Time left:                                  -
Status:                               Active
Filters:
  Dot1Q:                                 Any
  Second-dot1Q:                          Any
  Source MAC Address:          0000.0000.0001
  Destination MAC Address:     0000.0000.0002
  Class of Service:                         5
```

関連項目

- イーサネット データ プレーン ループバック （5 ページ）

関連コマンド

- ethernet loopback

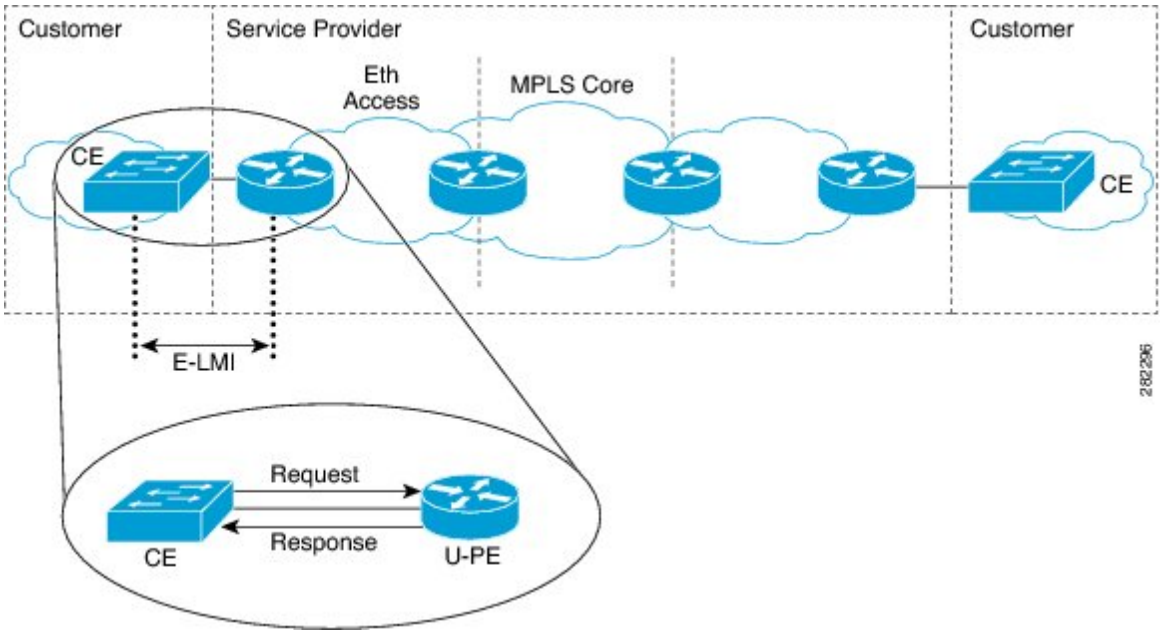
- show ethernet loopback

イーサネット ローカル管理インターフェイス（E-LMI）

Cisco NCS 540 シリーズ ルータは、『*Metro Ethernet Forum, Technical Specification MEF 16, Ethernet Local Management Interface (E-LMI), January 2006* standard』で定義されているイーサネット ローカル管理インターフェイス（E-LMI）プロトコルをサポートしています。

E-LMI はカスタマー エッジ（CE）デバイスとプロバイダー エッジ（PE）デバイス間のリンク、またはユーザ ネットワーク インターフェイス（UNI）で動作し、PE デバイスによって提供されるサービスを、CE デバイスで自動設定またはモニタする方法を提供します（次の図を参照）。

図 *1 : CE-to-PE* リンクでの *E-LMI* 通信



E-LMI は、CE からユーザ側 PE（uPE）に送信されたステータス問い合わせメッセージの応答にステータス メッセージを使用して、CE への接続ステータスおよび設定パラメータを提供する uPE デバイスを必要とする基本動作を行う非対称プロトコルです。

E-LMI メッセージング

MEF 16 規格で定義されているように E-LMI プロトコルは、2 つのメッセージ タイプ（ステータス問い合わせとステータス）だけの使用を定義します。

これらの E-LMI メッセージは情報要素という必須およびオプションのフィールドで構成され、すべての情報要素が、割り当て済み識別子に関連付けられます。すべてのメッセージには、プ

ロトコル バージョン、メッセージ タイプ、およびレポート情報要素が含まれ、その後に情報要素とサブ情報要素が続きます。

E-LMI メッセージは、IEEE 802.3 タグなし MAC フレーム形式に基づく 46 ～ 1500 バイトのイーサネット フレームにカプセル化されます。E-LMI フレームは次のフィールドがあります。

- 宛先アドレス（6 バイト）：標準の MAC アドレスである 01:80:C2:00:00:07 を使用します。
- 送信元アドレス（6 バイト）：送信側デバイスまたはポートの MAC アドレス。
- E-LMI Ethertype（2 バイト）：88-EE を使用します。
- E-LMI PDU（46 ～ 1500 バイト）：最小 46 バイト長を満たす必要があれば、データに 0x00 のパディングを足します。
- CRC（4 バイト）：エラー検出用の巡回冗長検査。

E-LMI メッセージおよびサポートされる情報要素の詳細については、『Ethernet Forum, Technical Specification MEF 16, Ethernet Local Management Interface (E-LMI), January 2006』を参照してください。

E-LMI メッセージは次の製品ではサポートされていません。

- N540-28Z4C-SYS-A
- N540-28Z4C-SYS-D
- N540X-16Z4G8Q2C-A
- N540X-16Z4G8Q2C-D
- N540-12Z20G-SYS-A
- N540-12Z20G-SYS-D
- N540X-12Z16G-SYS-A
- N540X-12Z16G-SYS-D

E-LMI 動作

E-LMI の基本動作は、定期的にステータス問い合わせメッセージを PE デバイスに送信する CE デバイスで構成されます。このメッセージに続いて、PE デバイスによって、要求された情報を含むステータス メッセージ応答が行われます。CE と PE 間のステータス問い合わせおよびステータス メッセージを関連付けるためにシーケンス番号が使用されます。

CE は、レポート タイプと呼ばれる、ステータス問い合わせメッセージの次の 2 つのフォームを送信します。

- E-LMI チェック：PE を使用してデータ インスタンス（DI）番号を検証し、CE に最新の E-LMI 情報があることを確認します。
- フル ステータス：UNI とすべての EVC に関する PE からの情報を要求します。

CE デバイスはステータス問い合わせメッセージの送信を追跡するためにポーリング タイマーを使用しますが、PEデバイスはポーリング検証タイマー（PVT）を使用することもできます。これは、PE のステータス メッセージが送信されてから CE デバイスからのステータス問い合わせが受信されるまでの許容時間を指定するものであり、この時間を過ぎるとエラーが記録されます。

E-LMI 情報を交換するための定期的なステータス問い合わせ/ステータス メッセージ シーケンスに加え、PEデバイスは、EVC ステータスに変更が発生するとすぐに、その情報の送信を CE デバイスが指示しなくても、情報を伝達するために CE デバイスに非同期ステータス メッセージも送信できます。

CE と PE デバイスは両方、ステータス カウンタ（N393）を使用して、E-LMI プロトコル ステータスの変更を宣言するまで、受信した連続するエラーを追跡することで E-LMI のローカル動作ステータスを決定します。

イーサネット ローカル管理インターフェイス（E-LMI）の設定

ルータで E-LMI を設定する前に、次の要件を実行してください。

- E-LMI を実行するネットワークのローカルおよびリモート UNI を特定し、その命名規則を定義します。
- E-LMI CE 動作をサポートするデバイス上の対応する CE インターフェイス リンクで E-LMI を有効にします。

E-LMI は、物理サブインターフェイスとバンドル メイン インターフェイスおよびサブインターフェイスではサポートされていません。E-LMI は、イーサネットの物理インターフェイスでのみ設定できます。

CE と PE 間での正しいやり取りを保証するため、各デバイスには 2 つの設定可能パラメータがあります。CE はポーリング タイマー（PT）とポーリング カウンタを使用します。PE はポーリング確認タイマー（PVT）とステータス カウンタを使用します。

イーサネット LMI を設定するには、次の作業を実行します。

- E-LMI の EVC の設定（必須）
- E-LMI のイーサネット CFM の設定（必須）
- 物理インターフェイス上での E-LMI の有効化（必須）
- ポーリング確認タイマーの設定（任意）
- ステータス カウンタの設定（任意）

```
/* Configure EVCs for E-LMI/

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface TenGigE0/3/0/9/1.1 l2transport
```

```
RP/0/RSP0/CPU0:router(config-subif)# encapsulation dot1q 1
RP/0/RSP0/CPU0:router(config-subif)# xconnect group evpn
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# xconnect group evpn
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p p1
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)# interface TenGigE0/3/0/9/1.1
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)# neighbor evpn evi 1 target 3001 source 1
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)#commit


/* Configure Ethernet CFM for E-LMI */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)#interface TenGigE0/3/0/9/1.1 l2transport
RP/0/RSP0/CPU0:router(config-subif)# encapsulation dot1q 1
RP/0/RSP0/CPU0:router(config-subif)# ethernet cfm
RP/0/RSP0/CPU0:router(config-if-cfm)#  mep domain irf_evpn_up service up_mep_evpn_1
mep-id 3001
RP/0/RSP0/CPU0:router(config-if-cfm-mep)#exit
RP/0/RSP0/CPU0:router(config)#ethernet cfm
RP/0/RSP0/CPU0:router(config-cfm)# domain irf_evpn_up level 3 id null
RP/0/RSP0/CPU0:router(config-cfm-dmn)#service up_mep_evpn_1 xconnect group evpn p2p p1
id number 1
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)# mip auto-create all ccm-learning
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)# continuity-check interval 1m loss-threshold
3
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)#continuity-check archive hold-time 10
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)#mep crosscheck
RP/0/RSP0/CPU0:router(config-cfm-xcheck)# mep-id 1
RP/0/RSP0/CPU0:router(config-cfm-xcheck)#ais transmission interval 1m cos 6
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)#log ais
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)#log continuity-check errors
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)#log crosscheck errors
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)#log continuity-check mep changes
RP/0/RSP0/CPU0:router(config-cfm-dmn-svc)#commit

/* Enable E-LMI on the Physical Interface */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)#interface TenGigE0/3/0/9/1
RP/0/RSP0/CPU0:router(config-if)# ethernet lmi
RP/0/RSP0/CPU0:router(config-if-elmi)#commit


/* Configure the Polling Verification Timer */

The MEF T392 Polling Verification Timer (PVT) specifies the allowable time between
transmission of a STATUS message and receipt of a STATUS ENQUIRY from the UNI-C before
recording an error. The default value is 15 seconds.

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)#interface gigabitethernet 0/0/0/0
RP/0/RSP0/CPU0:router(config-if)# ethernet lmi
RP/0/RSP0/CPU0:router(config-if-elmi)#polling-verification-timer 30
RP/0/RSP0/CPU0:router(config-if-elmi)#commit

/* Configure the Status Counter */

The MEF N393 Status Counter value is used to determine E-LMI operational status by
tracking receipt of consecutive good packets or successive expiration of the PVT on
packets. The default counter is four, which means that while the E-LMI protocol is in
Down state, four good packets must be received consecutively to change the protocol state
 to Up, or while the E-LMI protocol is in Up state, four consecutive PVT expirations
```

```
must occur before the state of the E-LMI protocol is changed to Down on the interface.

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)#interface gigabitethernet 0/0/0/0
RP/0/RSP0/CPU0:router(config-if)# ethernet lmi
RP/0/RSP0/CPU0:router(config-if-elmi)#status-counter 5
RP/0/RSP0/CPU0:router(config-if-elmi)#commit
```

実行コンフィギュレーション

この項では、E-LMI の実行コンフィギュレーションを示します。

```
/* Configure EVCs for E-LMI */

configure
 interface TenGigE0/3/0/9/1.1 l2transport
  encapsulation dot1q 1

!

l2vpn
 xconnect group evpn
  p2p p1
   interface TenGigE0/3/0/9/1.1
   neighbor evpn evi 1 target 3001 source 1
   commit
!


/* Configure Ethernet CFM for E-LMI */

configure
 interface TenGigE0/3/0/9/1.1 l2transport
  encapsulation dot1q 1
  ethernet cfm
   mep domain irf_evpn_up service up_mep_evpn_1 mep-id 3001
!
configure
 ethernet cfm
  domain irf_evpn_up level 3 id null
   service up_mep_evpn_1 xconnect group evpn p2p p1 id number 1
    mip auto-create all ccm-learning
    continuity-check interval 1m loss-threshold 3
    continuity-check archive hold-time 10
    mep crosscheck
    mep-id 1
    !
    ais transmission interval 1m cos 6
    log ais
    log continuity-check errors
    log crosscheck errors
    log continuity-check mep changes
!

/* Enable E-LMI on the Physical Interface */

configure
 interface TenGigE0/3/0/9/1
  ethernet lmi
!
```

```
/* Configure the Polling Verification Timer */

configure
 interface gigabitethernet 0/0/0/0
  ethernet lmi
   polling-verification-timer 30
!

/* Configure the Status Counter */

configure
 interface gigabitethernet 0/0/0/0
  ethernet lmi
   status-counter 5
!
```

イーサネット Local Management Interface（LMI）設定の確認

特定のインターフェイス、またはすべてのインターフェイスのイーサネット LMI 設定の値を表示するには、**show ethernet lmi interfaces detail** コマンドを使用します。次の例は、コマンドのサンプル出力を示しています。

```
RP/0/RSP0/CPU0:router# show ethernet lmi interfaces detail

Interface: TenGigE0/3/0/9/1
 Ether LMI Link Status: Up
  Line Protocol State: Up
  MTU: 1514 (1 PDU reqd. for full report)
  CE-VLAN/EVC Map Type: Service Multiplexing with no bundling (1 EVC)
  Configuration: Status counter 4, Polling Verification Timer 15 seconds
  Last Data Instance Sent: 130
  Last Sequence Numbers: Sent 179, Received 108


  Reliability Errors:
    Status Enq Timeouts                  0 Invalid Sequence Number             0
    Invalid Report Type                  0

  Protocol Errors:
    Malformed PDUs                       0 Invalid Protocol Version            0
    Invalid Message Type                 0 Out of Sequence IE                  0
    Duplicated IE                        0 Mandatory IE Missing                0
    Invalid Mandatory IE                 0 Invalid non-Mandatory IE            0
    Unrecognized IE                      0 Unexpected IE                       0


  Full Status Enq Received  00:03:17 ago   Full Status Sent      00:03:17 ago
  PDU Received              00:00:07 ago   PDU Sent              00:00:07 ago
  LMI Link Status Changed   01:59:54 ago   Last Protocol Error      never
  Counters Cleared             never


  Sub-interface: TenGigE0/3/0/9/1.1
    VLANs: 1
    EVC Status: Active
    EVC Type: Point-to-Point
    OAM Protocol: CFM
```

```
    CFM Domain: irf_evpn_up (level 3)
    CFM Service: up_mep_evpn_1

  Remote UNI Count: Configured = 1, Active = 1
   Remote UNI Id                                                    Status
  -------------                                                    ------
  <Remote UNI Reference Id: 1>                                     Up
```

次を確認します。

- プロトコル（Ether LMI リンク ステータス）が「Up」か。
- ローカル UNI 名（UNI ID）がプロビジョニングどおりとなっているか。
- インターフェイス（回線プロトコル状態）が「Up」か。
- CE-VLAN/EVC マップ タイプが予想どおりであり、正しい EVC 数が表示されているか。
- エラー カウンタがすべて 0 か。
- LMI リンク ステータス変更タイマーにプロトコルが起動してからの時間が表示されているか。
- サブインターフェイス名が設定した EFP に対応しているか。
- 各インターフェイス上の VLAN が設定どおりとなっているか。
- EVC ステータスが「Active」か。
- CFM ドメインと CFM サービスがプロビジョニングと一致しているか。
- リモート UNI ID がプロビジョニングどおりとなっているか。

CFM の確認（UP MEP）

```
RP/0/RSP0/CPU0:router# show ethernet cfm peer meps
Flags:
> - Ok                         I - Wrong interval
R - Remote Defect received     V - Wrong level
L - Loop (our MAC received)    T - Timed out
C - Config (our ID received)   M - Missing (cross-check)
X - Cross-connect (wrong MAID) U - Unexpected (cross-check)
* - Multiple errors received   S - Standby

Domain irf_evpn_up (level 3), Service up_mep_evpn_1
Up MEP on TenGigE0/3/0/9/1.1 MEP-ID 3001
================================================================================
St    ID MAC Address    Port    Up/Downtime   CcmRcvd SeqErr   RDI Error
-- ----- -------------- ------- ----------- --------- ------ ----- -----
 >     1 008a.964b.6410 Up      00:09:59           12      0     0     0
================================================================================
```

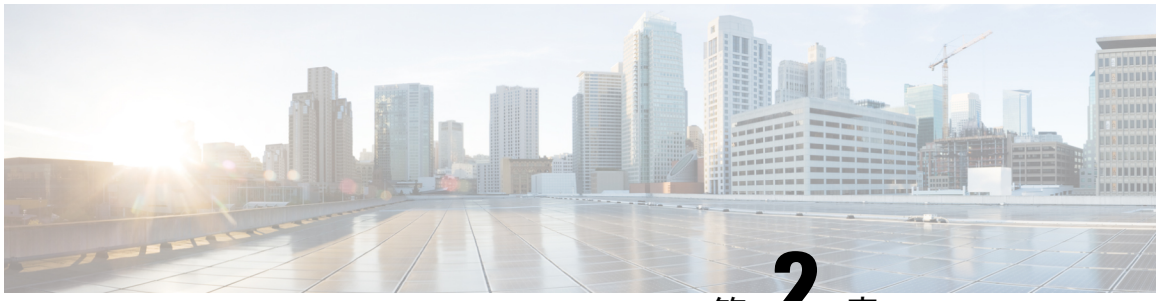
St が >、つまり OK（up）であるかを確認します。

関連項目

- イーサネット ローカル管理インターフェイス（E-LMI） （10 ページ）
- E-LMI メッセージング （10 ページ）
- E-LMI メッセージング （10 ページ）

関連コマンド

- ethernet lmi
- show ethernet lmi interfaces
- show ethernet cfm peer meps



第 2 章

レイヤ 2 アクセス コントロール リスト

イーサネット サービス アクセス コントロール リスト（ACL）は、レイヤ 2 ネットワーク トラフィック プロファイルを集合的に定義する 1 つ以上のアクセス コントロール エントリ（ACE）で構成されます。このプロファイルは、Cisco IOS XR ソフトウェア機能で参照できます。各イーサネット サービス ACL には、送信元および宛先アドレス、サービス クラス（CoS）、ether-type、または 802.1ad DEI などの基準に基づいたアクション要素（許可または拒否）が含まれます。

レイヤ 2 ACL は入力トラフィックのみでサポートされています。出力トラフィックでは、レイヤ 2 ACL はサポートされていません。

また、レイヤ 2 アクセス コントロール リストはイーサネット サービス コントロール アクセス リストとも呼ばれています。

レイヤ 2 アクセス コントロール リスト設定の前提条件

この前提条件は、アクセス コントロール リストおよびプレフィックス リストの設定に適用されます。

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

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

レイヤ 2 アクセス コントロール リスト機能の特長

レイヤ 2 アクセス コントロール リストには次の機能上の特長があります。

- 特定のシーケンス番号を使用してアクセス リストのカウンタをクリアする機能。
- 別のアクセス リストに既存のアクセス リストの内容をコピーする機能。
- ユーザがシーケンス番号を permit ステートメントまたは deny ステートメントに適用できること。
- レイヤ2ACLはインターフェイス、VLANサブインターフェイス、バンドルイーサネットインターフェイス、L2ポートのあるバンドルサブインターフェイス上に適用できること。レイヤ2ACLのアトミックな置換は、これらの物理インターフェイスとバンドルインターフェイス上でサポートされています。

レイヤ 2 アクセス コントロール リストの目的

レイヤ 2 アクセス コントロール リストは、パケット フィルタリングを実行して、ネットワークを介して移動するパケットとその場所を制御します。そのような制御は、着信および発信ネットワーク トラフィックを制限し、ポート レベルでネットワークにユーザおよびデバイスのアクセスを制限するために役立ちます。

レイヤ 2 アクセス コントロール リストの仕組み

レイヤ 2 アクセス コントロール リストは、レイヤ 2 設定に適用される permit および deny ステートメントで構成された順序付きリストです。アクセス リストには、参照に使用される名前があります。

アクセス リストを設定して名前を付けることは可能ですが、アクセス リストを受け取るコマンドによってアクセス リストが参照されるまで、有効にはなりません。複数のコマンドから同じアクセス リストを参照できます。アクセス リストはルータに着信するレイヤ 2 トラフィックを制御できますが、ルータを起点とするトラフィックやルータを離れるトラフィックは制御できません。

レイヤ2アクセス コントロール リストのプロセスとルール

レイヤ2アクセス コントロール リストを設定する際に、次のプロセスとルールを使用します。

- ソフトウェアは、アクセス リストの条件に対してフィルタされる各パケットの送信元アドレスや宛先アドレスをテストします。一度に 1 つの条件（permit または deny ステートメント）がテストされます。
- パケットがアクセス リストのステートメントに一致しないと、そのパケットはリスト内の次のステートメントに対してテストされます。
- パケットとアクセス リストのステートメントが一致すると、リスト内の残りのステートメントはスキップされ、パケットは一致したステートメントに指定されたとおりに許可または拒否されます。パケットが許可されるか拒否されるかは、パケットが一致する最初のエントリによって決まります。つまり、一致すると、それ以降のエントリは考慮されません。
- アクセス リストがアドレスまたはプロトコルを拒否する場合は、ソフトウェアはパケットを廃棄します。
- 各アクセス リストの最後には暗黙の deny ステートメントがあるため、一致する条件がない場合は、パケットはドロップされます。つまり、各ステートメントに対してテストするときまでにパケットを許可または拒否しないと、パケットは拒否されます。
- アクセス リストには permit ステートメントを 1 つ以上含める必要があります。そうしないと、パケットはすべて拒否されます。
- 最初に一致が見つかった後は条件のテストが終了するため、条件の順序は重要です。同じ permit ステートメントまたは deny ステートメントでも、順序が異なる場合、ある状況では通過し、別の状況では拒否されるパケットが生じる可能性があります。
- インバウンド アクセス リストは、ルータに到達するパケットを処理します。インバウンド アクセス リストが効率的なのは、フィルタリング テストで拒否されたことでパケットが廃棄される場合、ルーティング検索のオーバーヘッドが抑えられるためです。パケットがテストで許可されると、そのパケットに対してルーティングの処理が実施されます。インバウンドリストの場合、permit とは、インバウンドインターフェイスで受信したパケットを引き続き処理することを意味します。deny とは、パケットを破棄することです。
- アクセス リストは、使用中のアクセス グループによって適用されている場合には削除できません。アクセス リストを削除するには、まずアクセス リストを参照しているアクセス グループを削除してから、アクセス リストを削除します。
- アクセス リストは、**ethernet-services access-group** コマンドを使用する前に存在している必要があります。

レイヤ 2 アクセス コントロール リストの作成

レイヤ 2 アクセス コントロール リストを作成するときは以下を考慮します。

- アクセス リストは、インターフェイスに適用する前に作成します。
- より具体的な参照が、より全般的な参照よりも前に出現するように、アクセス リストを構成します。

レイヤ 2 アクセス コントロール リスト設定の制約事項

次の制約事項は、レイヤ 2 アクセス コントロール リストの設定に適用されます。

- レイヤ 2 アクセス コントロール リストは、管理インターフェイスではサポートされていません。
- NetIO（ソフトウェア低速パス）は、レイヤ 2 アクセス コントロール リストではサポートされていません。
- レイヤ 2 アクセス コントロール リストは、インターフェイスの入力方向にのみ付加できます。
- レイヤ 2 アクセス コントロール リストでは COS（サービス クラス）と DEI（Discard Eligibility Indication）のみがサポートされています。

設定

この項では、レイヤ 2 アクセス コントロール リストを設定する方法について説明します。

```
Router# configure
Router(config)# ethernet-services access-list es_acl_1
Router(config-es-acl)# deny 00ff.eedd.0010 ff00.0000.00ff 0000.0100.0001 0000.0000.ffff
Router(config-es-acl)# permit host 000a.000b.000c host 00aa.ab99.1122 cos 1 dei
Router(config-es-acl)# deny host 000a.000b.000c host 00aa.dc11.ba99 cos 7 dei
Router(config-es-acl)# commit
Router(config)# interface tengige0/0/0/4
Router(config-if)# l2transport
Router(config-if-l2)# commit
Router(config-if-l2)# exit
Router(config-if)# ethernet-services access-group es_acl_1 ingress
Router(config-if)# commit
```

実行コンフィギュレーション

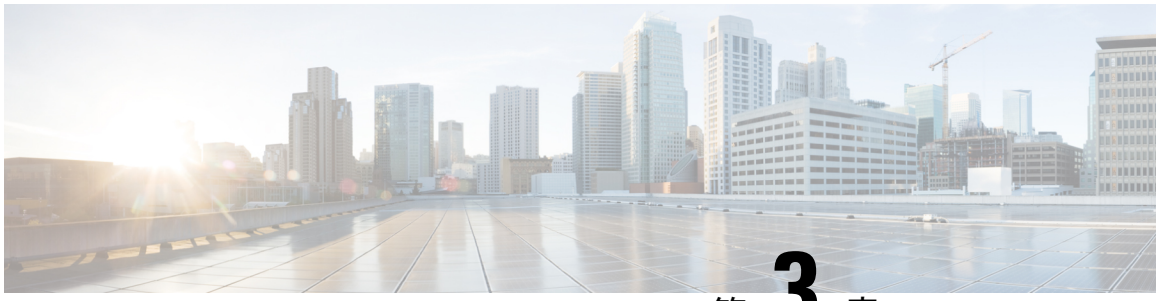
```
!
Configure
ethernet-services access-list es_acl_1
10 deny 00ff.eedd.0000 ff00.0000.00ff 0000.0100.0000 0000.0000.ffff
20 permit host 000a.000b.000c host 00aa.ab99.1122 cos 1 dei
30 deny host 000a.000b.000c host 00aa.dc11.ba99 cos 7 dei
!
```

確認

レイヤ 2 アクセス コントロール リストが設定されていることを確認します。

```
/* Verify the Layer 2 access control lists configuration */
```

```
Router# show access-lists ethernet-services es_acl_1  hardware ingress location 0/0/CPU0

Fri Oct 21 09:39:52.904 UTC
ethernet-services access-list es_acl_1
10 deny 00ff.eedd.0000 ff00.0000.00ff 0000.0100.0000 0000.0000.ffff (2051 matches)
20 permit host 000a.000b.000c host 00aa.ab99.1122 cos 1 dei
30 deny host 000a.000b.000c host 00aa.dc11.ba99 cos 7 dei (2050 matches)
```



第 3 章

VLAN サブインターフェイスの設定

サブインターフェイスは、ハードウェアインターフェイス上に作成される論理インターフェイスです。これらのソフトウェア定義のインターフェイスにより、単一のハードウェアインターフェイス上でトラフィックを論理チャネルに分割することができ、また、物理インターフェイス上で帯域幅を効率的に利用することができます。

サブインターフェイスは、インターフェイス名の末尾に拡張子を追加することで、他のインターフェイスと区別されます。たとえば、物理インターフェイス TenGigE 0/1/0/0 上のイーサネット サブインターフェイス 23 は、TenGigE 0/1/0/0.23 となります。

サブインターフェイスがトラフィックを渡すことができるようにするには、有効なタグ付きプロトコルのカプセル化と VLAN 識別子の割り当てが必要です。すべてのイーサネット サブインターフェイスは常に、デフォルトで 802.1Q VLAN でカプセル化されます。ただし、VLAN 識別子は明示的に定義する必要があります。

サブインターフェイスの最大伝送ユニット（MTU）は、物理インターフェイスから継承されます。これには、802.1Q VLAN タグに許可されている追加の 4 バイトも含まれます。

次のモードの VLAN サブインターフェイスの設定がサポートされています。

- 基本の dot1q 接続回線
- Q-in-Q 接続回線

基本の dot1q 接続回線を設定するには、次のカプセル化モードを使用します。

encapsulation dot1q *vlan-id*

基本の dot1ad 接続回線を設定するには、次のカプセル化モードを使用します。

encapsulation dot1ad *vlan-id*

Q-in-Q 接続回線を設定するには、次のカプセル化モードを使用します。

- **encapsulation dot1q** *vlan-id* **second-dot1q** *vlan-id*
- **encapsulation dot1ad** *vlan-id* **dot1q** *vlan-id*

制約事項と制限

VLAN サブインターフェイスを設定する場合、次の制限事項が適用されます。

- 二重タグ付きパケットの場合、VLAN 範囲は内部タグでのみサポートされます。
- VLAN リストはサポートされていません。

  カンマで区切られた VLAN は、VLAN リストと呼ばれます。次の例を参照してください。

```
Router(config)#interface tenGigE 0/0/0/2.0 l2transport
Router(config-subif)#encapsulation dot1q 1,2  >> VLAN range with comma
Router(config-subif)#commit
```

- 0x9100/0x9200 がトンネリング イーサタイプとして設定されている場合、dot1ad（0x88a8）カプセル化はサポートされません。
- いずれかのサブインターフェイスがメインインターフェイス配下ですでに設定されている場合、トンネリング イーサタイプの変更はサポートされません。
- ルータで最大 16 個の仮想 MAC アドレスをプログラムできます。

設定例

VLAN サブインターフェイスの設定には、以下が含まれます。

- 10 ギガビット イーサネット サブインターフェイスの作成
- インターフェイスでの L2 転送モードの有効化
- インターフェイス上の入力フレームを適切なサービス インスタンスにマッピングするために使用する一致基準（カプセル化モード）の定義

基本の dot1q 接続回線の設定

実行コンフィギュレーション

```
configure
 interface TenGigE 0/0/0/10.1
  l2transport
  encapsulation dot1q 10 exact
 !
!
```

確認

VLAN サブインターフェイスがアクティブであることを確認します。

```
router# show interfaces TenGigE 0/0/0/10.1

...
TenGigE0/0/0/10.1 is up, line protocol is up
  Interface state transitions: 1
  Hardware is VLAN sub-interface(s), address is 0011.1aac.a05a
  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 10
    Ethertype Any, MAC Match src any, dest any
  loopback not set,
...
```

関連コマンド

- encapsulation dot1ad dot1q
- encapsulation dot1q
- encapsulation dot1q second-dot1q
- l2transport（イーサネット）
- encapsulation dot1ad

- イーサネット フロー ポイントの概要 （27 ページ）
- VLAN ヘッダー書き換えの設定 （30 ページ）
- プライオリティタグのリライト （43 ページ）

イーサネット フロー ポイントの概要

イーサネットフローポイント（EFP）とは、物理またはバンドルインターフェイスにおいて、トラフィックの分類に使用されるレイヤ2の論理サブインターフェイスです。EFPは、特定のEFPに属するフレームを分類するために、すべての入力トラフィックに適用されるフィルタのセット（エントリのセット）によって定義されます。各エントリには、通常、0、1、または2つのVLANタグが含まれます。VLANまたはQinQタギングを指定して、入力上で照合できます。パケットが、フィルタのエントリと同じタグで始まる場合、そのパケットはフィルタに一致することになります。パケットの先頭部分がフィルタのエントリに対応しない場合、パケットはフィルタに一致しません。

入力上のすべてのトラフィックは、一致が見つかるとそのEFPによって処理され、VLAN IDの変更、VLANタグの削除、およびEtherTypeの変更を順々に行うことができます。フレームが特定のEFPに一致した後、適切な機能（設定によって指定されたフレーム操作、QoSやACLなど）を適用できます。

EFPの利点には次のものがあります。

- 特定のインターフェイスで特定のフローに属するすべてのフレームの識別
- VLANヘッダー書き換えの実行

  （VLAN ヘッダー書き換えの設定 （30 ページ） を参照）
- 識別されたフレームへの機能の追加。
- オプションで、データ パスでのフレームの転送方法の定義。

EFP の制限

出力 EFP のフィルタリングは、Cisco IOS XR ではサポートされていません。

EFP のフレームの識別

EFPは、イーサネットカプセル化に関係なく、指定ポートで特定フローに属するフレームを識別します。EFP は、フレーム ヘッダー内のフィールドに基づいてフローまたは EFP に柔軟にフレームをマッピングできます。VLAN タグを使用して、フレームと EFP を照合できます。

これを介して、フレームと EFP を照合することはできません。

- 以下のような、最も外側のイーサネット フレーム ヘッダーおよび関連するタグの外部の情報
  - IPv4、IPv6、または MPLS のタグ ヘッダーのデータ
  - C-DMAC、C-SMAC、または C-VLAN

VLAN タグの識別

次の表では、さまざまなカプセル化タイプとそれぞれに対応するEFP識別子について説明します。

カプセル化タイプ	EFP 識別子
単一タグ付きフレーム	802.1Q カスタマー タグ付きイーサネット フレーム
二重タグ付きフレーム 二重タグ付きフレームは、次のいずれかのタイプになります。 • 単一範囲 • Range-in-Q • Q-in-Range	802.1Q（ethertype 0x9100）二重タグ付きフレーム 802.1ad（ethertype 0x9200）二重タグ付きフレーム • 単一範囲では、EFP に対して VLAN ID の範囲を追加できます。 • Range-in-Q では、外部 VLAN ID の範囲に単一の内部 VLAN ID を持たせることができます。 • Q-in-Range では、単一の外部 VLAN ID に内部 VLAN ID の範囲を持たせることができます。

特定のEFPにマップされるフレームを定義する際にワイルドカードを使用できます。EFPは、単一の VLAN タグ、VLAN タグのスタック、または両方の組み合わせ（VLAN スタックとワイルドカード）に基づいてフローを区別できます。EFPは、EFPモデル、カプセル化非依存に

する柔軟性を提供しています。また、新しいタギングまたはトンネリング方式を追加することで、EFP を拡張できるようになっています。

機能の適用

フレームが特定の EFP に一致した後、適切な機能を適用できます。このコンテキストでは、「機能」とは、設定や QoS、ACL などによって指定されたフレーム操作を意味します。イーサネット インフラストラクチャは、機能オーナーが EFP に機能を適用できるように適切なインターフェイスを提供しています。そのため、EFP を表すために IM インターフェイス ハンドルが使用され、これにより機能のオーナーは、通常のインターフェイスまたはサブインターフェイス上で機能が管理されるのと同じように EFP で機能を管理できます。

イーサネットインフラストラクチャの一部である EFP で適用できる唯一の L2 機能は、L2 ヘッダーのカプセル化の変更です。この L2 機能については、次の項で説明します。

カプセル化の変更

EFP は、入力と出力の両方で、次の L2 ヘッダーのカプセル化の変更をサポートしています。

- 1 つまたは 2 つの VLAN タグのプッシュ処理
- 1 つまたは 2 つの VLAN タグのポップ処理

（注） この変更では、EFP に部分一致するタグのポップ処理のみ実行できます。

- 1 つまたは 2 つの VLAN タグの書き換え
  - 外部タグの書き換え
  - 2 つの外部タグの書き換え
  - 外部タグの書き換え、および追加タグのプッシュ処理

  各 VLAN ID 操作に対して、以下を指定できます。
- VLAN タグ タイプ、つまり、C-VLAN、S-VLAN、または I-TAG。802.1Q C-VLAN タグの Ethertype は、dot1q tunneling type コマンドで定義されます。
- VLAN ID。0 は、プライオリティ タグ付きフレームを生成するために、外部 VLAN タグに対し指定できます。

（注） タグの書き換えでは、以前のタグの CoS ビットを、802.1ad カプセル化フレームの DEI ビットと同じ方法で維持する必要があります。

データ転送動作の定義

データパスで転送される特定のイーサネットフローに属するフレームを指定するために、EFPを使用できます。次の転送ケースが、Cisco IOS XR ソフトウェアでのEFPに対しサポートされます。

- L2 スイッチド サービス（ブリッジング）：EFP はブリッジ ドメインにマッピングされ、そこでフレームは宛先 MAC アドレスに基づいてスイッチングされます。これには、マルチポイント サービスが含まれます。
  - イーサネットとイーサネットのブリッジング
  - マルチポイント レイヤ 2 サービス
- L2 スイッチド サービス（AC と AC の xconnect）：これは、静的に確立されるポイントツーポイント L2 アソシエーションに対応し、MAC アドレス ルックアップを必要としません。
  - イーサネットとイーサネットのローカルスイッチング：EFPは同じポートまたは別のポートのS-VLANにマッピングされます。S-VLANは同一にすること、または別にすることができます。
- トンネル型サービス（xconnect）：EFP はレイヤ 3 トンネルにマッピングされます。これは、EoMPLS などのポイントツーポイントを対象としています。

VLAN ヘッダー書き換えの設定

EFPは、入力ポートおよび出力ポートの両方で次のVLANヘッダー書き換えをサポートしています。

- 1 つの VLAN タグのプッシュ処理
- 1 つの VLAN タグのポップ処理

（注） この書き換えでは、EFP に部分一致するタグのポップ処理のみ実行できます。

- 1 つまたは 2 つの VLAN タグの変換
  - Translate 1-to-1 tag：最も外側のタグを別のタグに変換します
  - Translate 1-to-2 tags：最も外側のタグを 2 つのタグに変換します
  - Translate 2-to-2 tags：最も外側の 2 つのタグを 2 つの別のタグに変換します

以降の項に、入力および出力 VLAN 変換時に入力および出力 VLAN と対応するタグ アクションのさまざまな組み合わせを示します。

• 有効な入力書き換えアクション （33 ページ）
• 有効な入力と出力の書き換えの組み合わせ （34 ページ）

制限事項

VLAN ヘッダー書き換えの制限は次のとおりです。

- Push 1 は dot1ad 設定ではサポートされていません。
- Push 2 は以下でのみサポートされています。
  - タグなしの EFP
  - **exact** コンフィギュレーション ステートメントによる Dot1q EFP
- Translate 1 to 1 は dot1ad コンフィギュレーションではサポートされていません。
- Translate 1 to 2 は **dot1q tunneling ethertype** コンフィギュレーション ステートメントではサポートされていません。
- Pop 2 はサポートされていません。
- Translate 2 to 1 はサポートされていません。

設定例

この項では、次のようなさまざまな接続回線での VLAN ヘッダー書き換えについて説明します。

- L2 一重タグ付きサブインターフェイス
- L2 二重タグ付きサブインターフェイス

VLAN ヘッダー書き換えの設定には、以下が含まれます。

- TenGigabit イーサネット サブインターフェイスの作成
- インターフェイスでの L2 転送モードの有効化
- インターフェイス上の一重タグ付きフレーム入力を適切なサービスインスタンスにマッピングするために使用する一致基準（カプセル化モード）の定義。
- 入力フレームで行われるカプセル化調整の指定

VLAN ヘッダー書き換え（一重タグ付きサブインターフェイス）の設定

```
Router# configure
Router(config)# interface TenGigE 0/0/0/10.1 l2transport
Router(config-if)# encapsulation dot1q 10 exact
Router(config-if)# rewrite ingress tag push dot1q 20 symmteric
```

実行コンフィギュレーション

```
/* Configuration without rewrite */

configure
 interface TenGigE0/0/0/0.1 l2transport
  encapsulation dot1q 10 exact
 !
!

/* Configuration with rewrite */

/* PUSH 1 */
interface TenGigE0/0/0/0.1 l2transport
 encapsulation dot1q 10
 rewrite ingress tag push dot1q 20 symmteric
 !
!

/* POP 1 */
interface TenGigE0/0/0/0.1 l2transport
 encapsulation dot1q 10
  rewrite ingress tag pop 1
 !
!

/* TRANSLATE 1-1 */

interface TenGigE0/0/0/0.1 l2transport
 encapsulation dot1q 10
  rewrite ingress tag translate 1-to-1 dot1q 20
 !
!

/* TRANSLATE 1-2 */

interface TenGigE0/0/0/0.1 l2transport
 encapsulation dot1q 10
  rewrite ingress tag translate 1-to-2 dot1q 20 second-dot1q 30
 !
!
```

実行コンフィギュレーション（二重タグ付きサブインターフェイスでの VLAN ヘッダー書き換え）

```
/* Configuration without rewrite */

interface TenGigE0/0/0/0.1 l2transport
 encapsulation dot1q 10 second-dot1q 11
 !
!

/* Configuration with rewrite */

/* PUSH 1 */
interface TenGigE0/0/0/0.1 l2transport
 encapsulation dot1q 10 second-dot1q 11
  rewrite ingress tag push dot1q 20 symmteric
 !
!
```

```
/* TRANSLATE 1-1 */

interface TenGigE0/0/0/0.1 l2transport
 encapsulation dot1q 10 second-dot1q 11
  rewrite ingress tag translate 1-to-1 dot1q 20
 !
!

/* TRANSLATE 1-2 */

interface TenGigE0/0/0/0.1 l2transport
 encapsulation dot1q 10 second-dot1q 11
  rewrite ingress tag translate 1-to-2 dot1q 20 second-dot1q 30
 !
!

/* TRANSLATE 2-2 */

interface TenGigE0/0/0/0.1 l2transport
 encapsulation dot1q 10 second-dot1q 11
  rewrite ingress tag translate 2-to-2 dot1q 20 second-dot1q 30
 !
!
```

関連コマンド

- encapsulation dot1ad dot1q
- encapsulation dot1q
- encapsulation dot1q second-dot1q
- l2transport（イーサネット）
- rewrite ingress tag

有効な入力書き換えアクション

表 *1*:有効な入力書き換えアクション

インターフェイスコンフィギュレーション	入力書き換え操作
dot1q	書き換えなし
dot1q	Pop 1
dot1q	Push 1
dot1q	Push 2
dot1q	Translate 1 to 1
dot1q	Translate 1 to 2

インターフェイスコンフィギュレーション	入力書き換え操作
QinQ	書き換えなし
QinQ	Pop 1
QinQ	Push 1
QinQ	Translate 1 to 1
QinQ	Translate 1 to 2
QinQ	Translate 2 to 2
タグなし	書き換えなし
タグなし	Push 1
タグなし	Push 2

表に示した書き換えアクションには次の表記を使用します。

- Translate 1-to-1 tag：最も外側のタグを別のタグに変換します
- Translate 1-to-2 tags：最も外側のタグを 2 つのタグに変換します
- Translate 2-to-2 tags：最も外側の 2 つのタグを 2 つの別のタグに変換します

有効な入力と出力の書き換えの組み合わせ

表 *2:* 有効な入力と出力の書き換えの組み合わせ

入力インターフェイスの設定	入力インターフェイスの書き換えアクション	出力インターフェイスの設定	出力インターフェイスの書き換えアクション
dot1q	書き換えなし	dot1q	書き換えなし
dot1q	書き換えなし	dot1q	Pop 1
dot1q	書き換えなし	dot1q	Push 1
dot1q	書き換えなし	dot1q	Translate 1-to-1
dot1q	Pop 1	dot1q	書き換えなし
dot1q	Pop 1	dot1q	Pop 1
dot1q	Push 1	dot1q	書き換えなし
dot1q	Push 1	dot1q	Push 1

入力インターフェイスの設定	入力インターフェイスの書き換えアクション	出力インターフェイスの設定	出力インターフェイスの書き換えアクション
dot1q	Push 1	dot1q	Push 2
dot1q	Push 1	dot1q	Translate 1-to-1
dot1q	Push 1	dot1q	Translate 1-to-2
dot1q	Push 2/Translate 1-to-2	dot1q	Push 1
dot1q	Push 2/Translate 1-to-2	dot1q	Push 2
dot1q	Push 2/Translate 1-to-2	dot1q	Translate 1-to-2
dot1q	Translate 1-to-1	dot1q	書き換えなし
dot1q	Translate 1-to-1	dot1q	Push 1
dot1q	Translate 1-to-1	dot1q	Translate 1-to-1
dot1q	書き換えなし	dot1q range	書き換えなし
dot1q	書き換えなし	dot1q range	Push 1
dot1q	Pop 1	dot1q range	書き換えなし
dot1q	Push 1	dot1q range	書き換えなし
dot1q	Push 1	dot1q range	Push 1
dot1q	Push 1	dot1q range	Push 2
dot1q	Translate 1-to-1	dot1q range	書き換えなし
dot1q	Translate 1-to-1	dot1q range	Push 1
dot1q	Translate 1-to-2	dot1q range	Push 1
dot1q	Translate 1-to-2	dot1q range	Push 2
dot1q	書き換えなし/Translate 1-to-1	QinQ	書き換えなし
dot1q	書き換えなし/Translate 1-to-1	QinQ	Pop 1
dot1q	書き換えなし/Translate 1-to-1	QinQ	Push 1
dot1q	書き換えなし/Translate 1-to-1	QinQ	Translate 1-to-1
dot1q	Pop 1	QinQ	書き換えなし
dot1q	Pop 1	QinQ	Pop 1

入力インターフェイスの設定	入力インターフェイスの書き換えアクション	出力インターフェイスの設定	出力インターフェイスの書き換えアクション
dot1q	Push 1	QinQ	書き換えなし
dot1q	Push 1	QinQ	Pop 1
dot1q	Push 1	QinQ	Push 1
dot1q	Push 1	QinQ	Translate 1-to-1
dot1q	Push 1	QinQ	Translate 1-to-2
dot1q	Push 1	QinQ	Translate 2-to-2
dot1q	Push 2/Translate 1-to-2	QinQ	書き換えなし
dot1q	Push 2/Translate 1-to-2	QinQ	Push 1
dot1q	Push 2/Translate 1-to-2	QinQ	Translate 1-to-1
dot1q	Push 2/Translate 1-to-2	QinQ	Translate 1-to-2
dot1q	Push 2/Translate 1-to-2	QinQ	Translate 2-to-2
dot1q	書き換えなし/Translate 1-to-1	QinQ range	書き換えなし
dot1q	書き換えなし/Translate 1-to-1	QinQ range	Pop 1
dot1q	書き換えなし/Translate 1-to-1	QinQ range	Push 1
dot1q	書き換えなし/Translate 1-to-1	QinQ range	Translate 1-to-1
dot1q	Pop 1	QinQ range	書き換えなし
dot1q	Pop 1	QinQ range	Pop 1
dot1q	Push 1	QinQ range	書き換えなし
dot1q	Push 1	QinQ range	Pop 1
dot1q	Push 1	QinQ range	Push 1
dot1q	Push 1	QinQ range	Translate 1-to-1
dot1q	Push 1	QinQ range	Translate 1-to-2
dot1q	Push 2/Translate 1-to-2	QinQ range	書き換えなし
dot1q	Push 2/Translate 1-to-2	QinQ range	Push 1
dot1q	Push 2/Translate 1-to-2	QinQ range	Translate 1-to-1
dot1q	Push 2/Translate 1-to-2	QinQ range	Translate 1-to-2

入力インターフェイスの設定	入力インターフェイスの書き換えアクション	出力インターフェイスの設定	出力インターフェイスの書き換えアクション
dot1q	書き換えなし	QinQ range	書き換えなし
dot1q	書き換えなし	タグなし	Push 1
dot1q	Pop 1	タグなし	書き換えなし
dot1q	Push 1	タグなし	Push 1
dot1q	Push 1	タグなし	Push 2
dot1q	Push 2	タグなし	Push 2
dot1q	Translate 1-to-1	タグなし	Push 1
dot1q	Translate 1-to-2	タグなし	Push 2
dot1q range	書き換えなし	dot1q range	書き換えなし
dot1q range	書き換えなし	dot1q range	Push 1
dot1q range	Push 1	dot1q range	書き換えなし
dot1q range	Push 1	dot1q range	Push 1
dot1q range	Push 1	dot1q range	Push 2
dot1q range	Push 2	dot1q range	Push 1
dot1q range	Push 2	dot1q range	Push 2
dot1q range	書き換えなし	QinQ	書き換えなし
dot1q range	書き換えなし	QinQ	Pop 1
dot1q range	書き換えなし	QinQ	Push 1
dot1q range	書き換えなし	QinQ	Translate 1-to-1
dot1q range	Push 1	QinQ	書き換えなし
dot1q range	Push 1	QinQ	Pop 1
dot1q range	Push 1	QinQ	Push 1
dot1q range	Push 1	QinQ	Translate 1-to-1
dot1q range	Push 1	QinQ	Translate 1-to-2
dot1q range	Push 1	QinQ	Translate 2-to-2

入力インターフェイスの設定	入力インターフェイスの書き換えアクション	出力インターフェイスの設定	出力インターフェイスの書き換えアクション
dot1q range	Push 2	QinQ	書き換えなし
dot1q range	Push 2	QinQ	Push 1
dot1q range	Push 2	QinQ	Translate 1-to-1
dot1q range	Push 2	QinQ	Translate 1-to-2
dot1q range	Push 2	QinQ	Translate 2-to-2
dot1q range	書き換えなし	QinQ range /QinAny	書き換えなし
dot1q range	書き換えなし	QinQ range	Pop 1
dot1q range	書き換えなし	QinQ range /QinAny	Push 1
dot1q range	書き換えなし	QinQ range /QinAny	Translate 1-to-1
dot1q range	Push 1	QinQ range /QinAny	書き換えなし
dot1q range	Push 1	QinQ range /QinAny	Pop 1
dot1q range	Push 1	QinQ range	Push 1
dot1q range	Push 1	QinQ range /QinAny	Translate 1-to-1
dot1q range	Push 1	QinQ range /QinAny	Translate 1-to-2
dot1q range	Push 2	QinQ range /QinAny	書き換えなし
dot1q range	Push 2	QinQ range /QinAny	Push 1
dot1q range	Push 2	QinQ range /QinAny	Translate 1-to-1

入力インターフェイスの設定	入力インターフェイスの書き換えアクション	出力インターフェイスの設定	出力インターフェイスの書き換えアクション
dot1q range	Push 2	QinQ range /QinAny	Translate 1-to-2
dot1q range	書き換えなし	タグなし	書き換えなし
dot1q range	書き換えなし	タグなし	Push 1
dot1q range	Push 1	タグなし	Push 1
dot1q range	Push 1	タグなし	Push 2
dot1q range	Push 2	タグなし	Push 2
QinQ	書き換えなし/push 1/Translate 1-to-1	QinQ	書き換えなし
QinQ	書き換えなし/push 1/Translate 1-to-1	QinQ	Pop 1
QinQ	書き換えなし/push 1/Translate 1-to-1	QinQ	Push 1
QinQ	書き換えなし/push 1/Translate 1-to-1	QinQ	Translate 1-to-1
QinQ	書き換えなし/push 1/Translate 1-to-1	QinQ	Translate 1-to-2
QinQ	書き換えなし/push 1/Translate 1-to-1	QinQ	Translate 2-to-2
QinQ	Pop 1	QinQ	書き換えなし
QinQ	Pop 1	QinQ	Pop 1
QinQ	Pop 1	QinQ	Push 1
QinQ	Pop 1	QinQ	Translate 1-to-1
QinQ	Translate 1-to-2/Translate 2-to-2	QinQ	書き換えなし
QinQ	Translate 1-to-2/Translate 2-to-2	QinQ	Push 1
QinQ	Translate 1-to-2/Translate 2-to-2	QinQ	Translate 1-to-1
QinQ	Translate 1-to-2/Translate 2-to-2	QinQ	Translate 1-to-2
QinQ	Translate 1-to-2/Translate 2-to-2	QinQ	Translate 2-to-2

入力インターフェイスの設定	入力インターフェイスの書き換えアクション	出力インターフェイスの設定	出力インターフェイスの書き換えアクション
QinQ	書き換えなし/push 1/Translate 1-to-1	QinQ range /QinAny	書き換えなし
QinQ	書き換えなし/push 1/Translate 1-to-1	QinQ range /QinAny	Pop 1
QinQ	書き換えなし/push 1/Translate 1-to-1	QinQ range /QinAny	Push 1
QinQ	書き換えなし/push 1/Translate 1-to-1	QinQ range /QinAny	Translate 1-to-1
QinQ	書き換えなし/push 1/Translate 1-to-1	QinQ range /QinAny	Translate 1-to-2
QinQ	Pop 1	QinQ range /QinAny	書き換えなし
QinQ	Pop 1	QinQ range /QinAny	Pop 1
QinQ	Pop 1	QinQ range /QinAny	Push 1
QinQ	Pop 1	QinQ range /QinAny	Translate 1-to-1
QinQ	Translate 1-to-2/Translate 2-to-2	QinQ range /QinAny	書き換えなし
QinQ	Translate 1-to-2/Translate 2-to-2	QinQ range /QinAny	Push 1
QinQ	Translate 1-to-2/Translate 2-to-2	QinQ range /QinAny	Translate 1-to-1
QinQ	Translate 1-to-2/Translate 2-to-2	QinQ range /QinAny	Translate 1-to-2
QinQ	書き換えなし	タグなし	書き換えなし
QinQ	書き換えなし	タグなし	Push 1

入力インターフェイスの設定	入力インターフェイスの書き換えアクション	出力インターフェイスの設定	出力インターフェイスの書き換えアクション
QinQ	書き換えなし	タグなし	Push 2
QinQ	Pop 1	タグなし	書き換えなし
QinQ	Pop 1	タグなし	Push 1
QinQ	Push 1/Translate 1-to-1	タグなし	Push 1
QinQ	Push 1/Translate 1-to-1	タグなし	Push 2
QinQ	Translate 1-to-2/Translate 2-to-2	タグなし	Push 2
QinQ range /QinAny	書き換えなし/push 1/Translate 1-to-1	QinQ range /QinAny	書き換えなし
QinQ range /QinAny	書き換えなし/push 1/Translate 1-to-1	QinQ range /QinAny	Pop 1
QinQ range /QinAny	書き換えなし/push 1/Translate 1-to-1	QinQ range /QinAny	Push 1
QinQ range /QinAny	書き換えなし/push 1/Translate 1-to-1	QinQ range /QinAny	Translate 1-to-1
QinQ range /QinAny	書き換えなし/push 1/Translate 1-to-1	QinQ range /QinAny	Translate 1-to-2
QinQ range /QinAny	Pop 1	QinQ range /QinAny	書き換えなし
QinQ range /QinAny	Pop 1	QinQ range /QinAny	Pop 1
QinQ range /QinAny	Pop 1	QinQ range /QinAny	Push 1
QinQ range	Pop 1	QinQ range	Translate 1-to-1
QinQ range /QinAny	Translate 1-to-2	QinQ range /QinAny	書き換えなし
QinQ range /QinAny	Translate 1-to-2	QinQ range /QinAny	Push 1

入力インターフェイスの設定	入力インターフェイスの書き換えアクション	出力インターフェイスの設定	出力インターフェイスの書き換えアクション
QinQ range /QinAny	Translate 1-to-2	QinQ range /QinAny	Translate 1-to-1
QinQ range /QinAny	Translate 1-to-2	QinQ range /QinAny	Translate 1-to-2
QinQ range /QinAny	書き換えなし	タグなし	書き換えなし
QinQ range /QinAny	書き換えなし	タグなし	Push 1
QinQ range /QinAny	書き換えなし	タグなし	Push 2
QinQ range /QinAny	Pop 1	タグなし	書き換えなし
QinQ range /QinAny	Pop 1	タグなし	Push 1
QinQ range /QinAny	Push 1/Translate 1-to-1	タグなし	Push 1
QinQ range /QinAny	Push 1/Translate 1-to-1	タグなし	Push 2
QinQ range /QinAny	Translate 1-to-2	タグなし	Push 2
タグなし	書き換えなし	タグなし	書き換えなし
タグなし	Push 1	タグなし	Push 1
タグなし	Push 2	タグなし	Push 2

表に示した書き換えアクションには次の表記を使用します。

- Translate 1-to-1 tag：最も外側のタグを別のタグに変換します
- Translate 1-to-2 tags：最も外側のタグを 2 つのタグに変換します
- Translate 2-to-2 tags：最も外側の 2 つのタグを 2 つの別のタグに変換します

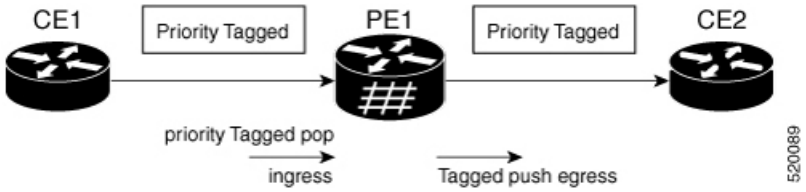
プライオリティタグのリライト

プライオリティタグのリライト機能を使用すると、プライオリティタグ付き VLAN のリライトタグを設定できます。この機能により、入力方向のプライオリティタグ付き VLAN が削除され、出力方向にプライオリティタグ付き VLAN が追加されます。

PE1 でプライオリティタグ付きイーサネット仮想接続（EVC）に対して **rewrite ingress tag symmetric** コマンドを設定できます。

この機能は、プライオリティタグのリライトタグ pop1 のみをサポートしています。

図 *2:* プライオリティタグのリライト



プライオリティタグのリライト設定

プライオリティタグ機能のリライトを設定するには、次のタスクを実行します。

```
Router#configure
Router(config)#interface FortyGigE0/5/0/0.1 l2transport
Router(config-subif)#encapsulation dot1q priority-tagged
Router(config-subif)#rewrite ingress tag pop 1 symmetric
Router(config-subif)#commit
```

実行コンフィギュレーション

この項では、プライオリティタグのリライトの実行コンフィギュレーションを示します。

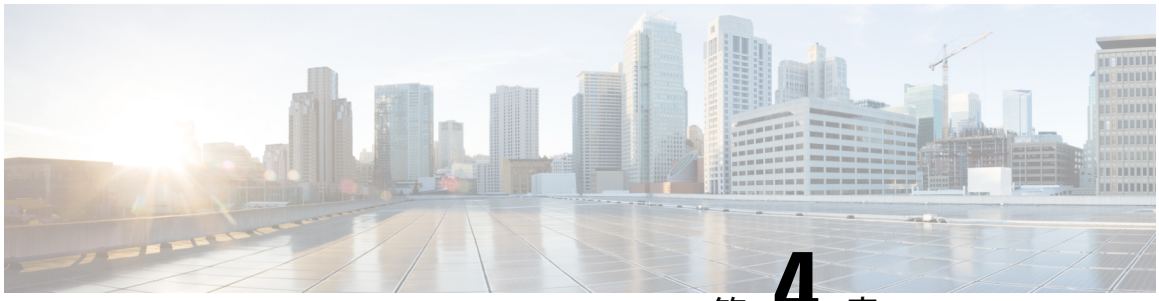
```
configure
 interface FortyGigE0/5/0/0.1 l2transport
  encapsulation dot1q priority-tagged
  rewrite ingress tag pop 1 symmetric
!
```

関連項目

プライオリティタグのリライト （43 ページ）

関連コマンド

- rewrite ingress tag pop 1 symmetric



第 4 章

L2CP トンネリング

システムは、次のトンネル プロトコルをサポートします。

- リンク層検出プロトコル（LLDP）
- リンク集約制御プロトコル（LACP）
- 運用、運営、および管理（OAM）
- イーサネット ローカル管理インターフェイス（ELMI）
- Cisco Discovery Protocol（CDP）

サブインターフェイスでは、LLDP や LACP などのコントロール パケットがトンネリングされると、システムは同じコントロールパケットをメインインターフェイスにトンネリングします。

ルータでは、CE 間にレイヤ 2 パケットをトンネリングできます。次の図に、レイヤ 2 プロトコルのトンネリングを示します。レイヤ 2 トラフィックが S ネットワークを通じて送信され、S ネットワークはトラフィックをエンドツーエンドで切り替えます。シスコのマルチキャスト アドレスがフレームに追加され、UNI から NNI に送信されます。逆のパス（NNI から UNI）では、プロトコル固有のマルチキャスト アドレスがフレームに付加され、UNI に送信されます。

L2CP トンネリングの前提条件

レイヤ 2 制御プロトコル トンネリングをサポートする Cisco IOS ソフトウェアを事前にルータにインストールしておく必要があります。

L2CP トンネリングの制限事項

- 受信した L2CP コントロール パケット（STP、CDP 他）は宛先ポートにミラーリングされません。
- ローカル クロスコネクトを介した L2CP トンネリング化パケットの転送はサポートされていません。

L2CP トンネリングの設定

プロトコル	パケット タイプ	アクション
CDP	タグなし	ピア
LACP	タグなし	ピア
LLDP	タグなし	ピア以外トンネル化
STP	タグなし	ピア
VTP	タグなし	ピア
OAM	タグなし	ピア
BPDU	タグなし	トンネル化
CDP	タグ付き	トンネル化
LACP	タグ付き	トンネル化
LLDP	タグ付き	トンネル化
STP	タグ付き	トンネル化
VTP	タグ付き	トンネル化
BPDU	タグ付き	トンネル化
OAM	タグ付き	トンネル化
ELMI	タグ付き	トンネル化

L2CP トンネリングを設定するには、次のステップを実行します。

```
/* Configure Attachment Circuit interface. *
RP/0/RP0/CPU0:ios(config)#int tenGigE 0/1/0/8/0
RP/0/RP0/CPU0:ios(config-if)#no shut
RP/0/RP0/CPU0:ios(config-if)#ipv4 addr 13.1.1.1/24
RP/0/RP0/CPU0:ios(config-if)#commit
Fri Sep  1 17:02:57.130 UTC
rRP/0/RP0/CPU0:ios(config-if)#int loop 1
RP/0/RP0/CPU0:ios(config-if)#ipv4 addr 2.2.2.6/32
RP/0/RP0/CPU0:ios(config-if)#commit
Fri Sep  1 17:03:08.163 UTC

RP/0/RP0/CPU0:ios(config)#l2vpn
RP/0/RP0/CPU0:ios(config-l2vpn)#xconnect group g1
RP/0/RP0/CPU0:ios(config-l2vpn-xc)#p2p 1
RP/0/RP0/CPU0:ios(config-l2vpn-xc-p2p)#int tenGigE 0/1/0/8/3.1
RP/0/RP0/CPU0:ios(config-l2vpn-xc-p2p)#neighbor  12.12.12.1 pw-id 1
```

```
RP/0/RP0/CPU0:ios(config-l2vpn-xc-p2p-pw)#commit
Fri Sep  1 17:11:19.516 UTC

/* Configure OSPF. */
RP/0/RP0/CPU0:ios(config-if)#router ospf 100 area 0
RP/0/RP0/CPU0:ios(config-ospf-ar)#int tenGigE 0/1/0/8/0
RP/0/RP0/CPU0:ios(config-ospf-ar-if)#int loop 1
RP/0/RP0/CPU0:ios(config-ospf-ar-if)#commit
Fri Sep  1 17:03:20.753 UTC
RP/0/RP0/CPU0:ios(config-ospf-ar-if)#exit
RP/0/RP0/CPU0:ios(config-ospf-ar)#exit
RP/0/RP0/CPU0:ios(config-ospf)#exit

/* Configure MPLS LDP. */
RP/0/RP0/CPU0:ios(config)#mpls ldp
RP/0/RP0/CPU0:ios(config-ldp)#int tenGigE 0/1/0/8/0
RP/0/RP0/CPU0:ios(config-ldp-if)#exit
RP/0/RP0/CPU0:ios(config-ldp)#
```

実行コンフィギュレーション

```
RP/0/RP0/CPU0:ios#   show run
Fri Sep  1 17:27:52.682 UTC
Building configuration...
!! IOS XR Configuration version = 6.4.1.11I
!! Last configuration change at Fri Sep  1 17:26:37 2017 by root
!
telnet vrf default ipv4 server max-servers 10
username root
group root-lr
group cisco-support
secret 5 $1$X9aA$9qdjKAnEbvNG8pfSNsgm/0
!
interface Loopback1
ipv4 address 2.2.2.6 255.255.255.255
!
interface MgmtEth0/RP0/CPU0/0
ipv4 address 5.10.10.122 255.255.0.0
!
interface TenGigE0/1/0/8/0
ipv4 address 13.1.1.1 255.255.255.0
!
interface TenGigE0/1/0/8/1
shutdown
!
interface TenGigE0/1/0/8/2
shutdown
!
interface TenGigE0/1/0/8/3
l2transport
!
!
controller Optics0/1/0/8
breakout 4x10
!
interface HundredGigE0/1/0/0
shutdown
!
interface HundredGigE0/1/0/1
shutdown
!
interface HundredGigE0/1/0/2
shutdown
!
```

```
interface HundredGigE0/1/0/3
shutdown
!
interface HundredGigE0/1/0/4
shutdown
!
interface HundredGigE0/1/0/5
shutdown
!
interface HundredGigE0/1/0/6
shutdown
!
interface HundredGigE0/1/0/7
shutdown
!
interface HundredGigE0/1/0/9
shutdown
!
interface HundredGigE0/1/0/10
shutdown
!
interface HundredGigE0/1/0/11
shutdown
!
interface HundredGigE0/1/0/12
shutdown
!
interface HundredGigE0/1/0/13
shutdown
!
interface HundredGigE0/1/0/14
shutdown
!
interface HundredGigE0/1/0/15
shutdown
!
interface HundredGigE0/1/0/16
shutdown
!
interface HundredGigE0/1/0/17
shutdown
!
interface HundredGigE0/1/0/18
shutdown
!
interface HundredGigE0/1/0/19
shutdown
!
interface HundredGigE0/1/0/20
shutdown
!
interface HundredGigE0/1/0/21
shutdown
!
interface HundredGigE0/1/0/22
shutdown
!
interface HundredGigE0/1/0/23
shutdown
!
router static
address-family ipv4 unicast
  202.153.144.0/24 5.10.0.1
!
```

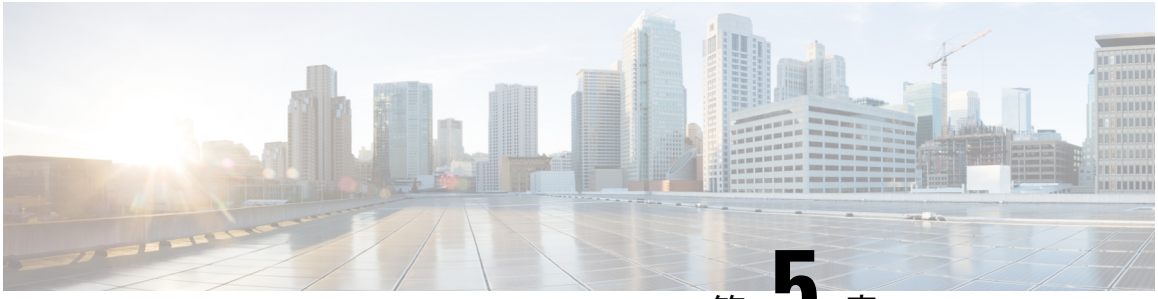
```
!
router ospf 100
area 0
  interface Loopback1
  !
  interface TenGigE0/1/0/8/0
  !
!
!

l2vpn
bridge group b1
  bridge-domain b1
   interface TenGigE0/1/0/8/3
   !
   vfi vf
    neighbor 12.12.12.1 pw-id 1
    !
   !
  !
!
!
mpls ldp
interface TenGigE0/1/0/8/0
!
!
end
```

確認

```
RP/0/RP0/CPU0:ios#show ospf neighbor
Fri Sep  1 17:24:43.641 UTC

* Indicates MADJ interface
# Indicates Neighbor awaiting BFD session up

Neighbors for OSPF 100

Neighbor ID     Pri   State           Dead Time   Address         Interface
12.12.12.1      1     FULL/DR         00:00:31    13.1.1.2        TenGigE0/1/0/8/0
    Neighbor is up for 00:21:15

Total neighbor count: 1
RP/0/RP0/CPU0:ios#show mpls ldp neighbor
Fri Sep  1 17:24:46.602 UTC

Peer LDP Identifier: 12.12.12.1:0
  TCP connection: 12.12.12.1:64120 - 2.2.2.6:646
  Graceful Restart: No
  Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 19/26; Downstream-Unsolicited
  Up time: 00:01:46
  LDP Discovery Sources:
    IPv4: (1)
      TenGigE0/1/0/8/0
    IPv6: (0)
  Addresses bound to this peer:
    IPv4: (8)
      5.5.5.1        5.10.23.254    12.12.12.1     13.1.1.2
      17.1.1.1       88.8.8.8       102.0.0.2      200.169.0.1
    IPv6: (0)

RP/0/RP0/CPU0:ios#show bgp neighbor
Fri Sep  1 17:24:50.158 UTC
```

```
BGP neighbor is 12.12.12.1
 Remote AS 15169, local AS 15169, internal link
 Remote router ID 88.8.8.8
  BGP state = Established, up for 00:00:05
  NSR State: None
  Last read 00:00:00, Last read before reset 00:00:00
  Hold time is 180, keepalive interval is 60 seconds
  Configured hold time: 180, keepalive: 60, min acceptable hold time: 3
  Last write 00:00:00, attempted 29, written 29
  Second last write 00:00:05, attempted 19, written 19
  Last write before reset 00:00:00, attempted 0, written 0
  Second last write before reset 00:00:00, attempted 0, written 0
  Last write pulse rcvd  Sep  1 17:24:50.144 last full not set pulse count 6
  Last write pulse rcvd before reset 00:00:00
  Socket not armed for io, armed for read, armed for write
  Last write thread event before reset 00:00:00, second last 00:00:00
  Last KA expiry before reset 00:00:00, second last 00:00:00
  Last KA error before reset 00:00:00, KA not sent 00:00:00
  Last KA start before reset 00:00:00, second last 00:00:00
  Precedence: internet
  Non-stop routing is enabled
  Multi-protocol capability received
  Neighbor capabilities:
    Route refresh: advertised (old + new) and received (old + new)
    4-byte AS: advertised and received
    Address family L2VPN VPLS: advertised and received
  Received 3 messages, 0 notifications, 0 in queue
  Sent 3 messages, 0 notifications, 0 in queue
  Minimum time between advertisement runs is 0 secs
  Inbound message logging enabled, 3 messages buffered
  Outbound message logging enabled, 3 messages buffered

For Address Family: L2VPN VPLS
  BGP neighbor version 1
  Update group: 0.2 Filter-group: 0.1  No Refresh request being processed
  NEXT_HOP is always this router
  Route refresh request: received 0, sent 0
  0 accepted prefixes, 0 are bestpaths
  Exact no. of prefixes denied : 0.
  Cumulative no. of prefixes denied: 0.
  Prefix advertised 0, suppressed 0, withdrawn 0
  Maximum prefixes allowed 2097152
  Threshold for warning message 75%, restart interval 0 min
  AIGP is enabled
  An EoR was received during read-only mode
  Last ack version 1, Last synced ack version 0
  Outstanding version objects: current 0, max 0
  Additional-paths operation: None
  Send Multicast Attributes

  Connections established 1; dropped 0
  Local host: 2.2.2.6, Local port: 34285, IF Handle: 0x00000000
  Foreign host: 12.12.12.1, Foreign port: 179
  Last reset 00:00:00
RP/0/RP0/CPU0:ios#

RP/0/RP0/CPU0:ios#show l2vpn bridge-domain
Fri Sep  1 17:27:25.002 UTC
Legend: pp = Partially Programmed.
Bridge group: b1, bridge-domain: b1, id: 0, state: up, ShgId: 0, MSTi: 0
  Aging: 300 s, MAC limit: 32000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 1 (1 up), VFIs: 1, PWs: 1 (1 up), PBBs: 0 (0 up), VNIs: 0 (0 up)
```

```
  List of ACs:
    Te0/1/0/8/3, state: up, Static MAC addresses: 0
  List of Access PWs:
  List of VFIs:
    VFI vf (up)
      Neighbor 12.12.12.1 pw-id 1, state: up, Static MAC addresses: 0
  List of Access VFIs:
RP/0/RP0/CPU0:ios#

RP/0/RP0/CPU0:ios#show l2vpn xconnect
Fri Sep  1 17:28:58.259 UTC
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

------------------------   -----------------------------   -----------------------------
1          1          UP    Te0/1/0/8/3            UP       12.12.12.1      1      UP

------------------------------------------------------------------------------------------
RP/0/RP0/CPU0:ios#

RP/0/RP0/CPU0:ios#show l2vpn xconnect
Fri Sep  1 17:28:58.259 UTC
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

------------------------   -----------------------------   -----------------------------
1          1          UP    Te0/1/0/8/3            UP       12.12.12.1      1      UP

------------------------------------------------------------------------------------------
RP/0/RP0/CPU0:ios#
```



第 5 章

ギガビット イーサネット リンク バンドルの設定

Cisco IOS XR ソフトウェアは、イーサネット インターフェイスのバンドルを形成する EtherChannel メソッドをサポートしています。EtherChannel は、ユーザがリンクを設定してバンドルに参加させることができるシスコ独自の技術であり、バンドル内のリンクに互換性があるかどうかを確認するための仕組みはありません。

IEEE 802.3ad カプセル化では、イーサネット バンドル内のすべてのメンバー リンクの互換性を確保するため、Link Aggregation Control Protocol（LACP）を採用しています。リンクに互換性がない、または障害が発生すると、そのリンクはバンドルから自動的に削除されます。

Cisco NCS 540 シリーズ ルータは 100G リンク バンドルをサポートしています。

制約事項

- 単一のイーサネット リンク バンドル内のすべてのリンクは 802.3ad（LACP）または EtherChannel（非 LACP）のいずれかを実行するように設定する必要があります。1 つのバンドル内の混合リンクはサポートされません。
- イーサネット リンク バンドルでは MAC アカウンティングはサポートされていません。
- 各イーサネット リンク バンドルでサポートされているリンクの最大数は 64 です。
- サポートされているイーサネット リンク バンドルの最大数は 1281024 です。

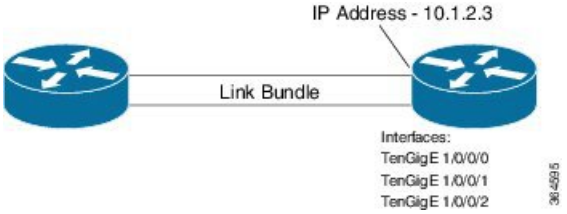
設定例

2 つのルータ間にリンク バンドルを作成するには、次の設定を実行する必要があります。

1. バンドル インスタンスの作成
2. バンドルへの物理インターフェイスのマッピング

次の図に値の例を示します。

図 *3:* リンク バンドルのトポロジ



イーサネットバンドルをアクティブにするには、バンドルの両方の接続エンドポイントで同じ設定を行う必要があります。

設定

```
/* Enter the global configuration mode and create the ethernet link bundle */
Router# configure
Router(config)# interface Bundle-Ether 3
Router(config-if)# ipv4 address 10.1.2.3 255.0.0.0
Router(config-if)# bundle maximum-active links 32 hot-standby
Router(config-if)# bundle minimum-active links 1
Router(config-if)# bundle minimum-active bandwidth 30000000
Router(config-if)# exit

/* Map physical interfaces to the bundle */
/* Note: Mixed link bundle mode is supported only when active-standby operation is
configured */
Router(config)# interface TenGigE 1/0/0/0
Router(config-if)# bundle id 3 mode on
Router(config-if)# no shutdown
Router(config)# exit

Router(config)# interface TenGigE 1/0/0/1
Router(config-if)# bundle id 3 mode on
Router(config-if)# no shutdown
Router(config-if)# exit

Router(config)# interface TenGigE 1/0/0/2
Router(config-if)# bundle id 3 mode on
Router(config-if)# no shutdown
Router(config-if)# exit
```

実行コンフィギュレーション

```
Router# show running-configuration
configure
interface Bundle-Ether 3
 ipv4 address 10.1.2.3 255.0.0.0
 bundle maximum-active links 32 hot-standby
 bundle minimum-active links 1
 bundle minimum-active bandwidth 30000000
!
interface TenGigE 1/0/0/0
 bundle-id 3 mode on
!

interface TenGigE 1/0/0/1
 bundle-id 3 mode on
```

```
!
interface TenGigE 1/0/0/2
 bundle-id 3 mode on
!
```

確認

バンドルを形成しているインターフェイスがアクティブであり、バンドルのステータスが Up であることを確認します。

```
Router# show bundle bundle-ether 3
Tue Feb  4 18:24:25.313 UTC

Bundle-Ether1
  Status:                                  Up
  Local links <active/standby/configured>:   3 / 0 / 3
  Local bandwidth <effective/available>:     30000000 (30000000) kbps
  MAC address (source):                      1234.1234.1234 (Configured)
  Inter-chassis link:                        No
  Minimum active links / bandwidth:          1 / 1 kbps
  Maximum active links:                      32
  Wait while timer:                          2000 ms
  Load balancing:                            Default
  LACP:                                      Not operational
    Flap suppression timer:                  Off
    Cisco extensions:                        Disabled
    Non-revertive:                           Disabled
  mLACP:                                     Not configured
  IPv4 BFD:                                  Not configured

  Port                  Device           State        Port ID         B/W, kbps
  --------------------  ---------------  -----------  --------------  ----------
  Te1/0/0/0             Local            Active       0x8000, 0x0000    10000000
      Link is Active
  Te1/0/0/1             Local            Active       0x8000, 0x0000    10000000
      Link is Active
  Te1/0/0/2             Local            Active       0x8000, 0x0000    10000000
      Link is Active

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

関連コマンド

- bundle maximum-active links
- interface Bundle-Ether
- show bundle Bundle-Ether
- VLAN バンドルの設定 （55 ページ）

VLAN バンドルの設定

VLANバンドルを作成する手順は、物理イーサネットインターフェイスにVLANサブインターフェイスを作成する手順と同じです。

設定例

VLAN バンドルを設定するには、次の設定を実行します。

- バンドル インスタンスを作成します。
- VLAN インターフェイス（バンドル サブインターフェイス）を作成します。
- バンドルに物理インターフェイスをマッピングします。

アクティブにする VLAN バンドルでは、VLAN バンドルの両方のエンド ポイントで同じ設定を実行する必要があります。

設定

```
/* Enter global configuration mode and create VLAN bundle */
Router# configure
Router(config)# interface Bundle-Ether 2
Router(config-if)# ipv4 address 50.0.0.1/24
Router(config-if)# bundle maximum-active links 32 hot-standby
Router(config-if)# bundle minimum-active bandwidth 30000000
Router(config-if)# bundle minimum-active links 1
Router(config-if)# commit

/* Create VLAN sub-interface and add to the bundle */
Router(config)# interface Bundle-Ether 2.201
Router(config-subif)# ipv4 address 12.22.1.1 255.255.255.0
Router(config-subif)# encapsulation dot1q 201
Router(config-subif)# commit

/* Map the physical interface to the bundle */
Router(config)# interface TenGigE 0/0/0/14
Router(config-if)# bundle id 2 mode on
Router(config-if)# no shutdown
Router(config-if)# commit

/* Repeat the above steps for all the member interfaces:
   0/0/0/15, 0/0/0/16 and 0/0/0/17 in this example */
```

実行コンフィギュレーション

```
configure
interface Bundle-Ether2
 ipv4 address 50.0.0.1 255.255.255.0
 mac-address 1212.1212.1212
 bundle maximum-active links 32 hot-standby
 bundle minimum-active links 1
 bundle minimum-active bandwidth 30000000
!
interface Bundle-Ether2.201
 ipv4 address 12.22.1.1 255.255.255.0
 encapsulation dot1q 201
!
interface TenGigE0/0/0/14
 bundle id 2 mode on
!
interface TenGigE0/0/0/15
 bundle id 2 mode on
!
```

```
interface TenGigE0/0/0/16
 bundle id 2 mode on
!
interface TenGigE0/0/0/17
 bundle id 2 mode on
!
```

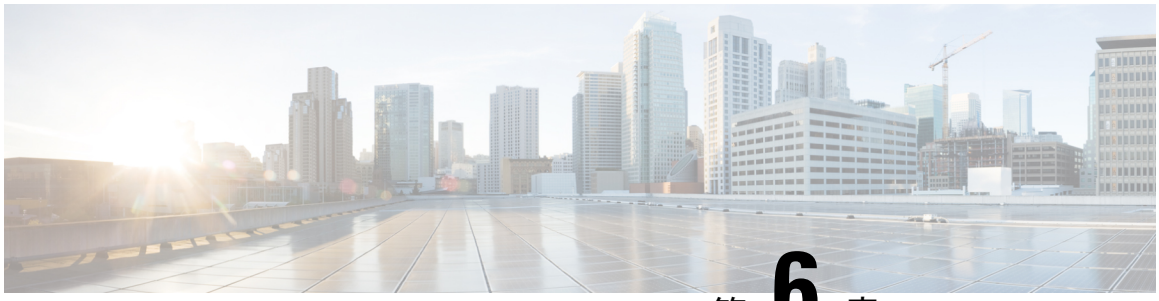
確認

VLAN ステータスが UP であることを確認します。

```
Router# show interfaces bundle-ether 2.201

Wed Feb  5 17:19:53.964 UTC
Bundle-Ether2.201 is up, line protocol is up
  Interface state transitions: 1
  Hardware is VLAN sub-interface(s), address is 28c7.ce01.dc7b
  Internet address is 12.22.1.1/24
  MTU 1518 bytes, BW 20000000 Kbit (Max: 20000000 Kbit)
     reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation 802.1Q Virtual LAN, VLAN Id 201,  loopback not set,
  Last link flapped 07:45:25
  ARP type ARPA, ARP timeout 04:00:00
  Last input 00:00:00, output never
  Last clearing of "show interface" counters never
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     2938 packets input, 311262 bytes, 0 total input drops
  - - -
  - - -
```

関連コマンド

- bundle maximum-active links
- interface Bundle-Ether
- show bundle Bundle-Ether



第 6 章

Ethernet over MPLS

Ethernet-over-MPLS（EoMPLS）は、MPLS 対応、レイヤ 3 コアを通じてイーサネット トラフィックのトンネリング メカニズムを提供し、（ラベル スタックを使用して）イーサネット プロトコルデータ ユニット（PDU）を MPLS パケット内部にカプセル化して、それらを MPLS ネットワーク経由で転送します。

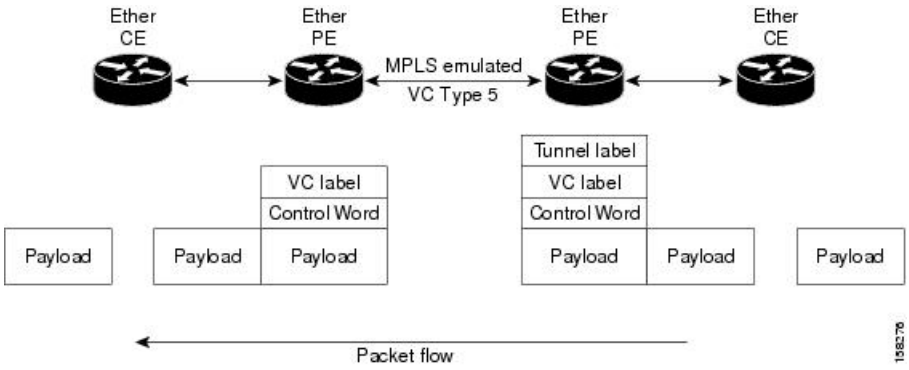
次の項では、EoMPLS を実装するさまざまなモードについて説明します。

イーサネット ポート モード

イーサネット ポート モードでは、疑似回線の両端がイーサネット ポートに接続されます。このモードでは、ポートが疑似回線を介してトンネル化されるか、またはローカル スイッチング（接続回線から接続回線へのクロス コネクトと呼ばれる）を使用して、1 つの接続回線（AC）から同じ PE ノードに接続されている別の AC にパケットまたはフレームを切り替えます。

次の図に、イーサネット ポート モードのパケット フローの例を示します。

図 *4:* イーサネット ポート モードのパケット フロー

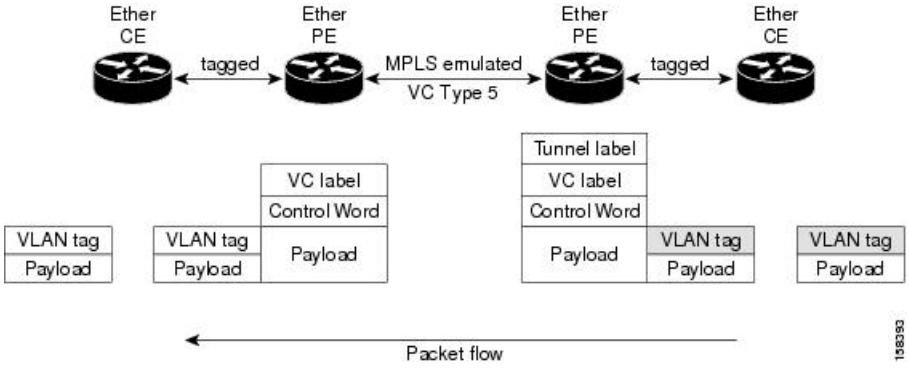


VLAN モード

VLANモードでは、カスタマー側とプロバイダー側のリンクで、各VLANは、仮想接続（VC）タイプ 4 またはVC タイプ 5 を使用して個別 L2VPN 接続として設定できます。VC タイプ 5 がデフォルト モードです。

次の図に示されているように、イーサネット PE は、入力ポートから疑似回線にトラフィックを内部的に切り替えるために、イーサネット ポートに内部 VLAN タグを関連付けます。ただし、疑似回線にトラフィックを移動する前に、内部 VLAN タグを削除します。

図 *5: VLAN* モードのパケット フロー



出力 VLAN PE では、PE は、疑似回線から到着するフレームに VLAN タグを関連付け、トラフィックを内部的に切り替えた後、イーサネット トランク ポートにトラフィックを送信します。

（注） ポートがトランク モードであるため、VLAN PE は VLAN タグを削除せず、追加されたタグを持つポート経由でフレームを転送します。

QinQ モード

QinQ は、複数の 802.1Q タグ（IEEE 802.1QinQ VLAN タグ スタッキング）を指定するための 802.1Q の拡張です。レイヤ 3 VPN サービス終了および L2VPN サービス転送は、QinQ サブインターフェイスではイネーブルです。

Cisco NCS 500x シリーズ ルータは、プロバイダー エッジ ルータでのサブインターフェイスの設定に応じて、レイヤ 2 トンネリングまたはレイヤ 3 転送を実装します。この機能は、ルータ上の最大 2 つの QinQ タグのみをサポートします。

- L2VPN 接続回線のレイヤ 2 QinQ VLAN：QinQ L2VPN 接続回線は、仮想回線タイプ 4 とタイプ 5 の両方の疑似回線を使用して、ポイントツーポイント EoMPLS ベースのクロス コネクト用と、802.1q VLAN およびポート モードでの QinQ の完全なインターワーキングのサポートなど、ポイントツーポイント ローカル スイッチングベースのクロス コネクト用のレイヤ 2 転送サブインターフェイスで設定されます。
- レイヤ 3 QinQ VLAN：レイヤ 3 の終端ポイントとして使用されます。VLAN はいずれも入力プロバイダーエッジで削除され、フレームが転送されるときリモートプロバイダーエッジで追加され戻されます。

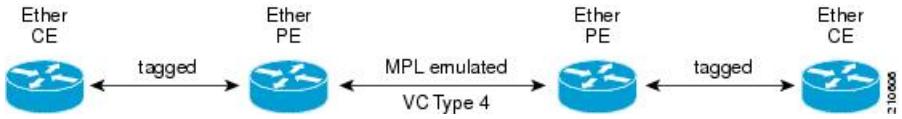
QinQ 上のレイヤ 3 サービスは次のとおりです。

- IPv4 ユニキャストおよびマルチキャスト
- IPv6 ユニキャストおよびマルチキャスト
- MPLS
- Intermediate System-to-Intermediate System（IS-IS）で使用されるコネクションレス型ネットワーク サービス（CLNS）

QinQ モードでは、各 CE VLAN は SP VLAN 内に伝送されます。QinQ モードでは VC タイプ 5 を使用する必要がありますが、VC タイプ 4 もサポートされます。各イーサネット PE では、内部（CE VLAN）と外部（SP VLAN）の両方を設定する必要があります。

次の図に、VC タイプ 4 を使用した QinQ を示します。

図 *6 : QinQ* を介した *EoMPLS* モード



（注） EoMPLS は、疑似回線のスティッチングおよびマルチセグメントをサポートしていません。

接続回線間のローカル スイッチングの設定

ローカル スイッチングでは、1 つの接続回線（AC）から別の AC へと、同じルータ上の同じタイプの 2 つのインターフェイス間で L2 データの交換が行われます。ローカルスイッチング接続で設定されている 2 つのポートで接続回線（AC）を形成します。ローカル スイッチング接続の動作は、2つのブリッジポートしかないブリッジドメインの動作と似ており、トラフィックはローカル接続の一方のポートに入り、もう一方のポートを通じて出て行きます。

レイヤ 2 ローカル スイッチングには次のような特性があります。

- レイヤ 2 ローカル スイッチングでは、レイヤ 3 IP アドレスの代わりにレイヤ 2 MAC アドレスを使用します。
- ローカル接続に関するブリッジングがないため、MAC 学習やフラッディングはありません。
- ブリッジ ドメインとは異なり、インターフェイスの状態が DOWN の場合、ローカル接続の AC は UP 状態ではありません
- ローカル スイッチング AC は、レイヤ 2 トランク（メイン）インターフェイス、バンドル インターフェイス、EFP など、多種多様なレイヤ 2 インターフェイスを使用します。
- 同一ポートのローカルスイッチング機能を使用すると、同じインターフェイス上の2つの回線の間でレイヤ 2 データをスイッチングできます。

制約事項

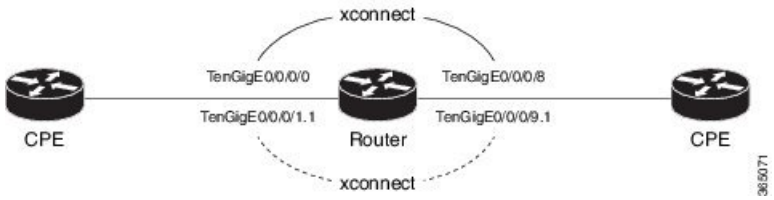
- 所定の物理ポートにあるすべてのサブインターフェイスは、次のような2つのタグプロトコル識別子（TPID）のみをサポートしています。
  - 0x88a8、0x8100
  - 0x9100、0x8100
  - 0x9200、0x8100
- VLAN および TPID ベースの入力パケット フィルタリングはサポートされていません。
- 出力 TPID の書き換えはサポートされていません。

トポロジ

接続回線（AC）は、カスタマー エッジ（CE）ルータをプロバイダー エッジ（PE）ルータにバインドします。PE ルータは MPLS ネットワークを介して疑似回線を使用し、リモート PE ルータとルートを交換します。レイヤ 2 VPN でポイントツーポイント接続をカスタマー エッジ（CE）ルータから別のルータ（リモート ルータ）に確立するには、接続回線を疑似回線にバインドするメカニズムが必要です。接続回線を疑似回線にバインドしてレイヤ 2 VPN でのポイントツーポイント接続をエミュレートするには、クロスコネクト回線（CCC）を使用します。

設定には次のトポロジを使用します。

図 7: 接続回線間のローカル スイッチング



設定

AC-AC ローカル スイッチングを設定するには、次の設定を実行します。

- メイン インターフェイス上でレイヤ 2 転送を有効にします。
- L2 転送を有効にしたサブインターフェイスを作成し、それぞれに対して個別のカプセル化を指定します。
- メイン インターフェイス間およびサブインターフェイス間のローカル スイッチングを有効にします。
  - クロスコネクト グループを設定します。
  - ポイントツーポイント クロス コネクト回線（CCC）を作成します。
  - インターフェイスをポイントツーポイント クロス コネクト グループに割り当てます。

```
/* Enter the interface configuration mode and configure
  L2 transport on the TenGigE interfaces */
Router# configure
Router(config)# interface TenGigE 0/0/0/1 l2transport
Router(config-if-l2)# no shutdown
Router(config-if)# exit
Router(config)# interface TenGigE 0/0/0/9 l2transport
Router(config-if-l2)# no shutdown
Router(config-if-l2)# commit

/* Configure L2 transport and encapsulation on the VLAN sub-interfaces */
Router# configure
Router(config)# interface TenGigE 0/0/0/0.1 l2transport
Router(config-subif)# encapsulation dot1q 5
Router(config-subif)# exit
Router(config)# interface TenGigE 0/0/0/8.1 l2transport
Router(config-subif)# encapsulation dot1q 5
Router(config-subif)# commit


/* Configure ethernet link bundles */
Router# configure
Router(config)# interface Bundle-Ether 3
Router(config-if)# ipv4 address 10.1.3.3 255.0.0.0
Router(config-if)# bundle maximum-active links 32 hot-standby
Router(config-if)# bundle minimum-active links 1
Router(config-if)# bundle minimum-active bandwidth 30000000
Router(config-if)# exit
```

```
Router(config)# interface Bundle-Ether 2
Router(config-if)# ipv4 address 10.1.2.2 255.0.0.0
Router(config-if)# bundle maximum-active links 32 hot-standby
Router(config-if)# bundle minimum-active links 1
Router(config-if)# bundle minimum-active bandwidth 30000000
Router(config-if)# exit

/* Add physical interfaces to the ethernet link bundles */
Router(config)# interface TenGigE 0/0/0/1
Router(config-if)# bundle id 3 mode on
Router(config-if)# no shutdown
Router(config)# exit
Router(config)# interface TenGigE 0/0/0/2
Router(config-if)# bundle id 3 mode on
Router(config-if)# no shutdown
Router(config)# exit
Router(config)# interface TenGigE 0/0/0/9
Router(config-if)# bundle id 2 mode on
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface TenGigE 0/0/0/8
Router(config-if)# bundle id 2 mode on
Router(config-if)# no shutdown
Router(config-if)# exit

/* Configure Layer 2 transport on the ethernet link bundles */
Router(config)# interface Bundle-Ether 3 l2transport
Router(config-if-l2)# no shutdown
Router(config-if)# exit
Router(config)# interface Bundle-Ether 2 l2transport
Router(config-if-l2)# no shutdown
Router(config-if-l2)# commit

/* Configure local switching on the TenGigE Interfaces */
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group XCON1
Router(config-l2vpn-xc)# p2p XCON1_P2P3
Router(config-l2vpn-xc-p2p)# interface TenGigE0/0/0/1
Router(config-l2vpn-xc-p2p)# interface TenGigE0/0/0/9
Router(config-l2vpn-xc-p2p)# commit
Router(config-l2vpn-xc-p2p)# exit

/* Configure local switching on the VLAN sub-interfaces */
Router(config-l2vpn-xc)# p2p XCON1_P2P1
Router(config-l2vpn-xc-p2p)# interface TenGigE0/0/0/0.1
Router(config-l2vpn-xc-p2p)# interface TenGigE0/0/0/8.1
Router(config-l2vpn-xc-p2p)# commit
Router(config-l2vpn-xc-p2p)# exit

/* Configure local switching on ethernet link bundles */
Router(config-l2vpn-xc)# p2p XCON1_P2P4
Router(config-l2vpn-xc-p2p)# interface Bundle-Ether 3
Router(config-l2vpn-xc-p2p)# interface Bundle-Ether 2
Router(config-l2vpn-xc-p2p)# commit
```

実行コンフィギュレーション

```
configure
```

```
 interface tenGigE 0/0/0/1 l2transport
 !
 interface tenGigE 0/0/0/9 l2transport
 !
!

interface tenGigE 0/0/0/0.1 l2transport
 encapsulation dot1q 5
 rewrite ingress tag push dot1q 20 symmetric
 !
interface tenGigE 0/0/0/8.1 l2transport
  encapsulation dot1q 5
 !
interface Bundle-Ether 3 l2transport
 !
interface Bundle-Ether 2 l2transport
!

l2vpn
 xconnect group XCON1
   p2p XCON1_P2P3
    interface TenGigE0/0/0/1
    interface TenGigE0/0/0/9
    !
   !
 !
l2vpn
 xconnect group XCON1
   p2p XCON1_P2P1
    interface TenGigE0/0/0/0.1
    interface TenGigE0/0/0/8.1
    !
   !
 !
l2vpn
 xconnect group XCON1
   p2p XCON1_P2P4
    interface Bundle-Ether 3
    interface Bundle-Ether 2
    !
   !
 !
```

確認

- 設定されたクロスコネクトが動作しているかどうかを確認します

```
router# show l2vpn xconnect brief

Locally Switching

  Like-to-Like                          UP        DOWN        UNR

    EFP                                  1           0          0

    Total                                1           0          0


  Total                                  1           0          0

Total: 1 UP, 0 DOWN, 0 UNRESOLVED
```

```
router# show 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
------------------------
------------------------------------------------------------------
XCON1      XCON_P2P1 UP    Te0/0/0/1      UP  Te0/0/0/9      UP
XCON1      XCON_P2P3 UP    Te0/0/0/0.1    UP  Te0/0/0/8.1    UP
-------------------------------------------------------------------------------------------
```

関連コマンド

- interface（p2p）
- l2vpn
- p2p
- xconnect group

クロスコネクト回線を使用したスタティック ポイントツーポイント接続の設定

この項では、レイヤ 2 VPN にスタティック ポイントツーポイント クロス コネクトを設定する方法について説明します。

要件および制約事項

レイヤ2 VPNにクロスコネクト回線を設定する前に、次の要件が満たされていることを確認します。

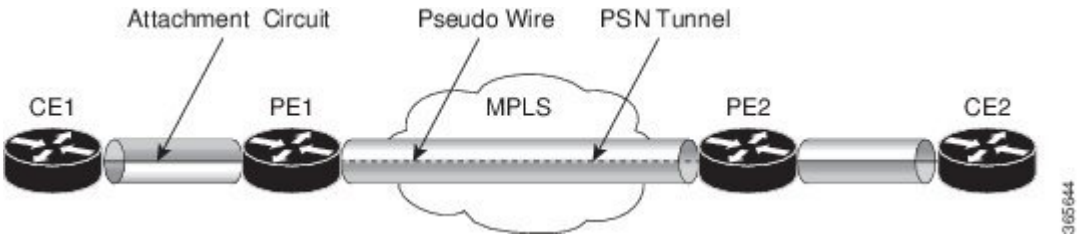
- CE ルータと PE ルータは MPLS ネットワークで動作するように設定されています。
- クロスコネクト回線の名前が PE のペアを識別するように設定されており、クロスコネクト グループ内で一意である必要があります。
- セグメント（接続回線または疑似回線）は一意であり、単一のクロスコネクト回線にのみ属すことができます。
- スタティック仮想回線のローカル ラベルはグローバルに一意であり、1 つの疑似回線にのみ使用できます。
- PE ルータ ごとに最大 4000 のクロスコネクトを設定できます。

（注） スタティック疑似回線接続はシグナリングに LDP を使用しません。

トポロジ

レイヤ 2 VPN にスタティック クロスコネクト回線を設定するには、次のトポロジを使用します。

図 *8 :* レイヤ *2 VPN* のスタティック クロスコネクト回線



設定

```
/* Configure PE1 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group XCON1
Router(config-l2vpn-xc)# p2p xc1
Router(config-l2vpn-xc-p2p)# interface gigabitethernet0/1/0/0.1
Router(config-l2vpn-xc-p2p)# neighbor 10.165.100.151 pw-id 100
Router(config-l2vpn-xc-p2p-pw)# mpls static label local 50 remote 40
Router(config-l2vpn-xc-p2p-pw)# commit
```

```
/*Configure PE2 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group XCON1
Router(config-l2vpn-xc)# p2p xc1
Router(config-l2vpn-xc-p2p)# interface gigabitethernet0/2/0/0.4
Router(config-l2vpn-xc-p2p)# neighbor 10.165.200.254 pw-id 100
Router(config-l2vpn-xc-p2p-pw)# mpls static label local 40 remote 50
Router(config-l2vpn-xc-p2p-pw)# commit
```

実行コンフィギュレーション

```
/* On PE1 */
!
l2vpn
 xconnect group XCON1
  p2p xc1
   interface GigabitEthernet0/1/0/0.1
   neighbor ipv4 10.165.100.151 pw-id 100
    mpls static label local 50 remote 40
!

/* On PE2 */
!
l2vpn
 xconnect group XCON2
```

```
 p2p xc1
  interface GigabitEthernet0/2/0/0.4
  neighbor ipv4 10.165.200.254 pw-id 100
   mpls static label local 40 remote 50
 !
```

確認

```
/* Verify the static cross connect on PE1 */
Router# show l2vpn xconnect
Tue Apr 12 20:18:02.971 IST
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

------------------------   ------------------------------   ------------------------------
XCON1      xc1        UP    Gi0/1/0/0.1            UP       10.165.100.151  100    UP

-------------------------------------------------------------------------------------------

/* Verify the static cross connect on PE2 */

Router# show l2vpn xconnect
Tue Apr 12 20:18:02.971 IST
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

------------------------   ------------------------------   ------------------------------
XCON2      xc1        UP    Gi0/2/0/0.4            UP       10.165.200.254  100    UP

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

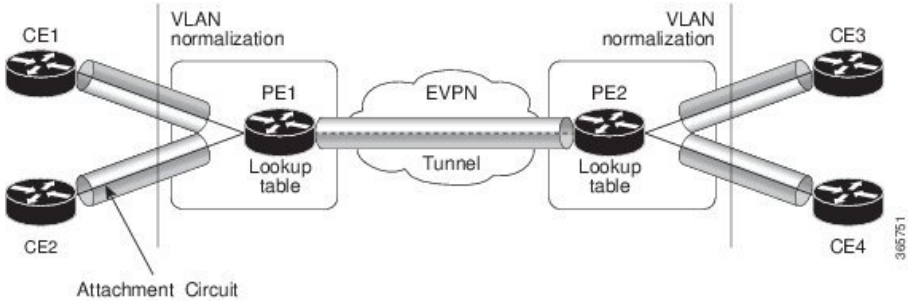
フレキシブル クロスコネクト サービス

フレキシブル クロスコネクト サービス機能では、同じプロバイダー エッジ（PE）上の単一のイーサネット VPN 仮想プライベート ワイヤ サービス（EVPN-VPWS）サービス内の複数のエンドポイントにわたって接続回線（AC）を集約することができます。AC は、一重 VLAN タグか、または二重 VLAN タグのいずれかで表されます。リモート PE 上の同じ VLAN タグで関連付けられた AC がクロスコネクトです。VLAN タグは、インターフェイス上のフレームを適切なサービス インスタンスにマッピングするために使用する一致基準を定義します。その結果、ルックアップ テーブルを作成するには、VLAN 書き換え値がフレキシブル クロスコネクト（FXC）インスタンス内で一意である必要があります。VLAN タグは書き換え設定を使用して一意に作成できます。ルックアップテーブルは、対応する宛先 AC にトラフィックを転送するために取るパスの決定に役立ちます。この機能は、多くのインターフェイスにわたって VLAN を多重化することで、トンネル数を削減します。また、ルータが使用する MPLS ラベル数も削減します。この機能は、シングルホーミングとマルチホーミングの両方をサポートします。

フレキシブル クロスコネクト サービス：シングルホーム

AC を通じた CE1 と CE2 から PE1 へのトラフィック フローの次のトポロジを考えてみます。AC は同じ PE1 上の複数のエンドポイント全体にわたって集約されています。VLAN（書き換え）は、PE1 上の AC インターフェイスに設定されている書き換えに基づいてルックアップ テーブルを作成します。PE1 は BGP を使用して PE2 とルートを交換し、EVPN MPLS ネットワーク上にトンネルを作成します。PE2 の VLAN（書き換え）は、PE1 に設定されている書き換えと一致している必要があります。書き換えタグに基づいて、PE2はトラフィックを対応する AC に転送します。たとえば、CE1 と CE2 の AC が同じ書き換えタグで設定されている場合、エンドツーエンド トラフィックは CE1 から CE3 に送信されます。

図 *9:* フレキシブル クロスコネクト サービス

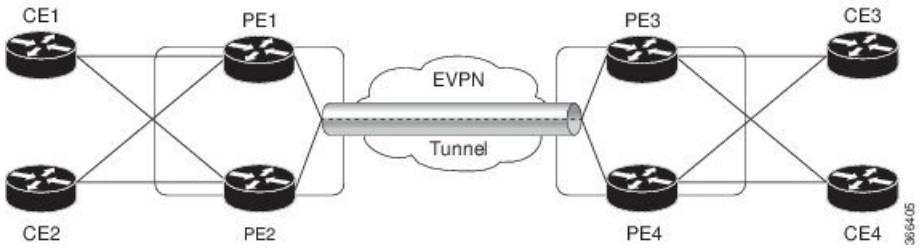


フレキシブル クロスコネクト サービス：マルチホーム

フレキシブルクロスコネクトサービスのマルチホーミング機能では、カスタマーエッジ（CE）デバイスを 2 台以上のプロバイダー エッジ（PE）デバイスに接続し、ロードバランシングと冗長接続を提供します。PE と CE 間のトラフィックの送信にフローベースのロード バランシングが使用されます。送信元とリモートの PE の接続にもフローベースのロード バランシングが使用されます。カスタマー エッジ デバイスは、イーサネット バンドル インターフェイスを通じて PE に接続されます。

CE デバイスが 2 つ以上の PE のマルチホームで、すべての PE が VLAN のマルチホーム デバイスとの間で発着信するトラフィックを転送できる場合のマルチホーミングをオールアクティブ マルチホーミングと呼びます。

図 *10:* フレキシブル クロスコネクト サービス マルチホーム



CE1 と CE2 が PE1 と PE2 のマルチホームで、CE3 と CE4 が PE3 と PE4 のマルチホームであるトポロジを考えてみます。PE1 と PE2 はイーサネット A-D のイーサネット接続（ES-EAD）

ルートをリモート PE、つまり PE3 と PE4 にアドバタイズします。同様に、PE3 と PE4 は ES-EAD ルートをリモート PE、つまり PE1 と PE2 にアドバタイズします。ES-EAD ルートはメイン インターフェイスごとにアドバタイズされます。

CE1 から CE3 へのトラフィック フローを考えてみます。PE1 または PE2 のいずれかにトラフィックが送信されます。パスの選択は、LAG を介して転送する CE の実装によって異なります。トラフィックは各 PE でカプセル化され、MPLS トンネルを通じてリモート PE（PE3 と PE4）に転送されます。宛先 PE の選択は、フローベースのロード バランシングによって確立されます。PE3 と PE4 は CE3 にトラフィックを送信します。PE3 または PE4 から CE3 へのパスの選択は、フローベースのロードバランシングによって確立されます。

フレキシブルクロスコネクトサービスサポート対象モード

フレキシブル クロスコネクト サービス機能は、次のモードをサポートしています

- VLAN 非対応
- VLAN 対応
- ローカル スイッチング

VLAN 非対応

この動作モードでは、単一のエンドポイントまたはインターフェイス宛の単一の ES 上で正規化されている AC のグループは、単一の VPWS サービス ID で表される単一の EVPN VPWS トンネルに多重化されます。VLAN 非対応 FXC は、BGP の状態の数を低減します。VLAN 障害は、BGP を介して通知されません。AC ごとではなく、VLAN 非対応 FXC ごとに 1 つの EVI/EAD ルートがアドバタイズされます。マルチホーミング シナリオでは、ES-EAD ルートもあります。EVI は他の VLAN 非対応 FXC または EVPN VPWS と共有できます。AC が PE1 上でダウンした場合、リモート PE には障害が通知されず、PE3 または PE 4 はトラフィックを PE1 と PE2 に送信し続けた結果、パケットがドロップされます。

マルチホーミングは、すべての AC が同じメインインターフェイスに属している場合にのみ、VLAN 非対応 FXC でサポートされます。

ESI が複数ある場合は、ゼロ ESI か非ゼロ ESI かに関係なく、ESI 0 のみがシグナリングされます。このシナリオでは、シングルホーム モードのみがサポートされています。

VLAN 非対応を使用したシングルホーム フレキシブル クロスコネクト サービスの設定

この項では、VLAN 非対応を使用してシングルホーム フレキシブル クロスコネクト サービスを設定する方法について説明します。

```
/* Configure PE1 */
Router# configure
Router(config)# interface GigabitEthernet 0/2/0/3.1 l2transport
```

```
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-2 dot1q 500 second-dot1q
 100 symetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)# interface GigabitEthernet 0/2/0/0.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-2 dot1q 600 second-dot1q
 200 symetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-unaware fxs1
Router(config-l2vpn-fxs-vu)# interface GigabitEthernet 0/2/0/3.1
Router(config-l2vpn-fxs-vu)# interface GigabitEthernet 0/2/0/0.1
Router(config-l2vpn-fxs-vu)# neighbor evpn evi 1 target 1
Router(config-l2vpn-fxs-vu)# commit

/* Configure PE2 */
Router# configure
Router(config)# interface GigabitEthernet 0/0/0/3.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-2 dot1q 500 second-dot1q
 100 symetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)# interface GigabitEthernet 0/0/0/0.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-2 dot1q 600 second-dot1q
 200 symetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-unaware fxs1
Router(config-l2vpn-fxs-vu)# interface GigabitEthernet 0/0/0/3.1
Router(config-l2vpn-fxs-vu)# interface GigabitEthernet 0/0/0/0.1
Router(config-l2vpn-fxs-vu)# neighbor evpn evi 1 target 1
Router(config-l2vpn-fxs-vu)# commit
```

実行コンフィギュレーション

```
/* On PE1 */
!
Configure
interface GigabitEthernet 0/2/0/3.1 l2transport
  encapsulation dot1q 1
  rewrite ingress tag translate 1-to-2 dot1q 500 second-dot1q 100 symetric
!

Configure
interface GigabitEthernet 0/2/0/0.1 l2transport
  encapsulation dot1q 1
  rewrite ingress tag translate 1-to-2 dot1q 600 second-dot1q 200 symetric
!

l2vpn
  flexible-xconnect-service vlan-unaware fxs1
   interface GigabitEthernet 0/2/0/3.1
   interface GigabitEthernet0/2/0/0.1
   neighbor evpn evi 1 target 1

!
```

```
/* On PE2 */
!
Configure
interface GigabitEthernet 0/0/0/3.1 l2transport
  encapsulation dot1q 1
  rewrite ingress tag translate 1-to-2 dot1q 500 second-dot1q 100 symetric
!

Configure
interface GigabitEthernet 0/0/0/0.1 l2transport
  encapsulation dot1q 1
  rewrite ingress tag translate 1-to-2 dot1q 600 second-dot1q 200 symetric
!

l2vpn
  flexible-xconnect-service vlan-unaware fxs1
   interface GigabitEthernet 0/0/0/3.1
   interface GigabitEthernet0/0/0/0.1
   neighbor evpn evi 1 target 1

!
```

VLAN 非対応を使用したマルチホーム フレキシブル クロスコネクト サービスの設定

この項では、VLAN 非対応を使用してマルチホーム フレキシブル クロスコネクト サービスを設定する方法について説明します。

```
/* Configure PE1 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-unaware fxc1_16
Router(config-l2vpn-fxs)# interface Bundle-Ether10.11
Router(config-l2vpn-fxs)# interface Bundle-Ether10.12
Router(config-l2vpn-fxs)# neighbor evpn evi 1 target 16
Router(config-l2vpn-fxs)# commit
Router(config-l2vpn-fxs)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether10.11 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-1 dot1q 11 symmetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)# interface Bundle-Ether10.12 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 2
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-1 dot1q 12 symmetric
Router(config-subif)# commit
Router(config-subif)# exit
Router(config)# evpn
Router (config-evpn)# interface Bundle-Ether10
Router (config-evpn-ac)# ethernet-segment
Router (config-evpn-ac-es)# identifier type  0 00.01.00.ac.ce.55.00.0a.00
Router (config-evpn-ac-es)# commit

/* Configure PE2 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-unaware fxc1_16
Router(config-l2vpn-fxs)# interface Bundle-Ether10.11
Router(config-l2vpn-fxs)# interface Bundle-Ether10.12
Router(config-l2vpn-fxs)# neighbor evpn evi 1 target 16
Router(config-l2vpn-fxs)# commit
```

```
Router(config-l2vpn-fxs)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether10.11 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-1 dot1q 11 symmetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)# interface Bundle-Ether10.12 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 2
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-1 dot1q 12 symmetric
Router(config-subif)# commit
Router(config-subif)# exit
Router(config)# evpn
Router (config-evpn)# interface Bundle-Ether10
Router (config-evpn-ac)# ethernet-segment
Router (config-evpn-ac-es)# identifier type  0 00.01.00.ac.ce.55.00.0a.00
Router (config-evpn-ac-es)# commit

/* Configure PE3 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-unaware fxc1_16
Router(config-l2vpn-fxs)# interface Bundle-Ether20.11
Router(config-l2vpn-fxs)# interface Bundle-Ether20.12
Router(config-l2vpn-fxs)# neighbor evpn evi 1 target 16
Router(config-l2vpn-fxs)# commit
Router(config-l2vpn-fxs)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether20.11 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-1 dot1q 11 symmetric
Router(config-l2vpn-subif)# commit
Router(config-subif)# exit
Router(config)# interface Bundle-Ether20.12 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 2
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-1 dot1q 12 symmetric
Router(config-l2vpn-subif)# commit
Router(config-subif)# exit
Router(config)# evpn
Router (config-evpn)# interface Bundle-Ether20
Router (config-evpn-ac)# ethernet-segment
Router (config-evpn-ac-es)# identifier type  0 00.01.00.ac.ce.55.00.14.00
Router (config-evpn-ac-es)# commit

/* Configure PE4 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-unaware fxc1_16
Router(config-l2vpn-fxs)# interface Bundle-Ether20.11
Router(config-l2vpn-fxs)# interface Bundle-Ether20.12
Router(config-l2vpn-fxs)# neighbor evpn evi 1 target 16
Router(config-l2vpn-fxs)# commit
Router(config-l2vpn-fxs)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether20.11 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-1 dot1q 11 symmetric
Router(config-l2vpn-subif)# commit
Router(config-subif)# exit
Router(config)# interface Bundle-Ether20.12 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 2
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-1 dot1q 12 symmetric
Router(config-l2vpn-subif)# commit
```

```
Router(config-subif)# exit
Router(config)# evpn
Router (config-evpn)# interface Bundle-Ether20
Router (config-evpn-ac)# ethernet-segment
Router (config-evpn-ac-es)# identifier type  0 00.01.00.ac.ce.55.00.14.00
Router (config-evpn-ac-es)# commit
```

実行コンフィギュレーション

```
/* On PE1 */

configure
l2vpn
 flexible-xconnect-service vlan-unaware fxc1_16
  interface Bundle-Ether10.11
  interface Bundle-Ether10.12
  neighbor evpn evi 1 target 16

!

configure
interface Bundle-Ether10.11 l2transport
  encapsulation dot1q 1
  rewrite ingress tag translate 1-to-1 dot1q 11 symmetric

!


configure
interface Bundle-Ether10.12 l2transport
  encapsulation dot1q 2
  rewrite ingress tag translate 1-to-1 dot1q 12 symmetric

!

evpn
  interface Bundle-Ether10
   ethernet-segment identifier type 0 00.01.00.ac.ce.55.00.0a.00

!

/* On PE2 */

configure
l2vpn
 flexible-xconnect-service vlan-unaware fxc1_16
  interface Bundle-Ether10.11
  interface Bundle-Ether10.12
  neighbor evpn evi 1 target 16

!

configure
interface Bundle-Ether10.11 l2transport
  encapsulation dot1q 1
  rewrite ingress tag translate 1-to-1 dot1q 11 symmetric

!


configure
interface Bundle-Ether10.12 l2transport
  encapsulation dot1q 2
```

```
  rewrite ingress tag translate 1-to-1 dot1q 12 symmetric

!

evpn
  interface Bundle-Ether10
   ethernet-segment identifier type 0 00.01.00.ac.ce.55.00.0a.00

!

/* On PE3 */

configure
l2vpn
 flexible-xconnect-service vlan-unaware fxc1_16
  interface Bundle-Ether20.11
  interface Bundle-Ether20.12
  neighbor evpn evi 1 target 16

!

configure
interface Bundle-Ether20.11 l2transport
  encapsulation dot1q 1
  rewrite ingress tag translate 1-to-1 dot1q 11 symmetric

!

configure
interface Bundle-Ether20.12 l2transport
  encapsulation dot1q 2
  rewrite ingress tag translate 1-to-1 dot1q 12 symmetric

!

evpn
  interface Bundle-Ether20
   ethernet-segment identifier type 0 00.01.00.ac.ce.55.00.14.00

!

/* On PE4 */

configure
l2vpn
 flexible-xconnect-service vlan-unaware fxc1_16
  interface Bundle-Ether20.11
  interface Bundle-Ether20.12
  neighbor evpn evi 1 target 16

!

configure
interface Bundle-Ether20.11 l2transport
  encapsulation dot1q 1
  rewrite ingress tag translate 1-to-1 dot1q 11 symmetric

!

configure
interface Bundle-Ether20.12 l2transport
  encapsulation dot1q 2
  rewrite ingress tag translate 1-to-1 dot1q 12 symmetric
```

```
!

evpn
  interface Bundle-Ether20
   ethernet-segment identifier type 0 00.01.00.ac.ce.55.00.14.00

!
```

VLAN 対応

この動作モードでは、さまざまなイーサネットセグメントやインターフェイス全体にわたって正規化された AC を単一の EVPN VPWS サービス トンネルに多重化します。この単一のトンネルは、多くの VPWS サービス ID （正規化された VLAN ID（VID）ごとに 1 つ）によって表され、これらの正規化された VID は EVPN BGP を使用して通知されます。VLAN 対応の FXC は PW の数を削減しますが、BGP の状態は低減しません。VLAN 障害は、BGP を介して通知されます。VLAN 対応の FXC は FXC ごとではなく、AC ごとに 1 つの EAD ルートをアドバタイズします。VLAN 対応の FXC の場合、EVI は FXC 自体に一意である必要があります。FXC、EVPN、EVPN-VPWS、PBB-EVPN などの他のサービスと共有できません。PE 上で単一の AC がダウンした場合、その AC に関連付けられている EAD ルートのみを撤回します。メイン インターフェイスの障害時には ES-EAD ルートも撤回されます。PE3 または PE4 上の等コストマルチパス（ECMP）は、この AC から PE1 へのトラフィックの送信を中止し、PE2 にのみトラフィックを送信します。

同じ VLAN 対応 FXC では、すべて非ゼロ ESI かすべてゼロ ESI のどちらかを設定できます。同じ VLAN 対応 FXC に対して、ゼロ ESI と非ゼロ ESI の両方を設定することはできません。このことはシングルホーム モードにのみ適用されます。

VLAN 対応を使用したシングルホーム フレキシブル クロスコネクトの設定

この項では、VLAN 対応を使用してシングルホーム フレキシブル クロスコネクト サービスを設定する方法について説明します。

```
/* Configure PE1 */
Router# configure
Router(config)#  interface GigabitEthernet 0/2/0/7.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-2 dot1q 500 second-dot1q
 100 symetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)#  interface GigabitEthernet 0/2/0/7.2 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 2
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-2 dot1q 600 second-dot1q
 200 symetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-aware evi 4
Router(config-l2vpn-fxs)# interface GigabitEthernet 0/2/0/7.1
Router(config-l2vpn-fxs)# interface GigabitEthernet 0/2/0/7.2
Router(config-l2vpn-fxs)# commit

/* Configure PE2 */
Router# configure
Router(config)#  interface GigabitEthernet 0/0/0/7.1 l2transport
```

```
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-2 dot1q 500 second-dot1q
 100 symetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)#  interface GigabitEthernet 0/0/0/7.2 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 2
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-2 dot1q 600 second-dot1q
 200 symetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-aware evi 4
Router(config-l2vpn-fxs)# interface GigabitEthernet 0/0/0/7.1
Router(config-l2vpn-fxs)# interface GigabitEthernet 0/0/0/7.2
Router(config-l2vpn-fxs)# commit
```

実行コンフィギュレーション

```
/* On PE1 */
!
Configure
interface GigabitEthernet 0/2/0/7.1 l2transport
  encapsulation dot1q 1
  rewrite ingress tag translate 1-to-2 dot1q 500 second-dot1q 100 symetric
!

Configure
interface GigabitEthernet 0/2/0/7.2 l2transport
  encapsulation dot1q 2
  rewrite ingress tag translate 1-to-2 dot1q 600 second-dot1q 200 symetric
!

l2vpn
  flexible-xconnect-service vlan-aware evi 4
   interface GigabitEthernet 0/2/0/7.1
   interface GigabitEthernet 0/2/0/7.2


!

/* On PE2 */
!
Configure
interface GigabitEthernet 0/0/0/7.1 l2transport
  encapsulation dot1q 1
  rewrite ingress tag translate 1-to-2 dot1q 500 second-dot1q 100 symetric
!

Configure
interface GigabitEthernet 0/0/0/7.2 l2transport
  encapsulation dot1q 2
  rewrite ingress tag translate 1-to-2 dot1q 600 second-dot1q 200 symetric
!

l2vpn
  flexible-xconnect-service vlan-aware evi 4
   interface GigabitEthernet 0/0/0/7.1
   interface GigabitEthernet 0/0/0/7.2

!
```

VLAN 対応を使用したマルチホーム フレキシブル クロスコネクト サービスの設定

この項では、VLAN 対応を使用してマルチホーム フレキシブル クロスコネクト サービスを設定する方法について説明します。

```
/* Configure PE1 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-aware evi 6
Router(config-l2vpn-fxs)# interface Bundle-Ether2.1
Router(config-l2vpn-fxs)# interface Bundle-Ether3.1
Router(config-l2vpn-fxs)# commit
Router(config-l2vpn-fxs)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether2.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-1 dot1q 11 symmetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)# interface Bundle-Ether3.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 2
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-1 dot1q 12 symmetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether2
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 22.33.44.55.66.77.88.99.aa
Router(config-evpn-ac-es)# commit
Router(config-evpn-ac-es)# exit
Router(config-evpn-ac)# exit
Router(config-evpn)# interface Bundle-Ether3
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 33.44.55.66.77.88.99.aa.bb
Router(config-evpn-ac-es)# commit

/* Configure PE2 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-aware evi 6
Router(config-l2vpn-fxs)# interface Bundle-Ether2.1
Router(config-l2vpn-fxs)# interface Bundle-Ether3.1
Router(config-l2vpn-fxs)# commit
Router(config-l2vpn-fxs)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether2.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-1 dot1q 11 symmetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)# interface Bundle-Ether3.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 2
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-1 dot1q 12 symmetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether2
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 22.33.44.55.66.77.88.99.aa
Router(config-evpn-ac-es)# commit
Router(config-evpn-ac-es)# exit
Router(config-evpn-ac)# exit
```

```
Router(config-evpn)# interface Bundle-Ether3
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 33.44.55.66.77.88.99.aa.bb
Router(config-evpn-ac-es)# commit

/* Configure PE3 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-aware evi 6
Router(config-l2vpn-fxs)# interface Bundle-Ether4.1
Router(config-l2vpn-fxs)# interface Bundle-Ether5.1
Router(config-l2vpn-fxs)# commit
Router(config-l2vpn-fxs)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether4.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-1 dot1q 11 symmetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)# interface Bundle-Ether5.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 2
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-1 dot1q 12 symmetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether4
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 00.01.00.ac.ce.55.00.14.00
Router(config-evpn-ac-es)# commit
Router(config-evpn-ac-es)# exit
Router(config-evpn-ac)# exit
Router(config-evpn)# interface Bundle-Ether5
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type identifier type 0 00.01.00.ac.ce.55.00.15.00
Router(config-evpn-ac-es)# commit

/* Configure PE4 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-aware evi 6
Router(config-l2vpn-fxs)# interface Bundle-Ether4.1
Router(config-l2vpn-fxs)# interface Bundle-Ether5.1
Router(config-l2vpn-fxs)# commit
Router(config-l2vpn-fxs)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether4.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-1 dot1q 11 symmetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)# interface Bundle-Ether5.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 2
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-1 dot1q 12 symmetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether4
Router(config-evpn-ac)# ethernet-segment
Router config-evpn-ac-es)# identifier type 0 00.01.00.ac.ce.55.00.14.00
Router(config-evpn-ac-es)# commit
Router(config-evpn-ac-es)# exit
Router(config-evpn-ac)# exit
Router(config-evpn)# interface Bundle-Ether5
```

```
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type identifier type 0 00.01.00.ac.ce.55.00.15.00
Router(config-evpn-ac-es)# commit
```

実行コンフィギュレーション

```
/* On PE1 */
!
configure
l2vpn
 flexible-xconnect-service vlan-aware evi 6
  interface Bundle-Ether2.1
  interface Bundle-Ether3.1

!

configure
interface Bundle-Ether2.1 l2transport
  encapsulation dot1q 1
  rewrite ingress tag translate 1-to-1 dot1q 11 symmetric

!

configure
interface Bundle-Ether3.1 l2transport
  encapsulation dot1q 2
  rewrite ingress tag translate 1-to-1 dot1q 12 symmetric
!

evpn
  interface Bundle-Ether2
   ethernet-segment identifier type 0 22.33.44.55.66.77.88.99.aa
  interface Bundle-Ether3
   ethernet-segment identifier type 0 33.44.55.66.77.88.99.aa.bb

!

/* On PE2 */
!
configure
l2vpn
 flexible-xconnect-service vlan-aware evi 6
  interface Bundle-Ether2.1
  interface Bundle-Ether3.1

!

configure
interface Bundle-Ether2.1 l2transport
  encapsulation dot1q 1
  rewrite ingress tag translate 1-to-1 dot1q 11 symmetric

!

configure
interface Bundle-Ether3.1 l2transport
  encapsulation dot1q 2
  rewrite ingress tag translate 1-to-1 dot1q 12 symmetric
!

evpn
  interface Bundle-Ether2
   ethernet-segment identifier type 0 22.33.44.55.66.77.88.99.aa
  interface Bundle-Ether3
```

```
   ethernet-segment identifier type 0 33.44.55.66.77.88.99.aa.bb

!

/* On PE3 */
!
configure
l2vpn
 flexible-xconnect-service vlan-aware evi 6
  interface Bundle-Ether4.1
  interface Bundle-Ether5.1

!

configure
interface Bundle-Ether4.1 l2transport
  encapsulation dot1q 1
  rewrite ingress tag translate 1-to-1 dot1q 11 symmetric

!

configure
interface Bundle-Ether5.1 l2transport
  encapsulation dot1q 2
  rewrite ingress tag translate 1-to-1 dot1q 12 symmetric
!

evpn
  interface Bundle-Ether4
   ethernet-segment identifier type 0 00.01.00.ac.ce.55.00.14.00
  interface Bundle-Ether5
   ethernet-segment identifier type 0 00.01.00.ac.ce.55.00.15.00

!

/* On PE4 */
!
configure
l2vpn
 flexible-xconnect-service vlan-aware evi 6
  interface Bundle-Ether4.1
  interface Bundle-Ether5.1

!

configure
interface Bundle-Ether4.1 l2transport
  encapsulation dot1q 1
  rewrite ingress tag translate 1-to-1 dot1q 11 symmetric

!

configure
interface Bundle-Ether5.1 l2transport
  encapsulation dot1q 2
  rewrite ingress tag translate 1-to-1 dot1q 12 symmetric
!

evpn
  interface Bundle-Ether4
   ethernet-segment identifier type 0 00.01.00.ac.ce.55.00.14.00
  interface Bundle-Ether5
   ethernet-segment identifier type 0 00.01.00.ac.ce.55.00.15.00
```

!

ローカル スイッチング

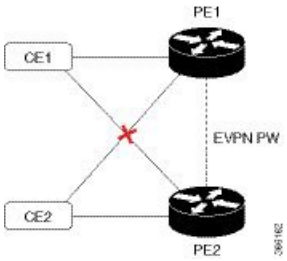
異なるイーサネット セグメントに属している 2 つの AC に同じ正規化 VLAN がある場合、2 つの AC 間のトラフィックは PE 内でローカルに切り替えられます。ローカル スイッチングは FXC VLAN 対応でのみサポートされています。

CE1 と CE2 に異なるイーサネット セグメントがあるトポロジを考えてみます。ただし、それらは両方とも、正規化された同じ VLAN です。したがって、トラフィックが CE1 から CE2 に送信されると、PE1 はローカル スイッチングを使用してトラフィックを CE2 にルーティングします。

障害があり、CE1 から PE1 へのリンクがダウンする場合、PE1 は EVPN 疑似回線を通じてトラフィックを PE2 に送信します。次に、PE2 がそのトラフィックを CE2 に送信します。

CE1 と CE2 は異なる非ゼロ ESI に存在する必要があります。

図 *11 :* ローカル スイッチング



ローカル スイッチングを使用したマルチホーム フレキシブル クロスコネクト サービスの設定

この項では、ローカル スイッチングを使用してマルチホーム フレキシブル クロスコネクト サービスを設定する方法について説明します。

```
/* Configure PE1 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-aware evi 6
Router(config-l2vpn-fxs)# interface Bundle-Ether2.1
Router(config-l2vpn-fxs)# interface Bundle-Ether3.1
Router(config-l2vpn-fxs)# commit
Router(config-l2vpn-fxs)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether2.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-2 dot1q 3 second-dot1q 3
 symmetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)# interface Bundle-Ether3.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-2 dot1q 3 second-dot1q 3
 symmetric
```

```
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether2
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 22.33.44.55.66.77.88.99.aa
Router(config-evpn-ac-es)# commit
Router(config-evpn-ac-es)# exit
Router(config-evpn-ac)# exit
Router(config-evpn)# interface Bundle-Ether3
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 33.44.55.66.77.88.99.aa.bb
Router(config-evpn-ac-es)# commit

/* Configure PE2 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-aware evi 6
Router(config-l2vpn-fxs)# interface Bundle-Ether2.1
Router(config-l2vpn-fxs)# interface Bundle-Ether3.1
Router(config-l2vpn-fxs)# commit
Router(config-l2vpn-fxs)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether2.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-2 dot1q 3 second-dot1q 3
 symmetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)# interface Bundle-Ether3.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-2 dot1q 3 second-dot1q 3
 symmetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether2
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 22.33.44.55.66.77.88.99.aa
Router(config-evpn-ac-es)# commit
Router(config-evpn-ac-es)# exit
Router(config-evpn-ac)# exit
Router(config-evpn)# interface Bundle-Ether3
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 33.44.55.66.77.88.99.aa.bb
Router(config-evpn-ac-es)# commit
```

実行コンフィギュレーション

```
/* On PE1 */

configure
l2vpn
 flexible-xconnect-service vlan-aware evi 6
  interface Bundle-Ether2.1
  interface Bundle-Ether3.1

!

configure
interface Bundle-Ether2.1 l2transport
  encapsulation dot1q 1
  rewrite ingress tag translate 1-to-2 dot1q 3 second-dot1q 3 symmetric
```

```
!

configure
interface Bundle-Ether3.1 l2transport
  encapsulation dot1q 1
  rewrite ingress tag translate 1-to-2 dot1q 3 second-dot1q 3 symmetric
!

evpn
  interface Bundle-Ether2
   ethernet-segment identifier type 0 22.33.44.55.66.77.88.99.aa
  interface Bundle-Ether3
   ethernet-segment identifier type 0 33.44.55.66.77.88.99.aa.bb

!

/* On PE2 */

configure
l2vpn
 flexible-xconnect-service vlan-aware evi 6
  interface Bundle-Ether2.1
  interface Bundle-Ether3.1

!

configure
interface Bundle-Ether2.1 l2transport
  encapsulation dot1q 1
  rewrite ingress tag translate 1-to-2 dot1q 3 second-dot1q 3 symmetric

!

configure
interface Bundle-Ether3.1 l2transport
  encapsulation dot1q 1
  rewrite ingress tag translate 1-to-2 dot1q 3 second-dot1q 3 symmetric
!

evpn
  interface Bundle-Ether2
   ethernet-segment identifier type 0 22.33.44.55.66.77.88.99.aa
  interface Bundle-Ether3
   ethernet-segment identifier type 0 33.44.55.66.77.88.99.aa.bb


!
```

優先トンネル パスの設定

優先トンネル パスの機能により、特定のトラフィック エンジニアリング トンネルに疑似回線をマッピングできます。接続回線は、リモート PE ルータの IP アドレス（IGP または LDP を使用して到達可能）ではなく、特定の MPLS トラフィック エンジニアリング トンネル インターフェイスに相互接続されます。

優先トンネル パスを使用する場合、レイヤ 2 トラフィックを転送するトラフィック エンジニアリング トンネルが 2 つの PE ルータ間で動作することが想定されます（つまり、始端はインポジション PE ルータで、終端はディスポジション PE ルータです）。

設定

```
/* Enter global configuration mode */
Router# configure
Router(config)# l2vpn

/* Configure pseudowire class name */
Router(config-l2vpn)# pw-class path1

/* Configure MPLS encapsulation for the pseudowire */
Router(config-l2vpn-pwc)# encapsulation mpls


/* Configure preferred path tunnel settings.
If fallback disable configuration is used, and when
 the TE/ tunnel is configured,
 if the preferred path goes down,
 the corresponding pseudowire can also go down. */

Router(config-l2vpn-pwc-encap-mpls)# preferred-path
                  interface tunnel-te 11 fallback disable

/* Commit your configuration */
Router(config-l2vpn-pwc)# exit
Router(config-l2vpn)# commit
```

実行コンフィギュレーション

```
Router# show running-configuration
!
l2vpn
 pw-class path1
  encapsulation mpls
   preferred-path interface tunnel-te 11 fallback disable
  !
 !
!
```

マルチセグメント疑似回線

マルチセグメント擬似回線機能により、AS 間境界を越えて、または 2 つの別個の MPLS ネットワークにまたがって、L2VPN 擬似回線を拡張することができます。マルチセグメント擬似回線は、2 つ以上の連続した擬似回線セグメントを接続して、エンドツーエンドのマルチホップ擬似回線を単一のポイントツーポイント疑似回線として形成します。これらのセグメントは単一の疑似回線として機能し、以下を実行できます。

- 管理ドメインまたはプロビジョニング ドメインを隔離することで、エンドツーエンドサービスを管理する。
- 相互自律システム（Inter-AS）の境界を越えて、プロバイダー エッジ（PE）ノードの IP アドレスをプライベートにする。自律システム境界ルータ（ASBR）の IP アドレスを使用し、それらのルータを疑似回線の集約ルータとして扱う。ASBR は、2 つのドメインの擬似回線を結合します。

マルチセグメント疑似回線は、Inter-AS境界または2つのマルチプロトコル ラベル スイッチング（MPLS）ネットワークにまたがることができます。

疑似回線は、2 台の PE ノード間のトンネルです。2 種類の PE ノードがあります。

- スイッチング PE（S-PE）ノード
  - マルチセグメント疑似回線の先行する疑似回線セグメントと後続の疑似回線セグメントの PSN トンネルを終端させます。
  - マルチセグメント疑似回線の先行する疑似回線セグメントと後続の疑似回線セグメントのコントロール プレーンとデータ プレーンを切り替えます。
- 終端 PE（T-PE）ノード
  - マルチセグメント疑似回線の最初と最後の両方のセグメントに配置されます。
  - このノードで、カスタマー方向の接続回線（AC）が疑似回線フォワーダにバインドされます。

（注） すべてのマルチセグメント擬似回線は、T-PE で終端する必要があります。

マルチセグメント擬似回線は、次の場合に 2 つの一般的なケースで使用されます。

- 送信元と宛先の PE ノード間で PW 制御チャネルを確立することができない場合。

  PW コントロールチャネルを確立するには、リモート PE ノードがアクセス可能である必要があります。場合によっては、トポロジ、動作、またはセキュリティ上の制約により、ローカル PE ノードがリモートノードにアクセスできない場合があります。

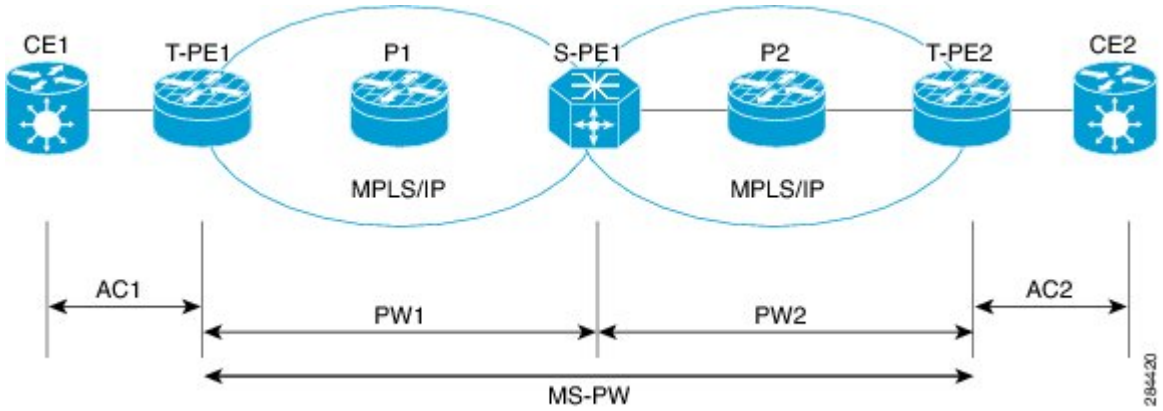
  マルチセグメントの擬似回線は、2つの独立した疑似回線セグメントを動的に構築し、擬似回線スイッチングを実行して、送信元と宛先の PE ノード間の PW 制御チャネルを確立します。

- エッジ間の擬似回線エミュレーション（PWE3）のシグナリングとカプセル化プロトコルが異なる場合。

  PE ノードの接続先のネットワークでは、異なる PW シグナリングおよびカプセル化プロトコルが使用されています。場合によっては、1 つのセグメント PW を使用できません。

  マルチセグメント擬似回線はPWスイッチングポイントで適切なインターワーキングが実行されており、ネットワーク内の PE ノード間で PW 接続を有効にします。

図 *12 :* マルチセグメント疑似回線



このトポロジでは、PW1 と PW2 間の MS-PW スティッチングが示されています。1 つのポイントツーポイント PW として動作および機能する 2 つ以上の連続する PW セグメントのセットを設定できます。静的または動的マルチセグメント PW（MS PW）を設定できます。連続する PW セグメントの最大数は 254 です。MS-PW の各端は、T-PE で終端します。スイッチング PE（S-PE）は、MS-PW 内の先行および後続の PW セグメントの PSN トンネルを終端します。S-PE スイッチは、MS-PW の先行および後続の PW セグメントのコントロールプレーンとデータプレーンを切り替えることができます。すべての SS-PW が起動すると、MS-PW が起動します。

制約事項

マルチセグメント疑似回線機能を設定する際には、次の制限事項を考慮する必要があります。

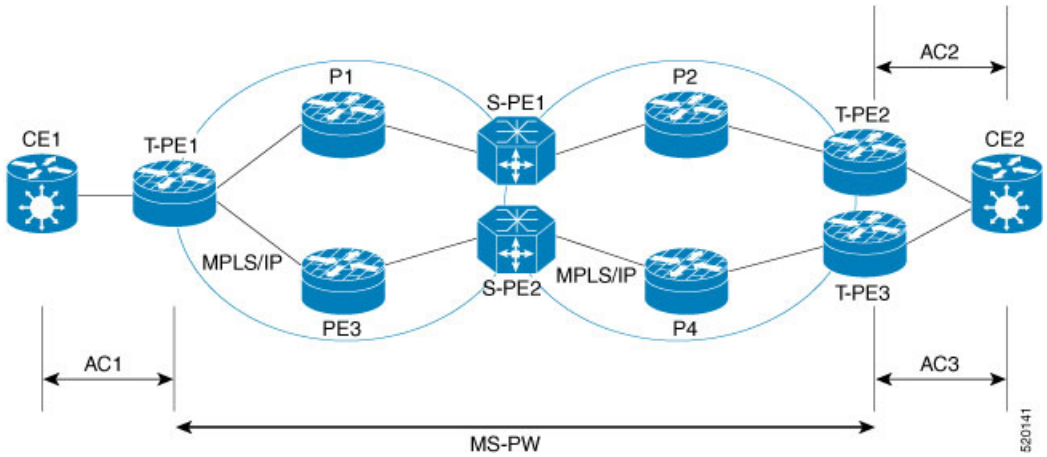
- MS-PW の 両方のセグメントを異なるピアに接続します。
- LDP のみをサポートし、L2TPv3 をサポートしていません。MS-PW xconnect の各 PW セグメントは、静的または動的です。
- MS-PW の各 PW セグメントのネイバー pw-id ペアは、ノード上で一意です。
- エンドツーエンドの pw-type は同じである必要があります。したがって、MS-PW の両方のセグメントでは、トランスポートモードを同じにする必要があります。
- S-PE の MS-PW xconnect では、PW の冗長化を設定できません。PW の冗長化は、T-PE で設定できます。
- MS-PW xconnect の両方のセグメントで、同じ優先パスを持つことはできません。
- LDP、MPLS-TE、SR、SR-TE を介した MS-PW をトランスポートプロトコルとしてサポートしています。
- BGP-LU および LDPoTE を介した MS-PW をサポートしていません。
- S-PE で MSPW を有効にする場合は、MSPW ping とトレースレートが機能するように、*ip-ttl-propagation disable* コマンドを設定します。または、*segment-count 255 option* を使用し

て MSPW ping が T-PE1 から実行されるようにします。MSPW は、部分的な ping をサポートしていません。

マルチセグメント疑似回線の冗長化

擬似回線冗長化機能を使用すると、T-PE 間でバックアップ MS-PW を作成できます。また、擬似回線冗長化機能を使用して、ネットワーク内の障害を検出するようにネットワークを設定できます。さらに、サービスを継続して提供できる別のエンドポイントにレイヤ 2 サービスを再ルーティングします。

図 *13*：マルチセグメント疑似回線の冗長化



2 つの MS-PW を作成して、CE2 T-PE2 と T-PE3 にマルチホームするトポロジについて考えてみます。P1、S-PE1、および P2 を介して接続された T-PE1 と T-PE2 の間にプライマリ MS-PW を作成します。P3、S-PE2、および P4 を介して接続された T-PE1 と T-PE3 の間にスタンバイ MS-PW を作成します。

プライマリ PW のセグメントに障害が発生すると、S-PE1 はラベル撤回メッセージを受信するか、LDP トランスポートがダウンします。S-PE1 は、他の PW セグメントを使用してラベル撤回メッセージを送信します。これにより、T-PE でバックアップへのスイッチオーバーがトリガーされます。次に例を示します。

- T-PE1 が LDP トランスポートの障害を検出すると、ラベル撤回メッセージを S-PE1 に送信し、バックアップ MS-PW に切り替えます。
- S-PE1 はラベル撤回メッセージを受信すると、T-PE2 にラベル撤回メッセージを送信します。
- T-PE2 は、ラベル撤回メッセージを受信した後、AC2 の「Tx 無効化」を実行します。
- CE2 は、AC3 でトラフィックの送受信を開始します。

マルチセグメント疑似回線の設定

マルチセグメント擬似回線を設定するには、次のタスクを実行します。

```
/* Configure on T-PE1 */
Router#configure
Router(config)#l2vpn
Router(config-l2vpn)#pw-class dynamic_mpls
Router(config-l2vpn-pwc)#encapsulation mpls
Router(config-l2vpn-pwc-encap-mpls)#protocol ldp
Router(config-l2vpn-pwc-encap-mpls)#control-word disable
Router(config-l2vpn-pwc-encap-mpls)#exit
Router(config-l2vpn-pwc)#exit
Router(config-l2vpn)#xconnect group XCON1
Router(config-l2vpn-xc)#p2p xc1
Router(config-l2vpn-xc-p2p)#description T-PE1 MS-PW to 172.16.0.1 through 192.168.0.1
Router(config-l2vpn-xc-p2p)#interface gig0/1/0/0.1
Router(config-l2vpn-xc-p2p)#neighbor 192.168.0.1 pw-id 100
Router(config-l2vpn-xc-p2p-pw)#pw-class dynamic_mpls
Router(config-l2vpn-xc-p2p-pw)#commit

/* Configure on S-PE1 */
Router#configure
Router(config)#l2vpn
Router(config-l2vpn)#xconnect group MS-PW1
Router(config-l2vpn-xc)#p2p ms-pw1
Router(config-l2vpn-xc-p2p)#description S-PE1 MS-PW between 10.0.0.1 and 172.16.0.1
Router(config-l2vpn-xc-p2p)#neighbor 10.0.0.1 pw-id 100
Router(config-l2vpn-xc-p2p-pw)#pw-class dynamic_mpls
Router(config-l2vpn-xc-p2p-pw)#exit
Router(config-l2vpn-xc-p2p)#neighbor 172.16.0.1 pw-id 300
Router(config-l2vpn-xc-p2p-pw)#pw-class dynamic_mpls
Router(config-l2vpn-xc-p2p-pw)#exit
Router#configure
Router(config)#l2vpn
Router(config-l2vpn)#pw-class dynamic_mpls
Router(config-l2vpn-pwc)#encapsulation mpls
Router(config-l2vpn-pwc-encap-mpls)#protocol ldp
Router(config-l2vpn-pwc-encap-mpls)#control-word disable
Router(config-l2vpn-pwc-encap-mpls)#commit

/* Configure on T-PE2 */
Router#configure
Router(config)#l2vpn
Router(config-l2vpn)#pw-class dynamic_mpls
Router(config-l2vpn-pwc)#encapsulation mpls
Router(config-l2vpn-pwc-encap-mpls)#protocol ldp
Router(config-l2vpn-pwc-encap-mpls)#control-word disable
Router(config-l2vpn-pwc-encap-mpls)#exit
Router(config-l2vpn-pwc)#exit
Router(config-l2vpn)#xconnect group XCON1
Router(config-l2vpn-xc)#p2p xc1
Router(config-l2vpn-xc-p2p)#description T-PE2 MS-PW to 10.0.0.1 through 192.168.0.1
Router(config-l2vpn-xc-p2p)#interface gig0/2/0/0.4
Router(config-l2vpn-xc-p2p)#neighbor 192.168.0.1 pw-id 300
Router(config-l2vpn-xc-p2p-pw)#pw-class dynamic_mpls
Router(config-l2vpn-xc-p2p-pw)#commit
```

実行コンフィギュレーション

この項では、マルチセグメント疑似回線の実行コンフィギュレーションを示します。

```
/* T-PE1 Configuration */
Configure
 l2vpn
  pw-class dynamic_mpls
   encapsulation mpls
   protocol ldp
  control-word disable
 !
  xconnect group XCON1
   p2p xc1
    description T-PE1 MS-PW to 172.16.0.1 through 192.168.0.1
    interface gig0/1/0/0.1
    neighbor 192.168.0.1 pw-id 100
     pw-class dynamic_mpls
    !
  !

/* S-PE1 Configuration */
 l2vpn
  xconnect group MS-PW1
   p2p ms-pw1
    description S-PE1 MS-PW between 10.0.0.1 and 172.16.0.1
    neighbor 10.0.0.1 pw-id 100
     pw-class dynamic_mpls
     !
    neighbor 172.16.0.1 pw-id 300
     pw-class dynamic_mpls
    !
   !
l2vpn
 pw-class dynamic_mpls
  encapsulation mpls
  protocol ldp
  control-word disable
  !
 !


/* T-PE2 Configuration */
Configure
 l2vpn
  pw-class dynamic_mpls
   encapsulation mpls
   protocol ldp
  control-word disable
 !
  xconnect group XCON1
   p2p xc1
    description T-PE1 MS-PW to 10.0.0.1 through 192.168.0.1
    interface gig0/2/0/0.4
    neighbor 192.168.0.1 pw-id 300
     pw-class dynamic_mpls
    !
  !
```

確認

マルチセグメント擬似回線機能が正しく設定されていることを確認します。

```
Router:S-PE1#show l2vpn xocnnect
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
LU = Local Up, RU = Remote Up, CO = Connected

XConnect Group  Name     ST   Segment 1     ST    Segment 2     ST
                               Description         Description
--------------  -----    ---- ------------ ---  ------------  ---
MS-PW1          ms-pw1   UP   10.0.0.1      UP   172.16.0.1    UP
-----------------------------------------------------------------------


Router:S-PE1#show l2vpn xconnect detail
Group MS-PW1, XC ms-pw1, state is up; Interworking none
  PW: neighbor 70.70.70.70, PW ID 100, state is up ( established )
    PW class not set
    Encapsulation MPLS, protocol LDP
    PW type Ethernet VLAN, control word enabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set
        MPLS         Local                          Remote
      ------------ ------------------------------ ------------------------------
      Label        16004                          16006
      Group ID     0x2000400                      0x2000700
      Interface    GigabitEthernet0/1/0/2.2       GigabitEthernet0/1/0/0.3
      MTU          1500                           1500
      Control word enabled                        enabled
      PW type      Ethernet VLAN                  Ethernet VLAN
      VCCV CV type 0x2                            0x2
                   (LSP ping verification)        (LSP ping verification)
      VCCV CC type 0x5                            0x7
                   (control word)                 (control word)
                                                  (router alert label)
                   (TTL expiry)                   (TTL expiry)
      ------------ ------------------------------ ------------------------------
    Incoming PW Switching TLV:
      IP Address: 70.70.70.70, PW ID: 100
      Description: T-PE1 MS-PW to 172.16.0.1via 192.168.0.1
    Outgoing PW Switching TLV:
      IP Address: 90.90.90.70, PW ID: 300
      Description: T-PE2 MS-PW to 10.0.0.1via 192.168.0.1
      IP Address: 192.168.0.1, PW ID: 100
      Description: S-PE1 MS-PW between 10.0.0.1and 90.90.90.90
    Create time: 04/04/2008 23:18:24 (00:01:24 ago)
    Last time status changed: 04/04/2008 23:19:30 (00:00:18 ago)
    Statistics:
      packet totals: receive 0
      byte totals: receive 0
  PW: neighbor 90.90.90.90, PW ID 300, state is up ( established )
    PW class not set
    Encapsulation MPLS, protocol LDP
    PW type Ethernet VLAN, control word enabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set
        MPLS         Local                          Remote
      ------------ ------------------------------ ------------------------------
      Label        16004                          16006
      Group ID     0x2000800                      0x2000200
      Interface    GigabitEthernet0/1/0/0.3       GigabitEthernet0/1/0/2.2
      MTU          1500                           1500
      Control word enabled                        enabled
      PW type      Ethernet VLAN                  Ethernet VLAN
      VCCV CV type 0x2                            0x2
                   (LSP ping verification)        (LSP ping verification)
```

```
  VCCV CC type 0x5                          0x7
               (control word)               (control word)
                                            (router alert label)
               (TTL expiry)                 (TTL expiry)
  ------------ ---------------------------- ----------------------------
Incoming PW Switching TLV:
  IP Address: 90.90.90.90, PW ID: 300
  Description: T-PE2 MS-PW to 10.0.0.1via 192.168.0.1
Outgoing PW Switching TLV:
  IP Address: 70.70.70.70, PW ID: 100
  Description: T-PE1 MS-PW to 172.16.0.1via 192.168.0.1
  IP Address: 192.168.0.1, PW ID: 300
  Description: S-PE1 MS-PW between 10.0.0.1and 90.90.90.90
Create time: 04/04/2008 23:18:24 (00:01:24 ago)
Last time status changed: 04/04/2008 23:19:30 (00:00:18 ago)
Statistics:
  packet totals: receive 0
  byte totals: receive 0
```

関連項目

- マルチセグメント疑似回線 （85 ページ）
- マルチセグメント疑似回線の冗長化 （88 ページ）

関連コマンド

- show l2vpn xconnect
- show l2vpn xconnect detail
- show l2vpn xconnect summary

スプリット ホライズン グループ

Cisco IOS XR ブリッジ ドメインは、スプリット ホライズン グループと呼ばれる 3 つのグループの 1 つに接続回線（AC）を集約します。ブリッジ ドメインに適用した場合、スプリット ホライズンは、スプリット ホライズン グループのメンバー間のフラッディングと転送動作を示します。次の表では、スプリット ホライズン グループの 1 つのメンバーで受信したフレームがどのように処理されるかを示し、トラフィックが同じスプリット ホライズン グループの他のメンバーに転送される場合について説明します。

ブリッジ ドメイン トラフィックは、ユニキャストまたはマルチキャストのいずれかです。

フラッディング トラフィックは、次の不明のユニキャスト宛先 MAC アドレス フレームで構成されます。

- フレームはイーサネット マルチキャスト アドレス（スパニング ツリー BPDU）に送信されます。
- イーサネット ブロードキャスト フレーム （MAC アドレス FF-FF-FF-FF-FF-FF）。

既知のユニキャスト トラフィックは、MAC 学習を使用するポートから学習されたブリッジ ポートに送信されるフレームで構成されます。

トラフィック フラッディングは、ブロードキャスト、マルチキャスト、不明なユニキャスト宛先アドレスに対して実行されます。

表 *3 : Cisco IOS-XR* でサポートされているスプリット ホライズン グループ

スプリット ホライズン グループ	このグループに属しているメンバー	グループ内のマルチキャスト	グループ内のユニキャスト
0	デフォルト：グループ 1 または 2 でカバーされないメンバー。	対応	対応
1	VFI で設定されるすべての PW。	非対応	非対応
2	split-horizon キーワードで設定された任意の AC。	非対応	非対応

スプリット ホライズン グループに関する重要事項：

- ブリッジ ドメインのメンバーであるすべてのブリッジ ポートまたは PW が、3 つのグループのうちの 1 つに属している必要があります。
- デフォルトでは、すべてのブリッジ ポートまたは PW がグループ 0 のメンバーです。
- ブリッジ ドメイン設定の VFI コンフィギュレーション サブモードは、このドメインのメンバーがグループ 1 に含まれていることを示しています。
- **split-horizon group** コマンドは、グループ 2 のメンバーとしてブリッジ ポートまたは PW を指定する場合に使用します。
- 既知のユニキャストは、ブロードキャスト、未知のユニキャスト、およびマルチキャスト（BUM）トラフィックとともに、グループのメンバー内でもフィルタリングされます。

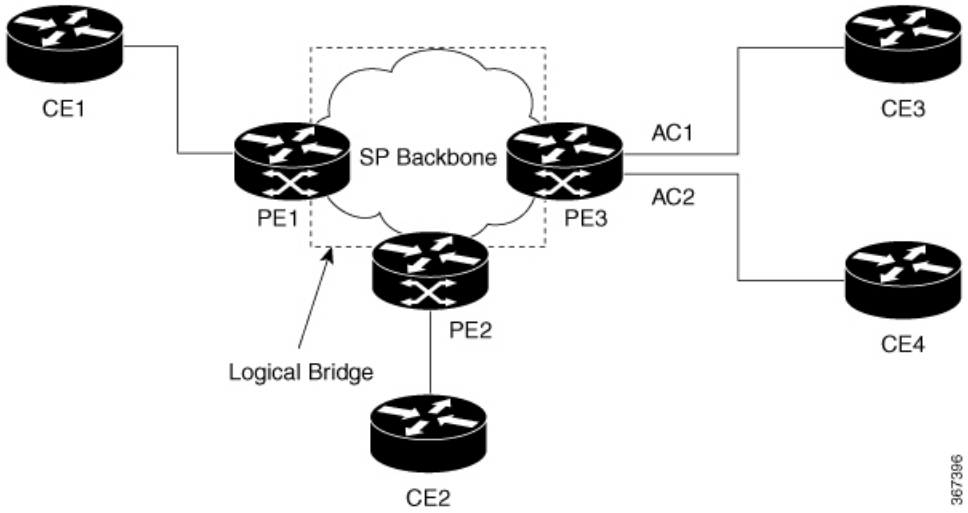
スプリット ホライズン グループ 2

スプリット ホライズン グループ 2 機能を使用すると、ブリッジ ドメイン内において、ある AC から別の AC への BUM および既知のユニキャスト トラフィックのフラッディングを防止できます。この機能により、効率的な帯域幅の割り当てとリソースの最適化が可能になります。

AC1 と AC2 が同じ VPLS ブリッジ ドメインの一部となっている次のトポロジを考えてみます。スプリット ホライズン グループ 2 を AC1 に設定すると、PE3 上の AC2、BUM、および AC1 からの既知のユニキャスト トラフィックは AC2 にフラッディングされません。逆も同様です。

しかし、PE3 上の疑似回線から、グループ 2 の一部である AC1 および AC2 への、着信 BUM トラフィックはフラッディングされます。既知のユニキャスト トラフィックは、対応する AC に送信されます。

図 *14 :* スプリット ホライズン グループ *2*



AC1 がグループ 0 の一部であり、AC2 がグループ 2 の一部である場合、BUM と既知のユニキャスト トラフィックは AC1 と AC2 の間でフラッディングされます。同様に、AC2 がグループ 0 の一部であり、AC1 がグループ 2 の一部である場合、BUM と既知のユニキャスト トラフィックは AC1 と AC2 の間でフラッディングされます。

スプリット ホライズン グループ 2 の設定

スプリット ホライズン グループ 2 機能を設定するには、次の作業を実行します。

設定例

次の例は、レイヤ2トランスポート用のインターフェイスを設定し、それらをブリッジ ドメインに追加して、スプリット ホライズン グループ 2 に割り当てる方法を示しています。

```
/* Configure on PE3 */
Router#configure
Router(config)l2vpn
Router(config-l2vpn)#router-id 3.3.3
Router(config-l2vpn)#pw-class class1
Router(config-l2vpn-pwc)#encapsulation mpls
Router(config-l2vpn-pwc-encapmpls)#protocol ldp
Router(config-l2vpn-pwc-encapmpls)#ipv4 source 3.3.3.3
Router(config-l2vpn-pwc-encapmpls)#exit
Router(config-l2vpn-pwc)#exit
Router(config-l2vpn)#bridge goup bg1
Router(config-l2vpn-bg)#bridge-domain bd
Router(config-l2vpn-bg-bd)#exit
Router(config-l2vpn-bg)#bridge-domain bd1
Router(config-l2vpn-bg-bd)#interface TenGigE
Router(config-l2vpn-bg-bd-ac)#split-horizon group
Router(config-l2vpn-bg-bd-ac)#exit
Router(config-l2vpn-bg-bd)#interface TenGigE

Router(config-l2vpn-bg-bd-ac)#split-horizon group
Router(config-l2vpn-bg-bd-ac)#exit
```

```
Router(config-l2vpn-bg-bd)#vfi vfi1
Router(config-l2vpn-bg-bd-vfi)#neighbor 1.1.1.1 pw-id 1
Router(config-l2vpn-bg-bd-vfi-pw)#pw-class class1
Router(config-l2vpn-bg-bd-vfi-pw-pwc)#commit
```

実行コンフィギュレーション

```
configure
 l2vpn
  router-id 3.3.3.3
  pw-class classs1
   encapsulation mpls
    protocol ldp
    ipv4 source 3.3.3.3
    !
   !
   bridge group bg1
    bridge-domain bd
    !
    bridge-domain bd1
     interface TenGigE
      split-horizon group
     !
     interface TenGigE
      split-horizon group
     !
     vfi vfi1
      neighbor 1.1.1.1 pw-id 1
       pw-class class1
      !
     !
    !
```

確認

トラフィックがそれぞれのグループ 2 AC から出力されているかどうかを確認します。

```
Router#show l2vpn bridge-domain bd-name bd1
Thu Jun 14 08:04:47.431 IST

  Legend: pp = Partially Programmed.
Bridge group: bg1, bridge-domain: bd1, id: 1, state: up, ShgId: 0, MSTi: 0
  Aging: 300s, MAC limit: 64000, Action: none, Notification: syslong
  Filter MAC addresses: 0
  ACs: 2 (2 up), VFIs: 1, PWs: 1 (up), PBBs: 0 (0 up), VNIs: 0 (0 up)
  List of ACs:
    Te
, stage: up, Static MAC addresses: 0
    Te, stage: up, Static MAC addresses: 0
  List of Access PWs:
  List of VFIs:
    VFI vfi1 (up)
     Neighbor 1.1.1.1 pw-id 1, stage: up, Static MAC Addresses: 0
```

G.8032 イーサネット リング保護

G.8032 イーサネット リング保護機能は、リング トポロジ内のイーサネット トラフィックの保護を提供します。この機能により、事前設定されたリンクも障害リンクもブロックされ、イーサネット レイヤにおけるリング内のループが防止されます。この機能は、物理インターフェイスとバンドルインターフェイスで設定できます。

概要

各イーサネット リング ノードは、2 個の独立したリンクを使用してイーサネット リングに参加する隣接イーサネット リング ノードに接続されます。リング リンクは、ネットワークに影響を及ぼすループの編成を許可しません。イーサネット リングは、イーサネット リングを保護するために特定のリンクを使用します。この特定のリンクは、リング予備リンク（RPL）と呼ばれます。リング リンクは、リング リンク（別名リング ポート）の 2 個の隣接するイーサネット リング ノードとポートで区切られます。

（注） イーサネット リングでのイーサネット リング ノードの最小数は 2 です。

リング保護スイッチングの基礎は次のとおりです。

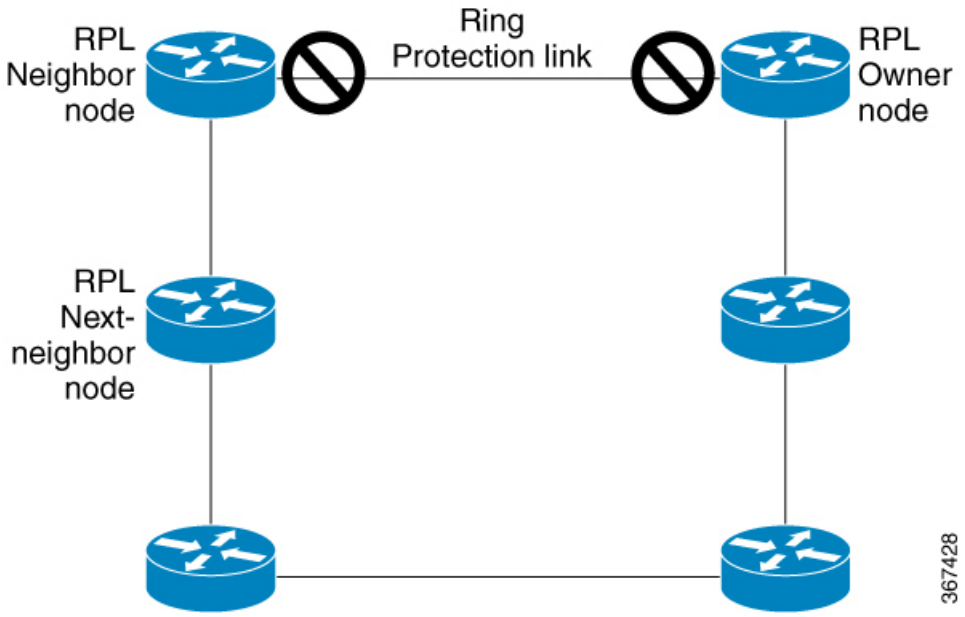
- ループ回避の原則。
- 学習、転送、およびフィルタリング データベース（FDB）メカニズムの使用。

イーサネット リングでのループ回避は、RPL である 1 つのリング リンクを除くすべてで常にトラフィック フローを確保することで行います。複数のノードが、リングの形成に使用されます。

- RPL オーナー：ループがイーサネット トラフィックで形成されないように、RPL を介してトラフィックをブロックします。リングには RPL オーナーは 1 つだけ存在します。
- RPL ネイバー ノード：RPL ネイバー ノードは、RPL に隣接するイーサネット リング ノードです。通常の状態で RPL の終了をブロックします。このノード タイプはオプションであり、保護されている場合 RPL の使用を防止します。
- RPL の次のネイバー ノード：RPL の次のネイバー ノードは、RPL オーナー ノードまたは RPL ネイバー ノードに隣接するイーサネット リング ノードです。これは、主にリングでの FDB フラッシュ最適化に使用されます。このノードはオプションです。

次の図は G.8032 イーサネット リングの例です。

図 *15 : G.8032* イーサネット リング



リングのノードは、RAPS と呼ばれる制御メッセージを使用して、RPL リンクのオンとオフを切り替えるアクティビティを調整します。リンクの障害によって、障害が発生したリンクに面するポートをノードがブロックした後で、障害が発生したリンクに隣接するノードから両方の方向に RAPS 信号障害（RAPS SF）メッセージがトリガーされます。このメッセージの取得時に、RPL オーナーは、RPL ポートのブロックを解除します。

（注） リングの単一のリンク障害によって、ループフリー トポロジが確保されます。

リング リンクおよびノードの障害を検出するために、回線ステータスおよび接続障害管理プロトコルが使用されます。回復フェーズ中に、障害が発生したリンクが復元されると、復元されたリンクに隣接するノードは、RAPS no request（RAPS NR）メッセージを送信します。このメッセージの取得時に、RPL オーナーは RPL ポートをブロックし、RAPS no request, root blocked（RAPS NR, RB）メッセージを送信します。これにより、リング内の RPL オーナー以外のその他すべてのノードが、すべてのブロックされたポートのブロックを解除します。ERP プロトコルは、リング トポロジの単方向障害と複数のリンク障害シナリオの両方で機能するために十分に強力です。

G.8032 リングは、次の基本的なオペレータ管理コマンドをサポートします。

- Force switch（FS）：オペレータは、特定のリング ポートを強制的にブロックできます。
  - 既存の SF 状態がある場合でも有効です。
  - サポートされるリング用の複数の FS コマンド。
  - 即時のメンテナンス操作を可能にするために使用できます。

- Manual switch（MS）：オペレータは、特定のリング ポートを手動でブロックできます。
  - 既存の FS または SF 状態では無効です。
  - 新しい FS または SF 状態によって上書きされます。
  - 過去のすべての MS コマンドをクリアします。

- Clear：リング ポートで既存の FS または MS コマンドを取り消します。
  - 非リバーティブ モードをクリアするために（RPL オーナーで）使用されます。

（注） MAC フラッシュ イベント中に生じる ERPS リング リンク障害/Force switch/Manual switch イベントは、結果として予測不可能なコンバージェンスになります。

G.8032 リングは2つのインスタンスをサポートできます。インスタンスは、物理的なリングに実行される論理リングです。そのようなインスタンスは、リング上のロード バランシング VLAN などのさまざまな理由で使用されます。たとえば、奇数の VLAN はリングの 1 方向に送信され、偶数の VLAN は他の方向に送信されることがあります。特定の VLAN は 1 つのインスタンスだけで設定できます。これらは複数のインスタンスと重複できません。重複すると、データ トラフィックまたはRAPSパケットは論理リングを通過する可能性があるため、望ましくありません。

タイマー

G.8032 は、競合状態および不要なスイッチング操作を回避するために異なる ERP タイマーを使用することを指定します。

- 遅延タイマー：RPLをブロックする前にネットワークが安定していることを確認するために RPL オーナーによって使用されます。
  - SF 状態の後で、SF が断続的に中断していないことを確認するために、Wait-to-Restore（WTR）タイマーが使用されます。WTR タイマーはオペレータが設定できます。デフォルトの時間間隔は 5 分です。時間間隔の範囲は 1 ～ 12 分です。
  - FS/MS コマンドの後で、バックグラウンド状態でないことを確認するために、Wait-to-Block タイマーが使用されます。

（注） Wait-to-Block タイマーは、Wait-to-Restore タイマーよりも短くなることがあります。

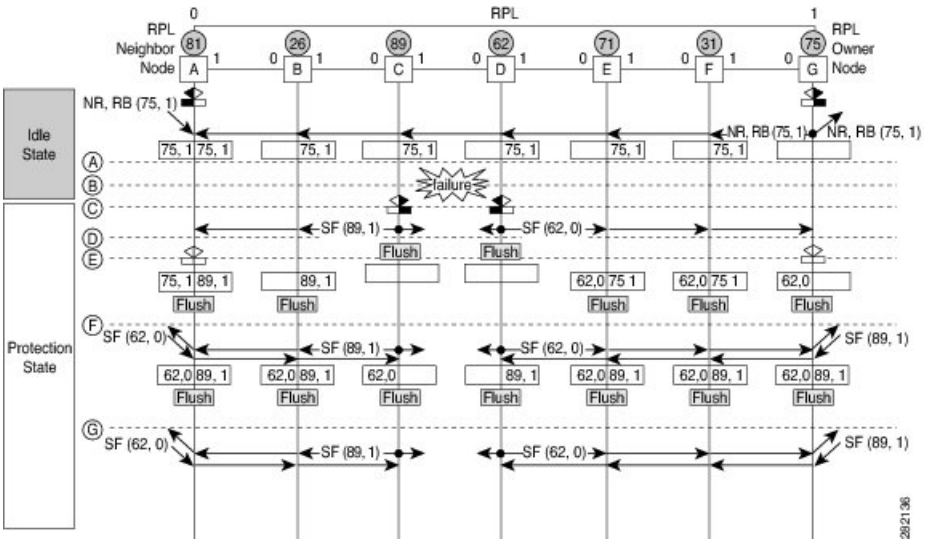
- ガードタイマー：状態の変更時にすべてのノードで使用されます。これは、潜在的な古いメッセージが不要な状態変更を引き起こさないようにします。ガードタイマーは設定可能であり、デフォルトの時間間隔は 500 ミリ秒です。時間間隔の範囲 10 ～ 2000 ミリ秒です。

- hold-off タイマー：断続的なリンク障害をフィルタリングするために、基盤となるイーサネット レイヤによって使用されます。hold-off タイマーは設定可能であり、デフォルトの時間間隔は 0 秒です。時間間隔の範囲は 0 ～ 10 秒です。
  - 障害は、このタイマーの有効期限が切れた場合だけリング保護メカニズムに報告されます。

単一のリンク障害

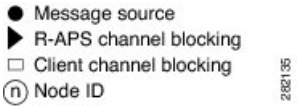
次の図は、単一のリンク障害が発生した場合の保護スイッチングを表しています。

図 *16 : G.8032* の単一のリンク障害



前述の図は、7 つのイーサネット リング ノードで構成されたイーサネット リングを表しています。RPL は、イーサネット リング ノード A と G の間のリング リンクです。このようなシナリオでは、RPL の両端がブロックされます。イーサネット リング ノード G は RPL オーナー ノードで、イーサネット リング ノード A は RPL ネイバー ノードです。

次の記号が使用されます。



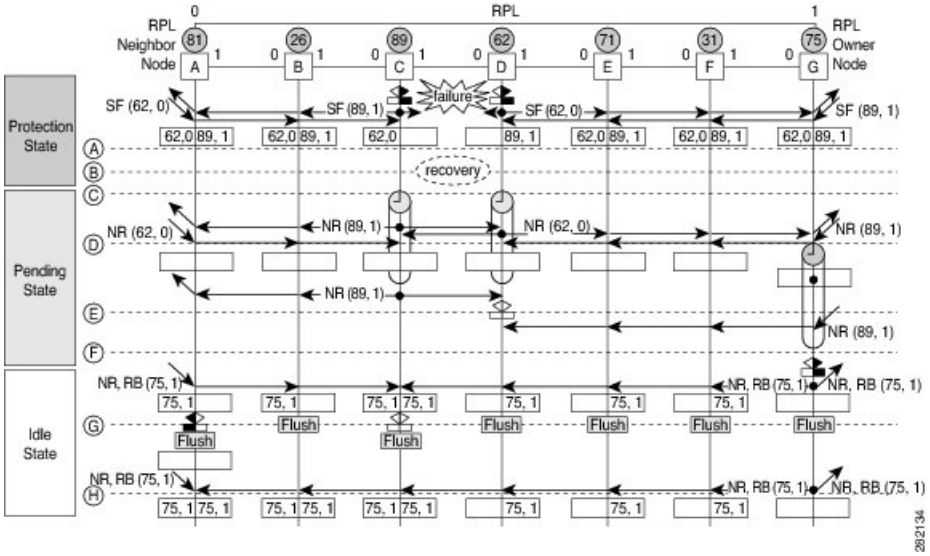
次の流れでは、単一のリンク障害でのステップについて説明します。

1. リンクは正常な状態で動作しています。
2. 障害が発生します。
3. イーサネット リング ノード C と D は、ローカルの信号障害を検出し、ホールドオフ時間間隔後に障害が発生したリング ポートをブロックし、FDB フラッシュを実行します。

4. イーサネット リング ノード C と D は、SF 状態が続いている間、両方のリング ポートの（ノード ID、BPR）ペアとともに RAPS（SF）メッセージの定期的な送信を開始します。
5. RAPS（SF）メッセージを受信するすべてのイーサネット リング ノードが FDB フラッシュを実行します。RPL オーナー ノード G と RPL ネイバー ノード A が RAPS（SF）メッセージを受信すると、イーサネット リング ノードは自身の RPL の終端をブロック解除し、FDB フラッシュを実行します。
6. 2 番目の RAPS（SF）メッセージを受信するすべてのイーサネット リング ノードは、FDB フラッシュを再度実行します。これは、ノード ID と BPR ベース メカニズムが原因です。
7. 安定した SF 状態：イーサネット リングの RAPS メッセージ（SF）。これ以上の RAPS（SF）メッセージは、さらなるアクションをトリガーしません。

次の図は、単一のリンク障害が発生した場合の復帰を表しています。

図 *17*：単一のリンク障害回復（リバーティブ操作）



次の流れでは、単一のリンク障害での復帰のステップについて説明します。

1. リンクが安定した SF 状態で動作しています。
2. リンク障害回復が行われます。
3. イーサネット リング ノード C と D は、信号障害（SF）状態のクリアを検出し、ガード タイマーを開始し、両方のリング ポートの RAPS（NR）メッセージの定期的な送信を開始します。（ガード タイマーは、RAPS メッセージの受信を防止します）。
4. イーサネット リング ノードが RAPS（NR）メッセージを受信すると、受信側リング ポートのノード ID および BPR のペアが削除され、RPL オーナー ノードは WTR タイマーを開始します。
5. イーサネット リング ノード C と D でガード タイマーの有効期限が切れると、受信する新しい RAPS メッセージを受け入れることがあります。イーサネット リング ノード D は、

イーサネット リング ノード C から上位のノード ID を持つ RAPS（NR）メッセージを受信し、障害が発生していないリング ポートのブロックを解除します。

6. WTR タイマーの有効期限が切れると、RPL オーナー ノードは、RPL の終端をブロックし、（ノード ID、BPR）ペアを持つ RAPS（NR、RB）メッセージを送信し、FDB フラッシュを実行します。

7. イーサネット リング ノード C が RAPS（NR、RB）メッセージを受信すると、ブロックされたリング ポートのブロックを解除し、RAPS（NR）メッセージの送信を停止します。一方、RPL ネイバー ノード A が RAPS（NR、RB）メッセージを受信すると、RPL の終了をブロックします。さらに、イーサネット リング ノード A ～ F は、ノード ID と BPR ベース メカニズムが存在することが原因で、RAPS（NR、RB）メッセージを受信すると FDB フラッシュを実行します。

G.8032 イーサネット リング保護の設定

ERP機能は、リバーティブと非リバーティブ動作モードの両方をサポートしています。デフォルトでは、ERP プロファイル設定で明示的に非リバーティブ モードとして設定されていない限り、ERP リングはリバーティブ モードで動作します。

イーサネット リング保護機能を設定するには、次の作業を実行します。

- ERP プロファイルの設定
- ERP インスタンスの設定

（注） タグの再書き込み（リング自動保護スイッチング（RAPS）チャネルとして使用されているサブインターフェイスのプッシュまたはポップ）はサポートされていません。

ERP プロファイルの設定

イーサネット リング保護（ERP）プロファイルを設定するには、次の作業を実行します。

設定例

```
Router#configure
Router(config)ethernet ring g8032 profile p1
Router(config-g8032-ring-profile)#timer wtr 5
Router(config-g8032-ring-profile)#non-revertive
Router(config-g8032-ring-profile)#commit
```

リバーティブモード：このモードでは、障害が発生したERPリンクがアップ状態になり、WTR タイマーが期限切れになった後、RPLがブロックされます。このモードを有効にするための特定のコマンドや設定はありません。デフォルトでは、ERP プロファイル設定で明示的に非リバーティブ モードとして設定されていない限り、ERP リングはリバーティブ モードで動作します。

非リバーティブモード：このモードでは、RPLがブロック状態のままになります。回復したリンクもRPLオーナーノードで**erp clear**コマンドを実行するか、リングに新しいSFが生じるまで、ブロック状態のままになります。

実行コンフィギュレーション

```
configure
 Ethernet ring g8032 profile p1
  timer wtr 5
  non-revertive
  !
 !
```

ERP インスタンスの設定

ERP インスタンスを設定するには、次の作業を実行します。

設定例

```
Router#configure
Router(config)l2vpn
Router(config-l2vpn)#ethernet ring g8032 ring1
Router(config-l2vpn-erp)#port0 interface TenGigE0/0/0/0
/* To configure an ERP on bundle interface, use the following command */
Router(config-l2vpn-erp)#port0 interface bundle-ether1
Router(config-l2vpn-erp-port0)#exit
Router(config-l2vpn-erp)#port1 interface TenGigE0/0/0/8
/* To configure an ERP on bundle interface, use the following command */
Router(config-l2vpn-erp)#port1 interface bundle-ether2
Router(config-l2vpn-erp-port1)#exit
Router(config-l2vpn-erp)#instance 1
Router(config-l2vpn-erp-instance)#profile p1
Router(config-l2vpn-erp-instance)#rpl port0 owner
Router(config-l2vpn-erp-instance)#inclusion-list vlan-ids 1,7-150
Router(config-l2vpn-erp-instance)#aps-channel
Router(config-l2vpn-erp-instance-aps)#port0 interface TenGigE
Router(config-l2vpn-erp-instance-aps)#port1 interface TenGigE
/* To configure an ERP instance on bundle sub-interfaces, use the following command */
Router(config-l2vpn-erp-instance-aps)#port0 interface bundle-ether1.1
Router(config-l2vpn-erp-instance-aps)#port1 interface bundle-ether2.1
Router(config-l2vpn-erp-instance-aps)#commit
```

包含リストvlan id：これらのvlanのポートは保護され、トラフィックはこれらのポートに対してのみスイッチングされます。

除外リストvlan id：これらのvlan idはG.8032によって保護されません。これらのvlanのトラフィックは通常どおり転送され、これらのvlanのポートはG.8032によってブロックされません。

どちらのリストにも含まれていないvlanは、デフォルトインスタンスの一部となり、これらのvlanのトラフィックはドロップされます。

実行コンフィギュレーション

```
configure
```

```
l2vpn
 ethernet ring g8032 ring1
  port0 interface TenGigE0/0/0/0
 !
  port1 interface TenGigE0/0/0/8
 !
 instance 1
  profile fretta
  rpl port0 owner
  inclusion-list vlan-ids 1,7-150
  aps-channel
   port0 interface TenGigE
   port1 interface TenGigE
  !
 !

!
```

確認

イーサネット リングのステータスを確認します。

```
Router#show ethernet ring g8032 ring1
Thu Jun 14 08:04:47.431 IST

  R: Interface is the RPL-link
  F: Interface is faulty
  B: Interface is blocked
  N: Interface is not present
 FS: Local forced switch
 MS: Local manual switch

RingName                          Inst  NodeType  NodeState    Port0    Port1
-------------------------------------------------------------------------------
ring1                               1    Owner     Idle         R,B
-------------------------------------------------------------------------------------------------

Router#show ethernet ring g8032 status
Thu Jun 14 08:05:35.263 IST

Ethernet ring ring1 instance 1 is RPL Owner node in Idle state
  Port0: TenGigE0/0/0/0 (Monitor: TenGigE0/0/0/0)
         APS-Channel: TenGigE0/0/0/0.1
         Status: RPL, blocked
         Remote R-APS NodeId: 0000.0000.0000, BPR: 0
  Port1: TenGigE0/0/0/8 (Monitor: TenGigE0/0/0/8)
         APS-Channel: TenGigE0/0/0/8.1
         Status: NonRPL
         Remote R-APS NodeId: 0000.0000.0000, BPR: 0
  APS Level: 7
  Open APS ring topology
  Profile: p1
    WTR interval: 1 minutes
    Guard interval: 500 milliseconds
    Hold-off interval: 0 seconds
    Revertive mode
```

G.8032 イーサネット リング保護の設定：例

この設定例では、完全な G.8032 設定に含まれている要素について説明します。

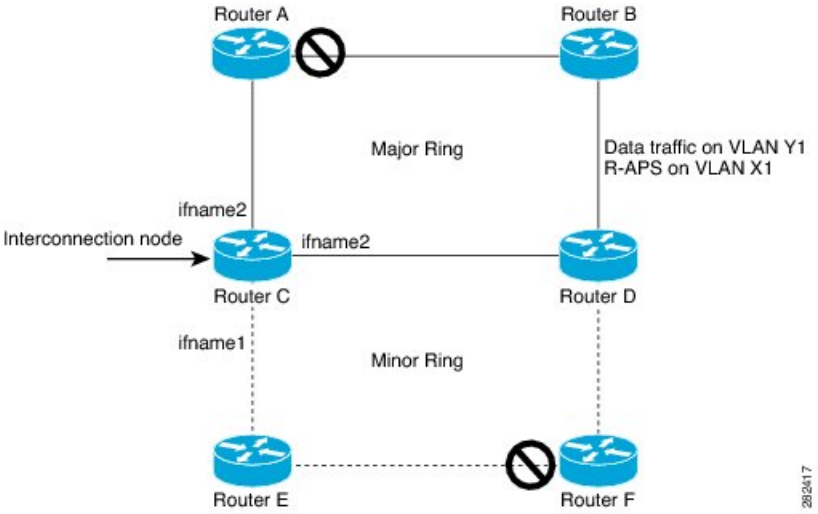
```
# Configure the ERP profile characteristics if ERP instance behaviors are non-default.
ethernet ring g8032 profile ERP-profile
  timer wtr 10
  timer guard 100
  timer hold-off 1
  non-revertive

# Configure CFM MEPs and configure to monitor the ring links.
ethernet cfm
  domain domain1
    service link1 down-meps
   continuity-check interval 100ms
      efd
   mep crosscheck
  mep-id 2
  domain domain2
    service link2 down-meps
   continuity-check interval 100ms
      efd protection-switching
   mep crosscheck
  mep id 2

Interface Gig 0/0/0/0
  ethernet cfm mep domain domain1 service link1 mep-id 1
Interface Gig
  ethernet cfm mep domain domain2 service link2 mep-id 1

# Configure the ERP instance under L2VPN
l2vpn
  ethernet ring g8032 RingA
    port0 interface g0/0/0/0
    port1 interface g
    instance 1
      description BD2-ring
      profile ERP-profile
      rpl port0 owner
      inclusion-list vlan-ids 10-100
      aps channel
        level 3
        port0 interface g0/0/0/0.1
        port1 interface g

# Set up the bridge domains
bridge group ABC
    bridge-domain BD2
      interface Gig

      interface Gig
      interface Gig

    bridge-domain BD2-APS
      interface Gig
      interface Gig

# EFPs configuration
interface Gig  l2transport
  encapsulation dot1q 5
```

```
interface Gig  l2transport
  encapsulation dot1q 5

interface g l2transport
  encapsulation dot1q 10-100

interface g  l2transport
  encapsulation dot1q 10-100

interface g  l2transport
  encapsulation dot1q 10-100
```

相互接続ノードの設定：例

次に、相互接続ノードを設定する例を示します。次の図では、開いたリングのシナリオについて説明します。

図 *18*：リング シナリオ：相互接続ノード



ルータ C（開いたリング：ルータ C）で G.8032 を設定するために必要な最小設定：

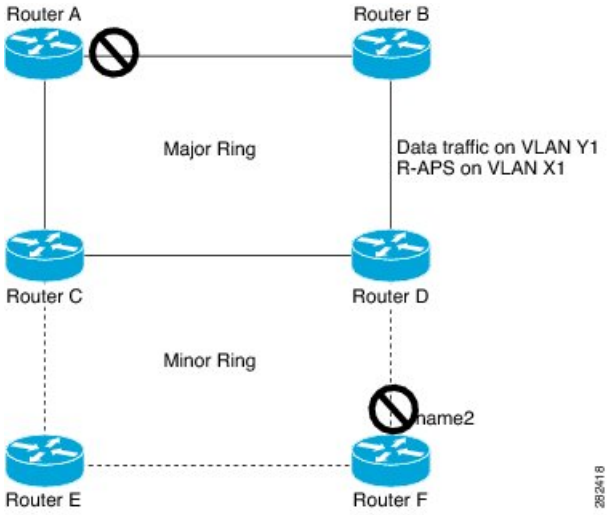
```
interface Gig 0/0/0/1.1 l2transport
 encapsulation dot1q 5
interface Gig 0/0/0/1.10 l2transport
 encapsulation dot1q 6
interface Gig 0/0/0/2.10 l2transport
 encapsulation dot1q 6
interface Gig 0/0/0/3.10 l2transport
 encapsulation dot1q 6
l2vpn
ethernet ring g8032 ring8
      port0 interface Gig 0/0/0/1
      port1 none  /* This router is connected to an interconnection node. */
      open-ring
     !
     instance 1
      inclusion-list vlan-ids 1,7-150
      aps-channel
       port0 interface Gig 0/0/0/1.1
       port1 none /* This router is connected to an interconnection node */
```

```
     !
bridge group bg1
 bridge-domain BD2 /* Data traffic has its own bridge domain */
  interface Gig 0/0/0/1.10
  interface Gig 0/0/0/2.10
  interface Gig 0/0/0/3.10
 !
 bridge-domain BD2-APS /* APS-channel has its own bridge domain */
  interface Gig 0/0/0/1.1 /* There is only one APS-channel at the interconnection node
*/
```

開いたリングのノードの設定：例

次に、開いたリングのノード部分を設定する例を示します。次の図では、開いたリングのシナリオについて説明します。

図 *19*：開いたリング シナリオ



開いたリングのノード（ルータ F で開いたリングのノード部分）で G.8032 を設定するに必要な最小設定：

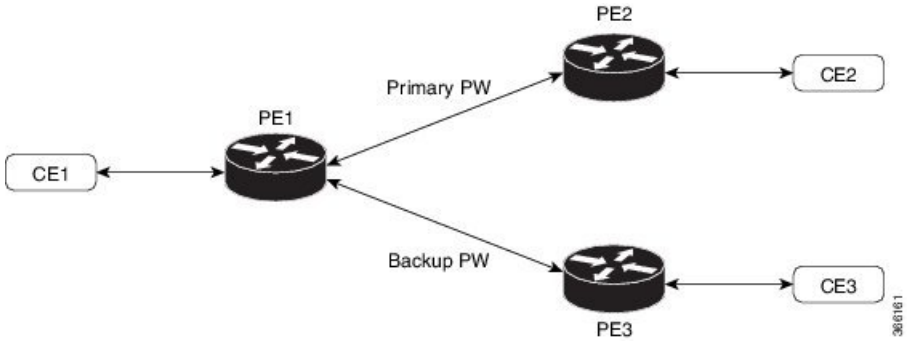
```
interface Gig 0/0/0/1.1 l2transport
 encapsulation dot1q 5
interface Gig 0/0/0/2.1 l2transport
 encapsulation dot1q 5
interface Gig 0/0/0/1.10 l2transport
 encapsulation dot1q 6
interface Gig 0/0/0/2.10 l2transport
 encapsulation dot1q 6
l2vpn
   ethernet ring g8032 ringB
      port0 interface Gig 0/0/0/1
      port1 interface Gig 0/0/0/2
      open-ring
     !
     instance 1
      inclusion-list vlan-ids 1,7-150
      rpl port0 owner  /* This node is RPL owner and interface Gig 0/0/0/2 is blocked
      aps-channel
```

```
       port0 interface Gig 0/0/0/1.1
       port1 interface Gig 0/0/0/2.1

/* Set up the bridge domain
 bridge group bg1
   bridge-domain BD2
    bridge-domain BD2-APS /* APS-channel has its own bridge domain */
     interface Gig 0/0/0/1.1
     interface Gig 0/0/0/2.1
   !
/* Data traffic has its own bridge domain */
   bridge-domain BD2
    interface Gig 0/0/0/1.10
    interface Gig 0/0/0/2.10
```

疑似回線冗長性

疑似回線冗長性機能により、プライマリ疑似回線のバックアップとなる冗長疑似回線を設定できます。プライマリ疑似回線で障害が発生すると、PE ルータが冗長疑似回線に切り替わります。復旧後にプライマリ疑似回線の運用が再開するように選択できます。プライマリ擬似回線での障害発生は、PE ルータに障害が発生した場合、またはネットワークの停止が発生した場合に起こります。

図 *20 :* 疑似回線冗長性



バックアップ疑似回線への強制的な手動切り替え

ルータを強制的にバックアップに切り替える、またはプライマリ疑似回線に戻すには、EXEC モードで **l2vpn switchover** コマンドを使用します。

手動切り替えは、コマンドが入力されたとき、コマンドで指定されたピアが実際に使用可能であり、相互接続が完全なアクティブ状態に移行する場合に限り実行されます。

疑似回線冗長性の設定

ここでは、疑似回線冗長性を設定する方法について説明します。

擬似回線冗長性機能を設定する際には、次の制限事項を考慮する必要があります。

- 2000 のアクティブ PW と 2000 のバックアップ PW がサポートされています。

- MPLS LDP のみがサポートされています。

```
/* Configure PW on PE1 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group XCON1
Router(config-l2vpn-xc)# p2p xc1
Router(config-l2vpn-xc-p2p)# interface GigabitEthernet
Router(config-l2vpn-xc-p2p)# neighbor ipv4 2.2.2.2 pw-id 1
Router(config-l2vpn-xc-p2p-pw)# backup neighbor 3.3.3.3 pw-id 1
Router(config-subif)# commit

/* Configure PW on PE2 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group XCON1
Router(config-l2vpn-xc)# p2p xc1
Router(config-l2vpn-xc-p2p)# interface GigabitEthernet
Router(config-l2vpn-xc-p2p)# neighbor ipv4 1.1.1.1 pw-id 1
Router(config-subif)# commit

/* Configure PW on PE3 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group XCON1
Router(config-l2vpn-xc)# p2p xc1
Router(config-l2vpn-xc-p2p)# interface GigabitEthernet
Router(config-l2vpn-xc-p2p)# neighbor ipv4 1.1.1.1 pw-id 1
Router(config-subif)# commit
```

実行コンフィギュレーション

```
/* On PE1 */
!
l2vpn
 xconnect group XCON1
  p2p XCON1_P2P2
   interface GigabitEthernet
   neighbor ipv4 2.2.2.2 pw-id 1
    backup neighbor 3.3.3.3 pw-id 1
!

/* On PE2 */
!
l2vpn
 xconnect group XCON1
  p2p XCON1_P2P2
   interface GigabitEthernet
   neighbor ipv4 1.1.1.1 pw-id 1

!

/* On PE3 */
!
l2vpn
 xconnect group XCON1
  p2p XCON1_P2P2
   interface GigabitEthernet
   neighbor ipv4 1.1.1.1 pw-id 1

!
```

確認

設定した擬似回線冗長性がアップ状態であることを確認します。

```
/* On PE1 */

Router#show l2vpn xconnect group XCON_1
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
        SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect                    Segment 1                       Segment 2
Group      Name       ST    Description            ST       Description            ST

------------------------   -----------------------------   -----------------------------
XCON_1     XCON1_P2P2 UP    Gi0/1/0/0.1            UP       2.2.2.2     1000   UP
                                                            Backup

                                                            3.3.3.3     1000   SB
--------------------------------------------------------------------------------

/* On PE2 */

Router#show l2vpn xconnect group XCON_1
Tue Jan 17 15:36:12.327 UTC
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
        SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect                    Segment 1                       Segment 2
Group      Name       ST    Description            ST       Description            ST

------------------------   -----------------------------   -----------------------------
XCON_1     XCON1_P2P2 UP    BE100.1                UP       1.1.1.1     1000   UP
--------------------------------------------------------------------------------------

/* On PE3 */

Router#show l2vpn xconnect group XCON_1
Tue Jan 17 15:38:04.785 UTC
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
        SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect                    Segment 1                       Segment 2
Group      Name       ST    Description            ST       Description            ST

------------------------   -----------------------------   -----------------------------
XCON_1     XCON1_P2P2 DN    BE100.1                UP       1.1.1.1     1000   SB
--------------------------------------------------------------------------------------

Router#show l2vpn xconnect summary
Number of groups: 3950
Number of xconnects: 3950
  Up: 3950  Down: 0  Unresolved: 0 Partially-programmed: 0
  AC-PW: 3950  AC-AC: 0  PW-PW: 0 Monitor-Session-PW: 0
Number of Admin Down segments: 0
Number of MP2MP xconnects: 0
  Up 0 Down 0
  Advertised: 0 Non-Advertised: 0
Number of CE Connections: 0
  Advertised: 0 Non-Advertised: 0
Backup PW:
  Configured   : 3950
  UP           : 0
  Down         : 0
```

```
  Admin Down   : 0
  Unresolved   : 0
  Standby      : 3950
  Standby Ready: 0
Backup Interface:
  Configured   : 0
  UP           : 0
  Down         : 0
  Admin Down   : 0
  Unresolved   : 0
  Standby      : 0
```

疑似回線冗長性の設定

疑似回線冗長性を使用すると、ネットワーク内の障害を検出して、サービスの提供を続行可能な別のエンドポイントにレイヤ2サービスを再ルーティングするようにネットワークを設定できます。この機能により、リモートPEルータで発生した障害、またはPEルータとCEルータ間のリンクで発生した障害から回復できます。

L2VPNは、ルーティング プロトコルを通じて疑似回線冗長化機能を提供します。エンドツーエンドPEルータ間の接続が障害になった場合、指示されたLDPセッションとユーザ データの代替パスに引き継ぐことができます。ただし、ネットワークの一部は、この再ルーティング メカニズムでサービスの中断から保護されません。

疑似回線冗長性を使用すると、バックアップ疑似回線を設定できます。ネットワークに冗長疑似回線と冗長ネットワーク エレメントを設定することもできます。

プライマリ疑似回線の障害前に、バックアップ疑似回線にトラフィックをスイッチングする機能が使用され、ルータのメンテナンスなどの計画された疑似回線の停止が処理されます。

設定

ここでは、疑似回線冗長性の設定について説明します。

```
/* Configure a cross-connect group with a static point-to-point
cross connect */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group A
Router(config-l2vpn-xc)# p2p xc1
ROuter(config-l2vpn-xc-p2p)# interface tengige 0/0/0/0.2
Router(config-l2vpn-xc-p2p)# neighbor 10.1.1.2 pw-id 2

/*Configure the pseudowire segment for the cross-connect group */
Router(config-l2vpn-xc-p2p-pw)#pw-class path1

/*Configure the backup pseudowire segment for the cross-connect group */
Router(config-l2vpn-xc-p2p-pw)# backup neighbor 10.2.2.2 pw-id 5
Router(config-l2vpn-xc-p2p-pw-backup)#end

/*Commit your configuration */
Router(config-l2vpn-xc-p2p-pw-backup)#commit
Uncommitted changes found, commit them before exiting(yes/no/cancel)?
[cancel]: yes
```

実行コンフィギュレーション

```
Router# show-running configuration
...
l2vpn
 encapsulation mpls
 !
 xconnect group A
  p2p xc1
   interface tengige 0/0/0/0.2
   neighbor ipv4 10.1.1.2 pw-id 2
    pw-class path1
    backup neighbor 10.2.2.2 pw-id 5
    !
   !
...
```

L2VPN での仮想回線接続検証

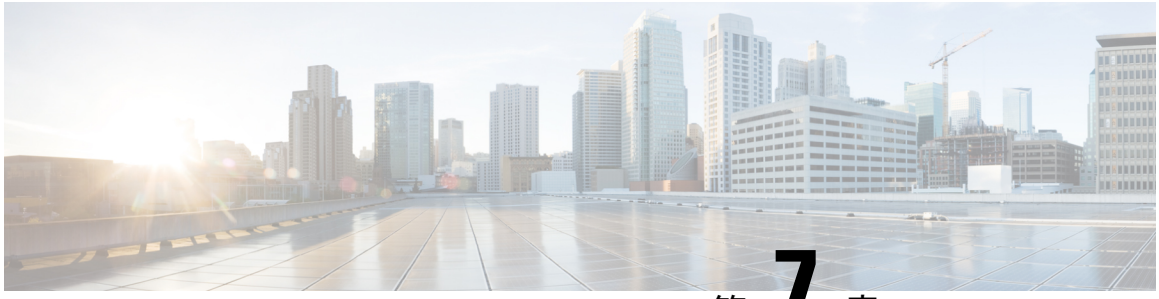
仮想回線接続性検証（VCCV）は、L2VPN の運用、管理、およびメンテナンス（OAM）機能であり、ネットワーク オペレータが、指定した疑似回線上で IP ベースのプロバイダー エッジ間（PE-to-PE）キープアライブ プロトコルを実行できるようにし、疑似回線データ パス転送で障害が発生しないようにします。ディスポジション PE は、指定した疑似回線に関連付けられる制御チャネルで VCCV パケットを受信します。疑似回線が各方向の PE 間で確立されると、VCCV に使用される制御チャネル タイプと接続検証タイプがネゴシエートされます。

2 つのタイプのパケットが判定結果出力に着信します。

- タイプ 1：通常の Ethernet-over-MPLS（EoMPLS）データ パケットを指定します。これには、a）シグナリング時にネゴシエートした場合はインバウンド コントロール ワード、および b）MPLS TTL 有効期限が含まれています。
- タイプ 2：ルータ アラート レベル（ラベル 0）を指定します。

ルータは、タイプ 1 のラベル スイッチド パス（LSP）VCCV パケットをサポートしています。VCCV エコー応答は IPv4 パケットとして送信されます。つまり、応答モードは IPv4 です。

ルータは、VCCV パケットのアカウンティングをサポートしていません。.



第 7 章

マルチポイント レイヤ 2 サービス実装の前提条件

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

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

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

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

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

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

- マルチポイント レイヤ 2 サービスの実装に関する情報 （114 ページ）
- マルチポイント レイヤ 2 サービスの実装方法 （125 ページ）
- MAC アドレス取り消し （151 ページ）
- マルチポイント レイヤ 2 サービスの設定例 （154 ページ）
- LDP ベースの VPLS および VPWS FAT 擬似回線 （164 ページ）

マルチポイント レイヤ 2 サービスの実装に関する情報

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

マルチポイント レイヤ 2 サービスの概要

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

（注） VPLS PW は、BGP マルチパスではサポートされていません。

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

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

ブリッジ ドメイン

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

ブリッジ ドメインと BVI スケール

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

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

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

必要な LIF の数は、

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

疑似回線

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

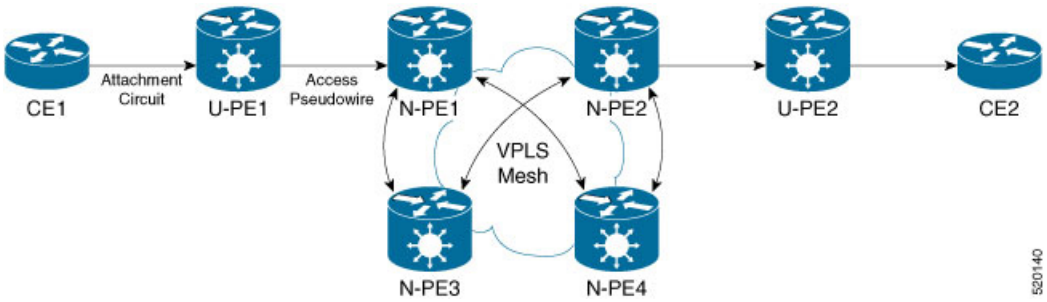
アクセス疑似回線

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

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

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

図 *21* : アクセス疑似回線



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

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

アクセス疑似回線の設定

アクセス疑似配線を設定するには、次のタスクを実行します。

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

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

実行コンフィギュレーション

この項では、アクセス疑似回線の実行コンフィギュレーションを示します。

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

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

確認

アクセス擬似回線の設定を確認します。

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

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

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

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

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

関連項目

- アクセス疑似回線 （115 ページ）

関連コマンド

- show l2vpn xconnect group
- show l2vpn bridge-domain

仮想転送インスタンス

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

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

MPLS ベースのプロバイダー コアの VPLS

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

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

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

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

レイヤ 2 スイッチングの VPLS

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

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

次の機能がサポートされています。

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

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

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

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

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

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

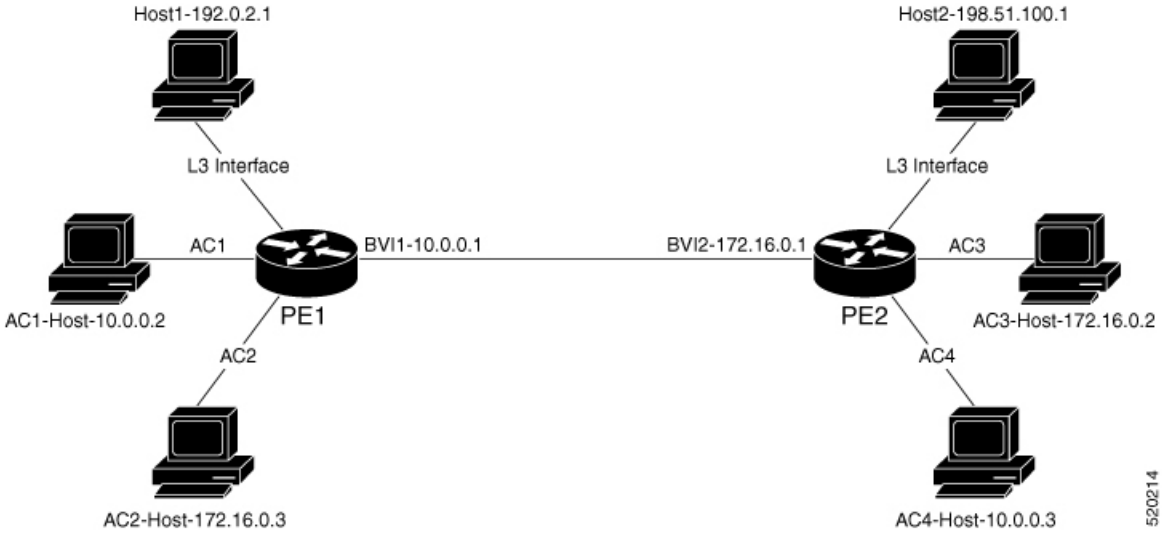
ルーテッドインターフェイスとして BVI を使用した VPLS VFI

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

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

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

図 *22 : ルーテッドインターフェイスとして BVI を使用した VPLS VFI*



このトポロジは、次の 2 種類のトラフィックフローを示しています。

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

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

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

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

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

設定例

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


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

実行コンフィギュレーション

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

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

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


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

確認

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

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

        PW Status TLV in use
```

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

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

関連項目

- ルーテッドインターフェイスとして BVI を使用した VPLS VFI （120 ページ）

関連コマンド

- show l2vpn bridge-domain detail

MAC アドレス関連パラメータ

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

次のトピックでは、MAC アドレス関連パラメータについて説明します。

MAC アドレス フラッディング

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

MAC アドレスベース転送

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

MAC アドレスの送信元ベースの学習

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

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

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

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

MAC アドレス エージング

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

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

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

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

MAC アドレス制限

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

制限を超えると、これらの通知を行うようシステムが設定されています。

- syslog（デフォルト）

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

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

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

MAC アドレス取り消し

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

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

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

LDP MAC 取り消し機能は、次のイベントが原因で生成されます。

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

マルチポイント レイヤ 2 サービスの実装方法

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

ブリッジ ドメインの設定

次のトピックでは、ブリッジ ドメインの設定方法について説明します。

ブリッジ ドメインの作成

ブリッジ ドメインを作成するには、次の作業を実行します。

手順

ステップ 1 **configure**

例：

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

XR コンフィギュレーション モードを開始します。

ステップ 2 **l2vpn**

例：

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

L2VPN コンフィギュレーション モードを開始します。

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

例：

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

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

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

例：

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

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

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

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

end ：次のいずれかのアクションを実行することをユーザに要求します。

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

メンバのブリッジ ドメインへの関連付け

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

- イーサネットおよび VLAN
- VFI

手順

ステップ 1 **configure**

例：

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

XR コンフィギュレーション モードを開始します。

ステップ 2 **l2vpn**

例：

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

L2VPN コンフィギュレーション モードを開始します。

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

例：

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

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

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

例：

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

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

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

例：

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

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

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

例：

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

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

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

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

end ：次のいずれかのアクションを実行することをユーザに要求します。

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

ブリッジ ドメイン パラメータの設定

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

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

手順

ステップ 1 **configure**

例：

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

XR コンフィギュレーション モードを開始します。

ステップ 2 **l2vpn**

例：

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

l2vpn コンフィギュレーション モードを開始します。

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

例：

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

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

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

例：

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

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

ステップ 5 **flooding disable**

例：

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

フラッディングを無効にします。

ステップ 6 **mtu** *bytes*

例：

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

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

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

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

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

end ：次のいずれかのアクションを実行することをユーザに要求します。

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

ブリッジ ドメインのディセーブル化

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

手順

ステップ 1 **configure**

例：

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

XR コンフィギュレーション モードを開始します。

ステップ 2 **l2vpn**

例：

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

L2VPN コンフィギュレーション モードを開始します。

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

例：

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

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

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

例：

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

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

ステップ 5 **shutdown**

例：

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

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

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

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

end ：次のいずれかのアクションを実行することをユーザに要求します。

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

フラッディングの無効化

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

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

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

フラッディング無効化の設定

フラッディング無効化機能を設定するには、次のタスクを実行します。

次のフラッディングを無効にできます。

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

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

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

設定例

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

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

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

実行コンフィギュレーション

ここでは、フラッディング無効化の実行コンフィギュレーションを示します。

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

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

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


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

関連コマンド

- flooding disable
- flooding unknown-unicast disable

レイヤ 2 仮想転送インスタンスの設定

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

仮想転送インスタンスの作成

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

手順

ステップ 1 **configure**

例：

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

XR コンフィギュレーション モードを開始します。

ステップ 2 **l2vpn**

例：

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

L2VPN コンフィギュレーション モードを開始します。

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

例：

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

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

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

例：

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

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

ステップ 5 **vfi** {*vfi-name*}

例：

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

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

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

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

end ：次のいずれかのアクションを実行することをユーザに要求します。

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

疑似回線の仮想転送インスタンスへの関連付け

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

手順

ステップ 1 **configure**

例：

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

XR コンフィギュレーション モードを開始します。

ステップ 2 **l2vpn**

例：

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

L2VPN コンフィギュレーション モードを開始します。

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

例：

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

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

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

例：

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

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

ステップ 5 **vfi** { *vfi name* }

例：

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

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

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

例：

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

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

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

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

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

end ：次のいずれかのアクションを実行することをユーザに要求します。

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

ブリッジ ドメインへの仮想転送インスタンスの関連付け

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

手順

ステップ 1 **configure**

例：

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

XR コンフィギュレーション モードを開始します。

ステップ 2 **l2vpn**

例：

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

L2VPN コンフィギュレーション モードを開始します。

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

例：

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

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

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

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

例：

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

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

ステップ 5 **vfi** { *vfi name* }

例：

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

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

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

例：

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

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

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

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

例：

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

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

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

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

end ：次のいずれかのアクションを実行することをユーザに要求します。

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

疑似回線への疑似回線クラスの接続

疑似回線に疑似回線クラスを接続するには、次の作業を実行します。

手順

ステップ 1 **configure**

例：

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

XR コンフィギュレーション モードを開始します。

ステップ 2 **l2vpn**

例：

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

L2VPN コンフィギュレーション モードを開始します。

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

例：

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

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

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

例：

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

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

ステップ 5 **vfi** { *vfi-name* }

例：

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

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

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

例：

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

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

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

ステップ 7 **pw-class** { *class-name* }

例：

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

疑似回線に使用する疑似回線クラス テンプレート名を設定します。

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

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

end ：次のいずれかのアクションを実行することをユーザに要求します。

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

スタティック ラベルを使用した擬似回線の設定

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

手順

ステップ 1 **configure**

例：

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

XR コンフィギュレーション モードを開始します。

ステップ 2 **l2vpn**

例：

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

L2VPN コンフィギュレーション モードを開始します。

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

例：

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

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

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

例：

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

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

ステップ 5 **vfi** { *vfi-name* }

例：

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

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

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

例：

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

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

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

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

例：

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

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

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

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

end ：次のいずれかのアクションを実行することをユーザに要求します。

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

仮想転送インスタンスのディセーブル化

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

手順

ステップ 1 **configure**

例：

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

XR コンフィギュレーション モードを開始します。

ステップ 2 **l2vpn**

例：

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

L2VPN コンフィギュレーション モードを開始します。

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

例：

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

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

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

例：

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

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

ステップ 5 **vfi** { *vfi-name* }

例：

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

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

ステップ 6 **shutdown**

例：

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

仮想転送インターフェイス（VFI）をディセーブルにします。

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

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

end ：次のいずれかのアクションを実行することをユーザに要求します。

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

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

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

例：

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

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

MAC アドレス関連パラメータの設定

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

MAC テーブル属性は、ブリッジ ドメインについて設定されます。

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

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

MAC アドレスの送信元ベースの学習の設定

MAC アドレスの送信元ベースの学習を設定するには、次の作業を実行します。

手順

ステップ 1 **configure**

例：

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

XR コンフィギュレーション モードを開始します。

ステップ 2 **l2vpn**

例：

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

L2VPN コンフィギュレーション モードを開始します。

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

例：

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

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

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

例：

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

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

ステップ 5 **mac**

例：

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

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

ステップ 6 **learning disable**

例：

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

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

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

end ：次のいずれかのアクションを実行することをユーザに要求します。

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

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

例：

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

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

MAC アドレス制限の設定

MAC アドレス制限のパラメータを設定するには、次の作業を実行します。

手順

ステップ 1 **configure**

例：

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

XR コンフィギュレーション モードを開始します。

ステップ 2 **l2vpn**

例：

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

L2VPN コンフィギュレーション モードを開始します。

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

例：

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

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

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

例：

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

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

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

例：

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

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

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

ステップ 6 **mac**

例：

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

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

ステップ 7 **limit**

例：

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

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

ステップ 8 **maximum** { *value* }

例：

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

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

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

例：

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

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

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

例：

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

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

ステップ 11 **mac limit threshold** *80*

例：

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

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

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

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

end ：次のいずれかのアクションを実行することをユーザに要求します。

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

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

例：

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

MAC アドレス制限の詳細が表示されます。

MAC アドレス エージングの設定

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

手順

ステップ 1 **configure**

例：

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

XR コンフィギュレーション モードを開始します。

ステップ 2 **l2vpn**

例：

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

L2VPN コンフィギュレーション モードを開始します。

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

例：

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

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

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

例：

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

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

ステップ 5 **mac**

例：

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

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

ステップ 6 **aging**

例：

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

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

ステップ 7 **time** { *seconds* }

例：

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

最大エージング タイムを設定します。

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

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

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

end ：次のいずれかのアクションを実行することをユーザに要求します。

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

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

例：

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

エージング フィールドに関する詳細を表示します。

ブリッジ ポート レベルでの MAC フラッシュのディセーブル化

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

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

手順

ステップ 1 **configure**

例：

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

XR コンフィギュレーション モードを開始します。

ステップ 2 **l2vpn**

例：

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

L2VPN コンフィギュレーション モードを開始します。

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

例：

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

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

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

例：

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

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

ステップ 5 **mac**

例：

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

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

ステップ 6 **port-down flush disable**

例：

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

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

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

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

end ：次のいずれかのアクションを実行することをユーザに要求します。

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

MAC アドレス取り消し

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

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

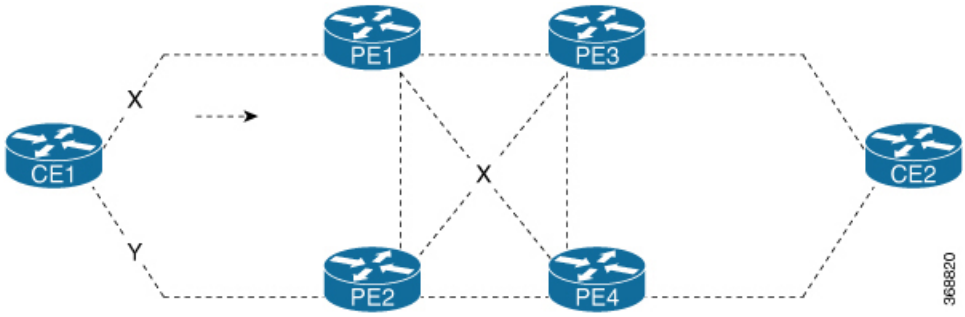
MAC アドレス取り消し機能はデフォルトでイネーブルになっています。MAC アドレス取り消し機能をディセーブルにするには、**mac withdraw disable** コマンドを使用します。

トポロジ

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

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

図 *23 : MAC* アドレス取り消し



制約事項

MAC アドレス取り消しを設定する場合、次の制限事項が適用されます。

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

MAC アドレス取り消しの設定

設定例

MAC アドレス取り消しを設定するには、次の作業を実行します。

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

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

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

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

実行コンフィギュレーション

ここでは、MAC アドレス取り消しの実行コンフィギュレーションを示します。

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

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


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

確認

MAC アドレス取り消しの設定を確認します。

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

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

関連項目

- MAC アドレス取り消し （151 ページ）

関連コマンド

- mac withdraw
- show l2vpn bridge-domain detail

マルチポイント レイヤ 2 サービスの設定例

ここで示す設定例は、次のとおりです。

プロバイダーエッジ間のマルチポイント レイヤ2サービスの設定：例

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

この設定は、PE 1 を設定する例を示しています。

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

この設定は、PE 2 を設定する例を示しています。

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

    vfi 1
```

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

この設定は、PE 3 を設定する例を示しています。

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

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

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

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

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

MAC アドレス取り消しフィールドの表示：例

この出力は、MAC アドレス取り消しフィールドの例を示しています。

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

Legend: pp = Partially Programmed.
Bridge group: 222, bridge-domain: 222, id: 0, state: up, ShgId: 0, MSTi: 0
  Coupled state: disabled
  MAC learning: enabled
  MAC withdraw: enabled
    MAC withdraw sent on: bridge port up
    MAC withdraw relaying (access to access): disabled
  Flooding:
    Broadcast & Multicast: enabled
    Unknown unicast: enabled
  MAC aging time: 300 s, Type: inactivity
  MAC limit: 4000, Action: none, Notification: syslog
  MAC limit reached: no
  MAC port down flush: enabled
  MAC Secure: disabled, Logging: disabled
  Split Horizon Group: none
```

```
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping: enabled
IGMP Snooping profile: none
MLD Snooping profile: none
Storm Control: disabled
Bridge MTU: 1500
MIB cvplsConfigIndex: 1
Filter MAC addresses:
P2MP PW: disabled
Create time: 01/03/2017 11:01:11 (00:21:33 ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 1 (1 up), PBBs: 0 (0 up)
List of ACs:
  AC: TenGigE0/2/0/1.7, state is up
    Type VLAN; Num Ranges: 1
    Outer Tag: 21
    VLAN ranges: [22, 22]
    MTU 1508; XC ID 0x208000b; interworking none
    MAC learning: enabled
    Flooding:
      Broadcast & Multicast: enabled
      Unknown unicast: enabled
    MAC aging time: 300 s, Type: inactivity
    MAC limit: 4000, Action: none, Notification: syslog
    MAC limit reached: no
    MAC port down flush: enabled
    MAC Secure: disabled, Logging: disabled
    Split Horizon Group: none
    Dynamic ARP Inspection: disabled, Logging: disabled
    IP Source Guard: disabled, Logging: disabled
    DHCPv4 snooping: disabled
    IGMP Snooping: enabled
    IGMP Snooping profile: none
    MLD Snooping profile: none
    Storm Control: bridge-domain policer
    Static MAC addresses:
    Statistics:
     packets: received 714472608 (multicast 0, broadcast 0, unknown unicast 0, unicast
0), sent 97708776
      bytes: received 88594603392 (multicast 0, broadcast 0, unknown unicast 0, unicast
0), sent 12115888224
      MAC move: 0
    Storm control drop counters:
      packets: broadcast 0, multicast 0, unknown unicast 0
      bytes: broadcast 0, multicast 0, unknown unicast 0
    Dynamic ARP inspection drop counters:
      packets: 0, bytes: 0
    IP source guard drop counters:
      packets: 0, bytes: 0
List of VFIs:
  VFI 222 (up)
    PW: neighbor 1.1.1.1, PW ID 222, state is up ( established )
      PW class not set, XC ID 0xc000000a
      Encapsulation MPLS, protocol LDP
      Source address 21.21.21.21
      PW type Ethernet, control word disabled, interworking none
      Sequencing not set

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

```
    Group ID     0x0                            0x0
    Interface    222                            222
    MTU          1500                           1500
    Control word disabled                       disabled
    PW type      Ethernet                       Ethernet
    VCCV CV type 0x2                            0x2
                 (LSP ping verification)        (LSP ping verification)
    VCCV CC type 0x6                            0x6
                 (router alert label)           (router alert label)
                 (TTL expiry)                   (TTL expiry)
    ------------ ------------------------------ -------------------------
  Incoming Status (PW Status TLV):
    Status code: 0x0 (Up) in Notification message
  MIB cpwVcIndex: 3221225482
  Create time: 01/03/2017 11:01:11 (00:21:33 ago)
  Last time status changed: 01/03/2017 11:21:01 (00:01:43 ago)
  Last time PW went down: 01/03/2017 11:15:21 (00:07:23 ago)
  MAC withdraw messages: sent 0, received 0
  Forward-class: 0
  Static MAC addresses:
  Statistics:
    packets: received 95320440 (unicast 0), sent 425092569
    bytes: received 11819734560 (unicast 0), sent 52711478556
    MAC move: 0
  Storm control drop counters:
    packets: broadcast 0, multicast 0, unknown unicast 0
    bytes: broadcast 0, multicast 0, unknown unicast 0
DHCPv4 snooping: disabled
IGMP Snooping profile: none
MLD Snooping profile: none
VFI Statistics:
  drops: illegal VLAN 0, illegal length 0
```

IOS XR トランク インターフェイスでのブリッジング：例

次に、を単純な L2 スイッチとして設定する例を示します。

特記事項：

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

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

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

設定例

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

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

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

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

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

次の表に、設定手順（アクション）およびこの例の対応する目的を示します。

手順

ステップ 1 **configure**

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **interface Bundle-ether10**

新しいバンドル トランク インターフェイスを作成します。

ステップ 3 **l2transport**

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

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

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

ステップ 5 **bundle id 10 mode active**

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

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

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

ステップ 7 **bundle id 10 mode active**

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

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

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

ステップ 9 **l2transport**

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

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

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

ステップ 11 **l2transport**

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

ステップ 12 **interface TenGigE0/1/0/2**

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

ステップ 13 **l2transport**

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

ステップ 14 **l2vpn**

L2VPN コンフィギュレーション モードを開始します。

ステップ 15 **bridge group examples**

ブリッジ グループ **examples** を作成します。

ステップ 16 **bridge-domain test-switch**

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

ステップ 17 **interface Bundle-ether10**

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

ステップ 18 **exit**

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

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

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

ステップ 20 **exit**

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

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

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

ステップ 22 **exit**

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

ステップ 23 **interface TenGigE0/1/0/2**

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

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

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

end ：次のいずれかのアクションを実行することをユーザに要求します。

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

イーサネット フロー ポイントでのブリッジング：例

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

特記事項：

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

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

設定例

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

次の表に、設定手順（アクション）およびこの例の対応する目的を示します。

手順

ステップ 1 **configure**

グローバル コンフィギュレーション モードを開始します。

ステップ 2 **interface Bundle-ether10**

新しいバンドル トランク インターフェイスを作成します。

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

新しいバンドル トランクに EFP を作成します。

ステップ 4 **encapsulation dot1q 999**

この EFP に VLAN ID 999 を割り当てます。

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

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

ステップ 6 **bundle id 10 mode active**

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

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

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

ステップ 8 **bundle id 10 mode active**

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

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

GigabitEthernet0/6/0/7 に EFP を作成します。

ステップ 10 **encapsulation dot1q 999**

この EFP に VLAN ID 999 を割り当てます。

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

TenGigE0/1/0/2 に EFP を作成します。

ステップ 12 **encapsulation dot1q 999**

この EFP に VLAN ID 999 を割り当てます。

ステップ 13 **l2vpn**

L2VPN コンフィギュレーション モードを開始します。

ステップ 14 **bridge group examples**

examples という名前のブリッジ グループを作成します。

ステップ 15 **bridge-domain test-efp**

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

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

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

ステップ 17 **exit**

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

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

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

ステップ 19 **exit**

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

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

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

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

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

end ：次のいずれかのアクションを実行することをユーザに要求します。

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

LDP ベースの VPLS および VPWS FAT 擬似回線

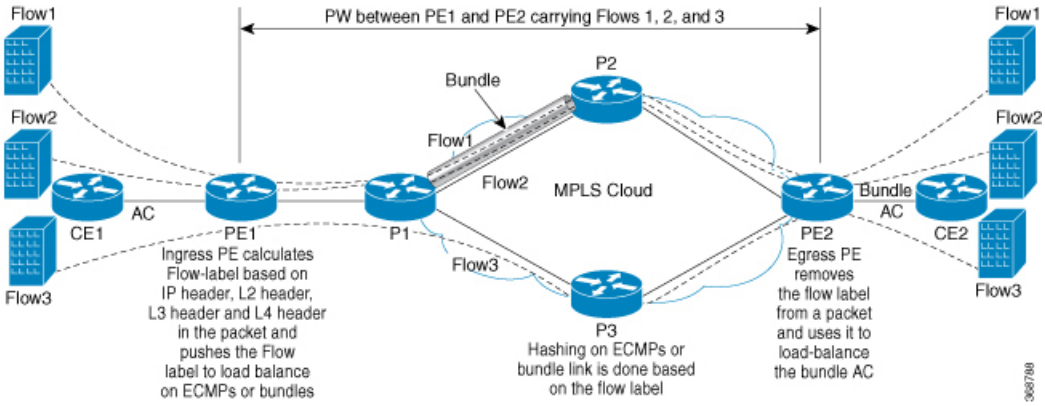
LDP ベースの VPLS および VPWS FAT 擬似回線機能を使用すると、プロバイダー（P）のルータでフローベースのロード バランシングを使用してプロバイダー エッジ（PE）デバイス間でトラフィックを転送できます。この機能は、MPLS パケット スイッチド ネットワーク上で疑似回線（PW）のフロー認識型転送（FAT）を使用して、仮想プライベート LAN サービス（VPLS）およびバーチャル プライベート ワイヤ サービス（VPWS）の LDP ベースのシグナリング擬似回線間でトラフィックのロードバランシングを行います。

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

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

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

図 *24 : FAT PW* と *ECMP* およびバンドルされたリンクに分配される *2* つのフロー



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

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

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

LDP ベースの VPLS および VPWS FAT 擬似回線の設定

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

設定例

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

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

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

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

実行コンフィギュレーション

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

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

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

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

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

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

確認

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

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

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

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

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

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

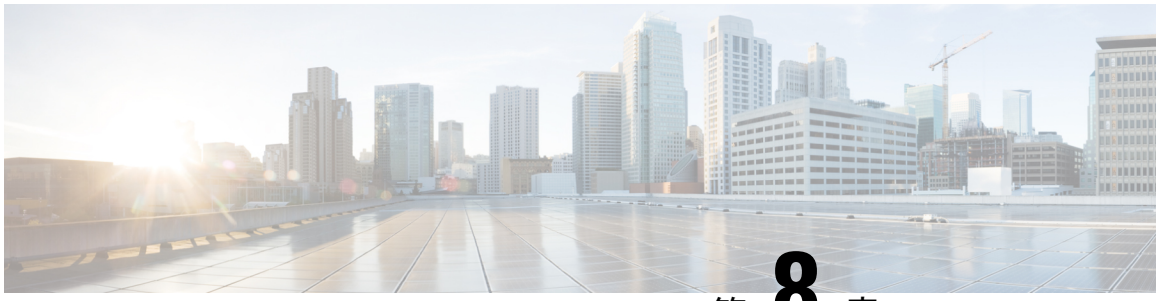
```
Statistics:
  packets: received 0, sent 0
 bytes: received 0, sent 0
```

関連項目

- LDP ベースの VPLS および VPWS FAT 擬似回線 （164 ページ）

関連コマンド

- show l2vpn xconnect detail



第 8 章

EVPN の概要

イーサネット VPN（EVPN）は、MPLS ネットワークを介してイーサネット マルチポイント サービスを提供する次世代のソリューションです。EVPN は、コアでコントロールプレーン ベースの MAC ラーニングを可能にする既存の仮想プライベート LAN サービス（VPLS）とは対照的に動作します。EVPN では、EVPN インスタンスに参加している PE が MP-BGP プロトコルを使用してコントロールプレーン内でカスタマー MAC ルートを学習します。コントロールプレーン MAC ラーニングは、フローごとのロードバランシングによるマルチホーミングのサポートなど、VPLS の欠点に EVPN で対処できるようにする数多くの利点をもたらします。

EVPNは、ネットワークでの次の新たなニーズに対応するソリューションをネットワーク オペレータに提供します。

- データセンター相互接続操作（DCI）
- クラウドおよびサービスの仮想化
- プロトコルの排除とネットワークの簡素化
- 同じ VPN を介した L2 サービスと L3 サービスの統合
- サービスとワークロードの柔軟な配置
- L2 および L3 VPN によるマルチテナント
- 最適な転送とワークロード モビリティ
- 高速コンバージェンス
- 効率的な帯域幅利用

EVPN の利点

EVPN には次の利点があります。

- 統合サービス：L2 および L3 VPN サービスの統合、拡張性と制御における L3VPN のような原則と運用経験、ECMP を使用したオールアクティブ マルチホーミングと PE ロードバランシング、複数の PE に対してマルチホームである CE との間で発着信するトラフィックのロードバランシングが可能。

- ネットワーク効率：フラッドと学習メカニズムの排除、デュアルホーム接続サーバへのリンクでの障害発生時の高速再ルーティング、復元力、および高速な再コンバージェンス、ブロードキャスト、不明ユニキャスト、マルチキャスト（BUM）トラフィック配信の最適化。
- サービスの柔軟性：MPLS データ プレーンのカプセル化、既存および新しいサービス タイプのサポート（E-LAN、E-Line）、ピア PE 自動検出、および冗長グループ自動感知。

EVPN のモード

次の EVPN モードがサポートされています。

- シングルホーミング：これにより、カスタマー エッジ（CE）デバイスをプロバイダー エッジ（PE）デバイス 1 台に接続できます。
- マルチホーミング：これにより、カスタマーエッジ（CE）デバイスを複数のプロバイダーエッジ（PE）デバイスに接続できます。マルチホーミングにより、冗長接続が確保されます。冗長 PE デバイスは、ネットワーク障害が発生している場合にトラフィックが中断されないようにします。次にマルチホーミングのタイプを示します。
  - オールアクティブ：オールアクティブ モードでは、特定のイーサネットセグメントに接続されているすべての PE が、そのイーサネット セグメントとの間で発着信するトラフィックを転送できます。

EVPN の概念

EVPN 機能を実装するには、次の概念を理解する必要があります。

- イーサネット セグメント（ES）：イーサネット セグメントは、マルチホーム デバイスに接続する一連のイーサネット リンクです。マルチホーム デバイスまたはネットワークが 2 つ以上の PE に一連のイーサネット リンクを通じて接続されている場合に、その一連のリンクをイーサネット セグメントと呼びます。イーサネット セグメント ルートはルート タイプ 4 とも呼びます。このルートは、BUM トラフィックの指定フォワーダ（DF）の選択に使用されます。
- イーサネットセグメント識別子（ESI）：イーサネットセグメントには一意の非ゼロの識別子が割り当てられます。これをイーサネットセグメント識別子（ESI）と呼びます。ESI は、ネットワーク全体にわたってイーサネット セグメントを一意に表します。
- EVI：EVPN インスタンス（EVI）は仮想ネットワーク識別子（VNI）で表されます。EVI は、PE ルータ上の VPN を表します。EVI は IP VPN ルーティングおよび転送（VRF）と同じ役割を果たし、インポート/エクスポート ルート ターゲット（RT）が割り当てられます。ユーザ ネットワーク インターフェイス（UNI）でのサービス多重化動作に応じて、ポート上のすべてのトラフィック（すべて対 1 のバンドリング）、VLAN 上のトラフィック（1 対 1 のマッピング）、または VLAN のリスト/範囲のトラフィック（選択的バンドリング）をブリッジ ドメイン（BD）にマップできます。この BD は EVI に関連付けられ、MPLS コアに転送されます。
- EAD/ES：ES ごとのイーサネット自動検出ルートはルート タイプ 1 とも呼ばれます。このルートは、アクセス失敗のシナリオ時にトラフィックを早急に収束するために使用されます。このルートにはイーサネット タグ 0xFFFFFFFF が使用されます。
- EAD/EVI：EVI ごとのイーサネット自動検出ルートはルート タイプ 1 とも呼ばれます。このルートは、トラフィックはスイッチの 1 つにのみハッシュされるときのエイリアシングとロードバランシングに使用されます。EAD/ES ルートと区別するため、このルートにはイーサネット タグ値 0xFFFFFF を使用できません。
- エイリアシング：ルート タイプ 1 の EAD/EVI ルートを使用する所定のイーサネット セグメントで接続されているすべてのスイッチへのトラフィックのロードバランシングに使用されます。これはホストを実際に学習するスイッチとは関係なく実行されます。
- 大量撤回：ルート タイプ 1 の EAD/ES ルートを使用し、アクセス障害シナリオ時に早急に収束するために使用されます。
- DF の選択：ループの転送を防ぐために使用されます。カプセル化を解除し、所定のイーサネット セグメントにトラフィックを転送するため、単一のルータのみを使用します。

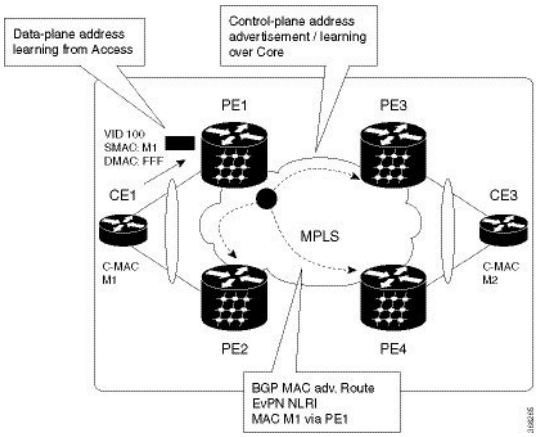
EVPN 動作

以下をアドバタイズするため、PE は起動時に EVPN ルートを交換します。

- **VPN メンバーシップ**：PE は所定のリモート PE のすべてのメンバーを検出します。マルチキャスト入力レプリケーション モデルの場合、EVI に関連付けられている PE フラッド リストの構築にこの情報が使用されます。MAC アドレスを学習した時点で BUM ラベルとユニキャスト ラベルが交換されます。

- **イーサネット セグメント到達可能性**：マルチホーミングのシナリオでは、PE がリモート PE と対応するそれらの冗長モード（オールアクティブまたはシングルアクティブ）を自動的に検出します。セグメント障害が発生した場合、PE はこの段階で使用していたルートを撤回し、リモート PE 上の MAC 大量撤回をシグナリングすることで高速コンバージェンスをトリガーします。
- **冗長グループ メンバーシップ**：同じイーサネット セグメントに接続している（マルチホーミング）PE は互いに自動的に検出され、所定の EVI に対するブロードキャスト、不明ユニキャストおよびマルチキャスト（BUM）トラフィックの転送を担う指定フォワーダ（FD）を選択します。

図 *25 : EVPN* 動作



EVPN はシングルホーミング モードまたはデュアルホーミング モードで動作できます。PE 上で EVPN が有効になっており、各 PE が所定の EVPN インスタンスの他のすべてのメンバー PE を検出したときにルート タイプ 3 がアドバタイズされるシングルホーミングのシナリオを考えてみます。不明ユニキャスト（または BUM）MAC を PE で受信すると、EVPN ルート タイプ 2 として他の PE にアドバタイズされます。MAC ルートは EVPN ルート タイプ 2 を使用して他の PE にアドバタイズされます。マルチホーミングのシナリオでは、ルート タイプ 1、3、および 4 がアドバタイズされ、他の PE とそれらの冗長モード（シングルアクティブまたはオールアクティブ）を検出します。ルート タイプ 1 を使用するのは、同じ CE をホストする他の PE を自動検出するためです。この他にも、このルート タイプは CE と PE 間の破損リンクから離れている高速ルートユニキャスト トラフィックにも使用されます。ルート タイプ 4 は、指定フォワーダの選択に使用されます。たとえば、カスタマー トラフィックが PE に着信し、ローカル イーサネット セグメント上で学習した各カスタマー MAC アドレスの到達可能性情報を EVPN MAC アドバタイズメント ルートでコアを介して配布するトポロジを考えてみます。各 EVPN MAC ルートは、カスタマー MAC アドレスと、MAC を学習したポートに関連付けられたイーサネット セグメントおよびその関連付けられた MPLS ラベルをアナウンスします。この EVPN MPLS ラベルは、アドバタイズされた MAC アドレス宛にトラフィックを送信するときにリモート PE によって後で使用されます。

ESI ラベル割り当てによる動作の変更

RFC 7432 の推奨事項に準拠するため、MPLS ラベルの符号化や復号化が、拡張コミュニティで変更されました。これまでは、スプリット ホライズン グループ（SHG）ラベルを符号化するために、拡張コミュニティの下位 20 ビットが使用されていました。今回のリリースから、SHG ラベルの符号化では拡張コミュニティの上位 20 ビットが使用されるようになりました。

この変更により、新旧のソフトウェア リリース バージョンを実行している同じイーサネット セグメント内のルータは、拡張コミュニティを異なる方法で復号化します。この変更により、ピアリング EVPN PE ルータの SHG ラベルで不整合が発生します。ほとんどの場合、ルータは誤った SHG ラベルを持つ BUM パケットをドロップします。ただし、特定の状況では、リモート PE がこのようなパケットを受け入れて CE に転送し、ループが発生する可能性があります。このような状況が発生するのは、ラベルが誤って NULL と読み取られる場合です。

この問題を解決するには、次のことを行うことをお勧めします。

- 両方の PE が異なるソフトウェア リリース バージョンを実行している時間を最小限に抑えます。
- 新しいリリースにアップグレードする前に、アップグレードしたノードを分離し、対応する AC バンドルをシャットダウンします。
- 両方の PE を同じリリースにアップグレードした後、両方のサービスを稼働できます。

同様の推奨事項は、RFC 7432 に準拠していない SHG ラベル割り当てを持つ異なるベンダーとのピアリング PE に適用可能です。

EVPN ルート タイプ

EVPN ネットワーク層到達可能性情報（NLRI）は、さまざまなルート タイプを提供します。

表 *4 : EVPN* ルート タイプ

ルート タイプ	名前	使用法
1	イーサネット自動検出（AD）ルート	ES ごとの少数ルートの送信、ES に属する EVI のリストの伝送
2	MAC/IP アドバタイズメント ルート	MAC のアドバタイズ、アドレス到達可能性、IP/MAC バインディングのアドバタイズ
3	包括的なマルチキャスト イーサネット タグ ルート	マルチキャスト トンネル エンド ポイントの検出
4	イーサネット セグメント ルート	冗長グループの検出、DF の選択

ルート タイプ	名前	使用法
5	IP プレフィックス ルート	IP プレフィックスのアドバタイズ

ルート タイプ 1：**イーサネット自動検出（AD）ルート**

イーサネット自動検出（AD）ルートは、EVI ごとと ESI ごとにアドバタイズされます。これらのルートは、ES ごとに送信されます。これらは ES に属している EVI のリストを伝送します。ESI フィールドは、CE がシングルホームの場合はゼロに設定されます。このルート タイプは、ロードバランシングのための MAC アドレスの大量撤回とエイリアシングに使用されます。

ルート タイプ 2：**MAC/IP アドバタイズメント ルート**

これらのルートは VLAN ごとのルートであるため、VNI に含まれている PE のみにこれらのルートが必要です。ホストの IP アドレスと MAC アドレスが NRLI 内のピアにアドバタイズされます。MAC アドレスのコントロール プレーン学習は不明ユニキャストのフラッディングを削減します。

ルート タイプ 3：**包括的なマルチキャスト イーサネット タグ ルート**

このルートは、送信元 PE からリモート PE へのブロードキャスト、不明ユニキャスト、およびマルチキャスト（BUM）トラフィック用の接続を確立します。このルートは、VLAN ごとと ESI ごとにアドバタイズされます。

ルート タイプ 4：**イーサネット セグメント ルート**

イーサネット セグメント ルートでは CE デバイスを 2 台のデバイスまたは PE デバイスを接続できます。ES ルートでは同じイーサネット セグメントに接続されている PE デバイスを検出できます。

ルート タイプ 5：**IP プレフィックス ルート**

IP プレフィックスが MAC アドバタイズメント ルートとは関係なくアドバタイズされます。EVPN IRB では、ホスト ルート /32 は RT-2 を使用してアドバタイズされ、サブネット /24 は RT-5 を使用してアドバタイズされます。

（注） EVPN IRB では、ホスト ルート /32 は RT-2 を使用してアドバタイズされ、サブネット /24 は RT-5 を使用してアドバタイズされます。

EVPN L2 ブリッジング サービスの設定

EVPN L2 ブリッジング サービスを設定するには、次のステップを実行します。

（注） 必ず、ラベル モードをプレフィックス単位から VRF ラベル モード単位に変更してください。L2FIB および VPNv4 ルート（ラベル）は同じリソースを共有しているため、リソースを枯渇させると BVI の ping は失敗します。

（注） EVPN または VPLS ブリッジで直接接続されたネイバーへのトラフィックは、次の場合は機能しません。

- ネイバーに暗黙的ヌルが設定されている場合。
- インポジションノードにラベルの付いていない（プライマリ）パスとラベルの付いたパス（バックアップ）が混在している場合。

（注） デバイスには最大 128K の MAC アドレス エントリを含めることができます。デバイス上のブリッジ ドメインには最大 64K の MAC アドレス エントリを含めることができます。

（注） フラッディングの無効化は、EVPN ブリッジ ドメインではサポートされていません。

```
/* Configure address family session in BGP */
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router#(config)# router bgp 200
RP/0/RSP0/CPU0:router#(config-bgp)# bgp router-id 209.165.200.227
RP/0/RSP0/CPU0:router#(config-bgp)# address-family l2vpn evpn
RP/0/RSP0/CPU0:router#(config-bgp)# neighbor 10.10.10.10
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# remote-as 200
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# description MPLSFACING-PEER
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# update-source Loopback 0
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# address-family l2vpn evpn

/* Configure EVI and define the corresponding BGP route targets */

Router# configure
Router(config)# evpn
Router(config-evpn)# evi 6005
Router(config-evpn-evi)# bgp
Router(config-evpn-evi-bgp)# rd 200:50
Router(config-evpn-evi-bgp)# route-target import 100:6005
Router(config-evpn-evi-bgp)# route-target export 100:6005
Router(config-evpn-evi-bgp)# exit
Router(config-evpn-evi)# advertise-mac

/* Configure a bridge domain */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group 1
Router(config-l2vpn-bg)# bridge-domain 1-1
```

```
Router(config-l2vpn-bg-bd)# interface GigabitEthernet
Router(config-l2vpn-bg-bd-ac)# evi 6005
Router(config-l2vpn-bg-bd-ac-evi)# commit
Router(config-l2vpnbg-bd-ac-evi)# exit
```

実行コンフィギュレーション

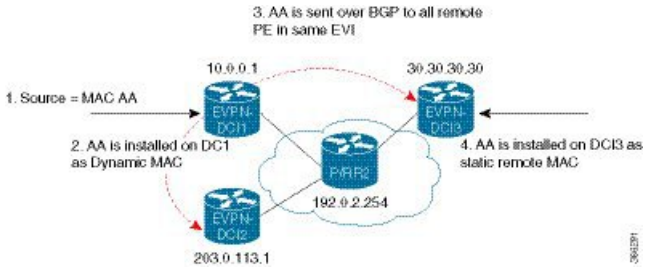
```
router bgp 200 bgp
 router-id 209.165.200.227
 address-family l2vpn evpn
 neighbor 10.10.10.10
  remote-as 200 description MPLS-FACING-PEER
  updatesource Loopback0
  addressfamily l2vpn evpn
!

configure
evpn
 evi 6005
  bgp
   rd 200:50
   route-target import 100:6005
   route-target export 100:6005
!
  advertise-mac


configure
l2vpn
 bridge group 1
  bridge-domain 1-1
   interface GigabitEthernet

    evi 6005
!
```

EVPN ソフトウェア MAC ラーニング

あるデバイス上で学習した MAC アドレスは、VLAN 内の別のデバイス上で学習されるか、配布されるようにする必要があります。EVPN ソフトウェア MAC ラーニング機能では、あるデバイス上で学習された MAC アドレスをネットワークに接続された別のデバイスに配布できます。MAC アドレスは、BGP を使用してリモート デバイスから学習されます。

（注） デバイスには最大 128K の MAC アドレス エントリを含めることができます。デバイス上のブリッジ ドメインには最大 64K の MAC アドレス エントリを含めることができます。

図 *26 : EVPN* ソフトウェア *MAC* ラーニング



上の図は、ソフトウェア MAC ラーニングのプロセスを示しています。次に、このプロセスに関わるステップを示します。

1. トラフィックは、ブリッジ ドメイン内の 1 つのポートに着信します。
2. 送信元 MAC アドレス（AA）は PE 上で学習され、ダイナミック MAC エントリとして格納されます。
3. MAC アドレス（AA）がタイプ 2 BGP ルーtに変換され、BGP を介して同じ EVI 内のすべてのリモート PE に送信されます。
4. MAC アドレス（AA）は、リモート MAC アドレスとして PE で更新されます。

EVPN ソフトウェア MAC ラーニングの設定

次の項では、EVPN ソフトウェア MAC ラーニングの設定方法について説明します。

（注） ルータは、フロー認識型トランスポート（FAT）擬似回線をサポートしていません。

```
/* Configure bridge domain. */

RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group EVPN_SH
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain EVPN_2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface TenGigE
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# exit
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface BundleEther 20.2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# storm-control broadcast pps 10000 ← Enabling
 storm-control is optional
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# exit
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# evi 2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-evi)# commit

/* Configure address family session in BGP. */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router bgp 200
RP/0/RSP0/CPU0:router(config-bgp)# bgp router-id 209.165.200.227
RP/0/RSP0/CPU0:router(config-bgp)# address-family l2vpn evpn

RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 200
```

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# description MPLSFACINGPEER
RP/0/RSP0/CPU0:router(config-bgp-nbr)# update-source Loopback 0
RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family l2vpn evpn
```

EVPN ソフトウェア MAC ラーニングでサポートされているモード

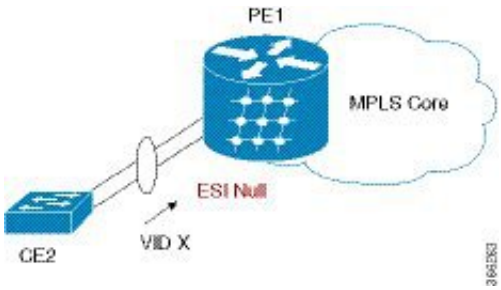
EVPN ソフトウェア MAC ラーニングでサポートされているモードは次のとおりです。

- シングル ホーム デバイス（SHD）またはシングル ホーム ネットワーク（SHN）
- デュアル ホーム デバイス（DHD）：オール アクティブ ロード バランシング

シングル ホーム デバイスまたはシングル ホーム ネットワーク モード

次の項では、EVPN ソフトウェア MAC ラーニング機能をシングル ホーム デバイスまたはシングル ホーム ネットワーク（SHD/SHN）モードで設定する方法について説明します。

図 *27:* シングル ホーム デバイスまたはシングル ホーム ネットワーク モード



上の図では、PE（PE1）はバンドルインターフェイスまたは物理インターフェイスを使用してイーサネット セグメントに接続されています。SHD/SHN にはヌル イーサネット セグメント識別子（ESI）を使用します。

シングル ホーム デバイスまたはシングル ホーム ネットワーク モードでの EVPN の設定

この項では、シングル ホーム デバイスまたはシングル ホーム ネットワーク モードで EVPN ソフトウェア MAC ラーニング機能を設定する方法について説明します。

```
/* Configure bridge domain. */

RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group EVPN_ALL_ACTIVE
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain EVPN_2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface BundleEther1.2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# evi 2001


/* Configure advertisement of MAC routes. */

RP/0/RSP0/CPU0:router(config)# evpn
RP/0/RSP0/CPU0:router(config-evpn)# evi 2001
RP/0/RSP0/CPU0:router(config-evpn-evi)# advertise-mac
```

```
/* Configure address family session in BGP. */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router#(config)# router bgp 200
RP/0/RSP0/CPU0:router#(config-bgp)# bgp router-id 09.165.200.227
RP/0/RSP0/CPU0:router#(config-bgp)# address-family l2vpn evpn
RP/0/RSP0/CPU0:router#(config-bgp)# neighbor 10.10.10.10
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# remote-as 200
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# description MPLSFACING-PEER
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# update-source Loopback 0
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# address-family l2vpn evpn
```

実行コンフィギュレーション

```
l2vpn
bridge group EVPN_ALL_ACTIVE
 bridge-domain EVPN_2001
  interface BundleEther1.2001
  evi 2001
!
evpn
 evi 2001
  advertise-mac
!
router bgp 200 bgp
 router-id 40.40.40.40
 address-family l2vpn evpn
 neighbor 10.10.10.10
  remote-as 200 description MPLS-FACING-PEER
  updatesource Loopback0
  addressfamily l2vpn evpn
```

確認

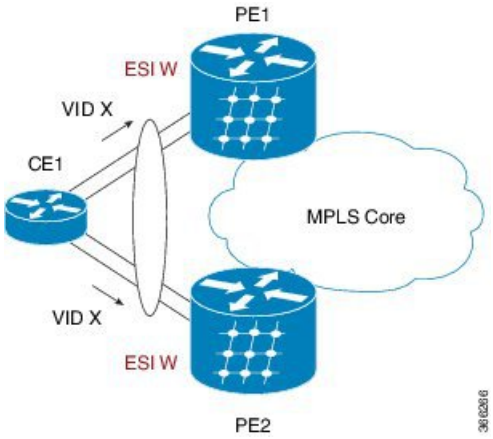
シングル ホーム デバイスの EVPN を確認します。

```
RP/0/RSP0/CPU0:router# show evpn ethernet-segment interface Te0/4/0/10 detail

Ethernet Segment Id    Interface   Nexthops
---------------------  ----------  ----------
N/A                    Te0/4/0/10  20.20.20.20
……
 Topology :
 Operational : SH
 Configured : Single-active (AApS) (default)
```

デュアル ホーム デバイス：オールアクティブ ロード バランシング モード

次の項では、デュアルホームデバイス（DHD）にオールアクティブロードバランシングモードで EVPN ソフトウェア MAC ラーニング機能を設定する方法について説明します。

図 *28 :* デュアル ホーム デバイス：オールアクティブ ロード バランシング モード



オールアクティブ ロード バランシングはフローごとのアクティブ/アクティブ（AApF）と呼ばれています。上の図では、両方の EVPN PE に同一のイーサネット セグメント識別子を使用しています。PE は、バンドル インターフェイスを使用してイーサネット セグメントに接続されています。CE では、単一のバンドルが 2 つの EVPN PE に向けて設定されます。このモードでは、学習した MAC アドレスが PE1 と PE2 の両方に格納されます。PE1 と PE2 は両方とも同じ EVI 内でトラフィックを転送できます。

デュアル ホーム デバイスでの EVPN ソフトウェア MAC ラーニングの設定：オールアクティブ モード

この項では、オールアクティブ モードのデュアル ホーム デバイスで EVPN ソフトウェア MAC ラーニング機能を設定する方法について説明します。

```
/* Configure bridge domain. */

RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group EVPN_ALL_ACTIVE
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain EVPN_2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface BundleEther1.2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# evi 2001


/* Configure advertisement of MAC routes. */

RP/0/RSP0/CPU0:router(config)# evpn
RP/0/RSP0/CPU0:router(config-evpn)# evi 2001
RP/0/RSP0/CPU0:router(config-evpn-evi)# advertise-mac
RP/0/RSP0/CPU0:router(config-evpn-evi)# exit
RP/0/RSP0/CPU0:router(config-evpn)# interface bundle-ether1
RP/0/RSP0/CPU0:router(config-evpn-ac)# ethernet-segment
RP/0/RSP0/CPU0:router(config-evpn-ac-es)# identifier type 0 01.11.00.00.00.00.00.00.01


/* Configure address family session in BGP. */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router#(config)# router bgp 200
RP/0/RSP0/CPU0:router#(config-bgp)# bgp router-id 209.165.200.227
RP/0/RSP0/CPU0:router#(config-bgp)# address-family l2vpn evpn
RP/0/RSP0/CPU0:router#(config-bgp)# neighbor 10.10.10.10
```

```
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# remote-as 200
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# description MPLSFACING-PEER
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# update-source Loopback 0
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# address-family l2vpn evpn


/* Configure Link Aggregation Control Protocol (LACP) bundle. */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether1 300
RP/0/RSP0/CPU0:router(config-if)# lacp switchover suppress-flaps 300
RP/0/RSP0/CPU0:router(config-if)# exit


/* Configure VLAN Header Rewrite.*/

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface bundle-Ether1.2001 l2transport
RP/0/RSP0/CPU0:router(config-if)# encapsulation dot1q 10
RP/0/RSP0/CPU0:router(config-if)# rewrite ingress tag pop 1 symmetric
```

実行コンフィギュレーション

```
l2vpn
bridge group EVPN_ALL_ACTIVE
 bridge-domain EVPN_2001
 interface Bundle-Ether1.2001
 !
 evi 2001
 !
!
evpn
 evi 2001
 !
 advertise-mac
 !
 interface bundle-ether1
  ethernet-segment
  identifier type 0 01.11.00.00.00.00.00.00.01
  !
 !
router bgp 200
bgp router-id  209.165.200.227
address-family l2vpn evpn
!
neighbor 10.10.10.10
 remote-as 200
 description MPLS-FACING-PEER
 update-source Loopback0
 address-family l2vpn evpn
!
interface Bundle-Ether1
lacp switchover suppress-flaps 300
load-interval 30
!
interface bundle-Ether1.2001 l2transport
 encapsulation dot1aq 2001
 rewrite ingress tag pop 1 symmetric
!
```

確認

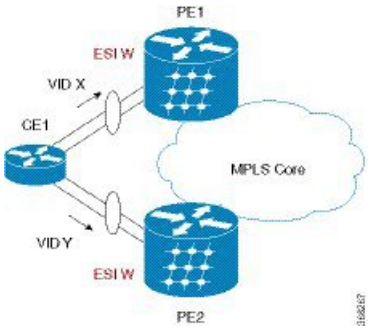
オールアクティブ モードのデュアル ホーム デバイスの EVPN を確認します。

```
RP/0/RSP0/CPU0:router# show evpn ethernet-segment interface bundle-Ether 1 carvin$

Ethernet Segment Id        Interface  Nexthops
-------- ----------        --------   --------
0100.211b.fce5.df00.0b00   BE11       10.10.10.10
 209.165.201.1
Topology :
 Operational : MHN
 Configured : All-active (AApF) (default)
 Primary Services : Auto-selection
 Secondary Services: Auto-selection
 Service Carving Results:
 Forwarders : 4003
 Elected : 2002
 EVI E : 2000, 2002, 36002, 36004, 36006, 36008
 ........
 Not Elected : 2001
 EVI NE : 2001, 36001, 36003, 36005, 36007, 36009

 MAC Flushing mode : Invalid

Peering timer : 3 sec [not running]
 Recovery timer : 30 sec [not running]
 Local SHG label : 34251
 Remote SHG labels : 1
  38216 : nexthop 209.165.201.1
```

デュアル ホーム デバイス：シングルアクティブ ロード バランシング モード

次の項では、デュアル ホーム デバイス（DHD）にシングルアクティブ ロード バランシング モードで EVPN ソフトウェア MAC ラーニング機能を設定する方法について説明します。

図 *29 :* デュアル ホーム デバイス：シングルアクティブ ロード バランシング



また、シングルアクティブ ロードバランシングは、サービスごとのオールアクティブ（AApS）とも呼ばれています。

両方の EVPN PE に同一の ESI が設定されます。CE では、2 つの EVPN PE への個別のバンドルまたは独立した物理インターフェイスが設定されます。このモードでは、学習した MAC アドレスが PE1 と PE2 の両方に格納されます。所定の時間に 1 つの PE のみが EVI 内にトラフィックを転送できます。

ディアル ホーム デバイスでの EVPN ソフトウェア MAC ラーニングの設定：シングルアクティブ モード

この項では、シングルアクティブモードのデュアル ホームでEVPN ソフトウェア MAC ラーニングを設定する方法について説明します。

```
/* Configure bridge domain. */

RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group EVPN_ALL_ACTIVE
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain EVPN_2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface BundleEther1.2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# evi 2001


/* Configure VLAN Header Rewrite (Single-tagged sub-interface).*/

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface bundle-Ether1.21 l2transport
RP/0/RSP0/CPU0:router(config-if)# lacp switchover suppress-flaps 300
RP/0/RSP0/CPU0:router(config-if)# exit
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether1.2001 l2transport
RP/0/RSP0/CPU0:router(config-if)# encapsulation dot1q 10
RP/0/RSP0/CPU0:router(config-if)# rewrite ingress tag pop 1 symmetric


/* Configure advertisement of MAC routes. */

RP/0/RSP0/CPU0:router(config)# evpn
RP/0/RSP0/CPU0:router(config-evpn)# evi 2001
RP/0/RSP0/CPU0:router(config-evpn-evi)# advertise-mac


/* Configure load balancing. */

RP/0/RSP0/CPU0:router(config)# evpn
RP/0/RSP0/CPU0:router(config-evpn)# evi 2001
RP/0/RSP0/CPU0:router(config-evpn-evi)# advertise-mac
RP/0/RSP0/CPU0:router(config-evpn-evi)# exit
RP/0/RSP0/CPU0:router(config-evpn)# interface bundle-ether1
RP/0/RSP0/CPU0:router(config-evpn)# ethernet-segment
RP/0/RSP0/CPU0:router(config-evpn-es)# load-balancing-mode single-active
RP/0/RSP0/CPU0:router(config-evpn-es)# identifier type 0 12.12.00.00.00.00.00.00.02
RP/0/RSP0/CPU0:router(config-evpn-es)# bgp route-target 1212.0000.0002


/* Configure address family session in BGP. */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router#(config)# router bgp 200
RP/0/RSP0/CPU0:router#(config-bgp)# bgp router-id 209.165.200.227
RP/0/RSP0/CPU0:router#(config-bgp)# address-family l2vpn evpn
RP/0/RSP0/CPU0:router#(config-bgp)# neighbor 10.10.10.10
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# remote-as 200
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# description MPLSFACING-PEER
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# update-source Loopback 0
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# address-family l2vpn evpn
```

確認

シングルアクティブ モードのデュアル ホーム デバイスの EPVN を確認します。

```
RP/0/RSP0/CPU0:router# show evpn ethernet-segment int bundleEther 21 carving detail

...
Ethernet Segment Id       Interface          Nexthops
----- ------------------  ----------         -----------
0012.1200.0000.0000.0002  BE21               10.10.10.10  209.165.201.1

ESI type : 0
 Value : 12.1200.0000.0000.0002
 ES Import RT : 1212.0000.0000 (from ESI)

Source MAC : 0000.0000.0000 (N/A)
Topology :
 Operational : MHN
 Configured : Single-active (AApS)
 Primary Services : Auto-selection
 Secondary Services: Auto-selection

 Service Carving Results:
 Forwarders : 2
 Elected : 1
 EVI E : 500
 Not Elected : 1
 EVI NE : 501
```

EVPN ソフトウェア MAC ラーニングの確認

パケット ドロップ統計情報を確認します。

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain bd-name EVPN_2001 details

Bridge group: EVPN_ALL_ACTIVE, bridge-domain: EVPN_2001, id: 1110,
state: up, ShgId: 0, MSTi: 0
 List of EVPNs:
 EVPN, state: up
 evi: 2001
 XC ID 0x80000458
 Statistics:
 packets: received 28907734874 (unicast 9697466652), sent
76882059953
 bytes: received 5550285095808 (unicast 1861913597184), sent
14799781851396
 MAC move: 0
 List of ACs:
 AC: TenGigE, state is up
 Type VLAN; Num Ranges: 1
...
 Statistics:
 packets: received 0 (multicast 0, broadcast 0, unknown
unicast 0, unicast 0), sent 45573594908
 bytes: received 0 (multicast 0, broadcast 0, unknown unicast
0, unicast 0), sent 8750130222336
 MAC move: 0
 ........
```

VPN-ID と MAC アドレス フィルタを使用して EVPN ID を確認します。

```
RP/0/RSP0/CPU0:router# show evpn evi vpn-id 2001 neighbor

Neighbor IP    vpn-id
```

```
-----------   --------
209.165.200.225   2001
209.165.201.30   2001
```

BGP L2VPN EVPN の概要を確認します。

```
RP/0/RSP0/CPU0:router# show bgp l2vpn evpn summary
...
Neighbor        Spk   AS      MsgRcvd  MsgSent   TblVer    InQ  OutQ  Up/Down   St/PfxRcd
209.165.200.225  0    200      216739  229871   200781341  0    0     3d00h    348032
209.165.201.30   0    200     6462962 4208831   200781341  10   0     2d22h    35750
```

ライン カードの L2FIB テーブルへの MAC の更新を確認します。

```
RP/0/RSP0/CPU0:router# show l2vpn mac mac all location 0/6/cPU0

Topo ID Producer Next Hop(s)     Mac Address    IP Address
------- -------- -----------     -------------- ----------
1112    0/6/CPU0 Te 00a3.0001.0001
```

ルート スイッチ プロセッサ（RSP）の L2FIB テーブルへの MAC の更新を確認します。

```
RP/0/RSP0/CPU0:router# show l2vpn mac mac all location 0/6/cPU0

Topo ID  Producer Next Hop(s)     Mac Address    IP Address
-------  -------- -----------     -------------- ----------
1112     0/6/CPU0  00a3.0001.0001
```

MAC アドレスの概要情報を確認します。

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain EVPN_ALL_ACTIVE:EVPN_2001
mac-address location 0/6/CPU0

.....
Mac Address     Type      Learned from/Filtered on   LC learned   Resync Age/Last Change
Mapped to
0000.2001.5555  dynamic   Te           N/A          11 Jan 14:37:22
N/A <-- local dynamic
00bb.2001.0001 dynamic    Te           N/A          11 Jan 14:37:22
N/A
0000.2001.1111 EVPN       BD id: 1110                N/A          N/A
N/A <-- remote static
00a9.2002.0001 EVPN       BD id: 1110                N/A          N/A
N/A
```

VPN-ID と MAC アドレス フィルタを使用して EVPN ID を確認します。

```
RP/0/RSP0/CPU0:router# show evpn evi vpn-id 2001 mac

EVI    MAC address     IP address        Nexthop      Label
----   -------------   -----------       -------      ------
2001   00a9.2002.0001  ::                10.10.10.10  34226      <-- Remote MAC
2001   00a9.2002.0001  ::                209.165.201.30  34202

2001   0000.2001.5555  20.1.5.55         TenGigE 34203    <-- local MAC
```

```
RP/0/RSP0/CPU0:router# RP/0/RSP0/CPU0:router# show evpn evi vpn-id 2001 mac 00a9.2002.0001
 detail

EVI     MAC address      IP address  Nexthop      Label
----    --------------   ----------  -------      -----
2001    00a9.2002.0001   ::          10.10.10.10  34226

2001    00a9.2002.0001   ::          209.165.201.30  34202

 Ethernet Tag : 0
 Multi-paths Resolved : True <--- aliasing to two remote PE with All-Active load balancing


 Static : No
 Local Ethernet Segment : N/A
 Remote Ethernet Segment : 0100.211b.fce5.df00.0b00
 Local Sequence Number : N/A
 Remote Sequence Number : 0
 Local Encapsulation : N/A
 Remote Encapsulation : MPLS
```

EVPNに関連付けられているBGPルートをブリッジドメインフィルタを使用して確認します。

```
RP/0/RSP0/CPU0:router# show bgp l2vpn evpn bridge-domain EVPN_2001 route-type 2

*> [2][0][48][00bb.2001.0001][0]/104
                         0.0.0.0             0 i <------ locally learnt MAC
*>i[2][0][48][00a9.2002.00be][0]/104
                         10.10.10.10 100     0 i <----- remotely learnt MAC
* i 209.165.201.30 100 0 i
```

EVPN アウト オブ サービス

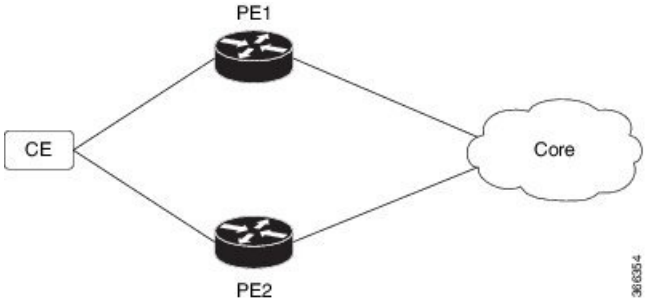
EVPN アウト オブ サービス機能では、Link Aggregation Control Protocol（LACP）を設定したイーサネット セグメントに含まれているバンドル インターフェイスの状態を制御することができます。この機能を使用すると、ノードをアウト オブ サービス（OOS）に移行させることができます。プロバイダー エッジ（PE）のすべてのバンドルを手動でシャットダウンする必要はありません。

cost-out コマンドを使用してノード上のイーサネット VPN（EVPN）のイーサネット セグメントに属するすべてのバンドル インターフェイスをダウンさせます。イーサネット A-D のイーサネット セグメント（ES EAD）ルートは、バンドルをシャット ダウンする前に撤回されます。PE は接続されているカスタマーエッジ（CE）デバイスにシグナリングし、対応するバンドル メンバーをダウンさせます。こうすることで、トラフィックを中断させることなく、トラフィックをこの PE ノードからそらします。CE からイーサネット セグメントへのトラフィックは、マルチホーミング環境内のピア PE へと方向付けられます。

（注） EVPN のコストアウトは、手動で設定された ESI でのみサポートされます。

次に、CE が PE1 と PE2 に接続されているトポロジを示します。PE1 に cost-out コマンドを設定すると、イーサネットセグメント上のすべてのバンドルインターフェイスがダウンします。また、CE 上の対応するバンドル メンバーもダウンします。したがって、このイーサネット セグメントのトラフィックは CE から PE2 へと送信されるようになります。

図 *30 : EVPN* アウト オブ サービス



ノードをサービス状態に戻すには、no cost-out コマンドを使用します。これにより、PE 上の EPVN イーサネット セグメントに属するすべてのバンドル インターフェイスと CE 上の対応するバンドル メンバーが起動します。

ノードがコストアウト状態にある場合に新しいバンドル イーサネット セグメントを追加するとそのバンドルがダウンします。同様に、バンドル イーサネット セグメントを削除するとそのバンドルは起動します。

リロード時に指定した時間が経過した後にノードをサービス状態に戻すには、startup-cost-in コマンドを使用します。EPVN が初期化された時点でノードがコストアウトになり、設定時間までコストアウト状態が維持されます。タイマー実行中に evpn no startup-cost-in コマンドを実行すると、タイマーが停止し、ノードがコストイン状態になります。

「cost-out」設定は「startup-cost-in」タイマーよりも常に優先されます。そのため、両方の設定でリロードすると、コストアウト状態は「cost-out」設定で制御されます。タイマーは関係ありません。同様に、起動タイマーでリロードし、タイマーが実行している間に「cost-out」を設定するとタイマーが停止し、OOS 状態は「cost-out」設定のみで制御されます。

startup-cost-in timer が実行している間に何らかのプロシージャを実行すると、ノードはコストアウト状態を維持し、タイマーが再起動します。

EVPN アウト オブ サービスの設定

この項では、EVPN アウト オブ サービスを設定する方法について説明します。

```
/* Configuring node cost-out on a PE */

Router# configure
Router(config)# evpn
Router(config-evpn)# cost-out
Router(config-evpn)commit

/* Bringing up the node into service */

Router# configure
```

```
Router(config)# evpn
Router(config-evpn)# no cost-out
Router(config-evpn)commit

/* Configuring the timer to bring up the node into service after the specified time on
reload */

Router# configure
Router(config)# evpn
Router(config-evpn)# startup-cost-in 6000
Router(config-evpn)commit
```

実行コンフィギュレーション

```
configure
evpn
 cost-out
!

configure
evpn
 startup-cost-in 6000
!
```

確認

EVPN アウト オブ サービスの設定を確認します。

```
/* Verify the node cost-out configuration */

Router# show evpn summary
Fri Apr  7 07:45:22.311 IST
Global Information
----------------------------
Number of EVIs                : 2
Number of Local EAD Entries   : 0
Number of Remote EAD Entries  : 0
Number of Local MAC Routes    : 0
Number of Local MAC Routes    : 5
          MAC                 : 5
          MAC-IPv4            : 0
          MAC-IPv6            : 0
Number of Local ES:Global MAC : 12
Number of Remote MAC Routes   : 7
          MAC                 : 7
          MAC-IPv4            : 0
          MAC-IPv6            : 0
Number of Local IMCAST Routes : 56
Number of Remote IMCAST Routes: 56
Number of Internal Labels     : 5
Number of ES Entries          : 9
Number of Neighbor Entries    : 1
EVPN Router ID                : 192.168.0.1
BGP Router ID                 : ::
BGP ASN                       : 100
PBB BSA MAC address           : 0207.1fee.be00
Global peering timer          :      3 seconds
Global recovery timer         :     30 seconds
EVPN cost-out                 : TRUE
      startup-cost-in timer   : Not configured
```

```
/* Verify the no cost-out configuration */

Router# show evpn summary
Fri Apr  7 07:45:22.311 IST
Global Information
----------------------------
Number of EVIs                : 2
Number of Local EAD Entries   : 0
Number of Remote EAD Entries  : 0
Number of Local MAC Routes    : 0
Number of Local MAC Routes    : 5
          MAC                 : 5
          MAC-IPv4            : 0
          MAC-IPv6            : 0
Number of Local ES:Global MAC : 12
Number of Remote MAC Routes   : 7
          MAC                 : 7
          MAC-IPv4            : 0
          MAC-IPv6            : 0
Number of Local IMCAST Routes : 56
Number of Remote IMCAST Routes: 56
Number of Internal Labels     : 5
Number of ES Entries          : 9
Number of Neighbor Entries    : 1
EVPN Router ID                : 192.168.0.1
BGP Router ID                 : ::
BGP ASN                       : 100
PBB BSA MAC address           : 0207.1fee.be00
Global peering timer          :      3 seconds
Global recovery timer         :     30 seconds
EVPN cost-out                 : FALSE
      startup-cost-in timer   : Not configured


/* Verify the startup-cost-in timer configuration */

Router# show evpn summary
Fri Apr  7 07:45:22.311 IST
Global Information
----------------------------
Number of EVIs                : 2
Number of Local EAD Entries   : 0
Number of Remote EAD Entries  : 0
Number of Local MAC Routes    : 0
Number of Local MAC Routes    : 5
          MAC                 : 5
          MAC-IPv4            : 0
          MAC-IPv6            : 0
Number of Local ES:Global MAC : 12
Number of Remote MAC Routes   : 7
          MAC                 : 7
          MAC-IPv4            : 0
          MAC-IPv6            : 0
Number of Local IMCAST Routes : 56
Number of Remote IMCAST Routes: 56
Number of Internal Labels     : 5
Number of ES Entries          : 9
Number of Neighbor Entries    : 1
EVPN Router ID                : 192.168.0.1
BGP Router ID                 : ::
BGP ASN                       : 100
PBB BSA MAC address           : 0207.1fee.be00
```

```
Global peering timer          :      3 seconds
Global recovery timer         :     30 seconds
EVPN node cost-out            : TRUE
        startup-cost-in timer : 6000
```

EVPN 対応 CFM のサポート

イーサネット接続障害管理（CFM）はサービス レベル OAM プロトコルの 1 つで、VLAN ごとにエンドツーエンドのイーサネット サービスをモニタリングおよびトラブルシューティングするためのツールとなります。これには、予防的な接続モニタリング、障害検証、および障害分離の機能が含まれています。CFM は EVPN ネットワークに導入できます。EVPN ネットワークで CFM を使用して、ノード間の接続をモニタできます。

制約事項

EVPN 対応 CFM は、次の制限の下でサポートされています。

- アクティブ-アクティブ マルチホーミングのシナリオでは、マルチホーム CE デバイスとそれらに接続している PE デバイスとの間の接続をモニタする場合、CFM は CE と PE 間の個別のリンク間でのみ使用できます。CE デバイスと PE デバイス間のバンドルで CFM の使用を試みると、シーケンス番号エラーが発生し、統計情報が不正確になります。
- ループバックおよびリンクトレースの結果に副作用が生じる可能性があります。ループバックまたはリンクトレースのいずれかで同じインスタンスに対して複数の結果が報告されたり、同じ 2 つのエンドポイント間にあるループバックとリンクトレースの連続するインスタンスで異なる結果が生じたりする場合があります。

イーサネット セグメント単位の EVPN 複数サービス

イーサネット セグメント単位の EVPN 複数サービス機能を使用すると、単一のイーサネット セグメント（ES）で複数のサービスを設定できます。複数の ES で複数のサービスを設定する代わりに、1 つの ES で複数のサービスを設定できます。

単一のイーサネット バンドルで次のサービスを設定できます。サブインターフェイスごとにサービスを 1 つずつ設定できます。

- フレキシブル クロスコネクト（FXC） サービス。VLAN 非認識型、VLAN 認識型、およびローカル スイッチング モードをサポートしています。

  詳細については、『*L2VPN and Ethernet Services Configuration Guide for Cisco NCS 540 Series Routers*』の「*Configure Point-to-Point Layer 2 Services*」の章を参照してください。

- EVPN-VPWS Xconnect サービス

  詳細については、『*L2VPN and Ethernet Services Configuration Guide for Cisco NCS 540 Series Routers*』の「*EVPN Virtual Private Wire Service (VPWS)*」の章を参照してください。

- EVPN Integrated Routing and Bridging（IRB）

詳細については、『*L2VPN and Ethernet Services Configuration Guide for Cisco NCS 540 Series Routers*』の「*Configure EVPN IRB*」の章を参照してください。

- ネイティブ EVPN

  詳細については、『*L2VPN and Ethernet Services Configuration Guide for Cisco NCS 540 Series Routers*』の「*EVPN Features*」の章を参照してください。

これらのサービスはすべて、オールアクティブのマルチホーミングのシナリオでのみサポートされます。

イーサネット セグメント単位の EVPN 複数サービスの設定

イーサネット バンドル インターフェイス 22001 を介して 2 つのプロバイダー エッジ（PE）デバイスに接続しているカスタマー エッジ（CE）デバイスを考えてみます。バンドル イーサネット サブインターフェイスで複数のサービスを設定します。

設定例

Bundle-Ether22001 ES を考慮し、サブインターフェイスで複数のサービスを設定します。

```
/* Configure attachment circuits */
Router# configure
Router(config)# interface Bundle-Ether22001.12 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 12
Router(config-l2vpn-subif)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether22001.13 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 13
Router(config-l2vpn-subif)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether22001.14 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 14
Router(config-l2vpn-subif)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether22001.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 1
Router(config-l2vpn-subif)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether22001.2 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 2
Router(config-l2vpn-subif)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether22001.3 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 3
Router(config-l2vpn-subif)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether22001.4 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 4
Router(config-l2vpn-subif)# exit
Router(config-l2vpn)# exit

/*Configure VLAN Unaware FXC Service */
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-unaware fxc_mh1
Router(config-l2vpn-fxs-vu)# interface Bundle-Ether22001.1
```

```
Router(config-l2vpn-fxs-vu)# interface Bundle-Ether22001.2
Router(config-l2vpn-fxs-vu)# interface Bundle-Ether22001.3
Router(config-l2vpn-fxs-vu)# neighbor evpn evi 21006 target 22016
Router(config-l2vpn-fxs-vu)# commit

/* Configure VLAN Aware FXC Service */
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-aware evi 24001
Router(config-l2vpn-fxs-vu)# interface Bundle-Ether22001.12
Router(config-l2vpn-fxs-vu)# interface Bundle-Ether22001.13
Router(config-l2vpn-fxs-vu)# interface Bundle-Ether22001.14
Router(config-l2vpn-fxs-vu)# commit

/* Configure Local Switching - Local switching is supported only on VLAN-aware FXC */
PE1
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-aware evi 31400
Router(config-l2vpn-fxs)# interface Bundle-Ether22001.1400
Router(config-l2vpn-fxs)# interface Bundle-Ether23001.1400
Router(config-l2vpn-fxs)# commit
Router(config-l2vpn-fxs)# exit
PE2
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-aware evi 31401
Router(config-l2vpn-fxs)# interface Bundle-Ether22001.1401
Router(config-l2vpn-fxs)# interface Bundle-Ether23001.1401
Router(config-l2vpn-fxs)# commit
Router(config-l2vpn-fxs)# exit

/* Configure EVPN-VPWS xconnect service and native EVPN with IRB */

Router# configure
Router(config)# interface Bundle-Ether22001.11 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 11
Router(config-l2vpn-subif)# rewrite ingress tag pop 2 symmetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit

Router# configure
Router(config)# interface Bundle-Ether22001.21 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q  21
Router(config-l2vpn-subif)# rewrite ingress tag pop 2 symmetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit

Router# configure
Route(config)# l2vpn
Router(config-l2vpn)# xconnect group xg22001
Router(config-l2vpn-xc)# p2p evpn-vpws-mclag-22001
Router(config-l2vpn-xc-p2p)# interface Bundle-Ether22001.11
Router(config-l2vpn-xc-p2p)# neighbor evpn evi 22101 target 220101 source 220301
Router(config-l2vpn-xc-p2p)# commit
Router(config-l2vpn-xc-p2p)# exit

Router # configure
Router (config)# l2vpn
Router (config-l2vpn)# bridge group native_evpn1
Router (config-l2vpn-bg)#  bridge-domain bd21
Router (config-l2vpn-bg-bd)# interface Bundle-Ether22001.21
Router (config-l2vpn-bg-bd-ac)# routed interface BVI21
Router (config-l2vpn-bg-bd-bvi)# evi 22021
```

```
Router (config-l2vpn-bg-bd-bvi)# commit
Router (config-l2vpn-bg-bd-bvi)# exit

/* Configure Native EVPN */
Router # configure
Router (config)# evpn
Router (config-evpn)# interface Bundle-Ether22001
Router (config-evpn-ac)# ethernet-segment identifier type 0 ff.ff.ff.ff.ff.ff.ff.ff.ee
Router (config-evpn-ac-es)# bgp route-target 2200.0001.0001
Router (config-evpn-ac-es)# exit
Router (config-evpn)# evi 24001
Router (config-evpn-evi)# bgp
Router (config-evpn-evi-bgp)# route-target import 64:24001
Router (config-evpn-evi-bgp)# route-target export 64:24001
Router (config-evpn-evi-bgp)# exit
Router (config-evpn-evi)# exit
Router (config-evpn)# evi 21006
Router (config-evpn-evi)# bgp
Router (config-evpn-evi-bgp)# route-target route-target 64:10000
Router (config-evpn-evi-bgp)# exit
Router (config-evpn-evi)# exit
Router (config-evpn)# evi 22101
Router (config-evpn-evi)# bgp
Router (config-evpn-evi-bgp)# route-target import 64:22101
Router (config-evpn-evi-bgp)# route-target export 64:22101
Router (config-evpn-evi-bgp)# exit
Router (config-evpn-evi)# exit
Router (config-evpn)# evi 22021
Router (config-evpn-evi)# bgp
Router (config-evpn-evi-bgp)# route-target import 64: 22021
Router (config-evpn-evi-bgp)# route-target export 64: 22021
Router (config-evpn-evi-bgp)# exit
Router (config-evpn-evi)# exit
Router (config-evpn-evi)# advertise-mac
Router (config-evpn-evi)# exit
Router (config-evpn)# evi 22022
Router (config-evpn-evi)# bgp
Router (config-evpn-evi-bgp)# route-target import 64: 22022
Router (config-evpn-evi-bgp)# route-target export 64: 22022
Router (config-evpn-evi-bgp)# exit
Router (config-evpn-evi)# advertise-mac
Router (config-evpn-evi)# commit
Router (config-evpn-evi)# exit
```

実行コンフィギュレーション

```
/* Configure attachment circuits */
interface Bundle-Ether22001.12 l2transport
encapsulation dot1q 1 second-dot1q 12
!
interface Bundle-Ether22001.13 l2transport
encapsulation dot1q 1 second-dot1q 13
!
interface Bundle-Ether22001.14 l2transport
encapsulation dot1q 1 second-dot1q 14
!
interface Bundle-Ether22001.1 l2transport
 encapsulation dot1q 1 second-dot1q 1
!
interface Bundle-Ether22001.2 l2transport
```

```
encapsulation dot1q 1 second-dot1q 2
!
interface Bundle-Ether22001.3 l2transport
encapsulation dot1q 1 second-dot1q 3
!
interface Bundle-Ether22001.4 l2transport
encapsulation dot1q 1 second-dot1q 4

/*Configure VLAN Unaware FXC Service */
flexible-xconnect-service vlan-unaware fxc_mh1
  interface Bundle-Ether22001.1
  interface Bundle-Ether22001.2
  interface Bundle-Ether22001.3
 neighbor evpn evi 21006 target 22016
!
/*Configure VLAN Aware FXC Service */
l2vpn
 flexible-xconnect-service vlan-aware evi 24001
   interface Bundle-Ether22001.12
   interface Bundle-Ether22001.13
   interface Bundle-Ether22001.14

/* Configure Local Switching */
flexible-xconnect-service vlan-aware evi 31400
 interface Bundle-Ether22001.1400
 interface Bundle-Ether23001.1400
!
flexible-xconnect-service vlan-aware evi 31401
 interface Bundle-Ether22001.1401
 interface Bundle-Ether23001.1401
!

/* Configure EVPN-VPWS xconnect service and native EVPN with IRB */
interface Bundle-Ether22001.11 l2transport
  encapsulation dot1q 1 second-dot1q 11
  rewrite ingress tag pop 2 symmetric
 !
interface Bundle-Ether22001.21 l2transport
  encapsulation dot1q 1 second-dot1q  21
  rewrite ingress tag pop 2 symmetric
 !
!
l2vpn
xconnect group xg22001
p2p evpn-vpws-mclag-22001
 interface Bundle-Ether22001.11
 neighbor evpn evi 22101 target 220101 source 220301
!
bridge group native_evpn1
   bridge-domain bd21
   interface Bundle-Ether22001.21
    routed interface BVI21
     evi 22021
  !
/* Configure Native EVPN */
Evpn
 interface Bundle-Ether22001
  ethernet-segment   identifier type 0 ff.ff.ff.ff.ff.ff.ff.ff.ee
  bgp route-target 2200.0001.0001
  !
  evi 24001
   bgp
    route-target import 64:24001
    route-target export 64:24001
```

```
 !
 evi 21006
  bgp
    route-target 64:100006
 !
  evi 22101
   bgp
     route-target import 64:22101
     route-target export 64:22101
    !
 evi 22021
  bgp
    route-target import 64:22021
    route-target export 64:22021
  !
  advertise-mac
!
evi 22022
 bgp
  route-target import 64:22022
  route-target export 64:22022
 !
  advertise-mac
!
```

確認

各サービスがサブインターフェイスで設定されているかどうかを確認します。

```
Router# show l2vpn xconnect summary
Number of groups: 6
Number of xconnects: 505  Up: 505  Down: 0  Unresolved: 0 Partially-programmed: 0
AC-PW: 505  AC-AC: 0  PW-PW: 0 Monitor-Session-PW: 0
Number of Admin Down segments: 0
Number of MP2MP xconnects: 0
 Up 0 Down 0
Advertised: 0 Non-Advertised: 0


Router# show l2vpn xconnect-service summary
Number of flexible xconnect services: 74
 Up: 74

Router# show l2vpn flexible-xconnect-service name fxc_mh1
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed
Flexible XConnect Service  Segment
Name    ST  Type  Description  ST
----------------------- ----------------------------- -----------------------------
fxc_mh1 UP  AC:   BE22001.1    UP
            AC:   BE22001.2    UP
            AC:   BE22001.3    UP
-------------------------------------------------------------------------------------

Router# show l2vpn flexible-xconnect-service evi 24001
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed
Flexible XConnect Service  Segment
Name      ST  Type  Description  ST
----------------------- ----------------------------- -----------------------------
evi:24001 UP  AC:   BE22001.11    UP
              AC:   BE22001.12    UP
              AC:   BE22001.13    UP
```

```
              AC:   BE22001.14    UP
------------------------------------------------------------------------------------------


Router# show l2vpn xconnect group xg22001 xc-name evpn-vpws-mclag-22001
Fri Sep 1 17:28:58.259 UTC
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
----------------------- ----------------------------- ----------------------------------
xg22001  evpn-vpws-mclag-22001   UP    BE22001.101  UP      EVPN 22101, 220101,64.1.1.6
 UP
------------------------------------------------------------------------------------------
```

関連コマンド

- evpn
- evi
- ethernet-segment
- advertise-mac
- show evpn ethernet-segment
- show evpn evi
- show evpn summary
- show l2vpn xconnect summary
- show l2vpn flexible-xconnect-service
- show l2vpn xconnect group

EVPN MPLS と VPLS のシームレスな統合

EVPN MPLS と VPLS のシームレスな統合により、同じ VPN インスタンスに対して EVPN と VPLS を実行する PE ノードの共存が可能になります。VPLS またはレガシー ネットワークを、サービスの中断なしで次世代の EVPN ネットワークにアップグレードできます。選択したすべての VPLS プロバイダーエッジ（PE）ノードに、EVPN サービスを同時に導入できます。ただし、トラフィックの中断を回避するため、既存の VPLS 対応 PE で EVPN サービスを 1 つずつプロビジョニングします。

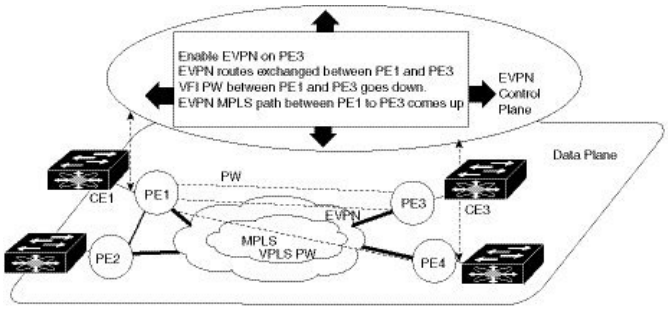
シームレスな統合による VPLS ネットワークの EVPN ネットワークへの移行

EVPN ネットワークでは、VPN インスタンスは EVPN インスタンス ID（EVI）によって識別されます。他の L2VPN テクノロジーと同様に、EVPN インスタンスもルートターゲットおよび

ルート識別子に関連付けられています。MAC をデータ プレーンで学習する（「フラッディングと学習の技術」を使用して学習する）従来の VPLS とは異なり、EVPN ではコントロール プレーンを使用して MAC を学習し伝播します。EVPN では、MAC ルートは MP BGP プロトコルによって伝送されます。EVPN 対応 PE では、PE のルート ターゲット（RT）が一致した場合にのみ、PE が MAC ルートをラベルとともにそれぞれの EVPN 転送テーブルにインポートします。EVPN PE ルータは、同じ VPN インスタンスで VPLS および EVPN L2 ブリッジングを実行する機能を備えています。EVPN と BGP-AD PW の両方が VPN インスタンスで設定されている場合、EVPN PE は、BGP VPLS 自動検出（AD）ルートと、BGP EVPN 包括マルチキャスト ルート（タイプ 3）を、特定の VPN インスタンスにアドバタイズします。ルート タイプ 3 は入力複製マルチキャスト ルートと呼ばれ、ブロードキャスト、未知のユニキャスト、およびマルチキャスト（BUM）トラフィックの送信に使用されます。その他のリモート PE は、送信側の PE RT が設定済みの RT と一致する場合にのみ、同じ VPN インスタンスに対してタイプ 3 ルートをインポートします。したがって、これらのルート交換の最後に、EVPN 対応 PE は、VPN インスタンスにある他のすべての PE とそれらの関連機能を検出します。PE が自身の BUM トラフィックを他の PE に送信するために使用するタイプ 3 ルートでは、同じ RT を持つ PE が BUM トラフィックを受信することが保証されます。EVPN は、タイプ 2 ルートを使用してカスタマー MAC アドレスをアドバタイズします。

EVPN MPLS と VPLS のシームレスな統合により、ネットワーク サービスを中断することなく、VPLS PE ルータを EVPN に 1 つずつアップグレードすることができます。PE1、PE2、PE3、および PE4 が VPLS PW を使用してフルメッシュ ネットワークで相互接続されている次のトポロジを考えてみます。

図 *31 : EVPN MPLS* と *VPLS* のシームレスな統合



EVPN サービスは、一度に 1 つの PE ノードずつ、ネットワークに導入できます。VPLS サービスの VPN インスタンスで EVPN を有効にすることによって、VPLS から EVPN への移行が PE1 で開始されます。EVPN が有効になるとすぐに、PE1 は他の PE ノードへの EVPN 包括マルチキャスト ルートのアドバタイズを開始します。PE1 は他の PE ノードからの包含マルチキャスト ルートを受信しないため、PE1 と他の PE ノード間の VPLS 擬似回線はアクティブなままです。PE1 は、VPLS 疑似回線を使用してトラフィックの転送を維持します。同時に、PE1 は EVPN ルート タイプ 2 を使用して CE1 から学習したすべての MAC アドレスをアドバタイズします。2 番目のステップでは、EVPN が PE3 で有効になっています。PE3 は、他の PE ノードへの包含マルチキャスト ルートのアドバタイズを開始します。PE1 と PE3 の両方が EVPN ルートを介して互いを検出します。その結果、PE1 と PE3 は両者間の擬似回線をシャットダウンします。EVPN サービスが、PE1 と PE3 の間で VPLS サービスの代わりとなります。この段階では、PE1 は PE2 と PE4 を使用して VPLS サービスを実行し続け、同じ VPN インスタンスで

PE3 を使用して EVPN サービスを開始します。このことを、EVPN と VPLS のシームレスな統合と呼びます。VPLS から EVPN への移行は残りの PE ノードに対して続けられます。最終的に、4 つすべての PE ノードが EVPN サービスで有効になります。VPLS サービスがネットワーク内の EVPN サービスに完全に置き換えられます。すべての VPLS 擬似回線がシャットダウンされます。

既存の VPLS ネットワークでの EVPN の設定

既存の VPLS ネットワークで EVPN を設定するには、次の作業を実行します。

- L2VPN EVPN アドレスファミリの設定
- EVPN コンフィギュレーション モードで、EVI と対応する BGP ルートターゲットを設定します。
- ブリッジドメインでの EVI の設定

さまざまな VPLS ベース ネットワークを EVPN に移行する方法については、L2VPN ブリッジドメインでの EVI の設定 （202 ページ）を参照してください。

L2 EVPN アドレスファミリの設定

BGP と参加ネイバーの両方で EVPN アドレス ファミリを有効にするには、次の作業を実行します。

設定例

```
Router# configure
Router(config)#router bgp 65530
Router(config-bgp)#nsr
Router(config-bgp)#bgp graceful-restart
Router(config-bgp)#bgp router-id 200.0.1.1
Router(config-bgp)#address-family l2vpn evpn
Router(config-bgp-af)#exit
Router(config-bgp)#neighbor 200.0.4.1
Router(config-bgp-nbr)#remote-as 65530
Router(config-bgp-nbr)#update-source Loopback0
Router(config-bgp-nbr)#address-family l2vpn evpn
Router(config-bgp-nbr-af)#commit
```

実行コンフィギュレーション

```
configure
 router bgp 65530
  nsr
  bgp graceful-restart
  bgp router-id 200.0.1.1
  address-family l2vpn evpn
  !
  neighbor 200.0.4.1
   remote-as 65530
```

```
  update-source Loopback0
  address-family l2vpn evpn
  !
!
```

EVPN コンフィギュレーション モードでの EVI と対応する BGP ルート ターゲットの設定

EVI を設定し、対応する BGP ルート ターゲットを定義するには、次の作業を実行します。また、advertise-mac を設定します。設定しないと MAC ルート（タイプ 2）がアドバタイズされません。

設定例

```
Router# configure
Router(config)#evpn
Router(config-evpn)#evi i
Router(config-evpn-evi-bgp)#bgp
Router(config-evpn-evi-bgp)#table-policy spp-basic-6
Router(config-evpn-evi-bgp)#route-target import 100:6005
Router(config-evpn-evi-bgp)#route-target export 100:6005
Router(config-evpn-evi-bgp)#exit
Router(config-evpn-evi)#advertise-mac
Router(config-evpn-evi)#commit
```

実行コンフィギュレーション

```
configure
 evpn
  evi
   bgp
    table-policy spp-basic-6
    route-target import 100:6005
    route-target export 100:6005
    !
   advertise-mac
   !
  !
 !
```

ブリッジ ドメインでの EVI の設定

対応する L2VPN ブリッジ ドメインで EVI を設定するには、次の作業を実行します。

設定例

```
Router# configure
Router(config)#l2vpn
Router(config-l2vpn)#bridge group bg1
Router(config-l2vpn-bg)#bridge-domain bd1
Router(config-l2vpn-bg-bd)#interface GigabitEthernet
Router(config-l2vpn-bg-bd-ac)#exit
```

```
Router(config-l2vpn-bg-bd)#evi 1
Router(config-l2vpn-bg-bd-evi)#exit
Router(config-l2vpn-bg-bd)#vfi v1
Router(config-l2vpn-bg-bd-vfi)#neighbor 10.1.1.2 pw-id 1000
Router(config-l2vpn-bg-bd-vfi-pw)#mpls static label local 20001 remote 10001
Router(config-l2vpn-bg-bd-vfi-pw)#commit
```

実行コンフィギュレーション

```
configure
 l2vpn
  bridge group bg1
   bridge-domain bd1
    interface GigabitEthernet
    !
    evi 1
    !
   vfi v1
    neighbor 10.1.1.2 pw-id 1000
     mpls static label local 20001 remote 10001
     !
    !
    evi 1
 !
```

L2VPN ブリッジ ドメインでの EVI の設定

次の例は、さまざまな VPLS ベース ネットワークの L2VPN ブリッジドメインでの EVI 設定を示しています。

MPLS スタティック ラベルをベースとする VPLS

```
l2vpn
 bridge group bg1
  bridge-domain bd-1-1
   interface GigabitEthernet
   !
   vfi vfi-1-1
    neighbor 200.0.2.1 pw-id 1200001
     mpls static label local 20001 remote 10001
    !
    neighbor 200.0.3.1 pw-id 1300001
     mpls static label local 30001 remote 10001
    !
    neighbor 200.0.4.1 pw-id 1400001
     mpls static label local 40001 remote 10001
    !
  !
  evi 1
!
```

自動検出 BGP および BGP シグナリングをベースとする VPLS

```
l2vpn
bridge group bg1
```

```
bridge-domain bd-1-2
   interface GigabitEthernet
   !
   vfi vfi-1-2
    vpn-id 2
    autodiscovery bgp
     rd 101:2
     route-target 65530:200
     signaling-protocol bgp
      ve-id 11
      ve-range 16
     !
    !
   evi 2
  !
```

ターゲット LDP をベースとする VPLS

```
bridge-domain bd-1-4
   interface GigabitEthernet
   !
   vfi vfi-1-4
    neighbor 200.0.2.1 pw-id 1200004
    !
    neighbor 200.0.3.1 pw-id 1300004
    !
    neighbor 200.0.4.1 pw-id 1400004
    !
   evi 3
   !
```

EVPN 設定の確認

EVPN の設定と MAC のアドバタイズメントを確認するには、次のコマンドを使用します。EVPN のステータス、AC のステータス、および VFI のステータスを確認します。

- show l2vpn bridge-domain
- show evpn summary
- show bgp rt l2vpn evpn
- show evpn evi
- show l2route evpn mac all

```
Router#show l2vpn bridge-domain bd-name bd-1-1
Mon Feb 20 21:03:40.244 EST
Legend: pp = Partially Programmed.
Bridge group: bg1, bridge-domain: bd-1-1, id: 0, state: up, ShgId: 0, MSTi: 0
  Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 1 (1 up), VFIs: 1, PWs: 3 (2 up), PBBs: 0 (0 up), VNIs: 0 (0 up)
  List of EVPNs:
    EVPN, state: up
  List of ACs:
    Gi0/2/0/0.1, state: up, Static MAC addresses: 0, MSTi: 2
  List of Access PWs:
```

```
  List of VFIs:
    VFI vfi-1-1 (up)
      Neighbor 200.0.2.1 pw-id 1200001, state: up, Static MAC addresses: 0
      Neighbor 200.0.3.1 pw-id 1300001, state: down, Static MAC addresses: 0
      Neighbor 200.0.4.1 pw-id 1400001, state: up, Static MAC addresses: 0
  List of Access VFIs:
 When PEs are evpn enabled, pseudowires that are associated with that BD will be brought
 down. The VPLS BD pseudowires are always up.
```

EVI の設定済みのローカルおよびリモート MAC ルートのうちアドバタイズされたものの数を確認します。

```
Router#show evpn summary
Mon Feb 20 21:05:16.755 EST
----------------------------
Global Information
----------------------------
Number of EVIs                 : 6
Number of Local EAD Entries    : 0
Number of Remote EAD Entries   : 0
Number of Local MAC Routes     : 4
          MAC                  : 4
          MAC-IPv4             : 0
          MAC-IPv6             : 0
Number of Local ES:Global MAC  : 1
Number of Remote MAC Routes    : 0
          MAC                  : 0
          MAC-IPv4             : 0
          MAC-IPv6             : 0
Number of Remote SOO MAC Routes    : 0
Number of Local IMCAST Routes  : 4
Number of Remote IMCAST Routes     : 4
Number of Internal Labels      : 0
Number of ES Entries           : 1
Number of Neighbor Entries     : 4
EVPN Router ID                 : 200.0.1.1
BGP ASN                        : 65530
PBB BSA MAC address            : 0026.982b.c1e5
Global peering timer           :      3 seconds
Global recovery timer          :     30 seconds
```

EVPN ルートターゲットを確認します。

```
Router#show bgp rt l2vpn evpn
Mon Feb 20 21:06:18.882 EST
EXTCOMM         IMP/EXP
RT:65530:1              1 / 1
RT:65530:2              1 / 1
RT:65530:3              1 / 1
RT:65530:4              1 / 1
Processed 4 entries

Locally learnt MAC routes can be viewed by forwarding table
show l2vpn forwarding bridge-domain mac-address location 0/0/cpu0
To Resynchronize MAC table from the Network Processors, use the command...
    l2vpn resynchronize forwarding mac-address-table location <r/s/i>

Mac Address    Type    Learned from/Filtered on    LC learned Resync Age/Last Change
Mapped to
-------------- ------- -------------------------- ---------- ----------------------
0033.0000.0001 dynamic Gi0/2/0/0.1                N/A        20 Feb 21:06:59     N/A
```

```
0033.0000.0002 dynamic Gi0/2/0/0.2                N/A        20 Feb 21:06:59     N/A

0033.0000.0003 dynamic Gi0/2/0/0.3                N/A        20 Feb 21:04:29     N/A

0033.0000.0004 dynamic Gi0/2/0/0.4                N/A        20 Feb 21:06:59     N/A

The remote routes learned via evpn enabled BD
show l2vpn forwarding bridge-domain mac-address location 0/0$
To Resynchronize MAC table from the Network Processors, use the command...
    l2vpn resynchronize forwarding mac-address-table location <r/s/i>

Mac Address    Type    Learned from/Filtered on    LC learned Resync Age/Last Change
Mapped to
-------------- ------- -------------------------- ---------- ----------------------
0033.0000.0001 EVPN    BD id: 0                   N/A        N/A                 N/A

0033.0000.0002 EVPN    BD id: 1                   N/A        N/A                 N/A

0033.0000.0003 EVPN    BD id: 2                   N/A        N/A                 N/A

0033.0000.0004 EVPN    BD id: 3                   N/A        N/A                 N/A
```

特定の VPN インスタンスに関係のある EVPN MAC ルートを確認します。

```
Router#show evpn evi vpn-id 1 mac
Mon Feb 20 21:36:23.574 EST

EVI        MAC address    IP address                  Nexthop
   Label
---------- -------------- ----------------------------------------
---------------------------------
1      0033.0000.0001      ::                       200.0.1.1
45106
```

L2 ルーティングを確認します。

```
Router#show l2route evpn mac all
Mon Feb 20 21:39:43.953 EST
Topo ID  Mac Address    Prod   Next Hop(s)
-------- -------------- ------ ---------------------------------------
0        0033.0000.0001 L2VPN  200.0.1.1/45106/ME
1        0033.0000.0002 L2VPN  200.0.1.1/45108/ME
2        0033.0000.0003 L2VPN  200.0.1.1/45110/ME
3        0033.0000.0004 L2VPN  200.0.1.1/45112/ME
```

EVPN ルート タイプ 2 ルートを確認します。

```
Router#show bgp l2vpn evpn route-type 2
Mon Feb 20 21:43:23.616 EST
BGP router identifier 200.0.3.1, local AS number 65530
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 21
BGP NSR Initial initsync version 1 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs
```

```
Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 200.0.1.1:1
*>i[2][0][48][0033.0000.0001][0]/104
                      200.0.1.1                100      0 i
Route Distinguisher: 200.0.1.1:2
*>i[2][0][48][0033.0000.0002][0]/104
                      200.0.1.1                100      0 i
Route Distinguisher: 200.0.1.1:3
*>i[2][0][48][0033.0000.0003][0]/104
                      200.0.1.1                100      0 i
Route Distinguisher: 200.0.1.1:4
*>i[2][0][48][0033.0000.0004][0]/104
                      200.0.1.1                100      0 i
Route Distinguisher: 200.0.3.1:1 (default for vrf bd-1-1)
*>i[2][0][48][0033.0000.0001][0]/104
                      200.0.1.1                100      0 i
Route Distinguisher: 200.0.3.1:2 (default for vrf bd-1-2)
*>i[2][0][48][0033.0000.0002][0]/104
                      200.0.1.1                100      0 i
Route Distinguisher: 200.0.3.1:3 (default for vrf bd-1-3)
*>i[2][0][48][0033.0000.0003][0]/104
                      200.0.1.1                100      0 i
Route Distinguisher: 200.0.3.1:4 (default for vrf bd-1-4)
*>i[2][0][48][0033.0000.0004][0]/104
                      200.0.1.1                100      0 i

Processed 8 prefixes, 8 paths
```

包含マルチキャスト ルートとルート タイプ 3 ルートを確認します。

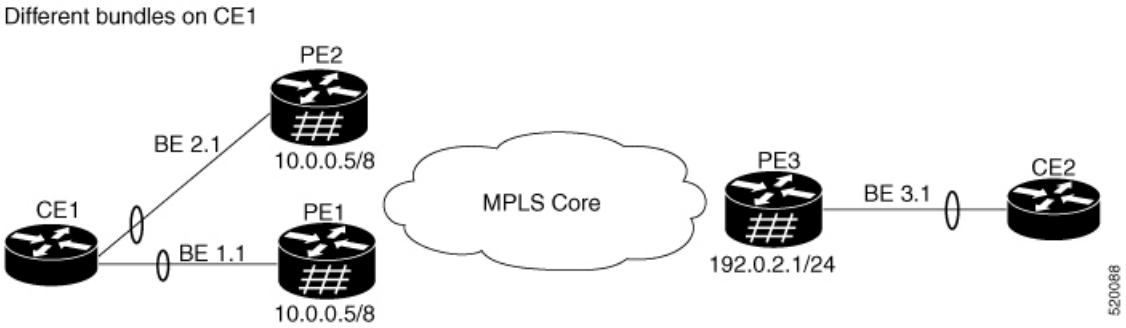
```
Router#show bgp l2vpn evpn route-type 3
Mon Feb 20 21:43:33.970 EST
BGP router identifier 200.0.3.1, local AS number 65530
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 21
BGP NSR Initial initsync version 1 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 200.0.1.1:1
*>i[3][0][32][200.0.1.1]/80
                      200.0.1.1                100      0 i
Route Distinguisher: 200.0.1.1:2
*>i[3][0][32][200.0.1.1]/80
                      200.0.1.1                100      0 i
Route Distinguisher: 200.0.1.1:3
*>i[3][0][32][200.0.1.1]/80
                      200.0.1.1                100      0 i
Route Distinguisher: 200.0.1.1:4
*>i[3][0][32][200.0.1.1]/80
                      200.0.1.1                100      0 i
Route Distinguisher: 200.0.3.1:1 (default for vrf bd-1-1)
*>i[3][0][32][200.0.1.1]/80
                      200.0.1.1                100      0 i
```

```
*> [3][0][32][200.0.3.1]/80
                      0.0.0.0                                0 i
Route Distinguisher: 200.0.3.1:2 (default for vrf bd-1-2)
*>i[3][0][32][200.0.1.1]/80
                      200.0.1.1                100       0 i
*> [3][0][32][200.0.3.1]/80
                      0.0.0.0                                0 i
Route Distinguisher: 200.0.3.1:3 (default for vrf bd-1-3)
*>i[3][0][32][200.0.1.1]/80
                      200.0.1.1                100       0 i
*> [3][0][32][200.0.3.1]/80
                      0.0.0.0                                0 i
Route Distinguisher: 200.0.3.1:4 (default for vrf bd-1-4)
*>i[3][0][32][200.0.1.1]/80
                      200.0.1.1                100       0 i
*> [3][0][32][200.0.3.1]/80
                      0.0.0.0                                0 i
```

エニーキャストゲートウェイ IRB の EVPN シングルアクティブ マルチホーミング

エニーキャストゲートウェイ IRB の EVPN シングルアクティブ マルチホーミング機能は、シングルアクティブ冗長モードをサポートしています。このモードでは、プロバイダーエッジ（PE）ノードは、EVPN サービスインスタンス（EVI）に基づいて、イーサネットセグメントとの間で発着信するイーサネット セグメント ロード バランス トラフィックにローカルに接続されます。EVPN サービスインスタンス内では、1 つの PE のみがイーサネットセグメント（ES）との間で発着信するトラフィックを転送します。この機能は、サブネット間シナリオのみをサポートします。

図 *32 : EVPN* : エニーキャストゲートウェイ *IRB* の *EVPN* シングルアクティブ マルチホーミング



CE1 が PE1 や PE2 にマルチホームされているトポロジについて考えてみます。バンドル イーサネット インターフェイスは BE 1.1、BE 2.1 です。入力インターフェイスは CE1 上の同じスイッチングドメインに属している必要があります。これらのピアリング PE の両方で、ホストルーティングを有効にし、エニーキャストゲートウェイ IP アドレスを設定します。PE1 と PE2 は MPLS コアを通じて PE3 に接続しています。PE3 は、サブネット 10.0.0.5/8 から両方のピアリング PE に到達可能です。ピアリング PE は、PE3 サブネット 192.0.2.1/24 に到達可能です。CE2 はイーサネット インターフェイス バンドルを通じて PE3 に接続されています。PE1 と PE2

はタイプ 4 ルートをアドバタイズしてから、指定フォワーダ（DF）の選択を実行します。非 DF はシングルアクティブ モードの両方向のトラフィックをブロックします。

CE1 から CE2 へのトラフィック フローを考えてみます。CE1 は PE1 と PE2 の両方に Address Resolution Protocol（ARP）ブロードキャスト要求を送信します。ピアリング PE は、共有 ESI に対して指定フォワーダー（DF）の選択を実行します。PE1 が EVI の指定フォワーダである場合、PE1 は CE1 からの ARP 要求に応答します。PE2 は CE1 からのトラフィックをドロップします。その後で、すべてのユニキャスト トラフィックが PE1 を通じて送信されます。PE2 は、スタンバイ状態またはブロック状態に設定されており、トラフィックはこのパスを介して送信されません。PE1 は PE3 に MAC をアドバタイズします。PE3 は常に PE1 を通じてトラフィックを送受信します。PE3 はイーサネット インターフェイス バンドルを介してトラフィックを CE2 に送信します。BE1 に障害が発生した場合、PE2 は、PE2 を通過する DF およびトラフィックフローになります。

EVPN シングルアクティブ マルチホーミングの設定

EVPN シングルアクティブ マルチホーミング機能を設定するには、PE1 と PE2 上で次のタスクを実行します。

- ホストルーティングを使用した EVPN IRB の設定
- EVPN イーサネット セグメントの設定
- レイヤ 2 インターフェイスの設定
- ブリッジ ドメインの設定
- VRF の設定

EVPN イーサネット セグメントの設定

EVPN イーサネット セグメントを設定するには、次のタスクを実行します。

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether1
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 40.00.00.00.00.00.00.00.01
Router(config-evpn-ac-es)# load-balancing-mode single-active
Router(config-evpn-ac-es)# bgp route-target 4000.0000.0001
Router(config-evpn-ac-es)# comit
```

実行コンフィギュレーション

```
configure
evpn
 interface Bundle-Ether1
   ethernet-segment
    identifier type 0 40.00.00.00.00.00.00.00.01
    load-balancing-mode single-active
    bgp route-target 4000.0000.0001
    !
```

```
!
!
```

EVPN サービス インスタンス（EVI）パラメータの設定

EVPN サービス インスタンス（EVI）パラメータを定義するには、このタスクを実行します。

```
Router# configure
Router(config)# evpn
Router(config-evpn)# evi 6005
Router(config-evpn-evi)# bgp
Router(config-evpn-evi-bgp)# rd 200:50
Router(config-evpn-evi-bgp)# route-target import 100:6005
Router(config-evpn-evi-bgp)# route-target export 100:6005
Router(config-evpn-evi-bgp)# commit
```

実行コンフィギュレーション

```
configure
 evpn
  evi 6005
   bgp
    rd 200:50
    route-target import 100:6005
    route-target export 100:6005
!
!
```

レイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスを定義するには、次のタスクを実行します。

```
Router# configure
Router(config)# interface bundle-ether2.1 l2transport
Router(config-subif-l2)# no shutdown
Router(config-subif-l2)# encapsulation dot1q 1
Router(config-subif-l2)# rewrite ingress tag pop 1 symmetric
Router(config-subif-l2)#commit
Router(config-subif-l2)#exit
```

実行コンフィギュレーション

この項では、レイヤ 2 インターフェイスの実行コンフィギュレーションを示します。

```
configure
 interface bundle-ether2.1 l2transport
  no shutdown
  encapsulation dot1q 1
  rewrite ingress tag pop 1 symmetric
!
```

ブリッジ ドメインの設定

次のステップを実行して PE1 と PE2 上にブリッジ ドメインを設定します。

```
Router# configure
```

```
Router(config)# l2vpn
Router(config-l2vpn)# bridge group 6005
Router(config-l2vpn-bg)# bridge-domain 6005
Router(config-l2vpn-bg-bd)# interface Bundle-Ether2.1
Router(config-l2vpn-bg-bd-ac)# evi 6005
Router(config-l2vpnbg-bd-evi)# commit
Router(config-l2vpnbg-bd-evi)# exit
```

実行コンフィギュレーション

この項では、ブリッジドレインの実行コンフィギュレーションを示します。

```
configure
l2vpn
 bridge group 6005
  bridge-domain 6005
   interface Bundle-Ether2.1
    evi 6005
!
```

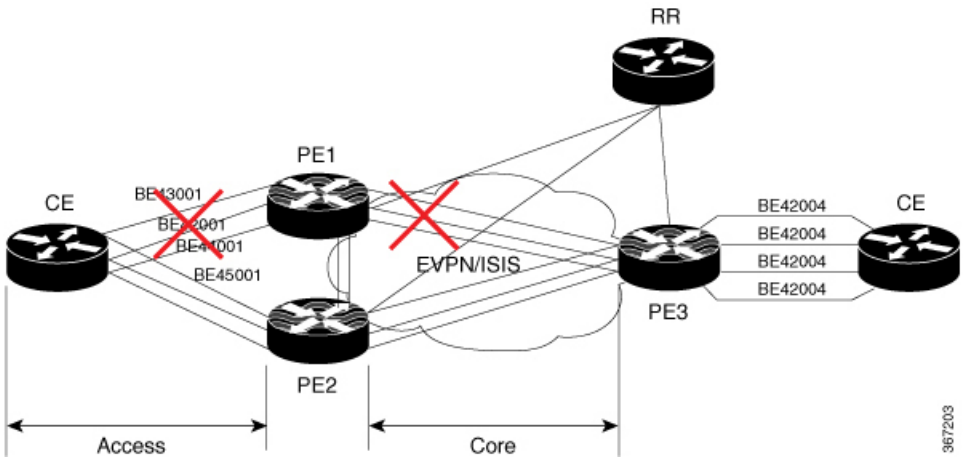
EVPN コア分離保護

EVPN コア分離保護機能を使用すると、コア内のリンク障害をモニタして検出することができます。プロバイダー エッジ（PE）デバイスでコア リンク障害が検出されると、EVPN は、PE のイーサネット セグメント（ES）を停止します。ES は、カスタマー エッジ（CE）デバイスに接続しているアクセス インターフェイスに関連付けられています。

EVPN は、ICCP のコア分離の検出を置き換えるものです。この新機能により、EVPN 環境で ICCP を使用する必要がなくなります。

CE が PE1 および PE2 に接続されているトポロジを考えてみます。PE1、PE2、および PE3 では、MPLS コア ネットワーク上で EVPN が実行されています。コア インターフェイスにはギガビット イーサネットまたはバンドル インターフェイスを使用できます。

図 *33 : EVPN* コア分離保護



PE1 のコア リンクがダウンすると、EVPN はリンク障害を検出し、アクセス ネットワークをダウンさせてコア ネットワークから PE1 ノードを分離します。これにより、CE は PE1 にトラ

フィックを送信できなくなります。BGP セッションもダウンしているため、BGP は、障害が発生したPEによってアドバタイズされたすべてのルートを無効にします。これにより、リモート PE2 および PE3 は、L2FIB 内のネクストホップ パスリストと MAC ルートを更新します。PE2はすべてのトラフィックの転送者になるため、コア ネットワークからPE1を分離します。

すべてのコア インターフェイスと BGP セッションがアップすると、PE1 はイーサネット A-D イーサネットセグメント（ES-EAD）ルートを再度アドバタイズし、サービス カービングをトリガーして、コア ネットワークの一部になります。

EVPN コア分離保護の設定

EVPN グループの配下にコア インターフェイスを設定し、そのグループを、CE に接続された接続回線（AC）であるイーサネット セグメントに関連付けます。すべてのコアインターフェイスがダウンすると、EVPNは、関連付けられているアクセスインターフェイスをダウンさせます。これにより、CE デバイスは自身のバンドル内でこれらのリンクを使用できなくなります。グループの一部であるすべてのインターフェイスがダウンすると、EVPNはバンドルをダウンさせ 、ES-EAD ルートを取り消します。

制約事項

- EVPN の配下には最大 24 のグループを作成できます。
- グループの下には最大 12 のコア インターフェイスを追加できます。
- コア インターフェイスはグループ間で再利用できます。コア インターフェイスは、バンドル インターフェイスにすることができます。
- EVPN グループにはコア インターフェイスのみを含める必要があります。 EVPN グループの配下にアクセス インターフェイスを追加しないでください。
- アクセス インターフェイスは、バンドル インターフェイスにしかなれません。
- EVPN コアに面するインターフェイスは、物理インターフェイスまたはバンドル メイン インターフェイスのみにする必要があります。サブインターフェイスはサポートされていません。

```
Router# configure
Router(config)# evpn
Router(config-evpn)# group 42001
Router(config-evpn-group)# core interface GigabitEthernet0/2/0/1
Router(config-evpn-group)# core interface GigabitEthernet0/2/0/3
Router(config-evpn-group)#exit
!
Router(config-evpn)# group 43001
Router(config-evpn-group)# core interface GigabitEthernet0/2/0/2
Router(config-evpn-group)# core interface GigabitEthernet0/2/0/4
Router(config-evpn-group)#exit
!
Router# configure
Router(config)# evpn
Router(config-evpn)# interface bundle-Ether 42001
Router(config-evpn-ac)# core-isolation-group 42001
```

```
Router(config-evpn-ac)# exit
!
Router(config-evpn)# interface bundle-Ether 43001
Router(config-evpn-ac)# core-isolation-group 43001
Router(config-evpn-ac)# commit
```

実行コンフィギュレーション

```
configure
 evpn
  group 42001
   core interface GigabitEthernet0/2/0/1
   core interface GigabitEthernet0/2/0/3
   !
  group 43001
   core interface GigabitEthernet0/2/0/2
   core interface GigabitEthernet0/2/0/4
   !
 !
configure
 evpn
  interface bundle-Ether 42001
   core-isolation-group 42001
   !
  interface bundle-Ether 43001
   core-isolation-group 43001
   !
  !
```

確認

show evpn group コマンドは、evpn グループの完全なリストと、それらに関連付けられているコア インターフェイスおよびアクセス インターフェイスを表示します。各インターフェイスのステータス（アップまたはダウン）も表示されます。アクセスインターフェイスがアップ状態になるには、コア インターフェイスが少なくとも 1 つアップ状態である必要があります。

```
Router# show evpn group /* Lists specific group with core-interfaces and access interface
 status */
EVPN Group: 42001
  State: Ready
  Core Interfaces:
     Bundle-Ethernet110: down
     Bundle-Ethernet111: down
     GigabethEthernet0/2/0/1: up
     GigabethEthernet0/2/0/3: up
     GigabethEthernet0/4/0/8: up
     GigabethEthernet0/4/0/9: up
     GigabethEthernet0/4/0/10: up
  Access Interfaces:
     Bundle-Ether42001: up

EVPN Group: 43001
  State: Ready
  Core Interfaces:
     Bundle-Ethernet110: down
     GigabethEthernet0/2/0/2: up
     GigabethEthernet0/2/0/4: up
```

```
    GigabethEthernet0/4/0/9: up

Access Interfaces:
    Bundle-Ether43001: up
```

EVPN ルーティング ポリシー

EVPN ルーティング ポリシー機能では、アドレスファミリ L2VPN EVPN のルート ポリシー サポートを提供します。この機能は、EVPN ルート フィルタリング機能をルーティング ポリシー言語（RPL）に追加します。フィルタリングはさまざまな EVPN 属性に基づきます。

ピアから受け入れるか、ピアにアドバタイズされる、または 1 個のルーティング プロトコルから別のプロトコルへ再配布されるときに、ルートを検査し、フィルタリングして、属性を変更するように、ルーティング ポリシーがルータに指示します。

この機能により、より粒度が高いルートポリシーの定義を提供するルートポリシー一致基準の EVPN ルートタイプ 1 ～ 5 の EVPN ネットワーク層到達可能性情報（NLRI）属性を使用してルートポリシーを設定できます。たとえば、ルートポリシーを特定の EVPN ルートタイプのみに適用したり、任意の組み合わせの EVPN NLRI 属性に適用できます。この機能は、ルートポリシーを有効にして EVPN NLRI 属性でフィルタリングすることで、ソリューションの設定および展開に柔軟性をもたらします。

この機能を実装するには、次の概念を理解する必要があります。

- ルーティング ポリシー言語
- ルーティング ポリシー言語の構造
- ルーティング ポリシー言語コンポーネント
- ルーティング ポリシー言語使用方法
- ポリシー定義
- パラメータ化
- ポリシー適用のセマンティック
- ポリシー ステートメント
- 接続点

これらの概念については「ルーティング ポリシーの実装」を参照してください。

現在、この機能は接続ポイント「イン」または「アウト」の BGP ネイバーでのみサポートされています。ルート ポリシーは BGP ネイバーのインバウンドまたはアウトバウンドのみに適用できます。

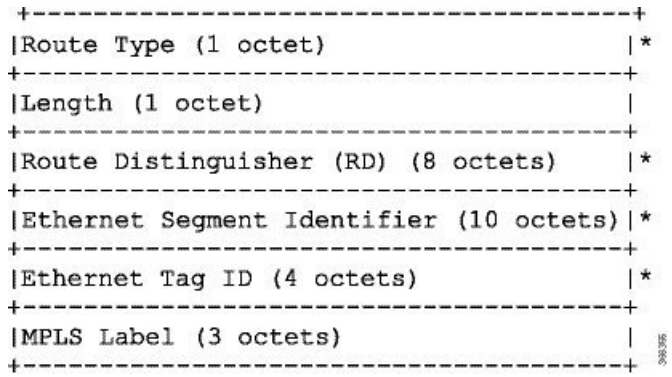
EVPN ルート タイプ

EVPN NLRI には次のさまざまなルート タイプがあります。

ルート タイプ 1：イーサネット自動検出（AD）ルート

イーサネット（AD）ルートは、EVI ごととイーサネットセグメント識別子（ESI）ごとにアドバタイズされます。これらのルートは、イーサネットセグメント（ES）ごとに送信されます。これらは ES に属している EVI のリストを伝送します。ESI フィールドは、CE がシングルホームの場合はゼロに設定されます。

イーサネット A-D ルート タイプ固有の EVPN NLRI は次のフィールドで構成されます。



NLRI の形式：**ルートタイプ 1**：

```
[Type][Len][RD][ESI][ETag][MPLS Label]
```

ネット属性：`[Type][RD][ESI][ETag]`

パス属性：`[MPLS Label]`

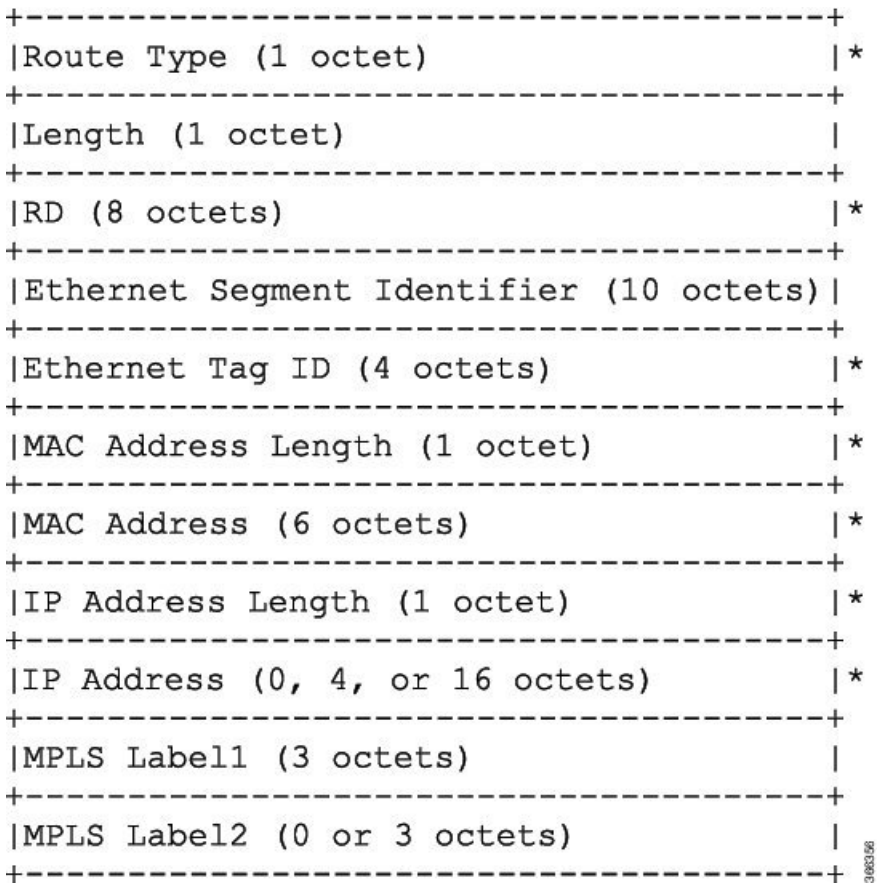
例

```
route-policy evpn-policy
  if rd in (1.1.1.1:0) [and/or evpn-route-type is 1] [and/or esi in
(0a1.a2a3.a4a5.a6a7.a8a9)] [and/or etag is 4294967295] then
    set ..
  endif
end-policy
!
route-policy evpn-policy
  if rd  in (1.1.1.2:0) [and/or evpn-route-type is 1] [and/or esi in
(00a1.a2a3.a4a5.a6a7.a8a9)] [and/or etag is 4294967295] then
    set ..
  endif
end-policy
```

ルート タイプ 2：MAC/IP アドバタイズメント ルート

ホストの IP アドレスと MAC アドレスが NLRI 内のピアにアドバタイズされます。MAC アドレスのコントロール プレーン学習は不明ユニキャストのフラッディングを削減します。

MAC/IP アドバタイズメント ルート タイプ固有の EVPN NLRI は次のフィールドで構成されます。



NLRI の形式：**ルートタイプ 2**：

```
[Type][Len][RD][ESI][ETag][MAC Addr Len][MAC Addr][IP Addr Len][IP Addr][MPLS Label1][MPLS
Label2]
```

ネット属性：`[Type][RD][ETag][MAC Addr Len][MAC Addr][IP Addr Len][IP Addr]`

パス属性：`[ESI], [MPLS Label1], [MPLS Label2]`

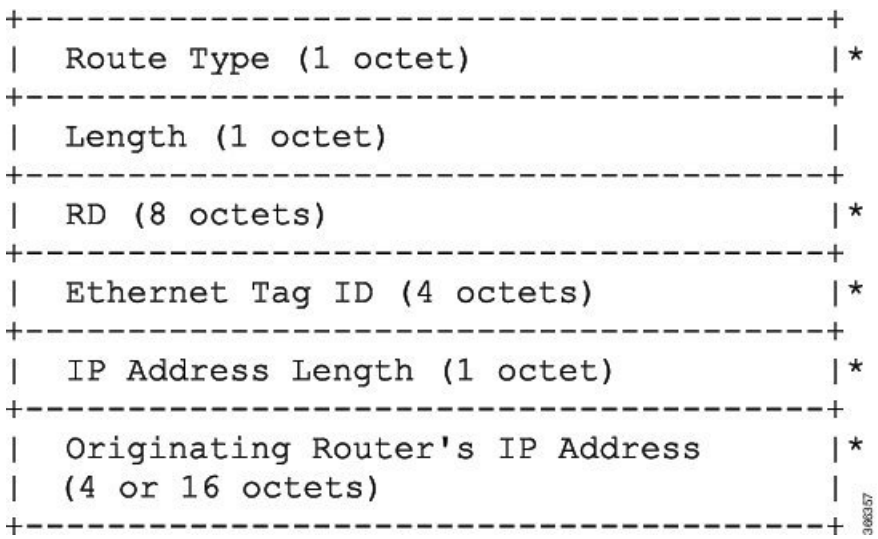
例

```
route-policy evpn-policy
  if rd in (1.1.1.2:0) [and/or evpn-route-type is 2] [and/or esi in
(0000.0000.0000.0000.0000)] [and/or etag is 0] [and/or macaddress in (0013.aabb.ccdd)]
[and/or destination in (1.2.3.4/32)] then
    set ..
  endif
end-policy
```

ルート タイプ 3：包括的なマルチキャスト イーサネット タグ ルート

このルートは、送信元 PE からリモート PE へのブロードキャスト、不明ユニキャスト、およびマルチキャスト（BUM）トラフィック用の接続を確立します。このルートは、VLAN ごとと ESI ごとにアドバタイズされます。

包括的マルチキャスト イーサネット タグ ルート タイプ固有の EVPN NLRI は次のフィールドで構成されます。



NLRI の形式：**ルートタイプ 3**：

```
[Type][Len][RD][ETag][IP Addr Len][Originating Router's IP Addr]
```

ネット属性：`[Type][RD][ETag][IP Addr Len][Originating Router's IP Addr]`

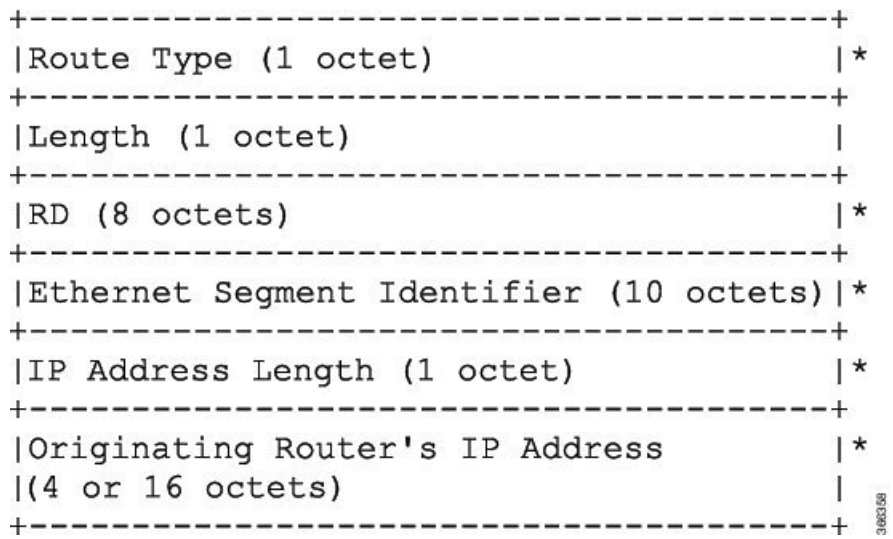
例

```
route-policy evpn-policy
  if rd  in (1.1.1.1:300) [and/or evpn-route-type is 3] [and/or etag is 0] [and/or
evpn-originator in (1.1.1.1)] then
    set ..
  endif
end-policy
```

ルート タイプ 4：イーサネット セグメント ルート

イーサネット セグメント ルートでは CE デバイスを 2 台のデバイスまたは PE デバイスを接続できます。ES ルートでは同じイーサネット セグメントに接続されている PE デバイスを検出できます。

イーサネットセグメントルートタイプ固有の EVPN NLRI は次のフィールドで構成されます。



NLRI の形式：**ルートタイプ 4**：

```
[Type][Len][RD][ESI][IP Addr Len][Originating Router's IP Addr]
```

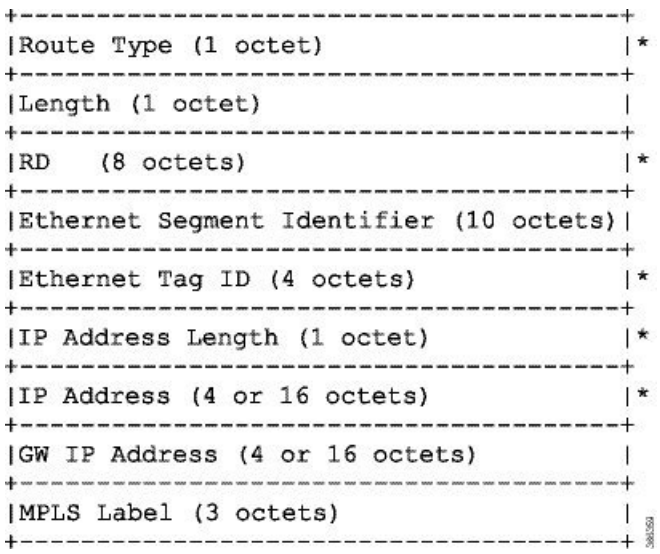
ネット属性：`[Type][RD][ESI][IP Addr Len][Originating Router's IP Addr]`

例

```
route-policy evpn-policy
  if rd  in (1.1.1.1:0) [and/or evpn-route-type is 4] [and/or esi in
(00a1.a2a3.a4a5.a6a7.a8a9)] [and/or evpn-originator in (1.1.1.1)] then
    set ..
  endif
end-policy
```

ルート タイプ 5：IP プレフィックス ルート

IP プレフィックス ルート タイプ固有の EVPN NLRI は次のフィールドで構成されます。



NLRI の形式：**ルートタイプ 5**：

```
[Type][Len][RD][ESI][ETag][IP Addr Len][IP Addr][GW IP Addr][Label]
```

ネット属性：`[Type][RD][ETag][IP Addr Len][IP Addr]`

パス属性：`[ESI], [GW IP Addr], [Label]`

例

```
route-policy evpn-policy
  if rd in (30.30.30.30:1) [and/or evpn-route-type is 5] [and/or esi in
(0000.0000.0000.0000.0000)] [and/or etag is 0] [and/or destination in (12.2.0.0/16)]
[and/or evpn-gateway in (0.0.0.0)] then
    set ..
  endif
end-policy
```

EVPN RPL 属性

ルート識別子

ルート識別子（rd）属性は、8 オクテットで構成されます。rd は EVPN ルートのタイプそれぞれに指定できます。この属性は、ルートポリシーでは必須ではありません。

例

```
rd in (1.2.3.4:0)
```

EVPN ルート タイプ

EVPN ルート タイプ属性は、1 オクテットで構成されます。これによって EVPN ルート タイプが指定されます。EVPN ルート タイプ属性は、特定の EPVN NLRI プレフィックス形式を識別するために使用されます。これは、すべての EVPN ルート タイプのネット属性の 1 つです。

例

```
evpn-route-type is 3


The following are the various EVPN route types that can be used:
1 - ethernet-ad
2 - mac-advertisement
3 - inclusive-multicast
4 - ethernet-segment
5 - ip-advertisement
```

IP プレフィックス

IP プレフィックス属性は、それぞれ 4 つの部分（アドレス、マスク長、最小一致長、最大一致長）がある IPv4 または IPv6 プレフィックス一致指定を保持しています。アドレスは必須ですが、他の 3 つの部分は任意です。EVPN ルート タイプ 2 での IP プレフィックスの指定により、IPv4 または IPv6 のいずれかのホスト IP アドレスを表します（/32 または /128）。EVPN ルート タイプ 5 の IP プレフィックスでの指定により、IPv4 または IPv6 のサブネットを表します。これは、EVPN ルート 2 と 5 のネット属性の 1 つです。

例

```
destination in (128.47.10.2/32)
destination in (128.47.0.0/16)
destination in (128:47::1/128)
destination in (128:47::0/112)
```

esi

イーサネット セグメント識別子（ESI）属性は、10 オクテットで構成されます。これは EVPN ルート タイプ 1 と 4 のネット属性であり、EVPN ルート タイプ 2 と 5 のパス属性です。

例

```
esi in (ffff.ffff.ffff.ffff.fff0)
```

etag

イーサネット タグ属性は 4 オクテットで構成されます。イーサネット タグは、特定のブロードキャスト ドメイン（VLAN など）を識別します。EVPN インスタンスは 1 つまたは複数のブ

ロード キャスト ドメインで構成されます。これは EVPN ルート タイプ 1、2、3、および 5 のネット属性です。

例

```
etag in (10000)
```

mac

MAC 属性は 6 オクテットで構成されます。これは、EVPN ルート 2 のネット属性です。

例

```
mac in (0206.acb1.e806)
```

evpn-originator

evpn-originator 属性は、発信元ルータの IP アドレス（4 または 16 オクテット）を指定します。これは、EVPN ルート 3 と 4 のネット属性です。

例

```
evpn-originator in (1.2.3.4)
```

evpn-gateway

evpn-gateway 属性は、ゲートウェイの IP アドレスを指定します。ゲートウェイ IP アドレスは 32 ビットまたは 128 ビットのフィールド（IPv4 または IPv6）であり、IP プレフィックスに応じてオーバーレイ ネクストホップをエンコードします。ゲートウェイ IP アドレス フィールドは、オーバーレイ ネクストホップとして使用しない場合はゼロに設定できます。これは、EVPN ルート 5 のパス属性です。

例

```
evpn-gateway in (1.2.3.4)
```

EVPN RPL 属性セット

このコンテキストでは、セットという用語を、順序付けのない固有のエレメントの集合を意味する数学的な概念で使用されます。ポリシー言語は、セットをマッチング用の値のグループに対するコンテナとして提供します。セットは、条件式で使用されます。セットの要素はカンマで区切ります。ヌル（空）のセットは許可されます。

prefix-set

prefix-set は、それぞれ 4 つの部分（アドレス、マスク長、最小一致長、最大一致長）がある IPv4 または IPv6 プレフィックス一致指定を保持しています。アドレスは必須ですが、他の 3 つの部分は任意です。prefix-set は 1 つまたは複数の IP プレフィックスを指定します。

例

```
prefix-set ip_prefix_set
14.2.0.0/16,
54.0.0.0/16,
12.12.12.0/24,
50:50::1:0/112
end-set
```

mac-set

mac-set は 1 つまたは複数の MAC プレフィックスを指定します。

例

```
mac-set mac_address_set
1234.2345.6789,
2345.3456.7890
end-set
```

esi-set

esi-set は、1 つまたは複数の ESI を指定します。

例

```
esi-set evpn_esi_set
1234.2345.3456.4567.5678,
1234.2345.3456.4567.5670
end-set
```

etag-set

etag-set は、1 つまたは複数のイーサネット タグを指定します。

例

```
etag-set evpn_etag_set
10000,
20000
end-set
```

EVPN RPL 機能の設定

次の項では、mac-set、esi-set、evpn-gateway、および evpn-originator を設定する方法について説明します。

```
/* Configuring a mac-set and refering it in a route-policy (Attach point - neighbor-in)
 */
Router# configure
Router(config)# mac-set demo_mac_set
Router(config-mac)# 1234.ffff.aaa3,
Router(config-mac)# 2323.4444.ffff
Router(config-mac)# end-set
Router(config)# !
Router(config)# route-policy policy_use_pass_mac_set
Router(config-rpl)# if mac in demo_mac_set then
Router(config-rpl-if)# set med 200
Router(config-rpl-if)# else
Router(config-rpl-else)# set med 1000
Router(config-rpl-else)# endif
Router(config-rpl)# end-policy
Router(config)# commit
Router(config)# router bgp 100
Router(config-bgp)# address-family ipv4 unicast
Router(config-bgp-af)# !
Router(config-bgp-af)# neighbor 10.0.0.10
Router(config-bgp-nbr)# remote-as 8
Router(config-bgp-nbr)# address-family ipv4 unicast
Router(config-bgp-nbr-af)# route-policy policy_use_pass_mac_set in
Router(config-bgp-nbr-af)# commit

/* Configuring a esi-set and refering it in a route-policy (Attach point - neighbor-in)
 */
Router# configure
Router(config)# esi-set demo_esi
Router(config-esi)# ad34.1233.1222.ffff.44ff,
Router(config-esi)# ad34.1233.1222.ffff.6666
Router(config-esi)# end-set
Router(config)# !
Router(config)# route-policy use_esi
Router(config-rpl)# if esi in demo_esi then
Router(config-rpl-if)# set local-preference 100
Router(config-rpl-if)# else
Router(config-rpl-else)# set local-preference 300
Router(config-rpl-else)# endif
Router(config-rpl)# end-policy
Router(config)# commit

/* Configuring evpn-gateway/evpn-originator in a route-policy (Attach point - neighbor-in
 and out) */
Router# configure
Router(config)# route-policy gateway_demo
Router(config-rpl)# if evpn-gateway in (10.0.0.0/32) then
Router(config-rpl-if)# pass
Router(config-rpl-if)# endif
Router(config-rpl)# end-policy
Router(config)# commit
Router(config)# route-policy originator_demo
Router(config-rpl)# if evpn-originator in (10.0.0.1/32) then
Router(config-rpl-if)# set local-preference 100
Router(config-rpl-if)# else
```

```
Router(config-rpl-else)# set med 200
Router(config-rpl-else)# endif
Router(config-rpl)# end-policy
Router(config)# commit
Router(config)# router bgp 100
Router(config-bgp)# address-family ipv4 unicast
Router(config-bgp-af)# !
Router(config-bgp-af)# neighbor 10.0.0.10
Router(config-bgp-nbr)# remote-as 8
Router(config-bgp-nbr)# address-family ipv4 unicast
Router(config-bgp-nbr-af)# route-policy gateway_demo in
Router(config-bgp-nbr-af)# route-policy originator_demo out
Router(config-bgp-nbr-af)# commit
```

実行コンフィギュレーション

```
/* Configuring a mac-set and refering it in a route-policy (Attach point - neighbor-in)
 */
mac-set demo_mac_set
  1234.ffff.aaa3,
  2323.4444.ffff
end-set
!
route-policy policy_use_pass_mac_set
  if mac in demo_mac_set then
    set med 200
  else
    set med 1000
  endif
end-policy
!
router bgp 100
 address-family ipv4 unicast
 !
 neighbor 10.0.0.10
  remote-as 8
  address-family ipv4 unicast
  route-policy policy_use_pass_mac_set in
  !
 !
!
end

/* Configuring a esi-set and refering it in a route-policy (Attach point - neighbor-in)
 */
Wed Oct 26 11:52:23.720 IST
esi-set demo_esi
  ad34.1233.1222.ffff.44ff,
  ad34.1233.1222.ffff.6666
end-set
!
route-policy use_esi
  if esi in demo_esi then
    set local-preference 100
  else
    set local-preference 300
  endif
end-policy
```

EVPN ルート ポリシーの例

```
route-policy ex_2
  if rd in (2.2.18.2:1004) and evpn-route-type is 1 then
    drop
  elseif rd in (2.2.18.2:1009) and evpn-route-type is 1 then
    drop
  else
    pass
  endif
end-policy
!
route-policy ex_3
  if evpn-route-type is 5 then
    set extcommunity bandwidth (100:9999)
  else
    pass
  endif
end-policy
!
route-policy samp
end-policy
!
route-policy samp1
  if rd in (30.0.101.2:0) then
    pass
  endif
end-policy
!
route-policy samp2
  if rd in (30.0.101.2:0, 1:1) then
    pass
  endif
end-policy
!
route-policy samp3
  if rd in (*:*) then
    pass
  endif
end-policy
!
route-policy samp4
  if rd in (30.0.101.2:*) then
    pass
  endif
end-policy
!
route-policy samp5
  if evpn-route-type is 1 then
    pass
  endif
end-policy
!
route-policy samp6
  if evpn-route-type is 2 or evpn-route-type is 5 then
    pass
  endif
end-policy
!
route-policy samp7
  if evpn-route-type is 4 or evpn-route-type is 3 then
    pass
```

```
  endif
end-policy
!
route-policy samp8
  if evpn-route-type is 1 or evpn-route-type is 2 or evpn-route-type is 3 then
    pass
  endif
end-policy
!
route-policy samp9
  if evpn-route-type is 1 or evpn-route-type is 2 or evpn-route-type is 3 or
evpn-route-type is 4 then
    pass
  endif
end-policy
!
route-policy test1
  if evpn-route-type is 2 then
    set next-hop 10.2.3.4
  else
    pass
  endif
end-policy
!
route-policy test2
  if evpn-route-type is 2 then
    set next-hop 10.10.10.10
  else
    drop
  endif
end-policy
!
route-policy test3
  if evpn-route-type is 1 then
    set tag 9988
  else
    pass
  endif
end-policy
!
route-policy samp21
  if mac in (6000.6000.6000) then
    pass
  endif
end-policy
!
route-policy samp22
  if extcommunity rt matches-any (100:1001) then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp23
  if evpn-route-type is 1 and esi in (aaaa.bbbb.cccc.dddd.eeee) then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp24
  if evpn-route-type is 5 and extcommunity rt matches-any (100:1001) then
```

```
    pass
  else
    drop
  endif
end-policy
!
route-policy samp25
  if evpn-route-type is 2 and esi in (1234.1234.1234.1234.1236) then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp26
  if etag in (20000) then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp27
  if destination in (99.99.99.1) and etag in (20000) then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp31
  if evpn-route-type is 1 or evpn-route-type is 2 or evpn-route-type is 3 or
evpn-route-type is 4 or evpn-route-type is 5 then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp33
  if esi in evpn_esi_set1 then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp34
  if destination in (90:1:1::9/128) then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp35
  if destination in evpn_prefix_set1 then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp36
```

```
  if evpn-route-type is 3 and evpn-originator in (80:1:1::3) then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp37
  if evpn-gateway in (10:10::10) then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp38
  if mac in evpn_mac_set1 then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp39
  if mac in (6000.6000.6002) then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp41
  if evpn-gateway in (10.10.10.10, 10:10::10) then
    pass
  else
    drop
  endif
end-policy
!
route-policy samp42
  if evpn-originator in (24.162.160.1/32, 70:1:1::1/128) then
    pass
  else
    drop
  endif
end-policy
!
route-policy example
  if rd in (62300:1903) and evpn-route-type is 1 then
    drop
  elseif rd in (62300:19032) and evpn-route-type is 1 then
    drop
  else
    pass
  endif
end-policy
!
route-policy samp100
  if evpn-route-type is 4 or evpn-route-type is 5 then
    drop
  else
    pass
  endif
end-policy
```

```
!
route-policy samp101
  if evpn-route-type is 4 then
    drop
  else
    pass
  endif
end-policy
!
route-policy samp102
  if evpn-route-type is 4 then
    drop
  elseif evpn-route-type is 5 then
    drop
  else
    pass
  endif
end-policy
!
route-policy samp103
  if evpn-route-type is 2 and destination in evpn_prefix_set1 then
    drop
  else
    pass
  endif
end-policy
!
route-policy samp104
  if evpn-route-type is 1 and etag in evpn_etag_set1 then
    drop
  elseif evpn-route-type is 2 and mac in evpn_mac_set1 then
    drop
  elseif evpn-route-type is 5 and esi in evpn_esi_set1 then
    drop
  else
    pass
  endif
end-policy
!
```

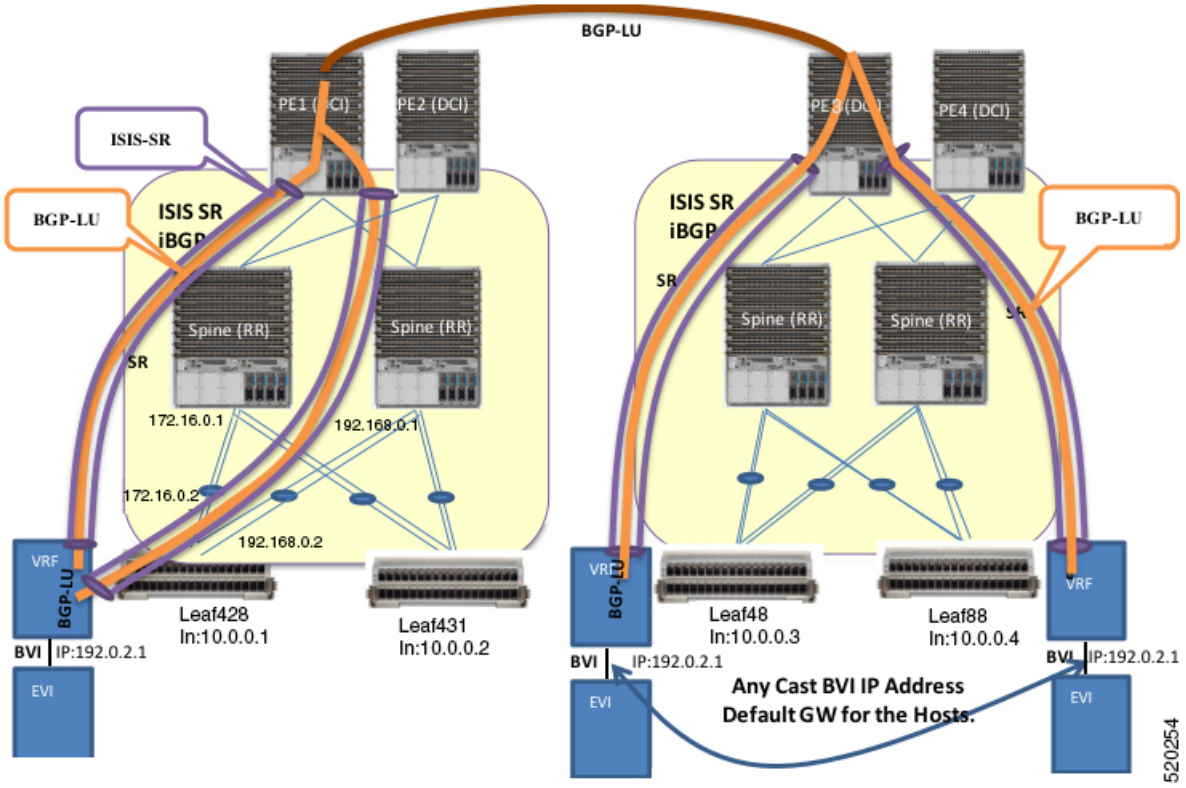
BGP-LU アンダーレイを介した EVPN ブリッジングおよび VPWS サービス

BGP-LU アンダーレイを介した EVPN ブリッジングおよび VPWS サービスでは、データセンター（DC）間のエンドツーエンド EVPN サービスを設定できます。この機能を使用すると、トランスポート、BGP-LU、サービスレベルの 3 レベルで ECMP を実行できます。

この機能は次のサービスをサポートしています。

- IGP を使用して BGP-LU を介した IRB VRF（SR または非 SR：LDP、IGP）
- IGP を使用して BGP-LU を介した EVPN のエイリアシング（SR または非 SR：LDP、IGP）
- IGP を使用して BGP-LU を介した VPWS

図 *34 : BGP-LU* アンダーレイを介した *EVPN* ブリッジングおよび *VPWS* サービス



この項では、BGP-LU アンダーレイ機能を使用した EVPN ブリッジングおよび VPWS サービスのトポロジについて説明します。

- DCI を介して接続されている 2 つのデータセンターについて考えてみます。リーフノードでのブリッジングおよびサブネット間ルーティングにより、EVPN を設定します。
- BVI 接続回線を備えた EVPN インスタンスを VRF を実装したインターフェイスに設定します。
- 同じ MAC アドレスを持つエニーキャスト IP アドレスを使用して、BVI インターフェイスを設定します。これは、同じ EVPN ブリッジドドメイン全体で、すべてのホストのデフォルトゲートウェイになります。
- リーフは、ローカルホストのデフォルトゲートウェイとして機能します。
- リーフノードにホストを接続します。リーフノードはスパインを介してルーティングされます。DC 相互接続の場合、スパインはプロバイダーエッジ（PE）デバイスとデータセンター相互接続（DCI）を介して接続されます。
- IGP や I-BGP というラベルが付けられた IS-IS は、リーフノード、スパイン、DCI の内部で有効になります。スパインは、ルートリフレクタ（RR）として機能します。
- リーフノード、スパイン、DCI の間で、IS-IS SR ポリシーを設定します。
- DC 間で BGP-LU を設定します。

- ラベル付けされたユニキャスト BGP ルータは、リーフノードとトンネリング全体で IGP ラベル付きパス（IS-IS SR）を介して学習されます。

  たとえば、Leaf428 では、BGP-LU ルートがリモートループバック 10.0.0.3 と 10.0.0.4 用に学習されます。

- IRB（BVI）インターフェイスルートは EVPN インスタンス全体で学習され、トンネリングされたラベル付きルートとして BGP-LU を介してプログラミングされます。

  たとえば Leaf428 では、192.0.2.1 は 10.0.0.3 と 10.0.0.4 の 2 つの BGP-LU パスを使用して到達できます。

BGP-LU アンダーレイを介した EVPN ブリッジングおよび VPWS サービスの設定

BGP-LU アンダーレイ機能を介して EVPN ブリッジングおよび VPWS サービスを設定するには、次のタスクを実行します。

- IGP の設定
- BGP の設定
- EVPN インスタンスと ESI の設定
- BVI（IRB）インターフェイスの設定
- VRF の設定
- VRF を使用した BVI の設定
- BGP での VRF の設定
- ブリッジドメインの設定と接続回線および EVPN インスタンスとの関連付け
- ブリッジドメインの設定と接続回線、EVPN インスタンス、および BVI との関連付け
- EVPN VPWS の設定

設定例

```
/* Configure IGP */
IGP configuration is a pre-requisite to configure EVPN. IGP can be OSPF or ISIS.
Router# configure
Router(config)#router ospf 1
Router(config-ospf)#router-id 209.165.201.1
Router(config-ospf)#area 10
Router(config-ospf-ar)#interface loopback0\
Router(config-ospf-ar-if)#exit
Router(config-ospf-ar)#interface TenGigE0/0/0/1\
Router(config-ospf-ar-if)#exit
Router(config-ospf-ar)#interface TenGigE0/0/0/17\
Router(config-ospf-ar-if)#commit
```

```
/* Configure BGP */
Router# configure
Router(config)#router bgp 100
Router(config-bgp)#router-id 209.165.201.1
Router(config-bgp)#bgp graceful-restart
Router(config-bgp)#address-family ipv4 unicast
Router(config-bgp-af)#redistribute connected
Router(config-bgp-af)#network 209.165.200.225/27
Router(config-bgp-af)#allocate-label all
Router(config-bgp-af)#exit
Router(config-bgp)#address-family ipv6 unicast
Router(config-bgp-af)#allocate-label all
Router(config-bgp-af)#exit
Router(config-bgp)#neighbor-group spines
Router(config-bgp-nbrgrp)#remote-as 100
Router(config-bgp-nbrgrp)#update-source loopback0
Router(config-bgp-nbrgrp)#address-family ipv4 labeled-unicast multipath
Router(config-bgp-nbrgrp-af)#exit
Router(config-bgp-nbrgrp)#address-family ipv6 labeled-unicast multipath
Router(config-bgp-nbrgrp-af)#exit
Router(config-bgp-nbrgrp)#address-family l2vpn evpn
Router(config-bgp-nbrgrp-af)#advertise vpnv4 unicast re-originated
Router(config-bgp-nbrgrp-af)#advertise vpnv6 unicast re-originated
Router(config-bgp-nbrgrp-af)#exit
Router(config-bgp-nbrgrp)exit
Router(config-bgp)neighbor 209.165.200.225
Router(config-bgp-nbr)#use neighbor-group spines
Router(config-bgp-nbr)#commit

/* Configure VPN4 address-family */
Router(config)#router bgp 100
Router(config-bgp)#router-id 209.165.201.1
Router(config-bgp)#ibgp policy out enforce-modifications
Router(config-bgp)#address-family vpnv4 unicast
Router(config-bgp-af)#commit

/* Configure EVPN instance and ESI */
Router#configure
Router(config)#evpn
Router(config-evpn)#evi 100
Router(config-evpn-instance)#advertise-mac
Router(config-evpn-instance-mac)#exit
Router(config-evpn-instance)#exit
Router(config-evpn)#interface Bundle-Ether1
Router(config-evpn-ac)#ethernet-segment identifier type 0 aa.aa.aa.aa.aa.aa.aa.aa.ac
Router(config-evpn-ac-es)#bgp route-target 0011.0011.0012
Router(config-evpn-ac)#commit

/* Configure BVI (IRB) Interface */
Router#configure
Router(config)#interface BVI200
Router(config-if)#ipv4 address 192.0.2.1 255.255.255.0
Router(config-if)#commit

/*  Configure VRF */
Router# configure
Router(config)# vrf vpn2
Router(config-vrf)# address-family ipv4 unicast
Router(config-vrf-af)# import route-target 81:2
Router(config-vrf-af)# exit
Router(config-vrf)# address-family ipv6 unicast
Router(config-vrf-af)# import route-target 81:2
```

```
Router(config-vrf-af)# commit

/* Configure BVI with VRF */
Router(config)# interface BVI200
Router(config-if)# host-routing
Router(config-if)# vrf vpn72
Router(config-if-vrf)# ipv4 address ipv4 address 192.0.2.1 255.255.255.0
Router(config-if-vrf)# mac-address 10.1111.1
Router(config-if)# commit

/* Configure VRF under BGP */
Router(config)# router bgp 100
Router(config-bgp)# vrf vpn2
Router(config-bgp-vrf)# rd 102:2
Router(config-bgp-vrf)# address-family ipv4 unicast
Router(config-bgp-vrf-af)# label mode per-vrf
Router(config-bgp-vrf-af)# maximum-paths ibgp 8
Router(config-bgp-vrf-af)# redistribute connected
Router(config-bgp-vrf-af)# exit
Router(config-bgp-vrf)# address-family ipv6 unicast
Router(config-bgp-vrf-af)# label mode per-vrf
Router(config-bgp-vrf-af)# maximum-paths ibgp 8
Router(config-bgp-vrf-af)# redistribute connected
Router(config-bgp-vrf-af)# commit

/* Configure bridge domain and associate with attachment circuits and EVPN instance */
Router(config)#l2vpn
Router(config-l2vpn)#bridge group bg1
Router(config-l2vpn-bg)#bridge-domain bd1
Router(config-l2vpn-bg-bd)#interface BundleEther1.100
Router(config-l2vpn-bg-bd-ac)#evi 100
Router(config-l2vpn-bg-bd-evi)#commit

/* Configure bridge domain and associate with attachment circuits, EVPN instance and BVI
 */
Router(config)#l2vpn
Router(config-l2vpn)#bridge group bg2
Router(config-l2vpn-bg)#bridge-domain bd2
Router(config-l2vpn-bg-bd)#interface TenGigE0/0/0/38.200
Router(config-l2vpn-bg-bd-ac)#routed interface BVI200
Router(config-l2vpn-bg-bd-bvi)#evi 200
Router(config-l2vpn-bg-bd-bvi)#commit
Router(config-l2vpn-bg-bd-bvi)#exit

Router(config)#l2vpn
Router(config-l2vpn)#bridge group bg3
Router(config-l2vpn-bg)#bridge-domain bd3
Router(config-l2vpn-bg-bd)#interface TenGigE0/0/0/38.202
Router(config-l2vpn-bg-bd-ac)#routed interface BVI202
Router(config-l2vpn-bg-bd-bvi)#evi 202
Router(config-l2vpn-bg-bd-bvi)#commit

/* Configure EVPN VPWS */
Router#configure
Router(config)#router bgp 100
Router(config-bgp)#neighbor-group spines
Router(config-bgp-nbrgrp)#remote-as 100
Router(config-bgp-nbrgrp)#update-source loopback0
Router(config-bgp-nbrgrp)#address-family ipv4 labeled-unicast multipath
Router(config-bgp-nbrgrp-af)#exit
Router(config-bgp-nbrgrp)#address-family ipv6 labeled-unicast multipath
Router(config-bgp-nbrgrp-af)#exit
Router(config-bgp-nbrgrp)#address-family l2vpn evpn
```

```
Router(config-bgp-nbrgrp-af)#exit
Router(config-bgp-nbrgrp)exit
Router(config-bgp)neighbor 209.165.200.225
Router(config-bgp-nbr)#use neighbor-group spines
Router(config-bgp-nbr)#commit
Router(config-bgp-af)#exit
Router(config-bgp)#exit
Router(config)#l2vpn
Router(config-l2vpn)#xconnect group aa-evpn-vpws
Router(config-l2vpn-xc)#p2p vpws_513
Router(config-l2vpn-xc-p2p)#interface Bundle-Ether1.513
Router(config-l2vpn-xc-p2p)#neighbor evpn evi 513 target 513 source 513
Router(config-l2vpn-xc-p2p)# commit
```

実行コンフィギュレーション

この項では、フラッディング無効化の実行コンフィギュレーションを示します。

```
/* Configure IGP */
router ospf 1
 router-id 209.165.201.1
 area 10
  interface Loopback0
  !
  interface TenGigE0/0/0/1
  !
  interface TenGigE0/0/0/17
  !
 !
/* Configure BGP */
router bgp 100
 router-id 209.165.201.1
 bgp graceful-restart
 address-family ipv4 unicast
  redistribute connected
  network 209.165.200.225/27
  allocate-label all
address-family ipv6 unicast
  allocate-label all
neighbor-group spines
  remote-as 100
  update-source loopback0
  address-family ipv4 labeled-unicast multipath
  !
  address-family ipv6 labeled-unicast multipath
  !
  address-family l2vpn evpn
   advertise vpnv4 unicast re-originated
   advertise vpnv6 unicast re-originated
 !
 neighbor 209.165.200.225
  use neighbor-group spines
!

/* Configure VPN4 address-family */
router bgp 100
 router-id 209.165.201.1
 ibgp policy out enforce-modifications
 address-family vpnv4 unicast
!

/* Configure EVPN instance and ESI */
```

```
evpn
 evi 100
  advertise-mac
 !
 interface Bundle-Ether1
  ethernet-segment
   identifier type 0 aa.aa.aa.aa.aa.aa.aa.aa.ac
   bgp route-target 0011.0011.0012
  !
 !
!

/* Configuring BVI (IRB) Interface */
configure
 interface BVI200
  ipv4 address 192.0.2.1 255.255.255.0

/* Configure VRF */
vrf vpn2
 address-family ipv4 unicast
  import route-target 81:2
  !
  !
!
 address-family ipv6 unicast
  import route-target 81:2
  !
  !
!

/* Configure BVI with VRF */
interface BVI200
 host-routing
 vrf vpn72
  ipv4 address ipv4 address ipv4 address 192.0.2.1 255.255.255.0
   mac-address 10.1111.1
!

/* Configure VRF under BGP */
router bgp 100
 vrf vpn2
  rd 102:2
  address-family ipv4 unicast
   label mode per-vrf
   maximum-paths ibgp 8
   redistribute connected
  !
  address-family ipv6 unicast
   label mode per-vrf
   maximum-paths ibgp 8
   redistribute connected
  !
!

/* Configure bridge domain and associate with attachment circuits and EVPN instance */
l2vpn
 bridge group bg1
  bridge-domain b1
   interface Bundle-Ether1.100
   !
   evi 100

/*
bridge group bg2
```

```
  bridge-domain bd2
   interface TenGigE0/0/0/38.200
   !
   routed interface BVI200
   !
   evi 200
   !
  !

/* Configurige bridge domain and associate with attachment circuits, EVPN instance and
BVI */
bridge group bg3
  bridge-domain bd3
   interface TenGigE0/0/0/38.202
   !
   routed interface BVI202
   !
   evi 202
   !
  !
 !

/* Configure EVPN VPWS */
configure
 router bgp 100
  neighbor-group spines
  remote-as 100
  update-source Loopback0
  address-family ipv4 labeled-unicast multipath
  !
  address-family ipv6 labeled-unicast multipath
  !
  address-family l2vpn evpn

neighbor 209.165.200.225
   use neighbor-group spines
 !
!
 l2vpn
  xconnect group aa-evpn-vpws
   p2p vpws_513
    interface Bundle-Ether1.513
    neighbor evpn evi 513 target 513 source 513
```

確認

BGP-LUアンダーレイ機能によりEVPNブリッジングとVPWSサービスが正しく設定されていることを確認します。

```
Router#show cef vrf AIM9 10.0.0.1
Tue Jan 20 22:00:56.233 UTC
10.0.0.1/8, version 4, internal 0x5000001 0x0 (ptr 0x97d34b44) [1], 0x0 (0x0), 0x208
(0x98bef0f0)
 Updated Mar 18 06:01:46.175
 Prefix Len 32, traffic index 0, precedence n/a, priority 3
   via 10.0.0.3/8, 7 dependencies, recursive, bgp-multipath [flags 0x6080]
    path-idx 0 NHID 0x0 [0x972c6f08 0x0]
    recursion-via-/32
    next hop VRF - 'default', table - 0xe0000000
    next hop 10.0.0.3/8 via 16448/0/21
     next hop 192.0.2.1/24 BE128        labels imposed {16111 64013 80002}
```

```
   via 100.0.0.88/32, 7 dependencies, recursive, bgp-multipath [flags 0x6080]
    path-idx 1 NHID 0x0 [0x972c6d68 0x0]
    recursion-via-/32
    next hop VRF - 'default', table - 0xe0000000
    next hop 10.0.0.4/8 via 16488/0/21
     next hop 192.0.2.1/24 BE128        labels imposed {16111 64009 80002}

Router#show l2vpn xconnect group aa-evpn-vpws xc-name vpws_513 detail
Wed Jan 22 13:14:05.878 GMT+4

Group aa-evpn-vpws, XC vpws_513, state is up; Interworking none
  AC: Bundle-Ether1.513, state is up
    Type VLAN; Num Ranges: 1
    Rewrite Tags: []
    VLAN ranges: [513, 513]
    MTU 1500; XC ID 0xa00005f7; interworking none
    Statistics:
      packets: received 0, sent 0
      bytes: received 0, sent 0
      drops: illegal VLAN 0, illegal length 0
  EVPN: neighbor 24000, PW ID: evi 513, ac-id 513, state is up ( established )
    XC ID 0xc0000001
    Encapsulation MPLS
    Source address 209.165.200.225
    Encap type Ethernet, control word enabled
    Sequencing not set
    LSP : Up
EVPN          Local      Remote
-----------------------------------
Label         29045      1048577
MTU           1500       1500
Control word  enabled    enabled
AC ID         513        513
EVPN type     Ethernet   Ethernet
-----------------------------------

Router# show evpn internal-label vpn-id 513 detail
Tue Jan 28 13:22:19.110 GMT+4

VPN-ID  Encap Ethernet Segment Id          EtherTag  Label
-----------------------------------------------------------------
513      MPLS 0099.9900.0000.0000.9999        0      None
 Multi-paths resolved: FALSE (Remote all-active)
 Multi-paths Internal label: None
  EAD/ES  10.0.0.5                            0

513 MPLS   0099.9900.0000.0000.9999          513    24000
 Multi-paths resolved: TRUE (Remote all-active)
 Multi-paths Internal label: 24000
 EAD/ES 10.0.0.5                             0
 EAD/EVI (P) 10.0.0.5                      29104
 Summary pathlist:
0xffffffff (P) 10.0.0.5                    29104
-----------------------------------------------------------------

Router# show mpls forwarding labels 24000 hardware egress detail location 0/0/CPU0

Tue Jan 28 13:22:19.110 GMT+4
Label  Label       or ID              Interface       Switched
-----------------------------------------------------------------
24000  29104       EVPN:513            10.0.0.5       N/A
     Updated: Oct 18 13:14:02.193
     Version: 137839, Priority: 3
     Label Stack (Top -> Bottom): { 29104 }
```

```
     NHID: 0x0, Encap-ID: 0x140ea00000002, Path idx: 0, Backup path idx: 0, Weight: 0
     MAC/Encaps: 0/4, MTU: 0
     Packets Switched: 0


 LEAF - HAL pd context :
 sub-type : MPLS, ecd_marked:0, has_collapsed_ldi:0
 collapse_bwalk_required:0, ecdv2_marked:0,
HW Walk:
LEAF:
    PI:0x308de88fb8 PD:0x308de89058 rev:5554240 type: MPLS (2)
    LEAF location: LEM
    FEC key: 0x23e0220000d71
    label action: MPLS_NOP
LWLDI:
        PI:0x309faa82c8 PD:0x309faa8308 rev:5554239 p-rev:5459825 5459825  ldi
type:EOS0_EOS1
        FEC key: 0x23e0220000d71 fec index: 0x0(0) num paths:2, bkup paths: 0
        Collpased IMP LDI: ECD_MARKED
        IMP pattern:3
        PI:0x309faa82c8 PD:0x309faa8308 rev:5554239 p-rev:5459825 5459825
        FEC key: 0x257c720000d71 fec index: 0x20000003(3) num paths:2
        Path:0  fec index: 0x20018f14(102164) DSP fec index: 0x200001f8(504),
                MPLS encap key: 0xf1b00000400140ea MPLS encap id: 0x400140ea Remote: 0
                Label Stack: 29104 16012  dpa-rev:55458217
        Path:1  fec index: 0x20018f15(102165) DSP fec index: 0x200001f9(505),
                MPLS encap key: 0xf1b00000400140eb MPLS encap id: 0x400140eb Remote: 0
                Label Stack: 29104 16012  dpa-rev:55458218

 REC-SHLDI HAL PD context :
ecd_marked:10, collapse_bwalk_required:0, load_shared_lb:0

    RSHLDI:
        PI:0x3093d16af8 PD:0x3093d16bc8 rev:5494421 dpa-rev:36033167 flag:0x1
        FEC key: 0x249e440000d71 fec index: 0x2001c169(115049) num paths: 1
        p-rev:5459825
        Path:0 fec index: 0x2001c169(115049) DSP fec index: 0x200001f8(504),

 LEAF - HAL pd context :
 sub-type : MPLS, ecd_marked:1, has_collapsed_ldi:0
 collapse_bwalk_required:0, ecdv2_marked:0,

HW Walk:
LEAF:
    PI:0x308de433b8 PD:0x308de43458 rev:5459864 type: MPLS (2)
    LEAF location: LEM
    FEC key: 0

    LWLDI:
        PI:0x309ffe9798 PD:0x309ffe97d8 rev:5459825 p-rev:4927729 4927729  ldi
type:IMP_EOS0_EOS1
        FEC key: 0x1a1c740000d71 fec index: 0x0(0) num paths:2, bkup paths: 0
        IMP LDI: ECD_MARKED  SERVICE_MARKED
        IMP pattern:3
        PI:0x309ffe9798 PD:0x309ffe97d8 rev:5459825 p-rev:4927729 4927729
        FEC key: 0x23e0220000d71 fec index: 0x20000002(2) num paths:2
        Path:0  fec index: 0x2001f8b4(129204) DSP fec index: 0x200001f8(504),
                MPLS encap key: 0xf1b0000040013ef0 MPLS encap id: 0x40013ef0 Remote: 0
                Label Stack: 16012  dpa-rev:35993054.  <<< LU Label>>>>
        Path:1  fec index: 0x2001f8b5(129205) DSP fec index: 0x200001f9(505),
                MPLS encap key: 0xf1b0000040013ef2 MPLS encap id: 0x40013ef2 Remote: 0
                Label Stack: 16012  dpa-rev:35993055  <<< LU Label>>>>
```

```
 REC-SHLDI HAL PD context :
ecd_marked:10, collapse_bwalk_required:0, load_shared_lb:0

    RSHLDI:
        PI:0x308dd32c38 PD:0x308dd32d08 rev:4927729 dpa-rev:35005343 flag:0x3
        FEC key: 0x1a1c740000d71 fec index: 0x20000813(2067) num paths: 2
        p-rev:4926086
        Path:0 fec index: 0x2001eefd(126717) DSP fec index: 0x200001f8(504),
        Path:1 fec index: 0x2001eefe(126718) DSP fec index: 0x200001f9(505),
LEAF - HAL pd context :
 sub-type : MPLS, ecd_marked:1, has_collapsed_ldi:0
 collapse_bwalk_required:0, ecdv2_marked:0,
HW Walk:
LEAF:
    PI:0x308dde33b8 PD:0x308dde3458 rev:4924403 type: MPLS (2)
    LEAF location: LEM
    FEC key: 0

    LWLDI:
       PI:0x308b04ea58 PD:0x308b04ea98 rev:4924400 p-rev:4924389 4924389 4924389 4924389
  ldi type:IMP_EOS0_EOS1
        FEC key: 0x1a75340000d71 fec index: 0x0(0) num paths:4, bkup paths: 0
        IMP LDI: ECD_MARKED
        IMP pattern:3
       PI:0x308b04ea58 PD:0x308b04ea98 rev:4924400 p-rev:4924389 4924389 4924389 4924389

        FEC key: 0x1a74720000d71 fec index: 0x200001f8(504) num paths:4
        Path:0  fec index: 0x2001ee86(126598) DSP:0x21
                MPLS encap key: 0xf1b0000040015878 MPLS encap id: 0x40015878 Remote: 0
                Label Stack: 16005  dpa-rev:34999715
        Path:1  fec index: 0x2001ee87(126599) DSP:0x22
                MPLS encap key: 0xf1b000004001587a MPLS encap id: 0x4001587a Remote: 0
                Label Stack: 16005  dpa-rev:34999716
        Path:2  fec index: 0x2001ee88(126600) DSP:0xc000002
                MPLS encap key: 0xf1b0000040016980 MPLS encap id: 0x40016980 Remote: 0
                Label Stack: 16005  dpa-rev:34989935
        Path:3  fec index: 0x2001ee89(126601) DSP:0xc000003
                MPLS encap key: 0xf1b00000400157fc MPLS encap id: 0x400157fc Remote: 0
                Label Stack: 16005  dpa-rev:34989936

SHLDI:
            PI:0x30927740c8 PD:0x3092774198 rev:4924389 dpa-rev:34999705 flag:0x0
           FEC key: 0x1a75340000d71 fec index: 0x200001ff(511) num paths: 4 bkup paths:
 0
            p-rev:4924311 4924329 8779 4920854
            Path:0 fec index: 0x2001ee8f(126607) DSP:0x21 Dest fec index: 0x0(0)
            Path:1 fec index: 0x2001ee90(126608) DSP:0x22 Dest fec index: 0x0(0)
            Path:2 fec index: 0x2001ee91(126609) DSP:0xc000002 Dest fec index: 0x0(0)
            Path:3 fec index: 0x2001ee92(126610) DSP:0xc000003 Dest fec index: 0x0(0)
TX-NHINFO:
                PI: 0x308dc51298 PD: 0x308dc51318 rev:4924311 dpa-rev:34994174 Encap
hdl: 0x3091632e98
                Encap id: 0x40010003 Remote: 0 L3 int: 1670 flags: 0x3
                npu_mask: 0x1 DMAC: 84:78:ac:2d:f8:1f

            TX-NHINFO:
                PI: 0x308dc51c20 PD: 0x308dc51ca0 rev:4924329 dpa-rev:34994264 Encap
hdl: 0x30916332c8
                Encap id: 0x40010001 Remote: 0 L3 int: 1679 flags: 0x3
                npu_mask: 0x1 DMAC: d4:6d:50:7c:f9:4d

            TX-NHINFO:
                PI: 0x308dc51ff0 PD: 0x308dc52070 rev:8779 dpa-rev:61964 Encap hdl:
0x308e9f4980
```

```
                Encap id: 0x40010007 Remote: 0 L3 int: 1728 flags: 0x807
                npu_mask: 0x1 DMAC: 84:78:ac:2d:f8:22

            TX-NHINFO:
                PI: 0x308dc51480 PD: 0x308dc51500 rev:4920854 dpa-rev:34989846 Encap
hdl: 0x308e9f4db0
                Encap id: 0x40010005 Remote: 0 L3 int: 1727 flags: 0x807
                npu_mask: 0x1 DMAC: 40:55:39:11:37:39

 LEAF - HAL pd context :
 sub-type : MPLS, ecd_marked:1, has_collapsed_ldi:0
 collapse_bwalk_required:0, ecdv2_marked:0,
HW Walk:
LEAF:
    PI:0x308dde35b8 PD:0x308dde3658 rev:4926089 type: MPLS (2)
    LEAF location: LEM
    FEC key: 0

    LWLDI:
       PI:0x308b04eb48 PD:0x308b04eb88 rev:4926086 p-rev:4924389 4924389 4924389 4924389
  ldi type:IMP_EOS0_EOS1
        FEC key: 0x1a75340000d71 fec index: 0x0(0) num paths:4, bkup paths: 0
        IMP LDI: ECD_MARKED
        IMP pattern:3
       PI:0x308b04eb48 PD:0x308b04eb88 rev:4926086 p-rev:4924389 4924389 4924389 4924389

        FEC key: 0x1a74820000d71 fec index: 0x200001f9(505) num paths:4
        Path:0  fec index: 0x2001ee81(126593) DSP:0x21
                MPLS encap key: 0xf1b000004001587c MPLS encap id: 0x4001587c Remote: 0
                Label Stack: 16006  dpa-rev:35002526
        Path:1  fec index: 0x2001ee82(126594) DSP:0x22
                MPLS encap key: 0xf1b000004001588a MPLS encap id: 0x4001588a Remote: 0
                Label Stack: 16006  dpa-rev:35002527
        Path:2  fec index: 0x2001ee83(126595) DSP:0xc000002
                MPLS encap key: 0xf1b0000040016964 MPLS encap id: 0x40016964 Remote: 0
                Label Stack: 16006  dpa-rev:34991843
        Path:3  fec index: 0x2001ee84(126596) DSP:0xc000003
                MPLS encap key: 0xf1b00000400157fe MPLS encap id: 0x400157fe Remote: 0
                Label Stack: 16006  dpa-rev:34991844
SHLDI:
            PI:0x30927740c8 PD:0x3092774198 rev:4924389 dpa-rev:34999705 flag:0x0
           FEC key: 0x1a75340000d71 fec index: 0x200001ff(511) num paths: 4 bkup paths:
 0
            p-rev:4924311 4924329 8779 4920854
            Path:0 fec index: 0x2001ee8f(126607) DSP:0x21 Dest fec index: 0x0(0)
            Path:1 fec index: 0x2001ee90(126608) DSP:0x22 Dest fec index: 0x0(0)
            Path:2 fec index: 0x2001ee91(126609) DSP:0xc000002 Dest fec index: 0x0(0)
            Path:3 fec index: 0x2001ee92(126610) DSP:0xc000003 Dest fec index: 0x0(0)

            TX-NHINFO:
                PI: 0x308dc51298 PD: 0x308dc51318 rev:4924311 dpa-rev:34994174 Encap
hdl: 0x3091632e98
                Encap id: 0x40010003 Remote: 0 L3 int: 1670 flags: 0x3
                npu_mask: 0x1 DMAC: 84:78:ac:2d:f8:1f

            TX-NHINFO:
                PI: 0x308dc51c20 PD: 0x308dc51ca0 rev:4924329 dpa-rev:34994264 Encap
hdl: 0x30916332c8
                Encap id: 0x40010001 Remote: 0 L3 int: 1679 flags: 0x3
                npu_mask: 0x1 DMAC: d4:6d:50:7c:f9:4d

            TX-NHINFO:
                PI: 0x308dc51ff0 PD: 0x308dc52070 rev:8779 dpa-rev:61964 Encap hdl:
0x308e9f4980
```

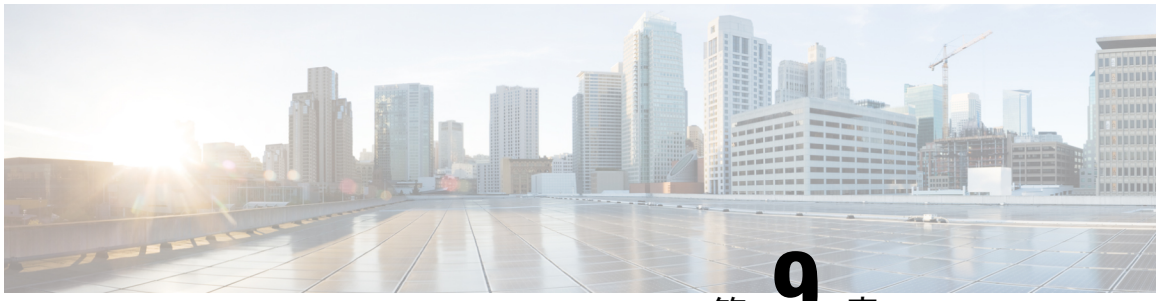
```
                Encap id: 0x40010007 Remote: 0 L3 int: 1728 flags: 0x807
                npu_mask: 0x1 DMAC: 84:78:ac:2d:f8:22

            TX-NHINFO:
                PI: 0x308dc51480 PD: 0x308dc51500 rev:4920854 dpa-rev:34989846 Encap
hdl: 0x308e9f4db0
                Encap id: 0x40010005 Remote: 0 L3 int: 1727 flags: 0x807
                npu_mask: 0x1 DMAC: 40:55:39:11:37:39
```

関連項目

BGP-LU アンダーレイを介した EVPN ブリッジングおよび VPWS サービス （228 ページ）

関連コマンド

- show l2vpn bridge-domain
- show bgp l2vpn evpn neighbors
- show cef vrf

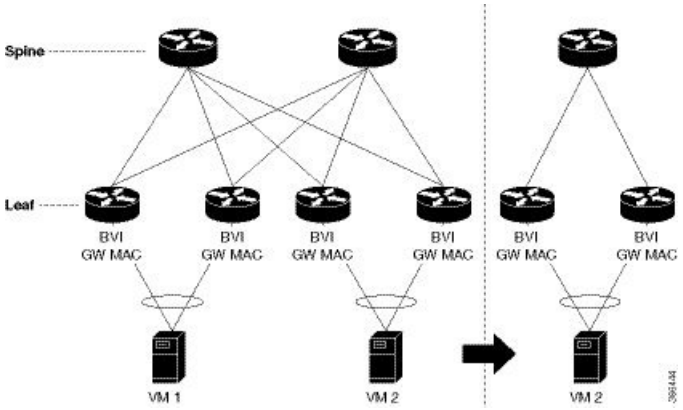


第 9 章

EVPN IRB

EVPN IRB 機能はレイヤ 2 VPN とレイヤ 3 VPNのオーバーレイを可能にし、オーバーレイ全体のエンド ホストが同じサブネット内や VPN 内の異なるサブネットにまたがって互いに通信できるようにします。

図 *35 : EVPN IRB*



EVPN IRB の利点は、IP サブネット内のホストをデータセンター内のどこでもプロビジョニングできることです。EVPN PE の背後でサブネット内の仮想マシン（VM）をプロビジョニングしており、同じサブネット内に別の VM が必要な場合は、別の EVPN PE の背後でプロビジョニングできます。VM をローカライズする必要はありません。直接接続する必要もありません。同じ複合体内に配置する必要もありません。VM は同じサブネット内で移動できます。すべての EVPN PE 全体にわたる IP MPLS ネットワークの可用性によって、VM モビリティのプロビジョニングが可能です。EVPN PE は、MPLS カプセル化を通じてトラフィックを相互にルーティングします。

EVPN PE はスパインによって相互に接続されるため、互いのループバック インターフェイスへの IP 到達可能性を備えています。これらの EVPN PE 間に存在する IP ネットワークと MPLS トンネルが IP MPLS アンダーレイ ファブリックを構成します。

レイヤ 2 トラフィックをトンネリングするように MPLS トンネルを設定することと、これらのトンネルに VPN をオーバーレイすることが可能です。EVPN コントロール プレーンは、VPN のコンテキスト内でレイヤ 2 の MAC 到達可能性とレイヤ 3 の IP 到達可能性の両方をホストにもたらします。つまり、MPLS アンダーレイ ファブリック上にテナントの VPN ネットワーク

をオーバーレイします。したがって、同じサブネット レイヤ 2 ドメイン内にあってもファブリック全体に分散されて、レイヤ2ネットワーク内に存在するかのように互いに通信するテナントのホストを配置できます。

レイヤ 2 VLAN と対応する IP サブネットはレイヤ 2 リンク上で物理的に接続されているホストのネットワークであるのみでなく、データセンター全体に展開している下層の IP MPLS ファブリックの上部のオーバーレイ ネットワークでもあります。

ファブリック全体でのサブネットのストレッチを可能にするルーティング サービスを使用できます。また、レイヤ 3 VPN を提供し、レイヤ 3 VPN のコンテキスト内でサブネット間のルーティングを実行します。EVPN PE は、ファブリック全体にストレッチされているレイヤ 2 ドメイン内のファブリック全体に展開しているホスト間にレイヤ2ブリッジング サービスと、レイヤ 3 VPN 内のさまざまなサブネット内のホストにレイヤ 3 VPN サービスまたはサブネット間ルーティング サービスを提供します。たとえば、上のトポロジ図に示したように、2 つの VM が同じサブネット内にあっても、レイヤ 2 リンクを通じて互いに直接していない場合があります。レイヤ2リンクは、それらを接続している MPLS トンネルで置き換えられます。ファブリック全体は単一のスイッチとして機能し、1 つの VM から別の VM にトラフィックをブリッジします。これも VM モビリティを可能にします。

（注） ブリッジ ドメイン内の L2 インターフェイスでは出力マーキングはサポートされていません。

上のトポロジ図では、VM、VM1 と VM2 が相互に接続されています。VM2 が別のスイッチおよび別のサーバに移行する場合、その VM の現在の MAC アドレスと IP アドレスはそのまま保たれます。サブネットが 2 つの EVPN PE 間にストレッチされている場合、同じ IRB 設定が両方のデバイスに適用されます。

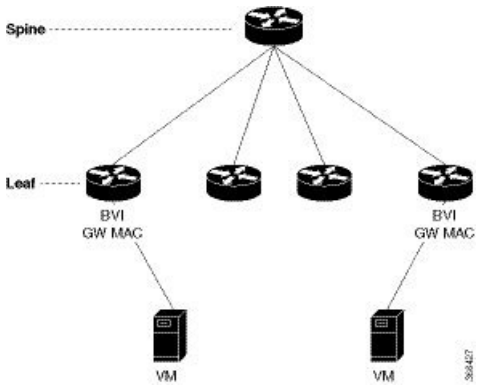
同じサブネット内でのストレッチングの場合は、AC インターフェイスと EVI を設定する必要があります。これは IRB インターフェイスや VRF の設定には必要ありません。

• IRB での DHCPv6 リレー IAPD （291 ページ）
• セッション冗長性を使用したオールアクティブ マルチホーミング対応 DHCPv6 PD 同期（294 ページ）
• DHCPv6 リレーにおける IAPD ルートの配布と取り消し （297 ページ）

EVPN シングルホーミング アクセス ゲートウェイ

EVPN プロバイダー エッジ（PE）デバイスは、カスタマー エッジ（CE）デバイスから受信する ARP トラフィックから MAC アドレスと IP アドレスを学習します。PE は MAC + IP ルートを作成します。PE は MAC + IP ルートを MPLS コアにアドバタイズします。これらはホスト IP ルートを IP-VPN ゲートウェイに挿入します。ホスト ルートの他に、アクセス EVPN PE からはサブネット ルートもアドバタイズされます。すべての PE ノードが IP-VRF テーブルにホスト ルートを追加します。EVPN PE ノードは、MAC-VRF テーブルに MAC ルートを追加します。IP-VPN PE は、サブネット ルートをプロバイダー エッジ デバイスにアドバタイズし、そのデバイスがサブネット ルートを IP VPN テーブルに追加します。PE デバイス上では、IRB ゲートウェイ IP アドレスと MAC アドレスは BGP を通じてアドバタイズされません。IRB ゲートウェイ IP アドレスまたは MAC アドレスは、データセンター CE への ARP 要求の送信に使用されます。

図 *36 : EVPN* シングルホーミング アクセス ゲートウェイ



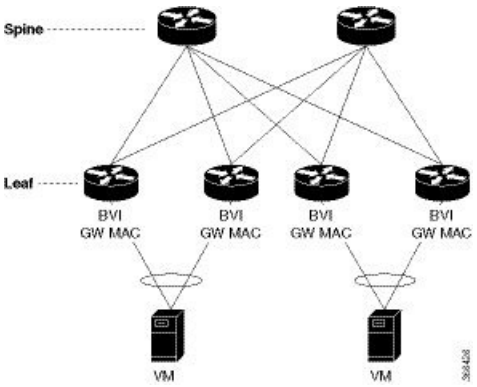
上記は、CE デバイスによる PE デバイス 1 台への接続を許可することによって EVPN シングルホーミング アクセス ゲートウェイがネットワーク接続を有効にするトポロジを示しています。PE デバイスはバンドルインターフェイスまたは物理インターフェイスを通じてイーサネット セグメントに接続されます。シングルホーミングにはヌル イーサネット セグメント識別子（ESI）を使用します。

EVPN マルチホーミング オールアクティブ

EVPN IRB では、EVPN と IP VPN の両方（VPNv4 と VPNv6 の両方）のアドレス ファミリがルータとデータセンターインターコネクト（DCI）ゲートウェイの間で有効になっています。レイヤ 2（L2）ストレッチが複数のデータセンター（DC）で使用できないときは、VPNv4 ルートまたは VPNv6 ルートを通じてルーティングが確立されます。レイヤ 2 ストレッチが使用で

きるときは、IP-MAC ルートを ARP で学習して EVPN/BGP に配布する場合にホスト ルーティングが適用されます。リモート ピア ゲートウェイでは、これらの IP-MAC EVPN ルートがセカンダリ ラベルとレイヤ 3 VRF ルートターゲットとともに EVPN ルートタイプ 2 ルートから IP VPN ルーティング テーブルにインポートされます。

図 *37 : EVPN* マルチ ホーミング オールアクティブ

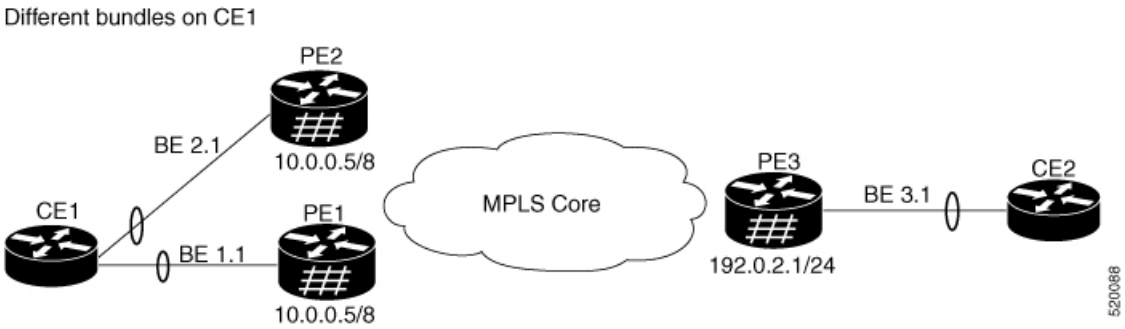


上記は、CE デバイスによる複数の PE デバイスへの接続を許可することによって、EVPN マルチホーム アクセス ゲートウェイが冗長ネットワーク接続を有効にするトポロジです。CE デバイスが 1 台の PE デバイス、またはマルチホーミングにより複数の PE デバイスに接続できるようにすることによってネットワーク接続の中断を防ぎます。イーサネットセグメントは一連のイーサネット リンクであり、それを通じて CE デバイスが複数の PE デバイスに接続されます。オールアクティブ リンク アグリゲーション グループ バンドルはイーサネット セグメントとして動作します。2 台のシャーシ間で動作する MC バンドルのみがサポートされています。

エニーキャストゲートウェイ IRB の EVPN シングルアクティブ マルチホーミング

エニーキャストゲートウェイ IRB の EVPN シングルアクティブ マルチホーミング機能は、シングルアクティブ冗長モードをサポートしています。このモードでは、プロバイダーエッジ（PE）ノードは、EVPN サービスインスタンス（EVI）に基づいて、イーサネットセグメントとの間で発着信するイーサネット セグメント ロードバランス トラフィックにローカルに接続されます。EVPN サービスインスタンス内では、1 つの PE のみがイーサネットセグメント（ES）との間で発着信するトラフィックを転送します。この機能は、サブネット間シナリオのみをサポートします。

図 *38 : EVPN* : エニーキャストゲートウェイ *IRB* の *EVPN* シングルアクティブ マルチホーミング



CE1 が PE1 や PE2 にマルチホームされているトポロジについて考えてみます。バンドル イーサネット インターフェイスは BE 1.1、BE 2.1 です。入力インターフェイスは CE1 上の同じスイッチングドメインに属している必要があります。これらのピアリング PE の両方で、ホストルーティングを有効にし、エニーキャストゲートウェイ IP アドレスを設定します。PE1 と PE2 は MPLS コアを通じて PE3 に接続しています。PE3 は、サブネット 10.0.0.5/8 から両方のピアリング PE に到達可能です。ピアリング PE は、PE3 サブネット 192.0.2.1/24 に到達可能です。CE2 はイーサネット インターフェイス バンドルを通じて PE3 に接続されています。PE1 と PE2 はタイプ 4 ルートをアドバタイズしてから、指定フォワーダ（DF）の選択を実行します。非 DF はシングルアクティブ モードの両方向のトラフィックをブロックします。

CE1 から CE2 へのトラフィック フローを考えてみます。CE1 は PE1 と PE2 の両方に Address Resolution Protocol（ARP）ブロードキャスト要求を送信します。ピアリング PE は、共有 ESI に対して指定フォワーダー（DF）の選択を実行します。PE1 が EVI の指定フォワーダである場合、PE1 は CE1 からの ARP 要求に応答します。PE2 は CE1 からのトラフィックをドロップします。その後で、すべてのユニキャスト トラフィックが PE1 を通じて送信されます。PE2 は、スタンバイ状態またはブロック状態に設定されており、トラフィックはこのパスを介して送信されません。PE1 は PE3 に MAC をアドバタイズします。PE3 は常に PE1 を通じてトラフィックを送受信します。PE3 はイーサネット インターフェイス バンドルを介してトラフィックを CE2 に送信します。BE1 に障害が発生した場合、PE2 は、PE2 を通過する DF およびトラフィック フローになります。

EVPN シングルアクティブ マルチホーミングの設定

EVPN シングルアクティブ マルチホーミング機能を設定するには、PE1 と PE2 上で次のタスクを実行します。

- ホストルーティングを使用した EVPN IRB の設定
- EVPN イーサネット セグメントの設定
- レイヤ 2 インターフェイスの設定
- ブリッジ ドメインの設定
- VRF の設定

ホストルーティングを使用した EVPN IRB の設定

ホストルーティングを使用して EVPN IRB を設定するには、次のタスクを実行します。

設定例

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group 6005
Router(config-l2vpn-bg)# bridge-domain 6005
Router(config-l2vpn-bg-bd)# routed interface BVI50
Router(config-l2vpn-bg-bd-bvi)# exit
Router(config-l2vpn-bg-bd-bvi)# interface Bundle-Ether2.1
Router(config-l2vpn-bg-bd-ac)# evi 6005
Router(config-l2vpnbg-bd-evi)# commit
Router(config-l2vpnbg-bd-evi)# exit
Router(config)# interface BVI50
Router(config-if)# host-routing
Router(config-if)# vrf 30
Router(config-if)# ipv4 address 10.0.0.5 255.0.0.0
Router(config-if)# local-proxy-arp
Router(config-if)# mac-address 1.1.1
Router(config-if)# comit
```

実行コンフィギュレーション

この項では、EVPN IRB の実行コンフィギュレーションを示します。

```
configure
l2vpn
 bridge group 6005
  bridge-domain 6005
   interface Bundle-Ether2.1
    evi 6005
!
   !
 interface BVI34
 host-routing
 vrf 30
 ipv4 address 10.0.0.5 255.0.0.0
 arp learning local
 local-proxy-arp
 mac-address 1.1.1
```

EVPN イーサネット セグメントの設定

EVPN イーサネット セグメントを設定するには、次のタスクを実行します。

```
Router# configure
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether1
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 40.00.00.00.00.00.00.00.01
Router(config-evpn-ac-es)# load-balancing-mode single-active
Router(config-evpn-ac-es)# bgp route-target 4000.0000.0001
Router(config-evpn-ac-es)# comit
```

実行コンフィギュレーション

```
configure
evpn
 interface Bundle-Ether1
   ethernet-segment
    identifier type 0 40.00.00.00.00.00.00.00.01
    load-balancing-mode single-active
    bgp route-target 4000.0000.0001
    !
!
!
```

EVPN サービス インスタンス（EVI）パラメータの設定

EVPN サービス インスタンス（EVI）パラメータを定義するには、このタスクを実行します。

```
Router# configure
Router(config)# evpn
Router(config-evpn)# evi 6005
Router(config-evpn-evi)# bgp
Router(config-evpn-evi-bgp)# rd 200:50
Router(config-evpn-evi-bgp)# route-target import 100:6005
Router(config-evpn-evi-bgp)# route-target export 100:6005
Router(config-evpn-evi-bgp)# commit
```

実行コンフィギュレーション

```
configure
 evpn
  evi 6005
   bgp
    rd 200:50
    route-target import 100:6005
    route-target export 100:6005
!
!
```

レイヤ 2 インターフェイスの設定

レイヤ 2 インターフェイスを定義するには、次のタスクを実行します。

```
Router# configure
Router(config)# interface bundle-ether2.1 l2transport
Router(config-subif-l2)# no shutdown
Router(config-subif-l2)# encapsulation dot1q 1
Router(config-subif-l2)# rewrite ingress tag pop 1 symmetric
Router(config-subif-l2)#commit
Router(config-subif-l2)#exit
```

実行コンフィギュレーション

この項では、レイヤ 2 インターフェイスの実行コンフィギュレーションを示します。

```
configure
 interface bundle-ether2.1 l2transport
  no shutdown
```

```
  encapsulation dot1q 1
  rewrite ingress tag pop 1 symmetric
!
```

ブリッジ ドメインの設定

次のステップを実行して PE1 と PE2 上にブリッジ ドメインを設定します。

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group 6005
Router(config-l2vpn-bg)# bridge-domain 6005
Router(config-l2vpn-bg-bd)# interface Bundle-Ether2.1
Router(config-l2vpn-bg-bd-ac)# evi 6005
Router(config-l2vpnbg-bd-evi)# commit
Router(config-l2vpnbg-bd-evi)# exit
```

実行コンフィギュレーション

この項では、ブリッジドレインの実行コンフィギュレーションを示します。

```
configure
l2vpn
 bridge group 6005
  bridge-domain 6005
   interface Bundle-Ether2.1
    evi 6005
!
```

VRF の設定

VRF を設定するには、次のタスクを実行します。

設定例

```
Router# configure
Router(config)# vrf vrf1
Router(config-vrf)# address-family ipv4 unicast
Router(config-l2vpn-vrf-af)# route-target import 100:6005
Router(config-l2vpn-vrf-af)# route-target export 100:6005
Router(config-l2vpn-vrf-af)# commt
```

実行コンフィギュレーション

この項では、VRF の実行コンフィギュレーションを示します。

```
configure
 vrf vrf1
  address-family ipv4 unicast
   route-target import 100:6005
   route-target export 100:6005

!
```

手動 ESI 設定を使用した自動 BGP RT の有効化

以前は、タイプ 0 ESI には ES インポート RT が必須でした。ES インポート RT はデフォルトで自動抽出され、その設定でデフォルト値がオーバーライドされます。この機能は、RFC 7432 に基づいていますが、具体的にはESIタイプ0に適用されます。詳細については、『RFC 7432』のセクション 5 を参照してください。

サポートされている EVPN IRB のシナリオ

EVPN IRB は次のシナリオをサポートしています。

- デュアルホーミングは次のメソッドをサポートしています。
  - EVI あたりの ESI ごとに 1 つの EFP のみがサポートされています。
  - オールアクティブ モードのみがサポートされています。
  - 冗長グループ内の 2 つの PEの ゲートウェイのみ
- シングルホーミングは次のメソッドをサポートしています。
  - 物理
  - VLAN
  - バンドル イーサネット
  - QinQ アクセス
- IPv4 だけがサポートされます。
- EVPN IRB を使用したサブネットストレッチ機能は VRF 内でのみサポートされ、グローバル VRF ではサポートされていません。つまり、EV-LAG マルチホーミングを使用した EVPN IRB は、マルチホーミング リーフを越えてストレッチされるサブネットなしにグローバル VRF でサポートされています。

分散型エニーキャスト ゲートウェイ

所定のサブネットの EVPN IRB は、このサブネット上でホストされているすべての EVPN PE 上に設定されます。最適なルーティングを促進しながら、透過的な仮想マシンモビリティをサポートするには、それらのローカル サブネットの単一のデフォルト ゲートウェイでホストを設定します。その単一の（エニーキャスト）ゲートウェイ アドレスは、そのサブネットをローカルでサポートしているすべての EVPN PE 上の単一の（エニーキャスト）MAC アドレスを使用して設定します。エニーキャスト ゲートウェイ サポートを必要とする、ローカルに定義された各サブネットにこのプロセスが繰り返されます。

ホスト間レイヤ 3 トラフィックは、レイヤ 3 VPN PE-PE 転送と同様に、送信元 EVPN PE で IP または MPLS トンネルを介して宛先 EVPN PE ネクストホップにルーティングされ、直接接続されたホストに再度ルーティングされます。このような転送は対称IRBとも呼ばれます。これは、レイヤ 3 フローが送信元と宛先の両方の EVPN PE でルーティングされるためです。

次に、分散型エニーキャスト ゲートウェイ機能に含まれているソリューションを示します。

ファブリック全体にわたってサブネットストレッチまたはホストルーティングを使用しないオールアクティブ マルチホーミングでの EVPN IRB

一連のマルチホーミング EVPN PE にローカルなサブネットの場合は、VRF がホストしているリモート リーフに EVPN ルート タイプ 5 を使用してアドバタイズされるサブネット ルートを通じて EVPN IRB 分散型エニーキャスト ゲートウェイが確立されます。サブネット内の /32 ルートをアドバタイズする必要はありませんが、ホストMACとARPエントリは、サーバがマルチホームされている EVPN PE 全体にわたって同期されている必要があります。

このタイプのマルチホーミングには、次の特性があります。

- アクセス時のオールアクティブ EV LAG
- サブネット ルートに基づくデュアルホーム接続ホストのファブリック用レイヤの 3 ECMP
- ファブリックを介したレイヤ 2 サブネットのストレッチなし
- 孤立ポートがあるリーフの冗長グループ内のレイヤ 2 ストレッチ

非ストレッチ サブネットのプレフィックスルーティング ソリューションを要約すると次のようになります。

マルチホーミング EVPN PE 全体：

- ローカル ARP キャッシュと MAC アドレスは、EVPN MAC + IP のホスト ルート アドバタイズメントを通じてデュアルホーム接続ホスト用に同期されます。これらはローカルとしてインポートされ、ローカルESIの一致に基づき、アクセス ゲートウェイへの最適な転送を実現します。
- 孤立した MAC アドレスとホスト IP アドレスはファブリックを介してリモート アドレスとしてインストールされます。
- ES/EADルートが指定フォワーダ（DF）選択とスプリットホライゾン ラベルの取得のために交換されます。

リモート EVPN PE 全体：

- デュアルホーム接続の MAC + IP EVPN ルート タイプ 2 は、ESI、EVI ラベル、レイヤ 2 ルート タイプと交換されます。サブネット ストレッチまたはホストルーティングがない場合、これはファブリック全体にはインポートされません。

- サブネット IP EVPN ルート タイプ 5 は VRF ラベルおよびレイヤ 3 ルート タイプと交換されます。
- ローカルにある VRF のレイヤ 3 ルート タイプがインポートされます。
- ローカルにある BD のレイヤ 2 ルート タイプがインポートされます。BD がストレッチされていない場合は、同じ冗長グループ内のリーフからのみインポートされます。

ファブリック全体にわたってサブネットストレッチまたはホストルーティングを使用したオールアクティブ マルチホーミングによる EVPN IRB

リモート EVPN PE の全体にわたってストレッチされているブリッジ ドメインまたはサブネットの場合、/32 ホスト ルートと MAC ルートの両方が EVPN オーバーレイ コントロール プレーンで配布され、ストレッチされているサブネット内のエンドポイントへのレイヤ2およびレイヤ 3 トラフィックを有効にします。

このタイプのマルチホーミングには、次の特性があります。

- アクセス ゲートウェイ上でのオールアクティブ EV-LAG
- ルート タイプ 1 とルート タイプ 2 に基づくデュアルホーム接続ホストの場合のレイヤ 2 または レイヤ 3 ECMP
- ルートタイプ2に基づくシングルホーム接続ホストの場合のファブリックを介したレイヤ 3 ユニパス
- ファブリックを介したレイヤ 2 サブネット ストレッチ
- 孤立ポートがあるリーフの冗長グループ内のレイヤ 2 ストレッチ

次に、ストレッチされているサブネットの MAC およびホストのルーティング ソリューションを要約します。

マルチホーミング EVPN PE 全体：

- ローカル ARP キャッシュと MAC アドレスが EVPN MAC + IP のホスト ルート アドバタイズメントを通じてデュアルホーム接続ホストに対応するために同期されます。これらはローカルとしてインポートされ、ローカル ESI の一致に基づき、アクセス ゲートウェイへの最適な転送を実現します。
- 同期された MAC + IP は、サブネット間レイヤ 3 ECMP に再発信されます。
- 孤立した MAC アドレスとホスト IP アドレスはファブリックを介してリモート アドレスとしてインストールされます。
- ES/EAD ルートが指定フォワーダ（DF）選択とスプリットホライゾン ラベル用に交換されます。

リモート EVPN PE 全体：

- デュアルホーム接続の MAC + IP EVPN ルート タイプ 2 が、ESI、EVI ラベル、レイヤ 2 ルート タイプ、VRF ラベル、およびレイヤ 3 ルート タイプと交換されます。
- サブネット IP EVPN ルート タイプ 5 が、VRF ラベル、サイレント ホストのレイヤ 3 ルート タイプ、およびストレッチされていないサブネット用に交換されます。
- レイヤ 3 ルート タイプがローカルにある VRF 用にインポートされます。
- レイヤ 2 ルート タイプがローカルにあるブリッジ ドメイン用にインポートされます。

MAC および IP ユニキャストのコントロール プレーン

この使用例には次のタイプが含まれています。

プレフィックス ルーティングまたはサブネット ストレッチなし

ファブリック全体への IP 到達可能性は、EVPN ルート タイプ 5 と VPN ラベルおよび VRF RT を使用してアドバタイズされるサブネット プレフィックス ルートを使用して確立されます。ホスト ARP と MAC の同期は、共有 ESI に基づいて MAC + IP ルート タイプ 2 を使用してマルチホーミング EVPN PE の全体にわたって確立され、両方のマルチホーミング EVPN PE を通じたローカル スイッチングを可能にします。

ホスト ルーティングまたはストレッチされたサブネット

ARP を通じてホストが検出されると、MAC と IP ルート タイプ 2 が MAC VRF および IP VRF の両方のルータ ターゲットと、MAC-VRF および IP-VRF の両方の VPN ラベルでアドバタイズされます。特に、VRF ルート ターゲットとレイヤ 3 VPN ラベルがルート タイプ 2 と関連付けられて従来の L3VPN と同じ PE-PE IP ルーティングを実現します。リモート EVPN PE は、レイヤ 3 VPN インポジション PE によく似たレイヤ 3 VPN ラベルのカプセル化による EVPN PE ネクスト ホップのアドバタイズメントを通じて IP/32 エントリをレイヤ 3 VRF テーブルに直接インストールします。このアプローチによって、ストレッチされたサブネット内の各リモート ホストに隣接関係の書き換えを個別にインストールする必要がなくなります。その代わりに、一連の EVPN PE を通じて到達可能なすべての IP ホスト エントリ全体にわたる共通転送書き換えやロードバランスのリソースの共有を可能にするというレイヤ 3 VPN スケールの主要な利点を継承しています。

ARP と MAC の同期

複数の EVPN PE に LAG を通じて接続されているホストの場合、ローカル ホスト ARP と MAC のエントリは、マルチホーミング EVPN PE のいずれか、または両方のデータ プレーンで学習されます。ローカル ARP と MAC エントリは、共有 ESI に基づいて MAC および IP ルート タイプ 2 を使用し、2 つのマルチホーミング EVPN PE 全体にわたって同期されるため、両方のマルチホーミング EVPN PE を通じたローカル スイッチングが可能になります。基本的に、ローカル ESI とともに受信した MAC と IP ルート タイプ 2 によって、ローカル AC をポイントする同期済みの MAC エントリとローカル BVI インターフェイスにインストールされている同期済みの ARP エントリがインストールされます。

（注） ブリッジ ドメインまたはEVI あたりで非ゼロ ESI ごとに 1 つのイーサネット フロー ポイント（EFP）のみがサポートされています。これが EVPN の制限の 1 つです。

MAC と IP ルートの再発信

ホストがローカルで学習されておらず、また、ホストがローカル学習に基づいてアドバタイズされる場合、MAC エントリと ARP エントリの同期に使用されるローカル ESI とともに受信した MAC と IP がルート タイプ 2 も SYNC エントリをインストールするルータから再発信されます。このルートの再発信は、リモート EVPN PE 上でのオーバーレイ IP ECMP パスの確立や、オーバーレイでの MAC および IP ルートの撤回となるおそれがあるローカル AC リンク障害時のトラフィック ヒットを最小化するために必要です。

（注） BVI インターフェイスでカスタムまたはスタティック MAC アドレスが設定されている場合、ワイヤ上の MAC アドレスは設定されているものと異なる場合があります。このことによる動作上または機能上の影響はありません。

サブネット内ユニキャスト データ プレーン

すべての ES と、ローカル EVPN PE からアドバタイズされたすべての EVI、ES および EAD ルート タイプ 2 のルートに対し MAC + IP RT2 を通じて確立されたリモート EVP PE への ECMP パスを使用して送信元 EVPN PE でレイヤ 2 トラフィックがブリッジされます。

サブネット間ユニキャスト データ プレーン

サブネット間トラフィックは送信元 ToR 上でオーバーレイ ECMP を通じて宛先 ToR ネクストホップにルーティングされます。データ パケットは、ToR からアドバタイズされた VPN ラベルとスパインへの BGP ネクストホップのトンネル ラベルでカプセル化されます。その後、ホストへのローカル ARP 隣接関係を使用して宛先 ToR 上で再度ルーティングされます。リモート ToR 上の IP ECMP がローカル ルートおよびローカル ToR からアドバタイズされた再発信ルートを通じて確立されます。

VM モビリティ サポート

VM モビリティは、既存の MAC アドレスと IP アドレスを保持しながら、1 つのサーバから別のサーバへ移行する仮想マシンの機能です。

次に、VM モビリティを可能にする EVPN ルート タイプ 2 の 2 つの主要コンポーネントを示します。

- ローカル ブリッジ MAC テーブルにインポートされたホスト MAC アドバタイズメント コンポーネントと、ネットワーク オーバーレイ全体にわたってブリッジされたレイヤ 2 トラフィック。
- 対称 IRB 設計の IP ルーティング テーブルにインポートされたホスト IP アドバタイズメント コンポーネント。ネットワーク オーバーレイ全体にわたってルーティングされたトラフィックを可能にします。

上記のコンポーネントが、単一の MAC + IP ホスト ルート アドバタイズメント内で一緒にアドバタイズされます。追加の MAC 専用ルートもアドバタイズされることがあります。

VM の次の動作がサポートされています。VM は以下を実行できます。

- 既存の MAC の保持と新しい IP アドレスの取得
- 既存の IP アドレスの保持と新しい MAC の取得
- 既存の MAC と IP アドレスの両方の保持

MAC および MAC-IP シーケンス番号

IRB ゲートウェイ デバイスは、ハードウェア学習を通じてローカルに学習した MAC ルートと、ARP を通じてローカルに学習した MAC-IP ルートに関連付けられているシーケンス番号の割り当て、管理、アドバタイズを行います。

MAC および MAC-IP シーケンス番号の同期

2 つの Tor のマルチホームであるホストでは、ローカルに学習した MAC と MAC-IPが ローカル ESI を使用して学習したルート タイプ 2 を通じて 2 つのマルチホーミング ピア間で同期されます。そのため、両方とも同期とローカル学習を通じて学習された MAC と MAC-IP のいずれか、またはその両方がデバイスに存在する場合があります。ローカル ルートと同期されたルートの全体にわたってシーケンス番号が同期されます。そのため、所定のルートの 2 つの ToR からアドバタイズされたシーケンス番号は常に同じになります。特定の状況では、同じ ESI を持つリモート同期ルートがローカル ルートよりも上位のシーケンス番号を持つ可能性があります。このような場合、ローカル ルート シーケンス番号が大きくなり、リモート同期のルート シーケンス 番号と一致します。

ローカル シーケンス番号の更新

リモート ルートがすでに存在している場合、ローカル ルートを学習した時点でホスト モビリティがトリガーされます。モビリティが発生すると、既存のリモート ルートよりも 1 つ上位のシーケンス番号がローカル ルートに割り当てられます。この新しいローカル ルートが残りのネットワークにアドバタイズされます。

ホスト移動後のベスト ルートの選択

ホストを移動すると、そのホストの新しい位置の EVPN-PE は、ネットワークへのより上位のシーケンスルートを生成し、アドバタイズします。より上位のシーケンス番号を持つルートを受信すると、RFC 7432 に従い、そのルートが新しいベスト ルートと見なされ、トラフィックの転送に使用されます。MAC ルートと MAC-IP ルートの両方に対してベスト ルートの選択が行われます。

ホスト移動後の古いルートの削除

ホストがローカルからリモート ESI に移動した後、別の ESI からリモート ルートを受信し、シーケンス番号が下位の同じホストのローカル ルートが存在する場合は、そのローカル ルートが削除され、ネットワークから撤回されます。

シーケンス番号が上位の新しいリモート MAC ルートが最適であると見なされ、トラフィックの転送に使用されます。ARP プローブが古いローカル位置にあるホストに送信されます。ホストはリモートの新しい位置にあるため、プローブは失敗し、古いローカル MAC-IP ルートがクリアされます。

GARP でのホスト移動検知

ホストが移動後の新しい位置で Gratuitous ARP（GARP）を送信した場合、ローカル MAC とローカル MAC-IP ラーニングが両方のルータに対して別々にモビリティをトリガーします。

サイレント ホストを使用したホスト移動検出

ホストが移動後に新しい位置で GARP またはデータ パケットを送信しない場合、以前の位置のローカル MAC のエージングが両方のルータに対してモビリティをトリガーします。

データ パケットを使用した GARP なしのホスト移動検出

移動後にホストが GARP を送信しない場合は、ホストからのデータ パケットがプロアクティブ ARP プローブをトリガーし、ホスト MAC-IP を検出してオーバーレイ上でこのホストのモビリティをトリガーします。

重複 MAC 検出

RFC 7432 に従い、重複 MAC 検出とフリージングがサポートされています。

検出：重複データ検出とリカバリのパラメータは設定可能です。デフォルト設定は、180 秒間に 5 回と重複サイクル 3 回後のルート フリージングです。デフォルト設定では、ホストが 180 秒以内に 5 回移動すると、30 秒間は重複とマークされます。重複状態のホストのルート アドバタイズメントは抑制されます。ホストは 30 秒後に重複状態が解除されます。ホストが重複

していると 3 回検出されると、4 回目の重複サイクルで、そのホストは完全に凍結されます。凍結されたホストについては、すべてのルート アドバタイズメントが抑制されます。

マルチホーム ホストでは、MAC をローカルに学習するとは限りませんが、同期を通じて学習されます。重複データ検出はローカル ホストとリモート同期ホストの両方でサポートされています。リモート同期ルートは、リモート ルートと区別されます。

MAC-IP 処理：MAC ルートが重複しているか、または凍結状態の場合、ルート削除が撤回されることを除き、対応するローカル MAC-IP が更新されます。

重複状態の処理：ホストが重複状態にある場合、ルート アドバタイズメントが抑制されます。ただし、ローカル EVPN-PE のトラフィックがローカル ホストに転送されるようにローカル ルートはハードウェアでプログラミングされます。

リカバリ：完全に凍結されたホストの凍結解除が可能です。次に、凍結ホストをクリアする推奨手順を示します。

- 重複トラフィックの原因となっているホストをシャットダウンします。
- **clear l2route evpn frozen-mac frozen-flag** コマンドを使用して凍結されたホストをクリアします。

EVPN IRB の設定

```
/* Configure CEF to prefer RIB prefixes over adjacency prefixes.*/

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 3
RP/0/RSP0/CPU0:router(config-if)# lacp system mac 1.1.1
RP/0/RSP0/CPU0:router(config-if)# exit
RP/0/RSP0/CPU0:router(config)# cef adjacency route override rib


/* Configure EVPN L3VRF per DC tenant. */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# vrf irb1
RP/0/RSP0/CPU0:router(config-vrf)# address-family ipv4 unicast
RP/0/RSP0/CPU0:router(config-vrf-af)# import route-target 1000:1
RP/0/RSP0/CPU0:router(config-vrf-af)# export route-target 1000:1
RP/0/RSP0/CPU0:router(config-vrf-af)# exit


/* Configure Layer 2 attachment circuit (AC) from multichassis (MC) bundle interface,
and bridge-group virtual interface (BVI) per bridge domain. */
/* Note: When a VM migrates from one subnet to another (subnet stretching), apply the
following IRB configuration to both the EVPN PEs. *\

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface bvi 1001
RP/0/RSP0/CPU0:router(config-if)# host-routing
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 10.10.0.4 255.255.255.0
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 172.16.0.1 secondary
RP/0/RSP0/CPU0:router(config-if)# mac-address 2001:DB8::1
```

```
/* Configure EVPN Layer 2 bridging service. Note: This configuration is performed in
Layer 2 gateway or bridging scenario. */

Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group 1
Router(config-l2vpn-bg)# bridge-domain 1-1
Router(config-l2vpn-bg-bd)# interface GigabitEthernet 0/0/0/1.1
Router(config-l2vpn-bg-bd-ac)# evi 1
Router(config-l2vpn-bg-bd-ac-evi)# commit
Router(config-l2vpnbg-bd-ac-evi)# exit


/* Configure BGP. */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router bgp 3107
RP/0/RSP0/CPU0:router(config-bgp)# vrf irb1
RP/0/RSP0/CPU0:router(config-bgp-vrf)# rd auto
RP/0/RSP0/CPU0:router(config-bgp-vrf)# address-family ipv4 unicast
RP/0/RSP0/CPU0:router(config-bgp-vrf-af)# redistribute connected
RP/0/RSP0/CPU0:router(config-bgp-vrf-af)# redistribute static
RP/0/RSP0/CPU0:router(config-bgp-vrf-af)# exit
RP/0/RSP0/CPU0:router(config-bgp-vrf-af)# redistribute connected
RP/0/RSP0/CPU0:router(config-bgp-vrf-af)# redistribute static


/* Configure EVPN, and configure main bundle ethernet segment parameters in EVPN. */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# evpn
RP/0/RSP0/CPU0:router(config-evpn)# evi 2001
RP/0/RSP0/CPU0:router(config-evpn-evi)# bgp
RP/0/RSP0/CPU0:router(config-evpn-evi-bgp)# route-target import 1000:1
RP/0/RSP0/CPU0:router(config-evpn-evi-bgp)# route-target export 1000:1
RP/0/RSP0/CPU0:router(config-evpn-evi-bgp)# exit
RP/0/RSP0/CPU0:router(config-evpn-evi)# advertise-mac
RP/0/RSP0/CPU0:router(config-evpn-evi)# unknown-unicast-suppression


/* Configure Layer 2 VPN. */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group irb
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain irb1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface bundle-Ether3.1001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# routed interface BVI100
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-bvi)# split-horizon group core
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-bvi)# evi 10001
```

EVPN IRB の実行コンフィギュレーション

```
/* Configure LACP */

interface Bundle-Ether3
 lacp system mac 1.1.1
!
```

```
/* Configure CEF adjacency overwrite. */

cef adjacency route override rib

/* Configure EVPN Layer 3 VRF per DC tenant. */

vrf irb1
address-family ipv4 unicast
  import route-target
   1000:1
  !
  export route-target
   1000:1
  !

!
!

/* Configure Layer 2 attachment circuit (AC) from multichassis (MC) bundle interface,
and bridge-group virtual interface (BVI) per bridge domain./*


interface Bundle-Ether3.1001 l2transport
 encapsulation dot1q 1001
 rewrite ingress tag pop 1 symmetric
!
interface BVI1001
 host-routing
 vrf irb1
 ipv4 address 10.0.1.1 255.255.255.0
 mac-address 0000.3030.1
!

/* Configure BGP. */

router bgp 3107
 vrf irb1
  rd auto
  address-family ipv4 unicast
  redistribute connected
  redistribute static
!
!

/* Configure EVPN. */

evpn
evi 10001
  bgp
   route-target import 1000:1
   route-target export 1000:1
  !
  advertise-mac
  unknown-unicast-suppression
!

/* Configure Layer2 VPN. */

l2vpn
bridge group irb
  bridge-domain irb1
   interface Bundle-Ether3.1001
   !
   routed interface BVI1001
```

```
   split-horizon group core
  !
  evi 10001
  !
 !
```

EVPN IRB の確認

マルチホーミング シナリオでの Address Resolution Protocol（ARP）プロトコル エントリおよび同期済みエントリを確認します。EVPN IRB では、マルチホーミング アクティブ-アクティブ モードのみがサポートされています。

```
RP/0/RSP0/CPU0:router# show arp vrf evpn1

------------------------------------------------------------------
0/1/CPU0
------------------------------------------------------------------
Address    Age        Hardware Addr   State      Type   Interface

10.1.1.1    -         0010.0001.0001  Interface  ARPA   BVI1
10.1.1.11 02:23:46    1000.0001.0001  Dynamic    ARPA   BVI1
10.1.1.93   -         0000.f65a.357c  EVPN_SYNC  ARPA   BVI1
10.1.2.1    -         0011.0112.0001  Interface  ARPA   BVI2
10.1.2.91 02:24:14    0000.f65a.3570  Dynamic    ARPA   BVI2
10.1.2.93 02:21:52    0000.f65a.357d  Dynamic    ARPA   BVI2
------------------------------------------------------------------
0/0/CPU0
------------------------------------------------------------------
Address   Age         Hardware Addr   State      Type  Interface

10.1.1.1  -           0010.0001.0001  Interface  ARPA  BVI1
10.1.1.11 02:23:46    1000.0001.0001  Dynamic    ARPA  BVI1
10.1.1.93 -           0000.f65a.357c  EVPN_SYNC  ARPA  BVI1
10.1.2.1  -           0011.0112.0001  Interface  ARPA BVI2
10.1.2.91 02:24:14    0000.f65a.3570  Dynamic    ARPA BVI2
10.1.2.93 02:21:52    0000.f65a.357d  Dynamic    ARPA BVI2
```

隣接関係エントリを確認します。特に、同期済み IPv4 および IP ARP エントリに新しく追加された情報を確認します。

```
RP/0/RSP0/CPU0:router# show adjacency ipv4 BVI 1 internal detail location 0/0/CPU0

BVI1, 10.1.1.93 (ipv4)
Version: 1169, references: 2, transient lock: 0
Encapsulation information (14 bytes) 0000f65a357c0000f65a357c0800 MTU: 1500
 Adjacency pointer is: 0x770a9278
 Platform adjacency pointer is: 0x7d7bc380
 Last updated: Feb 28 15:58:21.998
 Adjacency producer: arp (prod_id: 10)
 Flags: incomplete adj,
 Additional Adjacency Information (4 bytes long),
 Upto first 4 bytes (in hex): 01000000
 Netio idb pointer not cached Cached interface type: 78

Adjacency references:
bfd_agent (JID 150, PID 3637), 0 reference
```

```
l2fib_mgr (JID 185, PID 4003), 0 reference
fib_mgr (JID 294, PID 3605), 1 reference
aib (JID 314, PID 3590), 1 reference

BVI1, 10.1.1.11 (ipv4) Version: 1493,
references: 3, transient lock: 0
Encapsulation information (14 bytes) 10000001000100100000100010800
MTU: 1500
Adjacency pointer is: 0x770ab778
Platform adjacency pointer is: 0x7d7bcb10
Last updated: Mar 2 17:22:00.544
Adjacency producer: arp (prod_id: 10)
Flags: incomplete adj,
Netio idb pointer not cached Cached interface type: 78
Adjacency references:
bfd_agent (JID 150, PID 3637), 0 reference
l2fib_mgr (JID 185, PID 4003), 1 reference
fib_mgr (JID 294, PID 3605), 1 reference
aib (JID 314, PID 3590), 1 reference
```

L2FIB ラインカードで学習した詳細を取得するためのエントリを確認します。マルチホーミング アクティブ-アクティブ シナリオでは、リンクローカル アドレスも更新され、EVPN ピア ゲートウェイに配布されます。

```
RP/0/RSP0/CPU0:router# show l2vpn mac-learning mac-ipv4 all location 0/0/cPU0

Topo ID  Producer  Next Hop(s)  Mac Address     IP Address

6        0/0/CPU0   BV1        1000.0001.0001      10.1.1.11
7        0/0/CPU0   BV2        0000.f65a.3570      10.1.2.91
7       0/0/CPU0    BV2        0000.f65a.357d      10.1.2.93
```

```
RP/0/RSP0/CPU0:router# show l2vpn mac-learning mac-ipv4 all location 0/0/cPU0

Topo ID  Producer  Next Hop(s)  Mac Address    IP Address

6      0/0/CPU0    BV1       0000.f65a.357c    fe80::200:f6ff:fe5a:357c
7      0/0/CPU0    BV2       0000.f65a.3570    10:1:2::91
7      0/0/CPU0    BV2       0000.f65a.357d    10:1:2::93
7      0/0/CPU0    BV2       0000.f65a.3570    fe80::200:f6ff:fe5a:3570
```

VM モビリティのシーケンス ID を確認します。

```
RP/0/RSP0/CPU0:router# show l2route evpn mac-ip all detail

Sun Apr 30 18:09:19.368 PDT
Flags: (Stt)=Static; (L)=Local; (R)=Remote; (F)=Flood;
(N)=No Redistribution; (Rtr)=Router MAC; (B)=Best Route;
(P)=Probe; (S)=Peer Sync; (F)=Flush;
(D)=Duplicate MAC; (Z)=Frozen MAC;

Topo ID    Mac Address     IP Address  Prod   Next Hop(s)        Seq No  Flags
Opaque Data Type    Opaque Data Len   Opaque Data Value
-------    -----------     ----------  ----   ----------         ------  -----
-----------------    ---------------   ------------------
33         0022.6730.0001  10.130.0.2  L2VPN  Bundle-Ether6.1300  0      SB 0 12
0x06000000           0x22000080        0x00000000
```

```
Last Update: Sun Apr 30 15:00:01.911 PDT

33         0022.6730.0002 10.130.0.3  LOCAL  Bundle-Ether6.1300   0       B
N/A                  N/A              N/A


RP/0/RSP0/CPU0:router# show l2route evpn mac all detail


Flags:  (Stt)=Static; (L)=Local; (R)=Remote; (F)=Flood;
        (N)=No Redistribution; (Rtr)=Router MAC; (B)=Best Route;
        (S)=Peer Sync; (Spl)=Split; (Rcv)=Recd;
        (D)=Duplicate MAC; (Z)=Frozen MAC;

Topo ID  Mac Address     Prod   Next Hop(s)         Seq No  Flags  Slot ESI   Opaque
Data Type  Opaque Data Len Opaque Data Value
-------- --------------  ------ -----------         ------  ------ ---- ----
----------------  ---------------- ------------------
36       0022.5830.0001  L2VPN  Bundle-Ether5.1300  0       BSSpl  0    (F)    0
         12             0x06000000 0x25000080 0x00000000

Last Update: Thu Apr 20 09:04:44.358 PDT
```

重複データ検出とリカバリのパラメータを確認します。

```
/* Use the show run evpn mac to verify the current parameters:  *\

RP/0/RSP0/CPU0:router# show run evpn mac

evpn
mac
  secure
   freeze-time 5
   move-count 1000
   move-interval 60
   retry-count 1000
  !
!
!


/* Perform the following steps to change the existing parameters. */

RP/0/RP0/CPU0:EVPN-LF1# configure
RP/0/RP0/CPU0:EVPN-LF1(config)# evpn
RP/0/RP0/CPU0:EVPN-LF1(config-evpn)# mac
RP/0/RP0/CPU0:EVPN-LF1(config-evpn-mac)# secure
RP/0/RP0/CPU0:EVPN-LF1(config-evpn-mac-secure)# move-count 1000
RP/0/RP0/CPU0:EVPN-LF1(config-evpn-mac-secure)# end

/* Use the show run evpn mac to verify the changed parameters:  *\

RP/0/RSP0/CPU0:router# show run evpn mac

evpn
mac
  secure
   move-count 1000
  !
```

```
!
!
```

L2FIB RP がアグリゲータの場合に、その L2FIB RP で学習した詳細を取得するためのエントリを確認します。ルート プロセッサ（RP）のエントリは、ライン カードから取得した集約エントリです。MAC 移動の場合、同じ MAC が異なる状態になることがあります。これは、RP 集約エントリに表示されます。RP は、MAC ラーニング アルゴリズムに従って、L2RIB に送信する更新を決定します。

```
RP/0/RSP0/CPU0:router#  show l2vpn mac-learning mac-ipv4 all location 0/RSP0/CPU0

Topo ID  Producer        Next Hop(s)        Mac Address         IP Address
-------  --------    -----------        --------------      ----------
6            0/0/CPU0       BV1            1000.0001.0001      10.1.1.11
7            0/0/CPU0       BV2            0000.f65a.3570      10.1.2.91
7            0/0/CPU0       BV2            0000.f65a.357d      10.1.2.93
```

RP L2FIB によって更新される L2RIB 内のエントリを確認します。エントリを確認するときは、次の点に注意してください。

- L2VPN としてのプロデューサ、リモート IP としての NH を持つエントリは、リモート ピア ゲートウェイから学習されます。これらのゲートウェイは BGP から学習され、EVPN に更新されてから L2RIB に更新されます。そのため、これらのエントリはローカル IP-MAC ラーニングによるものではありません。
- L2VPN としてプロデューサ、ローカル バンドル インターフェイスとして NH を持つエントリは、MH-AA ピア ゲートウェイからの同期済みエントリです。
- ローカルとしてプロデューサ、ローカル バンドル インターフェイスとして NH を持つエントリは、動的に学習されたローカル エントリです。

```
RP/0/RSP0/CPU0:router# show l2route evpn mac-ip evi 6

Topo ID      Mac Address         IP Address                Prod        Next Hop(s)
--------     --------------      ---------------           ------      -------------
6            0000.f65a.3569      10.1.1.101                L2VPN     172.16.0.2/24014/ME
6            0000.f65a.3575      10.1.1.97                 L2VPN     172.16.0.7/24025/ME
6            0000.f65a.3575      10:1:1::97                L2VPN     172.16.0.7/24025/ME
6            0000.f65a.3575      fe80::200:f6ff:fe5a:3575  L2VPN     172.16.0.7/24025/ME
6            0000.f65a.357c      10.1.1.93                 L2VPN      Bundle-Ether1.11
6            0000.f65a.357c      10:1:1::93                L2VPN      Bundle-Ether1.11
6            0000.f65a.357c      fe80::200:f6ff:fe5a:357c  LOCAL      Bundle-Ether1.11
6            0010.0001.0012      10.1.1.12                 L2VPN      172.16.0.7/24025/ME

6            1000.0001.0001      10.1.1.11                 LOCAL      Bundle-Ether1.11
6            90e2.ba8e.c0c9      10.1.1.102                L2VPN      172.16.0.2/24014/ME
```

EVPN の詳細を取得するためのエントリを確認します。

```
RP/0/RSP0/CPU0:router# show evpn evi vpn-id 1 mac ipv4 10.1.1.93 detail

EVI       MAC address         IP address            Nexthop             Label
----      --------------      ----------            ----------          -----
1          0000.f65a.357c      10.1.1.93            172.16.0.2          24014

Ethernet Tag : 0
Multi-paths Resolved : True
Static : No
Local Ethernet Segment : N/A
Remote Ethernet Segment : 0100.6cbc.a77c.c180.0000
Local Sequence Number : N/A
Remote Sequence Number : 0
Local Encapsulation : N/A
Remote Encapsulation : MPLS
```

適切な 2 番目のラベルと、2 番目の IP VRF ルートターゲットを使用してローカル BGP エントリを確認します。

```
RP/0/RSP0/CPU0:router# show bgp l2vpn evpn rd 172.16.0.1:1
[2][0][48][0000.f65a.357c][32][10.1.1.93]/136

BGP routing table entry for [2][0][48][0000.f65a.357c][32][10.1.1.93]/136, Route
Distinguisher: 172.16.0.1:1
Versions:
Process bRIB/RIB SendTblVer
Speaker 3772 3772
Local Label: 24013
Last Modified: Feb 28 16:06:37.073 for 2d19h
Paths: (2 available, best #1)
Advertised to peers (in unique update groups):
172.16.0.9
Path #1: Received by speaker 0
Advertised to peers (in unique update groups):
172.16.0.9
Local
0.0.0.0 from 0.0.0.0 (172.16.0.1)
Second Label 24027                              >>>>  Second label when IRB host-routing
 is enabled.
Origin IGP, localpref 100, valid, redistributed, best, group-best, import-candidate,
rib-install
Received Path ID 0, Local Path ID 0, version 3772
Extended community: SoO:172.16.0.2:1 RT:100:100
EVPN ESI: 0100.6cbc.a77c.c180.0000
Path #2: Received by speaker 0
Not advertised to any peer
Local
172.16.0.2 (metric 101) from 172.16.0.9 (172.16.0.2)
Received Label 24014, Second Label 24031
Origin IGP, localpref 100, valid, internal, add-path, import-candidate, imported,
rib-install
Received Path ID 0, Local Path ID 2, version 3769
Extended community: SoO:172.16.0.2:1 RT:200:1 RT:700:100  >>>  Second RT is IP VRF RT
for remote to import into IP VRF routing table.
Originator: 172.16.0.2, Cluster list: 172.16.0.9
EVPN ESI: 0100.6cbc.a77c.c180.0000
Source AFI: L2VPN EVPN, Source VRF: default, Source Route Distinguisher: 172.16.0.2:1
```

```
RP/0/RSP0/CPU0:router# show bgp l2vpn evpn rd 172.16.0.1:1
[2][0][48][0000.f65a.357c][128][10:1:1::93]/232

[2][0][48][0000.f65a.357c][128][10:1:1::93]/232
BGP routing table entry for [2][0][48][0000.f65a.357c][128][10:1:1::93]/232, Route
Distinguisher: 172.16.0.1:1
Versions:
Process bRIB/RIB SendTblVer
Speaker 3172 3172
Local Label: 24013
Last Modified: Feb 28 11:34:33.073 for 3d00h
Paths: (2 available, best #1)
Advertised to peers (in unique update groups):
172.16.0.9
Path #1: Received by speaker 0
Advertised to peers (in unique update groups):
172.16.0.9
Local
0.0.0.0 from 0.0.0.0 (172.16.0.1)
Second Label 24029
Origin IGP, localpref 100, valid, redistributed, best, group-best, import-candidate,
rib-install
Received Path ID 0, Local Path ID 0, version 3172
Extended community: SoO:172.16.0.2:1 RT:100:100
EVPN ESI: 0100.6cbc.a77c.c180.0000
Path #2: Received by speaker 0
Not advertised to any peer
Local
172.16.0.2 (metric 101) from 172.16.0.9 (172.16.0.2)
Received Label 24014, Second Label 24033
Origin IGP, localpref 100, valid, internal, add-path, import-candidate, imported,
rib-install
Received Path ID 0, Local Path ID 2, version 3167
Extended community: SoO:172.16.0.2:1 RT:200:1 RT:700:100
Originator: 172.16.0.2, Cluster list: 172.16.0.9
EVPN ESI: 0100.6cbc.a77c.c180.0000
Source AFI: L2VPN EVPN, Source VRF: default, Source Route Distinguisher: 172.16.0.2:1
```

適切なラベルとルートターゲットを使用してリモート ピア ゲートウェイ BGP エントリを確認します。特に、リモート EVPN ゲートウェイ上の自動生成されたローカル RD を確認します。EVPN タイプ 2 ルートが EVPN にインポートされます。IPv4 /32 アドレスのホスト ルートは、リモート EVPN ゲートウェイの IP VRF ルートテーブルにのみインポートされますが、ローカル BVI 隣接関係を RIB エントリの上書きに使用するローカル EVPN ゲートウェイにはインポートされません。

```
RP/0/RSP0/CPU0:router#  show bgp l2vpn evpn rd 172.16.0.7:1
[2][0][48][0000.f65a.357c][32][10.1.1.93]/136
BGP routing table entry for [2][0][48][0000.f65a.357c][32][10.1.1.93]/136, Route
Distinguisher: 172.16.0.7:1
Versions:
Process bRIB/RIB SendTblVer
Speaker 16712 16712
Last Modified: Feb 28 16:06:36.448 for 2d19h
Paths: (2 available, best #1)
Not advertised to any peer
Path #1: Received by speaker 0
```

```
Not advertised to any peer
Local
172.16.0.1 from 172.16.0.9 (172.16.0.1)
Received Label 24013, Second Label 24027 >>>> First label for L2 MAC unicast bridging;
 second label for EVPN IRB host-routing
Origin IGP, localpref 100, valid, internal, best, group-best, import-candidate, imported,
 rib-install
Received Path ID 0, Local Path ID 0, version 16712
Extended community: SoO:172.16.0.2:1 RT:100:1 RT:100:100
Originator: 172.16.0.1, Cluster list: 172.16.0.9
EVPN ESI: 0100.6cbc.a77c.c180.0000
Source AFI: L2VPN EVPN, Source VRF: default, Source Route Distinguisher: 172.16.0.1:1
Path #2: Received by speaker 0
Not advertised to any peer
Local
172.16.0.2 from 172.16.0.9 (172.16.0.2)
Received Label 24014, Second Label 24031
Origin IGP, localpref 100, valid, internal, backup, add-path, import-candidate, imported,
 rib-install
Received Path ID 0, Local Path ID 1, version 16706
Extended community: SoO:172.16.0.2:1 RT:200:1 RT:700:100
Originator: 172.16.0.2, Cluster list: 172.16.0.9
EVPN ESI: 0100.6cbc.a77c.c180.0000
Source AFI: L2VPN EVPN, Source VRF: default, Source Route Distinguisher: 172.16.0.2:1
```

```
RP/0/RSP0/CPU0:router# show bgp l2vpn evpn rd 172.16.0.7:1
[2][0][48][0000.f65a.357c][128][10:1:1::93]/232

BGP routing table entry for [2][0][48][0000.f65a.357c][128][10:1:1::93]/232, Route
Distinguisher: 172.16.0.7:1
Versions:
Process bRIB/RIB SendTblVer
Speaker 6059 6059
Last Modified: Feb 28 12:03:22.448 for 2d23h
Paths: (2 available, best #1)
Not advertised to any peer
Path #1: Received by speaker 0
Not advertised to any peer
Local
172.16.0.1 from 172.16.0.9 (172.16.0.1)
Received Label 24013, Second Label 24029
Origin IGP, localpref 100, valid, internal, best, group-best, import-candidate, imported,
 rib-install
Received Path ID 0, Local Path ID 0, version 6043
Extended community: SoO:172.16.0.2:1 RT:100:1 RT:100:100
Originator: 172.16.0.1, Cluster list: 172.16.0.9
EVPN ESI: 0100.6cbc.a77c.c180.0000
Source AFI: L2VPN EVPN, Source VRF: default, Source Route Distinguisher: 172.16.0.1:1
Path #2: Received by speaker 0
Not advertised to any peer
Local
172.16.0.2 from 172.16.0.9 (172.16.0.2)
Received Label 24014, Second Label 24033
Origin IGP, localpref 100, valid, internal, backup, add-path, import-candidate, imported,
 rib-install
Received Path ID 0, Local Path ID 1, version 6059
Extended community: SoO:172.16.0.2:1 RT:200:1 RT:700:100
Originator: 172.16.0.2, Cluster list: 172.16.0.9
EVPN ESI: 0100.6cbc.a77c.c180.0000
Source AFI: L2VPN EVPN, Source VRF: default, Source Route Distinguisher: 172.16.0.2:1
```

IP VRF ルーティング テーブルにインポートされた IPv4 /32 アドレスのホスト ルートを持つリモート ピア ゲートウェイを確認します。

```
RP/0/RSP0/CPU0:router#  show bgp vpnv4 unicast vrf evpn1 10.1.1.93/32

BGP routing table entry for 10.1.1.93/32, Route Distinguisher: 172.16.0.7:11
Versions:
Process bRIB/RIB SendTblVer
Speaker 22202 22202
Last Modified: Feb 28 16:06:36.447 for 2d19h
Paths: (2 available, best #1)
Not advertised to any peer
Path #1: Received by speaker 0
Not advertised to any peer
Local
172.16.0.1 from 172.16.0.9 (172.16.0.1)
Received Label 24027
Origin IGP, localpref 100, valid, internal, best, group-best, import-candidate, imported
Received Path ID 0, Local Path ID 0, version 22202
Extended community: SoO:172.16.0.2:1 RT:100:1 RT:100:100
Originator: 172.16.0.1, Cluster list: 172.16.0.9
Source AFI: L2VPN EVPN, Source VRF: default, Source Route Distinguisher: 172.16.0.1:1
 >>>> The source from L2VPN and from synced ARP entry.
Path #2: Received by speaker 0
Not advertised to any peer
Local
172.16.0.2 from 172.16.0.9 (172.16.0.2)
Received Label 24031
Origin IGP, localpref 100, valid, internal, backup, add-path, import-candidate, imported
Received Path ID 0, Local Path ID 1, version 22201
Extended community: SoO:172.16.0.2:1 RT:200:1 RT:700:100
Originator: 172.16.0.2, Cluster list: 17.0.0.9
Source AFI: L2VPN EVPN, Source VRF: default, Source Route Distinguisher: 172.16.0.2:1
 >>>> source from L2VPN and from dynamic ARP entry
```

```
RP/0/RSP0/CPU0:router# show bgp vpnv6 unicast vrf evpn1 10:1:1::93/128

BGP routing table entry for 10:1:1::93/128, Route Distinguisher: 172.16.0.7:11
Versions:
Process bRIB/RIB SendTblVer
Speaker 22163 22163
Last Modified: Feb 28 12:09:30.447 for 2d23h
Paths: (2 available, best #1)
Not advertised to any peer
Path #1: Received by speaker 0
Not advertised to any peer
Local
172.16.0.1 from 172.16.0.9 (172.16.0.1)
Received Label 24029
Origin IGP, localpref 100, valid, internal, best, group-best, import-candidate, imported
Received Path ID 0, Local Path ID 0, version 22163
Extended community: SoO:172.16.0.2:1 RT:100:1 RT:100:100
Originator: 172.16.0.1, Cluster list: 172.16.0.9
```

```
Source AFI: L2VPN EVPN, Source VRF: default, Source Route Distinguisher: 172.16.0.1:1
>>> Source from L2VPN and from synced ARP entry.
Path #2: Received by speaker 0
Not advertised to any peer
Local
172.16.0.2 from 172.16.0.9 (172.16.0.2)
Received Label 24033
Origin IGP, localpref 100, valid, internal, backup, add-path, import-candidate, imported
Received Path ID 0, Local Path ID 1, version 22163
Extended community: SoO:172.16.0.2:1 RT:200:1 RT:700:100
Originator: 172.16.0.2, Cluster list: 172.16.0.9
Source AFI: L2VPN EVPN, Source VRF: default, Source Route Distinguisher: 172.16.0.2:1
>>> Source from L2VPN and from dynamic ARP entry.
```

```
RP/0/RSP0/CPU0:router# show bgp vpnv6 unicast vrf evpn1 10:1:1::93/128

BGP routing table entry for 10:1:1::93/128, Route Distinguisher: 172.16.0.7:11
Versions:
Process bRIB/RIB SendTblVer
Speaker 22163 22163
Last Modified: Feb 28 12:09:30.447 for 2d23h
Paths: (2 available, best #1)
Not advertised to any peer
Path #1: Received by speaker 0
Not advertised to any peer
Local
172.16.0.1 from 172.16.0.9 (172.16.0.1)
Received Label 24029
Origin IGP, localpref 100, valid, internal, best, group-best, import-candidate, imported
Received Path ID 0, Local Path ID 0, version 22163
Extended community: SoO:172.16.0.2:1 RT:100:1 RT:100:100
Originator: 172.16.0.1, Cluster list: 172.16.0.9
Source AFI: L2VPN EVPN, Source VRF: default, Source Route Distinguisher: 172.16.0.1:1

Path #2: Received by speaker 0
Not advertised to any peer
Local
172.16.0.2 from 172.16.0.9 (172.16.0.2)
Received Label 24033
Origin IGP, localpref 100, valid, internal, backup, add-path, import-candidate, imported
Received Path ID 0, Local Path ID 1, version 22163
Extended community: SoO:172.16.0.2:1 RT:200:1 RT:700:100
Originator: 172.16.0.2, Cluster list: 172.16.0.9
Source AFI: L2VPN EVPN, Source VRF: default, Source Route Distinguisher: 172.16.0.2:1
```

RIB エントリを上書きするローカル隣接関係と、IP VPN 転送に IP VRF ホスト ルート エントリを使用するリモート ピアによるローカル転送を確認します。

```
RP/0/RSP0/CPU0:router#  show bgp vpnv4 unicast vrf evpn1 10.1.1.93/32

-- For local routing and forwarding
RP/0/RSP0/CPU0:PE11-R1#show route vrf evpn1 10.1.1.93
```

```
Routing entry for 10.1.1.93/32
Known via "bgp 3107", distance 200, metric 0, type internal
Installed Feb 28 15:57:28.154 for 2d20h
Routing Descriptor Blocks
172.16.0.2, from 172.16.0.9      >>>  From MH-AA peer.
Nexthop in Vrf: "default", Table: "default", IPv4 Unicast, Table Id: 0xe0000000
Route metric is 0
No advertising protos.

RP/0/RSP0/CPU0:PE11-R1# show cef vrf evpn1 10.1.1.93 location 0/0/CPU0
10.1.1.93/32, version 0, internal 0x1120001 0x0 (ptr 0x7b40052c) [1], 0x0 (0x7b286010),
 0x0 (0x0)
Updated Feb 28 15:58:22.688
local adjacency 10.1.1.93
Prefix Len 32, traffic index 0, Adjacency-prefix, precedence n/a, priority 15
via 10.1.1.93/32, BVI1, 2 dependencies, weight 0, class 0 [flags 0x0]
path-idx 0 NHID 0x0 [0x7f531f88 0x0]
next hop
local adjacency              >>> Forwarding with local synced ARP adjacency entries.


For remote routing and forwarding:

RP/0/RSP0/CPU0:router# show route vrf evpn1 10.1.1.93

Routing entry for 10.1.1.93/32
Known via "bgp 3107", distance 200, metric 0
Number of pic paths 1 , type internal
Installed Feb 28 16:06:36.431 for 2d20h
Routing Descriptor Blocks
172.16.0.1, from 172.16.0.9
Nexthop in Vrf: "default", Table: "default", IPv4 Unicast, Table Id: 0xe0000000
Route metric is 0
172.16.0.2, from 172.16.0.9, BGP backup path
Nexthop in Vrf: "default", Table: "default", IPv4 Unicast, Table Id: 0xe0000000
Route metric is 0
No advertising protos.

RP/0/RSP0/CPU0:router# show cef vrf evpn1 10.1.1.93 location 0/0/CPU0

10.1.1.93/32, version 86, internal 0x5000001 0x0 (ptr 0x99fac884) [1], 0x0 (0x0), 0x208
 (0x96c58494)
Updated Feb 28 16:06:39.285
Prefix Len 32, traffic index 0, precedence n/a, priority 3
via 172.16.0.1/32, 15 dependencies, recursive [flags 0x6000]
path-idx 0 NHID 0x0 [0x97955380 0x0]
recursion-via-/32
next hop VRF - 'default', table - 0xe0000000
next hop 172.16.0.1/32 via 34034/0/21
next hop 100.0.57.5/32 Te0/0/0/3 labels imposed {ImplNull 24011 24027}
next hop 100.0.67.6/32 Te0/0/0/1 labels imposed {ImplNull 24009 24027}
via 172.16.0.2/32, 11 dependencies, recursive, backup [flags 0x6100]
path-idx 1 NHID 0x0 [0x979554a0 0x0]
recursion-via-/32
next hop VRF - 'default', table - 0xe0000000
next hop 172.16.0.2/32 via 34035/0/21
next hop 100.0.57.5/32 Te0/0/0/3 labels imposed {ImplNull 24012 24031}
next hop 100.0.67.6/32 Te0/0/0/1 labels imposed {ImplNull 24010 24031}
```

次の各項では、サブネット ストレッチングの確認方法について説明します。

VRF を確認ます。

```
RP/0/RP0/CPU0:leafW# show run vrf cust130

vrf cust130
address-family ipv4 unicast
  import route-target
   130:130
  !
  export route-target
   130:130
  !
!
!
```

BGP 設定を確認します。

```
 RP/0/RP0/CPU0:leafW# show run router bgp | begin vrf cust130

vrf cust130
  rd auto
  address-family ipv4 unicast
   label mode per-vrf
   maximum-paths ibgp 10
   redistribute connected
  !
!
```

L2VPN を確認します。

```
RP/0/RP0/CPU0:leafW# show run l2vpn bridge group bg130

l2vpn
bridge group bg130
  bridge-domain bd130
   interface Bundle-Ether1.1300
   !
   interface Bundle-Ether5.1300
   !
   routed interface BVI130
   evi 130
   !
  !
!
!
```

重複 IP アドレス検出

重複 IP アドレス検出機能は、重複する IP アドレスを持つすべてのホストを自動的に検出し、重複する IP アドレスを持つすべての MAC-IP ルートをブロックします。

これにより、意図せずに、または EVPN ファブリック内の悪意によって、重複する IP アドレスが割り当てられたホストから、ネットワークが保護されます。IP アドレスが重複しているホ

ストは、ネットワーク内で不要な変化を引き起こし、同じ IP アドレスを持つホストの一方または両方でトラフィックが損失する原因となります。

システムでは、あるホストから別のホストにMACアドレスやIPアドレスが移動する際に、それらを追跡することによって、EVPN ホストのモビリティを処理します。2 つのホストに同じ IP アドレスが割り当てられている場合、IOS XR システムは両方のホストからの MAC-IP ルートの学習と再学習を維持します。一方のホストからMAC-IPルートを学習すると、新しく学習したルートの方が以前に他のホストから学習したルートよりも優先されるため、学習のたびに1回の移動としてカウントされます。この動作は、設定されたパラメータに基づいてIPアドレスが重複としてマークされるまで続きます。

どのような場合に IP アドレスを重複としてマークし、異なるホスト間で移動する際に凍結または凍結解除するかは、次のパラメータで決定されます。これらのパラメータは設定可能です。

- **move-interval**：この間隔以内にMACまたはIPアドレスが異なるホスト間で特定の回数移動すると、重複または一時的な凍結と見なされます。回数の数値は **move-count** パラメータで指定します。
- **move-count**：**move-interval** で指定した間隔以内に MAC または IP アドレスが異なるホスト間でこの回数移動すると、重複と見なされます。
- **freeze time**：MAC または IP アドレスが重複として検出された後にロックされる時間の長さ。この期間が経過すると、IP アドレスはロック解除され、再学習が許可されます。
- **retry-count**：MAC または IP アドレスが重複として検出された後、永続的に凍結されるまでの、MAC または IP アドレスのロック解除回数。

システムでは、あるホストから別のホスト（別のローカル ホストか、リモートのトップ オブ ラック（TOR）の背後にあるホストのどちらか）に IP アドレスが移動した回数を管理しています。**move-interval** パラメータで指定された間隔以内に、**move-count** パラメータで指定された回数だけ移動したIPアドレスは、重複するIPアドレスと見なされます。そのIPアドレスを持つ MAC-IP ルートはすべて、**freeze-time** パラメータで指定された時間のあいだ凍結されます。特定の IP アドレスが凍結していることは syslog でユーザに通知されます。IP アドレスが凍結されている間、凍結されたIPアドレスを持つ新しいMAC-IPルートまたは既存のMAC-IPルートに対する更新は、すべて無視されます。

freeze-time が経過すると、対応する MAC-IP ルートが凍結解除され、 **move-count** の値がゼロにリセットされます。凍結されていないローカルMAC-IPルートでは、リモートMAC-IPルートがプローブ モードになっている間、ARP のプローブとフラッシュが開始されます。これにより、重複検出プロセスが再開されます。

また、システムでは、特定の IP アドレスが凍結および凍結解除された回数に関する情報も保持しています。IP アドレスが、**retry-count** 回数の後に重複としてマークされると、ユーザが手動で凍結解除するまで永続的に凍結されます。凍結されたMAC、IPv4、およびIPV6アドレスを手動で凍結解除するには、それぞれ次のコマンドを使用します。

- **clear l2route evpn mac** { *mac-address* } | **all** [**evi** *evi*] **frozen-flag**
- **clear l2route evpn ipv4** { *ipv4-address* } | **all** [**evi** *evi*] **frozen-flag**

- **clear l2route evpn ipv6** { *ipv6-address* } | **all** [**evi** *evi*] **frozen-flag**

重複 IP アドレス検出の設定

重複 IP アドレス検出機能を設定するには、次のタスクを実行します。

設定例

```
/* Ipv4 Address Duplicate Detection Configuration */
Router# configure
Router(config)# evpn
Router(config-evpn)# host ipv4-address duplicate-detection
Router(config-evpn-host-ipv4-addr)# move-count 2
Router(config-evpn-host-ipv4-addr)# freeze-time 10
Router(config-evpn-host-ipv4-addr)# retry-count 2
Router(config-evpn-host-ipv4-addr)# commit

/* Ipv6 Address Duplicate Detection Configuration */
Router# configure
Router(config)# evpn
Router(config-evpn)# host ipv6-address duplicate-detection
Router(config-evpn-host-ipv6-addr)# move-count 2
Router(config-evpn-host-ipv6-addr)# freeze-time 10
Router(config-evpn-host-ipv6-addr)# retry-count 2
Router(config-evpn-host-ipv6-addr)# commit
```

実行コンフィギュレーション

ここでは、重複する IP アドレスを検出するための実行コンフィギュレーションを示します。

```
evpn
 host ipv4-address duplicate-detection
  move-count 2
  freeze-time 10
  retry-count 2
 !
evpn
 host ipv6-address duplicate-detection
  move-count 2
  freeze-time 10
  retry-count 2
 !
```

確認

次に示すshow出力は、重複するIPアドレスの検出パラメータとリカバリ パラメータの詳細を示しています。

```
Router#show l2route evpn mac-ip all detail

Flags:  (Stt)=Static; (L)=Local; (R)=Remote; (F)=Flood;
        (N)=No Redistribution; (Rtr)=Router MAC; (B)=Best Route;
        (S)=Peer Sync; (Spl)=Split; (Rcv)=Recd;
        (D)=Duplicate MAC; (Z)=Frozen MAC;
```

```
Topo ID    Mac Address     IP Address  Prod   Next Hop(s)         Seq No  Flags
Opaque Data Type    Opaque Data Len   Opaque Data Value
-------    ----------     ----------  ----   ----------          ------  -----
---------------    ---------------   -----------------
33         0022.6730.0001  10.130.0.2  L2VPN  Bundle-Ether6.1300  0       SB 0 12
0x06000000
```

関連項目

- 重複 IP アドレス検出 （269 ページ）

関連コマンド

- evpn host ipv4-address duplicate-detection
- evpn host ipv6-address duplicate-detection
- show l2route evpn mac-ip all detail

オールアクティブ マルチホーミング対応 DHCPv4 リレー同期

オールアクティブ マルチホーミング対応DHCPv4 リレー同期機能は、エンドユーザとDHCPv4 サーバ間で一時的なエンティティを有効にするもので、DHCPv4 バインディングを作成しません。この機能により、エンドユーザ間において接続ポイント（PoA）全体にわたるDHCP コントロールプレーン パケットの均等な分散がサポートされます。単一ユーザ向けの DHCP 制御パケットはすべて同じDHCPv4 リレー（PoA）上に存在します。そのため、エンドユーザは介入や遅延を受けずに IP アドレス割り当てをリースできます。

マルチプロトコル拡張 BGP セッションが MPLS-SR を介してエッジ ルータへの PE ルータ間で確立され、学習された MAC-IP 情報が BGP を介してエッジ ルータに送信されます。MP-BGP は、指定されたイーサネットセグメント識別子（ESI）とイーサネットタグについて、学習した MAC-IP 情報をルート タイプ 2 を使用してアドバタイズします。エッジ ルータは、PE1 または PE2 から学習したルートを他の PE に再配布する機能、およびその逆の機能を備えています。このメカニズムにより、MAC IP ルートがエッジ ルータに配信されます。その結果、個々の PE が完全な MAC IP ルーティング情報を持ちます。

この機能により、双方向トラフィックの転送が保証されます。ハイ アベイラビリティの場合は、ノード（PoA#1 または PoA#2）の障害時、アクセス インターフェイスの障害時、またはコア リンクの障害時に、他の PoA がデータ トラフィックを転送します。

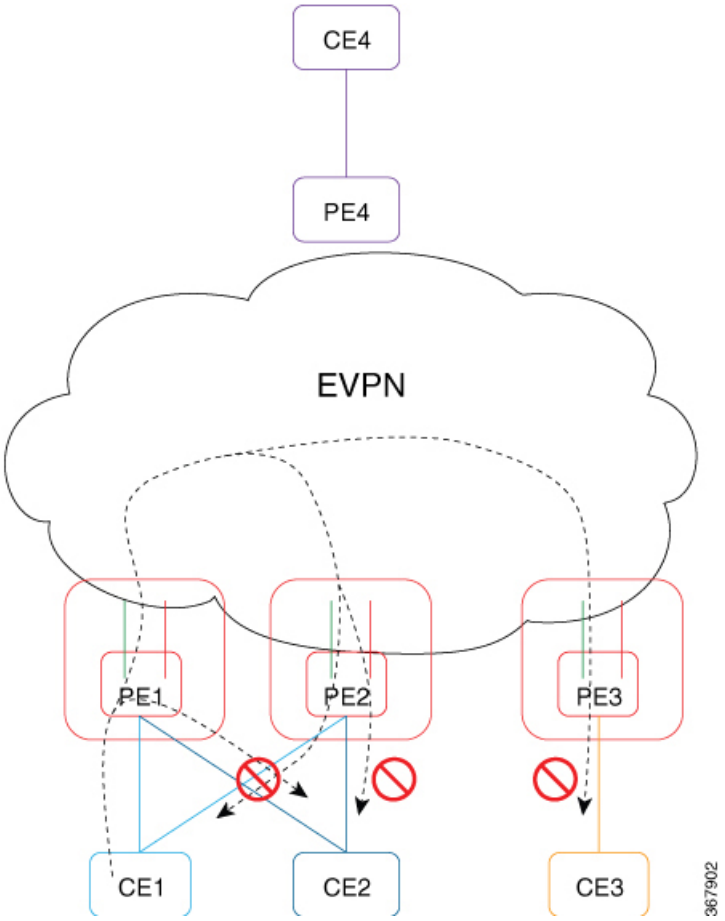
EVPN E-Tree

EVPN E-Tree 機能は、MPLS コアを介したルーテッドマルチポイントイーサネットサービスを提供します。EVPNイーサネットツリー（E-Tree）サービスを使用することで、接続回線（AC）

をルート サイトまたはリーフ サイトとして定義できます。これにより、ネットワークのロード バランシングやループの回避が容易になります。

次のトポロジでは、PE1、PE2、および PE3 をリーフ AC と見なし、PE4 をルート AC と見なしています。ルート AC は、他のすべての AC と通信できます。リーフ AC は、ルート AC と通信できますが、L2 ユニキャストまたは L2 BUM トラフィックのどちらを使用しても他のリーフ AC とは通信できません。E-Tree のリーフとして設定されていない PE は、デフォルトでルートと見なされます。この機能では、PE 単位でのリーフ サイトまたはルート サイトのみがサポートされます。

図 *39 : EVPN E-Tree*



E-Tree リーフは、EVI ブリッジ ドメイン（BD）ごとに設定されます。BD のルートおよびリーフ EVI は、単一のルーテッド ターゲット（RT）をエクスポートまたはインポートします。E-Tree リーフが EVI ごとに設定されるため、次のことが導かれます。

- すべての AC がリーフ インジケータを継承します。
- 同じ EVI の AC（リーフ）間でスプリットホライズン グループが自動的に有効になります。

- 各 PE リーフは、Ethernet Segment per Ethernet Auto Discovery（ES-EAD）ごと、Ethernet Segment Identifier（ESI）ごと、およびリーフインジケータと E-Tree ラベルを持つ ES-EAD ESI 0 ルートごとに、BGP へのアドバタイズを行います。
- この EVI の下で学習されたすべてのローカル MAC は、E-Tree リーフインジケータを使用して BGP に再アドバタイズされます。
- PE はそれぞれリモート PE のリストを維持します。

（注） E-Tree リーフ設定を変更した場合、ローカルに学習された MAC アドレスはすべて消去されます。ローカルに学習された MAC アドレスは、ブリッジ ポートのサブインターフェイスでの「カプセル化」または「リライト」、あるいは「スプリットホライズン グループ」設定が、ブリッジ ポートの下で変更された場合であっても、すべて消去されます。

ユニキャストのルール

次の表は、ルートおよびリーフで タイプ 2 MAC ルートを受信したときのユニキャストのルールを示しています。

受信した MAC ルート	MAC ルートの処理
ルート EVI（BD）からの非ローカル ESI を持つ MAC アドレス	リモート MAC アドレス。
ルート EVI（BD）からのローカル ESI を持つ MAC アドレス	MAC アドレスの同期、再発信。
リーフ EVI（BD）からの非ローカル ESI を持つ MAC アドレス	リモート MAC アドレス。 リーフインジケータを持つリモート MAC ルートはドロップされます。
リーフ EVI（BD）からの非ローカル ESI を持つ MAC アドレス	MAC アドレスの同期、再発信。MAC アドレスはローカル AC を指し示します。 ローカル AC の障害時に、同期 MAC ルートがリモート MAC ルートになります。リーフ インジケータを持つリモート MAC ルートは、ピアリング PE を指し示すのではなく、ドロップされます。

マルチキャストのルール

マルチキャストは、次の場合にネットワーク内のリーフの検出に使用されます。

- どの EVI が E-Tree リーフとして設定されているかを他のネットワーク PE に示すために、E-Tree 拡張コミュニティを持つ RT-1 ES-EAD ESI-0 ルートが EVI（BD）ごとに送信される場合。
- リーフ EVI（BD）で、E-Tree 拡張コミュニティを持つ RT-1 ES-EAD ESI-0 ルートおよび RT-3 IMCAST ルートを受信した場合。

（注） ローカル EVI（BD）ごとのスプリットホライズン グループによって、ローカル AC から AC へのトラフィック フローが阻止されます。

CE1 と CE4 間の通信（サブネット間）

1. CE1 が、自身のゲートウェイ（IRB インターフェイス）に ARP 要求を送信します。CE1 が、BVI の IP アドレスを解決します。
2. ARP 要求が PE1 のブリッジ ドメインに到達します。PE1 が、エントリを学習し、フラッディングします。
3. すべてのリモート PE への ARP 要求のうち、プルーニングされたものがドロップされます。これは、すべてのルートのリモート PE およびローカル BVI インターフェイスに複製されます。
4. PE1 の BVI インターフェイスが、自身の BVI IP アドレスと BVI MAC アドレスを使用して、ARP 応答を CE1 に送信します。
5. 同時に、ホスト ルーティングが設定されているため、PE1 がルート タイプ 2 を使用して EVPN を介して CE1 ホスト ルートをアドバタイズします。
6. タイプ 2 ルートの受信後、PE に基づいて異なるルールが適用されます。ルート タイプ 2 を受信した後、それぞれの PE の動作は次のようになります。
    1. PE2：ESI の MAC および IP アドレスがローカル ESI と一致します。MAC アドレスを同期ルートとしてプログラムします。RIB の IP アドレスを、PE1 を指し示すようにプログラムしますが、MAC アドレスは CE1 を指し示します。CE1 へのリンク障害が発生すると、MAC アドレスは、ピアリング PE1 を指し示すのではなく、ハードウェアでドロップ済みとマークされます。
    2. PE3：ESI の MAC および IP アドレスはローカルではありません。ローカル EVI（BD）はリーフであるため、MAC アドレスはハードウェアでドロップ済みとマークされます。RIB の IP アドレスを、PE1 を指し示すようにプログラムします。
    3. PE4：ESI の MAC および IP アドレスはローカルではありません。ローカル EVI（BD）はルートであるため、MAC をリモートとしてプログラムします。RIB の IP アドレスを、PE1 を指し示すようにプログラムします。
7. PE4 が CE1 を認識します。CE1 と CE4 が相互に通信します。

8. たとえば、CE4 から着信するルーティング パケットが PE4 に到達します。IP ルックアップが実行されます。PE1 が、ホスト ルート /32 によって最適な宛先として検出されます。PE1 にパケットが転送されます。
9. PE1 で、IP ルックアップが実行されます。BVI インターフェイスが見つかります。パケットが、ARP によって学習された宛先 MAC アドレスとして、CE1 を使用してカプセル化されます。送信元 MAC アドレスは BVI MAC アドレスのままです。宛先 MAC アドレスのルックアップが、対応するブリッジ ドメインで実行されます。適切な出力インターフェイスにパケットが転送されます。

（注） CE1 が通信を開始する前に CE4 が CE1 にパケットを送信した場合、パケットがピアリング PE2 に到達する可能性があります。GLEAN の隣接関係が影響を受け、解決するまでトラフィックはドロップされます。エントリを解決するため、PE2 BVI インターフェイスはプローブを開始します。

1. BVI からの ARP プローブが、すべての AC に送信され、EVI にも送信されます（L2 ストレッチ）。
2. PE1 と PE3 が、EVI インターフェイスから ARP プローブを受信し、すべてのローカル AC に複製します。CE1 が ARP 応答を送信します。すべてのリーフ上の IRB が分散型エニーキャスト ゲートウェイで設定されているため、PE1 BVI インターフェイスが応答を受け取ります。

CE1 と CE3 間の通信（サブネット内）

1. CE1 と CE3 は同じサブネット内にあります。
2. CE1 が、CE3 に ARP 要求を送信します。
3. ARP 要求が PE1 のブリッジ ドメインに到達します。PE1 が、エントリを学習し、フラッディングします。
4. すべてのリモート PE への ARP 要求のうち、プルーニングされたものがドロップされます。これは、すべてのルートのリモート PE およびローカル BVI インターフェイスに複製されます。
5. CE3 は、CE1 から ARP 要求を受信しません。CE1 は、CE3 と通信しません。
6. CE1 と CE3 をサブネット内で通信させる場合は、ローカルとリモートの両方の PE で、BVI インターフェイスの配下で local_proxy_arp を設定する必要があります。

CE1 と CE2 間の通信（サブネット内）

1. CE1 と CE2 は同じサブネット内にあります。
2. CE1 が、CE2 に ARP 要求を送信します。

3. ARP 要求が PE1 のブリッジ ドメインに到達します。PE1 が、エントリを学習し、フラッディングします。
4. すべてのリモート PE への ARP 要求のうち、プルーニングされたものがドロップされます。共通のスプリットホライズン グループが原因で、どのローカル AC にも複製されません。
5. CE2 は CE1 から ARP 要求を受信しません。CE1 は CE2 と通信しません。

（注） ローカル CE1 とリモート CE1 間の通信は次のようになります。

- PE1 のローカル CE1 から PE2 のリモート CE1 への BUM トラフィックは、PE2 がプルーニングされているためドロップされます。
- AC 対応 VLAN バンドル機能の場合、PE1 のローカル CE1 から PE1 のローカル CE1 への BUM トラフィックは、ESI フィルタリングによってドロップされます。

EVPN E-Tree の設定

EVPN E-Tree 機能を設定するには、次の作業を実行します。

```
/* Configure EVPN E-Tree service on PE1 and PE2 */

Router# configure
Router(config)# evpn
Router(config-evpn)# evi 1
Router(config-evpn-evi)# etree leaf
```

設定例

```
/* Configure MCLAG on PE1 for dual-home all-active EVPN */

Router# configure
Router(config)# redundancy
Router(config-redundancy)# ICCP group 1
Router(config-iccp-group)# mlacp node 1
Router(config-iccp-group)# mlacp system mac 000d.0002.0011
Router(config-iccp-group)# mlacp system priority 1
Router(config-iccp-group)# mode singleton
Router(config-iccp-group)# backbone
Router(config-iccp-group-backbone)# interface Bundle-Ether110
!

Router# configure
Router(config)# interface Bundle-Ether1121
Router(config-if)# description DH-F2-1
Router(config-if)# lacp switchover supress-flaps 300
Router(config-if)# mlacp iccp-group 1
Router(config-if)# bundle wait-while 100
Router(config-if)# load-inerval 30

/* Configure MCLAG on PE2 for dual-home all-active EVPN  */
```

```
Router# configure
Router(config)# redundancy
Router(config-redundancy)# ICCP group 1
Router(config-iccp-group)# mlacp node 2
Router(config-iccp-group)# mlacp system mac 000d.0002.0011
Router(config-iccp-group)# mlacp system priority 1
Router(config-iccp-group)# mode singleton
Router(config-iccp-group)# backbone
Router(config-iccp-group-backbone)# interface Bundle-Ether120
!
Router# configure
Router(config)# interface Bundle-Ether1121
Router(config-if)# description DH-F2-1
Router(config-if)# lacp switchover supress-flaps 300
Router(config-if)# mlacp iccp-group 1
Router(config-if)# bundle wait-while 100
Router(config-if)# load-inerval 30

/* Configure AC interface on PE1 and PE2*/

Router(config)# interface Bundle-Ether1121.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag pop 1 symmetric

/* Configure BVI interface on PE1 and PE2 */

Router(config)# interface BVI1
Router(config-if)# host-routing
Router(config-if)# vrf vpn1
Router(config-if-vrf)# ipv4 address 192.0.2.1 255.255.255.0
Router(config-if-vrf)# proxy-arp
Router(config-if-vrf)# local-proxy-arp
Router(config-if-vrf)# 2001:DB8::1/32
Router(config-if-vrf)# mac-address 10.1111.aaaa
Router(config-if-vrf)# load-interval 30

/* Configure the bridge on PE1 and PE2 */

Router(config)# l2vpn
Router(config-l2vpn)# bridge group bg1
Router(config-l2vpn-bg)# bridge-domain bd1
Router(config-l2vpn-bg-bd)# interface Bundle-Ether1121.1
Router(config-l2vpn-bg-bd-ac)# exit
Router(config-l2vpn-bg-bd)# routed interface BVI1
Router(config-l2vpn-bg-bd-bvi)# exit
Router(config)# evpn
Router(config-evpn)# evi
Router(config-evpn-evi)# commit
```

実行コンフィギュレーション

ここでは、EVPN E-Tree の実行コンフィギュレーションを示します。

```
/* EVPN E-Tree running configuration on PE1 */
redundancy
 iccp
  group 1
   mlacp node 1
   mlacp system mac 000d.0002.0011
   mlacp system priority 1
```

```
   mode singleton
   backbone
    interface Bundle-Ether110
  !
interface Bundle-Ether1121
 description DH-F2-1
 lacp switchover suppress-flaps 300
 mlacp iccp-group 1
 bundle wait-while 100
 load-interval 30

!

evpn
 evi 1
  etree leaf
  !

l2vpn
 bridge group bg1
  bridge-domain bd1
   interface Bundle-Ether1121.1
   routed interface BVI1
  !
  evi 1

interface Bundle-Ethe1121.1
l2transport
 encapsulation dot1q 1
 rewrite ingress tag pop 1 symmetric
 !
!
interface BVI1
 host-routing
 vrf vpn1
 ipv4 address 192.0.2.1 255.255.255.0
 proxy-arp
 local-proxy-arp
 ipv6 address 2001:DB8::1/32
 mac-address 10.1111.aaaa
 load-interval 30
 !
!


/* EVPN E-Tree running configuration On PE2 */
redundancy
 iccp
  group 1
   mlacp node 2
   mlacp system mac 000d.0002.0011
   mlacp system priority 1
   mode singleton
   backbone
    interface Bundle-Ether120
  !
!
interface Bundle-Ether1121
 description DH-F2-1
 lacp switchover suppress-flaps 300
 mlacp iccp-group 1
 bundle wait-while 100
 load-interval 30
```

```
evpn
 evi 1
  etree leaf
  !
 !

l2vpn
 bridge group bg1
  bridge-domain bd1
   interface Bundle-Ether1121.1
   routed interface BVI1
  !
  evi
 !
interface Bundle-Ethe1121.1
l2transport
 encapsulation dot1q 1
 rewrite ingress tag pop 1 symmetric
 !
!
interface BVI1
 host-routing
 vrf vpn1
 ipv4 address 192.0.2.1 255.255.255.0
 proxy-arp
 local-proxy-arp
 ipv6 address 2001:DB8::1/32
 mac-address 10.1111.aaaa
 load-interval 30
 !
!
```

確認

次の項に示す show 出力には、EVPN E-Tree の設定の詳細が表示されます。

```
Router#show bgp l2vpn evpn rd 10.0.0.1:0
Route Distinguisher: 10.0.0.1:0
*> [1][10.0.0.1:1][0000.0000.0000.0000.0000][4294967295]/184
                     0.0.0.0                              0 i
*> [1][10.0.0.1:2][0000.0000.0000.0000.0000][4294967295]/184
                     0.0.0.0                              0 i

Each RT-1 ES0 has up to 200 RTs. Two RT-1 ES0 is displayed if you have 250 RTs.
```

次の出力は、RT-1 ES0 でアドバタイズされたリーフ excom を示しています。

```
Router#show bgp l2vpn evpn rd 10.0.0.1:0
[1][10.0.0.1:1][0000.0000.0000.0000.0000][4294967295]/184
Extended community: EVPN E-TREE:0x00:824348 RT:100:1 RT:100:2 RT:100:3 RT:100:4 RT:100:5
 RT:100:10 RT:100:11
RT:100:12 RT:100:13 RT:100:14 RT:100:15 RT:100:16 RT:100:17 RT:100:18 RT:100:19 RT:100:20
 RT:100:21 RT:100:22 RT:100:23
RT:100:24 RT:100:25 RT:100:26 RT:100:27 RT:100:28 RT:100:29 RT:100:30 RT:100:31 RT:100:32
 RT:100:33 RT:100:34 RT:100:35
RT:100:36 RT:100:37 RT:100:38 RT:100:39 RT:100:40 RT:100:41 RT:100:42 RT:100:43 RT:100:44
 RT:100:45 RT:100:46 RT:100:47
 RT:100:48 RT:100:49 RT:100:50
```

次の出力は、MAC アドバタイズメントの RT 2 を示しています。

```
Router#show bgp l2vpn evpn rd 10.0.0.1:1 [2][1][48][0011.1100.0001][0]/104
Paths: (2 available, best #1)
  Advertised to peers (in unique update groups):
    172.16.0.1
  Path #1: Received by speaker 0
  Advertised to peers (in unique update groups):
    172.16.0.1
  Local
    0.0.0.0 from 0.0.0.0 (10.0.0.1)
     Origin IGP, localpref 100, valid, redistributed, best, group-best, import-candidate,
 rib-install
      Received Path ID 0, Local Path ID 1, version 315227
      Extended community: SoO:192.168.0.1:1 EVPN E-TREE:0x01:0 RT:100:1
      EVPN ESI: 0020.0000.0000.0000.1121
```

次の出力は、MAC アドレスと IP アドレスのアドバタイズメントにおける 1 つの RT 2 を示しています。

```
Router#show bgp l2vpn evpn rd 10.0.0.1:1 [2][1][48][0011.1100.0001][32][101.0.1.103]/136
Tue Oct  2 16:44:26.755 EDT
BGP routing table entry for [2][1][48][0011.1100.0001][32][101.0.1.103]/136, Route
Distinguisher: 10.0.0.1:1
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker             313139      313139
    Local Label: 820002
Last Modified: Oct  2 13:26:08.477 for 03:18:18
Paths: (2 available, best #1)
  Advertised to peers (in unique update groups):
    172.16.0.1
  Path #1: Received by speaker 0
  Advertised to peers (in unique update groups):
    172.16.0.1
  Local
    0.0.0.0 from 0.0.0.0 (10.0.0.1)
      Second Label 825164
     Origin IGP, localpref 100, valid, redistributed, best, group-best, import-candidate,
 rib-install
      Received Path ID 0, Local Path ID 1, version 313139
      Extended community: Flags 0xe: SoO:192.168.0.1:1 EVPN E-TREE:0x01:0 RT:100:1
RT:991:1
      EVPN ESI: 0020.0000.0000.0000.1121
```

次の出力は、EVPN における RT-3 包含マルチキャストおよび RT-1 ES0 ルートの集約を示しています。

```
Router#show evpn evi vpn-id 1 inclusive-multicast detail
1          MPLS   0          192.168.0.1
    TEPid  : 0x02000001
    PMSI Type: 0
    Nexthop: 192.168.0.1
    Label  : 810120
    Source : Remote
    E-Tree: Leaf
1          MPLS   0          10.0.0.1
    TEPid  : 0xffffffff
    PMSI Type: 6
    Nexthop: ::
    Label  : 820120
    Source : Local
    E-Tree: Leaf
```

```
1          MPLS    0          172.16.0.1
    TEPid  : 0x02000003
    PMSI Type: 0
    Nexthop: 172.16.0.1
    Label  : 840120
    Source : Remote
    E-Tree: Root
```

関連項目

- EVPN E-Tree （272 ページ）

関連コマンド

- etree leaf
- show bgp l2vpn evpn rd

IRB での DHCPv4 リレー

統合ルーティングおよびブリッジング（IRB）での DHCPv4 リレー機能は、EVPN オールアクティブ マルチホーミングのシナリオにおいて DHCP のサポートをエンドユーザに提供します。この機能により、トラフィックのフラッディングの削減、ロード シェアリングの増加、トラフィックの最適化、リンクやデバイスの障害時におけるコンバージェンスの高速化、およびデータセンター自動化のシンプル化が実現します。

DHCPv4 リレー エージェントは、エンド ユーザ用のアドレス（/32）割り当てを要求するために、アクセス インターフェイスを介して着信した要求パケットを外部 DHCPv4 サーバに向けて送信します。DHCPv4 リレー エージェントは、DHCPv4 バインディングと、割り当てられたアドレスの各ルート エントリを維持しません。そのため、エンド ユーザに対してステートレスとして機能します。

DHCPv4 リレー プロファイルはブリッジグループ仮想インターフェイス（BVI）インターフェイス上で設定されます。BVI インターフェイスは、エンド ユーザのルーティング ドメインとブリッジ ドメインを統合することによってアクセスインターフェイスとして機能します。これにより、レイヤ 2 接続回線（AC）からの DHCPv4 要求がホスト IPv4 アドレス（/32）の外部 DHCP サーバにリレーされます。

マルチホーミング オールアクティブ EVPN ゲートウェイ

マルチホーミング オールアクティブ EVPN ゲートウェイは、エニーキャスト IP アドレスと MAC アドレスを使用して設定されます。シスコのルータには、集中型 L2 または L3 ゲートウェイがあります。IRB は、ネイティブ EVPN と MAC ラーニングに基づいて、分散エニーキャスト IP アドレスとエニーキャスト MAC アドレスを使用します。スタティック クライアントは、エニーキャスト ゲートウェイアドレスを使用して、デフォルト ゲートウェイとして設定されます。DHCP クライアントは、BVI インターフェイスを介して IP アドレス割り当てのための DHCP 要求を送信します。L2 アクセスは、シングル ホーミングまたはマルチホーミングのどちらにもなり、すべてのアクセス プロトコルが IRB でサポートされるわけではありません。BVI の IP アドレスは、エンド ユーザのデフォルト ゲートウェイとして機能します。外部

DHCPv4 サーバは、この BVI インターフェイスの IP アドレスをルート オプションのデフォルト ゲートウェイとして提供します。インターネット ゲートウェイでは EVPN は設定されません。

EVPN IRB ルート配布

EVPN IRB DHCPv4 では、DHCP アプリケーションプロセスと DHCP パケット転送は EVPN IRB L2 および L3 ルーティングとは独立しています。ステートレス DHCP リレーに関するサブスクライバ ルーティング情報はありません。ただし、DHCP クライアントは、L2 および L3 ブリッジングおよびルーティングを行うために、EVPN コアでスタティック クライアントと同様に機能します。DHCP リレー エージェントで **relay information option** コマンドおよび **relay information option vpn** コマンドを設定すると、DHCP リレー エージェントによって DHCP オプション 82 のサブ オプション（サブネット選択や VPN ID オプションなど）が挿入されます。これらのオプションは、IP アドレスの割り当て時に DHCP サーバによって考慮されます。

DHCPv4 サーバにおけるエンド ユーザの IP アドレスの割り当ては、**relay agent information** オプション（リモート ID と回線 ID）に基づいて行われます。DHCP クライアントは L2 AC インターフェイスを使用して、EVPN ブリッジ ドメインにアクセスし、BVI インターフェイスをデフォルト ゲートウェイとして使用します。そのためクライアントは、BVI インターフェイスの同じサブネットの DHCP サーバから IP アドレスを取得する必要があります。

DHCPv4 アプリケーションが **relay-option policy {encapsulate | drop | keep}** コマンドに基づいて BVI インターフェイスを介してアクセス側の DHCPv4 パケットを受信すると、DHCPv4 アプリケーションには、DHCPv4 サーバのオプション 82 リレーエージェント情報、リモート ID、および回線 ID が追加されます。

次の表に、設定されたリレー情報の詳細を得るために DHCPv4 リレー パケットを絞り込む属性を示します。この表に記載されている情報は、**relay-option policy {encapsulate | drop | keep}** コマンドの設定に使用します。

リレーオプションポリシー	DHCPv4 アクセス側パケット	ローカル設定	DHCPv4 リレー パケットの決定
Encapsulate	リレー情報なし	リモート ID を持つ DHCPv4 プロファイル 回線 ID を持つ L2 トランスポート AC	リモート ID と回線 ID を持つリレーエージェント
Encapsulate	リレー情報（リモート ID と回線 ID）	リモート ID を持つ DHCPv4 プロファイル 回線 ID を持つ L2 トランスポート AC	リレーエージェント情報をローカル設定（リモート ID と回線 ID）にオーバーライド

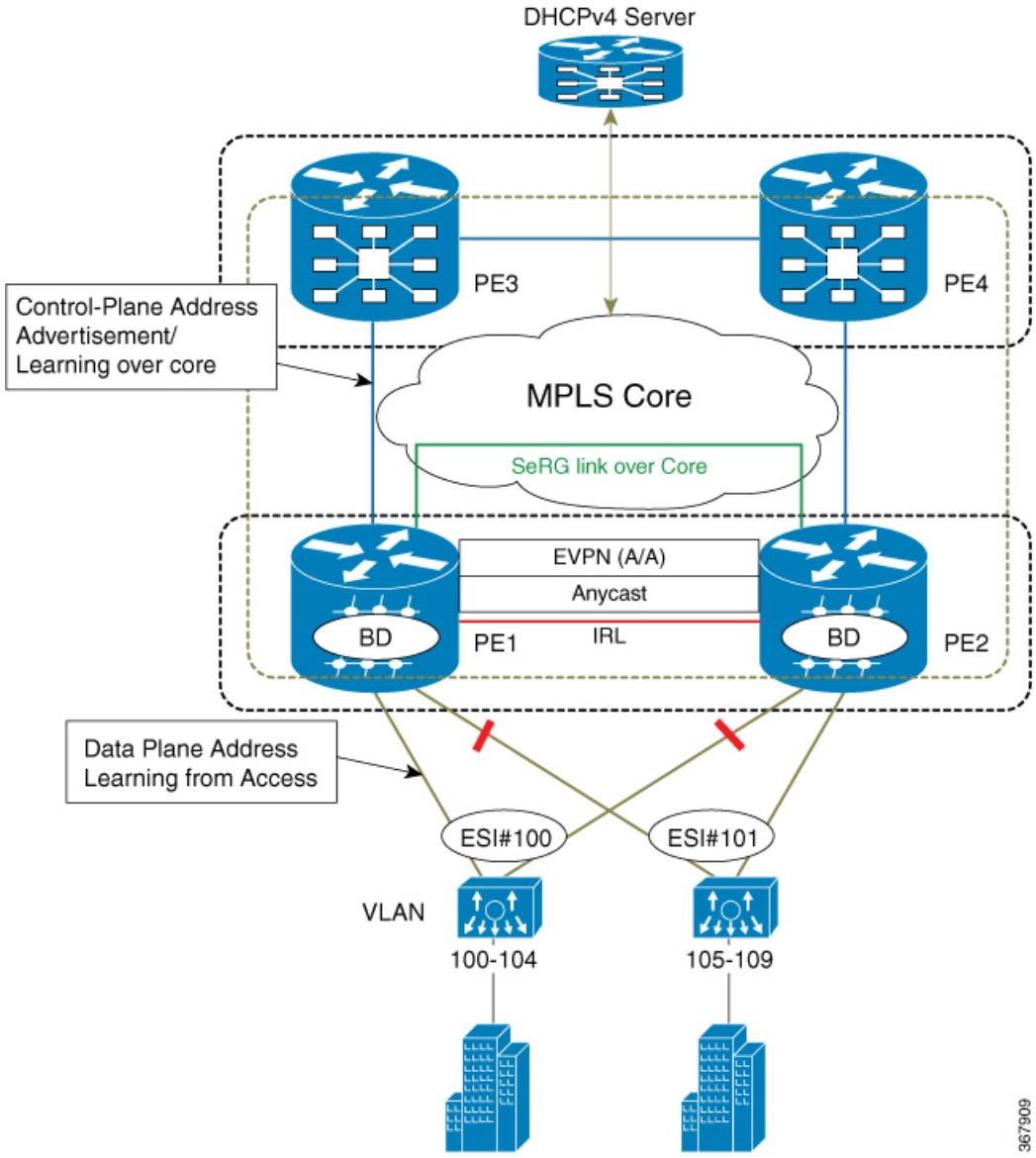
リレーオプションポリシー	DHCPv4 アクセス側パケット	ローカル設定	DHCPv4 リレー パケットの決定
Encapsulate	リレー情報なし	リモート ID および VPN 情報を持つ DHCPv4 プロファイル 回線 ID を持つ L2 トランスポート AC	リモート ID、回線 ID、および VPN 情報を持つリレーエージェント
Keep	リレー情報（リモート ID と回線 ID）	設定なし	DHCPv4 リレーエージェントはリレー情報を変更しない
Keep	リレー情報（リモート ID と回線 ID）	リモート ID を持つ DHCPv4 プロファイル 回線 ID を持つ L2 トランスポート AC	DHCPv4 リレーエージェントはリレー情報を変更しない
Keep	リレー情報（リモート ID と回線 ID）	リモート ID および VPN 情報を持つ DHCPv4 プロファイル 回線 ID を持つ L2 トランスポート AC	DHCPv4 リレーエージェントはリレー情報を変更しない
Drop	リレー情報（リモート ID と回線 ID）	設定なし	リレーエージェント情報を除外し、リレーパケットに「None」を追加
Drop	リレー情報（リモート ID と回線 ID）	リモート ID を持つ DHCPv4 プロファイル 回線 ID を持つ L2 トランスポート AC	リレーエージェント情報を除外し、リレーパケットに「None」を追加
Drop	リレー情報（リモート ID と回線 ID）	リモート ID および VPN 情報を持つ DHCPv4 プロファイル 回線 ID を持つ L2 トランスポート AC	リレーエージェント情報を除外し、リレーパケットに「None」を追加

DHCP 要求転送パス

クライアントは、要求をアクセス スイッチにブロードキャストし、DH-AA を EVPN PE ルータにブロードキャストします。アクセス スイッチはロード バランシングを行います。アクセス スイッチのロード バランシング設定は、DHCP 要求を送信する DH-AA および DHCP の PE に

影響を及ぼします。DHCP 要求は、DHCP リレーで設定されたブリッジ ドメイン（BD）BVI インターフェイスに到達します。オールアクティブ PE ルータは同じ IP アドレスを使用して設定されているため、BVI IP アドレスを DHCP リレー送信元 IP アドレスとして使用することはできません。DHCPv4 リレーの場合、アクセス（BVI）インターフェイスはリレー プロファイルを使用して関連付けられます。デバイス インターセプト パケットは BVI インターフェイスを介して受信され、各リレー プロファイルはゲートウェイ IP アドレス（GIADDR）を使用して定義されます。GIADDR は、DHCPv4 サーバに向けて開始されたリレー パケットの送信元 IP アドレスとして機能します。この GIADDR は、それぞれの BVI インターフェイスのトップ オブ ラック（ToR）全体で一意です。一意の IPv4 アドレスを持つループバック インターフェイスは、DHCP サーバに到達可能な VRF で設定できます。DHCP リレー送信元アドレスの設定はサポートされていません。

図 *40 : EVPN* オールアクティブ マルチホーミングを行うための *DHCPv4* サーバの処理における *PON* の動作



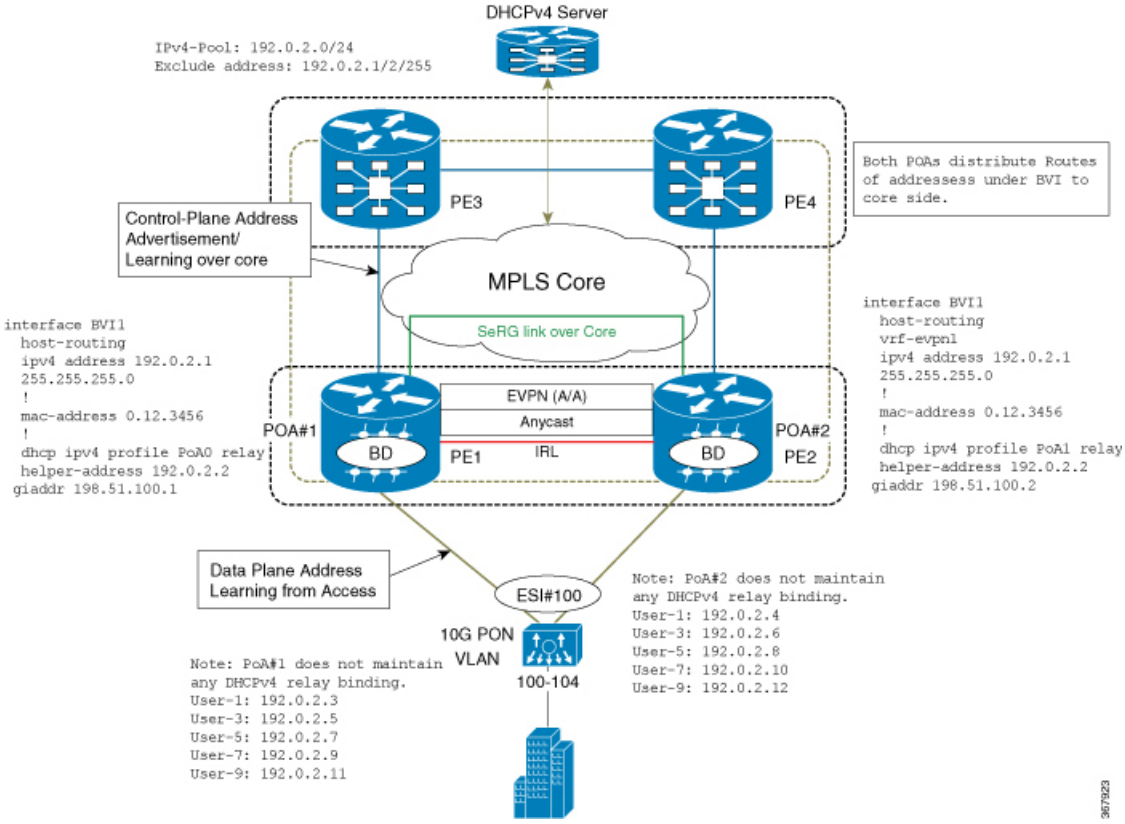
EVPN オールアクティブ マルチホーミングを行うための DHCPv4 サーバの処理における PON の動作

このトポロジでは、PE1 と PE2 はアクセス側のエッジルータです。エッジルータは、ルーティングおよびブリッジング ドメインを関連付けて DHCPv4 パケットを処理することにより、BVI インターフェイスを介した CE（10G-OLT）として機能します。CE（L2 OLT、PON、任意の L2 ドメイン スイッチ）は、着信した制御パケット（DHCPv4 パケット）を、それぞれの PE に接続されているポート チャネルに向けてハッシュします。CE は、エンドユーザから受信したパケットの 5 つのタプル（src mac、dst mac、src-ip、dst-ip、L4（tcp/udp）dst/src port）に基づいてハッシュ メカニズムを利用し、転送メカニズムを定義します。そのために、デュアルホームのアクティブ-アクティブ モデルにおいて、各 PE への制御パケットのロード バランシングにおけるポート チャネルを選択します。

デフォルト VRF での EVPN および DHCPv4 サーバの DHPCv4 リレー処理

EVPN IRB および DHCPv4 サーバを介した DHCPv4 リレーは、同じデフォルト VRF に存在します。DHCPv4 リレー プロファイルは、デフォルト VRF 配下の DHCPv4 アドレスのヘルパー アドレスに関連付けられています。この特定のシナリオでは、PE には、DHCPv4 サーバに向けてリレーされた DHCPv4 パケット内のリレーエージェント情報は追加されません。ただし、DHCPv4 リレー プロファイルは、エニーキャスト IRB アドレス以外の ToR にわたって一意の GIADDR で定義されます。そうしないと、DHCPv4 サーバは、リンクの選択やサブネットの選択を行わないエンド ユーザのアドレス割り当てを実行することが困難になります。VPN 値を 0xFF として VPN 情報が追加されることで、PE にリレーエージェント情報が追加されます。

図 *41* : デフォルト *VRF* での *EVPN* および *DHCPv4* サーバの *DHPCv4* リレー処理

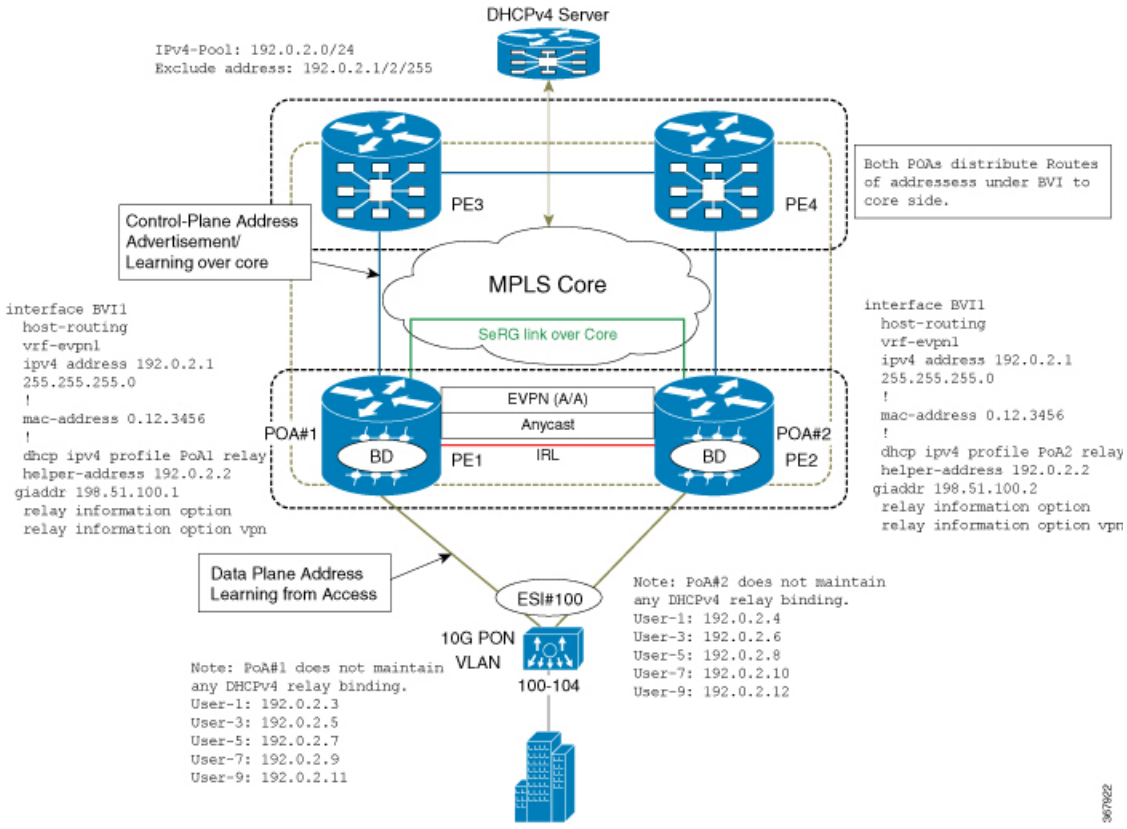


異なる VRF での EVPN および DHCPv4 サーバの DHPCv4 リレー処理

EVPN IRB および DHCPv4 サーバを介した DHCPv4 リレーは、異なる VRF に存在します。または、DHCPv4 サーバに、ToR にわたって一意の GIADDR（エニーキャスト IRB アドレスとは異なる）があります。そうしないと、DHCPv4 サーバは、リンクの選択やサブネットの選択を行わないエンドユーザのアドレス割り当てを実行することが困難になります。DHCPv4 サーバが、evpn の関連するエニーキャスト IRB アドレスのサブネット プールから確実にアドレス割り当てを行えるように、DHCPv4 リレー エージェントの ToR が仮想サブネット選択（リンク選択、server-id、vrf-id）を暗に指定する方法があります。それには、DHCPv4 サーバに向けてリレーされた DHCPv4 検出および要求パケットに、リレーエージェント情報（オプション 82）を追加します。

このトポロジでは、10G PON は、それぞれの接続ポイント（PoA）#1、#2 に向けて均等に DHCP ブロードキャストを配信し、パケットが外部 DHCPv4 サーバにリレーされます。

図 *42 :* 異なる *VRF* での *EVPN* および *DHCPv4* サーバの *DHPCv4* リレー処理



IRB での DHCPv4 リレーの設定

IRB で DHCPv4 リレーを設定するには、次の作業を実行します。

設定例

```
/* PE1 configuration */

Router# configure
Router(config)# interface BVI1
Router(config-if)# host-routing
Router(config-if)# vrf-evpn1
Router(config-if)# ipv4 address 192.0.2.1 255.255.255.0
Router(config-if)# exit
Router(config)# mac-address 0.12.3456
!
Router# configure
Router(config)# dhcp ipv4
Router(config-dhcpv4)# profile PoA1 relay
Router(config-dhcpv4-relay-profile)# helper-address 192.0.2.2 giaddr 198.51.100.1
Router(config-dhcpv4-relay-profile)# relay information option vpn
Router(config-dhcpv4-relay-profile)# relay information option vpn-mode rfc
Router(config-dhcpv4-relay-profile)# commit
```

```
/* PE2 configuration */

Router# configure
Router(config)# interface BVI1
Router(config-if)# host-routing
Router(config-if)# vrf-evpn1
Router(config-if)# ipv4 address 192.0.2.1 255.255.255.0
Router(config-if)# exit
Router(config)# mac-address 0.12.3456
!
Router# configure
Router(config)# dhcp ipv4
Router(config-dhcpv4)# profile PoA2 relay
Router(config-dhcpv4-relay-profile)# helper-address 192.0.2.2 giaddr 198.51.100.2
Router(config-dhcpv4-relay-profile)# relay information option vpn
Router(config-dhcpv4-relay-profile)# relay information option vpn-mode rfc
Router(config-dhcpv4-relay-profile)# commit
```

次の例は、リモート ID と回線 ID を持つリレーエージェント情報を追加するための DHCPv4 リレー エージェントの設定を示しています。リモート ID は、BVI インターフェイスの下で関連付けられている DHCPv4 リレープロファイルで設定されます。DHCPv4 は、回線 ID を持つ L2 トランスポート AC を使用して設定されます。

```
Dhcp ipv4
 Profile RELAY relay
  Relay information option remote-id format-type asci cisco
  Relay information policy encapsulate
 !

interface BE1.100 relay information option circuit-id format-type hex cisco
!
 interface bvi relay RELAY
!
```

実行コンフィギュレーション

ここでは、RB での DHCPv4 リレーの実行コンフィギュレーションを示します。

```
/* PE1 Configuration */
interface BVI1
 host-routing
 vrf-evpn1
 ipv4 address 192.0.2.1 255.255.255.0
 !
 mac-address 0.12.3456
!
 dhcp ipv4 profile PoA1 relay
 helper-address 192.0.2.2 giaddr 198.51.100.1
 relay information option
 relay information option vpn-mode rfc

/* PE2 Configuration */
interface BVI1
 host-routing
 vrf-evpn1
 ipv4 address 192.0.2.1 255.255.255.0
 !
 mac-address 0.12.3456
!
```

```
dhcp ipv4 profile PoA2 relay
helper-address 192.0.2.2 giaddr 198.51.100.2
relay information option
relay information option vpn-mode rfc
```

確認

RB での DHCPv4 リレーの設定を確認します。

```
/* Verify DHCPv4 relay statistics
Router# show dhcp vrf default ipv4 relay statistics

DHCP IPv4 Relay Statistics for VRF default:

     TYPE          |    RECEIVE    |    TRANSMIT   |     DROP      |
-----------------------------------------------------------------------
 DISCOVER          |          2000  |          2000  |             0  |
 OFFER             |          2000  |          2000  |             0  |
 REQUEST           |          5500  |          5500  |             0  |
 DECLINE           |             0  |             0  |             0  |
 ACK               |          5500  |          5500  |             0  |
 NAK               |             0  |             0  |             0  |
 RELEASE           |           500  |           500  |             0  |
 INFORM            |             0  |             0  |             0  |
 LEASEQUERY        |             0  |             0  |             0  |
 LEASEUNASSIGNED   |             0  |             0  |             0  |
 LEASEUNKNOWN      |             0  |             0  |             0  |
 LEASEACTIVE       |             0  |             0  |             0  |
 BOOTP-REQUEST     |             0  |             0  |             0  |
 BOOTP-REPLY       |             0  |             0  |             0  |
 BOOTP-INVALID     |             0  |             0  |             0  |


/* Verify DHCPv4 relay profile details */
Router# show dhcp ivp4 profile name PoA1 relay

Profile: PoA1 relay
Helper Addresses:
        192.0.2.2, vrf default, giaddr 198.51.100.1
Remote-Id Format  : [ascii | hex]
Remote-Id value   : cisco
Information Option: Enabled
Information Option Allow Untrusted: Enabled
Information Option VPN: Enabled
Information Option VPN Mode: RFC
Information Option Policy: Replace
```

関連項目

- IRB での DHCPv4 リレー （282 ページ）

関連コマンド

- show dhcp vrf default ipv4 relay statistics
- show dhcp ivp4 profile name

IRB での DHCPv6 リレー IAPD

Dynamic Host Configuration Protocol for IPv6（DHCPv6）の IRB でのリレー Identity Association for Prefix Delegation（IAPD）機能を使用すると、ユーザがリンク、サブネット、およびサイトアドレッシングの変更を管理できます。この機能により、顧客に自らのネットワーク内での使用を目的としてプレフィックスを割り当てるプロセスが自動化されます。プレフィックス委任は、DHCPv6 プレフィックス委任オプションを使用して、プロバイダー エッジ（PE）デバイスとカスタマー エッジ（CE）デバイスの間で行われます。委任されたプレフィックスが割り当てられたユーザは、プレフィックスをさらにサブネット化してネットワーク内のリンクに割り当てることができます。

DHCPv6 リレー エージェントは、エンドユーザ用の IAPD（::/64 または ::/48）割り当てを要求するために、アクセスインターフェイスを介して着信したすべての要求パケットを外部DHCPv6 サーバに向けて送信します。また、DHCPv6 リレーは、DHCPv6 サーバからの応答パケットを受信し、アクセスインターフェイスを介してエンドユーザにパケットを転送します。DHCPv6 リレーは、DHCPv6 PD バインディングと、割り当てられた IAPD の各ルート エントリを維持します。そのため、エンド ユーザに対してステートフルとして機能します。DHCPv6 リレーは、エンド ユーザ向けの Internet Assigned Numbers Authority（IANA）アドレス割り当てをサポートしていません。DHCPv6 リレーは、IAPD アドレス割り当てのみをサポートしています。IAPD プレフィックスは、DHCPv6 サーバで設定されているプレフィックス プールに基づきます。

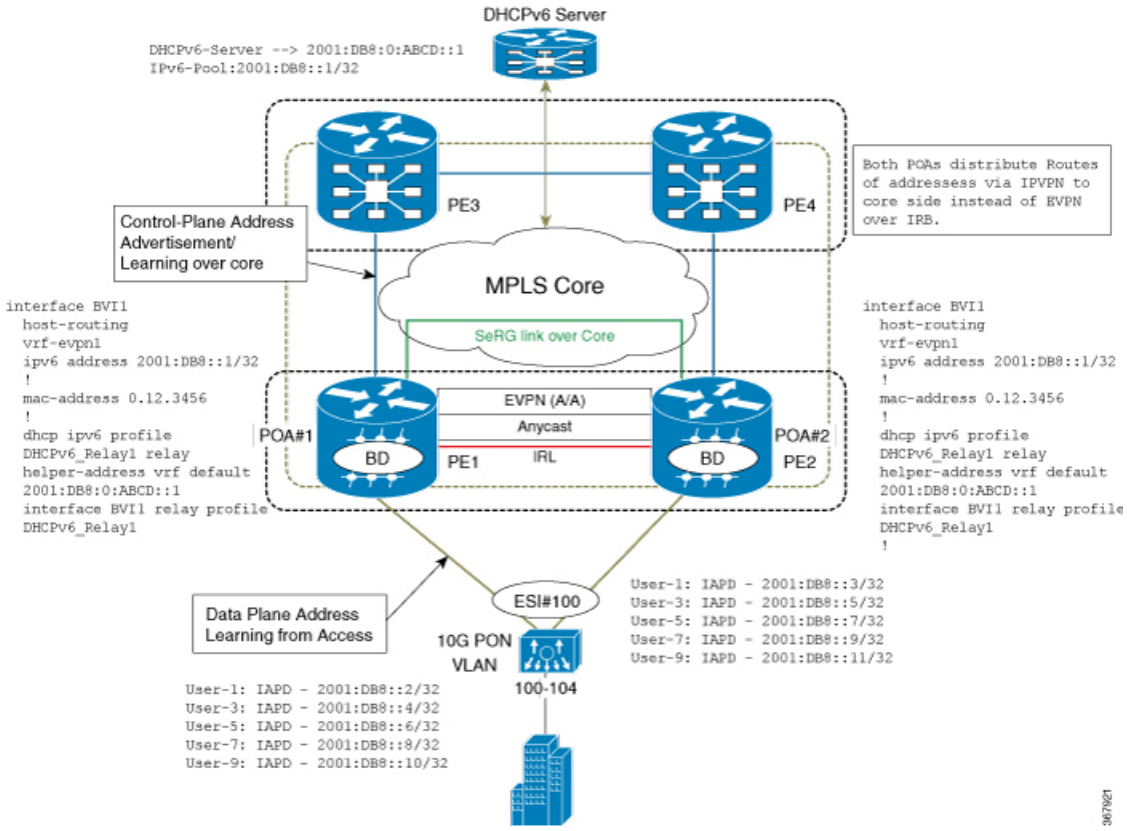
DHCPv6 リレーの場合、アクセス（BVI）インターフェイスはリレー プロファイルと関連付けられます。ToR は、クライアントから受信した DHCPv6 パケットを DHCPv6 サーバに送信するたびに、DHCPv6 サーバ IP アドレスの指定された定義済み VRF に対して最適な送信元 IP アドレスを検出します。ToR は、DHCPv6 サーバに到達するために、VRF ごとに一意の送信元 IP アドレスを維持しています。DHCPv6 リレーには、DHCPv6 ヘルパーアドレスの定義済み VRF のループバック インターフェイスで定義された一意の IPv4 送信元 IP アドレスがあり、MPLS コア ネットワークを介してルーティング可能です。

BVI インターフェイスで設定されたエニーキャスト IP アドレスは、エンド ユーザのデフォルト ゲートウェイとして機能し、同じサブネット上でアドレス割り当てが行われます。ToR は、MPLS コア ネットワークの IPVPN を介して DHCPv6 サーバに向けて DHCPv6 パケットをリレーするために、一意の送信元 IP アドレスを維持しています。同じ ToR は、外部 DHCPv6 サーバから応答パケットを受信します。DHCPv6 リレー配下における各 ToR の一意の送信元アドレスは、DHCPv6 プロセスにおいて、アクセス インターフェイスおよびリレー パケットを介して受信したパケットのコンテキストを維持するために必要です。このメカニズムは、BVI インターフェイスを介してエンド ユーザに応答を送信するのに役に立ちます。

デフォルト VRF での EVPN および DHCPv6 サーバの DHPCv6 リレー処理

EVPN IRB および DHCPv6 サーバを介した DHCPv6 リレーは、同じデフォルト VRF に存在します。DHCPv6 リレー プロファイルは、デフォルト VRF 配下の DHCPv6 アドレスのヘルパーアドレスに関連付けられています。DHCPv4 とは異なり、PE では DHPCv6 リレー パケットにリレー情報オプションが追加されません。

図 *43 :* デフォルト *VRF* での *EVPN* および *DHCPv6* サーバの *DHPCv6* リレー処理



IRB での DHCPv6 リレー IAPD の設定

IRB での DHCPv6 リレー IAPD を設定するには、次の作業を実行します。

設定例

```
/* PE1 configuration */

Router# configure
Router(config)# interface BVI1
Router(config-if)# host-routing
Router(config-if)# vrf-evpn1
Router(config-if)# ipv6 address 2001:DB8::1/32
Router(config-if)# exit
Router(config)# mac-address 0.12.3456
!
Router# configure
Router(config)# dhcp ipv6
Router(config-dhcpv6)# profile DHCPv6_Relay1 relay
Router(config-dhcpv6-relay-profile)# helper-address vrf default 2001: DB8:0:ABCD::1
Router(config-dhcpv6-relay-profile)# interface BVI1 relay profile DHCPv6_Relay
Router(config-dhcpv6-relay-profile)# commit
```

```
/* PE2 configuration */

Router# configure
Router(config)# interface BVI1
Router(config-if)# host-routing
Router(config-if)# vrf-evpn1
Router(config-if)# ipv6 address 2001:DB8::1/32
Router(config-if)# exit
Router(config)# mac-address 0.12.3456
!
Router# configure
Router(config)# dhcp ipv6
Router(config-dhcpv6)# profile DHCPv6_Relay1 relay
Router(config-dhcpv6-relay-profile)# helper-address vrf default 2001: DB8:0:ABCD::1
Router(config-dhcpv6-relay-profile)# interface BVI1 relay profile DHCPv6_Relay
Router(config-dhcpv6-relay-profile)# commit
```

実行コンフィギュレーション

ここでは、IRB での DHCPv6 リレー IAPD の実行コンフィギュレーションを示します。

```
/* PE1 Configuration */
interface BVI1
 host-routing
 vrf-evpn1
 ipv6 address 2001:DB8::1/32
 !
 mac-address 0.12.3456
!
 dhcp ipv6 profile DHCPv6_Relay1 relay
 helper-address vrf default 2001: DB8:0:ABCD::1
 interface BVI1 relay profile DHCPv6_Relay1
!

/* PE2 Configuration */interface BVI1
 host-routing
 vrf-evpn1
 ipv6 address 2001:DB8::1/32
 !
 mac-address 0.12.3456
!
 dhcp ipv6 profile DHCPv6_Relay1 relay
 helper-address vrf default 2001: DB8:0:ABCD::1
 interface BVI1 relay profile DHCPv6_Relay1
!
```

確認

IRB での DHCPv6 リレー IAPD の設定を確認します。

```
/* Verify DHCPv6 relay statistics
Router# show dhcp vrf default ipv6 relay statistics

DHCP IPv6 Relay Statistics for VRF default:

     TYPE         |    RECEIVE    |    TRANSMIT   |     DROP      |
-------------------------------------------------------------------
 DISCOVER         |         2000  |         2000  |            0  |
 OFFER            |         2000  |         2000  |            0  |
 REQUEST          |         5500  |         5500  |            0  |
```

```
DECLINE           |            0  |            0  |            0  |
ACK               |         5500  |         5500  |            0  |
NAK               |            0  |            0  |            0  |
RELEASE           |          500  |          500  |            0  |
INFORM            |            0  |            0  |            0  |
LEASEQUERY        |            0  |            0  |            0  |
LEASEUNASSIGNED   |            0  |            0  |            0  |
LEASEUNKNOWN      |            0  |            0  |            0  |
LEASEACTIVE       |            0  |            0  |            0  |
BOOTP-REQUEST     |            0  |            0  |            0  |
BOOTP-REPLY       |            0  |            0  |            0  |
BOOTP-INVALID     |            0  |            0  |            0  |
```

関連項目

- IRB での DHCPv6 リレー IAPD （291 ページ）

関連コマンド

- show dhcp ipv6 relay statistics vrf default

セッション冗長性を使用したオールアクティブ マルチホーミング対応 DHCPv6 PD 同期

セッション冗長性を使用したオールアクティブ マルチホーミング対応 DHCPv6 PD 同期機能は、制御パケットとデータ パケットの両方に対するロード バランシングを提供します。この機能は、スループット（ラインレート）と処理能力に関するデバイスの効率的な利用に役立ちます。

このリリースより前のリリースでは、セッション冗長性（SeRG）のメカニズムは、アクセス障害、コア障害、およびノード/シャーシ障害に対処するためのアクティブ-スタンバイをサポートしていました。これらすべての場合において、1 つのアクティブ PoA が、セッションを作成し、PoA 全体にわたって SeRG を使用してバインディング情報を同期する役割を担います。このメカニズムでは、SeRG グループ内の対象のアクセスリンクについて PoA がマスター/スレーブ モードであるために、EVPN オールアクティブ マルチホーミングの目的を果たすことができませんでした。この場合、制御パケットを処理し、バインディングを作成し、データ パスを転送するためにマスターとして機能するノードが 1 つだけに制限されます。

SeRG グループ設定を使用したオールアクティブ マルチホーミング対応 DHCPv6 PD 同期を使用すると、マスター/スレーブ モードとは異なり、両方の PoAA をアクティブにするように定義できます。また、それぞれの PoA のロールを交換またはネゴシエートする必要はありません。

SeRG では、どのルート タイプでも BGP を介して IAPD プレフィックス ルートが配布されることはありません。ルーテッド BVI インターフェイスは DHCPv6 リレーを使用して設定され、エンド ユーザに PD 割り当てを提供します。

個々のマルチホーミング ピア SeRG ロールは ACTIVE のみです。SeRG は、NONE および ACTIVE 以外のロールをサポートしていません。インターフェイスリストを BVI インターフェイスとし

て SeRG 配下に定義し、通常は 1 つまたは複数の BVI インターフェイスを使用します。ただし、L2 トランスポート AC を SeRG インターフェイスリスト配下に定義することは推奨されません。これは、L2 トランスポート AC は L2VPN BD 配下で定義されており、SeRG クライアントの DHCPv6 はこれらの AC 情報を認識しないためです。

SeRG アクティブ-アクティブ モードでは、IPv6-ND 同期は PoA 間で抑制されます。

制約事項

- SeRG はコア リンク障害をサポートしていません。
- SeRG はコアおよびアクセス トラッキング メカニズムをサポートしていません。
- `ACTIVE-ACTIVE` モードの設定中はバインディングが存在しないことを確認してください。
- 必ずすべての PoA で同じ設定を使用してください。バンドル-イーサ L2 トランスポート AC 設定は、BD と BVI の設定とともに、両側で同じにする必要があります。
- **clear session-redundancy** コマンドは、システムの不整合を回避するために、どのモードでもサポートされていません。
- SeRG アクティブ-アクティブ モードでは、両方の PoA が常にコア リンクを介して到達可能であることを確認してください。コア リンクをアクセス リンクにマッピングする EVPN コア分離機能を設定することをお勧めします。このメカニズムにより、コア リンクがダウンした場合は常に、それぞれのアクセス リンクが削除されることが保証されます。

DHCPv6 PD 同期の設定

SeRG を使用した DHCPv6 PD 同期を設定するには、次の作業を実行します。

設定例

```
/* PoA1 configuration */
Router# configure
Router(config)# session redundancy
Router(config-session-red)# source-interface Loopback0
Router(config-session-red)# group 1
Router(config-session-red-group)# peer 192.0.2.1
Router(config-session-red-group)# mode active-active
Router(config-session-red-group)# interface-list
Router(config-session-red-group-inft)# interface BVI1 id 1
Router(config-session-red-group-intf)# commit

/* PoA2 configuration */
Router# configure
Router(config)# session redundancy
Router(config-session-red)# source-interface Loopback0
Router(config-session-red)# group 1
Router(config-session-red-group)# peer 198.51.100.1
Router(config-session-red-group)# mode active-active
Router(config-session-red-group)# interface-list
```

```
Router(config-session-red-group-intf)# interface BVI1 id 1
Router(config-session-red-group-intf)# commit
```

実行コンフィギュレーション

ここでは、DHCPv6 PD 同期の実行コンフィギュレーションを示します。

```
/* PoA1 Configuration */
session-redundancy
source-interface Loopback0
group 1
  peer 192.0.2.1
  mode active-active
  interface-list
   interface BVI1 id 1
  !
!
!
/* PoA2 Configuration */
session-redundancy
source-interface Loopback0
group 1
  peer 198.51.100.1
  mode active-active
  interface-list
   interface BVI1 id 1
  !
!

!
```

確認

DHCPv6 PD 同期の設定を確認します。

```
/* Verify the session redundancy group */

Router# show session-redundancy group
Wed Nov 28 16:00:36.559 UTC
Session Redundancy Agent Group Summary
Flags    : E - Enabled, D - Disabled, M - Preferred Master, S - Preferred Slave
           H - Hot Mode, W - Warm Mode, T - Object Tracking Enabled
P/S      : Peer Status
           I - Initialize, Y - Retry, X - Cleanup, T - Connecting
           L - Listening, R- Registered, C - Connected, E - Established
I/F-P Count: Interface or Pool Count
SS Count : Session Count
------------------------------------------------------------------------------------------

   Node Name   | Group ID | Role | Flags  |         Peer Address        | P/S | I/F-P
Count |  SS Count  | Sync Pending
------------------------------------------------------------------------------------------
0/RP0/CPU0             1  Active   E-H-   120.1.1.1                     E
1           1              0
0/RP0/CPU0             2  Active   E-H-   120.1.1.1                     E
1           0              0
0/RP0/CPU0             3  Active   E-H-   120.1.1.1                     E
1           0              0
0/RP0/CPU0             4  Active   E-H-   120.1.1.1                     E
1           0              0
0/RP0/CPU0             5  Active   E-H-   120.1.1.1                     E
```

```
1           0               0
------------------------------------------------------------------------------------------------
Session Summary Count(Master/Slave/Active/Total): 0/0/1/1

/* Verify IPv6 relay binding */

Router# show dhcp ipv6 relay binding
Summary:
Total number of clients: 1

IPv6 Prefix: 60:1:1:1::/64 (BVI1)
    Client DUID: 000100015bfeb921001094000000
    IAID: 0x0
    VRF: default
    Lifetime: 120 secs (00:02:00)
    Expiration: 91 secs (00:01:31)
    L2Intf AC: Bundle-Ether1.1
    SERG State: SERG-ACTIVE
    SERG Intf State: SERG-ACTIVE
```

関連項目

- セッション冗長性を使用したオールアクティブ マルチホーミング対応 DHCPv6 PD 同期（294 ページ）

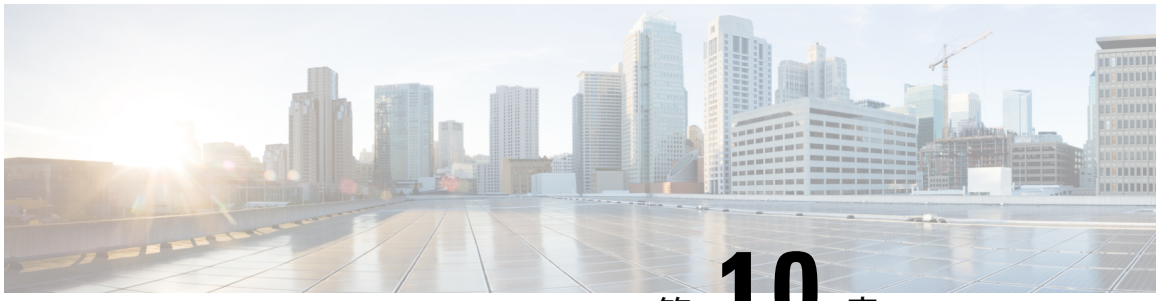
関連コマンド

- show session-redundancy group
- show dhcp ipv6 relay binding

DHCPv6 リレーにおける IAPD ルートの配布と取り消し

EVPN マルチホーミング アクティブ-アクティブのシナリオが存在する場合、DHCPv6 リレー エージェントは、接続回線（AC）および BVI インターフェイスに関連付けられた L2VPN ブリッジ ドメインを介してサポートされ、Identity Association for Prefix Delegation（IAPD）ルートの割り当てが行われます。また、DHCPv6 リレー エージェントは、iBGP を使用して MPLS コア ネットワーク経由でルート配布を実行します。コアからサブスクライバへのトラフィックでは、少数の AC がダウンする可能性がありますが、すべての AC がダウンするわけではないため、BVI は引き続きアップ状態です。このシナリオでは、ダウンした AC 内のサブスクライバでトラフィック ブロック ホールが生じる可能性があります。トラフィック ブロック ホールが生じる理由は IAPD ルートに関するものです。IAPD ルートは、AC がダウンしても MPLS コア ネットワークについては引き続きアップ状態です。

トラフィック ブロック ホールを防止するため、DHCPv6 リレー エージェントをイネーブルにして、セッションの iBGP を介して MPLS コア ネットワークからの IAPD ルートの取り消しを実行します。ルートの取り消しは、L2VPN ブリッジ ドメインの AC がダウンすると必ず発生します。また、AC がアップ状態に戻るたびに、DHCPv6 リレー エージェントは iBGP を介して IAPD ルートを MPLS コア ネットワークに配布できます。

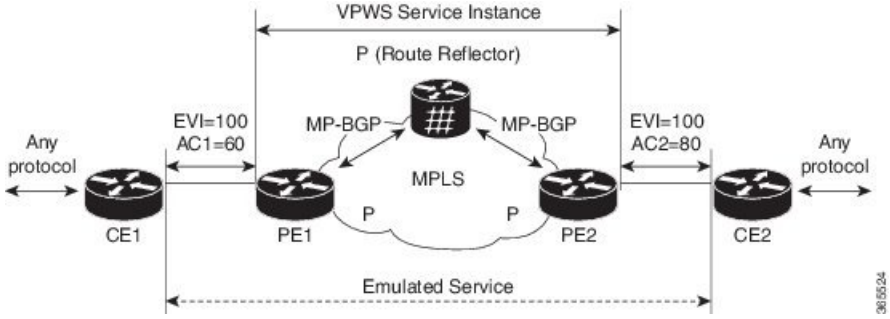


第 10 章

EVPN-VPWS シングル ホーム

EVPN-VPWS シングル ホーム ソリューションは、EVI イーサネット自動検出ルートごとに必要です。EVPN は、すべての EVPN ルートの伝送に使用する新しい BGP ネットワーク層到達可能性情報（NLRI）を定義します。BGP 機能アドバタイズメントを使用して、2 つのスピーカーが RFC 4760 に従い、EVPN NLRI（AFI 25、SAFI 70）を確実にサポートするようにします。

EVPN VPWS のアーキテクチャでは、PE3 がコントロール プレーンでマルチプロトコル BGP を実行します。次に、EVPN-VPWS 設定を説明する図を示します。



- PE1 上の VPWS サービスには、設定時に指定する次の 3 つの要素が必要です。
  - VPN ID（EVI）
  - ローカル AC 識別子（AC1）。エミュレートされたサービスのローカル エンドを識別します。
  - リモート AC 識別子（AC2）。エミュレートされたサービスのリモート エンドを識別します。

  PE1 は到達可能性を得るために、MPLS ラベルをローカル AC ごとに割り当てます。
- PE2 上の VPWS サービスは PE1 と同じ方法で設定されます。3 つの同じ要素が必要であり、サービス設定は対称になっている必要があります。

  PE2 は到達可能性を得るために、MPLS ラベルをローカル AC ごとに割り当てます。

- PE1は各ローカルエンドポイント（AC）のEVIイーサネットADごとの単一のEVPNを、関連付けられたMPLSラベルを使用してリモートPEにアドバタイズします。

  PE2は同じタスクを実行します。

- PE2からEVI EADルートごとのEVPNを受け取ると、PE1はそのローカルL2 RIBにエントリを追加します。PE1はAC2に到達するパスのリスト（たとえば、ネクストホップがPE2のIPアドレスであること）とAC2のMPLSラベルを把握しています。

  PE2は同じタスクを実行します。

- EVPN-VPWS シングル ホームの設定 （300 ページ）
- EVPN-VPWS マルチホーム （301 ページ）
- EVPN VPWS 対応フロー ラベルのサポート （304 ページ）

EVPN-VPWS シングル ホームの設定

この項では、シングルホームEVPN-VPWS機能を設定する方法について説明します。

```
Router# configure
Router(config)# router bgp 100
Router(config-bgp)# address-fmaily l2vpn evpn
Router(config-bgp-af)# neighbor 10.10.10.1
Router(config-bgp-af)# commit
Router(config-bgp-af)# exit
Router(config-bgp)# exit
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group evpn-vpws
Router(config-l2vpn-xc)# p2p evpn1
Router(config-l2vpn-xc-p2p)# interface TenGigE0/1/0/2
Router(config-l2vpn-xc-p2p)# neighbor evpn evi 100 target 12 source 10
Router(config-l2vpn-xc-p2p)# commit
Router(config-l2vpn-xc-p2p)# exit
```

実行コンフィギュレーション

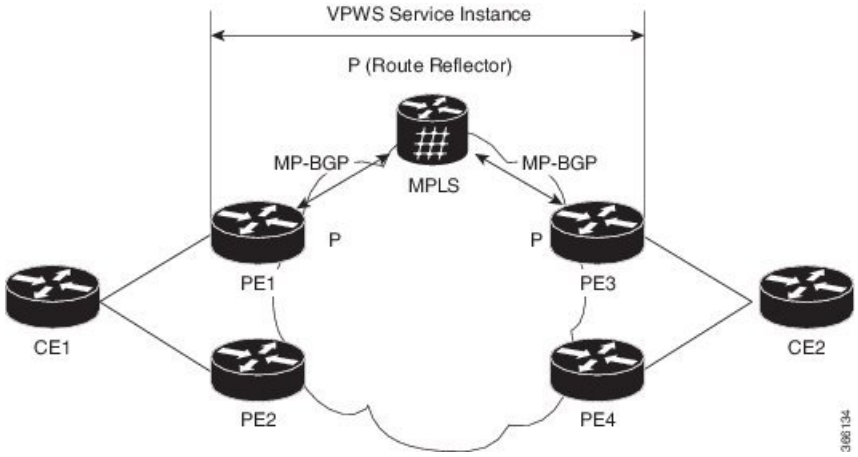
```
configure
router bgp 100
 address-fmaily l2vpn evpn
  neighbor 10.10.10.1
!

configure
l2vpn
 xconnect group evpn-vpws
  p2p evpn1
   interface TenGigE0/1/0/2
   neighbor evpn evi 100 target 12 source 10
!
```

EVPN-VPWS マルチホーム

EVPN VPWS 機能は、カスタマー エッジ デバイスを 2 台以上のプロバイダー エッジ（PE）デバイスに接続し、ロード バランシングと冗長接続を提供できるオールアクティブ マルチホーミング機能をサポートしています。ロードバランシングは等コストマルチパス（ECMP）を使用して実行されます。

CE デバイスが 2 つ以上の PE のマルチホームで、すべての PE が VLAN のマルチホーム デバイスとの間で発着信するトラフィックを転送できる場合のマルチホーミングをオールアクティブ マルチホーミングと呼びます。

図 *44 : EVPN VPWS* マルチホーム



CE1 が PE1 と PE2 のマルチホームで、CE2 が PE3 と PE4 のマルチホームであるトポロジを考えてみます。PE1 と PE2 は AC あたり EVI ルートごとの EAD をリモート PE、つまり PE3 と PE4 へ、関連付けられた MPLS ラベルを使用してアドバタイズします。ES-EAD ルートは ES（メインインターフェイス）ごとにアドバタイズされますが、これにはラベルはありません。同様に、PE3 と PE4 は AC あたり EVI ルートごとの EAD をリモート PE、つまり PE1 と PE2 へ、関連付けられた MPLS を使用してアドバタイズします。

CE1 から CE2 へのトラフィック フローを考えてみます。PE1 または PE2 のいずれかにトラフィックが送信されます。パスの選択は、LAG を介して転送する CE の実装によって異なります。トラフィックは各 PE でカプセル化され、MPLS コアを通じてリモート PE の（PE3 と PE4）に転送されます。宛先 PE の選択は、フローベースのロード バランシングによって確立されます。PE3 と PE4 は CE2 にトラフィックを送信します。PE3 または PE4 から CE2 へのパスの選択は、フローベースのロードバランシングによって確立されます。

障害が発生し、CE から PE1 へのリンクがダウンしている場合、PE1 は ES-EAD ルートを撤回し、リモート PE に信号を送信してこのマルチホーム ES に関連付けられているすべての VPWS サービス インスタンスをバックアップ PE、つまり PE2 に切り替えます。

EVPN-VPWS マルチホームの設定

この項では、マルチホーム EVPN-VPWS 機能を設定する方法について説明します。

```
/* Configure PE1 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)#  xconnect group evpn_vpws
Router(config-l2vpn-xc)#  p2p e1_5-6
Router(config-l2vpn-xc-p2p)#  interface Bundle-Ether10.2
Router(config-l2vpn-xc-p2p)#  neighbor evpn evi 1 target 5 source 6
Router(config-l2vpn-xc-p2p)# exit
Router(config-l2vpn-xc)# exit
Router(config-l2vpn)# exit
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether10
Router(config-evpn-ac)#  ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 00.01.00.ac.ce.55.00.0a.00
Router(config-evpn-ac-es)# commit


/* Configure PE2 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)#  xconnect group evpn_vpws
Router(config-l2vpn-xc)#  p2p e1_5-6
Router(config-l2vpn-xc-p2p)#  interface Bundle-Ether10.2
Router(config-l2vpn-xc-p2p)#  neighbor evpn evi 1 target 5 source 6
Router(config-l2vpn-xc-p2p)# exit
Router(config-l2vpn-xc)# exit
Router(config-l2vpn)# exit
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether10
Router(config-evpn-ac)#  ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 00.01.00.ac.ce.55.00.0a.00
Router(config-evpn-ac-es)# commit


/* Configure PE3 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)#  xconnect group evpn_vpws
Router(config-l2vpn-xc)#  p2p e1_5-6
Router(config-l2vpn-xc-p2p)#  interface Bundle-Ether20.1
Router(config-l2vpn-xc-p2p)#  neighbor evpn evi 1 target 6 source 5
Router(config-l2vpn-xc-p2p)# exit
Router(config-l2vpn-xc)# exit
Router(config-l2vpn)# exit
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether20
Router(config-evpn-ac)#  ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 00.01.00.ac.ce.55.00.14.00
Router(config-evpn-ac-es)# commit


/* Configure PE4 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)#  xconnect group evpn_vpws
Router(config-l2vpn-xc)#  p2p e1_5-6
Router(config-l2vpn-xc-p2p)#  interface Bundle-Ether20.1
Router(config-l2vpn-xc-p2p)#  neighbor evpn evi 1 target 6 source 5
```

```
Router(config-l2vpn-xc-p2p)# exit
Router(config-l2vpn-xc)# exit
Router(config-l2vpn)# exit
Router(config)# evpn
Router(config-evpn)# interface Bundle-Ether20
Router(config-evpn-ac)#  ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 00.01.00.ac.ce.55.00.14.00
Router(config-evpn-ac-es)# commit
```

実行コンフィギュレーション

```
/* On PE1 */
!
configure
l2vpn xconnect group evpn_vpws
 p2p e1_5-6
  interface Bundle-Ether10.2
  neighbor evpn evi 1 target 5 source 6
!
evpn
interface Bundle-Ether10
  ethernet-segment
   identifier type 0 00.01.00.ac.ce.55.00.0a.00

!


/* On PE2 */
!
configure
l2vpn xconnect group evpn_vpws
 p2p e1_5-6
  interface Bundle-Ether10.2
  neighbor evpn evi 1 target 5 source 6
!
evpn
interface Bundle-Ether10
  ethernet-segment
   identifier type 0 00.01.00.ac.ce.55.00.0a.00

!

/* On PE3 */
!
configure
l2vpn xconnect group evpn_vpws
 p2p e1_5-6
  interface Bundle-Ether20.1
  neighbor evpn evi 1 target 6 source 5
!
evpn
interface Bundle-Ether20
  ethernet-segment
      identifier type 0 00.01.00.ac.ce.55.00.14.00

!

/* On PE4 */
!
configure
l2vpn xconnect group evpn_vpws
 p2p e1_5-6
  interface Bundle-Ether20.1
```

```
  neighbor evpn evi 1 target 6 source 5
!
evpn
interface Bundle-Ether20
  ethernet-segment
      identifier type 0 00.01.00.ac.ce.55.00.14.00

!
```

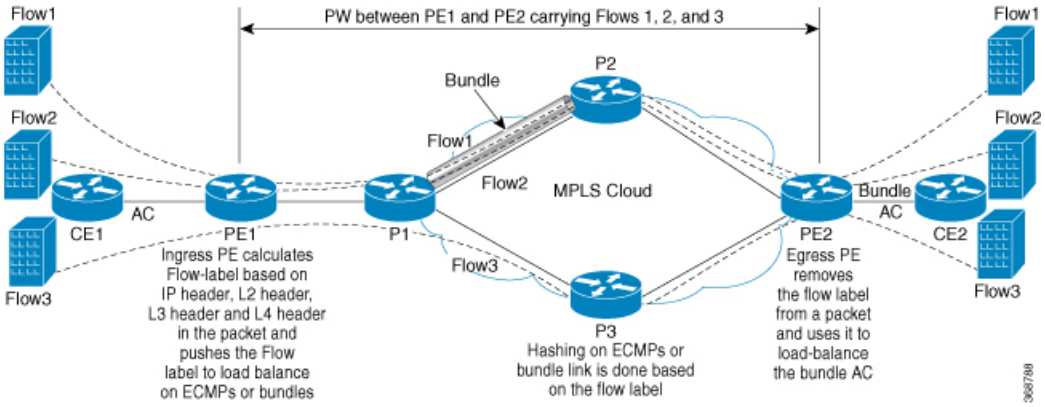
EVPN VPWS 対応フロー ラベルのサポート

EVPN VPWS のフロー ラベル サポート機能により、プロバイダー（P）ルータはフローベースのロード バランシングを使用して、プロバイダーエッジ（PE）デバイス間でトラフィックを転送できます。この機能は、MPLS パケット スイッチド ネットワーク上で疑似回線（PW）のフロー認識型転送（FAT）を使用して、仮想プライベート LAN サービス（VPLS）およびイーサネット VPN（EVPN）バーチャル プライベート ワイヤ サービス（VPWS）の BGP ベースのシグナリング擬似回線間でトラフィックのロードバランシングを行います。

FAT PW は、PW 内の個々のフローを識別する機能を提供します。また、ルータに対してこれらのフローを使用してトラフィックをロードバランスする機能を提供します。等価コストマルチパス（ECMP）が使用されている場合は、FAT PW はコア内のトラフィックのロード バランスに使用されます。インポジション PE に流入する不可分のパケット フローに基づいて、フロー ラベルが作成されます。このフロー ラベルは、パケットの一番下のラベルとして挿入されます。P ルータは、フロー ラベルをロードバランシングに使用し、コア内の ECMP パスに全体わたって、またはリンクがバンドルされたパス全体にわたって、より適切にトラフィックを分配します。フローは、トラフィックの送信元/宛先 IP アドレスとトラフィックのレイヤ 4 送信元/宛先ポートによって識別されるか、またはトラフィックの送信元/宛先 MAC アドレスによって識別されます。

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

図 *45 : FAT PW* と *ECMP* およびバンドルされたリンクに分配される *2* つのフロー



フロー ラベルと呼ばれるラベルがさらにスタックに追加されます。このラベルは、PE 上の一意の着信フローごとに生成されます。フロー ラベルは、PW 内のフローを区別する一意の ID

で、送信元/宛先 MAC アドレスと送信元/宛先 IP アドレスから取得されます。フロー ラベルには、ラベルスタック終端（EOS）ビットセットが含まれています。フロー ラベルは、VC ラベルの後ろ、およびコントロール ワード（存在する場合）の前に挿入されます。入力 PE は、フロー ラベルを計算し、転送します。FAT PW コンフィギュレーションは、フロー ラベルをイネーブルにします。出力 PE は、決定が行われないように、フロー ラベルを廃棄します。

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

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

制約事項

EVPN VPWS のフロー ラベルを設定する場合、次の制限事項が適用されます。

- この機能は、VPLS およびイーサネット LAN（E-LAN）サービスの EVPN ポイントツーマルチポイント（P2MP）ではサポートされていません。
- この機能は、EVPN VPWS シングル ホーミングでのみサポートされています。AC バンドル インターフェイスは ESI-0 でのみ設定する必要があります。
- この機能は、EVPN フレキシブル クロスコネクト サービスではサポートされていません。
- この機能は、EVPN VPWS マルチホーミングではサポートされていません。

EVPN VPWS のためのフロー ラベルの設定

設定例

PE1 と PE2 の両方で EVPN VPWS のフロー ラベルを設定するには、次の作業を実行します。

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group evpn-vpws
Router(config-l2vpn-xc)# p2p evpn1
Router(config-l2vpn-xc-p2p)# interface TenGigE0/0/0/0
Router(config-l2vpn-xc-p2p)# neighbor evpn evi 1 target 2 source 1
Router(config-l2vpn-xc-p2p)# exit
!
Router# configure
Router(config)# evpn
Router(config-evpn)# evi 1
Router(config-evpn-instance)# control-word-disable
Router(config-evpn-instance)# load-balancing
Router(config-evpn-instance-lb)# flow-label static
Router(config-evpn-instance-lb)# commit
```

実行コンフィギュレーション

ここでは、EVPN VPWS のフロー ラベルの実行コンフィギュレーションを示します。

```
l2vpn
 xconnect group evpn-vpws
  p2p evpn1
   interface TenGigE0/0/0/0
   neighbor evpn evi 1 target 2 source 1
   !
  !
evpn
 evi 1
  control-word-disable
  load-balancing
   flow-label static
  !
!
```

確認

EVPN VPWS のフロー ラベルの設定を確認します。

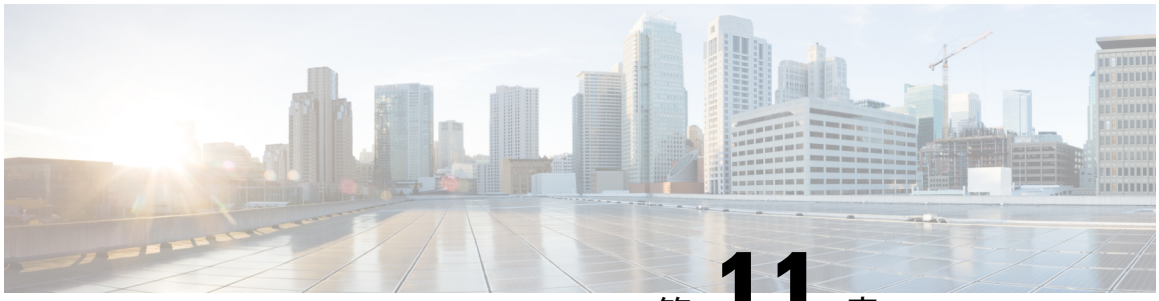
```
Router# show l2vpn xconnect detail
Group evpn-vpws, XC evpn1, state is up; Interworking none
  AC: TenGigE0/0/0/0, state is up
    Type Ethernet
    MTU 1500; XC ID 0x1; interworking none
    Statistics:
      packets: received 21757444, sent 0
      bytes: received 18226521128, sent 0
  EVPN: neighbor 100.100.100.2, PW ID: evi 1, ac-id 2, state is up ( established )
    XC ID 0xc0000001
    Encapsulation MPLS
   Encap type Ethernet, control word disabled
    Sequencing not set
    LSP : Up
    Flow Label flags configured (Tx=1,Rx=1) statically

      EVPN         Local                          Remote
      ------------ ------------------------------ ------------------------------
      Label        64002                          64002
      MTU          1500                           1500
      Control word disabled                       disabled
      AC ID        1                              2
      EVPN type    Ethernet                       Ethernet

      ------------ ------------------------------ ------------------------------
    Create time: 30/10/2018 03:04:16 (00:00:40 ago)
    Last time status changed: 30/10/2018 03:04:16 (00:00:40 ago)
    Statistics:
      packets: received 0, sent 21757444
      bytes: received 0, sent 18226521128
```

関連項目

- EVPN VPWS 対応フロー ラベルのサポート （304 ページ）

関連コマンド

- show evpn evi



第 11 章

SR-TE ポリシーを介した EVPN VPWS 優先パス

SR-TE ポリシーを介した EVPN VPWS 優先パス機能では、SR-TE ポリシーを使用して、EVPN VPWS 疑似回線（PW）の 2 つのエンドポイント間に優先パスを設定できます。SR ポリシーでは、EVPN インスタンス（EVI）ごとにパスを選択できます。この機能はバンドル接続回線（AC）と物理 AC でサポートされています。

制約事項

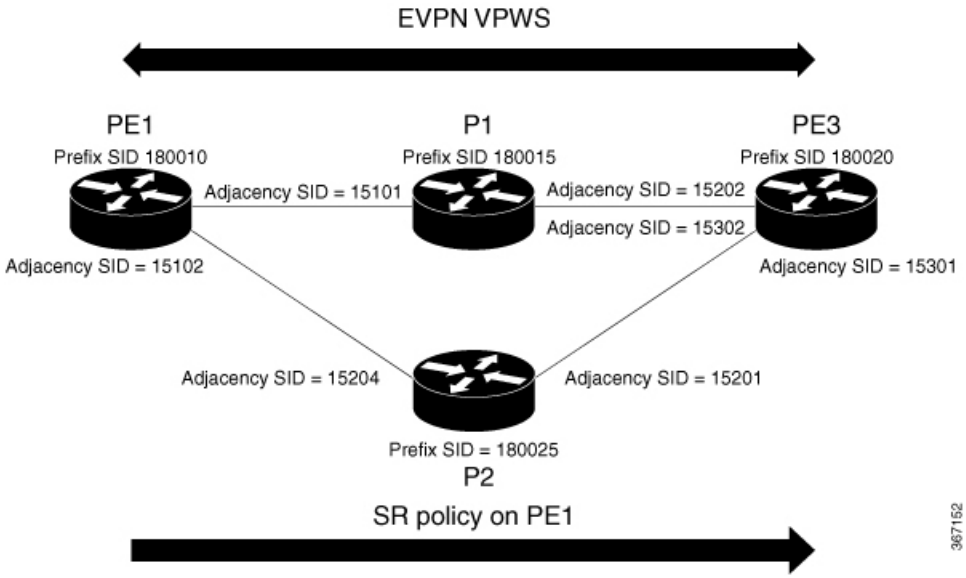
- オン デマンド ネクスト ホップ（ODN）を備えた EVPN VPWS を設定し、優先パスがある EVPN VPWS も同じ PW に設定すると、優先パスが優先されます。
- EVPN VPWS SR ポリシーは EVPN VPWS デュアル ホーミングではサポートされていません。
- EVPN はルートがシングル ホーム ネクスト ホップ用であるかどうかを検証します。そうでない場合は、不適切な SR-TE ポリシーに関するエラー メッセージを発行し、そのポリシーなしで EVPN-VPWS のセットアップを続行します。EVPN は、これがシングル ホームかどうかの決定をゼロに設定されている ESI 値に依存します。AC が LACP を実行しているバンドルイーサ インターフェイスの場合は、ESI 値を手動でゼロに設定して、自動感知 ESI を上書きする必要があります。これは、EVPN VPWS マルチホーミングがサポートされていないためです。

  EVPN デュアル ホーミングを無効にするには、バンドルイーサ AC を ESI 値セットをゼロに設定します。

```
evpn
interface Bundle-Ether12
  ethernet-segment
   identifier type 0 00.00.00.00.00.00.00.00.00
/* Or globally */
Evpn
 ethernet-segment type 1 auto-generation-disable
```

トポロジ

図 *46 : SR-TE* ポリシーを介した *EVPN VPWS* 優先パス



PE1 と PE3 が 2 つの EVPN VPWS PW エンドポイントであるトポロジを考えてみます。トラフィックはコア内の SR を通じて PE1 から PE3 に送信されます。PE1 からのトラフィックは、P1 ノードか P2 ノードのいずれかを通じて PE3 に送信できます。この例では、SR ポリシーを介した EVPN VPWS 優先パスが設定されており、プレフィックス SID を使用した PE1 から PE3 へのトラフィック フローが示されています。隣接 SID を使用することで、PE1 から PE3 へトラフィック フローを誘導し、P1 ノードを通過するか、P2 ノードを通過するかを指定します。

- SR-TE ポリシーを介した EVPN VPWS 優先パスの設定 （310 ページ）
- SR-TE ポリシーを介した L2VPN VPLS または VPWS 優先パス （323 ページ）
- SR-TE を使用した EVPN VPWS オンデマンド ネクスト ホップ （338 ページ）
- セグメント ルーティングの概要 （353 ページ）
- セグメント ルーティングの仕組み （354 ページ）
- セグメント ルーティング グローバル ブロック （355 ページ）

SR-TE ポリシーを介した EVPN VPWS 優先パスの設定

SR-TE ポリシー機能を介して EVPN VPWS 優先パスを確実に設定するには、次のタスクを実行する必要があります。

- IGP でのプレフィックス SID の設定：次の例は、IS-IS でプレフィックス SID を設定する方法を示しています。
- IGP での隣接関係 SID の設定：次の例は、IS-IS で隣接関係 SID を設定する方法を示しています。
- セグメントリストの設定

- SR-TE ポリシーの設定
- SR-TE ポリシーを介した EVPN VPWS の設定

ISIS でのプレフィックス SID の設定

PE1、P1、P2、および PE3 にプレフィックス SID を設定します。

```
/* Configure Prefix-SID on PE1 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# global-block 180000 200000
Router(config-sr)# exit
!
Router# configure
Route(config)# router isis core
Route(config-isis)# is-type level-2-only
Route(config-isis)# net 49.0002.0330.2000.0031.00
Route(config-isis)# nsr
Route(config-isis)# nsf ietf
Route(config-isis)# log adjacency changes
Route(config-isis)# address-family ipv4 unicast
Route(config-isis-af)# metric-style wide level 2
Route(config-isis-af)# mpls traffic-eng level-2-only
Route(config-isis-af)# mpls traffic-eng router-id 1.1.1.1
Route(config-isis-af)# segment-routing mpls sr-prefer
Route(config-isis-af)# segment-routing prefix-sid-map advertise-local
Route(config-isis-af)# exit
!
Route(config-isis)# interface loopback 0
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# prefix-sid index 180010
Route(config-isis-af)# commit
Route(config-isis-af)# exit

/* Configure Prefix-SID on P1 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# global-block 180000 200000
Router(config-sr)# exit
!
Router# configure
Router(config)# router isis core
Router(config-isis)# is-type level-2-only
Router(config-isis)# net 49.0002.0330.2000.0021.00
Router(config-isis)# nsr
Router(config-isis)# nsf ietf
Router(config-isis)# log adjacency changes
Router(config-isis)# address-family ipv4 unicast
Router(config-isis-af)# metric-style wide level 2
Router(config-isis-af)# mpls traffic-eng level-2-only
Router(config-isis-af)# mpls traffic-eng router-id loopback0
Router(config-isis-af)# segment-routing mpls sr-prefer
Router(config-isis-af)# segment-routing prefix-sid-map advertise-local
Router(config-isis-af)# exit
!
Router(config-isis)# interface loopback 0
```

```
Router(config-isis-if)# address-family ipv4 unicast
Router(config-isis-af)# prefix-sid index 180015
Router(config-isis-af)# commit
Router(config-isis-af)# exit

/* Configure Prefix-SID on P2 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# global-block  180000 200000
Router(config-sr)# exit
!
Router# configure
Route(config)# router isis core
Route(config-isis)# is-type level-2-only
Route(config-isis)# net 49.0002.0330.2000.0022.00
Route(config-isis)# nsr
Route(config-isis)# nsf ietf
Route(config-isis)# log adjacency changes
Route(config-isis)# address-family ipv4 unicast
Route(config-isis-af)# metric-style wide level 2
Route(config-isis-af)# mpls traffic-eng level-2-only
Route(config-isis-af)# mpls traffic-eng router-id loopback0
Route(config-isis-af)# segment-routing mpls sr-prefer
Route(config-isis-af)# segment-routing prefix-sid-map advertise-local
Route(config-isis-af)# exit
!
Route(config-isis)# interface loopback 0
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# prefix-sid index 180025
Route(config-isis-af)# commit
Route(config-isis-af)# exit

/* Configure Prefix-SID on PE3 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# global-block 180000 200000
Router(config-sr)# exit
!
Router# configure
Route(config)# router isis core
Route(config-isis)# is-type level-2-only
Route(config-isis)# net 49.0002.0330.2000.3030.0030.0035.00
Route(config-isis)# address-family ipv4 unicast
Route(config-isis-af)# metric-style wide level 2
Route(config-isis-af)# mpls traffic-eng level-2-only
Route(config-isis-af)# mpls traffic-eng router-id loopback0
Route(config-isis-af)# segment-routing mpls sr-prefer
Route(config-isis-af)# segment-routing prefix-sid-map advertise-local
Route(config-isis-af)# exit
!
Route(config-isis)# interface loopback0
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# prefix-sid index 180020
Route(config-isis-af)# commit
Route(config-isis-af)# exit
```

ISIS での隣接関係 SID の設定

PE1、P1、P2、および PE3 に隣接関係 SID を設定します。

```
/* Configure Adjacency-SID on PE1 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# local-block 15000 15999
!
Router# configure
Route(config)# router isis core
Route(config-isis)# interface Bundle-Ether121
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# adjacency-sid absolute 15101
Route(config-isis-if-af)# exit
!
Router# configure
Route(config)# router isis core
Route(config-isis)# interface TenGigE0/0/1/6
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# adjacency-sid absolute 15102
Route(config-isis-if-af)# commit

/* Configure Adjacency-SID on P1 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# local-block 15000 15999
!
Router# configure
Route(config)# router isis core
Route(config-isis)# interface Bundle-Ether121
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# metric 20
Route(config-isis-if-af)# adjacency-sid absolute 15200
Route(config-isis-if-af)# commit
!
Router# configure
Route(config)# router isis core
Route(config-isis)# interface TenGigE0/0/0/7
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# adjacency-sid absolute 15202
Route(config-isis-if-af)# commit
!
/* Configure Adjacency-SID on P2 */

Router# configure
```

```
Router(config)# segment-routing
Router(config-sr)# local-block 15000 15999
!
Router# configure
Route(config)# router isis core
Route(config-isis)# interface TenGigE0/0/0/7
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# metric 20
Route(config-isis-if-af)# adjacency-sid absolute 15201
Route(config-isis-if-af)# exit
!
Router# configure
Route(config)# router isis core
Route(config-isis)# interface TenGigE0/0/0/5
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# metric 20
Route(config-isis-if-af)# adjacency-sid absolute 15204
Route(config-isis-if-af)# commit

/* Configure Adjacency-SID on PE3 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# local-block 15000 15999
!
Router# configure
Route(config)# router isis core
Route(config-isis)# interface TenGigE0/0/0/1
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# adjacency-sid absolute 15301
Route(config-isis-if-af)# exit
!
Router# configure
Route(config)# router isis core
Route(config-isis)# interface TenGigE0/0/0/2
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# adjacency-sid absolute 15302
Route(config-isis-if-af)# commit
```

セグメントリストの設定

```
/* Configure Segment-list on PE1 using prefix-SID */

Router# configure
Router(config)# segment-routing
Router(config-sr)# global-block 180000 200000
Router(config-sr)# traffic-eng
Router(config-sr-te)# logging
```

```
Router(config-sr-te-log)# policy status
Router(config-sr-te-log)# exit
!
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# segment-list name pref_sid_to_PE3
Router(config-sr-te-sl)# index 1 mpls label 180020 <-----------------------using prefix-SID
Router(config-sr-te-sl)# exit

/* Configure Segment-list on PE1 using adjacency-SID */

Router# configure
Router(config)# segment-routing
Router(config-sr)# local-block  15000 15999
Router(config-sr)# traffic-eng
Router(config-sr-te)# logging
Router(config-sr-te-log)# policy status
Router(config-sr-te-log)# exit
!
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# segment-list name pref_adj_sid_to_PE3
Router(config-sr-te-sl)# index 1 mpls label 15101 <------------------------using
adjacency-SID
Router(config-sr-te-sl)# index 2 mpls label 15202 <------------------------using
adjacency-SID
Router(config-sr-te-sl)# exit
```

SR-TE ポリシーの設定

```
/* Configure SR-TE Policy */

Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy pref_sid_to_PE3
Router(config-sr-te-policy)# color 9001 end-point ipv4 20.20.20.20
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy)# preference 10
Router(config-sr-te-pp-info)# explicit segment-list pref_sid_to_PE3
Router(config-sr-te-pp-info)# commit
Router(config-sr-te-pp-info)# exit
!
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy pref_adj_sid_to_PE3
Router(config-sr-te-policy)# color 9001 end-point ipv4 20.20.20.20
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy)# preference 200
Router(config-sr-te-pp-info)# explicit segment-list pref_adj_sid_to_PE3
Router(config-sr-te-pp-info)# commit
Router(config-sr-te-pp-info)# exit

/* You can configure multiple preferences for an SR policy. Among the configured
preferences, the largest number takes the highest precedence */

Router# configure
```

```
Router(config)# segment-routing
Router(config-sr)# global-block 180000 200000
Router(config-sr)# local-block 15000 15999
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy 1013
Router(config-sr-te-policy)# color 1013 end-point ipv4 2.2.2.2
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy)# preference 100
Router(config-sr-te-pp-info)# explicit segment-list PE1-P1_BE121
Router(config-sr-te-pp-info)# exit
!
Router(config-sr-te-policy)# preference 200
Router(config-sr-te-pp-info)# explicit segment-list PE1-PE3-P1-t0016
Router(config-sr-te-pp-info)# exit
!
Router(config-sr-te-policy)# preference 700 <----------largest number takes the precendence
Router(config-sr-te-pp-info)# explicit segment-list PE1-P1
Router(config-sr-te-pp-info)# commit
Router(config-sr-te-pp-info)# exit
```

SR-TE ポリシーを介した EVPN VPWS の設定

（注） 自動生成された SR-TE ポリシー名を使用して、L2VPN インスタンスにポリシーをアタッチします。ポリシー名は、ポリシーの色とエンドポイントに基づいて自動生成されます。自動生成されたポリシー名を表示するには、**show segment-routing traffic-eng policy candidate-path name** *policy_name* コマンドを使用します。

```
Router# show segment-routing traffic-eng policy candidate-path name pref_sid_to_PE3

SR-TE policy database
---------------------
Color: 9001, End-point: 20.20.20.20
 Name: srte_c_9001_ep_20.20.20.20

Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# pw-class 1001
Router(config-l2vpn-pwc)# encapsulation mpls
Router(config-l2vpn-pwc-mpls)# preferred-path sr-te policy srte_c_9001_ep_20.20.20.20
fallback disable
Router(config-l2vpn-pwc-mpls)# commit
Router(config-l2vpn-pwc-mpls)# exit
!
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group evpn_vpws
Router(config-l2vpn-xc)# p2p evpn_vpws_1001
Router(config-l2vpn-xc-p2p)# interface tengi0/1/0/1.1001
Router(config-l2vpn-xc-p2p)# neighbor evpn evi 1001 target 10001 source 20001
Router(config-l2vpn-xc-p2p-pw)# pw-class 1001
Router(config-l2vpn-xc-p2p-pw)# commit
Router(config-l2vpn-xc-p2p-pw)# exit
```

```
/* If Fallback Enable is configured, which is the default option, and if the SR-policy
is down, then EVPN VPWS will still continue to be UP using the regular IGP path, and not
 using the SR-policy */
show l2vpn xconnect detail
  EVPN: neighbor 20.20.20.20, PW ID: evi 1001, ac-id 10001, state is up ( established )
    Preferred path Inactive : SR TE srte_c_9001_ep_20.20.20.20, Statically configured,
fallback enabled
    Tunnel : Down
    LSP: Up

/* If Fallback Disable is configured, and if the SR-policy is down, or if it misconfigured
 in dual homed mode, then the L2VPN PW will be down */
show l2vpn xconnect detail
EVPN: neighbor 20.20.20.20, PW ID: evi 1001, ac-id 10001, state is down ( local ready )
Preferred path Active : SR TE srte_c_9001_ep_20.20.20.20, Statically configured, fallback
 disabled
Tunnel : Down
```

実行コンフィギュレーション

```
/* Configure Prefix-SID in ISIS */
PE1:

configure
 segment-routing
  global-block 180000 200000
!
router isis core
 is-type level-2-only
 net 49.0002.0330.2000.0031.00
 nsr
 nsf ietf
 log adjacency changes
 address-family ipv4 unicast
  metric-style wide level 2
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id 1.1.1.1
  segment-routing mpls sr-prefer
  segment-routing prefix-sid-map advertise-local

interface Loopback0
  address-family ipv4 unicast
   prefix-sid index 180010

P1:

configure
 segment-routing
  global-block 180000 200000

router isis core
 is-type level-2-only
 net 49.0002.0330.2000.0021.00
 nsr
 nsf ietf
 log adjacency changes
 address-family ipv4 unicast
  metric-style wide level 2
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
```

```
  segment-routing mpls sr-prefer
  segment-routing prefix-sid-map advertise-local

 interface Loopback0
  address-family ipv4 unicast
   prefix-sid index 180015
```

P2:

```
configure
 segment-routing
  global-block 180000 200000

router isis core
 is-type level-2-only
 net 49.0002.0330.2000.0022.00
 nsr
 nsf ietf
 log adjacency changes
 address-family ipv4 unicast
  metric-style wide level 2
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
  segment-routing mpls sr-prefer
  segment-routing prefix-sid-map advertise-local

 interface Loopback0
  address-family ipv4 unicast
   prefix-sid index 180025
```

PE3:

```
configure
 segment-routing
  global-block 180000 200000

router isis core
 is-type level-2-only
 net 49.0002.0330.2000.3030.0030.0035.00
 address-family ipv4 unicast
  metric-style wide level 2
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
  segment-routing mpls sr-prefer
  segment-routing prefix-sid-map advertise-local

interface Loopback0
  address-family ipv4 unicast
   prefix-sid index 180020

/* Configure Adjacency-SID in ISIS */
```

PE1:

```
configure
 segment-routing
  local-block 15000 15999
!

router isis core
 !
interface Bundle-Ether121
  circuit-type level-2-only
  point-to-point
```

```
  hello-padding disable
  address-family ipv4 unicast
   adjacency-sid absolute 15101

interface TenGigE0/0/1/6
  circuit-type level-2-only
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
   adjacency-sid absolute 15102
```

P1:

```
configure
 segment-routing
  local-block 15000 15999

router isis core
 !
interface Bundle-Ether121
  circuit-type level-2-only
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
   metric 20
   adjacency-sid absolute 15200

interface TenGigE0/0/0/0/7
  circuit-type level-2-only
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
   metric 20
   adjacency-sid absolute 15202
```

P2:

```
configure
 segment-routing
  local-block 15000 15999

router isis core
 !
interface TenGigE0/0/0/5
  circuit-type level-2-only
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
   metric 20
   adjacency-sid absolute 15204

interface TenGigE0/0/0/0/7
  circuit-type level-2-only
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
   metric 20
   adjacency-sid absolute 15201
```

PE3:

```
configure
 segment-routing
  local-block 15000 15999
```

```
router isis core
  !
interface TenGigE0/0/0/1
  circuit-type level-2-only
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
   adjacency-sid absolute 15301
  !
 !
 interface TenGigE0/0/0/2
  circuit-type level-2-only
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
   adjacency-sid absolute 15302

/* Configure Segment-list */
PE1:

configure
 segment-routing
  global-block 180000 200000
  traffic-eng
   logging
    policy status

segment-routing
 traffic-eng
  segment-list name pref_sid_to_PE3
   index 1 mpls label 180020
  !
 !
configure
 segment-routing
  local-block 15000 15999
  traffic-eng
   logging
    policy status

segment-routing
 traffic-eng
  segment-list name pref_adj_sid_to_PE3
   index 1 mpls label 15101
   index 2 mpls label 15202
  !
 !

/* Configure SR-TE policy */

segment-routing
 traffic-eng
  policy pref_sid_to_PE3
   color 9001 end-point ipv4 20.20.20.20
   candidate-paths
    preference 10
     explicit segment-list pref_sid_to_PE3
     !
    !
segment-routing
 traffic-eng
  policy pref_adj_sid_to_PE3
   color 9001 end-point ipv4 20.20.20.20
```

```
   candidate-paths
    preference 200
     explicit segment-list pref_adj_sid_to_PE3
     !
    !

/* You can configure multiple preferences for an SR policy. Among the configured
preferences, the largest number takes the highest precedence */

segment-routing
 traffic-eng
  policy 1013
   color 1013 end-point ipv4 2.2.2.2
   candidate-paths
    preference 100
     explicit segment-list PE1-P1_BE121
     !
    preference 200
     explicit segment-list PE1-PE3-P1-t0016
     !
    preference 700
     explicit segment-list PE1-P1
     !

/* Configure EVPN VPWS over SR-TE policy */
PE1:
configure
 l2vpn
  pw-class 1001
   encapsulation mpls
    preferred-path sr-te policy srte_c_9001_ep_20.20.20.20 fallback disable
xconnect group evpn_vpws
  p2p evpn_vpws_1001
   interface tengi0/1/0/1.1001
   neighbor evpn evi 1001 target 10001 source 20001
    pw-class 1001
   !
```

SR-TE ポリシーを介した EVPN VPWS 優先パスの確認

```
PE1#show segment-routing traffic-eng forwarding policy name pref_sid_to_PE3 detail
Policy        Segment         Outgoing    Outgoing            Next Hop        Bytes
Name          List            Label       Interface                           Switched
------------- --------------- ----------- ------------------- --------------- ------------
pref_sid_to_PE3

                              15102       TenGigE0/0/1/6      20.20.20.20     81950960
                Label Stack (Top -> Bottom): { 15101, 15102 }
                Path-id: 1, Weight: 0
                Packets Switched: 787990
   Local label: 34555
   Packets/Bytes Switched: 1016545/105720680
   (!): FRR pure backup


PE1#show segment-routing traffic-eng policy candidate-path name pref_sid_to_PE3

SR-TE policy database
---------------------

Color: 9001, End-point: 20.20.20.20
```

```
  Name: srte_c_9001_ep_20.20.20.20


PE1#show mpls forwarding tunnels sr-policy name  pref_sid_to_PE3
Tunnel        Outgoing    Outgoing     Next Hop        Bytes
Name          Label       Interface                    Switched
------------- ----------- ------------ --------------- ------------
pref_sid_to_PE3 (SR) 15102 TenGigE0/0/1/6 20.20.20.20       836516512


PE1#show l2vpn xconnect group evpn_vpws xc-name evpn_vpws_1001 detail
Group evpn_vpws, XC evpn_vpws_1001, state is up; Interworking none
  AC: Bundle-Ether12.1001, state is up
    Type VLAN; Num Ranges: 1
    Outer Tag: 1000
    Rewrite Tags: []
    VLAN ranges: [1, 1]
    MTU 1500; XC ID 0xc0000018; interworking none
    Statistics:
      packets: received 642304, sent 642244
      bytes: received 61661184, sent 61655424
      drops: illegal VLAN 0, illegal length 0
  EVPN: neighbor 20.20.20.20, PW ID: evi 1001, ac-id 10001, state is up ( established )
    XC ID 0xa0000007
    Encapsulation MPLS
    Source address 10.10.10.10
    Encap type Ethernet, control word enabled
    Sequencing not set
    Preferred path Active : SR TE pref_sid_to_PE3, Statically configured, fallback
disabled
    Tunnel : Up
    Load Balance Hashing: src-dst-mac
```

関連コマンド

- adjacency-sid
- index
- prefix-sid
- router isis
- segment-routing

該当するセグメント ルーティング コマンドについては、『*Segment Routing Command Reference for Cisco NCS 5500 Series Routers and Cisco NCS 540 Series Routers*』を参照してください。

関連項目

- セグメント ルーティングの概要　（353 ページ）
- セグメント ルーティングの仕組み　（354 ページ）
- セグメント ルーティング グローバル ブロック　（355 ページ）

SR-TE ポリシーを介した L2VPN VPLS または VPWS 優先パス

SR-TE ポリシーを介した L2VPN VPLS または VPWS 優先パス機能では、L2VPN 仮想プライベート LAN サービス（VPLS）または仮想プライベート ワイヤ サービス（VPWS）の 2 つのエンドポイント間に SR-TE ポリシーを使用して優先パスを設定できます。

制約事項

- SR ポリシーが VPLS 回線の優先パスとして設定されている場合、トラフィックは SR ポリシー パスを通過します。

  PW カウンタは、送受信されたパケットに関する統計情報を使用して更新されます。

  SR ポリシーの設定が削除されても、トラフィックの送信が PE 間の通常の LSP パスに戻るため、トラフィック セッションは引き続き機能します。送信されたエンドツーエンドのトラフィックにはドロップはありません。

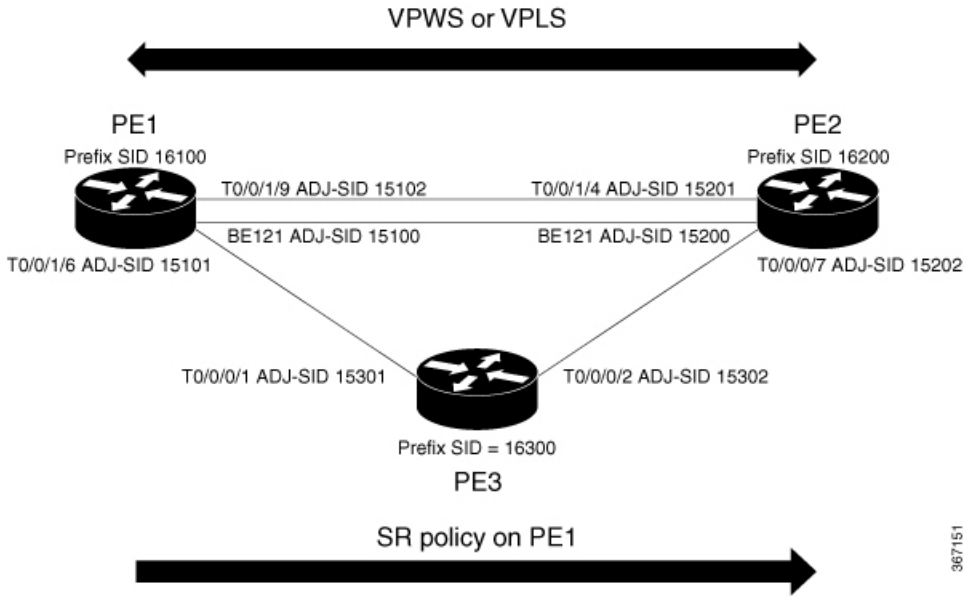
  ただし、パケット統計カウンタはリセットされ、ゼロから始まります。

  これは、SR ポリシーが削除されると PW も削除され、古い PW に関連付けられている統計情報がクリアされるためです。切り替え後に新しい PW が作成されると、再びカウンタがゼロから始まります。

SR-TE ポリシーを介した L2VPN VPLS または VPWS 優先パスの設定

SR-TE ポリシー機能を介して L2VPN VPLS または VPWS 優先パスを設定するには、次のステップを実行します。設定ステップを説明するため、次の図を参考として使用します。

図 *47 : SR-TE* ポリシーを介した *L2VPN VPWS* および *VPLS* 優先パス



- IGP でのプレフィックス SID の設定：次の例は、IS-IS でプレフィックス SID を設定する方法を示しています。
- IGP での隣接関係 SID の設定：次の例は、IS-IS で隣接関係 SID を設定する方法を示しています。
- セグメントリストの設定
- SR-TE ポリシーの設定
- SR-TE ポリシーを介した VPLS の設定

（注） デバイスには最大 128K の MAC アドレス エントリを含めることができます。デバイス上のブリッジドメインには最大64KのMACアドレス エントリを含めることができます。

- SR-TE ポリシーを介した VPWS の設定

IS-IS でのプレフィックス SID の設定

PE1、PE2、および PE3 にプレフィックス SID を設定します。

```
/* Configure Prefix-SID on PE1 */

Router# configure
Route(config)# router isis core
Route(config-isis)# is-type level-2-only
Route(config-isis)# net 49.0002.0330.2000.0031.00
```

```
Route(config-isis)# nsr
Route(config-isis)# nsf ietf
Route(config-isis)# log adjacency changes
Route(config-isis)# address-family ipv4 unicast
Route(config-isis-af)# metric-style wide level 2
Route(config-isis-af)# mpls traffic-eng level-2-only
Route(config-isis-af)# mpls traffic-eng router-id 1.1.1.1
Route(config-isis-af)# segment-routing mpls sr-prefer
Route(config-isis-af)# segment-routing prefix-sid-map advertise-local
Route(config-isis-af)# exit
!
Route(config-isis)# interface loopback 0
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# prefix-sid index 16100
Route(config-isis-af)# commit
Route(config-isis-af)# exit

/* Configure Prefix-SID on PE2 */

Router# configure
Route(config)# router isis core
Route(config-isis)# is-type level-2-only
Route(config-isis)# net 49.0002.0330.2000.0021.00
Route(config-isis)# nsr
Route(config-isis)# nsf ietf
Route(config-isis)# log adjacency changes
Route(config-isis)# address-family ipv4 unicast
Route(config-isis-af)# metric-style wide level 2
Route(config-isis-af)# mpls traffic-eng level-2-only
Route(config-isis-af)# mpls traffic-eng router-id loopback0
Route(config-isis-af)# segment-routing mpls sr-prefer
Route(config-isis-af)# segment-routing prefix-sid-map advertise-local
Route(config-isis-af)# exit
!
Route(config-isis)# interface loopback 0
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# prefix-sid index 16200
Route(config-isis-af)# commit
Route(config-isis-af)# exit

/* Configure Prefix-SID on PE3 */

Router# configure
Route(config)# router isis core
Route(config-isis)# is-type level-2-only
Route(config-isis)# net 49.0002.0330.2000.3030.0030.0035.00
Route(config-isis)# address-family ipv4 unicast
Route(config-isis-af)# metric-style wide level 2
Route(config-isis-af)# mpls traffic-eng level-2-only
Route(config-isis-af)# mpls traffic-eng router-id loopback0
Route(config-isis-af)# segment-routing mpls sr-prefer
Route(config-isis-af)# segment-routing prefix-sid-map advertise-local
Route(config-isis-af)# exit
!
Route(config-isis)# interface loopback 0
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# prefix-sid index 16300
Route(config-isis-af)# commit
Route(config-isis-af)# exit
```

IS-IS での隣接関係 SID の設定

PE1、PE2、および PE3 に隣接関係 SID を設定します。

```
/* Configure Adjacency-SID on PE1 */

Router# configure
Route(config)# router isis core
Route(config-isis)# interface Bundle-Ether121
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# adjacency-sid absolute 15100
Route(config-isis-if-af)# exit
!
Router# configure
Route(config)# router isis core
Route(config-isis)# interface TenGigE
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# adjacency-sid absolute 15101
Route(config-isis-if-af)# exit
!
Router# configure
Route(config)# router isis core
Route(config-isis)# interface TenGigE
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# adjacency-sid absolute 15102
Route(config-isis-if-af)# commit

/* Configure Adjacency-SID on PE2 */

Router# configure
Route(config)# router isis core
Route(config-isis)# interface Bundle-Ether121
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# adjacency-sid absolute 15200
Route(config-isis-if-af)# exit
!
Router# configure
Route(config)# router isis core
Route(config-isis)# interface TenGigE
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# adjacency-sid absolute 15201
Route(config-isis-if-af)# exit
!
Router# configure
Route(config)# router isis core
```

```
Route(config-isis)# interface TenGigE0/0/0/7
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# adjacency-sid absolute 15202
Route(config-isis-if-af)# commit

/* Configure Adjacency-SID on PE3 */

Router# configure
Route(config)# router isis core
Route(config-isis)# interface TenGigE0/0/0/1
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# adjacency-sid absolute 15301
Route(config-isis-if-af)# exit
!
Router# configure
Route(config)# router isis core
Route(config-isis)# interface TenGigE0/0/0/2
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# adjacency-sid absolute 15302
Route(config-isis-if-af)# commit
```

セグメントリストの設定

PE1、PE2、および PE3 にセグメントリストを設定します。

```
/* Configure segment-list on PE1 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# global-block 16000 23999
Router(config-sr)# local-block 15000 15999
Router(config-sr)# traffic-eng
Router(config-sr-te)# segment-list segment-list name PE1-PE2
Router(config-sr-te-sl)# index 1 mpls label 16200
Router(config-sr-te-sl)# exit
!
Router(config-sr-te)# segment-list segment-list name PE1-PE3
Router(config-sr-te-sl)# index 1 mpls label 16300
Router(config-sr-te-sl)# exit
!
Router(config-sr-te)# segment-list segment-list name PE1-PE2-PE3
Router(config-sr-te-sl)# index 1 mpls label 16200
Router(config-sr-te-sl)# index 2 mpls label 16300
Router(config-sr-te-sl)# exit
!
Router(config-sr-te)# segment-list segment-list name PE1-PE2_bad
Router(config-sr-te-sl)# index 1 mpls label 16900
Router(config-sr-te-sl)# exit
!
Router(config-sr-te)# segment-list segment-list name PE1-PE3-PE2
Router(config-sr-te-sl)# index 1 mpls label 16300
```

```
Router(config-sr-te-sl)# index 2 mpls label 16200
Router(config-sr-te-sl)# exit
!
Router(config-sr-te)# segment-list segment-list name PE1-PE2_BE121
Router(config-sr-te-sl)# index 1 mpls label 15100
Router(config-sr-te-sl)# exit
!
Router(config-sr-te)# segment-list segment-list name PE1-PE3-PE2_link
Router(config-sr-te-sl)# index 1 mpls label 15101
Router(config-sr-te-sl)# index 2 mpls label 15302
Router(config-sr-te-sl)# exit
!
Router(config-sr-te)# segment-list segment-list name PE1-PE3-PE2-t0016
Router(config-sr-te-sl)# index 1 mpls label 15101
Router(config-sr-te-sl)# index 2 mpls label 16200
Router(config-sr-te-sl)# commit

/* Configure segment-list on PE2 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# global-block 16000 23999
Router(config-sr)# local-block 15000 15999
Router(config-sr)# traffic-eng
Router(config-sr-te)# segment-list segment-list name PE2-PE1
Router(config-sr-te-sl)# index 1 mpls label 16100
Router(config-sr-te-sl)# exit
!
Router(config-sr-te)# segment-list segment-list name PE2-PE3-PE1
Router(config-sr-te-sl)# index 1 mpls label 16300
Router(config-sr-te-sl)# index 2 mpls label 16100
Router(config-sr-te-sl)# commit

/* Configure segment-list on PE3 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# global-block 16000 23999
Router(config-sr)# local-block 15000 15999
Router(config-sr)# traffic-eng
Router(config-sr-te)# segment-list segment-list name PE3-PE1
Router(config-sr-te-sl)# index 1 mpls label 16100
Router(config-sr-te-sl)# exit
!
Router(config-sr-te)# segment-list segment-list name PE3-PE2-PE1
Router(config-sr-te-sl)# index 1 mpls label 16200
Router(config-sr-te-sl)# index 2 mpls label 16100
Router(config-sr-te-sl)# commit
```

SR-TE ポリシーの設定

```
/* Configure SR-TE policy */

Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy 100
Router(config-sr-te-policy)# color 1 end-point ipv4 2.2.2.2
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy)# preference 400
```

```
Router(config-sr-te-pp-info)# explicit segment-list PE1-PE3-PE2
Router(config-sr-te-pp-info)# exit
!
Router(config-sr-te-policy)# preference 500 <-----------------largest number takes the
precedence
Router(config-sr-te-pp-info)# explicit segment-list PE1-PE2
Router(config-sr-te-pp-info)# commit
Router(config-sr-te-pp-info)# exit
!
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy 1013
Router(config-sr-te-policy)# color 1013 end-point ipv4 2.2.2.2
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy)# preference 100
Router(config-sr-te-pp-info)# explicit segment-list PE1-PE2_BE121
Router(config-sr-te-pp-info)# exit
!
Router(config-sr-te-policy)# preference 200
Router(config-sr-te-pp-info)# explicit segment-list PE1-PE3-PE2-t0016
Router(config-sr-te-pp-info)# exit
!
Router(config-sr-te-policy)# preference 500
Router(config-sr-te-pp-info)# explicit segment-list PE1-PE2
Router(config-sr-te-pp-info)# exit
!
Router(config-sr-te-policy)# preference 600
Router(config-sr-te-pp-info)# explicit segment-list PE1-PE3-PE2
Router(config-sr-te-pp-info)# exit
!
Router(config-sr-te-policy)# preference 700
Router(config-sr-te-pp-info)# explicit segment-list PE1-PE3-PE2_link
Router(config-sr-te-pp-info)# commit
!
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy 1300
Router(config-sr-te-policy)# color 1300 end-point ipv4 3.3.3.3
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy)# preference 100
Router(config-sr-te-pp-info)# explicit segment-list PE1-PE3
Router(config-sr-te-pp-info)# commit
!
```

SR-TE ポリシーを介した VPLS の設定

（注） 自動生成された SR-TE ポリシー名を使用して、L2VPN インスタンスにポリシーをアタッチします。ポリシー名は、ポリシーの色とエンドポイントに基づいて自動生成されます。自動生成されたポリシー名を表示するには、**show segment-routing traffic-eng policy candidate-path name** *policy_name* コマンドを使用します。

```
Router# show segment-routing traffic-eng policy candidate-path name 100

SR-TE policy database
```

```
---------------------
Color: 1, End-point: 2.2.2.2
 Name: srte_c_1_ep_2.2.2.2

Router# show segment-routing traffic-eng policy candidate-path name 1013

SR-TE policy database
---------------------
Color: 1013, End-point: 2.2.2.2
 Name: srte_c_1013_ep_2.2.2.2

Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# pw-class pw100
Router(config-l2vpn-pwc)# encapsulation mpls
Router(config-l2vpn-pwc-mpls)# preferred-path sr-te policy srte_c_1_ep_2.2.2.2
Router(config-l2vpn-pwc-mpls)# exit
!
Router(config-l2vpn)# pw-class pw1013
Router(config-l2vpn-pwc)# encapsulation mpls
Router(config-l2vpn-pwc-mpls)# preferred-path sr-te policy srte_c_1013_ep_2.2.2.2 fallback
 disable
Router(config-l2vpn-pwc-mpls)# exit

/* The default is Fallback Enable. If the SR-policy is down, then L2VPN VPWS/VPLS will
try to be UP using the regular IGP path, and not using the SR policy. If Fallback Disable
 is configured, the L2VPN PW will be down when the SR-policy is down. Preferred-path is
 the action of pinning down a PW to a SR TE policy */


Router(config)#l2vpn
Router(config-l2vpn)#bridge group bg1
Router(config-l2vpn-bg)#bridge-domain vpls501
Router(config-l2vpn-bg-bd)#interface Bundle-Ether41.501
Router(config-l2vpn-bg-bd-ac)#exit
!
Router(config-l2vpn-bg-bd)#interface TenGigE
Router(config-l2vpn-bg-bd-ac)#split-horizon group
Router(config-l2vpn-bg-bd-ac)#exit
!
Router(config-l2vpn-bg-bd)#vfi vpls1
Router(config-l2vpn-bg-bd-vfi)#neighbor 2.2.2.2 pw-id 501
Router(config-l2vpn-bg-bd-vfi-pw)#pw-class pw100
Router(config-l2vpn-bg-bd-vfi-pw)#exit
!
Router(config-l2vpn-bg-bd-vfi)#neighbor 3.3.3.3 pw-id 501
Router(config-l2vpn-bg-bd-vfi-pw)#commit
```

SR-TE ポリシーを介した VPWS の設定

（注） 自動生成された SR-TE ポリシー名を使用して、L2VPN インスタンスにポリシーをアタッチします。ポリシー名は、ポリシーの色とエンドポイントに基づいて自動生成されます。自動生成されたポリシー名を表示するには、**show segment-routing traffic-eng policy candidate-path name** *policy_name* コマンドを使用します。

```
Router# show segment-routing traffic-eng policy candidate-path name 1300
```

```
SR-TE policy database
---------------------
Color: 1300, End-point: 3.3.3.3
 Name: srte_c_1300_ep_3.3.3.3

Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# pw-class pw1300
Router(config-l2vpn-pwc)# encapsulation mpls
Router(config-l2vpn-pwc-mpls)# load-balancing
Router(config-l2vpn-pwc-mpls-load-bal)# flow-label both
Router(config-l2vpn-pwc-mpls-load-bal)# exit
!
Router(config-l2vpn-pwc-mpls)# preferred-path sr-te policy srte_c_1300_ep_3.3.3.3 fallback
 disable
Router(config-l2vpn-pwc-mpls)# exit
!
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group xcon1
Router(config-l2vpn-xc)# p2p vplw1002
Router(config-l2vpn-xc-p2p)# interface TenGigE
Router(config-l2vpn-xc-p2p)# neighbor 3.3.3.3 pw-id 1002
Router(config-l2vpn-xc-p2p-pw)# pw-class pw1300
Router(config-l2vpn-xc-p2p-pw)# commit
Router(config-l2vpn-xc-p2p-pw)# exit
```

実行コンフィギュレーション

```
/* Configure prefix-SID */
PE1:
router isis core
 is-type level-2-only
 net 49.0002.0330.2000.0031.00
 nsr
 nsf ietf
 log adjacency changes
 address-family ipv4 unicast
  metric-style wide level 2
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id 1.1.1.1
  segment-routing mpls sr-prefer
  segment-routing prefix-sid-map advertise-local

interface Loopback0
  address-family ipv4 unicast
   prefix-sid index 16100

PE2:
router isis core
 is-type level-2-only
 net 49.0002.0330.2000.0021.00
 nsr
 nsf ietf
 log adjacency changes
 address-family ipv4 unicast
  metric-style wide level 2
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
  segment-routing mpls sr-prefer
  segment-routing prefix-sid-map advertise-local
```

```
 interface Loopback0
  address-family ipv4 unicast
   prefix-sid index 16200

PE3:
router isis core
 is-type level-2-only
 net 49.0002.0330.2000.3030.0030.0035.00
 address-family ipv4 unicast
  metric-style wide level 2
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
  segment-routing mpls sr-prefer
  segment-routing prefix-sid-map advertise-local

interface Loopback0
  address-family ipv4 unicast
   prefix-sid index 16300

/* Configure Adjacency-SID */
PE1:
router isis core
!
 interface Bundle-Ether121
  circuit-type level-2-only
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
   adjacency-sid absolute 15100
  !
 interface TenGigE

  circuit-type level-2-only
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
   adjacency-sid absolute 15101
  !
 interface TenGigE
  circuit-type level-2-only
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
   adjacency-sid absolute 15102

PE2
router isis core
 !
interface Bundle-Ether121
  circuit-type level-2-only
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
   adjacency-sid absolute 15200

interface TenGigE0/0/0/0/4
  circuit-type level-2-only
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
   adjacency-sid absolute 15201

interface TenGigE0/0/0/0/7
  circuit-type level-2-only
```

```
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
   adjacency-sid absolute 15202

PE3:
router isis core
!
interface TenGigE0/0/0/1
  circuit-type level-2-only
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
   adjacency-sid absolute 15301
  !
 !
 interface TenGigE0/0/0/2
  circuit-type level-2-only
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
   adjacency-sid absolute 15302

/* Configure segment-list */
PE1:
segment-routing
 global-block 16000 23999
 local-block 15000 15999
  traffic-eng
 segment-list name PE1-PE2
   index 1 mpls label 16200
  !
  segment-list name PE1-PE3
   index 1 mpls label 16300
  !
  segment-list name PE1-PE2-PE3
   index 1 mpls label 16200
   index 2 mpls label 16300
  !
  segment-list name PE1-PE2_bad
   index 1 mpls label 16900
  !
  segment-list name PE1-PE3-PE2
   index 1 mpls label 16300
   index 2 mpls label 16200
  !
  segment-list name PE1-PE2_BE121
   index 1 mpls label 15100
!
  segment-list name PE1-PE3-PE2_link
   index 1 mpls label 15101
   index 2 mpls label 15302
  !

  segment-list name PE1-PE3-PE2-t0016
   index 1 mpls label 15101
   index 2 mpls label 16200

PE2:
segment-routing
 global-block 16000 23999
 local-block 15000 15999
 traffic-eng
  segment-list name PE2-PE1
```

```
   index 1 mpls label 16100
  !
  segment-list name PE2-PE3-PE1
   index 1 mpls label 16300
   index 2 mpls label 16100

PE3:
segment-routing
 global-block 16000 23999
 local-block 15000 15999
 traffic-eng
  segment-list name PE3-PE1
   index 1 mpls label 16100
  !
  segment-list name PE3-PE2-PE1
   index 1 mpls label 16200
   index 2 mpls label 16100

/* Configure SR-TE policy */

segment-routing
 traffic-eng
  policy 100
   color 1 end-point ipv4 2.2.2.2
   candidate-paths
    preference 400
     explicit segment-list PE1-PE3-PE2
     !
    preference 500
     explicit segment-list PE1-PE2

 policy 1013
   color 1013 end-point ipv4 2.2.2.2
   candidate-paths
    preference 100
     explicit segment-list PE1-PE2_BE121
     !
    preference 200
     explicit segment-list PE1-PE3-PE2-t0016
     !
    preference 500
     explicit segment-list PE1-PE2
      !
    preference 600
     explicit segment-list PE1-PE3-PE2
     !
    preference 700
     explicit segment-list PE1-PE3-PE2_link
     !
 policy 1300
   color 1300 end-point ipv4 3.3.3.3
   candidate-paths
    preference 100
     explicit segment-list PE1-PE3
     !

/* Configure VPLS over SR-TE policy
l2vpn
 pw-class pw100
  encapsulation mpls
   preferred-path sr-te policy srte_c_1_ep_2.2.2.2
 pw-class pw1013
  encapsulation mpls
   preferred-path sr-te policy srte_c_1013_ep_2.2.2.2 fallback disable
```

```
l2vpn
 bridge group bg1
  bridge-domain vpls501
   interface Bundle-Ether41.501
   !
   interface TenGigE

    split-horizon group
   !
   vfi vpls1
    neighbor 2.2.2.2 pw-id 501
     pw-class pw100
    !
    neighbor 3.3.3.3 pw-id 501

/*Configure VPWS over SR-TE policy
l2vpn
 pw-class pw1300
  encapsulation mpls
    load-balancing
    flow-label both
   preferred-path sr-te policy srte_c_1300_ep_3.3.3.3 fallback disable


Xconnect group xcon1
  p2p vplw1002
   interface TenGigE
   neighbor 3.3.3.3 pw-id 1002
    pw-class pw1300
```

SR-TE ポリシー設定を介した L2VPN VPLS または VPWS 優先パスの確認

```
/* The prefix-sid and Adjacency-sid must be in the SR topology */

PE1#show segment-routing traffic-eng ipv4 topology | inc Prefix
Thu Feb  1 20:28:43.343 EST
  Prefix SID:
    Prefix 1.1.1.1, label 16100 (regular)
  Prefix SID:
    Prefix 3.3.3.3, label 16300 (regular)
  Prefix SID:
    Prefix 2.2.2.2, label 16200 (regular)


PE1#show segment-routing traffic-eng ipv4 topology | inc Adj SID
Thu Feb  1 20:30:25.760 EST
    Adj SID: 61025 (unprotected) 15102 (unprotected)
    Adj SID: 61023 (unprotected) 15101 (unprotected)
    Adj SID: 65051 (unprotected) 15100 (unprotected)
    Adj SID: 41516 (unprotected) 15301 (unprotected)
    Adj SID: 41519 (unprotected) 15302 (unprotected)
    Adj SID: 46660 (unprotected) 15201 (unprotected)
    Adj SID: 24003 (unprotected) 15202 (unprotected)
    Adj SID: 46675 (unprotected) 15200 (unprotected)

PE1# show segment-routing traffic-eng policy candidate-path name 100

SR-TE policy database
---------------------

Color: 100, End-point: 2.2.2.2
```

```
 Name: srte_c_1_ep_2.2.2.2


PE1#show segment-routing traffic-eng policy name 100
Thu Feb  1 23:16:58.368 EST

SR-TE policy database
---------------------

Name: 100 (Color: 1, End-point: 2.2.2.2)
  Status:
    Admin: up  Operational: up for 05:44:25 (since Feb  1 17:32:34.434)
  Candidate-paths:
    Preference 500:
      Explicit: segment-list PE1-PE2 (active)
        Weight: 0, Metric Type: IGP
          16200 [Prefix-SID, 2.2.2.2]
    Preference 400:
      Explicit: segment-list PE1-PE3-PE2 (inactive)
      Inactive Reason: unresolved first label
        Weight: 0, Metric Type: IGP
  Attributes:
    Binding SID: 27498
      Allocation mode: dynamic
      State: Programmed
      Policy selected: yes
    Forward Class: 0

PE1#show segment-routing traffic-eng policy name 1013
Thu Feb  1 21:20:57.439 EST

SR-TE policy database
---------------------
Name: 1013 (Color: 1013, End-point: 2.2.2.2)
  Status:
    Admin: up  Operational: up for 00:06:36 (since Feb  1 21:14:22.057)
  Candidate-paths:
    Preference 700:
      Explicit: segment-list PE1-PE3-PE2_link (active)
        Weight: 0, Metric Type: IGP
          15101 [Adjacency-SID, 13.1.1.1 - 13.1.1.2]
          15302
    Preference 600:
      Explicit: segment-list PE1-PE3-PE2 (inactive)
      Inactive Reason:
        Weight: 0, Metric Type: IGP
    Preference 500:
      Explicit: segment-list PE1-PE2 (inactive)
      Inactive Reason:
        Weight: 0, Metric Type: IGP
    Preference 200:
      Explicit: segment-list PE1-PE3-PE2-t0016 (inactive)
      Inactive Reason: unresolved first label
        Weight: 0, Metric Type: IGP
    Preference 100:
      Explicit: segment-list PE1-PE2_BE121 (inactive)
      Inactive Reason: unresolved first label
        Weight: 0, Metric Type: IGP
  Attributes:
    Binding SID: 27525
      Allocation mode: dynamic
      State: Programmed
      Policy selected: yes
```

```
    Forward Class: 0

PE1#show segment-routing traffic-eng forwarding policy name 100
Thu Feb  1 23:19:28.951 EST
Policy        Segment         Outgoing    Outgoing            Next Hop        Bytes

Name          List            Label       Interface                           Switched

------------- --------------- ----------- ------------------- --------------- ------------
100           PE1-PE2         Pop         Te           12.1.9.2        0
                                         Pop         BE121               121.1.0.2
  0

PE1#show segment-routing traffic-eng forwarding policy name 1013 detail
Thu Feb  1 21:22:46.069 EST
Policy        Segment         Outgoing    Outgoing            Next Hop        Bytes

Name          List            Label       Interface                           Switched

------------- --------------- ----------- ------------------- --------------- ------------
1013          PE1-PE3-PE2_link
                              15302       Te           13.1.1.2        0
                 Label Stack (Top -> Bottom): { 15302 }
                 Path-id: 1, Weight: 0
                 Packets Switched: 0
   Local label: 24005
   Packets/Bytes Switched: 0/0
   (!): FRR pure backup

PE1#show mpls forwarding tunnels sr-policy name 1013
Thu Feb  1 21:23:22.743 EST
Tunnel        Outgoing    Outgoing     Next Hop        Bytes
Name          Label       Interface                    Switched
------------- ----------- ------------ --------------- ------------
1013         (SR) 15302       Te    13.1.1.2        0

PE1#show l2vpn bridge-domain bd-name vpls501 detail
Sat Feb  3 11:27:35.655 EST
Legend: pp = Partially Programmed.
Bridge group: bg1, bridge-domain: vpls501, id: 250, state: up, ShgId: 0, MSTi: 0
…….
List of VFIs:
    VFI vpls1 (up)
      PW: neighbor 2.2.2.2, PW ID 501, state is up ( established )
        PW class pw100, XC ID 0xa00020d5
        Encapsulation MPLS, protocol LDP
        Source address 1.1.1.1
        PW type Ethernet, control word disabled, interworking none
        Sequencing not set
        Preferred path Active : SR TE 100, Statically configured, fallback disabled
        Tunnel : Up
        PW Status TLV in use
          MPLS         Local                          Remote
          ------------ ------------------------------ --------------------------
          Label        41042                          24010
          Group ID     0xfa                           0x1
          Interface    vpls1                          vpls1
          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: 2684362965
Create time: 02/02/2018 16:20:59 (19:06:37 ago)
```

関連コマンド

- adjacency-sid
- index
- prefix-sid
- router isis
- segment-routing

該当するセグメント ルーティング コマンドについては、『*Segment Routing Command Reference for Cisco NCS 5500, NCS 540 Series Routers, and NCS 560 Series Routers*』を参照してください。

関連項目

- セグメント ルーティングの概要 （353 ページ）
- セグメント ルーティングの仕組み （354 ページ）
- セグメント ルーティング グローバル ブロック （355 ページ）

SR-TE を使用した EVPN VPWS オンデマンド ネクスト ホップ

SR-TE を使用した EVPN VPWS オンデマンド ネクスト ホップ機能では、送信元からポイントツーポイント サービスの宛先にトラフィックを送信する最適なパスを IOS XR トラフィック コントローラ（XTC）を使用して取得できます。SR-TE を使用したオンデマンド ネクスト ホップ（ODN）は EVPN 仮想プライベート ワイヤ サービス（VPWS）とフレキシブル クロス接続（FXC）VLAN 非対応サービスでサポートされています。

ドメイン全体にルーティング情報を再配布すると、マルチドメイン サービス（レイヤ 2 VPN とレイヤ 3 VPN）のプロビジョニングに複雑性と拡張性の問題が発生します。SR-TE を使用した ODN 機能は、エンドツーエンドのラベル スイッチド パス（LSP）の計算をパス計算要素（PCE）に委任します。この PCE には、再配布なしの制約事項とポリシーが含まれています。次に、サービスが Forwarding Information Base（FIB）へ移行する間に再適用されたマルチドメイン LSP をインストールします。

ODN は BGP ダイナミック SR-TE 機能を使用して、パスを PCE に追加します。PCE には、要件に基づいてエンドツーエンド パスを検出し、ダウンロードする機能があります。ODN は定

義された BGP ポリシーに基づいて SR-TE 自動トンネルをトリガーします。PCE は BGP または IGP、あるいはその両方を通じてリアルタイム トポロジを学習します。

IOS XR トラフィック コント ローラー（XTC）

パス計算要素（PCE）は、一連のプロシージャを記述します。これにより、パス計算クライアント（PCC）は PCC から発信されたヘッドエンド トンネルの制御を PCE ピアに報告し、委任します。PCE ピアは、PCC が制御している LSP のパラメータの更新と変更を PCC に要求します。また、PCC を有効にして PCE が計算を開始するとともに、ネットワーク全体の調整を行えるようにします。

制約事項

- 自動プロビジョニングされた TE ポリシーの最大数は 1,000 です。
- EVPN VPWS SR ポリシーは EVPN VPWS デュアル ホーミングではサポートされていません。

  EVPN はルートがシングル ホーム ネクスト ホップ用であるかどうかを検証します。そうでない場合は、不適切な SR-TE ポリシーに関するエラー メッセージを発行し、そのポリシーなしで EVPN-VPWS のセットアップを続行します。EVPN は、これがシングル ホームかどうかの決定をゼロに設定されている ESI 値に依存します。AC が LACP を実行しているバンドルイーサ インターフェイスの場合は、ESI 値を手動でゼロに設定して、自動感知 ESI を上書きする必要があります。これは、EVPN VPWS マルチホーミングがサポートされていないためです。

  EVPN デュアル ホーミングを無効にするには、バンドルイーサ AC を ESI 値セットをゼロに設定します。

```
evpn
interface Bundle-Ether12
ethernet-segment
identifier type 0 00.00.00.00.00.00.00.00.00
/* Or globally */
evpn
ethernet-segment type 1 auto-generation-disable
```

SR-TE を使用した EVPN VPWS オンデマンド ネクスト ホップの設定

SR-TE を使用して EVPN VPWS オン デマンド ネクスト ホップを設定するには、次のステップを実行します。設定ステップを説明するため、次の図を参考として使用します。

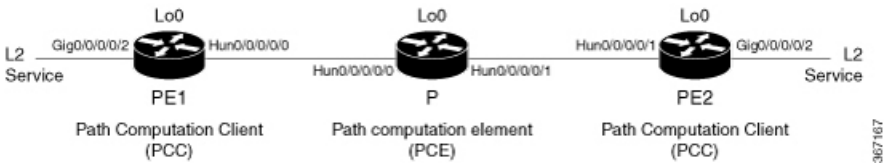
- ISIS でのプレフィックス SID の設定
- SR-TE の設定
- PCE と PCC の設定
- SR カラーの設定
- EVPN ルート ポリシーの設定

- BGP の設定
- EVPN VPWS の設定
- フレキシブル クロスコネクト サービス（FXC）VLAN 非対応の設定

トポロジ

PE1 と PE2 上に EVPN VPWS が設定されているトポロジを考えてみます。トラフィックはコア内の SR-TE を使用して PE1 から PE2 に送信されます。P ルータ上に設定されている PCE が PE1 から PE2 への最適なパスを計算します。パス計算クライアント（PCC）は PE1 と PE2 上に設定されています。

図 *48 : SR-TE* を使用した *EVPN VPWS* オンデマンド ネクスト ホップ



設定例

ISIS でのプレフィックス SID の設定

各ルータがプレフィックスに関連付けられている一意のセグメント識別子を使用するように、ISIS にプレフィックス SID を、コア内にトポロジ独立型ループフリー代替パス（TI-LFA）を設定します。

```
/* Configure Prefix-SID in ISIS and TI-LFA  on PE1 */

Router# configure
Route(config)# router isis ring
Route(config-isis)# is-type level-2-only
Route(config-isis)# net 49.0001.1921.6800.1001.00
Route(config-isis)# segment-routing global-block 30100 39100
Route(config-isis)# nsr
Route(config-isis)# distribute link-state
Route(config-isis)# nsf cisco
Route(config-isis)# address-family ipv4 unicast
Route(config-isis-af)# metric-style wide
Route(config-isis-af)# mpls traffic-eng level-1
Route(config-isis-af)# mpls traffic-eng router-id loopback0
Route(config-isis-af)# segment-routing mpls
Route(config-isis-af)# exit
!
Route(config-isis)# interface loopback0
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# prefix-sid index 30101
Route(config-isis-af)# exit
!
Route(config-isis)# interface HundredGigE0/0/0/0
Route(config-isis-if)# circuit-type level-1
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
```

```
Route(config-isis-if)# fast-reroute per-prefix
Route(config-isis-if-af)# fast-reroute per-prefix ti-lfa
Route(config-isis-if-af)# commit

/*Configure Prefix-SID in ISIS and TI-LFA  on P router */

Router# configure
Route(config)# router isis ring
Route(config-isis)# net 49.0001.1921.6800.1002.00
Route(config-isis)# segment-routing global-block 30100 39100
Route(config-isis)# nsr
Route(config-isis)# distribute link-state
Route(config-isis)# nsf cisco
Route(config-isis)# address-family ipv4 unicast
Route(config-isis-af)# metric-style wide
Route(config-isis-af)# mpls traffic-eng level-1
Route(config-isis-af)# mpls traffic-eng router-id loopback0
Route(config-isis-af)# segment-routing mpls
Route(config-isis-af)# exit
!
Route(config-isis)# interface loopback0
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# prefix-sid index 30102
Route(config-isis-af)# exit
!
Route(config-isis)# interface HundredGigE0/0/0/0
Route(config-isis-if)# circuit-type level-1
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# fast-reroute per-prefix
Route(config-isis-if-af)# fast-reroute per-prefix ti-lfa
Route(config-isis-if-af)# exit
!
Route(config-isis)# interface HundredGigE0/0/0/1
Route(config-isis-if)# circuit-type level-1
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# fast-reroute per-prefix
Route(config-isis-if-af)# fast-reroute per-prefix ti-lfa
Route(config-isis-if-af)# commit

/* Configure Prefix-SID in ISIS and TI-LFA  on PE2 */

Router# configure
Route(config)# router isis ring
Route(config-isis)# net 49.0001.1921.6800.1003.00
Route(config-isis)# segment-routing global-block 30100 39100
Route(config-isis)# nsr
Route(config-isis)# distribute link-state
Route(config-isis)# nsf cisco
Route(config-isis)# address-family ipv4 unicast
Route(config-isis-af)# metric-style wide
Route(config-isis-af)# mpls traffic-eng level-1
Route(config-isis-af)# mpls traffic-eng router-id loopback0
Route(config-isis-af)# segment-routing mpls
Route(config-isis-af)# exit
!
Route(config-isis)# interface loopback0
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# prefix-sid index 30103
Route(config-isis-af)# exit
!
Route(config-isis)# interface HundredGigE0/0/0/1
```

```
Route(config-isis-if)# circuit-type level-1
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# fast-reroute per-prefix
Route(config-isis-if-af)# fast-reroute per-prefix ti-lfa
Route(config-isis-if-af)# commit
```

SR-TE の設定

P ルータと PE ルータに SR-TE を設定します。

```
/Configure SR-TE on PE1 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# on-demand color 1
Router(config-sr-te-color)# dynamic mpls
Router(config-sr-te-color-dyn-mpls)# pce
Router(config-sr-te-color-dyn-mpls-pce)# exit
!
Router(config-sr-te)# on-demand color 2
Router(config-sr-te-color)# dynamic mpls
Router(config-sr-te-color-dyn-mpls)# pce
Router(config-sr-te-color-dyn-mpls-pce)# exit
!
Router(config-sr-te)# on-demand color 3
Router(config-sr-te-color)# dynamic mpls
Router(config-sr-te-color-dyn-mpls)# pce
Router(config-sr-te-color-dyn-mpls-pce)# commit

/*Configure SR-TE on P router */
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# commit


/Configure SR-TE on PE2 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# on-demand color 11
Router(config-sr-te-color)# dynamic mpls
Router(config-sr-te-color-dyn-mpls)# pce
Router(config-sr-te-color-dyn-mpls-pce)# exit
!
Router(config-sr-te)# on-demand color 12
Router(config-sr-te-color)# dynamic mpls
Router(config-sr-te-color-dyn-mpls)# pce
Router(config-sr-te-color-dyn-mpls-pce)# exit
!
Router(config-sr-te)# on-demand color 13
Router(config-sr-te-color)# dynamic mpls
Router(config-sr-te-color-dyn-mpls)# pce
Router(config-sr-te-color-dyn-mpls-pce)# commit
```

PCE と PCC の設定

P ルータに PCE を、PE1 と PE2 に PCC を設定します。必要に応じて、複数の PCE を設定することもできます。

```
/* Configure PCC on PE1 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# pcc
Router(config-sr-te-pcc)# source-address ipv4 205.1.0.1
Router(config-sr-te-pcc)# pce address ipv4 205.2.0.2
Router(config-sr-te-pcc)# commit

/* Configure PCE on P router */

Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# exit
Router(config)# pce
Router(config-pce)# address ipv4 205.2.0.2
Router(config-pce)# commit

/* Configure PCC on PE2 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# pcc
Router(config-sr-te-pcc)# source-address ipv4 205.3.0.3
Router(config-sr-te-pcc)# pce address ipv4 205.2.0.2
Router(config-sr-te-pcc)# commit
```

SR カラーの設定

PE ルータに SR カラーを設定します。

```
/* Define SR color on PE1 */

Router# configure
Router(config)# extcommunity-set opaque color1
Router(config-ext)# 1
Router(config-ext)# end-set
!
Router(config)# extcommunity-set opaque color2
Router(config-ext)# 2
Router(config-ext)# end-set
!
Router(config)# extcommunity-set opaque color3
Router(config-ext)# 3
Router(config-ext)# end-set
!
/* Define SR color on PE2 */

Router# configure
Router(config)# extcommunity-set opaque color11
```

```
Router(config-ext)# 11
Router(config-ext)# end-set
!
Router(config)# extcommunity-set opaque color12
Router(config-ext)# 12
Router(config-ext)# end-set
!
Router(config)# extcommunity-set opaque color13
Router(config-ext)# 13
Router(config-ext)# end-set
!
```

EVPN ルート ポリシーの設定

PE1 と PE2 に EVPN ルート ポリシーを設定します。次に、ルート ポリシー言語を定義し、EVPN ルートを追跡する例を示します。「rd」は PE のアドレスを参照し、L2 サービスのイーサネット仮想インターコネクトとして機能します。

```
/* Configure EVPN route policy on PE1 */

Router# configure
Router(config)# route-policy evpn_odn_policy
Router(config-rpl)# if rd in (205.3.0.3:2) then
Router(config-rpl-if)# set extcommunity color color1
Router(config-rpl-if)# set next-hop 205.3.0.3
Router(config-rpl-if)# elseif rd in (205.3.0.3:3) then
Router(config-rpl-elseif)# set extcommunity color color2
Router(config-rpl-elseif)# set next-hop 205.3.0.3
Router(config-rpl-elseif)# elseif rd in (205.3.0.3:4) then
Router(config-rpl-elseif)# set extcommunity color color3
Router(config-rpl-elseif)# set next-hop 205.3.0.3
Router(config-rpl-elseif)# endif
Router(config-rpl)# pass
Router(config-rpl)# end-policy


/* Configure EVPN route policy on PE2 */

Router# configure
Router(config)# route-policy evpn_odn_policy
Router(config-rpl)# if rd in (205.1.0.1:2) then
Router(config-rpl-if)# set extcommunity color color11
Router(config-rpl-if)# set next-hop 205.1.0.1
Router(config-rpl-if)# elseif rd in (205.1.0.1:3) then
Router(config-rpl-elseif)# set extcommunity color color12
Router(config-rpl-elseif)# set next-hop 205.1.0.1
Router(config-rpl-elseif)# elseif rd in (205.1.0.1:4) then
Router(config-rpl-elseif)# set extcommunity color color13
Router(config-rpl-elseif)# set next-hop 205.1.0.1
Router(config-rpl-elseif)# endif
Router(config-rpl)# pass
Router(config-rpl)# end-policy
```

BGP の設定

PE1 と PE2 に BGP を設定します。

```
/* Configure BGP on PE1 */
```

```
Router# configure
Router(config)# router bgp 100
Routerconfig-bgp)# bgp router-id 205.1.0.1
Routerconfig-bgp)# bgp graceful-restart
Router(config-bgp)# address-family l2vpn evpn
Router(config-bgp-af)# exit
!
Router(config-bgp)# neighbor 205.3.0.3
Router(config-bgp-nbr)# remote-as 100
Router(config-bgp-nbr)# update-source loopback 0
Router(config-bgp-nbr)# address-family l2vpn evpn
Router(config-bgp-nbr-af)# route-policy evpn_odn_policy in
Router(config-rpl)# commit

/* Configure BGP on PE2 */

Router# configure
Router(config)# router bgp 100
Routerconfig-bgp)# bgp router-id 205.3.0.3
Routerconfig-bgp)# bgp graceful-restart
Router(config-bgp)# address-family l2vpn evpn
Router(config-bgp-af)# exit
!
Router(config-bgp)# neighbor 205.1.0.1
Router(config-bgp-nbr)# remote-as 100
Router(config-bgp-nbr)# update-source loopback 0
Router(config-bgp-nbr)# address-family l2vpn evpn
Router(config-bgp-nbr-af)# route-policy evpn_odn_policy in
Router(config-rpl)# commit
```

EVPN VPWS の設定

PE1 と PE2 に EVPN VPWS を設定します。

```
/* Configure EVPN VPWS on PE1 */

Router# configure
Router(config)# interface GigE0/0/0/2.2 l2transport
Router(config-subif)# encapsulation dot1q 1
Router# exit
!
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group evpn_vpws
Router(config-l2vpn-xc)# p2p e1_10
Router(config-l2vpn-xc-p2p)# interface GigE0/0/0/2.2
Router(config-l2vpn-xc-p2p)# neighbor evpn evi 2 target 10 source 10
Router(config-l2vpn-xc-p2p)#commit

/* Configure EVPN VPWS on PE2 */

Router# configure
Router(config)# interface GigE0/0/0/2.4 l2transport
Router(config-subif)# encapsulation dot1q 1
Router# exit
!
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group evpn_vpws
Router(config-l2vpn-xc)# p2p e3_30
Router(config-l2vpn-xc-p2p)# interface GigE0/0/0/2.4
```

```
Router(config-l2vpn-xc-p2p)# neighbor evpn evi 2 target 10 source 10
Router(config-l2vpn-xc-p2p)#commit
```

フレキシブル クロスコネクト サービス（FXC）VLAN 非対応の設定

```
/* Configure FXC on PE1 */

Router# configure
Router(config)# interface GigE0/0/0/2.3 l2transport
Router(config-subif)# encapsulation dot1q 3
Router# exit
!
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-unaware evpn_vu
Router(config-l2vpn-fxs-vu)# interface GigE0/0/0/2.3
Router(config-l2vpn-fxs-vu)# neighbor evpn evi 3 target 20
Router(config-l2vpn-fxs-vu)#commit

/* Configure FXC on PE2 */

Router# configure
Router(config)# interface GigE0/0/0/2.3 l2transport
Router(config-subif)# encapsulation dot1q 3
Router# exit
!
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-unaware evpn_vu
Router(config-l2vpn-fxs-vu)# interface GigE0/0/0/2.3
Router(config-l2vpn-fxs-vu)# neighbor evpn evi 3 target 20
Router(config-l2vpn-fxs-vu)#commit
```

実行コンフィギュレーション

```
/* Configure Prefix-SID in ISIS and TI-LFA */

PE1:

configure
 router isis ring
  net 49.0001.1921.6800.1001.00
  segment-routing global-block 30100 39100
  nsr
  distribute link-state
  nsf cisco
  address-family ipv4 unicast
   metric-style wide
   mpls traffic-eng level-1
   mpls traffic-eng router-id Loopback0
   segment-routing mpls
 !
 interface Loopback0
  address-family ipv4 unicast
   prefix-sid index 30101
  !
 !
 interface HundredGigE0/0/0/0
  circuit-type level-1
  point-to-point
  hello-padding disable
```

```
  address-family ipv4 unicast
   fast-reroute per-prefix
   fast-reroute per-prefix ti-lfa
  !
 !
```

P:

```
configure
 router isis ring
  net 49.0001.1921.6800.1002.00
  segment-routing global-block 30100 39100
  nsr
  distribute link-state
  nsf cisco
  address-family ipv4 unicast
   metric-style wide
   mpls traffic-eng level-1
   mpls traffic-eng router-id Loopback0
   segment-routing mpls
 !
 interface Loopback0
  address-family ipv4 unicast
   prefix-sid index 30102
  !
 !
 interface HundredGigE0/0/0/0
  circuit-type level-1
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
   fast-reroute per-prefix
   fast-reroute per-prefix ti-lfa
  !
 !
 interface HundredGigE0/0/0/1
  circuit-type level-1
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
   fast-reroute per-prefix
   fast-reroute per-prefix ti-lfa
  !
```

PE2:

```
configure
 router isis ring
  net 49.0001.1921.6800.1003.00
  segment-routing global-block 30100 39100
  nsr
  distribute link-state
  nsf cisco
  address-family ipv4 unicast
   metric-style wide
   mpls traffic-eng level-1
   mpls traffic-eng router-id Loopback0
   segment-routing mpls
 !
 interface Loopback0
  address-family ipv4 unicast
   prefix-sid index 30103
  !
 !
```

```
 interface HundredGigE0/0/0/1
  circuit-type level-1
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
   fast-reroute per-prefix
   fast-reroute per-prefix ti-lfa
  !
 !


/* Configure SR-TE */

PE1:

configure
 segment-routing
  traffic-eng
   on-demand color 1
    dynamic mpls
     pce
    !
   !
   on-demand color 2
    dynamic mpls
     pce
     !
    !
   !
   on-demand color 3
    dynamic mpls
     pce
     !
P:

configure
 segment-routing
  traffic-eng
!

PE2:

configure
 segment-routing
  traffic-eng
   on-demand color 11
    dynamic mpls
     pce
    !
   !
   on-demand color 12
    dynamic mpls
     pce
     !
    !
   !
   on-demand color 13
    dynamic mpls
     pce
     !

/* Configure PCE and PCC */

PE1:
```

```
configure
 segment-routing
  traffic-eng
   pcc
    source-address ipv4 205.1.0.1
    pce address ipv4 205.2.0.2
    !
P:

configure
 segment-routing
  traffic-eng
 pce
  address ipv4 205.2.0.2
    !

PE2:

configure
 segment-routing
  traffic-eng
   pcc
    source-address ipv4 205.3.0.3
    pce address ipv4 205.2.0.2
    !

/* Configure SR Color */

PE1:

configure
 extcommunity-set opaque color1
  1
end-set
!
 extcommunity-set opaque color2
  2
end-set
!
 extcommunity-set opaque color3
  3
end-set
!

PE2:

configure
 extcommunity-set opaque color11
  11
end-set
!
 extcommunity-set opaque color12
  12
end-set
!
 extcommunity-set opaque color13
  13
end-set
!

/* Configure EVPN route policy */

PE1:
```

```
configure
 route-policy evpn_odn_policy
  if rd in (205.3.0.3:2) then
    set extcommunity color color1
    set next-hop 205.3.0.3
  elseif rd in (205.3.0.3:3) then
    set extcommunity color color2
    set next-hop 205.3.0.3
  elseif rd in (205.3.0.3:4) then
    set extcommunity color color3
    set next-hop 205.3.0.3
  endif
 pass
end-policy
```

PE2:

```
configure
 route-policy evpn_odn_policy
  if rd in (205.1.0.1:2) then
    set extcommunity color color11
    set next-hop 205.1.0.1
  elseif rd in (205.1.0.1:3) then
    set extcommunity color color12
    set next-hop 205.1.0.1
  elseif rd in (205.1.0.1:4) then
    set extcommunity color color13
    set next-hop 205.1.0.1
  endif
 pass
end-policy

/* Configure BGP */
```

PE1:

```
configure
 router bgp 100
  bgp router-id 205.1.0.1
  bgp graceful-restart
  address-family l2vpn evpn
 !
 neighbor 205.3.0.3
  remote-as 100
  update-source Loopback0
  address-family l2vpn evpn
   route-policy evpn_odn_policy in
  !
```

PE2:

```
configure
 router bgp 100
  bgp router-id 205.3.0.3
  bgp graceful-restart
  address-family l2vpn evpn
 !
 neighbor 205.1.0.1
  remote-as 100
  update-source Loopback0
  address-family l2vpn evpn
   route-policy evpn_odn_policy in
  !
```

```
/* Configure EVPN VPWS */

PE1:

configure
 interface GigE0/0/0/2.2 l2transport
  encapsulation dot1q 1
!
l2vpn
 xconnect group evpn_vpws
  p2p e1_10
   interface GigE0/0/0/2.2
   neighbor evpn evi 2 target 10 source 10
  !
 !

PE2:

configure
 interface GigE0/0/0/2.4 l2transport
  encapsulation dot1q 1
!
l2vpn
 xconnect group evpn_vpws
  p2p e3_30
   interface GigE0/0/0/2.4
   neighbor evpn evi 2 target 10 source 10
  !
 !
!

/* Configure Flexible Cross-connect Service (FXC) */

PE1:

configure
 interface GigE0/0/0/2.3 l2transport
  encapsulation dot1q 3
!
l2vpn
 flexible-xconnect-service vlan-unaware evpn_vu
  interface GigE0/0/0/2.3
  neighbor evpn evi 3 target 20
 !
!

PE2:

configure
 interface GigE0/0/0/2.3 l2transport
  encapsulation dot1q 3
!
l2vpn
 flexible-xconnect-service vlan-unaware evpn_vu
  interface GigE0/0/0/2.3
  neighbor evpn evi 3 target 20
 !
!
```

SR-TE 設定を使用した EVPN VPWS オン デマンド ネクスト ホップの確認

EVPN ODN 上に設定されている各 L2 サービスに SR-TE ポリシーが自動プロビジョニングされているかを確認します。

```
PE1# show segment-routing traffic-eng policy

SR-TE policy database
---------------------

Name: bgp_AP_1 (Color: 1, End-point: 205.3.0.3)
    Status:
      Admin: up  Operational: up for 07:16:59 (since Oct  3 16:47:04.541)
    Candidate-paths:
      Preference 100:
        Dynamic (pce 205.2.0.2) (active)
          Weight: 0
            30103 [Prefix-SID, 205.3.0.3]
    Attributes:
      Binding SID: 68007
        Allocation mode: dynamic
        State: Programmed
        Policy selected: yes
      Forward Class: 0
      Distinguisher: 0
    Auto-policy info:
      Creator: BGP
      IPv6 caps enable: no
PE1#show l2vpn xconnect group evpn_vpws xc-name evpn_vpws_1001 detail
Group evpn_vpws, XC evpn_vpws_1001, state is up; Interworking none
  AC: Bundle-Ether12.1001, state is up
    Type VLAN; Num Ranges: 1
    Outer Tag: 1000
    Rewrite Tags: []
    VLAN ranges: [1, 1]
    MTU 1500; XC ID 0xc0000018; interworking none
    Statistics:
      packets: received 642304, sent 642244
      bytes: received 61661184, sent 61655424
      drops: illegal VLAN 0, illegal length 0
  EVPN: neighbor 20.20.20.20, PW ID: evi 1001, ac-id 10001, state is up ( established )
    XC ID 0xa0000007
    Encapsulation MPLS
    Source address 10.10.10.10
    Encap type Ethernet, control word enabled
    Sequencing not set
    Preferred path Active : SR TE pref_sid_to_PE3, On-Demand, fallback enabled
    Tunnel : Up
    Load Balance Hashing: src-dst-mac

PE1#show bgp l2vpn evpn route-type 1

BGP router identifier 205.1.0.1, local AS number 100
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0 RD version: 0
BGP main routing table version 36
BGP NSR Initial initsync version 25 (Reached)
BGP NSR/ISSU Sync-Group versions 36/0
BGP scan interval 60 secs
```

```
Status codes: s suppressed, d damped, h history, * valid, > best
i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 205.1.0.1:2 (default for vrf VPWS:2)
*>i[1][0000.0000.0000.0000.0000][1]/120
205.3.0.3 T:bgp_AP_1
100 0 i

PE1# show evpn evi ead detail

EVI Ethernet Segment Id EtherTag Nexthop Label SRTE IFH
----- ---------------------- -------- ------------------------------------ --------
 ----------
2 0000.0000.0000.0000.0000 1 205.3.0.3 24000 0x5a0
Source: Remote, MPLS
```

関連コマンド

- adjacency-sid
- index
- prefix-sid
- router isis
- segment-routing

該当するセグメント ルーティング コマンドについては、『*Segment Routing Command Reference for Cisco NCS 5500 Series Routers, Cisco NCS 540 Series Routers, and Cisco NCS 560 Series Routers*』を参照してください。

関連項目

- セグメント ルーティングの概要 （353 ページ）
- セグメント ルーティングの仕組み （354 ページ）
- セグメント ルーティング グローバル ブロック （355 ページ）

セグメント ルーティングの概要

セグメント ルーティング（SR）は、送信元ルーティングを実行するための柔軟でスケーラブルな方法です。送信元がパスを選択し、セグメントの番号付きリストとしてパケットヘッダー内で暗号化します。セグメントは、すべてのタイプの命令の識別子です。各セグメントを識別するセグメント ID（SID）は、フラットな 32 ビットの符号なし整数で構成されます。次のようなセグメント命令があります。

- 最短パスを使用してノード N へ移動する
- ノード M への最短パスを介してノード N に移動した後にレイヤ 1、レイヤ 2、レイヤ 3 のリンクをたどる

- サービス S を適用する

セグメントルーティングを使用すると、ネットワークでアプリケーションごとやフロー状態ごとに管理する必要がなくなります。代わりに、パケット内に指定されている転送命令に従います。

セグメント ルーティングは、シスコの Intermediate System-to-Intermediate System（IS-IS）および Open Shortest Path First（OSPF）プロトコルのいくつかの拡張機能に依存しています。MPLS（マルチプロトコル ラベル スイッチング）または IPv6 データ プレーンで動作でき、レイヤ 3 VPN（L3VPN）、仮想プライベート ワイヤ サービス（VPWS）、仮想プライベート LAN サービス（VPLS）、イーサネット VPN（EVPN）などの、さまざまなマルチサービス機能と統合されます。

セグメント ルーティングは、転送プレーンを変更することなく、マルチプロトコル ラベル スイッチング（MPLS）アーキテクチャに直接適用できます。セグメントルーティングは従来の MPLS ネットワークよりも効率的にネットワーク帯域幅を利用し、遅延を低減します。セグメントは MPLS ラベルとしてエンコードされます。セグメントの番号付きリストはラベルのスタックとしてエンコードされます。処理するセグメントは、スタックの一番上にあります。セグメントの完了後に関連するラベルがスタックからポップします。

セグメントルーティングは自動トラフィック保護を提供しますが、トポロジ上の制約事項はありません。ネットワークがリンク障害やノード障害からトラフィックを保護し、ネットワーク内での追加シグナリングは必要ありません。既存の IP 高速再ルート（FRR）技術と、セグメント ルーティングの明示的なルーティング機能を組み合わせると、最適なバックアップ パスを備えた完全な保護適用範囲が保証されます。トラフィック保護には、他のシグナリング要件は適用されません。

セグメント ルーティングの仕組み

セグメント ルーティング ネットワーク内のルータは、明示的な最短パスか、または内部ゲートウェイ プロトコル（IGP）の最短パスかどうかにかかわらず、トラフィックを転送するパスを選択できます。セグメントは、ネットワークの宛先への完全なルートを形成するためにルータを組み合わせることができるサブパスを表しています。各セグメントには識別子（セグメント識別子）があり、新しい IGP 拡張機能を使用してネットワーク全体に配布されます。この拡張機能は IPv4 および IPv6 のコントロール プレーンに等しく適用されます。従来の MPLS ネットワークとは異なり、セグメント ルータ ネットワーク内のルータに Label Distribution Protocol（LDP）や Resource Reservation Protocol（RSVP）、つまり、セグメント識別子の割り当てや通知を行い、それらの転送情報をプログラミングするトラフィック エンジニアリング（RSVP-TE）は必要ありません。

セグメント ルーティングを設定するには、次の 2 つの方法があります。

- 「segment-routing traffic-eng」サブモードでの SR-TE ポリシー
- 「mpls traffic-eng」サブモードで SR オプションを使用した TE トンネル

（注） ただし、上記の L2VPN と EVPN サービスを設定するのに使用できるのは「segment-routing traffic-eng」サブノードのみです。

各ルータ（ノード）と各リンク（隣接関係）には関連付けられたセグメント識別子（SID）があります。ノードセグメント識別子はグローバルに一意であり、IGP で決定されたルータへの最短パスを表します。ネットワーク管理者は各ルータに予約済みブロックからノード ID を割り当てます。一方、隣接関係セグメント ID はローカルで有効なものであり、出力インターフェイスなどの隣接ルータに固有の隣接関係を表します。ルータは、ノード ID の予約済みブロック外の隣接関係識別子を自動的に生成します。MPLS ネットワークでは、セグメント識別子は MPLS ラベル スタック エントリとしてエンコードされます。セグメント ID は指定したパスに沿ってデータを移動します。次の 2 種類のセグメント ID があります。

- プレフィックス SID：サービス プロバイダー コア ネットワーク内で IGP が計算した IP アドレス プレフィックスが含まれたセグメント ID。プレフィックス SID はグローバルに一意です。プレフィックス セグメントは、特定のプレフィックスに到達する最短パス（IGP が計算）を表します。ノード セグメントは、ノードのループバック アドレスに結合された特殊なプレフィックス セグメントです。これは、インデックスとしてノード固有の SR グローバル ブロック（SRGB）にアドバタイズされます。
- 隣接関係 SID：ネイバーへのアドバタイジング ルータの隣接関係が含まれたセグメント ID。隣接関係 SID は 2 つのルータ間のリンクです。隣接関係 SID は特定のルータに関連しているため、ローカルに一意となっています。

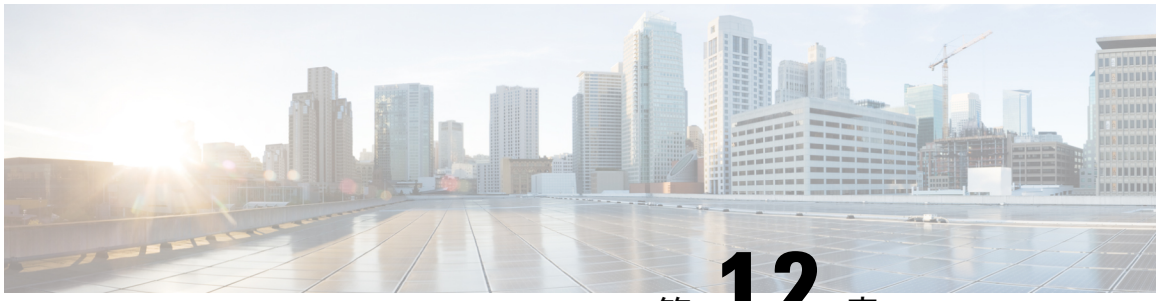
  ノードセグメントはマルチホップ パスを使用できますが、隣接関係セグメントはワンホップ パスです。

セグメント ルーティング グローバル ブロック

セグメント ルーティング グローバル ブロック（SRGB）は、セグメント ルーティングに予約されたラベルの範囲のことです。SRGB は、セグメント ルーティング ノードのローカル プロパティです。MPLS アーキテクチャでは、SRGB はグローバル セグメントに予約済みの一連のローカル ラベルです。セグメント ルーティングでは、各ノードを異なる SRGB で設定できます。そのため、IGP プレフィックス セグメントに関連付けられた絶対 SID はノードごとに変更できます。

SRGB のデフォルト値は 16000 ～ 23999 です。SRGBは、次のように設定できます。

```
Router(config)# router isis 1
Router(config-isis)#segment-routing global-block 45000 55000
```



第 12 章

MACsec を使用した BPDU 透過性の設定

この章では、MACsec 機能での BPDU 透過性について説明します。この機能を使用すると、送信元カスタマー エッジ（CE）デバイスと宛先 CE デバイス間にトンネルを作成し、このトンネルをこれら 2 つの CE 間でのトラフィックの伝送に使用します。

MACsec でのレイヤ 2 コントロール プレーンのトンネリング

レイヤ 2 コントロール プレーン トンネリングのパントの判断は、MACsec で設定されているインターフェイスによって異なります。メイン インターフェイスが MACsec ポリシーで設定されている場合、すべての MACsec パケットがパントされるため、カスタマー エッジ（CE）デバイスとプロバイダー エッジ（PE）デバイス間に MACsec セッションが確立されます。メイン インターフェイスが MACsec で設定されていない場合は、すべての MACsec パケットがリモート CE へトンネリングされます。

MACsec および MKA の概要

MACsec は、IEEE 802.1AE 規格ベースのレイヤ 2 ホップバイホップ暗号化であり、これにより、メディア アクセス非依存プロトコルに対してデータの機密性と完全性を確保できます。

MACsec は、暗号化キーにアウトオブバンド方式を使用して、有線ネットワーク上で MAC レイヤの暗号化を提供します。MACsec Key Agreement（MKA）プロトコルでは、必要なセッション キーを提供し、必要な暗号化キーを管理します。ホスト側のリンク（ネットワーク アクセス デバイスと、PC や IP フォンなどのエンドポイント デバイス間のリンク）だけが MACsec を使用して保護できます。

MACsec Key Agreement（MKA）による 802.1AE 暗号化は、ホスト デバイス間の暗号化用に、ダウンリンク ポートでサポートされています。

MACsec は、イーサネット パケットの送信元および宛先 MAC アドレスを除くすべてのデータを暗号化します。

WAN またはメトロ イーサネット上に MACsec サービスを提供するために、サービス プロバイダーは、Ethernet over Multiprotocol Label Switching（EoMPLS）および L2TPv3 などのさまざまなトランスポート レイヤ プロトコルを使用して、E-Line や E-LAN などのレイヤ 2 透過サービスを提供しています。

EAP-over-LAN（EAPOL）プロトコル データ ユニット（PDU）のパケット本体は、MACSec Key Agreement PDU（MKPDU）と呼ばれます。3 回のハートビート後（各ハートビートは 2 秒）に参加者から MKPDU を受信しなかった場合、ピアはライブ ピア リストから削除されます。たとえば、クライアントが接続を解除した場合、スイッチ上の参加者はクライアントから最後の MKPDU を受信した後、3 回のハートビートが経過するまで MKA の動作を継続します。

MKA 機能のサポートにより、暗号化されていない VLAN タグ（802.1Q タグ）などのトンネリング情報を提供します。そのため、サービス プロバイダーは、複数のポイントツーポイント サービスが単一の物理インターフェイス上で共存でき、表示されるようになった VLAN ID に基づいて差別化できるように、サービス多重化を提供できます。

サービス多重化の他に、暗号化されていない VLAN タグもサービス プロバイダーが 802.1Q タグの一部として表示されている 802.1P（CoS）に基づいて SP ネットワーク全体にわたり Quality of Service（QoS）を提供できるようにします。

L2CP トンネリング

レイヤ 2 コントロール プレーンは、数多くのカスタマー コントロール プレーンとプロバイダー コントロール プレーンに分割されています。IEEE 規格 802.1Q-2011 で定義されているように、L2CP フレームはコントロール プレーン用に予約されている 32 個のアドレスのうちの 1 つである宛先 MAC アドレスを含んでいるフレームです。VPWS または VPLS のサービスを使用してトラフィックを転送できます。

MACsec での L2CP トンネリング

パントの判断は、MACsec で設定されているインターフェイスによって異なります。インターフェイスが MACsec ポリシーで設定されている場合は、すべての MACsec パケットがパントされるため、2 つのカスタマー エッジ（CE）デバイス間で MACsec セッションが確立されます。インターフェイスが MACsec で設定されていない場合は、すべての MACsec パケットがリモート CE にトンネリングされます。MACsec はサブインターフェイスでは設定できません。

CE が MACsec で設定されていて、PE が L2VPN VPWS で設定されている場合、すべての MACsec パケットは VPWS を介してトンネリングされます。

PC のいずれかの CE 接続インターフェイスで MACsec が設定されている場合、このインターフェイス上のすべての MACsec パケットはパントされます。これらのパケットはリモート CE

に転送されません。PE のインターフェイスで MACsec が設定されている場合、PE デバイスと CE デバイス間で MACsec セッションは確立されません。

設定

以降の項では、MACsec 機能を使用して BPDU 透過性を設定する手順について説明します。

- MPLS のコアの設定
- L2VPN クロス コネクトの設定
- CE デバイスでの MACsec の設定

L2VPN クロス コネクトの設定

コアに接続するインターフェイス上に IPv4 アドレスを設定します。

```
Router# configure
Router(config)# interface tengige 0/1/0/8/2.1
Router(config-subif)# no shut
Router(config-subif)# ipv4 address 192.0.2.1/24
```

IPv4 ループバック インターフェイスを設定します。

```
Router# configure
Router(config)#  interface loopback 0
Router(config)# ipv4 address 10.0.0.1/32
```

IGP として OSPF を設定します。

```
Router# configure
Router(config)# router ospf 100 area 0
Router(config-ospf-ar)# interface Tengige 0/1/0/8/3
Router(config-ospf-ar-if)# exit
Router(config-ospf-ar)# interface loopback 1
```

物理コア インターフェイスに MPLS LDP を設定します。

```
Router(config-ospf-ar)# mpls ldp
Router(config-ldp)# interface TenGigE 0/1/8/3
```

コアに接続するインターフェイス上に IPv4 アドレスを設定します。

```
Router# configure
Router(config)#  router bgp 100
Router(config-bgp)# bgp router-id 10.10.10.1
Router(config-bgp)# address-family ipv4 unicast
Router(config-bgp-af)# exit
Router(config-bgp)# address-family l2vpn vpls-vpws
Router(config-bgp-af)# exit
Router(config-bgp)# neighbor 172.16.0.1
Router(config-bgp-nbr)# remote-as 2002
Router(config-bgp-nbr)# update-source loopback 2
Router(config-bgp-nbr)# address-family l2vpn vpls-vpws
Router(config-bgp-nbr-af)# next-hop-self
```

レイヤ 2 転送として AC を設定し、リモートの疑似回線にパケットを転送します。

```
Router# configure
Router(config)# interface TenGigE 0/1/0/8/2.1 l2tranport
Router(config-if)# encap dot1q 1
```

疑似回線であるネイバーを使用して L2VPN クロスコネクトを設定します。

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group g1
Router(config-l2vpn-xc)# p2p g1
Router(config-l2vpn-xc-p2p)# interface TenGigE 0/1/0/2.1
Router(config-l2vpn-xc-p2p)# neighbor 172.16.0.1 pw-id 1
Router(config-l2vpn-xc-p2p-pw)#
```

CE デバイスでの MACsec の設定

```
Router# configure
Router(config)# key chain KC1 macsec
Router(config-kc1-MacSec)# key 5010
Router(config-kc1-MacSec-5010)# key-string password
04795B232C766A6C513A5C4E37582F220F087178116703312446552501 7A0C7101 cryptographic-algorithm
 aes-128-cmac
Router(config-kc1-MacSec-5010)# lifetime 11:08:00 Aug 08 2017 infinite
Router(config-kc1-MacSec-5010)# commit
!
Router# configure
Router(config)# interface HundredGigE 0/0/0/3
Router(config-if)# macsec psk-keychain KC1
Router(config-if)# commit
```

実行コンフィギュレーション

ここでは、MACsec を使用した BFD 透過性の実行コンフィギュレーションを示します。

```
/* Configuring MPLS core.*/

/* Configure an IPv4 address on an interface that connects to the MPLS core. */

interface tengige 0/1/0/8/3
 no shut
 ipv4 address 192.0.2.0/24
!

/* Configure an IPv4 loopback interface. */

 interface loop 0
 ipv4 address 10.0.0.1/32

/* Configure OSPF as IGP. */

 router ospf 100 area 0
  interface TenGige 0/1/0/8/3
   interface loop 0
!

/* Configure MPLS LDP for the physical core interface. */
```

```
 mpls ldp
  interface TenGige 0/1/0/8/3
  !
!

/* Configuring L2VPN Xconnect. */

/* Configure an IPv4 address on an interface that connects to the MPLS core. */

router bgp 100
 bgp router-id 192.1.2.22
 address-family ipv4 unicast
 exit
 address-family l2vpn vpls-vpws
 neighbor 172.16.0.1
  remote-as 100
  update-source Loopback2
  address-family l2vpn vpls-vpws
   next-hop-self

/* Configure L2VPN Xconnect with a neighbour which is a pseudowire. */

l2vpn
 xconnect group g1
  p2p g1
  interface tengige 0/1/0/8/2.1
  neighbor 172.16.0.1 pw-id 1

/* Configure MACSec on CE device */
configure
 key chain KC1 macsec
  key 5010
   key-string password 04795B232C766A6C513A5C4E37582F220F087178116703312446552501 7A0C7101
 cryptographic-algorithm aes-128-cmac
   lifetime 11:08:00 Aug 08 2017 infinite
commit
!
configure
 interface HundredGigE0/0/0/3
  macsec psk-keychain KC1
commit
end
```

確認

次の項に示す show 出力には、MACsec 機能を使用した BPDU 透過性設定の詳細と、それらの設定のステータスが表示されます。

```
/* Verify if IGP on the core is up. */
Router# show ospf neighbor
Group Wed Aug 16 20:32:33.665 UTC
Indicates MADJ interface
# Indicates Neighbor awaiting BFD session up
Neighbors for OSPF 100
Neighbor ID     Pri   State           Dead Time   Address     Interface
172.16.0.1      1     FULL/DR         00:00:30    10.1.1.2    TenGigE0/1/0/8/0
 Neighbor is up for 06:05:27Total neighbor count: 1

/* Verify if the MPLS core is up. */
Router# show mpls ldp neighbor
```

```
Wed Aug 16 20:32:38.851 UTC

Peer LDP Identifier: 172.16.0.1:0
  TCP connection: 172.16.0.1:64932 - 172.31.255.254:646
  Graceful Restart: No
  Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 487/523; Downstream-Unsolicited
  Up time: 06:05:24
  LDP Discovery Sources:
    IPv4: (2)
      TenGigE0/1/0/8/0
      Targeted Hello (172.31.255.254 -> 172.16.0.1, active)
    IPv6: (0)
  Addresses bound to this peer:
    IPv4: (8)
      10.0.0.1       10.0.0.2         10.0.0.200       172.16.0.1
      192.168.0.1    172.31.255.255   172.16.0.2       10.255.255.254
    IPv6: (0)

/* Verify if the BGP neighbor is up. */
Router# show bgp neighbor 10.10.10.1

Wed Aug 16 20:32:52.578 UTC

BGP neighbor is 10.10.10.1
 Remote AS 15169, local AS 15169, internal link
 Remote router ID 172.31.255.255
  BGP state = Established, up for 06:03:40
  NSR State: None
  Last read 00:00:34, Last read before reset 00:00:00
  Hold time is 180, keepalive interval is 60 seconds
  Configured hold time: 180, keepalive: 60, min acceptable hold time: 3
  Last write 00:00:34, attempted 19, written 19
  Second last write 00:01:34, attempted 19, written 19
  Last write before reset 00:00:00, attempted 0, written 0
   *****************
Connections established 1; dropped 0

/* Verify if the BGP neighbor's next-hop information is valid. */
Router# show cef 10.10.10.1
Wed Aug 16 20:33:18.949 UTC
10.10.10.1/32, version 16, internal 0x1000001 0x0 (ptr 0x8e0ef628) [1], 0x0 (0x8e287bc0),

 0xa20 (0x8e9253e0)
 Updated Aug 16 14:27:15.149
 local adjacency 172.16.0.1
 Prefix Len 32, traffic index 0, precedence n/a, priority 3
   via 172.16.0.1/32, TenGigE0/1/0/8/0, 5 dependencies, weight 0, class 0 [flags 0x0]
    path-idx 0 NHID 0x0 [0x8eb60568 0x8eb60e70]
    next hop 172.16.0.1/32
    local adjacency
     local label 64001      labels imposed {ImplNull}

/* Verify if L2VPN Xconnect is up. */
Router# show l2vpn xconnect

Wed Aug 16 20:47:01.053 UTC
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

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

```
b1          b1          UP    BE100                    UP       10.10.10.1      1       UP

------------------------------------------------------------------------------------------

/* Note: If L2VPN is down even though the MPLS LDP neighbor is up, check if the AC is
down.
To do this, use the show l2vpn xconnect detail command. */


/* Verify if L2VPN Xconnect is up */
Router# show l2vpn xconnect detail

!
 !

AC: Bundle-Ether100, state is up      <<<< This indicates that the AC is up.
    Type Ethernet
    MTU 1500; XC ID 0xa0000002; interworking none
    Statistics:
      packets: received 761470, sent 0
      bytes: received 94326034, sent 0
  PW: neighbor 10.10.10.1, PW ID 1, state is up ( established )
    PW class not set, XC ID 0xc0000001
    Encapsulation MPLS, protocol LDP
    Source address 172.16.0.2
    PW type Ethernet, control word disabled, interworking none
    PW backup disable delay 0 sec
    Sequencing not set

!
 !
```