



Cisco NCS 540 シリーズ ルータ (IOS XR リリース 6.3.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 : 2017 年 3 月 30 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/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークボロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018 Cisco Systems, Inc. All rights reserved.



目次

はじめに :

はじめに xi

マニュアルの入手方法およびテクニカル サポート xi

第 1 章

レイヤ2 仮想プライベート ネットワークの概要 1

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 2

イーサネット データ プレーン ループバック 3

イーサネット データ プレーン ループバックの設定 4

実行コンフィギュレーション 5

確認 6

イーサネット ローカル管理インターフェイス (E-LMI) 7

E-LMI メッセージング 8

E-LMI 動作 9

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 9

実行コンフィギュレーション 11

イーサネット Local Management Interface (LMI) 設定の確認 12

第 2 章

L2CP トンネリング 15

L2CP トンネリングの設定 16

第 3 章

レイヤ2 アクセス コントロール リスト 25

レイヤ2 アクセス コントロール リスト設定の前提条件 25

レイヤ2 アクセス コントロール リスト機能の特長 26

レイヤ2 アクセス コントロール リストの目的 26

レイヤ2 アクセス コントロール リストの仕組み 26

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	26
レイヤ2アクセスコントロールリストの作成	27
レイヤ2アクセスコントロールリスト設定の制約事項	28
設定	28
実行コンフィギュレーション	28
確認	28

第 4 章

ギガビットイーサネット リンク バンドルの設定	31
VLAN バンドルの設定	33
リンク バンドルの設定に関する参照	35
リンク バンドルの特性	35
イーサネット インターフェイスのバンドルを構成する方法	36
LACP を通じたリンク集約	37
QoS およびリンク バンドル	38

第 5 章

Ethernet over MPLS	39
イーサネット ポート モード	39
VLAN モード	40
QinQ モード	41
接続回線間のローカル スイッチングの設定	41
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	46
フレキシブルクロスコネクト サービス	48
フレキシブルクロスコネクト サービス：シングルホーム	49
フレキシブルクロスコネクト サービス：マルチホーム	49
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	50
VLAN 非対応	50
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	50
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	52
VLAN 対応	56
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	56

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 57

ローカル スイッチング 62

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 62

L2VPN での仮想回線接続検証 64

第 6 章

VLAN サブインターフェイスの設定 67

イーサネット フロー ポイントの概要 68

EFP のフレームの識別 69

機能の適用 70

データ転送動作の定義 71

VLAN ヘッダー書き換えの設定 71

有効な入力書き換えアクション 73

有効な入力と出力の書き換えの組み合わせ 73

第 7 章

EVPN の概要 75

EVPN の概念 76

EVPN 動作 77

EVPN ルートタイプ 78

EVPN L2 ブリッジング サービスの設定 80

実行コンフィギュレーション 80

EVPN ソフトウェア MAC ラーニング 80

EVPN ソフトウェア MAC ラーニングの設定 81

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 82

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 82

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 82

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 84

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 84

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 87

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	87
EVPNソフトウェアMACラーニングの確認	89
EVPNアウトオブサービス	91
EVPNアウトオブサービスの設定	92
実行コンフィギュレーション	92
EVPNルーティングポリシー	94
EVPNルートタイプ	95
EVPNRPL属性	100
EVPNRPL属性セット	102
EVPNRPL機能の設定	104
実行コンフィギュレーション	105
<hr/>	
第8章	EVPN IRB 111
EVPNシングルホーミングアクセスゲートウェイ	112
EVPNマルチホーミングオールアクティブ	113
手動ESI設定を使用した自動BGPRTの有効化	114
サポートされているEVPNIRBのシナリオ	114
分散型ユニキャストゲートウェイ	115
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EVPNIRB	115
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EVPNIRB	116
MACおよびIPユニキャストのコントロールプレーン	117
サブネット内ユニキャストデータプレーン	118
サブネット間ユニキャストデータプレーン	118
VMモビリティサポート	119
MACおよびMAC-IPシーケンス番号	119
MACおよびMAC-IPシーケンス番号の同期	119
ローカルシーケンス番号の更新	120
ホスト移動後のベストルートの選択	120
ホスト移動後の古いルートの削除	120

GARP でのホスト移動検出	120
サイレント ホストを使用したホスト移動検出	120
データ パケットを使用した GARP なしのホスト移動検出	120
重複 MAC 検出	121
EVPN IRB の設定	121
EVPN IRB の実行コンフィギュレーション	123
EVPN IRB の確認	124

 第 9 章

EVPN-VPWS シングル ホーム	137
EVPN-VPWS シングル ホームの設定	138
実行コンフィギュレーション	138
EVPN-VPWS マルチホーム	139
EVPN-VPWS マルチホームの設定	140
実行コンフィギュレーション	141

 第 10 章

SR-TE ポリシーを介した EVPN VPWS 優先パス	143
SR-TE ポリシーを介した EVPN VPWS 優先パスの設定	144
ISIS でのプレフィックス SID の設定	145
ISIS での隣接関係 SID の設定	146
セグメントリストの設定	148
SR-TE ポリシーの設定	149
SR-TE ポリシーを介した EVPN VPWS の設定	150
実行コンフィギュレーション	150
SR-TE ポリシーを介した EVPN VPWS 優先パスの確認	155
関連コマンド	156
関連項目	156
SR-TE ポリシーを介した L2VPN VPLS または VPWS 優先パス	156
SR-TE ポリシーを介した L2VPN VPLS または VPWS 優先パスの設定	156
ISIS でのプレフィックス SID の設定	157
ISIS での隣接関係 SID の設定	158
セグメントリストの設定	160

SR-TE ポリシーの設定	161
SR-TE ポリシーを介した VPLS の設定	162
SR-TE ポリシーを介した VPWS の設定	163
実行コンフィギュレーション	163
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	167
関連コマンド	170
関連項目	170
SR-TE を使用した EVPN VPWS オンデマンドネクストホップ	170
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	171
トポロジ	172
ISIS でのプレフィックス SID の設定	172
SR-TE の設定	174
PCE と PCC の設定	175
SR カラーの設定	175
EVPN ルートポリシーの設定	176
BGP の設定	176
EVPN VPWS の設定	177
フレキシブルクロスコネクタサービス (FXC) VLAN 非対応の設定	178
実行コンフィギュレーション	178
関連項目	185
セグメントルーティングの概要	185
セグメントルーティングの仕組み	186
セグメントルーティング グローバルブロック	187

第 11 章**MSTP BPDU Guard 189**

MSTP BPDU Guard の設定	189
MSTP BPDU Guard を使用した実行コンフィギュレーション	190
MSTP BPDU Guard の確認	190

第 12 章**MACsec を使用した BPDU 透過性 191**

MACsec でのレイヤ 2 コントロールプレーンのトンネリング	191
----------------------------------	-----

MACsec および MKA の概要	191
L2CP トンネリング	192
MACsec での L2CP トンネリング	192
設定	193
実行コンフィギュレーション	194
確認	195



はじめに

「はじめに」の内容は次のとおりです。

- [マニュアルの入手方法およびテクニカルサポート](#) (xi ページ)

マニュアルの入手方法およびテクニカルサポート

マニュアルの入手方法、テクニカルサポート、その他の有用な情報について、次の URL で、毎月更新される『What's New in Cisco Product Documentation』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

『What's New in Cisco Product Documentation』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。



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 \(2 ページ\)](#)
- [イーサネット データ プレーン ループバック \(3 ページ\)](#)
- [イーサネット ローカル管理 インターフェイス \(E-LMI\) \(7 ページ\)](#)
- [E-LMI メッセージング \(8 ページ\)](#)
- [E-LMI 動作 \(9 ページ\)](#)
- [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 \(9 ページ\)](#)

ギガビットイーサネットインターフェイス上のレイヤ2VPN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。

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ず（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。



(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。

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。

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 ループバック 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。

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。

- 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 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。

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 0/2/0/0.1
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 0/2/0/0.1 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 0/2/0/0.1
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 0/2/0/0.1 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。

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、外部ループバックは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 ブレーン ループバック \(3 ページ\)](#)

関連コマンド

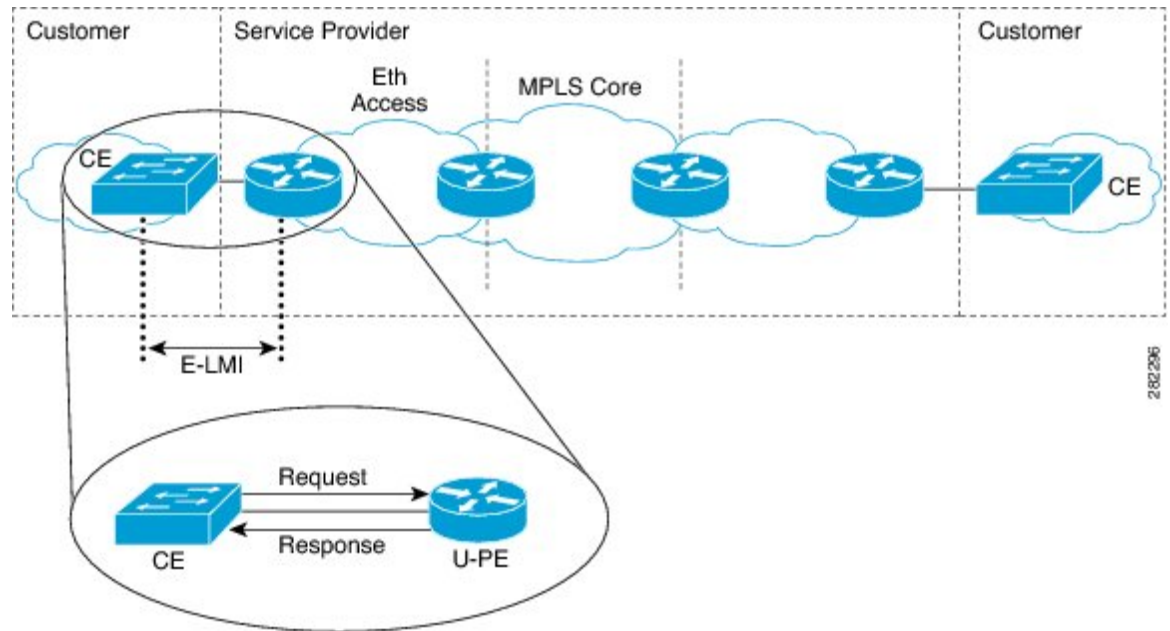
- ethernet loopback
- show ethernet loopback

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 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

Cisco NCS 540 シリーズルータで E-LMI を設定する前に、次の要件を満たしていることを確認します。

- 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) であることを確認します。

関連項目

- [イーサネット ローカル管理インターフェイス \(E-LMI\) \(7 ページ\)](#)
- [E-LMI メッセージング \(8 ページ\)](#)
- [E-LMI メッセージング \(8 ページ\)](#)

関連コマンド

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



第 2 章

L2CP トンネリング

レイヤ2コントロールプロトコルトンネリング (L2PT) は、レイヤ2スイッチングドメイン間でイーサネットプロトコルフレームをトンネリングするための、シスコ独自のプロトコルです。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)

次のような L2 転送インターフェイスがあります。

- VPWS I2 トランスポートメイン
- VPWS I2 サブインターフェイス
- L2 トランスポートメインブリッジポート
- I2 サブインターフェイスブリッジポート
- VPWS I2 バンドルメインポート
- VPWS I2 バンドルサブインターフェイス
- L2 バンドルメインブリッジポート

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。

Cisco NCS 540 シリーズルータでは、CE 間にレイヤ2パケットをトンネリングできます。NNI インターフェイスを介してパケットをトンネリングしている間は、シスコ独自のマルチキャストアドレス (01-00-0c-cd-cd-d0) が使用されます。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 Cisco NCS 540 シリーズ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（16 ページ）](#)

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

プロトコル	パケットタイプ	アクション
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)#

/* Configure BGP. */
RP/0/RP0/CPU0:ios(config)#router bgp 15169
RP/0/RP0/CPU0:ios(config-bgp)#bgp router-id 2.2.2.6
RP/0/RP0/CPU0:ios(config-bgp)#address-family l2vpn vpls-vpws
RP/0/RP0/CPU0:ios(config-bgp-af)#neigh 12.12.12.1
RP/0/RP0/CPU0:ios(config-bgp-nbr)#remote-as 15169
RP/0/RP0/CPU0:ios(config-bgp-nbr)#update-source loop 1
RP/0/RP0/CPU0:ios(config-bgp-nbr)#address-family l2vpn vpls-vpws
RP/0/RP0/CPU0:ios(config-bgp-nbr-af)#next-hop-
% Ambiguous command: "next-hop-"
RP/0/RP0/CPU0:ios(config-bgp-nbr-af)#next-hop-self
RP/0/RP0/CPU0:ios(config-bgp-nbr-af)#exit
RP/0/RP0/CPU0:ios(config-bgp-nbr)#exit
RP/0/RP0/CPU0:ios(config-bgp)#exit
RP/0/RP0/CPU0:ios(config)#

/* Configure L2VPn xconnect as vpws */
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 L2VPn xconnect as VPLS */
RP/0/RP0/CPU0:ios(config)#l2vpn
RP/0/RP0/CPU0:ios(config-l2vpn)#bridge group b1
RP/0/RP0/CPU0:ios(config-l2vpn-bg)#bridge-domain b1
RP/0/RP0/CPU0:ios(config-l2vpn-bg-bd)#int tenGigE 0/1/0/8/3
RP/0/RP0/CPU0:ios(config-l2vpn-bg-bd-ac)#exit
RP/0/RP0/CPU0:ios(config-l2vpn-bg-bd)#commit
Fri Sep 1 17:14:23.457 UTC
RP/0/RP0/CPU0:ios(config-l2vpn-bg-bd)#vfi vf
RP/0/RP0/CPU0:ios(config-l2vpn-bg-bd-vfi)#neighbor 12.12.12.1 pw-id 1

```

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 $l$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
!
!
!
router bgp 15169
bgp router-id 2.2.2.6
address-family l2vpn vpls-vpws
!
neighbor 12.12.12.1
remote-as 15169
update-source Loopback1
address-family l2vpn vpls-vpws
next-hop-self
!
!
!
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

/ * Running configuration for VPWS */

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
  !
!
!
router bgp 15169
bgp router-id 2.2.2.6
address-family l2vpn vpls-vpws
!
neighbor 12.12.12.1
  remote-as 15169
  update-source Loopback1
  address-family l2vpn vpls-vpws
  next-hop-self
!
!
!
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 Group	Name	ST	Segment 1 Description	ST	Segment 2 Description	ST
1	1	UP	Te0/1/0/8/3	UP	12.12.12.1	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 Group	Name	ST	Segment 1 Description	ST	Segment 2 Description	ST
1	1	UP	Te0/1/0/8/3	UP	12.12.12.1	UP

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



第 3 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2ACL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 \(25 ページ\)](#)
- [レイヤ2アクセスコントロールリスト機能の特長 \(26 ページ\)](#)
- [レイヤ2アクセスコントロールリストの目的 \(26 ページ\)](#)
- [レイヤ2アクセスコントロールリストの仕組み \(26 ページ\)](#)
- [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 \(26 ページ\)](#)
- [レイヤ2アクセスコントロールリストの作成 \(27 ページ\)](#)
- [レイヤ2アクセスコントロールリスト設定の制約事項 \(28 ページ\)](#)
- [設定 \(28 ページ\)](#)

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 が含まれません。

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 4 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 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。

機能制限

- 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 128 です。

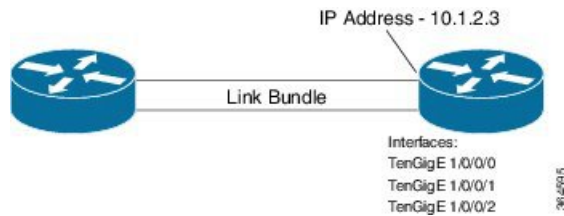
設定例

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 2: 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-if)# 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
Tel/0/0/0	Local	Active	0x8000, 0x0000	10000000
Link is Active				
Tel/0/0/1	Local	Active	0x8000, 0x0000	10000000
Link is Active				
Tel/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 \(33 ページ\)](#)
- [リンク バンドルの設定に関する参照 \(35 ページ\)](#)

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](#)

リンクバンドルの設定に関する参照

リンクバンドルの特性

- LACP (Link Aggregation Control Protocol) を使用するかにかかわらず、すべてのタイプのイーサネット インターフェイスをバンドルできます。
- 物理層とリンク層の設定は、バンドルの個々のメンバー リンクに対して実行します。
- ネットワーク層プロトコルおよび上位層のアプリケーションの設定は、バンドル自体に対して実行します。
- バンドルは、管理上イネーブルまたはディセーブルにできます。

- バンドル内のそれぞれのリンクは、管理上イネーブルまたはディセーブルにできます。
- イーサネット リンク バンドルは、EtheroKinet チャネルと同様の方法で作成され、両方のエンドシステムで同じコンフィギュレーションを入力します。
- バンドルに対して設定された MAC アドレスは、そのバンドル内の各リンクの MAC アドレスになります。
- LACP が設定されている場合、バンドル内の各リンクは、異なるメンバーに対して異なるキープアライブ周期を許可するよう設定できます。
- ロードバランシングはパケットではなくフローによって行われます。データはバンドル対するそのリンクの帯域幅に比例して、リンクに配信されます。
- QoS がサポートされており、各バンドルメンバーに均等に適用されます。
- CDP などのリンク層プロトコルは、バンドル内の各リンク上で独立して動作します。
- ルーティングアップデートや hello メッセージなどの上位層プロトコルは、インターフェイスバンドルのどのメンバリンク上でも送信されます。
- バンドルされたインターフェイスはポイント ツー ポイントです。
- リンクがバンドル内で分散状態になるには、その前にアップ状態なる必要があります。
- リンクバンドルでのアクセスコントロールリスト (ACL) 設定は、通常のインターフェイスでの ACL 設定と同じです。
- マルチキャストトラフィックは、バンドルのメンバー上でロードバランスされます。特定のフローに対し、内部プロセスによってメンバーリンクが選択され、そのフローのすべてのトラフィックがそのメンバー上で送信されます。

イーサネットインターフェイスのバンドルを構成する方法

Cisco IOS XR ソフトウェアでは、次の方法によるイーサネットインターフェイスのバンドル構成をサポートしています。

- IEEE 802.3ad : 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) を採用した標準テクノロジー。互換性がないリンクや障害になったリンクは、バンドルから自動的に削除されます。

バンドルメンバーとして設定された各リンクでは、この情報は、リンクバンドルの両端をホストするシステム間で交換されます。

- グローバルに一意的ローカルシステム ID
- リンクがメンバーになっているバンドルの ID (動作キー)
- リンクの ID (ポート ID)
- リンクの現在の集約ステータス

この情報は、リンク集約グループ ID (LAG ID) を構成するために使用されます。共通の LAG ID を共有するリンクは集約できます。個々のリンクには固有の LAG ID があります。

システム ID はルータを区別し、その一意性はシステムの MAC アドレスを使用することで保証されます。バンドル ID とリンク ID は、それを割り当てるルータでだけ意味を持ち、2 つのリンクが同じ ID を持たないことと、2 つのバンドルが同じ ID を持たないことが保証される必要があります。

ピアシステムからの情報はローカルシステムの情報と組み合わせられ、バンドルのメンバーとして設定されたリンクの互換性が判断されます。

ルータ内のバンドル MAC アドレスは、バックプレーン内の予約済み MAC アドレスのセットに由来します。この MAC アドレスは、バンドルインターフェイスが存在する限り、バンドルにとどまります。バンドルは、ユーザが別の MAC アドレスを設定するまで、この MAC アドレスを使用します。バンドルの MAC アドレスは、バンドルトラフィックを通過させる際にすべてのメンバーリンクによって使用されます。バンドルに対して設定されたすべてのユニキャストアドレスまたはマルチキャストアドレスも、すべてのメンバーリンクで設定されます。



(注) MAC アドレスを変更するとパケット転送に影響を与えるおそれがあるため、MAC アドレスは変更しないことを推奨します。

- EtherChannel : 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の専用テクノロジー。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。

LACP を通じたリンク集約

オプションの Link Aggregation Control Protocol (LACP) は IEEE 802 規格で定義されています。LACP では、2 台の直接接続されたシステム (ピア) 間で通信し、バンドルメンバーの互換性が確認されます。ルータの場合、ピアは、別のルータまたはスイッチにすることができます。LACP は、リンクバンドルの動作状態を監視し、次のことを確認します。

- すべてのリンクが同じ 2 台のシステム上で終端していること。
- 両方のシステムがリンクを同じバンドルの一部と見なしていること。
- すべてのリンクがピア上で適切に設定されていること

LACP で送信されるフレームの内容は、ローカルポート状態と、ローカルから見たパートナーシステムの状態です。これらのフレームが解析され、両方のシステムが同調していることが確認されます。

QoS およびリンクバンドル

入力方向では、バンドルのローカルインスタンスに QoS が適用されます。各バンドルはキューのセットに関連付けられます。QoS は、バンドル上で設定されているさまざまなネットワーク層プロトコルに適用されます。

出方向では、メンバーリンクへの参照を持つバンドルに QoS が適用されます。QoS は、メンバーの帯域幅の合計に基づいて適用されます。

QoS が入力または出力方向のいずれかのバンドルに適用される場合、QoS は各メンバーインターフェイスに適用されます。

詳細については、『*Modular QoS Configuration Guide for Cisco NCS 540 Series Routers*』の「*Configuring Modular QoS on Link Bundles*」の章を参照してください。



第 5 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。

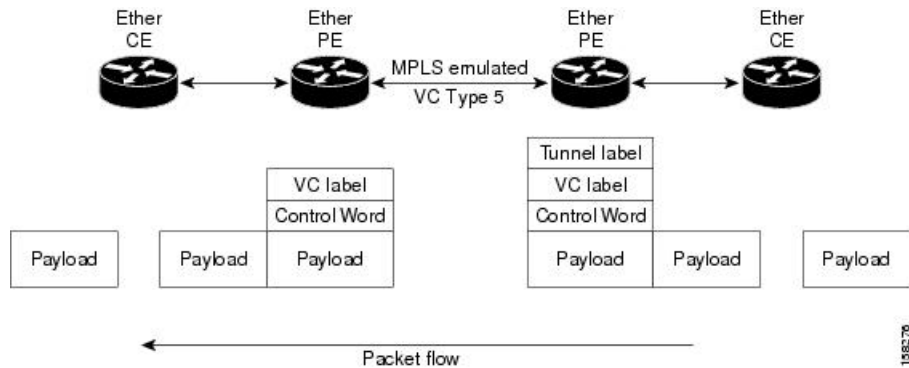
- [イーサネットポートモード \(39 ページ\)](#)
- [VLAN モード \(40 ページ\)](#)
- [QinQ モード \(41 ページ\)](#)
- [接続回線間のローカルスイッチングの設定 \(41 ページ\)](#)
- [クロスコネクト回線を使用したスタティックポイントツーポイント接続の設定 \(46 ページ\)](#)
- [フレキシブルクロスコネクトサービス \(48 ページ\)](#)
- [フレキシブルクロスコネクトサービスサポート対象モード \(50 ページ\)](#)
- [L2VPN での仮想回線接続検証 \(64 ページ\)](#)

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 3: イーサネットポートモードのパケットフロー

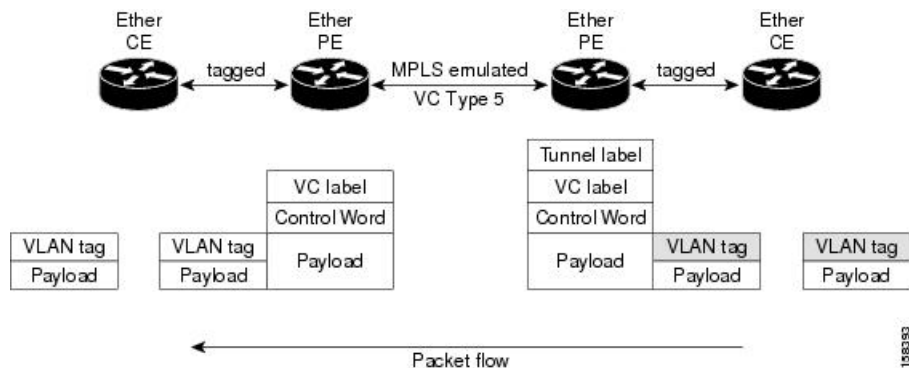


VLAN モード

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 4: 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 802.1Q QinQ 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。

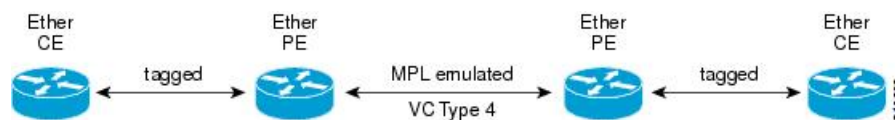
QinQ 上のレイヤ 3 サービスは次のとおりです。

- 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 5: QinQ を介した EoMPLS モード



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。

機能制限

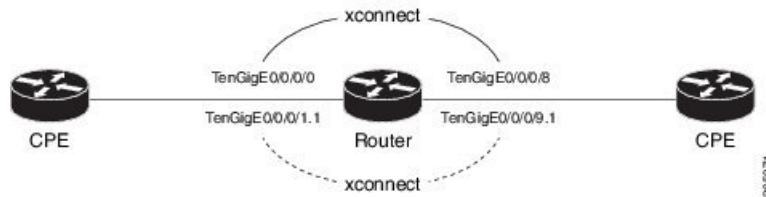
- 所定の物理ポートにあるすべてのサブインターフェイスは、次のような2つのタグプロトコル識別子（TPID）のみをサポートしています。
 - 0x88a8、0x8100
 - 0x9100、0x8100
 - 0x9200、0x8100
- VLAN および TPID ベースの入力パケット フィルタリングはサポートされていません。
- 出力 TPID の書き換えはサポートされていません。

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2VPN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2VPN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、クロスコネクタ回線（CCC）を使用します。

設定には次のトポロジを使用します。

図 6: 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 3000000
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 Group	Name	ST	Segment 1 Description	ST	Segment 2 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ることができます。
- 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。

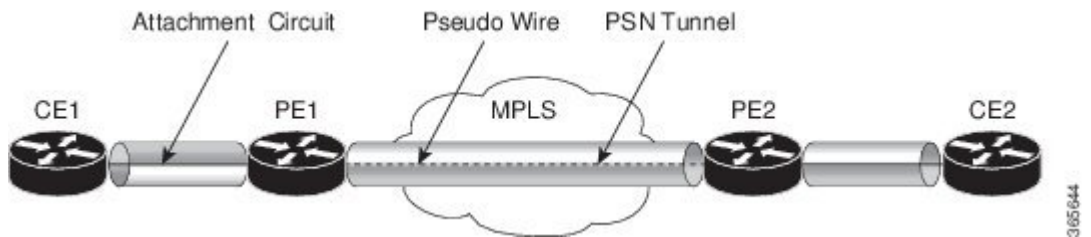


(注) スタティック疑似回線接続はシグナリングに LDP を使用しません。

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 7: 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 Group	Name	ST	Segment 1 Description	ST	Segment 2 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 Group	Name	ST	Segment 1 Description	ST	Segment 2 Description	ST
XCON2	xc1	UP	Gi0/2/0/0.4	UP	10.165.200.254 100	UP

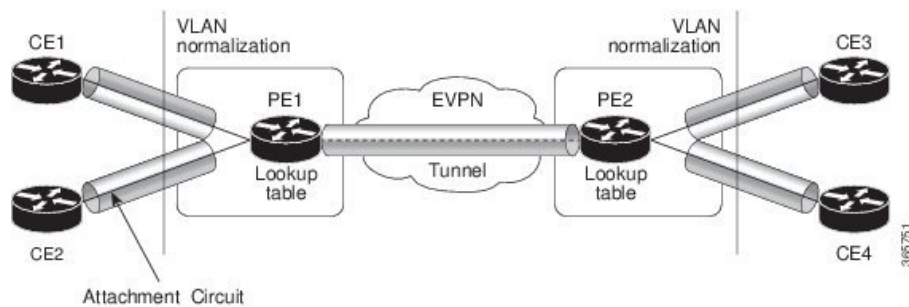
フレキシブルクロスコネク ト サービス

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 8: フレキシブルクロスコネク ト サービス

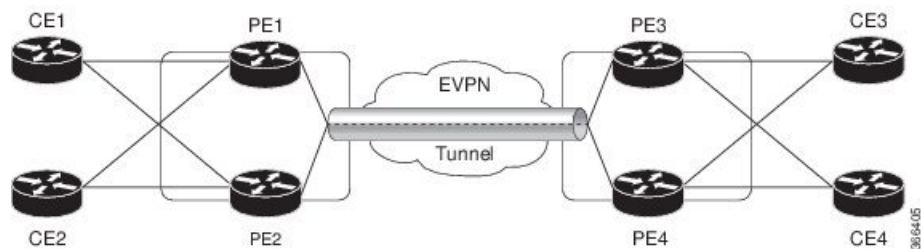


フレキシブルクロスコネク ト サービス : マルチホーム

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 9: 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 PE4 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。

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 symmetric
```

```

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 symmetric
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 symmetric
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 symmetric
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 symmetric
!

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

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 symmetric
!

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

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。

VLAN 対応を使用したシングルホーム フレキシブル クロスコネクタの設定

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 クロスコネクタ 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 symmetric
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 symmetric
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 symmetric
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 symmetric
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 symmetric
!

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

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 symmetric
!

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

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

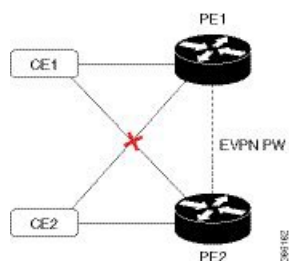
異なるイーサネットセグメントに属している2つのACに同じ正規化VLANがある場合、2つのAC間のトラフィックはPE内でローカルに切り替えられます。ローカルスイッチングはFXC VLAN対応でのみサポートされています。

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ESIを持っている必要があります。

図 10: 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タサービスの設定

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タ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

!

```

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。

Cisco NCS 540 シリーズ 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。

Cisco NCS 540 シリーズ ルータ。



第 6 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ン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せん。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***

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

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](#)（68 ページ）
- [VLAN ヘッダー書き換えの設定](#)（71 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せん。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 \(71 ページ\)](#) 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

カプセル化タイプ	EFP 識別子
二重タグ付きフレーム	

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、新しいタグging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 は同一にすることも、または別に行うことができます。
- 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 \(73 ページ\)](#)
- [有効な入力と出力の書き換えの組み合わせ \(73 ページ\)](#)

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

実行コンフィギュレーション

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)

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



第 7 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（76 ページ）](#)
- [EVPN 動作（77 ページ）](#)
- [EVPN ルートタイプ（78 ページ）](#)
- [EVPN L2 ブリッジング サービスの設定（80 ページ）](#)
- [EVPN ソフトウェア MAC ラーニング（80 ページ）](#)
- [EVPN アウトオブサービス（91 ページ）](#)
- [EVPN ルーティングポリシー（94 ページ）](#)

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。

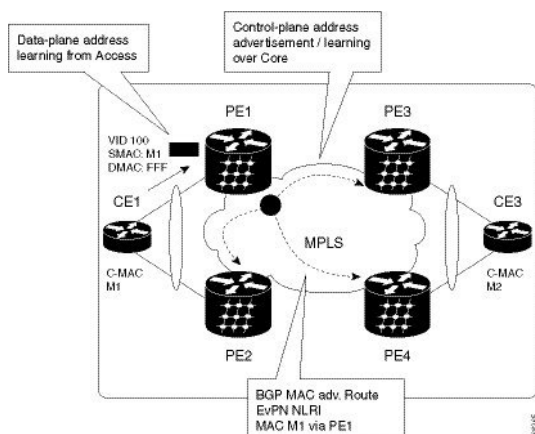
- **EVI** : EVPN インスタンス (EVI) は仮想ネットワーク識別子 (VNI) で表されます。EVI は、PE ルータ上の VPN を表します。EVI は IP VPN ルーティングおよび転送 (VRF) と同じ役割を果たし、インポート/エクスポートルートターゲット (RT) が割り当てられます。ユーザ ネットワーク インターフェイス (UNI) でのサービス多重化動作に応じて、ポート上のすべてのトラフィック (すべて対1のバンドリング)、VLAN 上のトラフィック (1対1のマッピング)、または VLAN のリスト/範囲のトラフィック (選択的バンドリング) をブリッジドメイン (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せん。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時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 `0xFFFFFFFF` 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 11: 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 を使用するのには、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。

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 1: 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

ルートタイプ	名前	使用法
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
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せん。

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 NRI 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。

```
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
```

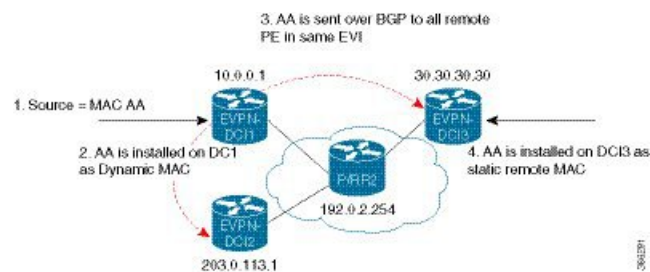
実行コンフィギュレーション

```
configure
l2vpn
  bridge group 1
    bridge-domain 1-1
      interface GigabitEthernet 0/0/0/1.1
        evi 1
!
```

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。

図 12: 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 ルーに交換され、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



(注) EVPN ブリッジングでは、**control-word-disable** コマンドはサポートされていません。

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。

```

/* 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 TenGigE0/4/0/10.2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface BundleEther 20.2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# storm-control broadcast pps 10000
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-nbr)# evi 2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# exit
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# exit
RP/0/RSP0/CPU0:router(config-l2vpn)# exit

/* Configure advertisement of MAC routes, suppress unknown unicast, disable the control
word, configure the flow label, configure BGP route-exchange using RT. */

RP/0/RSP0/CPU0:router(config)# evpn
RP/0/RSP0/CPU0:router(config-evpn)# evi 2001

/*Use the advertise-mac command to control the advertisement of MAC routes through BGP
to other neighbors. */
RP/0/RSP0/CPU0:router(config-evpn-evi)# advertise-mac

/* Use the unknown-unicast-suppress command to prevent unknown unicast traffic from going
to the MPLS core and then to all remote PE bridge-ports. */
RP/0/RSP0/CPU0:router(config-evpn-evi)# unknown-unicast-suppress

/* Use the control-word-disable command to prevent the control word from being sent in
the packet that is sent to MPLS core. The control word functionality is enabled by
default. */
RP/0/RSP0/CPU0:router(config-evpn-evi)# control-word-disable

/* Use the load-balance flow label static command to add additional flow label header
to the packet that is sent to MPLS core. The loadbalance flow functionality is disabled
by default. */
RP/0/RSP0/CPU0:router(config-evpn-evi)# load-balance flow label static

/* Perform the following steps to configure BGP route-exchange using RT */
RP/0/RSP0/CPU0:router(config-evpn-evi)# bgp

```

```

RP/0/RSP0/CPU0:router(config-evpn-evi)# route-target import 200:101
RP/0/RSP0/CPU0:router(config-evpn-evi)# route-target export 200:101

/* 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

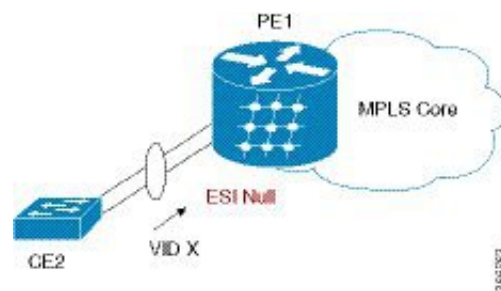
EVPN ソフトウェア MAC ラーニングでサポートされているモードは次のとおりです。

- 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 13: 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

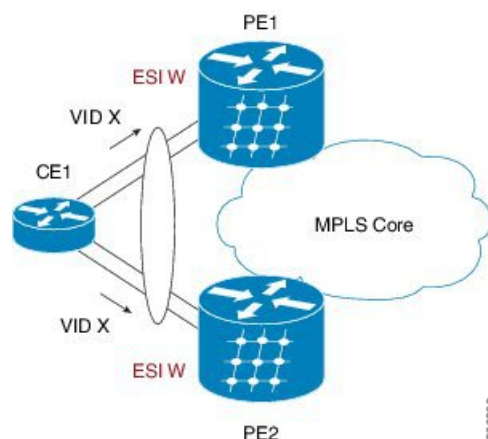
Ethernet Segment Id      Interface      Nexthops
-----
N/A                      Te0/4/0/10   20.20.20.20
.....
Topology :
Operational : SH
Configured : Single-active (AAPS) (default)

```

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 14: 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 01.11.00.00.00.00.00.01

/* 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 Multichassis Link Aggregation Control Protocol (MLACP) 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)# mlACP iccp-group 11
RP/0/RSP0/CPU0:router(config-if)# mlACP port-priority 1
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

/* Configure Interchassis Communication Protocol. */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# redundancy iccp group 100
RP/0/RSP0/CPU0:router(config-redundancy-iccp-group)# mlACP node 1
RP/0/RSP0/CPU0:router(config-redundancy-iccp-group)# mlACP system mac 0111.0222.0111
RP/0/RSP0/CPU0:router(config-redundancy-iccp-group)# mlACP system priority 1
RP/0/RSP0/CPU0:router(config-redundancy-iccp-group)# mode singleton
RP/0/RSP0/CPU0:router(config-redundancy-iccp-group)# backbone
RP/0/RSP0/CPU0:router(config-redundancy-iccp-group-backbone)# interface Bundle-Ether10
RP/0/RSP0/CPU0:router(config-redundancy-iccp-group-backbone)# interface HundredGigE
0/2/0/5

```

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 01.11.00.00.00.00.00.01

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
l2vpn switchover suppress-flaps 300
mlacp iccp-group 11
mlacp port-priority 1
load-interval 30
!
interface bundle-Ether1.2001 l2transport
  encapsulation dot1aq 2001
  rewrite ingress tag pop 1 symmetric
!
redundancy
iccp
  group 11
  mlacp node 1
  mlacp system mac 0111.0222.0111
  mlacp system priority 1
  mode singleton
  backbone
  interface Bundle-Ether10
  interface HundredGigE0/2/0/5

```

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

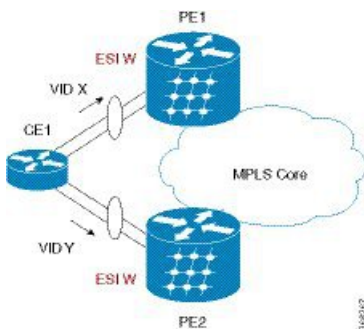
Peering timer : 3 sec [not running]
Recovery timer : 30 sec [not running]
Local SHG label : 34251
Remote SHG labels : 1
38216 : nexthop 209.165.201.1

```

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 15: 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 : 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 12.12.00.00.00.00.00.02
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EVPN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 (AAs)
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: TenGigE0/4/0/10.2001, 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 Te0/6/0/1.36001 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 Te0/6/0/1.36001 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   Te0/0/0/2/0.2001        N/A         11 Jan 14:37:22
N/A <-- local dynamic
00bb.2001.0001   dynamic   Te0/0/0/2/0.2001        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      TenGigE0/0/0/2/0.2001 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
```

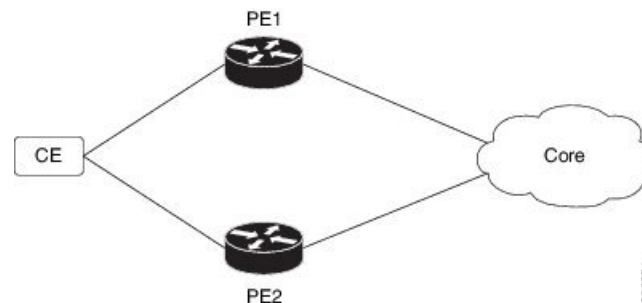
EVPN アウトオブサービス

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ー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ー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 ノードからそらしめます。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。

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ースがダウンします。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 16: 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 EVPN 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ースと 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。EVPN 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 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めます。

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。

```

+-----+
|Route Type (1 octet)          |*
+-----+
|Length (1 octet)             |
+-----+
|Route Distinguisher (RD) (8 octets) |*
+-----+
|Ethernet Segment Identifier (10 octets) |*
+-----+
|Ethernet Tag ID (4 octets)      |*
+-----+
|MPLS Label (3 octets)         |
+-----+

```

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。

Route Type (1 octet)	*
Length (1 octet)	
RD (8 octets)	*
Ethernet Segment Identifier (10 octets)	
Ethernet Tag ID (4 octets)	*
MAC Address Length (1 octet)	*
MAC Address (6 octets)	*
IP Address Length (1 octet)	*
IP Address (0, 4, or 16 octets)	*
MPLS Label1 (3 octets)	
MPLS Label2 (0 or 3 octets)	

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。

Route Type (1 octet)	*
Length (1 octet)	
RD (8 octets)	*
Ethernet Tag ID (4 octets)	*
IP Address Length (1 octet)	*
Originating Router's IP Address (4 or 16 octets)	*

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EVPNNLRIは次のフィールドで構成されます。

```

+-----+
|Route Type (1 octet)          |*
+-----+
|Length (1 octet)             |
+-----+
|RD (8 octets)                |*
+-----+
|Ethernet Segment Identifier (10 octets)|*
+-----+
|IP Address Length (1 octet)  |*
+-----+
|Originating Router's IP Address |*
|(4 or 16 octets)            |
+-----+

```

3-603-08

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。

Route Type (1 octet)	*
Length (1 octet)	
RD (8 octets)	*
Ethernet Segment Identifier (10 octets)	
Ethernet Tag ID (4 octets)	*
IP Address Length (1 octet)	*
IP Address (4 or 16 octets)	*
GW IP Address (4 or 16 octets)	
MPLS Label (3 octets)	

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 EVPN 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 referring 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 referring 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
!
```

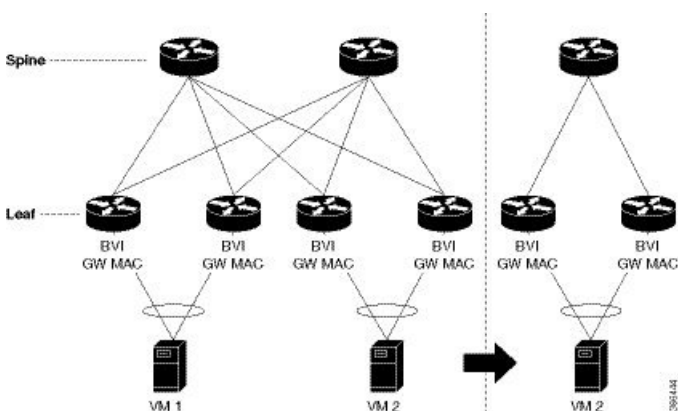


第 8 章

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 17: 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めます。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 ドメイン内で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であっても、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。

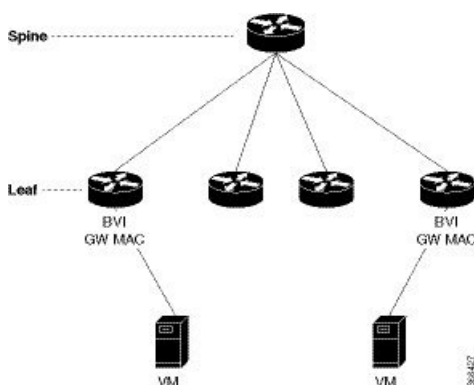
- [EVPN シングルホーミング アクセス ゲートウェイ \(112 ページ\)](#)
- [EVPN マルチホーミング オールアクティブ \(113 ページ\)](#)
- [手動 ESI 設定を使用した自動 BGP RT の有効化 \(114 ページ\)](#)
- [サポートされている EVPN IRB のシナリオ \(114 ページ\)](#)
- [分散型エニーキャスト ゲートウェイ \(115 ページ\)](#)
- [VM モビリティ サポート \(119 ページ\)](#)
- [EVPN IRB の設定 \(121 ページ\)](#)
- [EVPN IRB の実行コンフィギュレーション \(123 ページ\)](#)
- [EVPN IRB の確認 \(124 ページ\)](#)

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 18: EVPN シングルホーミング アクセスゲートウェイ

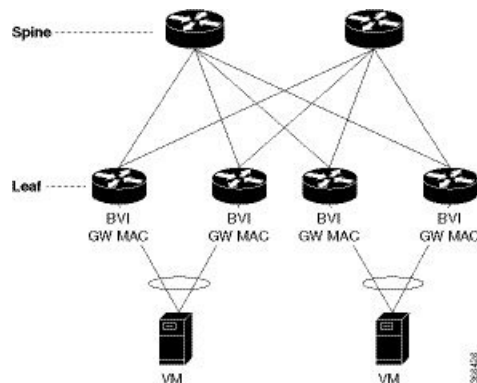


上記は、CE デバイスによる PE デバイス 1 台への接続を許可することによって EVPN シングルホーミングアクセスゲートウェイがネットワーク接続を有効にするトポロジを示しています。PE デバイスはバンドルインターフェイスまたは物理インターフェイスを通じてイーサネットセグメントに接続されます。シングルホーミングにはヌルイーサネットセグメント識別子 (ESI) を使用します。

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 Cisco NCS 540 シリーズルータのデータセンターインターコネクト (DCI) ゲートウェイ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 19: 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。

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。リリース 6.1.31 以降、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るようになりました。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

リリース 6.1.31 では、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ド (DF) 選択とスプリットホライズ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ズ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。

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 EVPN 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。

リリース 6.1.31 では、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 のエイ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 検出とフリーズ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ズングです。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 MLAG bundle into ICCP group and 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)# mlacp iccp-group 300
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 irbl
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 irbl
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

```
/* Include MCLAG bundle into the ICCP group. */

interface Bundle-Ether3
mlacp iccp-group 300
!

/* 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) 1000000100010010000100010800
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

RPL2FIB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 0x50000001 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 を確認します。

```
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
  !
!

```

!

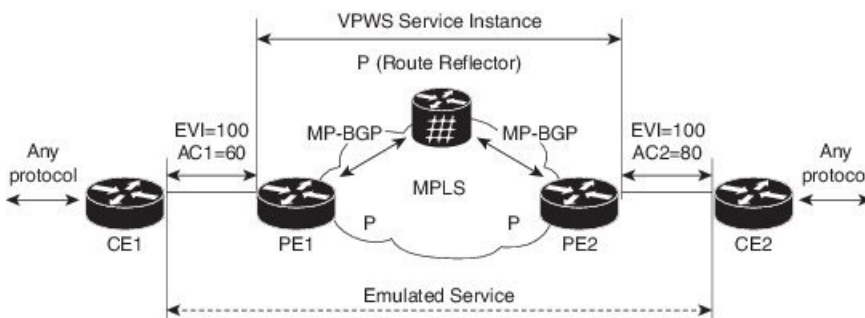


第 9 章

EVPN-VPWS シングル ホーム

EVPN-VPWS シングル ホーム ソリューションには EVI ごとのイーサネット自動検出ルートが必要です。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 にエントリーを追加します。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（138 ページ）](#)
- [EVPN-VPWS マルチホーム（139 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-family 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-family l2vpn evpn
  neighbor 10.10.10.1
!

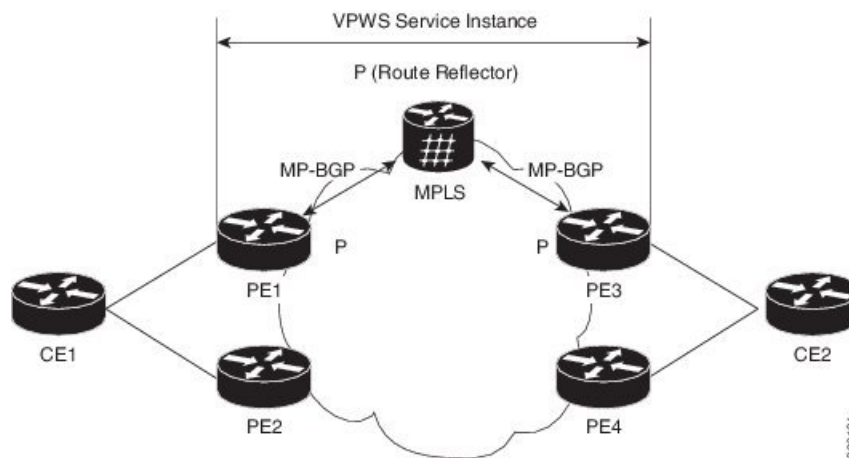
configure
l2vpn
  xconnect group evpn-vpws
  p2p evpn1
  interface TenGigE0/1/0/2
  neighbor evpn evi 100 target 12 source 10
!
```

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 20: 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
!
```



第 10 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。

機能制限

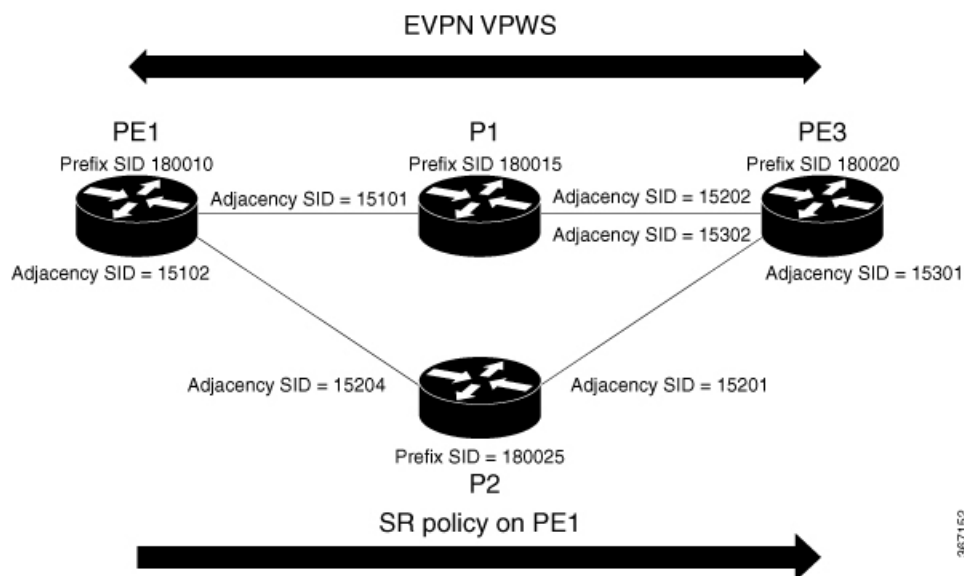
- ISIS プロトコルのみがサポートされています。
- オンデマンドネクストホップ (ODN) を備えた EVPN VPWS を設定し、優先パスがある EVPN VPWS も同じ PW に設定すると、優先パスが優先されます。
- EVPN VPWS SR ポリシーは EVPN VPWS デュアル ホーミングではサポートされていません。
- EVPN はルートがシングル ホーム ネクスト ホップ用であるかどうかを検証します。そうでない場合は、不適切な SR-TE ポリシーに関するエラー メッセージを発行し、そのポリシーなしで EVPN-VPWS のセットアップを続行します。EVPN は、これがシングル 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
/* Or globally */
Evpn
  ethernet-segment type 1 auto-generation-disable
```

トポロジ

図 21: 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 \(144 ページ\)](#)
- [SR-TE ポリシーを介した L2VPN VPLS または VPWS 優先パス \(156 ページ\)](#)
- [SR-TE を使用した EVPN VPWS オンデマンドネクストホップ \(170 ページ\)](#)
- [セグメントルーティングの概要 \(185 ページ\)](#)
- [セグメントルーティングの仕組み \(186 ページ\)](#)
- [セグメントルーティング グローバルブロック \(187 ページ\)](#)

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。

- ISIS でのプレフィックス SID の設定
- ISIS での隣接関係 SID の設定
- 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
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 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 precedence
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

```

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 pref_sid_to_PE3 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 pref_sid_to_PE3, 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 pref_sid_to_PE3, Statically configured, fallback disabled
Tunnel : Down

```

実行コンフィギュレーション

```
/* Configure Prefix-SID in ISIS */
P1:

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
```

PE2:

```
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 pref_sid_to_PE3 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 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*』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 \(185 ページ\)](#)
- [セグメントルーティングの仕組み \(186 ページ\)](#)
- [セグメントルーティング グローバルブロック \(187 ページ\)](#)

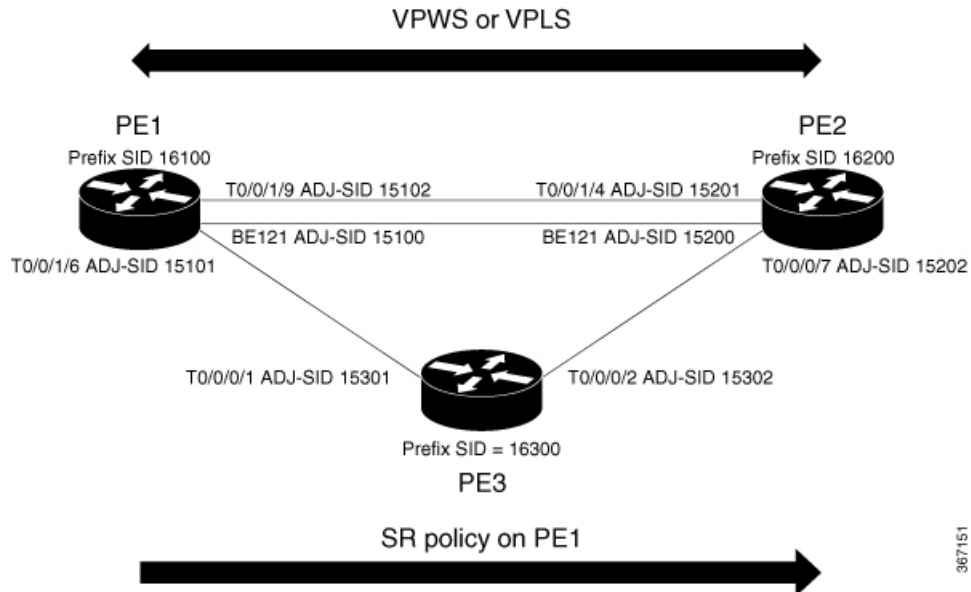
SR-TE ポリシーを介した L2VPN VPLS または VPWS 優先パス

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。ISIS プロトコルのみがサポートされています。

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 22: SR-TE ポリシーを介した L2VPN VPWS および VPLS 優先パス



367/151

- ISIS でのプレフィックス SID の設定
- ISIS での隣接関係 SID の設定
- 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
- SR-TE ポリシーを介した VPWS の設定

ISIS 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

```

ISIS 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 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 15101
Route(config-isis-if-af)# exit
!
Router# configure
Route(config)# router isis core
Route(config-isis)# interface TenGigE0/0/1/9
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 TenGigE0/0/1/4
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
Router(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

```

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 100
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 1013 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 TenGigE0/0/1/0.501
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

```

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 1300 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 TenGigE0/0/1/1.1002
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 TenGigE0/0/1/6
  circuit-type level-2-only
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
  adjacency-sid absolute 15101
!
interface TenGigE0/0/1/9
  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 100
pw-class pw1013
  encapsulation mpls
  preferred-path sr-te policy 1013 fallback disable

l2vpn
bridge group bg1
bridge-domain vpls501
  interface Bundle-Ether41.501
  !
  interface TenGigE0/0/1/0.501
  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 1300 fallback disable

Xconnect group xcon1
p2p vplw1002
  interface TenGigE0/0/1/1.1002
  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 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         Te0/0/1/9         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           Te0/0/1/6   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    Next Hop          Switched
-----
1013          (SR) 15302  Te0/0/1/6   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 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 \(185 ページ\)](#)
- [セグメント ルーティングの仕組み \(186 ページ\)](#)
- [セグメント ルーティング グローバルブロック \(187 ページ\)](#)

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。

機能制限

- 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
/* 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。

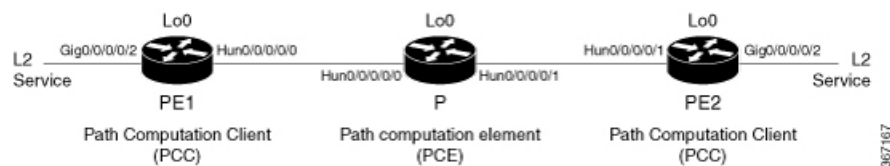
- ISIS でのプレフィックス SID の設定
- SR-TE の設定
- PCE と PCC の設定
- SR カラーの設定
- EVPN ルート ポリシーの設定

- 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 23: 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)# pce
Router(config-sr-te-pce)# address ipv4 205.2.0.2
Router(config-sr-te-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
!
```

PE:

```
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*』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 \(185 ページ\)](#)
- [セグメント ルーティングの仕組み \(186 ページ\)](#)
- [セグメント ルーティング グローバル ブロック \(187 ページ\)](#)

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 11 章

MSTP BPDU Guard

MSTP BPDU Guard 機能は、エッジポートの誤設定から保護します。



- (注) MSTP BPDU Guard をインターフェイスに対して有効にするには、**portfast bpduguard** コマンドをインターフェイス上に設定する必要があります。

PortFast

PortFast 機能は、スイッチドイーサネットネットワークのエッジでポートを管理します。スイッチドネットワーク（通常はホストデバイス）へのリンクが1つだけあるデバイスでは、使用可能なパスが1しかないため、MSTP を実行する必要はありません。さらに、代替パスがないため、単一のリンクで障害が発生するか復元された場合に、トポロジの変更（およびその結果の MAC フラッシュ）が起動されることは望ましくありません。

デフォルトでは、MSTP は、BPDU を受け取らないポートを監視して、タイムアウト後に、MSTP に参加しないようにするエッジモードにします。**portfast** がインターフェイスで明示的に設定されている場合、MSTP は、スパニングツリーの計算時に、そのインターフェイスをエッジポートであると見なし、考慮の対象から外します。したがって、**portfast** が設定されていると、ネットワーク全体のコンバージェンス時間が短縮されます。



- (注) MSTP BPDU Guard 機能は、PortFast モードでインターフェイスを設定することによってサポートされます。BPDU Guard 機能は、BPDU パケット受信時にポートを **error-disable** にします。

- [MSTP BPDU Guard の設定（189 ページ）](#)

MSTP BPDU Guard の設定

この項では、MSTP BPDU Guard を設定する方法について説明します。

```
Router# configure
Router(config)# l2vpn bridge group bg1
```

```

Router(config-l2vpn-bg)# bridge-domain bd1
Router(config-l2vpn-bg-bd)# int TenGigE 0/0/0/7
Router(config-l2vpn-bg-bd-ac)# root
Router(config)# spanning-tree mst m0
Router(config-mstp)# interface tenGigE 0/0/0/7
Router(config-mstp-if)# portfast bpduguard
Router(config-mstp-if)# root
Router(config)# int tenGigE 0/0/0/7 l2transport
Router(config-if-l2)# commit

```

MSTP BPDU Guard を使用した実行コンフィギュレーション

```

!
Configure
l2vpn
  bridge group bg1
  bridge-domain bd1
  interface TenGigE0/0/0/7
  !
spanning-tree mst m0
  interface TenGigE0/0/0/7
  portfast bpduguard
!
interface TenGigE0/0/0/7
  l2transport
!

```

MSTP BPDU Guard の確認

MSTP BPDU Guard が設定されていることを確認します。

```

/* Verify the MSTP BPDU Guard configuration */
Router# show interfaces tenGigE 0/0/0/7
Wed Nov  9 09:23:56.268 UTC
TenGigE0/0/0/7 is error disabled, line protocol is administratively down
  Interface state transitions: 2
  Hardware is TenGigE, address is 7cad.7425.c8c8 (bia 7cad.7425.c8c8)
  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,
  Last link flapped 00:00:49
  Last input 00:00:40, output 00:00:40
  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
    38752 packets input, 4611429 bytes, 0 total input drops
    1 drops for unrecognized upper-level protocol
  Received 1 broadcast packets, 38751 multicast packets
    0 runts, 0 giants, 0 throttles, 0 parity
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

```



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 \(191 ページ\)](#)
- [MACsec および MKA の概要 \(191 ページ\)](#)
- [L2CP トンネリング \(192 ページ\)](#)
- [MACsec での L2CP トンネリング \(192 ページ\)](#)
- [設定 \(193 ページ\)](#)

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 サービスやマルチポイント 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 制御プロトコル トンネリング (L2PT) は、レイヤ 2 スイッチング ドメイン間でイーサネット プロトコル フレームをトンネリングするための、シスコ独自のプロトコルです。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一つである宛先 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。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 デバイス (CE) とプロバイダー エッジ デバイス (PE) 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。

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

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。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tengige 0/1/0/8/2.1
RP/0/RSP0/CPU0:router(config-subif)# no shut
RP/0/RSP0/CPU0: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。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface loopback 0
RP/0/RSP0/CPU0:router(config)# ipv4 address 10.0.0.1/32
```

IGP として OSPF を設定します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router ospf 100 area 0
RP/0/0/CPU0:ios(config-ospf-ar)# interface Tengige 0/1/0/8/3
RP/0/0/CPU0:ios(config-ospf-ar-if)# exit
RP/0/0/CPU0:ios(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。

```
RP/0/0/CPU0:ios(config-ospf-ar)# mpls ldp
RP/0/0/CPU0:ios(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。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router bgp 100
RP/0/RSP0/CPU0:router(config-bgp)# bgp router-id 10.10.10.1
RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 unicast
RP/0/RSP0/CPU0:router(config-bgp-af)# exit
RP/0/RSP0/CPU0:router(config-bgp)# address-family l2vpn vpls-vpws
RP/0/RSP0/CPU0:router(config-bgp-af)# exit
RP/0/RSP0/CPU0:router(config-bgp)# neighbor 172.16.0.1
RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 2002
RP/0/RSP0/CPU0:router(config-bgp-nbr)# update-source loopback 2
RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family l2vpn vpls-vpws
RP/0/RSP0/CPU0: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。

```
RP/0/RSP0/CPU0:router# configure
```

```
RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/1/0/8/2.1 l2transport
RP/0/RSP0/CPU0: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。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/0/CPU0:ios(config-l2vpn)# xconnect group g1
RP/0/0/CPU0:ios(config-l2vpn-xc)# p2p g1
RP/0/0/CPU0:ios(config-l2vpn-xc-p2p)# interface TenGigE 0/1/0/2.1
RP/0/0/CPU0:ios(config-l2vpn-xc-p2p)# neighbor 172.16.0.1 pw-id 1
RP/0/0/CPU0:ios(config-l2vpn-xc-p2p-pw)#
```

実行コンフィギュレーション

この項では、疑似回線ヘッドエンド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

```

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. */
RP/0/RP0/CPU0: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. */
RP/0/RP0/CPU0: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. */
RP/0/RP0/CPU0: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. */
RP/0/RP0/CPU0: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. */
RP/0/RP0/CPU0: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
Group      Name      ST      Segment 1
          Description      ST      Segment 2
          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. */
RP/0/RP0/CPU0: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

!
!
```