



Cisco NCS 560 シリーズ ルータ (IOS XR リリース 6.6.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 : 2019 年 5 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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: 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)

© 2019 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

レイヤ 2 VPN のギガビットイーサネットの設定 1

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 5

実行コンフィギュレーション 6

確認 7

関連項目 8

関連コマンド 8

イーサネット ローカル管理インターフェイス (E-LMI) 8

E-LMI メッセージング 9

E-LMI 動作 10

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 10

実行コンフィギュレーション 12

イーサネット Local Management Interface (LMI) 設定の確認 13

第 2 章

レイヤ 2 アクセス コントロール リストの設定 17

レイヤ 2 アクセス コントロール リスト 17

レイヤ 2 アクセス コントロール リスト 設定の前提条件 18

レイヤ 2 アクセス コントロール リスト 機能の特長 18

レイヤ 2 アクセス コントロール リスト の目的 18

レイヤ 2 アクセス コントロール リスト の仕組み 18

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 19

レイヤ 2 アクセス コントロール リスト の作成 20

レイヤ2 アクセス コントロール リスト設定の制約事項	20
設定	20
実行コンフィギュレーション	21
確認	21

第 3 章

レイヤ 2 VPN の仮想 LAN の設定	23
VLAN サブインターフェイスの設定	24
イーサネット フロー ポイントの概要	26
EFP のフレームの識別	27
機能の適用	27
データ転送動作の定義	28
VLAN ヘッダー書き換えの設定	29
有効な入力書き換えアクション	30
有効な入力と出力の書き換えの組み合わせ	30

第 4 章

L2CP トンネリング MEF	31
L2CP トンネリング	31
L2CP トンネリングの設定	32

第 5 章

レイヤ 2 VPN のリンク バンドルの設定	43
ギガビットイーサネット リンク バンドルの設定	43
VLAN バンドルの設定	46
リンク バンドルの設定に関する参照	48
リンク バンドルの特性	48
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	49
LACP を通じたリンク集約	50

第 6 章

マルチポイント レイヤ 2 サービスの設定	51
マルチポイント レイヤ 2 サービス実装の前提条件	51
マルチポイント レイヤ 2 サービスの実装に関する情報	51
マルチポイント レイヤ 2 サービスの概要	51

ブリッジ ドメイン	52
疑似回線	52
アクセス疑似回線は VPLS ブリッジ ドメイン経由ではサポートされない	52
仮想転送インスタンス	53
MPLS ベースのプロバイダー コアの VPLS	53
レイヤ 2 スイッチングの VPLS	54
VPLS LDP シグナリングにおける Cisco IOS XR と Cisco IOS 間の相互運用性	54
MAC アドレス関連パラメータ	54
MAC アドレス フラッドイング	55
MAC アドレスベース転送	55
MAC アドレスの送信元ベースの学習	55
MAC アドレス エージング	55
MAC アドレス制限	56
MAC アドレス取り消し	56
マルチポイント レイヤ 2 サービスの実装方法	57
ブリッジ ドメインの設定	57
ブリッジ ドメインの作成	57
メンバのブリッジ ドメインへの関連付け	58
ブリッジ ドメインパラメータの設定	60
ブリッジ ドメインのディセーブル化	61
レイヤ 2 仮想転送インスタンスの設定	62
仮想転送インスタンスの作成	63
疑似回線の仮想転送インスタンスへの関連付け	64
ブリッジ ドメインへの仮想転送インスタンスの関連付け	65
疑似回線への疑似回線クラスの接続	67
スタティック ラベルを使用した疑似回線の設定	69
仮想転送インスタンスのディセーブル化	70
MAC アドレス関連パラメータの設定	72
MAC アドレスの送信元ベースの学習の設定	72
MAC アドレス制限の設定	74
MAC アドレス エージングの設定	77

ブリッジポートレベルでのMACフラッシュのディセーブル化	78
マルチポイントレイヤ2サービスの設定例	80
プロバイダーエッジ間のマルチポイントレイヤ2サービスの設定：例	80
プロバイダーエッジとカスタマーエッジ間のマルチポイントレイヤ2サービスの設定： 例	81
MACアドレス取り消しフィールドの表示：例	81
IOS XR トランク インターフェイスでのブリッジング：例	83
イーサネット フロー ポイントでのブリッジング：例	87
<hr/>	
第 7 章	ポイントツーポイントレイヤ2サービスの設定 91
Ethernet over MPLS	92
イーサネット ポート モード	92
VLAN モード	92
Inter-AS モード	93
QinQ モード	94
接続回線間のローカル スイッチングの設定	94
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	99
ダイナミック ポイントツーポイント相互接続の設定	101
Inter-AS の設定	102
フレキシブルクロスコネクト サービス	102
フレキシブルクロスコネクト サービス：シングルホーム	102
フレキシブルクロスコネクト サービス：マルチホーム	103
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	104
VLAN 非対応	104
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	104
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	106
VLAN 対応	110
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	110
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	111
ローカル スイッチング	116

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	116
AC 対応 VLAN バンドル	118
AC 対応 VLAN バンドルの設定	119
設定例	120
実行コンフィギュレーション	120
確認	120
スプリット ホライズン グループ	121
スプリット ホライズン グループ 2 の設定	123
G.8032 イーサネット リング保護	125
G.8032 イーサネット リング保護の設定	130
ERP プロファイルの設定	130
ERP インスタンスの設定	131
G.8032 イーサネット リング保護の設定：例	132
相互接続ノードの設定：例	133
開いたリングのノードの設定：例	134
疑似回線冗長性	136
疑似回線冗長性の設定	136
実行コンフィギュレーション	137
確認	137
疑似回線冗長性の設定	139
L2VPN での仮想回線接続検証	140

第 8 章
EVPN 機能 141

EVPN の概要	141
EVPN の概念	143
EVPN 動作	144
EVPN ルートタイプ	145
EVPN L2 ブリッジング サービスの設定	146
実行コンフィギュレーション	147
EVPN MAC アドレス制限の設定	148

EVPN ソフトウェア MAC ラーニング	150
EVPN ソフトウェア MAC ラーニングの設定	151
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	152
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	152
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	152
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	153
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	154
EVPN ソフトウェア MAC ラーニングの確認	156
EVPN アウト オブ サービス	158
EVPN アウト オブ サービスの設定	159
実行コンフィギュレーション	160
EVPN 対応 CFM のサポート	162
イーサネット セグメント単位の EVPN 複数サービス	162
イーサネット セグメント単位の EVPN 複数サービスの設定	163
設定例	163
実行コンフィギュレーション	165
関連コマンド	168
EVPN MPLS と VPLS のシームレスな統合	168
シームレスな統合による VPLS ネットワークの EVPN ネットワークへの移行	169
既存の VPLS ネットワークでの EVPN の設定	170
L2 EVPN アドレスファミリの設定	170
EVPN コンフィギュレーションモードでの EVI と対応する BGP ルートターゲットの設定	171
ブリッジ ドメインでの EVI の設定	171
L2VPN ブリッジ ドメインでの EVI の設定	172
EVPN 設定の確認	173
EVPN シングルアクティブ マルチホーミング	177
EVPN シングルアクティブ マルチホーミングの設定	178
EVPN イーサネット セグメントの設定	178
EVPN サービス インスタンス (EVI) パラメータの設定	179

レイヤ 2 インターフェイスの設定	179
ブリッジ ドメインの設定	179
EVPN コア分離保護	180
EVPN コア分離保護の設定	181
制約事項	181
実行コンフィギュレーション	182
確認	182
EVPN ルーティング ポリシー	183
EVPN ルート タイプ	183
EVPN RPL 属性	188
EVPN RPL 属性セット	190
EVPN RPL 機能の設定	192
実行コンフィギュレーション	193
EVPN ELAN での CFM	198
EVPN ELAN での CFM の設定	199

第 9 章

EVPN IRB の設定	203
EVPN IRB	203
EVPN シングルホーミング アクセス ゲートウェイ	205
EVPN マルチホーミング オールアクティブ	206
手動 ESI 設定を使用した自動 BGP RT の有効化	206
サポートされている EVPN IRB のシナリオ	207
分散型ユニキャスト ゲートウェイ	207
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	208
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	209
MAC および IP ユニキャストのコントロールプレーン	210
サブネット内ユニキャスト データ プレーン	211
サブネット間ユニキャスト データ プレーン	211
VM モビリティ サポート	211

MAC および MAC-IP シーケンス番号	212
MAC および MAC-IP シーケンス番号の同期	212
ローカル シーケンス番号の更新	212
ホスト移動後のベスト ルートの選択	212
ホスト移動後の古いルートの削除	212
GARP でのホスト移動検知	213
サイレント ホストを使用したホスト移動検出	213
データ パケットを使用した GARP なしのホスト移動検出	213
重複 MAC 検出	213
EVPN IRB の設定	214
EVPN IRB の実行コンフィギュレーション	215
EVPN IRB の確認	216
モビリティを備えた EVPN IPv6 ホスト	227
モビリティを備えた EVPN IPv6 ホストの設定	228
重複 IP アドレス検出	238
重複 IP アドレス検出の設定	239
設定例	239
実行コンフィギュレーション	240
確認	240
EVPN E-Tree	241
EVPN E-Tree の設定	245
設定例	245
実行コンフィギュレーション	247
確認	248
IRB での DHCPv4 リレー	250
IRB での DHCPv4 リレーの設定	256
設定例	256
実行コンフィギュレーション	257
オールアクティブ マルチホーミング対応 DHCPv4 リレー同期	259
IRB での DHCPv6 リレー IAPD	259
IRB での DHCPv6 リレー IAPD の設定	261

	設定例	261
	実行コンフィギュレーション	262
	セッション冗長性を使用したオールアクティブ マルチホーミング対応 DHCPv6 PD 同期	263
	DHCPv6 PD 同期の設定	264
	設定例	264
	実行コンフィギュレーション	265
	DHCPv6 リレーにおける IAPD ルートの配布と取り消し	266
<hr/>		
第 10 章	EVPN 仮想プライベート ワイヤ サービス (VPWS)	267
	EVPN-VPWS シングル ホーム	267
	EVPN-VPWS シングル ホームの設定	268
	実行コンフィギュレーション	269
	EVPN-VPWS マルチホーム	269
	EVPN-VPWS マルチホームの設定	270
	実行コンフィギュレーション	271
<hr/>		
第 11 章	トラフィック エンジニアリング ポリシーのセグメントルーティングを介した L2VPN サービス	273
	SR-TE ポリシーを介した EVPN VPWS 優先パス	274
	SR-TE ポリシーを介した EVPN VPWS 優先パスの設定	275
	ISIS でのプレフィックス SID の設定	275
	ISIS での隣接関係 SID の設定	277
	セグメントリストの設定	279
	SR-TE ポリシーの設定	280
	SR-TE ポリシーを介した EVPN VPWS の設定	281
	実行コンフィギュレーション	282
	SR-TE ポリシーを介した EVPN VPWS 優先パスの確認	286
	関連コマンド	287
	関連項目	287
	SR-TE ポリシーを介した L2VPN VPLS または VPWS 優先パス	287
	SR-TE ポリシーを介した L2VPN VPLS または VPWS 優先パスの設定	288

IS-IS でのプレフィックス SID の設定	289
IS-IS での隣接関係 SID の設定	290
セグメントリストの設定	291
SR-TE ポリシーの設定	293
SR-TE ポリシーを介した VPLS の設定	294
SR-TE ポリシーを介した VPWS の設定	295
実行コンフィギュレーション	295
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	299
関連コマンド	302
関連項目	302
SR-TE を使用した EVPN VPWS オンデマンドネクストホップ	303
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	304
トポロジ	304
ISIS でのプレフィックス SID の設定	304
SR-TE の設定	306
PCE と PCC の設定	307
SR カラーの設定	308
EVPN ルートポリシーの設定	308
BGP の設定	309
EVPN VPWS の設定	309
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	310
実行コンフィギュレーション	311
関連項目	318
セグメントルーティングの概要	318
セグメントルーティングの仕組み	319
セグメントルーティング グローバルブロック	320
<hr/>	
第 12 章	MACsec を使用した BPDU 透過性の設定
	321
	MACsec でのレイヤ 2 コントロールプレーンのトンネリング
	321
	MACsec および MKA の概要
	321
	L2CP トンネリング
	322

MACsec での L2CP トンネリング 322

設定 323

実行コンフィギュレーション 324

確認 325

第 13 章

参照 329

ギガビットイーサネットプロトコル規格 329

キャリアイーサネットモデルの参照 330

ギガビットイーサネットおよび 10 ギガビットイーサネットのデフォルト設定値 331

リンクバンドルの設定に関する参照 333

リンクバンドルの特性 333

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 334

LACP を通じたリンク集約 335



第 1 章

レイヤ 2 VPN のギガビット イーサネット の設定

この章では、レイヤ 2 の機能と標準規格について紹介し、L2VPN 機能の設定方法について説明します。

分散ギガビット イーサネット（10 ギガビットと 100 ギガビットを含む）のアーキテクチャと機能により、ネットワークのスケラビリティとパフォーマンスがもたらされます。同時にサービスプロバイダーは、ルータを POP で他のシステム（コアルータ、エッジルータ、レイヤ 2 スイッチ、レイヤ 3 スイッチなど）と相互接続するように設計された高密度、高帯域幅のネットワークングソリューションを提供できるようになります。

- [レイヤ 2 仮想プライベート ネットワークの概要](#)（1 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 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）](#)（8 ページ）
- [E-LMI メッセージング](#)（9 ページ）
- [E-LMI 動作](#)（10 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](#)（10 ページ）

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。
- ローカルの切り替え - 1 つの AC 上で到達するトラフィックは、疑似接続を介さずに別の AC へ送出されます。



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

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 ルックバック セッションをサポート

しています。フレーム ヘッダーに基づくフィルタを使用してループバック セッションを開始できます。これにより、インターフェイス上で受信されるトラフィックのサブセットのみがループバックされます。送信元 MAC、宛先 MAC、および VLAN 優先順位 (COS ビット) をフィルタとして使用できます。

イーサネット データ プレーン ループバック 設定の制限事項

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

- イーサネット データ プレーン ループバックは、L3 インターフェイス上または L3 サブインターフェイス上ではサポートされていません。
- 次のフィルタはサポートされていません。
 - 外部 VLAN または外部 VLAN の範囲
 - 内部 VLAN または内部 VLAN の範囲
 - イーサネット タイプ
- 外部ループバックでは、次のフィルタの組み合わせのみがサポートされています。
 - 送信元 MAC
 - 送信元 MAC と宛先 MAC
 - 送信元 MAC、宛先 MAC、および VLAN 優先順位
 - 宛先 MAC
 - 宛先 MAC と VLAN 優先順位
- ループバック トラフィックの書き換え変更はサポートされていません。



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

- イーサネット データ プレーン ループバックは、ブロードキャスト MAC アドレスとしての宛先アドレスを持つパケット上ではサポートされていません。
- イーサネット データ プレーン ループバックは、BVI インターフェイス上ではサポートされていません。
- イーサネット データ プレーン ループバックは、Cisco IOS XR リリース 6.3.2 のブリッジドメイン インターフェイスではサポートされていません。
レイヤ 2 VPN ブリッジドメインの内部ループバックはサポートされていません。
- 所定のインスタンスでアクティブにできるイーサネット ループバック セッションは内部または外部のいずれか 1 つのみです。

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

イーサネット データ プレーン ループバックの設定

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

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

設定例

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

/* On physical interface */

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

/* Starting an Ethernet Data Plane Loopback Session */

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

/* On physical sub-interface */

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

/* Starting an Ethernet Data Plane Loopback Session */

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

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

```

/* On physical interface

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

/* Starting an Ethernet Data Plane Loopback Session */

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

/* On physical sub-interface */

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

/* Starting an Ethernet Data Plane Loopback Session */

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

/* Stopping an Ethernet Data Plane Loopback Session */

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

```

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

イーサネットループバックは、SSOの後でも動作します。

実行コンフィギュレーション

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

```

/* External Loopback */

/* On physical interface */

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

/* On physical sub-interface */

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

```

```

/* Internal Loopback */

/* On physical interface */

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

/* On physical sub-interface */

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

```

確認

次に、インターフェイスごとのループバック機能の例を示します。次の出力には、内部ループバックは10ギガビットイーサネット0/0/0/1インターフェイス上で、外部ループバックは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 データプレーン ループバック \(3 ページ\)](#)

関連コマンド

- ethernet loopback
- show ethernet loopback

関連項目

- [イーサネット データプレーン ループバック \(3 ページ\)](#)

関連コマンド

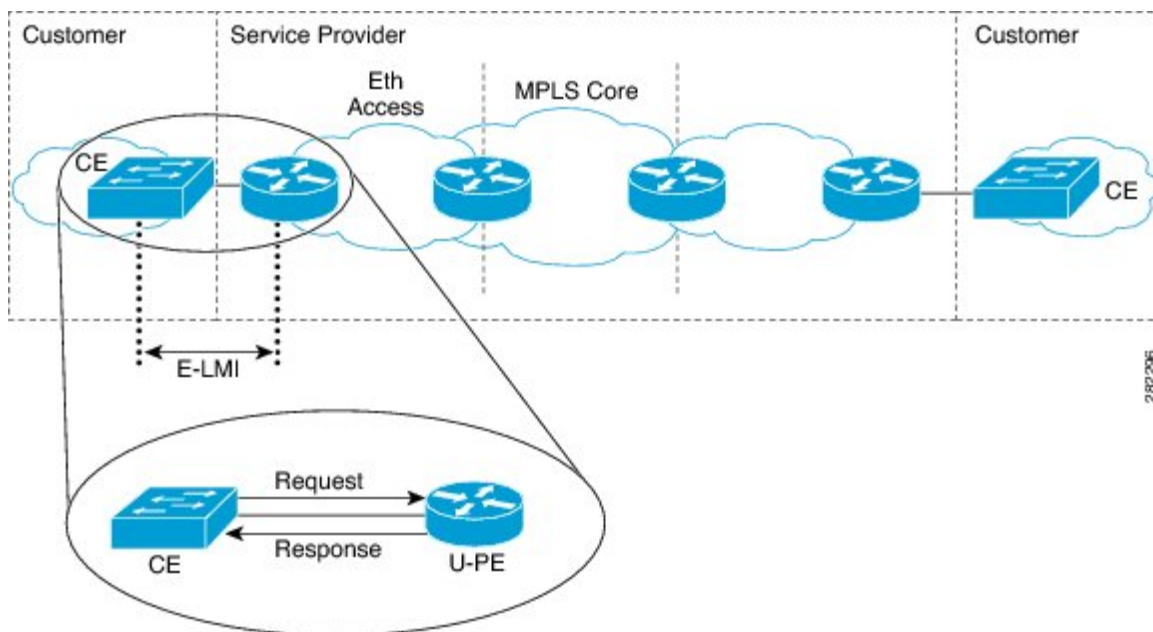
- ethernet loopback
- show ethernet loopback

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 pl
  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
R - Remote Defect received
L - Loop (our MAC received)
C - Config (our ID received)
X - Cross-connect (wrong MAID)
* - Multiple errors received
I - Wrong interval
V - Wrong level
T - Timed out
M - Missing (cross-check)
U - Unexpected (cross-check)
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 \(E-LMI\) \(8 ページ\)](#)
- [E-LMI メッセージング \(9 ページ\)](#)
- [E-LMI メッセージング \(9 ページ\)](#)

関連コマンド

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



第 2 章

レイヤ2アクセスコントロールリストの設定

この章では、レイヤ2アクセスコントロールリストについて紹介し、レイヤ2アクセスコントロールリストの設定方法について説明します。

- [レイヤ2アクセスコントロールリスト \(17 ページ\)](#)
- [レイヤ2アクセスコントロールリスト設定の前提条件 \(18 ページ\)](#)
- [レイヤ2アクセスコントロールリスト機能の特長 \(18 ページ\)](#)
- [レイヤ2アクセスコントロールリストの目的 \(18 ページ\)](#)
- [レイヤ2アクセスコントロールリストの仕組み \(18 ページ\)](#)
- [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 \(19 ページ\)](#)
- [レイヤ2アクセスコントロールリストの作成 \(20 ページ\)](#)
- [レイヤ2アクセスコントロールリスト設定の制約事項 \(20 ページ\)](#)
- [設定 \(20 ページ\)](#)

レイヤ2アクセスコントロールリスト

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

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

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

レイヤ2アクセスコントロールリスト設定の前提条件

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

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

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

レイヤ2アクセスコントロールリスト機能の特長

レイヤ2アクセスコントロールリストには次の機能上の特長があります。

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

レイヤ2アクセスコントロールリストの目的

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

レイヤ2アクセスコントロールリストの仕組み

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

アクセスリストを設定して名前を付けることは可能ですが、アクセスリストを受け取るコマンドによってアクセスリストが参照されるまで、有効にはなりません。複数のコマンドから同

じアクセス リストを参照できます。アクセス リストはルータに着信するレイヤ2トラフィックを制御できますが、ルータを起点とするトラフィックやルータを離れるトラフィックは制御できません。

レイヤ2アクセスコントロール リストのプロセスとルール

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

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

- アクセスリストは、**ethernet-services access-group** コマンドを使用する前に存在している必要があります。

レイヤ2アクセスコントロールリストの作成

レイヤ2アクセスコントロールリストを作成するときは以下を考慮します。

- アクセスリストは、インターフェイスに適用する前に作成します。
- より具体的な参照が、より一般的な参照よりも前に出現するように、アクセスリストを構成します。

レイヤ2アクセスコントロールリスト設定の制約事項

次の制約事項は、レイヤ2アクセスコントロールリストの設定に適用されます。

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

設定

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

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

実行コンフィギュレーション

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

確認

レイヤ2アクセスコントロールリストが設定されていることを確認します。

```
/* Verify the Layer 2 access control lists configuration */  
Router# show access-lists ethernet-services es_acl_1 hardware ingress location 0/0/CPU0  
  
Fri Oct 21 09:39:52.904 UTC  
ethernet-services access-list es_acl_1  
10 deny 00ff.eedd.0000 ff00.0000.00ff 0000.0100.0000 0000.0000.ffff (2051 matches)  
20 permit host 000a.000b.000c host 00aa.ab99.1122 cos 1 dei  
30 deny host 000a.000b.000c host 00aa.dc11.ba99 cos 7 dei (2050 matches)
```




第 3 章

レイヤ 2 VPN の仮想 LAN の設定

レイヤ 2 バーチャルプライベートネットワーク (L2VPN) 機能を利用すると、サービスプロバイダー (SP) は、地理的に離れたカスタマー サイトにレイヤ 2 サービスを提供できるようになります。

仮想ローカルエリア ネットワーク (VLAN) とは、実際は異なる LAN セグメント上のデバイスでも、同じセグメントで接続している場合と同様に通信できるように設定された、1 つまたは複数の LAN 上にあるデバイスのグループです。IEEE の 802.1Q 仕様は、イーサネットフレームに VLAN メンバーシップ情報を挿入する標準方式を確立します。

VLAN は、ユーザとホストの管理、帯域幅の割り当て、およびリソースの最適化に非常に役立ちます。VLAN の使用は、大規模なネットワークを小規模なパーツに分けるという問題に対処するもので、ブロードキャストおよびマルチキャストのトラフィックが必要以上の帯域を消費しないようになります。また、VLAN によって内部ネットワークのセグメント間におけるセキュリティのレベルを強化できます。

802.1Q 仕様は、イーサネット フレームに VLAN メンバーシップ情報を挿入する標準方式を確立します。Cisco IOS XR ソフトウェアは、ギガビットイーサネットおよび 10 ギガビットイーサネット インターフェイスでの VLAN サブインターフェイスの設定をサポートしています。

VLAN 接続回線 (AC) を設定するための設定モデルは、基本の VLAN の設定に使用するモデルに類似しています。ユーザはまず VLAN サブインターフェイスを作成し、次にサブインターフェイス コンフィギュレーション モードで VLAN を設定します。接続回路を作成するには、**interface** コマンド文字列に **l2transport** キーワードを含めて、そのインターフェイスが L2 インターフェイスであることを指定する必要があります。

VLAN AC は、次の L2VPN 動作モードをサポートしています。

- 基本の Dot1Q 接続回線：この接続回線は、特定の VLAN タグで送受信されるすべてのフレームに対応します。
- QinQ 接続回線：この接続回線は、特定の外部 VLAN タグおよび特定の内部 VLAN タグで送受信されるすべてのフレームに対応します。QinQ は、2 つのタグのスタックを使用する Dot1Q の拡張です。

CE-to-PE リンクの各 VLAN は、(VC タイプ 4 または VC タイプ 5 を使用する) 独立した L2VPN 接続として設定できます。

制約事項と制限

レイヤ 2 VPN の VLAN を設定する場合、次の制限事項が適用されます。

- ポイントツーポイント接続では、2つの接続回線を同じタイプにするべきではありません。たとえば、ポート モードのイーサネット接続回線は Dot1Q イーサネット接続回線に接続できます。
- 疑似回線は、VLAN モードまたはポート モードで実行できます。VLAN モードで実行される疑似回線は、常に Dot1Q または Dot1ad タグを伝送しますが、ポートモードで実行される疑似回線はタグを伝送する場合もあれば伝送しない場合もあります。これらの異なるタイプの回線を接続するには、タグのポップ、プッシュ、およびリライトが必要です。
- MPLS 疑似回線の両側にある接続回線は異なるタイプでもかまいません。この場合、接続回線の一方または両方のエンドで、疑似回線を行うための適切な変換が行われます。
- [VLAN サブインターフェイスの設定 \(24 ページ\)](#)
- [イーサネット フロー ポイントの概要 \(26 ページ\)](#)
- [VLAN ヘッダー書き換えの設定 \(29 ページ\)](#)

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す。これには、802.1Q VLAN タグに許可されている追加の 4 バイトも含まれます。

次のモードの VLAN サブインターフェイスの設定がサポートされています。

- 基本の dot1q 接続回線
- Q-in-Q 接続回線

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

encapsulation dot1q vlan-id

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

encapsulation dot1ad vlan-id

Q-in-Q 接続回線を設定するには、次のカプセル化モードを使用します。

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

制約事項と制限

VLAN サブインターフェイスを設定する場合、次の制限事項が適用されます。

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

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

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

- 0x9100/0x9200 がトンネリング イーサタイプとして設定されている場合、dot1ad (0x88a8) カプセル化はサポートされません。
- いずれかのサブインターフェイスがメインインターフェイス配下ですでに設定されている場合、トンネリング イーサタイプの変更はサポートされません。

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

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

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

EFPの利点には次のものがあります。

- 特定のインターフェイスで特定のフローに属するすべてのフレームの識別
- VLANヘッダー書き換えの実行
([VLANヘッダー書き換えの設定 \(29ページ\)](#) を参照)
- 識別されたフレームへの機能の追加。
- オプションで、データパスでのフレームの転送方法の定義。

EFPの制限

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

EFP のフレームの識別

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

これを介して、フレームと EFP を照合することはできません。

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

VLAN タグの識別

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

カプセル化タイプ	EFP 識別子
単一タグ付きフレーム	802.1Q カスタマー タグ付きイーサネット フレーム
二重タグ付きフレーム 二重タグ付きフレームは、次のいずれかのタイプになります。 <ul style="list-style-type: none"> • 単一範囲 • Range-in-Q • Q-in-Range 	<ul style="list-style-type: none"> • 単一範囲では、EFP に対して VLAN ID の範囲を追加できます。 • Range-in-Q では、外部 VLAN ID の範囲に単一の内部 VLAN ID を持たせることができます。 • Q-in-Range では、単一の外部 VLAN ID に内部 VLAN ID の範囲を持たせることができます。

特定の EFP にマップされるフレームを定義する際にワイルドカードを使用できます。EFP は、単一の VLAN タグ、VLAN タグのスタック、または両方の組み合わせ（VLAN スタックとワイルドカード）に基づいてフローを区別できます。EFP は、EFP モデル、カプセル化非依存にする柔軟性を提供しています。また、新しいタグ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、または別にすることができます。
- トンネル型サービス (xconnect) : EFP はレイヤ 3 トンネルにマッピングされます。これは、EoMPLS などのポイントツーポイントを対象としています。

VLAN ヘッダー書き換えの設定

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

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



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

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

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

- [有効な入力書き換えアクション \(30 ページ\)](#)
- [有効な入力と出力の書き換えの組み合わせ \(30 ページ\)](#)

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 4 章

L2CP トンネリング MEF

この章では、ローカル（カスタマーエッジ）CE デバイスからリモート CE デバイスへの制御パケットの開始に役立つ L2 制御プロトコル（L2CP）トンネリングについて説明します。

- [L2CP トンネリング（31 ページ）](#)
- [L2CP トンネリングの設定（32 ページ）](#)

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спорт メイン
- VPWS I2 サブ インターフェイス
- L2 トランспорт 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。

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ルータにインストールしておく必要があります。

L2CP トンネリングの制限事項

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

L2CP トンネリングの設定

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

プロトコル	パケットタイプ	アクション
LLDP	タグ付き	トンネル化
STP	タグ付き	トンネル化
VTP	タグ付き	トンネル化
BPDU	タグ付き	トンネル化
OAM	タグ付き	トンネル化
ELMI	タグ付き	トンネル化

L2CP トンネリングを設定するには、次のステップを実行します。

```

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

RP/0/RP0/CPU0:ios(config)#l2vpn
RP/0/RP0/CPU0:ios(config-l2vpn)#xconnect group g1
RP/0/RP0/CPU0:ios(config-l2vpn-xc)#p2p 1
RP/0/RP0/CPU0:ios(config-l2vpn-xc-p2p)#int tenGigE 0/1/0/8/3.1
RP/0/RP0/CPU0:ios(config-l2vpn-xc-p2p)#neighbor 12.12.12.1 pw-id 1
RP/0/RP0/CPU0:ios(config-l2vpn-xc-p2p-pw)#commit
Fri Sep 1 17:11:19.516 UTC

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

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

/* 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 $1$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

/ * 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          Segment 1          Segment 2
Group             Name              ST   Description      ST   Description      ST
-----
1                 1                 UP   Te0/1/0/8/3     UP   12.12.12.1      1   UP
-----
RP/0/RP0/CPU0:ios#

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

```

Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect Group	Name	ST	Segment 1 Description	ST	Segment 2 Description		ST
1	1	UP	Te0/1/0/8/3	UP	12.12.12.1	1	UP

RP/0/RP0/CPU0:ios#



第 5 章

レイヤ 2 VPN のリンクバンドルの設定

イーサネットリンクバンドルは、1つ以上のポートを集約したグループで、単一のリンクとして扱われます。各バンドルには、1つの MAC、1つの IP アドレス、1つの設定セット（ACL または Quality of Service など）があります。

リンクバンドリングの利点は次のとおりです。

- 冗長性：バンドルには複数のリンクがあるため、1つのリンクに障害が発生しても、接続は失われません。
- 帯域幅の増加：バンドルインターフェイスでは、個々のポート容量を集約しているバンドルの使用可能なすべてのメンバーを介してトラフィックが転送されます。

バンドルを構成するインターフェイスのタイプに応じて、サポートされる2つのタイプのリンクバンドリングがあります。

- イーサネットインターフェイス
- VLAN インターフェイス（バンドルサブインターフェイス）

この項では、レイヤ 2 VPN で使用するイーサネットと VLAN リンクバンドルの設定について説明します。

- [ギガビットイーサネットリンクバンドルの設定（43 ページ）](#)
- [VLAN バンドルの設定（46 ページ）](#)
- [リンクバンドルの設定に関する参照（48 ページ）](#)

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。

制約事項

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

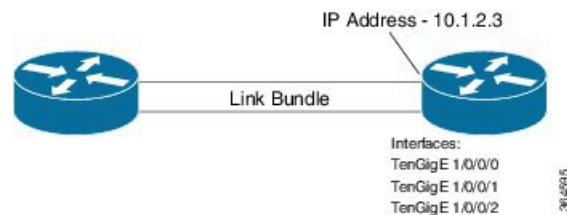
設定例

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

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

次の図に値の例を示します。

図 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)# 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

```

```
Tel1/0/0/1      Local      Active      0x8000, 0x0000  10000000
  Link is Active
Tel1/0/0/2      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

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。

- グローバルに一意のローカルシステム 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。



第 6 章

マルチポイント レイヤ 2 サービスの設定

このモジュールでは、マルチポイントレイヤ2ブリッジングサービス（バーチャルプライベート LAN サービス（VPLS）とも呼ばれます）の概念および設定情報を示します。



(注) VPLS は、レイヤ 2 VPN テクノロジーをサポートし、カスタマーにトランスペアレントなマルチポイントレイヤ 2 接続を提供します。このアプローチにより、サービスプロバイダーはブロードキャスト TV やレイヤ 2 VPN といった数多くの新しいサービスをホストすることができます。

- [マルチポイントレイヤ 2 サービス実装の前提条件](#) (51 ページ)
- [マルチポイントレイヤ 2 サービスの実装に関する情報](#) (51 ページ)
- [マルチポイントレイヤ 2 サービスの実装方法](#) (57 ページ)
- [マルチポイントレイヤ 2 サービスの設定例](#) (80 ページ)

マルチポイント レイヤ 2 サービス実装の前提条件

マルチポイント レイヤ 2 サービスの実装に関する情報

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

マルチポイント レイヤ 2 サービスの概要

マルチポイントレイヤ 2 サービスを使用すると、地理的に離れたローカルエリアネットワーク（LAN）セグメントを MPLS ネットワーク経由で単一ブリッジドメインとして相互接続できます。MAC アドレスラーニング、エイジング、およびスイッチングなどの従来の LAN の機能はすべて、単一のブリッジドメインに属する、リモート接続されたすべての LAN セグメント全体でエミュレートされます。サービスプロバイダーは、カスタマーごとに別のブリッジドメインを定義することで、MPLS ネットワーク上で複数のカスタマーに VPLS サービスを提

供できます。あるブリッジドメインからのパケットが別のブリッジドメインには伝送または配信されることはないため、LANサービスのプライバシーが確保されます。

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



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

ブリッジドメイン

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

疑似回線

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

アクセス疑似回線はVPLSブリッジドメイン経由ではサポートされない

アクセス疑似回線は、VPLSブリッジドメインではサポートされていません。VFI配下で設定されるコア疑似回線のみがサポートされています。

設定例

```
l2vpn
  bridge group bg1
    bridge-domain l2vpn
      interface TenGigE0/0/0/13.100
      !
    vfi 1
      neighbor 192.0.2.1 pw-id 12345
      pw-class mpls_csr
      !
      !
      !
```

仮想転送インスタンス

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

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

MPLS ベースのプロバイダー コアの VPLS

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

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

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

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

レイヤ2スイッチングのVPLS



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

次の機能がサポートされています。

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

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

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

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

```
router bgp 1
  address-family l2vpn vpls
    neighbor 5.5.5.2 activate
    neighbor 5.5.5.2 prefix-length-size 2 -----> NLRI length = 2 bytes
  exit-address-family
```

MAC アドレス関連パラメータ

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

次のトピックでは、MAC アドレス関連パラメータについて説明します。

MAC アドレス フラッディング

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

MAC アドレスベース転送

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

MAC アドレスの送信元ベースの学習

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

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



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

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

MAC アドレス エージング

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

ブリッジは、ブリッジテーブルに基づいてパケットの転送、フラッディング、ドロップを行います。ブリッジテーブルは、スタティック エントリとダイナミック エントリの両方を保持します。スタティック エントリは、ネットワーク マネージャまたはブリッジ自体によって入力

されます。ダイナミックエントリはブリッジ学習プロセスによって入力されます。ダイナミックエントリは、エントリが作成された時点か最後に更新された時点から、「エージングタイム」と呼ばれる指定された期間が経過すると、自動的に削除されます。

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

MAC アドレス制限

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

制限を超えると、これらの通知を行うようシステムが設定されています。

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

MAC アドレス取り消し

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

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



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

LDP MAC 取り消し機能は、次のイベントが原因で生成されます。

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

マルチポイントレイヤ2サービスの実装方法

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

ブリッジドメインの設定

次のトピックでは、ブリッジドメインの設定方法について説明します。

ブリッジドメインの作成

ブリッジドメインを作成するには、次の作業を実行します。

手順

ステップ1 **configure**

例：

```
RP/0/RP0/CPU0:router# configure
```

XR コンフィギュレーションモードを開始します。

ステップ2 **l2vpn**

例：

```
RP/0/RP0/CPU0:router(config)# l2vpn  
RP/0/RP0/CPU0:router(config-l2vpn)#
```

L2VPN コンフィギュレーションモードを開始します。

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group csco  
RP/0/RP0/CPU0:router(config-l2vpn-bg)#
```

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

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain abc  
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)#
```

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

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

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

end : 次のいずれかのアクションを実行することをユーザに要求します。

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

メンバのブリッジドメインへの関連付け

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

- イーサネットおよび VLAN
- VFI



(注) BVI は、VFI を使用して設定されたブリッジドメインではサポートされません。

手順

ステップ 1 configure

例 :

```
RP/0/RP0/CPU0:router# configure
```

XR コンフィギュレーション モードを開始します。

ステップ 2 l2vpn

例 :

```
RP/0/RP0/CPU0:router(config)# l2vpn
```

L2VPN コンフィギュレーション モードを開始します。

ステップ 3 bridge group *bridge group name*

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group cisco
```



```
RP/0/RP0/CPU0:router(config-l2vpn-bg)#
```

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

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

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)#
```

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

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

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# interface GigabitEthernet 0/4/0/0
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-ac)#
```

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

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

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-ac)# static-mac-address 1.1.1
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-ac)# exit
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)#
```

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

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

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

end : 次のいずれかのアクションを実行することをユーザに要求します。

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

ブリッジドメインパラメータの設定

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

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

手順

ステップ 1 **configure**

例 :

```
RP/0/RP0/CPU0:router# configure
```

XR コンフィギュレーション モードを開始します。

ステップ 2 **l2vpn**

例 :

```
RP/0/RP0/CPU0:router(config)# l2vpn  
RP/0/RP0/CPU0:router(config-l2vpn)#
```

l2vpn コンフィギュレーション モードを開始します。

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

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group cisco  
RP/0/RP0/CPU0:router(config-l2vpn-bg)#
```

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

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

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain abc  
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)#
```

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

ステップ 5 **flooding disable**

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# flooding disable
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)#
```

フラッディングを無効にします。

ステップ6 mtu bytes

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# mtu 1000
```

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

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

ステップ7 commit コマンドまたは end コマンドを使用します。

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

end：次のいずれかのアクションを実行することをユーザに要求します。

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

ブリッジドメインのディセーブル化

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

手順

ステップ1 configure

例：

```
RP/0/RP0/CPU0:router# configure
```

XR コンフィギュレーションモードを開始します。

ステップ2 l2vpn

例：

```
RP/0/RP0/CPU0:router(config)# l2vpn
RP/0/RP0/CPU0:router(config-l2vpn)#
```

L2VPN コンフィギュレーション モードを開始します。

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group cisco
RP/0/RP0/CPU0:router(config-l2vpn-bg)#
```

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

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)#
```

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

ステップ5 **shutdown**

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)#
```

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

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

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

end：次のいずれかのアクションを実行することをユーザに要求します。

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

レイヤ2仮想転送インスタンスの設定

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

仮想転送インスタンスの作成

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

手順

ステップ1 **configure**

例：

```
RP/0/RP0/CPU0:router# configure
```

XR コンフィギュレーション モードを開始します。

ステップ2 **l2vpn**

例：

```
RP/0/RP0/CPU0:router(config)# l2vpn  
RP/0/RP0/CPU0:router(config-l2vpn)#
```

L2VPN コンフィギュレーション モードを開始します。

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group cisco  
RP/0/RP0/CPU0:router(config-l2vpn-bg)#
```

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

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain abc  
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)#
```

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

ステップ5 **vfi {*vfi-name*}**

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# vfi v1  
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi)#
```

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

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

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

end : 次のいずれかのアクションを実行することをユーザに要求します。

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

疑似回線の仮想転送インスタンスへの関連付け

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

手順

ステップ 1 **configure**

例 :

```
RP/0/RP0/CPU0:router# configure
```

XR コンフィギュレーション モードを開始します。

ステップ 2 **l2vpn**

例 :

```
RP/0/RP0/CPU0:router(config)# l2vpn
RP/0/RP0/CPU0:router(config-l2vpn)#
```

L2VPN コンフィギュレーション モードを開始します。

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

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group cisco
RP/0/RP0/CPU0:router(config-l2vpn-bg)#
```

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

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

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)#
```

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

ステップ5 `vfi { vfi name }`

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# vfi v1
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi)#
```

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

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi-pw)#
```

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

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

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

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

end : 次のいずれかのアクションを実行することをユーザに要求します。

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

ブリッジドメインへの仮想転送インスタンスの関連付け

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

手順

ステップ1 `configure`

例：

```
RP/0/RP0/CPU0:router# configure
```

XR コンフィギュレーション モードを開始します。

ステップ2 l2vpn

例：

```
RP/0/RP0/CPU0:router(config)# l2vpn
RP/0/RP0/CPU0:router(config-l2vpn)#
```

L2VPN コンフィギュレーション モードを開始します。

ステップ3 bridge group *bridge group name*

例：

```
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group cisco
RP/0/RP0/CPU0:router(config-l2vpn-bg)#
```

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

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)#
```

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

ステップ5 vfi { *vfi name* }

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# vfi v1
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi)#
```

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

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi-pw)#
```

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

- 相互接続ピアの IP アドレスを指定するには、*A.B.C.D* 引数を使用します。

- 疑似回線 ID および ID 値を設定するには、**pw-id** キーワードを使用します。指定できる範囲は 1 ~ 4294967295 です。

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi-pw)# static-mac-address 1.1.1
```

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

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

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

end : 次のいずれかのアクションを実行することをユーザに要求します。

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

疑似回線への疑似回線クラスの接続

疑似回線に疑似回線クラスを接続するには、次の作業を実行します。

手順

ステップ1 **configure**

例：

```
RP/0/RP0/CPU0:router# configure
```

XR コンフィギュレーションモードを開始します。

ステップ2 **l2vpn**

例：

```
RP/0/RP0/CPU0:router(config)# l2vpn  
RP/0/RP0/CPU0:router(config-l2vpn)#
```

L2VPN コンフィギュレーションモードを開始します。

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group cisco
```

```
RP/0/RP0/CPU0:router(config-l2vpn-bg)#
```

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

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)#
```

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

ステップ5 **vfi** { *vfi-name* }

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# vfi v1
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi)#
```

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

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi-pw)#
```

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

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

ステップ7 **pw-class** { *class-name* }

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi-pw)# pw-class canada
```

疑似回線に使用する疑似回線クラス テンプレート名を設定します。

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

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

end : 次のいずれかのアクションを実行することをユーザに要求します。

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

スタティック ラベルを使用した疑似回線の設定

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

手順

ステップ1 **configure**

例 :

```
RP/0/RP0/CPU0:router# configure
```

XR コンフィギュレーションモードを開始します。

ステップ2 **l2vpn**

例 :

```
RP/0/RP0/CPU0:router(config)# l2vpn  
RP/0/RP0/CPU0:router(config-l2vpn)#
```

L2VPN コンフィギュレーションモードを開始します。

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

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group cisco  
RP/0/RP0/CPU0:router(config-l2vpn-bg)#
```

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

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

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain abc  
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)#
```

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

ステップ5 vfi { vfi-name }

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# vfi v1
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi)#
```

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

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi)# neighbor 10.1.1.2 pw-id 1000
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi-pw)#
```

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

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

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi-pw)# mpls static label local 800 remote 500
```

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

ステップ8 commit コマンドまたは end コマンドを使用します。

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

end：次のいずれかのアクションを実行することをユーザに要求します。

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

仮想転送インスタンスのディセーブル化

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

手順

ステップ 1 configure

例 :

```
RP/0/RP0/CPU0:router# configure
```

XR コンフィギュレーション モードを開始します。

ステップ 2 l2vpn

例 :

```
RP/0/RP0/CPU0:router(config)# l2vpn
```

```
RP/0/RP0/CPU0:router(config-l2vpn)#
```

L2VPN コンフィギュレーション モードを開始します。

ステップ 3 bridge group *bridge group name*

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group cisco
```

```
RP/0/RP0/CPU0:router(config-l2vpn-bg)#
```

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

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

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain abc
```

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)#
```

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

ステップ 5 vfi { *vfi-name* }

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# vfi v1
```

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi)#
```

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

ステップ 6 shutdown

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-vfi)# shutdown
```

仮想転送インターフェイス（VFI）をディセーブルにします。

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

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

end : 次のいずれかのアクションを実行することをユーザに要求します。

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

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

例 :

```
RP/0/RP0/CPU0:router# show l2vpn bridge-domain detail
```

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

MAC アドレス関連パラメータの設定

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

MAC テーブル属性は、ブリッジドメインについて設定されます。



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

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

MAC アドレスの送信元ベースの学習の設定

MAC アドレスの送信元ベースの学習を設定するには、次の作業を実行します。

手順

ステップ 1 configure

例 :

```
RP/0/RP0/CPU0:router# configure
```

XR コンフィギュレーション モードを開始します。

ステップ 2 l2vpn

例 :

```
RP/0/RP0/CPU0:router(config)# l2vpn
RP/0/RP0/CPU0:router(config-l2vpn)#
```

L2VPN コンフィギュレーション モードを開始します。

ステップ 3 bridge group *bridge group name*

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group cisco
RP/0/RP0/CPU0:router(config-l2vpn-bg)#
```

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

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

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)#
```

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

ステップ 5 mac

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac)#
```

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

ステップ 6 learning disable

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac)# learning disable
```

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

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

end : 次のいずれかのアクションを実行することをユーザに要求します。

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

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

例 :

```
RP/0/RP0/CPU0:router# show l2vpn bridge-domain detail
```

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

MAC アドレス制限の設定

MAC アドレス制限のパラメータを設定するには、次の作業を実行します。

手順

ステップ1 **configure**

例 :

```
RP/0/RP0/CPU0:router# configure
```

XR コンフィギュレーションモードを開始します。

ステップ2 **l2vpn**

例 :

```
RP/0/RP0/CPU0:router(config)# l2vpn
RP/0/RP0/CPU0:router(config-l2vpn)#
```

L2VPN コンフィギュレーションモードを開始します。

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

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group cisco
```



```
RP/0/RP0/CPU0:router(config-l2vpn-bg)#
```

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

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

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain abc
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)#
```

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

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

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# interface gigabitEthernet 0/2/0/1
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-ac)#
```

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

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

ステップ 6 **mac**

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# mac
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac)#
```

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

ステップ 7 **limit**

例 :

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac)# limit
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac-limit)#
```

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

ステップ 8 **maximum { value }**

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac-limit)# maximum 5000
```

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

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac-limit)# action flood
```

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

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac-limit)# notification both
```

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

ステップ 11 **mac limit threshold 80**

例：

```
RP/0/RP0/CPU0:router(config-l2vpn)# mac limit threshold 80
```

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

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

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

end : 次のいずれかのアクションを実行することをユーザに要求します。

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

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

例：

```
RP/0/RP0/CPU0:router# show l2vpn bridge-domain detail
```

MAC アドレス制限の詳細が表示されます。

MAC アドレス エージングの設定

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

手順

ステップ 1 **configure**

例：

```
RP/0/RP0/CPU0:router# configure
```

XR コンフィギュレーション モードを開始します。

ステップ 2 **l2vpn**

例：

```
RP/0/RP0/CPU0:router(config)# l2vpn  
RP/0/RP0/CPU0:router(config-l2vpn)#
```

L2VPN コンフィギュレーション モードを開始します。

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group cisco  
RP/0/RP0/CPU0:router(config-l2vpn-bg)#
```

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

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain abc  
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)#
```

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

ステップ 5 **mac**

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# mac
```

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac)#
```

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

ステップ6 aging

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac)# aging
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac-aging)#
```

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

ステップ7 time { seconds }

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac-aging)# time 300
```

最大エージングタイムを設定します。

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

ステップ8 commit コマンドまたは end コマンドを使用します。

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

end：次のいずれかのアクションを実行することをユーザに要求します。

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

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

例：

```
RP/0/RP0/CPU0:router# show l2vpn bridge-domain detail
```

エージングフィールドに関する詳細を表示します。

ブリッジポートレベルでのMACフラッシュのディセーブル化

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

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

手順

ステップ1 **configure**

例：

```
RP/0/RP0/CPU0:router# configure
```

XR コンフィギュレーションモードを開始します。

ステップ2 **l2vpn**

例：

```
RP/0/RP0/CPU0:router(config)# l2vpn
```

```
RP/0/RP0/CPU0:router(config-l2vpn)#
```

L2VPN コンフィギュレーションモードを開始します。

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn)# bridge group cisco
```

```
RP/0/RP0/CPU0:router(config-l2vpn-bg)#
```

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

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

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg)# bridge-domain abc
```

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)#
```

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

ステップ5 **mac**

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd)# mac
```

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac)#
```

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

ステップ6 **port-down flush disable**

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-bg-bd-mac)#
port-down flush disable
```

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

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

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

end : 次のいずれかのアクションを実行することをユーザに要求します。

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

マルチポイントレイヤ2サービスの設定例

ここで示す設定例は、次のとおりです。

プロバイダーエッジ間のマルチポイントレイヤ2サービスの設定 : 例

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

この設定は、PE 1 を設定する例を示しています。

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

この設定は、PE 2 を設定する例を示しています。

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

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

この設定は、PE 3 を設定する例を示しています。

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

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

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

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

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

MAC アドレス取り消しフィールドの表示：例

この出力は、MAC アドレス取り消しフィールドの例を示しています。

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

Legend: pp = Partially Programmed.
Bridge group: 222, bridge-domain: 222, id: 0, state: up, ShgId: 0, MSTi: 0
Coupled state: disabled
MAC learning: enabled
MAC withdraw: enabled
  MAC withdraw sent on: bridge port up
  MAC withdraw relaying (access to access): disabled
Flooding:
  Broadcast & Multicast: enabled
  Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
MAC port down flush: enabled
MAC Secure: disabled, Logging: disabled
Split Horizon Group: none
Dynamic ARP Inspection: disabled, Logging: disabled
IP Source Guard: disabled, Logging: disabled
DHCPv4 snooping: disabled
IGMP Snooping: enabled
IGMP Snooping profile: none
MLD Snooping profile: none
```

MAC アドレス取り消しフィールドの表示 : 例

```

Storm Control: disabled
Bridge MTU: 1500
MIB cvplsConfigIndex: 1
Filter MAC addresses:
P2MP PW: disabled
Create time: 01/03/2017 11:01:11 (00:21:33 ago)
No status change since creation
ACs: 1 (1 up), VFIs: 1, PWs: 1 (1 up), PBBs: 0 (0 up)
List of ACs:
  AC: TenGigE0/2/0/1.7, state is up
    Type VLAN; Num Ranges: 1
    Outer Tag: 21
    VLAN ranges: [22, 22]
    MTU 1508; XC ID 0x208000b; interworking none
    MAC learning: enabled
    Flooding:
      Broadcast & Multicast: enabled
      Unknown unicast: enabled
    MAC aging time: 300 s, Type: inactivity
    MAC limit: 4000, Action: none, Notification: syslog
    MAC limit reached: no
    MAC port down flush: enabled
    MAC Secure: disabled, Logging: disabled
    Split Horizon Group: none
    Dynamic ARP Inspection: disabled, Logging: disabled
    IP Source Guard: disabled, Logging: disabled
    DHCPv4 snooping: disabled
    IGMP Snooping: enabled
    IGMP Snooping profile: none
    MLD Snooping profile: none
    Storm Control: bridge-domain policer
    Static MAC addresses:
    Statistics:
      packets: received 714472608 (multicast 0, broadcast 0, unknown unicast 0, unicast
0), sent 97708776
      bytes: received 88594603392 (multicast 0, broadcast 0, unknown unicast 0, unicast
0), sent 12115888224
      MAC move: 0
    Storm control drop counters:
      packets: broadcast 0, multicast 0, unknown unicast 0
      bytes: broadcast 0, multicast 0, unknown unicast 0
    Dynamic ARP inspection drop counters:
      packets: 0, bytes: 0
    IP source guard drop counters:
      packets: 0, bytes: 0
List of VFIs:
  VFI 222 (up)
    PW: neighbor 1.1.1.1, PW ID 222, state is up ( established )
      PW class not set, XC ID 0xc000000a
      Encapsulation MPLS, protocol LDP
      Source address 21.21.21.21
      PW type Ethernet, control word disabled, interworking none
      Sequencing not set

PW Status TLV in use
  MPLS          Local                               Remote
  -----
  Label         24017                                           24010
  Group ID      0x0                                             0x0
  Interface     222                                             222
  MTU           1500                                           1500
  Control word  disabled                                       disabled
  PW type       Ethernet                                       Ethernet
  VCCV CV type  0x2                                             0x2

```



```

(LSP ping verification)                (LSP ping verification)
VCCV CC type 0x6                        0x6
(router alert label)                    (router alert label)
(TTL expiry)                            (TTL expiry)
-----
Incoming Status (PW Status TLV):
  Status code: 0x0 (Up) in Notification message
MIB cpwVcIndex: 3221225482
Create time: 01/03/2017 11:01:11 (00:21:33 ago)
Last time status changed: 01/03/2017 11:21:01 (00:01:43 ago)
Last time PW went down: 01/03/2017 11:15:21 (00:07:23 ago)
MAC withdraw messages: sent 0, received 0
Forward-class: 0
Static MAC addresses:
Statistics:
  packets: received 95320440 (unicast 0), sent 425092569
  bytes: received 11819734560 (unicast 0), sent 52711478556
  MAC move: 0
Storm control drop counters:
  packets: broadcast 0, multicast 0, unknown unicast 0
  bytes: broadcast 0, multicast 0, unknown unicast 0
DHCPv4 snooping: disabled
IGMP Snooping profile: none
MLD Snooping profile: none
VFI Statistics:
  drops: illegal VLAN 0, illegal length 0

```

IOS XR トランク インターフェイスでのブリッジング : 例

次に、を単純な L2 スイッチとして設定する例を示します。

特記事項 :

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

- 次の例では、実行コンフィギュレーションが空であり、すべてのコンポーネントが作成されていると想定します。
- この例では、インターフェイス間のスイッチングを実行するようにを設定するために必要なすべての手順を示しています。ただし、`no shut`、`negotiation auto` などのインターフェイスを準備するためのコマンドは除外されています。
- ブリッジドメインは、作成直後に `no shut` 状態になります。
- この例ではトランク (つまりメイン) インターフェイスだけが使用されます。
- トランク インターフェイスは、タグ付き (IEEE 802.1Q) またはタグなし (つまり VLAN ヘッダーなし) フレームを処理できます。
- ブリッジドメインは、MAC アドレスに基づいて学習、フラッディング、および転送を行います。この機能は、タグの設定に関係なくフレームで動作します。
- ブリッジドメインエンティティはシステム全体にわたります。単一の LC にすべてのブリッジドメイン AC を配置する必要はありません。これは、ブリッジドメインの設定に適用されます。

- ルータが予期したとおりに設定されていること、およびコマンドによあって新しい設定ステータスが表示されることを確認するには、`show bundle` および `show l2vpn bridge-domain` コマンドを使用します。
- 次の例の AC では、管理ダウン状態になっているインターフェイスを使用します。

設定例

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

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

Port	Device	State	Port ID	B/W, kbps
Gi0/2/0/5	Local	Configured	0x8000, 0x0001	1000000
Link is down				
Gi0/2/0/6	Local	Configured	0x8000, 0x0002	1000000
Link is down				

```
RP/0/RSP0/CPU0:router#
RP/0/RSP0/CPU0:router#show l2vpn bridge-domain group examples
Bridge group: examples, bridge-domain: test-switch, id: 2000, state: up, ShgId: 0, MSTi:
```

```

0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 4 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up)
List of ACs:
  BE10, state: down, Static MAC addresses: 0
  Gi0/2/0/0, state: up, Static MAC addresses: 0
  Gi0/2/0/1, state: down, Static MAC addresses: 0
  Te0/5/0/1, state: down, Static MAC addresses: 0
List of VFIs:
RP/0/RSP0/CPU0:router#

```

次の表に、設定手順（アクション）およびこの例の対応する目的を示します。

手順

-
- ステップ 1 configure**
グローバル コンフィギュレーション モードを開始します。
- ステップ 2 interface Bundle-ether10**
新しいバンドル トランク インターフェイスを作成します。
- ステップ 3 l2transport**
Bundle-ether10 を L3 インターフェイスから L2 インターフェイスに変更します。
- ステップ 4 interface GigabitEthernet0/2/0/5**
インターフェイス設定モードを開始します。GigabitEthernet0/2/0/5 で機能するようコンフィギュレーション モードを変更します。
- ステップ 5 bundle id 10 mode active**
GigabitEthernet0/2/0/5 を Bundle-ether10 のメンバーとして設定します。**mode active** キーワードは、LACP プロトコルを指定します。
- ステップ 6 interface GigabitEthernet0/2/0/6**
インターフェイス設定モードを開始します。GigabitEthernet0/2/0/6 で機能するようコンフィギュレーション モードを変更します。
- ステップ 7 bundle id 10 mode active**
GigabitEthernet0/2/0/6 を Bundle-ether10 のメンバーとして設定します。**mode active** キーワードは、LACP プロトコルを指定します。
- ステップ 8 interface GigabitEthernet0/2/0/0**
インターフェイス設定モードを開始します。GigabitEthernet0/2/0/0 で機能するようコンフィギュレーション モードを変更します。
- ステップ 9 l2transport**

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

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

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

ステップ 11 l2transport

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

ステップ 12 interface TenGigE0/1/0/2

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

ステップ 13 l2transport

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

ステップ 14 l2vpn

L2VPN コンフィギュレーションモードを開始します。

ステップ 15 bridge group examples

ブリッジグループ **examples** を作成します。

ステップ 16 bridge-domain test-switch

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

ステップ 17 interface Bundle-ether10

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

ステップ 18 exit

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

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

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

ステップ 20 exit

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

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

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

ステップ 22 exit

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

ステップ 23 `interface TenGigE0/1/0/2`

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

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

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

end : 次のいずれかのアクションを実行することをユーザに要求します。

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

イーサネット フローポイントでのブリッジング : 例

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

特記事項 :

- EFP は、レイヤ2 サブインターフェイスです。これは常に、トランク インターフェイスの下で作成されます。トランク インターフェイスは、EFP を作成する前に存在している必要があります。
- 空の設定では、バンドル インターフェイス トランクは存在しませんが、物理 トランク インターフェイスは自動的に設定されます。したがって、バンドル トランクだけが作成されます。
- この例では、サブインターフェイス番号および VLAN ID は同じですが、これは便利ではなく、必要性はありません。同じ値である必要はありません。
- ブリッジ ドメイン `test-efp` には、3 本の接続回線 (AC) があります。AC はすべて EFP です。
- VLAN ID が 999 のフレームだけが EFP に入ります。これによって、このブリッジ ドメインのすべてのトラフィックで同じ VLAN カプセル化を確保できます。
- 次の例の AC では、管理ダウン状態 (「未解決」状態) になっているインターフェイスを使用します。AC として存在しないインターフェイスを使用するブリッジ ドメインは正常であり、このような設定のコミットは失敗しません。この場合、ブリッジ ドメインのステータスは、欠落しているインターフェイスを設定するまで **unresolved** と表示されます。

設定例

```

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

```

次の表に、設定手順（アクション）およびこの例の対応する目的を示します。

手順

ステップ 1 configure

グローバル コンフィギュレーション モードを開始します。

ステップ 2 interface Bundle-ether10

新しいバンドル トランク インターフェイスを作成します。

ステップ 3 interface Bundle-ether10.999 l2transport

新しいバンドル トランクに EFP を作成します。

ステップ 4 encapsulation dot1q 999

この EFP に VLAN ID 999 を割り当てます。

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

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

ステップ 6 bundle id 10 mode active

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

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

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

ステップ 8 bundle id 10 mode active

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

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

GigabitEthernet0/6/0/7 に EFP を作成します。

ステップ 10 encapsulation dot1q 999

この EFP に VLAN ID 999 を割り当てます。

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

TenGigE0/1/0/2 に EFP を作成します。

ステップ 12 encapsulation dot1q 999

この EFP に VLAN ID 999 を割り当てます。

ステップ 13 l2vpn

L2VPN コンフィギュレーション モードを開始します。

ステップ 14 bridge group examples

examples という名前のブリッジ グループを作成します。

ステップ 15 bridge-domain test-efp

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

ステップ 16 interface Bundle-ether10.999

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

ステップ 17 exit

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

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

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

ステップ 19 exit

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

ステップ 20 interface TenGigE0/1/0/2.999

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

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

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

end : 次のいずれかのアクションを実行することをユーザに要求します。

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



第 7 章

ポイントツーポイント レイヤ 2 サービス の設定

この章では、ポイントツーポイントレイヤ2サービスについて紹介し、実装するための設定手順についても説明します。

次のポイントツーポイント サービスがサポートされています。

- ローカルスイッチング：ルータでのポイントツーポイント内部回線（ローカル接続とも呼ばれます）。
- 接続回線：PE CE ルータ ペア間の接続。
- 疑似回線：PE ルータ間の仮想ポイントツーポイント回線。疑似回線は、MPLS ネットワークを介して実装されます。



(注) ポイントツーポイント レイヤ 2 サービスは、MPLS レイヤ 2 VPN とも呼ばれます。

- [Ethernet over MPLS](#) (92 ページ)
- [接続回線間のローカル スwitching の設定](#) (94 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](#) (99 ページ)
- [ダイナミック ポイントツーポイント相互接続の設定](#) (101 ページ)
- [Inter-AS の設定](#) (102 ページ)
- [フレキシブルクロスコネク ト サービス](#) (102 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](#) (104 ページ)
- [AC 対応 VLAN バンドル](#) (118 ページ)
- [スプリット ホライズン グループ](#) (121 ページ)
- [G.8032 イーサネット リング保護](#) (125 ページ)
- [G.8032 イーサネット リング保護の設定：例](#) (132 ページ)
- [疑似回線冗長性](#) (136 ページ)
- [疑似回線冗長性 の設定](#) (139 ページ)

- L2VPN での仮想回線接続検証 (140 ページ)

Ethernet over MPLS

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

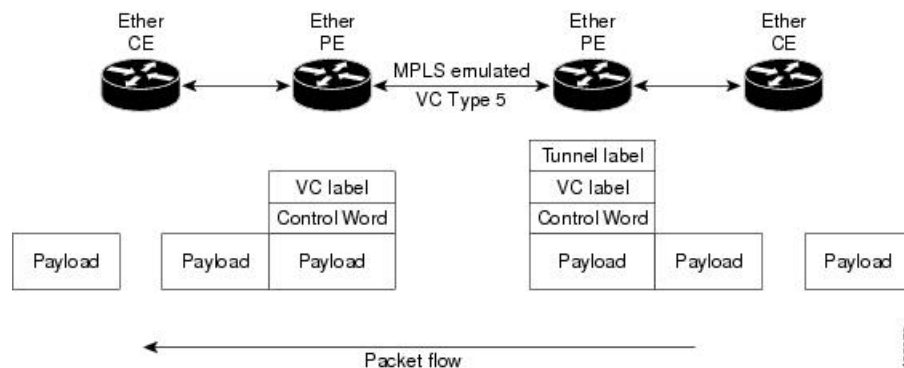
次の項では、EoMPLS を実装するさまざまなモードについて説明します。

イーサネットポートモード

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

次の図に、イーサネットポートモードのパケットフローの例を示します。

図 3: イーサネットポートモードのパケットフロー

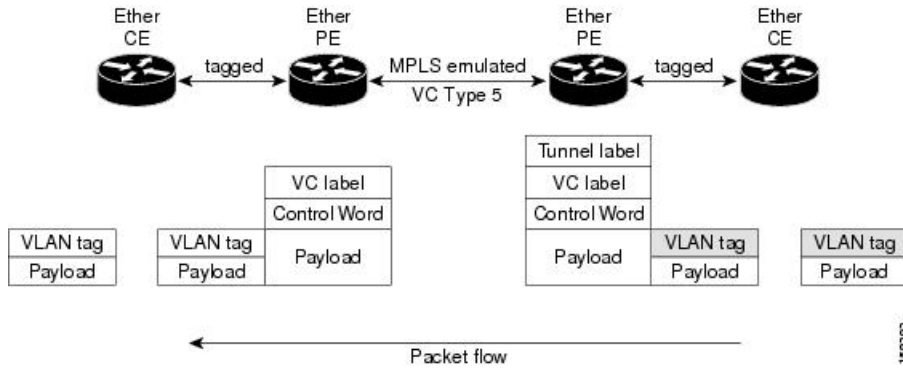


VLAN モード

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 packet 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。

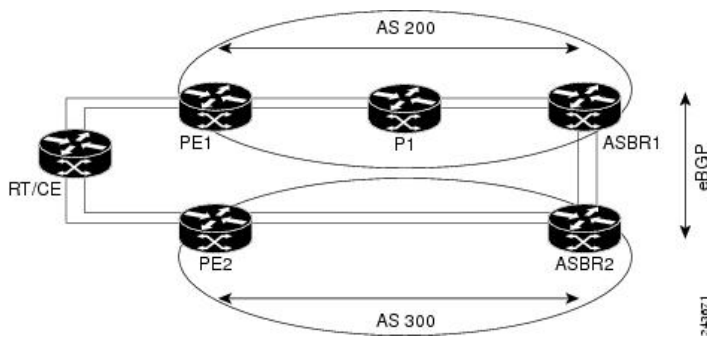
Inter-AS モード

Inter-AS は、複数のプロバイダーまたはマルチドメイン ネットワークを通じて VPN を拡張できるピアツーピア タイプ モデルです。これにより、サービス プロバイダーは相互にピアアップでき、地理的に離れた位置でエンドツーエンドの VPN 接続が実現します。

EoMPLS サポートでは、単一 AS トポロジを想定でき、このトポロジでは、ポイントツーポイント EoMPLS 相互接続の 2 つの終端にある PE ルータを接続する疑似回線が、同一自律システムに存在します。または、複数の AS トポロジを想定でき、このトポロジでは、PE ルータが iBGP および eBGP ピアリングを使用して 2 つの異なる AS に存在できます。

次の図は、各 AS で iBGP/LDP を使用した基本的な二重 AS トポロジを持つ Inter-AS を介した MPLS を示しています。

図 5: Inter-AS を介した EoMPLS : 基本的な二重 AS トポロジ



QinQ モード

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

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

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

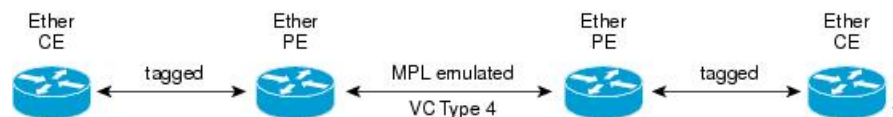
QinQ 上のレイヤ 3 サービスは次のとおりです。

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

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

次の図に、VC タイプ 4 を使用した QinQ を示します。

図 6: QinQ を介した EoMPLS モード



接続回線間のローカルスイッチングの設定

ローカルスイッチングでは、1つの接続回線 (AC) から別の AC へと、同じルータ上の同じタイプの 2 つのインターフェイス間で L2 データの交換が行われます。ローカルスイッチング接続で設定されている 2 つのポートで接続回線 (AC) を形成します。ローカルスイッチング

接続の動作は、2つのブリッジポートしかないブリッジドメインの動作と似ており、トラフィックはローカル接続の一方のポートに入り、もう一方のポートを通じて出て行きます。

レイヤ2 ローカル スイッチングには次のような特性があります。

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

制約事項

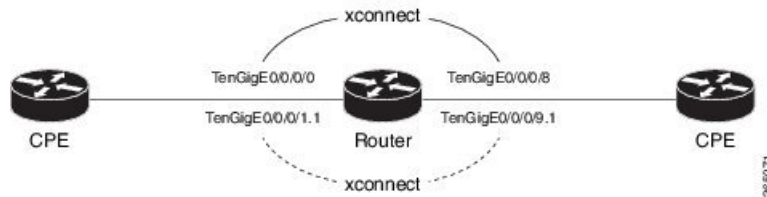
- 所定の物理ポートにあるすべてのサブインターフェイスは、次のような2つのタグプロトコル識別子（TPID）のみをサポートしています。
 - 0x88a8、0x8100
 - 0x9100、0x8100
 - 0x9200、0x8100
- VLAN および TPID ベースの入力パケット フィルタリングはサポートされていません。
- 出力 TPID の書き換えはサポートされていません。

トポロジ

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

設定には次のトポロジを使用します。

図 7: 接続回線間のローカルスイッチング



設定

AC-AC ローカルスイッチングを設定するには、次の設定を実行します。

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

```

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

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

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

Router(config)# interface Bundle-Ether 2

```

```

Router(config-if)# ipv4 address 10.1.2.2 255.0.0.0
Router(config-if)# bundle maximum-active links 32 hot-standby
Router(config-if)# bundle minimum-active links 1
Router(config-if)# bundle minimum-active bandwidth 3000000
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タ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。

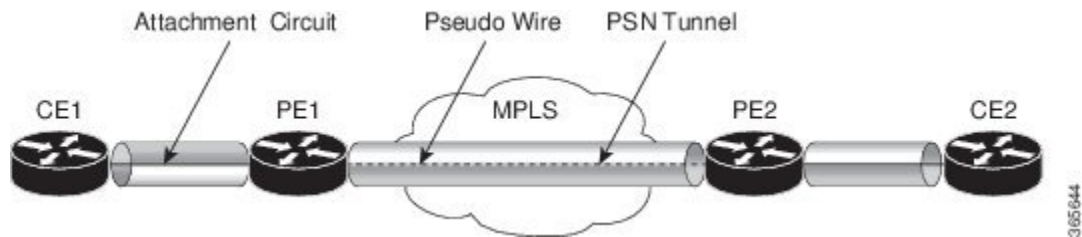


(注) スタティック疑似回線接続はシグナリングに LDP を使用しません。

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 8: レイヤ2 VPN のスタティック クロスコネクト回線



設定

```
/* Configure PE1 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group XCON1
Router(config-l2vpn-xc)# p2p xc1
Router(config-l2vpn-xc-p2p)# interface gigabitEthernet0/1/0/0.1
Router(config-l2vpn-xc-p2p)# neighbor 10.165.100.151 pw-id 100
Router(config-l2vpn-xc-p2p-pw)# mpls static label local 50 remote 40
Router(config-l2vpn-xc-p2p-pw)# commit

/*Configure PE2 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group XCON1
Router(config-l2vpn-xc)# p2p xc1
Router(config-l2vpn-xc-p2p)# interface gigabitEthernet0/2/0/0.4
Router(config-l2vpn-xc-p2p)# neighbor 10.165.200.254 pw-id 100
Router(config-l2vpn-xc-p2p-pw)# mpls static label local 40 remote 50
Router(config-l2vpn-xc-p2p-pw)# commit
```

実行コンフィギュレーション

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

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

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

確認

```
/* Verify the static cross connect on PE1 */
Router# show l2vpn xconnect
Tue Apr 12 20:18:02.971 IST
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
        SB = Standby, SR = Standby Ready, (PP) = Partially Programmed
```

XConnect 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

ダイナミックポイントツーポイント相互接続の設定

ダイナミックポイントツーポイント相互接続を設定するには、次の作業を実行します。



(注) ダイナミック相互接続では、LDP が稼働中である必要があります。

設定

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group vlan_grp_1
Router(config-l2vpn-xc)# p2p vlan1
Router(config-l2vpn-xc-p2p)# interface TenGigE 0/0/0/0.1
Router(config-l2vpn-xc-p2p)# neighbor 2.2.1.1 pw-id 1
Router(config-l2vpn-xc-p2p-pw)# commit
```

実行コンフィギュレーション

```

configure
  l2vpn
    xconnect group vlan_grp_1
      p2p vlan1
      interface TenGigE 0/0/0/0.1
      neighbor 2.2.1.1 pw-id 1
  !

```

Inter-AS の設定

Inter-AS の設定手順は、L2VPN 相互接続の設定作業と同じです（「[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（99 ページ）](#)」および「[ダイナミック ポイントツーポイント相互接続の設定（101 ページ）](#)」を参照）。ただし、相互接続設定で使用されるリモート PE の IP アドレスは iBGP ピアリングを通じて到達可能です。



(注) この設定を完了するには、IBGP、EBGP、および ASBR の用語および設定に関する知識が必要です。

フレキシブル クロスコネク ト サービス

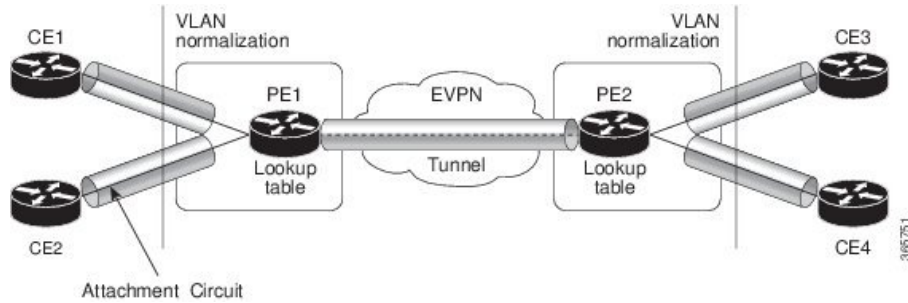
フレキシブルクロスコネク ト サービス機能では、同じプロバイダーエッジ (PE) 上の単一のイーサネット VPN 仮想プライベート ワイヤ サービス (EVPN-VPWS) サービス内の複数のエンドポイントにわたって接続回線 (AC) を集約することができます。AC は、一重 VLAN タグか、または二重 VLAN タグのいずれかで表されます。リモート PE 上の同じ VLAN タグで関連付けられた AC がクロスコネク ト です。VLAN タグは、インターフェイス上のフレームを適切なサービス インスタンスにマッピングするために使用する一致基準を定義します。その結果、ルックアップテーブルを作成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

フレキシブル クロスコネク ト サービス : シングルホーム

AC を通じた CE1 と CE2 から PE1 へのトラフィック フローの次のトポロジを考えてみます。AC は同じ PE1 上の複数のエンドポイント全体にわたって集約されています。VLAN (書き換え) は、PE1 上の AC インターフェイスに設定されている書き換えに基づいてルックアップテーブルを作成します。PE1 は BGP を使用して PE2 とルートを交換し、EVPN MPLS ネットワーク上にトンネルを作成します。PE2 の VLAN (書き換え) は、PE1 に設定されている書き

換えと一致している必要があります。書き換えタグに基づいて、PE2はトラフィックを対応する AC に転送します。たとえば、CE1 と CE2 の AC が同じ書き換えタグで設定されている場合、エンドツーエンドトラフィックは CE1 から CE3 に送信されます。

図 9: フレキシブルクロスコネク ト サービス

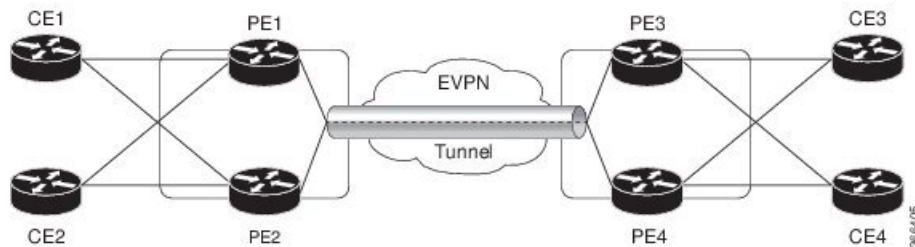


フレキシブル クロスコネク ト サービス : マルチホーム

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

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

図 10: フレキシブルクロスコネク ト サービス マルチホーム



CE1 と CE2 が PE1 と PE2 のマルチホームで、CE3 と CE4 が PE3 と PE4 のマルチホームであるトポロジを考えてみます。PE1 と PE2 はイーサネット A-D のイーサネット接続 (ES-EAD) ルートをリモート PE、つまり PE3 と PE4 にアドバタイズします。同様に、PE3 と PE4 は ES-EAD ルートをリモート PE、つまり PE1 と PE2 にアドバタイズします。ES-EAD ルートはメインインターフェイスごとにアドバタイズされます。

CE1 から CE3 へのトラフィック フローを考えてみます。PE1 または PE2 のいずれかにトラフィックが送信されます。パスの選択は、LAG を介して転送する CE の実装によって異なります。トラフィックは各 PE でカプセル化され、MPLS トンネルを通じてリモート PE (PE3 と

PE4) に転送されます。宛先 PE の選択は、フローベースのロードバランシングによって確立されます。PE3 と PE4 は CE3 にトラフィックを送信します。PE3 または PE4 から CE3 へのパスの選択は、フローベースのロードバランシングによって確立されます。

フレキシブルクロスコネク ト サービス サポート対象モード

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

- VLAN 非対応
- VLAN 対応
- ローカル スイッチング

VLAN 非対応

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

ESI が複数ある場合は、ゼロ ESI か非ゼロ ESI かに関係なく、ESI0 のみがシグナリングされます。このシナリオでは、シングルホーム モードのみがサポートされています。

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

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

```
/* Configure PE1 */
Router# configure
Router(config)# interface GigabitEthernet 0/2/0/3.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag translate 1-to-2 dot1q 500 second-dot1q 100 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。

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

VLAN 対応を使用したシングルホーム フレキシブル クロスコネクタの設定

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

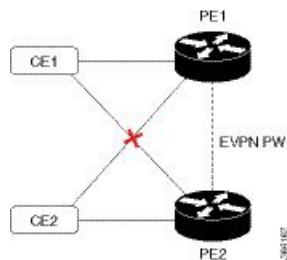
異なるイーサネットセグメントに属している2つのACに同じ正規化VLANがある場合、2つのAC間のトラフィックはPE内でローカルに切り替えられます。ローカルスイッチングはFXC VLAN対応でのみサポートされています。

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は異なる非ゼロESIに存在する必要があります。

図 11: ローカルスイッチング



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

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

!

```

AC 対応 VLAN バンドル

AC 対応 VLAN バンドル機能を使用すると、EVPN 対応ブリッジドメイン内の同じメインポートに複数のサブインターフェイスを設定できます。

この機能がない場合、MAC ルートは ESI のみを使用して発信元インターフェイスを識別します。同じ ESI を持つ複数のサブインターフェイスがある場合、それぞれのサブインターフェイスを区別する方法はありません。ブリッジポート (BP) のスタンプ付けは、EVI と ESI のみ実行されます。

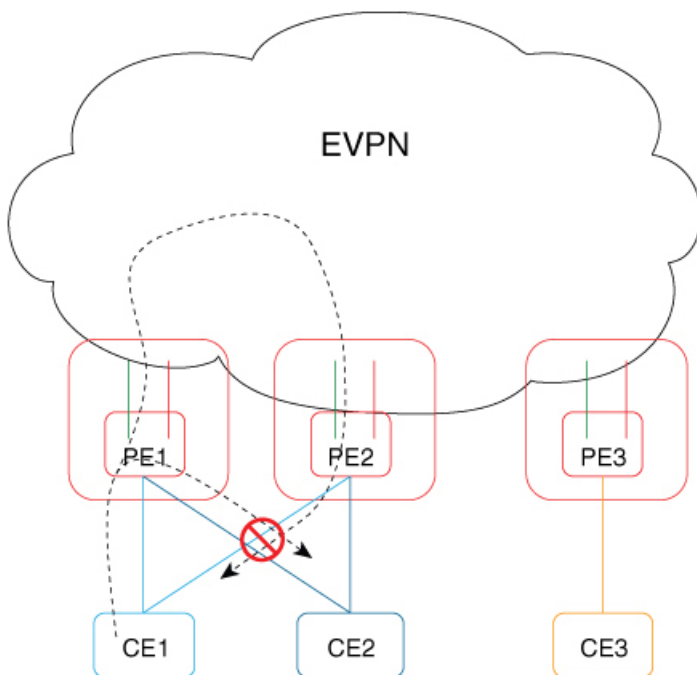
ac-aware-vlan-bundling コマンドを使用してこの機能を設定すると、サブインターフェイスを区別できるように、イーサネットタグ ID がサブインターフェイスの VLAN に設定されます。

アドバタイズされた ESI をホストするピアリングノードは、この機能を使用して、適切なローカルサブインターフェイスに対して BP スタンプ付けを実行します。

AC 対応 VLAN バンドルの設定

AC 対応 VLAN バンドル機能を設定するには、**ac-aware-vlan-bundling** コマンドを使用します。この機能を使用して、メインポートまたは ES で複数の AC を設定できます。

図 12: AC 対応 VLAN



このトポロジでは、CE1 からのトラフィックが PE1 に流れるときに、PE1 は他の PE にメッセージをフラッディングします。PE2 が CE1 に直接接続されているため、これらの PE 間でループが形成されます。ループを回避するため、PE1 上のローカル CE1 サブインターフェイスから PE2 上のリモート CE1 サブインターフェイスへのトラフィックは、ESI フィルタリングを使用して阻止されます。

VLAN 範囲付きの EFP がサポートされています。VLAN 範囲の設定では、最大 1 つのブリッジポートがサポートされます。このポートは **rewrite pop** コマンドが設定されていない場合にのみ使用できます。つまり、VLAN 範囲が使用されている場合、ブリッジドメイン内の BVI インターフェイスはサポートされません。PE1 と PE2 の両方で同じ VLAN 範囲を設定する必要があります。

AC 間のスプリットホライズングループは自動的に有効になりません。メインインターフェイスに ESI がない場合に、同じブリッジドメイン内の AC から AC への BUM トラフィックをブロックするには、スプリットホライズングループを設定する必要があります。

下位互換性

リモート PE の場合、この機能は Cisco IOS XR ソフトウェア リリース 6.3.3 以降でサポートされています。これは、非ゼロのイーサ タグを持つルート タイプ 2 MAC ルートがサポートされているためです。

ピアリング PE の場合、両方の PE で Cisco IOS XR ソフトウェア リリース 6.6.1 以降のバージョンが実行されている必要があります。または、この機能を有効にする前に、両方の PE を Cisco IOS XR ソフトウェア リリース 6.6.1 にアップグレードする必要があります。

設定例

```
/* Configure AC-aware VLAN bundle on PE1, PE2, and PE3 */
Router# configure
Router# l2vpn
Router(config-l2vpn)# bridge group bg1
Router(config-l2vpn-bg)# bridge-domain bd1
Router(config-l2vpn-bg-bd)# interface Bundle-Ether 1.1 split-horizon group
Router(config-l2vpn-bg-bd)# interface Bundle-Ether 1.2 split-horizon group
Router(config-l2vpn-bg-bd)# evi 1
Router(config-l2vpn-bg-bd-evi)# exit
Router(config-l2vpn-bg-bd)# exit
Router(config-l2vpn-bg)# exit
Router(config-l2vpn)# exit
Router(config)# evpn
Router(config-evpn)# evi 1
Router(config-evpn-instance)# advertise-mac
Router(config-evpn-instance)# ac-aware-vlan-bundling
Router(config-evpn-instance)# commit
```

実行コンフィギュレーション

ここでは、AC 対応 VLAN バンドルの実行コンフィギュレーションを示します。

```
l2vpn
 bridge group bg1
  bridge-domain bd1
    interface Bundle-Ether 1.1 split-horizon group
    interface Bundle-Ether 1.2 split-horizon group
    evi 1
  !
!
evpn
 evi 1
  advertise-mac
  ac-aware-vlan-bundling
  !
!
!
```

確認

AC のカプセル化の正しいイーサ タグ値を使用して EVPN を適切に設定していることを確認します。

```
Router#show evpn evi mac detail
```

```
VPN-ID      Encap  MAC address      IP address      Nexthop
```

```

-----
Label
-----
1          MPLS  0010.3000.0010 ::          Bundle-Ether
1.1        24003
Ethernet Tag : 1
Multi-paths Resolved          : False
Multi-paths Internal label    : 0
Local Static                  : Yes
Remote Static                 : No
Local Ethernet Segment       : 0000.0000.0000.0000.0000
Remote Ethernet Segment      : N/A
Local Sequence Number        : 0
Remote Sequence Number       : N/A
Local Encapsulation          : MPLS
Remote Encapsulation         : N/A

Router# show bgp l2vpn evpn bridge-domain bd1 detail

Route Distinguisher: 1606:101 (default for vrf bd1)
*> [2] [1] [48] [0010.3000.0010] [0]/104

```

関連項目

- [AC 対応 VLAN バンドル \(118 ページ\)](#)

関連コマンド

- ac-aware-vlan-bundling
- show evpn evi mac detail
- show evpn igmp detail

スプリット ホライズン グループ

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

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

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

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

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

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

表 1: Cisco IOS-XR でサポートされているスプリットホライズングループ

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

スプリットホライズングループに関する重要事項：

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

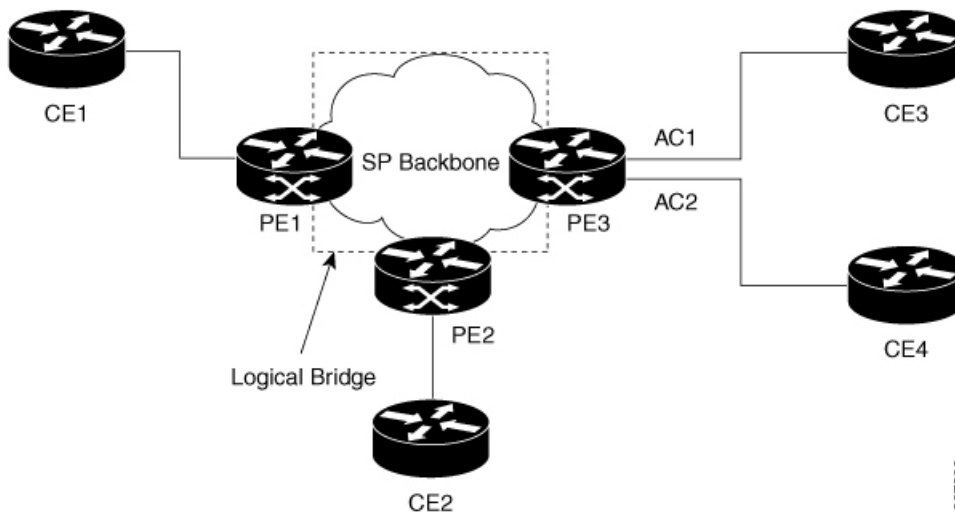
スプリットホライズングループ2

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

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

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

図 13: スプリット ホライズン グループ 2



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

スプリット ホライズン グループ 2 の設定

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

設定例

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

```

/* Configure on PE3 */
Router#configure
Router(config)#l2vpn
Router(config-l2vpn)#router-id 3.3.3
Router(config-l2vpn)#pw-class class1
Router(config-l2vpn-pwc)#encapsulation mpls
Router(config-l2vpn-pwc-encapmpls)#protocol ldp
Router(config-l2vpn-pwc-encapmpls)#ipv4 source 3.3.3.3
Router(config-l2vpn-pwc-encapmpls)#exit
Router(config-l2vpn-pwc)#exit
Router(config-l2vpn)#bridge group bg1
Router(config-l2vpn-bg)#bridge-domain bd
Router(config-l2vpn-bg-bd)#exit
Router(config-l2vpn-bg)#bridge-domain bd1
Router(config-l2vpn-bg-bd)#interface TenGigE0/0/0/0
Router(config-l2vpn-bg-bd-ac)#split-horizon group
Router(config-l2vpn-bg-bd-ac)#exit
Router(config-l2vpn-bg-bd)#interface TenGigE0/0/0/0

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

```

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

```

実行コンフィギュレーション

```

configure
l2vpn
router-id 3.3.3.3
pw-class classs1
encapsulation mpls
protocol ldp
ipv4 source 3.3.3.3
!
!
bridge group bgl
bridge-domain bd
!
bridge-domain bd1
interface TenGigE0/0/0/0
split-horizon group
!
interface TenGigE0/0/0/0
split-horizon group
!
vfi vfil
neighbor 1.1.1.1 pw-id 1
pw-class class1
!
!
!

```

確認

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

```

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

Legend: pp = Partially Programmed.
Bridge group: bgl, bridge-domain: bd1, id: 1, state: up, ShgId: 0, MSTi: 0
Aging: 300s, MAC limit: 64000, Action: none, Notification: syslong
Filter MAC addresses: 0
ACs: 2 (2 up), VFIs: 1, PWs: 1 (up), PBBs: 0 (0 up), VNIs: 0 (0 up)
List of ACs:
Te0/0/0/0
, stage: up, Static MAC addresses: 0
Te0/0/0/0, stage: up, Static MAC addresses: 0
List of Access PWs:
List of VFIs:
VFI vfil (up)
Neighbor 1.1.1.1 pw-id 1, stage: up, Static MAC Addresses: 0

```

G.8032 イーサネットリング保護

G.8032 イーサネットリング保護機能は、リングトポロジ内のイーサネットトラフィックの保護を提供します。この機能により、事前設定されたリンクも障害リンクもブロックされ、イーサネットレイヤにおけるリング内のループが防止されます。

概要

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



(注) イーサネットリングでのイーサネットリングノードの最小数は2です。

リング保護スイッチングの基礎は次のとおりです。

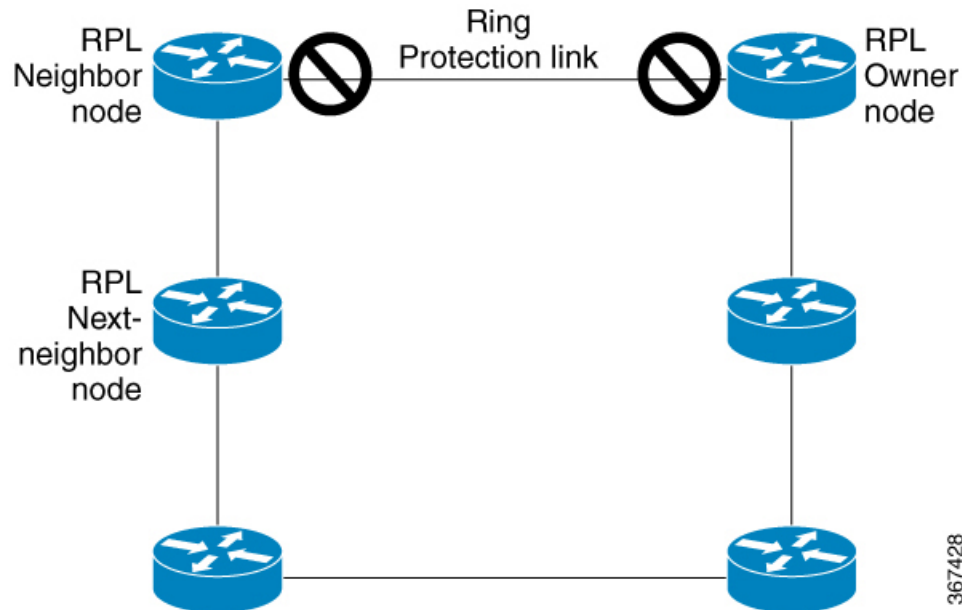
- ループ回避の原則。
- 学習、転送、およびフィルタリングデータベース（FDB）メカニズムの使用。

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

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

次の図はG.8032 イーサネットリングの例です。

図 14: G.8032 イーサネットリング



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

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

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

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

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

- **Manual switch (MS)** : オペレータは、特定のリング ポートを手動でブロックできます。
 - 既存の FS または SF 状態では無効です。
 - 新しい FS または SF 状態によって上書きされます。
 - 過去のすべての MS コマンドをクリアします。
- **Clear** : リング ポートで既存の FS または MS コマンドを取り消します。
 - 非リバーティブ モードをクリアするために (RPL オーナーで) 使用されます。

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

タイマー

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

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



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

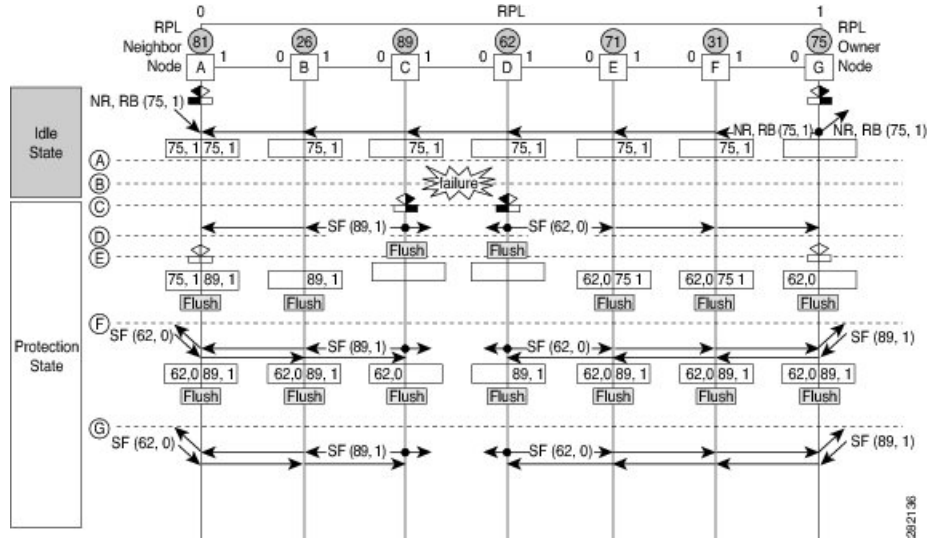
- **ガードタイマー** : 状態の変更時にすべてのノードで使用されます。これは、潜在的な古いメッセージが不要な状態変更を引き起こさないようにします。ガードタイマーは設定可能であり、デフォルトの時間間隔は 500 ミリ秒です。時間間隔の範囲 10 ~ 2000 ミリ秒です。
- **hold-off タイマー** : 断続的なリンク障害をフィルタリングするために、基盤となるイーサネット レイヤによって使用されます。hold-off タイマーは設定可能であり、デフォルトの時間間隔は 0 秒です。時間間隔の範囲は 0 ~ 10 秒です。

- 障害は、このタイマーの有効期限が切れた場合だけリング保護メカニズムに報告されます。

単一のリンク障害

次の図は、単一のリンク障害が発生した場合の保護スイッチングを表しています。

図 15: G.8032 の単一のリンク障害



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

次の記号が使用されます。

- Message source
- ▶ R-APS channel blocking
- Client channel blocking
- Ⓝ Node ID

次の流れでは、単一のリンク障害でのステップについて説明します。

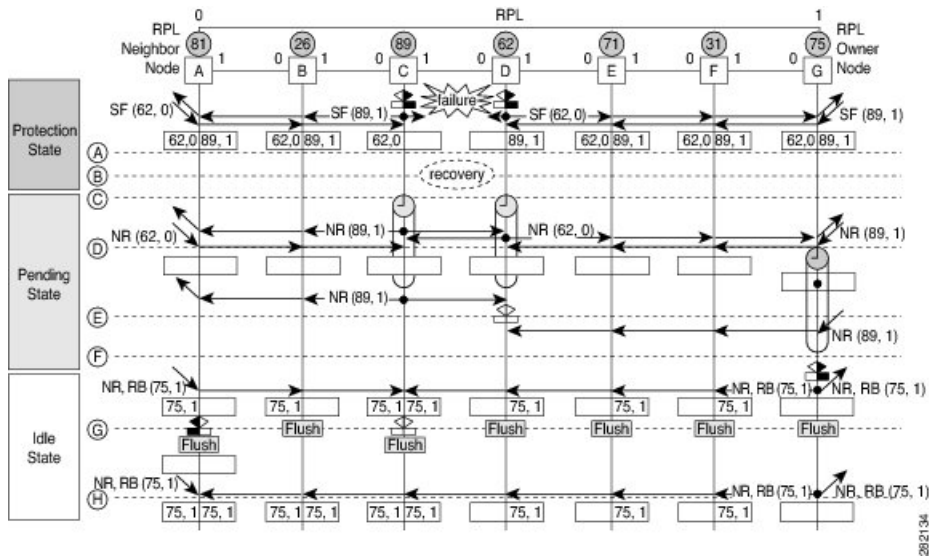
1. リンクは正常な状態で動作しています。
2. 障害が発生します。
3. イーサネットリングノードCとDは、ローカルの信号障害を検出し、ホールドオフ時間間隔後に障害が発生したリングポートをブロックし、FDBフラッシュを実行します。
4. イーサネットリングノードCとDは、SF状態が続いている間、両方のリングポートの（ノードID、BPR）ペアとともにRAPS（SF）メッセージの定期的な送信を開始します。
5. RAPS（SF）メッセージを受信するすべてのイーサネットリングノードがFDBフラッシュを実行します。RPLオーナーノードGとRPLネイバーノードAがRAPS（SF）メッセー

ジを受信すると、イーサネットリングノードは自身のRPLの終端をブロック解除し、FDBフラッシュを実行します。

6. 2番目の RAPS (SF) メッセージを受信するすべてのイーサネットリングノードは、FDBフラッシュを再度実行します。これは、ノード ID と BPR ベースメカニズムが原因です。
7. 安定した SF 状態：イーサネットリングの RAPS メッセージ (SF)。これ以上の RAPS (SF) メッセージは、さらなるアクションをトリガーしません。

次の図は、単一のリンク障害が発生した場合の復帰を表しています。

図 16: 単一のリンク障害回復 (リバーティブ操作)



次の流れでは、単一のリンク障害での復帰のステップについて説明します。

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

6. WTRタイマーの有効期限が切れると、RPL オーナーノードは、RPLの終端をブロックし、(ノードID、BPR) ペアを持つRAPS (NR、RB) メッセージを送信し、FDBフラッシュを実行します。
7. イーサネットリングノードCがRAPS (NR、RB) メッセージを受信すると、ブロックされたリングポートのブロックを解除し、RAPS (NR) メッセージの送信を停止します。一方、RPLネイバーノードAがRAPS (NR、RB) メッセージを受信すると、RPLの終了をブロックします。さらに、イーサネットリングノードA～Fは、ノードIDとBPRベースメカニズムが存在することが原因で、RAPS (NR、RB) メッセージを受信するとFDBフラッシュを実行します。

G.8032 イーサネットリング保護の設定

イーサネットリング保護機能を設定するには、次の作業を実行します。

- ERP プロファイルの設定
- ERP インスタンスの設定



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

ERP プロファイルの設定

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

設定例

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

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

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

実行コンフィギュレーション

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

ERP インスタンスの設定

ERP インスタンスを設定するには、次の作業を実行します。

設定例

```
Router#configure
Router (config)l2vpn
Router (config-l2vpn)#ethernet ring g8032 ring1
Router (config-l2vpn-erp)#port0 interface TenGigE0/0/0/0
Router (config-l2vpn-erp-port0)#exit
Router (config-l2vpn-erp)#port1 interface TenGigE0/0/0/8
Router (config-l2vpn-erp-port1)#exit
Router (config-l2vpn-erp)#instance 1
Router (config-l2vpn-erp-instance)#profile p1
Router (config-l2vpn-erp-instance)#rpl port0 owner
Router (config-l2vpn-erp-instance)#inclusion-list vlan-ids 1,7-150
Router (config-l2vpn-erp-instance)#aps-channel
Router (config-l2vpn-erp-instance-aps)#port0 interface TenGigE0/0/0/0
Router (config-l2vpn-erp-instance-aps)#port0 interface TenGigE0/0/0/8
Router (config-l2vpn-erp-instance-aps)#commit
```

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

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

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

実行コンフィギュレーション

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

```
!
!
!
```

確認

イーサネットリングのステータスを確認します。

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

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

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

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

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

G.8032 イーサネットリング保護の設定：例

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

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

# Configure CFM MEPs and configure to monitor the ring links.
ethernet cfm
domain domain1
service link1 down-meps
continuity-check interval 100ms
```

```
        efd
        mep crosscheck
        mep-id 2
        domain domain2
            service link2 down-meps
            continuity-check interval 100ms
            efd protection-switching
        mep crosscheck
        mep id 2

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

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

# Set up the bridge domains
bridge group ABC
    bridge-domain BD2
        interface Gig 0/0/0/0

        interface Gig 0/0/0/1
        interface Gig 0/0/0/2

    bridge-domain BD2-APS
        interface Gig 0/0/0/0
        interface Gig 0/0/0/1

# EFPs configuration
interface Gig 0/0/0/0 l2transport
    encapsulation dot1q 5

interface Gig 0/0/0/0 l2transport
    encapsulation dot1q 5

interface g0/0/0/2 l2transport
    encapsulation dot1q 10-100

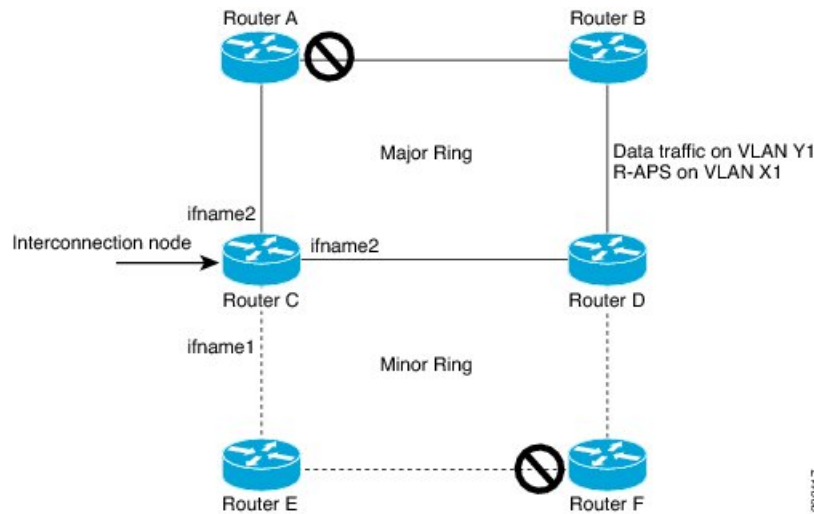
interface g 0/0/0/1 l2transport
    encapsulation dot1q 10-100

interface g 0/0/0/2 l2transport
    encapsulation dot1q 10-100
```

相互接続ノードの設定：例

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

図 17: リング シナリオ：相互接続ノード



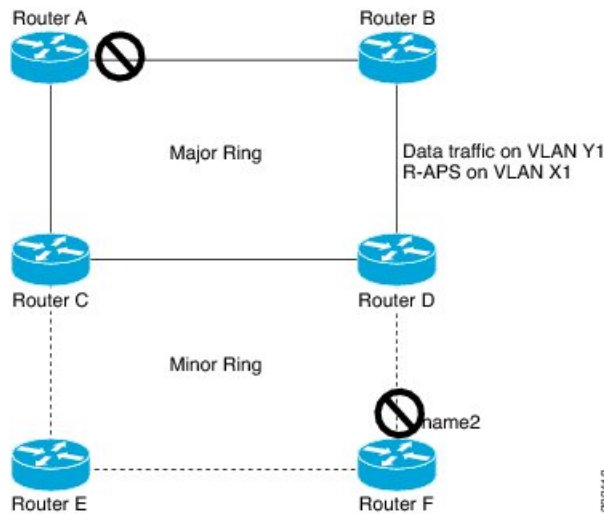
ルータ C（開いたリング：ルータ C）で G.8032 を設定するために必要な最小設定：

```
interface Gig 0/0/0/1.1 l2transport
 encapsulation dot1q 5
interface Gig 0/0/0/1.10 l2transport
 encapsulation dot1q 6
interface Gig 0/0/0/2.10 l2transport
 encapsulation dot1q 6
interface Gig 0/0/0/3.10 l2transport
 encapsulation dot1q 6
l2vpn
ethernet ring g8032 ring8
  port0 interface Gig 0/0/0/1
  port1 none /* This router is connected to an interconnection node. */
  open-ring
  !
  instance 1
  inclusion-list vlan-ids 1,7-150
  aps-channel
  port0 interface Gig 0/0/0/1.1
  port1 none /* This router is connected to an interconnection node */
  !
bridge group bg1
  bridge-domain BD2 /* Data traffic has its own bridge domain */
  interface Gig 0/0/0/1.10
  interface Gig 0/0/0/2.10
  interface Gig 0/0/0/3.10
  !
  bridge-domain BD2-APS /* APS-channel has its own bridge domain */
  interface Gig 0/0/0/1.1 /* There is only one APS-channel at the interconnection node */
  */
```

開いたリングのノードの設定：例

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

図 18:開いたリング シナリオ



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

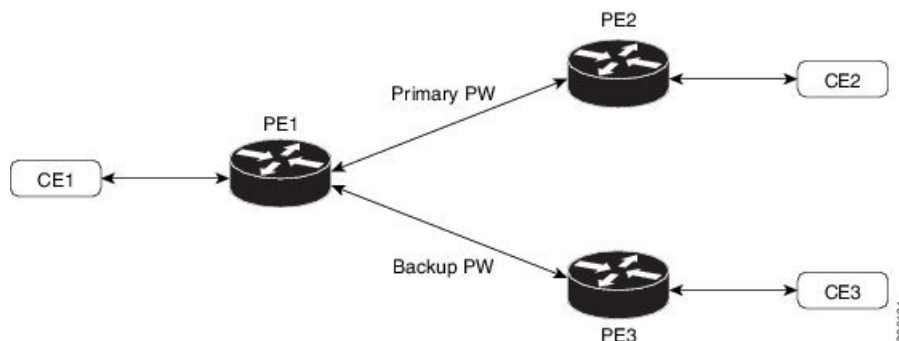
```
interface Gig 0/0/0/1.1 l2transport
 encapsulation dot1q 5
interface Gig 0/0/0/2.1 l2transport
 encapsulation dot1q 5
interface Gig 0/0/0/1.10 l2transport
 encapsulation dot1q 6
interface Gig 0/0/0/2.10 l2transport
 encapsulation dot1q 6
l2vpn
  ethernet ring g8032 ringB
    port0 interface Gig 0/0/0/1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

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

疑似回線冗長性

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

図 19: 疑似回線冗長性



バックアップ疑似回線への強制的な手動切り替え

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

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

疑似回線冗長性の設定

ここでは、疑似回線冗長性を設定する方法について説明します。

疑似回線冗長性機能を設定する際には、次の制限事項を考慮する必要があります。

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

```

/* Configure PW on PE1 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group XCON1
Router(config-l2vpn-xc)# p2p xc1
Router(config-l2vpn-xc-p2p)# interface GigabitEthernet0/0/0/0
Router(config-l2vpn-xc-p2p)# neighbor ipv4 2.2.2.2 pw-id 1
Router(config-l2vpn-xc-p2p-pw)# backup neighbor 3.3.3.3 pw-id 1
Router(config-subif)# commit

/* Configure PW on PE2 */
Router# configure

```

```

Router(config)# l2vpn
Router(config-l2vpn)# xconnect group XCON1
Router(config-l2vpn-xc)# p2p xc1
Router(config-l2vpn-xc-p2p)# interface GigabitEthernet0/0/0/0
Router(config-l2vpn-xc-p2p)# neighbor ipv4 1.1.1.1 pw-id 1
Router(config-subif)# commit

/* Configure PW on PE3 */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group XCON1
Router(config-l2vpn-xc)# p2p xc1
Router(config-l2vpn-xc-p2p)# interface GigabitEthernet0/0/0/0
Router(config-l2vpn-xc-p2p)# neighbor ipv4 1.1.1.1 pw-id 1
Router(config-subif)# commit

```

実行コンフィギュレーション

```

/* On PE1 */
!
l2vpn
xconnect group XCON1
  p2p XCON1_P2P2
    interface GigabitEthernet 0/0/0/0
    neighbor ipv4 2.2.2.2 pw-id 1
    backup neighbor 3.3.3.3 pw-id 1
!

/* On PE2 */
!
l2vpn
xconnect group XCON1
  p2p XCON1_P2P2
    interface GigabitEthernet 0/0/0/0
    neighbor ipv4 1.1.1.1 pw-id 1
!

/* On PE3 */
!
l2vpn
xconnect group XCON1
  p2p XCON1_P2P2
    interface GigabitEthernet 0/0/0/0
    neighbor ipv4 1.1.1.1 pw-id 1
!

```

確認

設定した擬似回線冗長性がアップ状態であることを確認します。

```

/* On PE1 */

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

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

```

```

-----
XCON_1      XCON1_P2P2 UP   Gi0/1/0/0.1      UP      2.2.2.2      1000  UP
                                           Backup
                                           3.3.3.3      1000  SB
-----

/* On PE2 */

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

XConnect
Group      Name      ST      Segment 1
          Description      ST      Segment 2
          Description      ST
-----
XCON_1    XCON1_P2P2 UP      BE100.1      UP      1.1.1.1      1000  UP
-----

/* On PE3 */

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

XConnect
Group      Name      ST      Segment 1
          Description      ST      Segment 2
          Description      ST
-----
XCON_1    XCON1_P2P2 DN      BE100.1      UP      1.1.1.1      1000  SB
-----

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

```


疑似回線冗長性の設定

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

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

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

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

設定

ここでは、疑似回線冗長性の設定について説明します。

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

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

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

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

実行コンフィギュレーション

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

```
backup neighbor 10.2.2.2 pw-id 5
!  
!  
...
```

L2VPN での仮想回線接続検証

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

2つのタイプのパケットが判定結果出力に着信します。

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

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 8 章

EVPN 機能

この章では、ルータでレイヤ 2 イーサネット VPN (EVPN) 機能を設定する方法について説明します。

- [EVPN の概要 \(141 ページ\)](#)
- [EVPN の概念 \(143 ページ\)](#)
- [EVPN 動作 \(144 ページ\)](#)
- [EVPN ルート タイプ \(145 ページ\)](#)
- [EVPN L2 ブリッジング サービスの設定 \(146 ページ\)](#)
- [EVPN MAC アドレス制限の設定 \(148 ページ\)](#)
- [EVPN ソフトウェア MAC ラーニング \(150 ページ\)](#)
- [EVPN アウト オブ サービス \(158 ページ\)](#)
- [EVPN 対応 CFM のサポート \(162 ページ\)](#)
- [イーサネット セグメント単位の EVPN 複数サービス \(162 ページ\)](#)
- [EVPN MPLS と VPLS のシームレスな統合 \(168 ページ\)](#)
- [既存の VPLS ネットワークでの EVPN の設定 \(170 ページ\)](#)
- [L2VPN ブリッジ ドメインでの EVI の設定 \(172 ページ\)](#)
- [EVPN 設定の確認 \(173 ページ\)](#)
- [EVPN シングルアクティブ マルチホーミング \(177 ページ\)](#)
- [EVPN コア分離保護 \(180 ページ\)](#)
- [EVPN ルーティング ポリシー \(183 ページ\)](#)
- [EVPN ELAN での CFM \(198 ページ\)](#)

EVPN の概要

イーサネット VPN (EVPN) は、MPLS ネットワークを介してイーサネット マルチポイント サービスを提供する次世代のソリューションです。EVPN は、コアでコントロールプレーンベースの MAC ラーニングを可能にする既存の仮想プライベート LAN サービス (VPLS) とは対照的に動作します。EVPN では、EVPN インスタンスに参加している PE が MP-BGP プロトコルを使用してコントロールプレーン内でカスタマー MAC ルートを学習します。コントロー

ルプレーン MAC ラーニングは、フローごとのロードバランシングによるマルチホーミングのサポートなど、VPLS の欠点に EVPN で対処できるようにする数多くの利点をもたらします。

EVPN は、ネットワークでの次の新たなニーズに対応するソリューションをネットワークオペレータに提供します。

- データセンター相互接続操作 (DCI)
- クラウドおよびサービスの仮想化
- プロトコルの排除とネットワークの簡素化
- 同じ VPN を介した L2 サービスと L3 サービスの統合
- サービスとワークロードの柔軟な配置
- L2 および L3 VPN によるマルチテナント
- 最適な転送とワークロード モビリティ
- 高速コンバージェンス
- 効率的な帯域幅利用

EVPN の利点

EVPN には次の利点があります。

- 統合サービス：L2 および L3 VPN サービスの統合、拡張性と制御における L3VPN のような原則と運用経験、ECMP を使用したオールアクティブマルチホーミングと PE ロードバランシング、複数の PE に対してマルチホームである CE との間で発着信するトラフィックのロードバランシングが可能。
- ネットワーク効率：フラッドと学習メカニズムの排除、デュアルホーム接続サーバへのリンクでの障害発生時の高速再ルーティング、復元力、および高速な再コンバージェンス、ブロードキャスト、不明ユニキャスト、マルチキャスト (BUM) トラフィック配信の最適化。
- サービスの柔軟性：MPLS データプレーンのカプセル化、既存および新しいサービスタイプのサポート (E-LAN、E-Line)、ピア PE 自動検出、および冗長グループ自動感知。

EVPN のモード

次の EVPN モードがサポートされています。

- シングルホーミング：これにより、カスタマー エッジ (CE) デバイスをプロバイダー エッジ (PE) デバイス 1 台に接続できます。
- マルチホーミング：これにより、カスタマーエッジ (CE) デバイスを複数のプロバイダーエッジ (PE) デバイスに接続できます。マルチホーミングにより、冗長接続が確保されます。冗長 PE デバイスは、ネットワーク障害が発生している場合にトラフィックが中断されないようにします。次にマルチホーミングのタイプを示します。

- オールアクティブ：オールアクティブモードでは、特定のイーサネットセグメントに接続されているすべての PE が、そのイーサネットセグメントとの間で発着信するトラフィックを転送できます。

EVPN の概念

EVPN 機能を実装するには、次の概念を理解する必要があります。

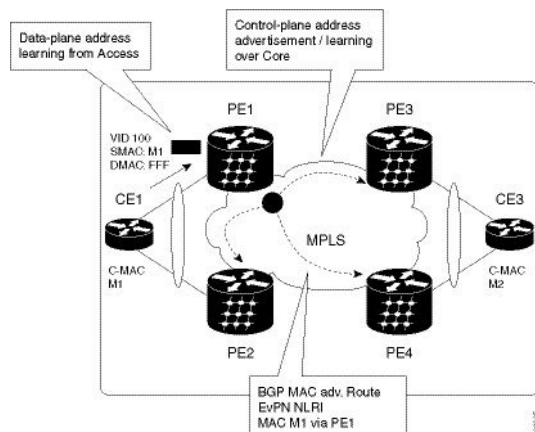
- イーサネットセグメント (ES)：イーサネットセグメントは、マルチホームデバイスに接続する一連のイーサネットリンクです。マルチホームデバイスまたはネットワークが 2 つ以上の PE に一連のイーサネットリンクを通じて接続されている場合に、その一連のリンクをイーサネットセグメントと呼びます。イーサネットセグメントルートはルートタイプ 4 とも呼びます。このルートは、BUM トラフィックの指定フォワーダ (DF) の選択に使用されます。
- イーサネットセグメント識別子 (ESI)：イーサネットセグメントには一意の非ゼロの識別子が割り当てられます。これをイーサネットセグメント識別子 (ESI) と呼びます。ESI は、ネットワーク全体にわたってイーサネットセグメントを一意に表します。
- EVI：EVPN インスタンス (EVI) は仮想ネットワーク識別子 (VNI) で表されます。EVI は、PE ルータ上の VPN を表します。EVI は IP VPN ルーティングおよび転送 (VRF) と同じ役割を果たし、インポート/エクスポートルートターゲット (RT) が割り当てられません。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ときのエイリアシングとロードバランシングに使用されます。EAD/ES ルートと区別するため、このルートにはイーサネットタグ値 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 20: 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 2: EVPN ルートタイプ

ルートタイプ	名前	使用法
1	イーサネット自動検出 (AD) ルート	ES ごとの少数ルートの送信、ES に属する EVI のリストの伝送
2	MAC/IP アドバタイズメント ルート	MAC のアドバタイズ、アドレス到達可能性、IP/MAC バインディングのアドバタイズ
3	包括的なマルチキャスト イーサネット タグ ルート	マルチキャスト トンネル エンドポイントの検出
4	イーサネットセグメントルート	冗長グループの検出、DF の選択
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 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ドングを削減します。

ルートタイプ3：包括的なマルチキャストイーサネットタグルート

このルートは、送信元 PE からリモート PE へのブロードキャスト、不明ユニキャスト、およびマルチキャスト (BUM) トラフィック用の接続を確立します。このルートは、VLAN ごとと ESI ごとにアドバタイズされます。

ルートタイプ4：イーサネットセグメントルート

イーサネットセグメントルートでは CE デバイスを 2 台のデバイスまたは PE デバイスを接続できます。ES ルートでは同じイーサネットセグメントに接続されている PE デバイスを検出できます。

ルートタイプ5：IP プレフィックスルート

IP プレフィックスが MAC アドバタイズメントルートとは関係なくアドバタイズされます。EVPN IRB では、ホストルート /32 は RT-2 を使用してアドバタイズされ、サブネット /24 は RT-5 を使用してアドバタイズされます。



- (注) EVPN IRB では、ホストルート /32 は RT-2 を使用してアドバタイズされ、サブネット /24 は RT-5 を使用してアドバタイズされます。

EVPN L2 ブリッジング サービスの設定

EVPN L2 ブリッジング サービスを設定するには、次のステップを実行します。



- (注) 必ず、ラベルモードをプレフィックス単位から VRF ラベルモード単位に変更してください。L2FIB および VPNv4 ルート (ラベル) は同じリソースを共有しているため、リソースを枯渇させると BVI の ping は失敗します。



- (注) デバイスには最大 128K の MAC アドレス エントリを含めることができます。デバイス上のブリッジドメインには最大 64K の MAC アドレス エントリを含めることができます。



- (注) フラッドイングの無効化は、EVPN ブリッジドメインではサポートされていません。

```
/* Configure address family session in BGP */
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router#(config)# router bgp 200
RP/0/RSP0/CPU0:router#(config-bgp)# bgp router-id 209.165.200.227
RP/0/RSP0/CPU0:router#(config-bgp)# address-family l2vpn evpn
```



```

RP/0/RSP0/CPU0:router#(config-bgp)# neighbor 10.10.10.10
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# remote-as 200
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# description MPLSFACING-PEER
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# update-source Loopback 0
RP/0/RSP0/CPU0:router#(config-bgp-nbr)# address-family l2vpn evpn

/* Configure EVI and define the corresponding BGP route targets */

Router# configure
Router(config)# evpn
Router(config-evpn)# evi 6005
Router(config-evpn-evi)# bgp
Router(config-evpn-evi-bgp)# rd 200:50
Router(config-evpn-evi-bgp)# route-target import 100:6005
Router(config-evpn-evi-bgp)# route-target export 100:6005
Router(config-evpn-evi-bgp)# exit
Router(config-evpn-evi)# advertise-mac

/* Configure a bridge domain */
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group 1
Router(config-l2vpn-bg)# bridge-domain 1-1
Router(config-l2vpn-bg-bd)# interface GigabitEthernet 0/0/0/1
Router(config-l2vpn-bg-bd-ac)# evi 6005
Router(config-l2vpn-bg-bd-ac-evi)# commit
Router(config-l2vpnbg-bd-ac-evi)# exit

```

実行コンフィギュレーション

```

router bgp 200 bgp
router-id 209.165.200.227
address-family l2vpn evpn
neighbor 10.10.10.10
  remote-as 200 description MPLS-FACING-PEER
  updatesource Loopback0
  addressfamily l2vpn evpn
!

configure
evpn
evi 6005
  bgp
    rd 200:50
    route-target import 100:6005
    route-target export 100:6005
!
  advertise-mac

configure
l2vpn
  bridge group 1
  bridge-domain 1-1
  interface GigabitEthernet 0/0/0/1

    evi 6005
!

```

EVPN MAC アドレス制限の設定

EVPN MAC アドレス制限を設定する場合、次の制限事項が適用されます。

- リモート MAC アドレスは、MAC アドレス制限が設定されているかどうかに関係なく、ハードウェアでプログラムされます。
- MAC アドレス制限のアクションは、ローカル MAC アドレスの数が設定された制限を超えた場合にのみ適用されます。MAC アドレス制限が、リモートおよびローカル MAC アドレスによって枯渇した場合、またはリモート MAC アドレスによってのみ割り当てられた場合、MAC アドレス制限のアクションは適用されません。超過したトラフィックは不明なユニキャストと見なされ、ブリッジドメイン全体にフラディングされます。
- MAC アドレス制限は、デバイスが MAC アドレスをアクティブに学習していない場合にのみ、正しく変更できます。これは予期された動作です。
- MAC ラーニングが有効になっている場合は、MAC アドレス制限を最大 6 つまで設定できます。ただし、MAC ラーニングが無効になっている場合は、MAC アドレス制限を最大 5 つまで設定できます。
- `clear l2vpn mac address table` コマンドはサポートされていません。MAC アドレス テーブルは、接続回線インターフェイスまたはサブインターフェイスで `shut` または `no shutdown` が実行された場合、あるいは MAC エージング タイマーが期限切れになった場合にクリアされます。

設定例

EVPN MAC アドレス制限を設定するには、次の作業を実行します。

次の表に、設定する MAC アドレス制限のパラメータと値を示します。

パラメータ	値
MAC アドレス制限	50
MAC 制限アクション	limit, no-flood
MAC 通知	syslog および SNMP トラップ メッセージ
MAC 制限しきい値	80%

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group EVPN-BG-SH
Router(config-l2vpn-bg)# bridge-domain EVPN_2701
Router(config-l2vpn-bg-bd)# mac
Router(config-l2vpn-bg-bd-mac)# limit
Router(config-l2vpn-bg-bd-mac-limit)# maximum 50
Router(config-l2vpn-bg-bd-mac-limit)# action no-flood
Router(config-l2vpn-bg-bd-mac-limit)# notification both
```

```
Router(config-l2vpn-bg-bd-mac-limit)# exit
Router(config-l2vpn-bg-bd)# exit
Router(config-l2vpn-bg)# exit
Router(config-l2vpn)# mac limit threshold 80
Router(config-l2vpn)# commit
```

実行コンフィギュレーション

```
l2vpn
bridge group EVPN-BG-SH
  bridge-domain EVPN_2701
  mac
    limit
      maximum 50
      action no-flood
      notification both
    !
  !
!
mac limit threshold 80
commit
```

確認

EVPN MAC アドレス制限パラメータが前述の表のように設定されていることを確認します。

```
Router# show l2vpn bridge-domain bd-name EVPN_2701 detail
Legend: pp = Partially Programmed.
Bridge group: EVPN-BG-SH, bridge-domain: EVPN_2701, id: 25, state: up, ShgId: 0, MSTi:
0
  Coupled state: disabled
  VINE state: EVPN Native
  MAC learning: enabled
  MAC withdraw: enabled
    MAC withdraw for Access PW: enabled
    MAC withdraw sent on: bridge port up
    MAC withdraw relaying (access to access): disabled
  Flooding:
    Broadcast & Multicast: enabled
    Unknown unicast: enabled
  MAC aging time: 300 s, Type: inactivity
MAC limit: 50, Action: limit, no-flood, Notification: syslog, trap
MAC limit reached: no, threshold: 80%
  MAC port down flush: enabled
  MAC Secure: disabled, Logging: disabled
  Split Horizon Group: none
  Dynamic ARP Inspection: disabled, Logging: disabled
  IP Source Guard: disabled, Logging: disabled
  DHCPv4 Snooping: disabled
  DHCPv4 Snooping profile: none
  IGMP Snooping: disabled
  IGMP Snooping profile: none
  MLD Snooping profile: none
  Storm Control: disabled
  Bridge MTU: 1500
  MIB cvplsConfigIndex: 26
  Filter MAC addresses:
  P2MP PW: disabled
  Create time: 21/04/2019 16:28:05 (2d23h ago)
  No status change since creation
  ACs: 1 (1 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up), VNIs: 0 (0 up)
```

```

List of EVPNs:
EVPN, state: up
  evi: 6101
  XC ID 0x8000040c
  Statistics:
    packets: received 0 (unicast 0), sent 0
    bytes: received 0 (unicast 0), sent 0
    MAC move: 0
List of ACs:
AC: Bundle-Ether101.2701, state is up, active in RG-ID 101
  Type VLAN; Num Ranges: 1
  Rewrite Tags: [1000, 2000]
  VLAN ranges: [2701, 2701]
  MTU 9112; XC ID 0xa000060b; interworking none; MSTi 6
  MAC learning: enabled
  Flooding:
    Broadcast & Multicast: enabled
    Unknown unicast: enabled
  MAC aging time: 300 s, Type: inactivity
MAC limit: 50, Action: limit, no-flood, Notification: syslog, trap
MAC limit reached: no, threshold: 80%
  MAC port down flush: enabled
  MAC Secure: disabled, Logging: disabled
  Split Horizon Group: none
  Dynamic ARP Inspection: disabled, Logging: disabled
  IP Source Guard: disabled, Logging: disabled
  DHCPv4 Snooping: disabled
  DHCPv4 Snooping profile: none
  IGMP Snooping: disabled
  IGMP Snooping profile: none
  MLD Snooping profile: none
  Storm Control:
    Broadcast: enabled(160000 pps)
    Multicast: enabled(160000 pps)
    Unknown unicast: enabled(160000 pps)
  Static MAC addresses:
  Statistics:
    packets: received 0 (multicast 0, broadcast 0, unknown unicast 0, unicast 0),
sent 0
    bytes: received 0 (multicast 0, broadcast 0, unknown unicast 0, unicast 0), sent
0
    MAC move: 0
  Storm control drop counters:
    packets: broadcast 0, multicast 0, unknown unicast 0
    bytes: broadcast 0, multicast 0, unknown unicast 0
  Dynamic ARP inspection drop counters:
    packets: 0, bytes: 0
  IP source guard drop counters:
    packets: 0, bytes: 0
List of Access PWs:
List of VFIs:
List of Access VFIs:

```

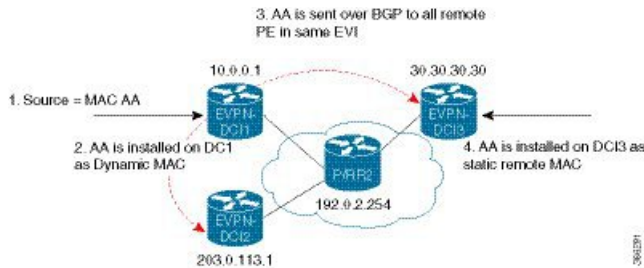
EVPN ソフトウェア MAC ラーニング

あるデバイス上で学習した MAC アドレスは、VLAN 内の別のデバイス上で学習されるか、配布されるようにする必要があります。EVPN ソフトウェア MAC ラーニング機能では、あるデバイス上で学習された MAC アドレスをネットワークに接続された別のデバイスに配布できます。MAC アドレスは、BGP を使用してリモートデバイスから学習されます。



- (注) デバイスには最大 128K の MAC アドレス エントリを含めることができます。デバイス上のブリッジドメインには最大 64K の MAC アドレス エントリを含めることができます。

図 21: EVPN ソフトウェア MAC ラーニング



上の図は、ソフトウェア MAC ラーニングのプロセスを示しています。次に、このプロセスに関わるステップを示します。

1. トラフィックは、ブリッジドメイン内の 1 つのポートに着信します。
2. 送信元 MAC アドレス (AA) は PE 上で学習され、ダイナミック MAC エントリとして格納されます。
3. MAC アドレス (AA) がタイプ 2 BGP ルー t に変換され、BGP を介して同じ EVI 内のすべてのリモート PE に送信されます。
4. MAC アドレス (AA) は、リモート MAC アドレスとして PE で更新されます。

EVPN ソフトウェア MAC ラーニングの設定

次の項では、EVPN ソフトウェア MAC ラーニングの設定方法について説明します。



- (注) ルータは、フロー認識型トランスポート (FAT) 擬似回線をサポートしていません。

```

/* Configure bridge domain. */

RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group EVPN_SH
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain EVPN_2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface TenGigE0/0/0/1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# exit
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface BundleEther 20.2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# storm-control broadcast pps 10000 ← Enabling
storm-control is optional
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# exit
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# evi 2001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-evi)# commit

```

```

/* Configure address family session in BGP. */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router bgp 200
RP/0/RSP0/CPU0:router(config-bgp)# bgp router-id 209.165.200.227
RP/0/RSP0/CPU0:router(config-bgp)# address-family l2vpn evpn

RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 200
RP/0/RSP0/CPU0:router(config-bgp-nbr)# description MPLSFACINGPEER
RP/0/RSP0/CPU0:router(config-bgp-nbr)# update-source Loopback 0
RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family l2vpn evpn

```

EVPN ソフトウェア MAC ラーニングでサポートされているモード

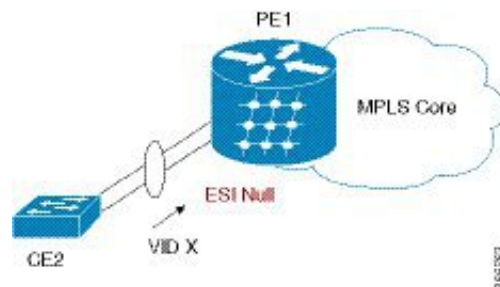
EVPN ソフトウェア MAC ラーニングでサポートされているモードは次のとおりです。

- シングル ホーム デバイス (SHD) またはシングル ホーム ネットワーク (SHN)
- デュアル ホーム デバイス (DHD) : オールアクティブ ロード バランシング

シングル ホーム デバイスまたはシングル ホーム ネットワーク モード

次の項では、EVPN ソフトウェア MAC ラーニング機能をシングル ホーム デバイスまたはシングル ホーム ネットワーク (SHD/SHN) モードで設定する方法について説明します。

図 22: 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

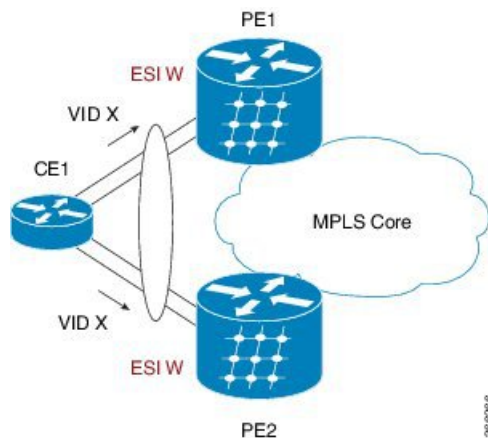
Ethernet Segment Id      Interface      Nexthops
-----
N/A                       Te0/4/0/10    20.20.20.20
.....
Topology :
Operational : SH
Configured : Single-active (AApS) (default)

```

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 23: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 Link Aggregation Control Protocol (LACP) bundle. */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether1 300
RP/0/RSP0/CPU0:router(config-if)# lacp switchover suppress-flaps 300
RP/0/RSP0/CPU0:router(config-if)# exit

/* Configure VLAN Header Rewrite.*/

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface bundle-Ether1.2001 l2transport
RP/0/RSP0/CPU0:router(config-if)# encapsulation dot1q 10
RP/0/RSP0/CPU0:router(config-if)# rewrite ingress tag pop 1 symmetric

```

実行コンフィギュレーション

```

l2vpn
bridge group EVPN_ALL_ACTIVE
bridge-domain EVPN_2001
interface Bundle-Ether1.2001
!
evi 2001
!
!
evpn
evi 2001
!
advertise-mac
!
interface bundle-ether1
ethernet-segment
identifier type 0 01.11.00.00.00.00.00.01
!
!
router bgp 200
bgp router-id 209.165.200.227
address-family l2vpn evpn
!
neighbor 10.10.10.10
remote-as 200
description MPLS-FACING-PEER
update-source Loopback0
address-family l2vpn evpn
!
interface Bundle-Ether1
lacp switchover suppress-flaps 300
load-interval 30
!
interface bundle-Ether1.2001 l2transport
encapsulation dot1q 2001
rewrite ingress tag pop 1 symmetric
!

```

確認

オールアクティブモードのデュアルホームデバイスのEVPNを確認します。

```
RP/0/RSP0/CPU0:router# show evpn ethernet-segment interface bundle-Ether 1 carvin$

Ethernet Segment Id      Interface  Nexthops
-----
0100.211b.fce5.df00.0b00 BE11      10.10.10.10
209.165.201.1
Topology :
Operational : MHN
Configured : All-active (AApF) (default)
Primary Services : Auto-selection
Secondary Services: Auto-selection
Service Carving Results:
Forwarders : 4003
Elected : 2002
EVI E : 2000, 2002, 36002, 36004, 36006, 36008
.....
Not Elected : 2001
EVI NE : 2001, 36001, 36003, 36005, 36007, 36009

MAC Flushing mode : Invalid

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

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: TenGigE0/0/0/1, 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 Te0/0/0/1 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 0/0/0/1 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                N/A         11 Jan 14:37:22
N/A <-- local dynamic
00bb.2001.0001   dynamic  Te0/0/0/2                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 000a.2002.1555 20.1.5.55 TenGigE0/0/0/2 34203 <-- local MAC
```

```
RP/0/RSP0/CPU0:router# RP/0/RSP0/CPU0:router# show evpn evi vpn-id 2001 mac 00a9.2002.0001 detail
```

EVI	MAC address	IP address	NextHop	Label
2001	00a9.2002.0001	::	10.10.10.10	34226
2001	00a9.2002.0001	::	209.165.201.30	34202

```
Ethernet Tag : 0
```

```
Multi-paths Resolved : True <--- aliasing to two remote PE with All-Active load balancing
```

```
Static : No
```

```
Local Ethernet Segment : N/A
```

```
Remote Ethernet Segment : 0100.211b.fce5.df00.0b00
```

```
Local Sequence Number : N/A
```

```
Remote Sequence Number : 0
```

```
Local Encapsulation : N/A
```

```
Remote Encapsulation : MPLS
```

EVPNに関連付けられているBGPルートをブリッジドメインフィルタを使用して確認します。

```
RP/0/RSP0/CPU0:router# show bgp l2vpn evpn bridge-domain EVPN_2001 route-type 2
```

```
*> [2][0][48][00bb.2001.0001][0]/104
      0.0.0.0 0 i <----- locally learnt MAC
*>i[2][0][48][00a9.2002.00be][0]/104
      10.10.10.10 100 0 i <----- remotely learnt MAC
* i 209.165.201.30 100 0 i
```

EVPN アウトオブサービス

EVPN アウト オブ サービス機能では、Link Aggregation Control Protocol (LACP) を設定したイーサネットセグメントに含まれているバンドルインターフェイスの状態を制御することができます。この機能を使用すると、ノードをアウト オブ サービス (OOS) に移行させることができます。プロバイダー エッジ (PE) のすべてのバンドルを手動でシャットダウンする必要はありません。

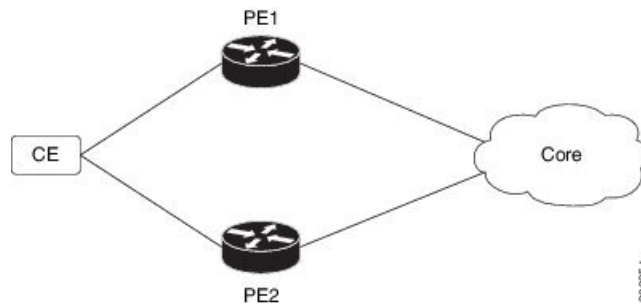
cost-out コマンドを使用してノード上のイーサネット VPN (EVPN) のイーサネットセグメントに属するすべてのバンドルインターフェイスをダウンさせます。イーサネット A-D のイーサネットセグメント (ES EAD) ルートは、バンドルをシャットダウンする前に撤回されます。PEは接続されているカスタマーエッジ (CE) デバイスにシグナリングし、対応するバンドルメンバーをダウンさせます。こうすることで、トラフィックを中断させることなく、トラフィックをこの PE ノードからそらしめます。CE からイーサネットセグメントへのトラフィックは、マルチホーミング環境内のピア PE へと方向付けられます。



(注) EVPN のコストアウトは、手動で設定された ESI でのみサポートされます。

次に、CE が PE1 と PE2 に接続されているトポロジを示します。PE1 に `cost-out` コマンドを設定すると、イーサネットセグメント上のすべてのバンドルインターフェイスがダウンします。また、CE 上の対応するバンドルメンバーもダウンします。したがって、このイーサネットセグメントのトラフィックは CE から PE2 へと送信されるようになります。

図 24: 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イスと CE 上の対応するバンドルメンバーが起動します。

ノードがコストアウト状態にある場合に新しいバンドルイーサネットセグメントを追加するとそのバンドルがダウンします。同様に、バンドルイーサネットセグメントを削除するとそのバンドルは起動します。

リロード時に指定した時間が経過した後にノードをサービス状態に戻すには、`startup-cost-in` コマンドを使用します。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 対応 CFM のサポート

イーサネット接続障害管理（CFM）はサービスレベル OAM プロトコルの 1 つで、VLAN ごとにエンドツーエンドのイーサネットサービスをモニタリングおよびトラブルシューティングするためのツールとなります。これには、予防的な接続モニタリング、障害検証、および障害分離の機能が含まれています。CFM は EVPN ネットワークに導入できます。EVPN ネットワークで CFM を使用して、ノード間の接続をモニタできます。

制約事項

EVPN 対応 CFM は、次の制限の下でサポートされています。

- アクティブ-アクティブ マルチホーミングのシナリオでは、マルチホーム CE デバイスとそれらに接続している PE デバイスとの間の接続をモニタする場合、CFM は CE と PE 間の個別のリンク間でのみ使用できます。CE デバイスと PE デバイス間のバンドルで CFM の使用を試みると、シーケンス番号エラーが発生し、統計情報が不正確になります。
- ループバックおよびリンクトレースの結果に副作用が生じる可能性があります。ループバックまたはリンクトレースのいずれかで同じインスタンスに対して複数の結果が報告されたり、同じ 2 つのエンドポイント間にあるループバックとリンクトレースの連続するインスタンスで異なる結果が生じたりする場合があります。

イーサネット セグメント単位の EVPN 複数サービス

イーサネットセグメント単位の EVPN 複数サービス機能を使用すると、単一のイーサネットセグメント（ES）で複数のサービスを設定できます。複数の ES で複数のサービスを設定する代わりに、1 つの ES で複数のサービスを設定できます。

単一のイーサネットバンドルで次のサービスを設定できます。サブインターフェイスごとにサービスを 1 つずつ設定できます。

- フレキシブルクロスコネクト（FXC）サービス。VLAN 非認識型、VLAN 認識型、およびローカルスイッチングモードをサポートしています。
詳細については、『*L2VPN and Ethernet Services Configuration Guide for Cisco NCS 540 Series Routers*』の「*Configure Point-to-Point Layer 2 Services*」の章を参照してください。
- EVPN-VPWS Xconnect サービス

詳細については、『*L2VPN and Ethernet Services Configuration Guide for Cisco NCS 540 Series Routers*』の「*EVPN Virtual Private Wire Service (VPWS)*」の章を参照してください。

- EVPN Integrated Routing and Bridging (IRB)

詳細については、『*L2VPN and Ethernet Services Configuration Guide for Cisco NCS 540 Series Routers*』の「*Configure EVPN IRB*」の章を参照してください。

- ネイティブ EVPN

詳細については、『*L2VPN and Ethernet Services Configuration Guide for Cisco NCS 540 Series Routers*』の「*EVPN Features*」の章を参照してください。

これらのサービスはすべて、オールアクティブのマルチホーミングのシナリオでのみサポートされます。

イーサネット セグメント単位の EVPN 複数サービスの設定

イーサネットバンドルインターフェイス 22001 を介して 2 つのプロバイダーエッジ (PE) デバイスに接続しているカスタマーエッジ (CE) デバイスを考えてみます。バンドルイーサネットサブインターフェイスで複数のサービスを設定します。

設定例

Bundle-Ether22001 ES を考慮し、サブインターフェイスで複数のサービスを設定します。

```
/* Configure attachment circuits */
Router# configure
Router(config)# interface Bundle-Ether22001.12 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 12
Router(config-l2vpn-subif)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether22001.13 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 13
Router(config-l2vpn-subif)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether22001.14 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 14
Router(config-l2vpn-subif)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether22001.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 1
Router(config-l2vpn-subif)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether22001.2 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 2
Router(config-l2vpn-subif)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether22001.3 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 3
Router(config-l2vpn-subif)# exit
Router(config-l2vpn)# exit
Router(config)# interface Bundle-Ether22001.4 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 4
Router(config-l2vpn-subif)# exit
```

```

Router(config-l2vpn)# exit

/*Configure VLAN Unaware FXC Service */
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-unaware fxc_mh1
Router(config-l2vpn-fxs-vu)# interface Bundle-Ether22001.1
Router(config-l2vpn-fxs-vu)# interface Bundle-Ether22001.2
Router(config-l2vpn-fxs-vu)# interface Bundle-Ether22001.3
Router(config-l2vpn-fxs-vu)# neighbor evpn evi 21006 target 22016
Router(config-l2vpn-fxs-vu)# commit

/* Configure VLAN Aware FXC Service */
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-aware evi 24001
Router(config-l2vpn-fxs-vu)# interface Bundle-Ether22001.12
Router(config-l2vpn-fxs-vu)# interface Bundle-Ether22001.13
Router(config-l2vpn-fxs-vu)# interface Bundle-Ether22001.14
Router(config-l2vpn-fxs-vu)# commit

/* Configure Local Switching - Local switching is supported only on VLAN-aware FXC */
PE1
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-aware evi 31400
Router(config-l2vpn-fxs)# interface Bundle-Ether22001.1400
Router(config-l2vpn-fxs)# interface Bundle-Ether23001.1400
Router(config-l2vpn-fxs)# commit
Router(config-l2vpn-fxs)# exit
PE2
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-aware evi 31401
Router(config-l2vpn-fxs)# interface Bundle-Ether22001.1401
Router(config-l2vpn-fxs)# interface Bundle-Ether23001.1401
Router(config-l2vpn-fxs)# commit
Router(config-l2vpn-fxs)# exit

/* Configure EVPN-VPWS xconnect service and native EVPN with IRB */

Router# configure
Router(config)# interface Bundle-Ether22001.11 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 11
Router(config-l2vpn-subif)# rewrite ingress tag pop 2 symmetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit

Router# configure
Router(config)# interface Bundle-Ether22001.21 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1 second-dot1q 21
Router(config-l2vpn-subif)# rewrite ingress tag pop 2 symmetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit

Router# configure
Route(config)# l2vpn
Router(config-l2vpn)# xconnect group xg22001
Router(config-l2vpn-xc)# p2p evpn-vpws-mclag-22001
Router(config-l2vpn-xc-p2p)# interface Bundle-Ether22001.11
Router(config-l2vpn-xc-p2p)# neighbor evpn evi 22101 target 220101 source 220301
Router(config-l2vpn-xc-p2p)# commit
Router(config-l2vpn-xc-p2p)# exit

Router # configure

```

```

Router (config)# l2vpn
Router (config-l2vpn)# bridge group native_evpn1
Router (config-l2vpn-bg)# bridge-domain bd21
Router (config-l2vpn-bg-bd)# interface Bundle-Ether22001.21
Router (config-l2vpn-bg-bd-ac)# routed interface BVI21
Router (config-l2vpn-bg-bd-bvi)# evi 22021
Router (config-l2vpn-bg-bd-bvi)# commit
Router (config-l2vpn-bg-bd-bvi)# exit

/* Configure Native EVPN */
Router # configure
Router (config)# evpn
Router (config-evpn)# interface Bundle-Ether22001
Router (config-evpn-ac)# ethernet-segment identifier type 0 ff.ff.ff.ff.ff.ff.ff.00
Router (config-evpn-ac-es)# bgp route-target 2200.0001.0001
Router (config-evpn-ac-es)# exit
Router (config-evpn)# evi 24001
Router (config-evpn-evi)# bgp
Router (config-evpn-evi-bgp)# route-target import 64:24001
Router (config-evpn-evi-bgp)# route-target export 64:24001
Router (config-evpn-evi-bgp)# exit
Router (config-evpn-evi)# exit
Router (config-evpn)# evi 21006
Router (config-evpn-evi)# bgp
Router (config-evpn-evi-bgp)# route-target route-target 64:10000
Router (config-evpn-evi-bgp)# exit
Router (config-evpn-evi)# exit
Router (config-evpn)# evi 22101
Router (config-evpn-evi)# bgp
Router (config-evpn-evi-bgp)# route-target import 64:22101
Router (config-evpn-evi-bgp)# route-target export 64:22101
Router (config-evpn-evi-bgp)# exit
Router (config-evpn-evi)# exit
Router (config-evpn)# evi 22021
Router (config-evpn-evi)# bgp
Router (config-evpn-evi-bgp)# route-target import 64: 22021
Router (config-evpn-evi-bgp)# route-target export 64: 22021
Router (config-evpn-evi-bgp)# exit
Router (config-evpn-evi)# exit
Router (config-evpn-evi)# advertise-mac
Router (config-evpn-evi)# exit
Router (config-evpn)# evi 22022
Router (config-evpn-evi)# bgp
Router (config-evpn-evi-bgp)# route-target import 64: 22022
Router (config-evpn-evi-bgp)# route-target export 64: 22022
Router (config-evpn-evi-bgp)# exit
Router (config-evpn-evi)# advertise-mac
Router (config-evpn-evi)# commit
Router (config-evpn-evi)# exit

```

実行コンフィギュレーション

```

/* Configure attachment circuits */
interface Bundle-Ether22001.12 l2transport
encapsulation dot1q 1 second-dot1q 12
!
interface Bundle-Ether22001.13 l2transport
encapsulation dot1q 1 second-dot1q 13
!
interface Bundle-Ether22001.14 l2transport

```

```

encapsulation dot1q 1 second-dot1q 14
!
interface Bundle-Ether22001.1 l2transport
 encapsulation dot1q 1 second-dot1q 1
!
interface Bundle-Ether22001.2 l2transport
 encapsulation dot1q 1 second-dot1q 2
!
interface Bundle-Ether22001.3 l2transport
 encapsulation dot1q 1 second-dot1q 3
!
interface Bundle-Ether22001.4 l2transport
 encapsulation dot1q 1 second-dot1q 4

/*Configure VLAN Unaware FXC Service */
flexible-xconnect-service vlan-unaware fxc_mh1
 interface Bundle-Ether22001.1
 interface Bundle-Ether22001.2
 interface Bundle-Ether22001.3
 neighbor evpn evi 21006 target 22016
!
/*Configure VLAN Aware FXC Service */
l2vpn
 flexible-xconnect-service vlan-aware evi 24001
 interface Bundle-Ether22001.12
 interface Bundle-Ether22001.13
 interface Bundle-Ether22001.14

/* Configure Local Switching */
flexible-xconnect-service vlan-aware evi 31400
 interface Bundle-Ether22001.1400
 interface Bundle-Ether23001.1400
!
flexible-xconnect-service vlan-aware evi 31401
 interface Bundle-Ether22001.1401
 interface Bundle-Ether23001.1401
!

/* Configure EVPN-VPWS xconnect service and native EVPN with IRB */
interface Bundle-Ether22001.11 l2transport
 encapsulation dot1q 1 second-dot1q 11
 rewrite ingress tag pop 2 symmetric
!
interface Bundle-Ether22001.21 l2transport
 encapsulation dot1q 1 second-dot1q 21
 rewrite ingress tag pop 2 symmetric
!
!
l2vpn
xconnect group xg22001
p2p evpn-vpws-mclag-22001
 interface Bundle-Ether22001.11
 neighbor evpn evi 22101 target 220101 source 220301
!
bridge group native_evpn1
 bridge-domain bd21
 interface Bundle-Ether22001.21
 routed interface BVI21
 evi 22021
!
/* Configure Native EVPN */
Evpn
 interface Bundle-Ether22001
 ethernet-segment identifier type 0 ff.ff.ff.ff.ff.ff.ff.ff.00

```

```

bgp route-target 2200.0001.0001
!
evi 24001
  bgp
    route-target import 64:24001
    route-target export 64:24001
  !
evi 21006
  bgp
    route-target 64:100006
  !
evi 22101
  bgp
    route-target import 64:22101
    route-target export 64:22101
  !
evi 22021
  bgp
    route-target import 64:22021
    route-target export 64:22021
  !
  advertise-mac
!
evi 22022
  bgp
    route-target import 64:22022
    route-target export 64:22022
  !
  advertise-mac
!

```

確認

各サービスがサブインターフェイスで設定されているかどうかを確認します。

```

Router# show l2vpn xconnect summary
Number of groups: 6
Number of xconnects: 505 Up: 505 Down: 0 Unresolved: 0 Partially-programmed: 0
AC-PW: 505 AC-AC: 0 PW-PW: 0 Monitor-Session-PW: 0
Number of Admin Down segments: 0
Number of MP2MP xconnects: 0
  Up 0 Down 0
Advertised: 0 Non-Advertised: 0

```

```

Router# show l2vpn xconnect-service summary
Number of flexible xconnect services: 74
Up: 74

```

```

Router# show l2vpn flexible-xconnect-service name fxc_mh1
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed
Flexible XConnect Service Segment
Name      ST  Type  Description  ST
-----
fxc_mh1  UP  AC:   BE22001.1   UP
          AC:   BE22001.2   UP
          AC:   BE22001.3   UP
-----

```

```

Router# show l2vpn flexible-xconnect-service evi 24001
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

```

```

Flexible XConnect Service Segment
Name      ST  Type  Description  ST
-----
evi:24001 UP  AC:   BE22001.11  UP
          AC:   BE22001.12  UP
          AC:   BE22001.13  UP
          AC:   BE22001.14  UP
-----

Router# show l2vpn xconnect group xg22001 xc-name evpn-vpws-mclag-22001
Fri Sep 1 17:28:58.259 UTC
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
SB = Standby, SR = Standby Ready, (PP) = Partially Programmed
XConnect
Group      Name                               ST      Segment 1      Segment 2
          Name                               ST      Description ST      Description
-----
xg22001   evpn-vpws-mclag-22001             UP      BE22001.101   UP      EVPN 22101, 220101, 64.1.1.6
          UP
-----

```

関連コマンド

- evpn
- evi
- ethernet-segment
- advertise-mac
- show evpn ethernet-segment
- show evpn evi
- show evpn summary
- show l2vpn xconnect summary
- show l2vpn flexible-xconnect-service
- show l2vpn xconnect group

EVPN MPLS と VPLS のシームレスな統合

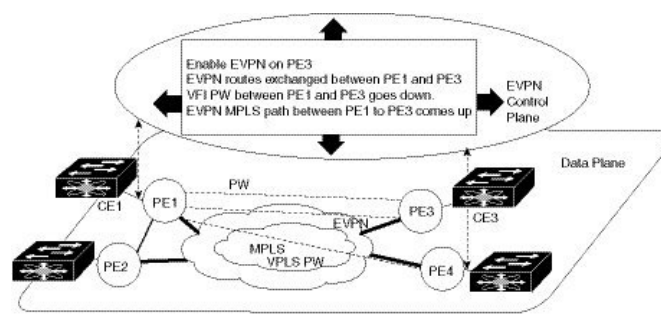
EVPN MPLS と VPLS のシームレスな統合により、同じ VPN インスタンスに対して EVPN と VPLS を実行する PE ノードの共存が可能になります。VPLS またはレガシー ネットワークを、サービス の中断なしで次世代の EVPN ネットワークにアップグレードできます。選択したすべての VPLS プロバイダーエッジ (PE) ノードに、EVPN サービスを同時に導入できます。ただし、トラフィックの中断を回避するため、既存の VPLS 対応 PE で EVPN サービスを 1 つずつプロビジョニングします。

シームレスな統合による VPLS ネットワークの EVPN ネットワークへの移行

EVPN ネットワークでは、VPN インスタンスは EVPN インスタンス ID (EVI) によって識別されます。他の L2VPN テクノロジーと同様に、EVPN インスタンスもルートターゲットおよびルート識別子に関連付けられています。MAC をデータプレーンで学習する（「フラッディングと学習の技術」を使用して学習する）従来の VPLS とは異なり、EVPN ではコントロールプレーンを使用して MAC を学習し伝播します。EVPN では、MAC ルートは MP BGP プロトコルによって伝送されます。EVPN 対応 PE では、PE のルートターゲット (RT) が一致した場合にのみ、PE が MAC ルートをラベルとともにそれぞれの EVPN 転送テーブルにインポートします。EVPN PE ルータは、同じ VPN インスタンスで VPLS および EVPN L2 ブリッジングを実行する機能を備えています。EVPN と BGP-AD PW の両方が VPN インスタンスで設定されている場合、EVPN PE は、BGP VPLS 自動検出 (AD) ルートと、BGP EVPN 包括マルチキャストルート (タイプ 3) を、特定の VPN インスタンスにアドバタイズします。ルートタイプ 3 は入力複製マルチキャストルートと呼ばれ、ブロードキャスト、未知のユニキャスト、およびマルチキャスト (BUM) トラフィックの送信に使用されます。その他のリモート PE は、送信側の PE RT が設定済みの RT と一致する場合にのみ、同じ VPN インスタンスに対してタイプ 3 ルートをインポートします。したがって、これらのルート交換の最後に、EVPN 対応 PE は、VPN インスタンスにある他のすべての PE とそれらの関連機能を検出します。PE が自身の BUM トラフィックを他の PE に送信するために使用するタイプ 3 ルートでは、同じ RT を持つ PE が BUM トラフィックを受信することが保証されます。EVPN は、タイプ 2 ルートを使用してカスタマー MAC アドレスをアドバタイズします。

EVPN MPLS と VPLS のシームレスな統合により、ネットワーク サービスを中断することなく、VPLS PE ルータを EVPN に 1 つずつアップグレードすることができます。PE1、PE2、PE3、および PE4 が VPLS PW を使用してフルメッシュ ネットワークで相互接続されている次のトポロジを考えてみます。

図 25: EVPN MPLS と VPLS のシームレスな統合



EVPN サービスは、一度に 1 つの PE ノードずつ、ネットワークに導入できます。VPLS サービスの VPN インスタンスで EVPN を有効にすることによって、VPLS から EVPN への移行が PE1 で開始されます。EVPN が有効になるとすぐに、PE1 は他の PE ノードへの EVPN 包括マルチキャストルートのアドバタイズを開始します。PE1 は他の PE ノードからの包含マルチキャストルートを受信しないため、PE1 と他の PE ノード間の VPLS 擬似回線はアクティブなままです。PE1 は、VPLS 擬似回線を使用してトラフィックの転送を維持します。同時に、PE1 は EVPN ルートタイプ 2 を使用して CE1 から学習したすべての MAC アドレスをアドバタイズし

まず、2 番目のステップでは、EVPN が PE3 で有効になっています。PE3 は、他の PE ノードへの包含マルチキャストルートのアドバタイズを開始します。PE1 と PE3 の両方が EVPN ルートを介して互いを検出します。その結果、PE1 と PE3 は両者間の擬似回線をシャットダウンします。EVPN サービスが、PE1 と PE3 の間で VPLS サービスの代わりとなります。この段階では、PE1 は PE2 と PE4 を使用して VPLS サービスを実行し続け、同じ VPN インスタンスで PE3 を使用して EVPN サービスを開始します。このことを、EVPN と VPLS のシームレスな統合と呼びます。VPLS から EVPN への移行は残りの PE ノードに対して続けられます。最終的に、4 つすべての PE ノードが EVPN サービスで有効になります。VPLS サービスがネットワーク内の EVPN サービスに完全に置き換えられます。すべての VPLS 擬似回線がシャットダウンされます。

既存の VPLS ネットワークでの EVPN の設定

既存の VPLS ネットワークで EVPN を設定するには、次の作業を実行します。

- L2VPN EVPN アドレスファミリの設定
- EVPN コンフィギュレーションモードで、EVI と対応する BGP ルートターゲットを設定します。
- ブリッジドメインでの EVI の設定

さまざまな VPLS ベース ネットワークを EVPN に移行する方法については、[L2VPN ブリッジドメインでの EVI の設定 \(172 ページ\)](#) を参照してください。

L2 EVPN アドレスファミリの設定

BGP と参加ネイバーの両方で EVPN アドレス ファミリを有効にするには、次の作業を実行します。

設定例

```
Router# configure
Router(config)#router bgp 65530
Router(config-bgp)#nsr
Router(config-bgp)#bgp graceful-restart
Router(config-bgp)#bgp router-id 200.0.1.1
Router(config-bgp)#address-family l2vpn evpn
Router(config-bgp-af)#exit
Router(config-bgp)#neighbor 200.0.4.1
Router(config-bgp-nbr)#remote-as 65530
Router(config-bgp-nbr)#update-source Loopback0
Router(config-bgp-nbr)#address-family l2vpn evpn
Router(config-bgp-nbr-af)#commit
```

実行コンフィギュレーション

```
configure
router bgp 65530
```



```
nsr
bgp graceful-restart
bgp router-id 200.0.1.1
address-family l2vpn evpn
!
neighbor 200.0.4.1
remote-as 65530
update-source Loopback0
address-family l2vpn evpn
!
!
```

EVPN コンフィギュレーションモードでの EVI と対応する BGP ルートターゲットの設定

EVI を設定し、対応する BGP ルートターゲットを定義するには、次の作業を実行します。また、`advertise-mac` を設定します。設定しないと MAC ルート（タイプ 2）がアドバタイズされません。

設定例

```
Router# configure
Router(config)#evpn
Router(config-evpn)#evi i
Router(config-evpn-evi-bgp)#bgp
Router(config-evpn-evi-bgp)#table-policy spp-basic-6
Router(config-evpn-evi-bgp)#route-target import 100:6005
Router(config-evpn-evi-bgp)#route-target export 100:6005
Router(config-evpn-evi-bgp)#exit
Router(config-evpn-evi)#advertise-mac
Router(config-evpn-evi)#commit
```

実行コンフィギュレーション

```
configure
evpn
evi
  bgp
    table-policy spp-basic-6
    route-target import 100:6005
    route-target export 100:6005
  !
  advertise-mac
  !
!
```

ブリッジドメインでの EVI の設定

対応する L2VPN ブリッジドメインで EVI を設定するには、次の作業を実行します。

設定例

```
Router# configure
Router(config)#l2vpn
Router(config-l2vpn)#bridge group bg1
Router(config-l2vpn-bg)#bridge-domain bd1
Router(config-l2vpn-bg-bd)#interface GigabitEthernet0/0/0/0
Router(config-l2vpn-bg-bd-ac)#exit
Router(config-l2vpn-bg-bd)#evi 1
Router(config-l2vpn-bg-bd-evi)#exit
Router(config-l2vpn-bg-bd)#vfi v1
Router(config-l2vpn-bg-bd-vfi)#neighbor 10.1.1.2 pw-id 1000
Router(config-l2vpn-bg-bd-vfi-pw)#mpls static label local 20001 remote 10001
Router(config-l2vpn-bg-bd-vfi-pw)#commit
```

実行コンフィギュレーション

```
configure
l2vpn
  bridge group bg1
  bridge-domain bd1
  interface GigabitEthernet0/0/0/0
  !
  evi 1
  !
  vfi v1
  neighbor 10.1.1.2 pw-id 1000
  mpls static label local 20001 remote 10001
  !
  evi 1
  !
```

L2VPN ブリッジドメインでの EVI の設定

次の例は、さまざまな VPLS ベース ネットワークの L2VPN ブリッジドメインでの EVI 設定を示しています。

MPLS スタティック ラベルをベースとする VPLS

```
l2vpn
  bridge group bg1
  bridge-domain bd-1-1
  interface GigabitEthernet0/0/0/0
  !
  vfi vfi-1-1
  neighbor 200.0.2.1 pw-id 1200001
  mpls static label local 20001 remote 10001
  !
  neighbor 200.0.3.1 pw-id 1300001
  mpls static label local 30001 remote 10001
  !
  neighbor 200.0.4.1 pw-id 1400001
  mpls static label local 40001 remote 10001
  !
```

```
!  
evi 1  
!
```

自動検出 BGP および BGP シグナリングをベースとする VPLS

```
l2vpn  
bridge group bg1  
bridge-domain bd-1-2  
  interface GigabitEthernet0/0/0/2  
  !  
  vfi vfi-1-2  
  vpn-id 2  
  autodiscovery bgp  
  rd 101:2  
  route-target 65530:200  
  signaling-protocol bgp  
  ve-id 11  
  ve-range 16  
  !  
  !  
evi 2  
!
```

ターゲット LDP をベースとする VPLS

```
bridge-domain bd-1-4  
  interface GigabitEthernet0/0/0/4  
  !  
  vfi vfi-1-4  
  neighbor 200.0.2.1 pw-id 1200004  
  !  
  neighbor 200.0.3.1 pw-id 1300004  
  !  
  neighbor 200.0.4.1 pw-id 1400004  
  !  
evi 3  
!
```

EVPN 設定の確認

EVPN の設定と MAC のアドバタイズメントを確認するには、次のコマンドを使用します。EVPN のステータス、AC のステータス、および VFI のステータスを確認します。

- show l2vpn bridge-domain
- show evpn summary
- show bgp rt l2vpn evpn
- show evpn evi
- show l2route evpn mac all

```
Router#show l2vpn bridge-domain bd-name bd-1-1  
Mon Feb 20 21:03:40.244 EST
```

```

Legend: pp = Partially Programmed.
Bridge group: bgl, bridge-domain: bd-1-1, id: 0, state: up, ShgId: 0, MSTi: 0
Aging: 300 s, MAC limit: 4000, Action: none, Notification: syslog
Filter MAC addresses: 0
ACs: 1 (1 up), VFIs: 1, PWs: 3 (2 up), PBBs: 0 (0 up), VNIs: 0 (0 up)
List of EVPNs:
  EVPN, state: up
List of ACs:
  Gi0/2/0/0.1, state: up, Static MAC addresses: 0, MSTi: 2
List of Access PWs:
List of VFIs:
  VFI vfi-1-1 (up)
    Neighbor 200.0.2.1 pw-id 1200001, state: up, Static MAC addresses: 0
    Neighbor 200.0.3.1 pw-id 1300001, state: down, Static MAC addresses: 0
    Neighbor 200.0.4.1 pw-id 1400001, state: up, Static MAC addresses: 0
  List of Access VFIs:
When PEs are evpn enabled, pseudowires that are associated with that BD will be brought
down. The VPLS BD pseudowires are always up.

```

EVI の設定済みのローカルおよびリモート MAC ルートのうちアドバタイズされたものの数を確認します。

```

Router#show evpn summary
Mon Feb 20 21:05:16.755 EST
-----
Global Information
-----
Number of EVIs                : 6
Number of Local EAD Entries   : 0
Number of Remote EAD Entries  : 0
Number of Local MAC Routes    : 4
      MAC                      : 4
      MAC-IPv4                 : 0
      MAC-IPv6                 : 0
Number of Local ES:Global MAC : 1
Number of Remote MAC Routes   : 0
      MAC                      : 0
      MAC-IPv4                 : 0
      MAC-IPv6                 : 0
Number of Remote SOO MAC Routes : 0
Number of Local IMCAST Routes : 4
Number of Remote IMCAST Routes : 4
Number of Internal Labels     : 0
Number of ES Entries          : 1
Number of Neighbor Entries    : 4
EVPN Router ID                : 200.0.1.1
BGP ASN                       : 65530
PBB BSA MAC address           : 0026.982b.c1e5
Global peering timer          :      3 seconds
Global recovery timer         :     30 seconds

```

EVPN ルートターゲットを確認します。

```

Router#show bgp rt l2vpn evpn
Mon Feb 20 21:06:18.882 EST
EXTCOMM      IMP/EXP
RT:65530:1   1 / 1
RT:65530:2   1 / 1
RT:65530:3   1 / 1
RT:65530:4   1 / 1
Processed 4 entries

```

```
Locally learnt MAC routes can be viewed by forwarding table
show l2vpn forwarding bridge-domain mac-address location 0/0/cpu0
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location <r/s/i>
```

Mac Address	Type	Learned from/Filtered on	LC learned	Resync Age/Last Change	Mapped to
0033.0000.0001	dynamic	Gi0/2/0/0.1	N/A	20 Feb 21:06:59	N/A
0033.0000.0002	dynamic	Gi0/2/0/0.2	N/A	20 Feb 21:06:59	N/A
0033.0000.0003	dynamic	Gi0/2/0/0.3	N/A	20 Feb 21:04:29	N/A
0033.0000.0004	dynamic	Gi0/2/0/0.4	N/A	20 Feb 21:06:59	N/A

```
The remote routes learned via evpn enabled BD
show l2vpn forwarding bridge-domain mac-address location 0/0$
To Resynchronize MAC table from the Network Processors, use the command...
l2vpn resynchronize forwarding mac-address-table location <r/s/i>
```

Mac Address	Type	Learned from/Filtered on	LC learned	Resync Age/Last Change	Mapped to
0033.0000.0001	EVPN	BD id: 0	N/A	N/A	N/A
0033.0000.0002	EVPN	BD id: 1	N/A	N/A	N/A
0033.0000.0003	EVPN	BD id: 2	N/A	N/A	N/A
0033.0000.0004	EVPN	BD id: 3	N/A	N/A	N/A

特定の VPN インスタンスに関係のある EVPN MAC ルートを確認します。

```
Router#show evpn evi vpn-id 1 mac
Mon Feb 20 21:36:23.574 EST
```

EVI Label	MAC address	IP address	NextHop
1 45106	0033.0000.0001	::	200.0.1.1

L2 ルーティングを確認します。

```
Router#show l2route evpn mac all
Mon Feb 20 21:39:43.953 EST
Topo ID Mac Address Prod Next Hop(s)
```

0	0033.0000.0001	L2VPN	200.0.1.1/45106/ME
1	0033.0000.0002	L2VPN	200.0.1.1/45108/ME
2	0033.0000.0003	L2VPN	200.0.1.1/45110/ME
3	0033.0000.0004	L2VPN	200.0.1.1/45112/ME

EVPN ルート タイプ 2 ルートを確認します。

```
Router#show bgp l2vpn evpn route-type 2
Mon Feb 20 21:43:23.616 EST
```

```

BGP router identifier 200.0.3.1, local AS number 65530
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 21
BGP NSR Initial initsync version 1 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
                i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network        Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 200.0.1.1:1
*>i[2][0][48][0033.0000.0001][0]/104
                200.0.1.1                100      0 i
Route Distinguisher: 200.0.1.1:2
*>i[2][0][48][0033.0000.0002][0]/104
                200.0.1.1                100      0 i
Route Distinguisher: 200.0.1.1:3
*>i[2][0][48][0033.0000.0003][0]/104
                200.0.1.1                100      0 i
Route Distinguisher: 200.0.1.1:4
*>i[2][0][48][0033.0000.0004][0]/104
                200.0.1.1                100      0 i
Route Distinguisher: 200.0.3.1:1 (default for vrf bd-1-1)
*>i[2][0][48][0033.0000.0001][0]/104
                200.0.1.1                100      0 i
Route Distinguisher: 200.0.3.1:2 (default for vrf bd-1-2)
*>i[2][0][48][0033.0000.0002][0]/104
                200.0.1.1                100      0 i
Route Distinguisher: 200.0.3.1:3 (default for vrf bd-1-3)
*>i[2][0][48][0033.0000.0003][0]/104
                200.0.1.1                100      0 i
Route Distinguisher: 200.0.3.1:4 (default for vrf bd-1-4)
*>i[2][0][48][0033.0000.0004][0]/104
                200.0.1.1                100      0 i

Processed 8 prefixes, 8 paths

```

包含マルチキャストルートとルートタイプ3ルートを確認します。

```

Router#show bgp l2vpn evpn route-type 3
Mon Feb 20 21:43:33.970 EST
BGP router identifier 200.0.3.1, local AS number 65530
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0   RD version: 0
BGP main routing table version 21
BGP NSR Initial initsync version 1 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
                i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network        Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 200.0.1.1:1
*>i[3][0][32][200.0.1.1]/80
                200.0.1.1                100      0 i
Route Distinguisher: 200.0.1.1:2
*>i[3][0][32][200.0.1.1]/80

```

```

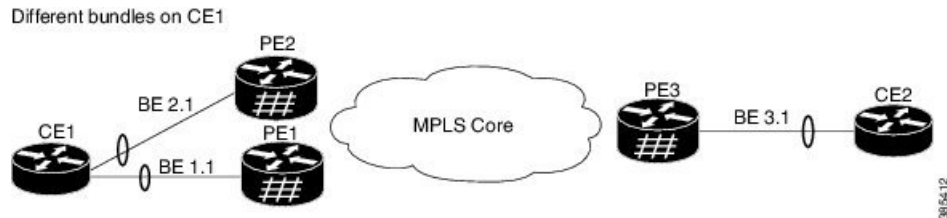
                200.0.1.1                100      0 i
Route Distinguisher: 200.0.1.1:3
*>i[3][0][32][200.0.1.1]/80
                200.0.1.1                100      0 i
Route Distinguisher: 200.0.1.1:4
*>i[3][0][32][200.0.1.1]/80
                200.0.1.1                100      0 i
Route Distinguisher: 200.0.3.1:1 (default for vrf bd-1-1)
*>i[3][0][32][200.0.1.1]/80
                200.0.1.1                100      0 i
*> [3][0][32][200.0.3.1]/80
                0.0.0.0                  0 i
Route Distinguisher: 200.0.3.1:2 (default for vrf bd-1-2)
*>i[3][0][32][200.0.1.1]/80
                200.0.1.1                100      0 i
*> [3][0][32][200.0.3.1]/80
                0.0.0.0                  0 i
Route Distinguisher: 200.0.3.1:3 (default for vrf bd-1-3)
*>i[3][0][32][200.0.1.1]/80
                200.0.1.1                100      0 i
*> [3][0][32][200.0.3.1]/80
                0.0.0.0                  0 i
Route Distinguisher: 200.0.3.1:4 (default for vrf bd-1-4)
*>i[3][0][32][200.0.1.1]/80
                200.0.1.1                100      0 i
*> [3][0][32][200.0.3.1]/80
                0.0.0.0                  0 i

```

EVPN シングルアクティブ マルチホーミング

EVPN シングルアクティブマルチホーミング機能はシングルアクティブ冗長モードをサポートしています。シングルアクティブモードでは、PE ノードは EVPN サービス インスタンス (EVI) に基づいて、イーサネット セグメントとの間で発着信するイーサネット セグメントロード バランス トラフィックにローカルに接続されます。EVPN サービス インスタンス内では、1つのPEのみがイーサネットセグメントとの間で発着信するトラフィックを転送します。

図 26: EVPN: シングルアクティブマルチホーミング



ここには、CE1 が PE1 と PE2 のマルチホームであるトポロジが示されています。PE1 と PE2 は MPLS コアを通じて PE3 に接続しています。CE3 はイーサネット インターフェイス バンドルを通じて PE3 に接続されています。PE1 と PE2 はタイプ 4 ルートをアドバタイズしてから、指定フォワーダ (DF) の選択を実行します。非 DF はシングルアクティブモードの両方向のトラフィックをブロックします。

CE1 から CE2 へのトラフィック フローを考えてみます。CE1 は PE1 と PE2 の両方に Address Resolution Protocol (ARP) ブロードキャスト要求を送信します。PE1 が EVI の指定フォワーダである場合、PE1 は CE1 から ARP 要求を転送します。PE2 は CE1 からのトラフィックをド

ロップします。その後で、すべてのユニキャストトラフィックがPE1を通じて送信されます。PE2はスタンバイになるか、またはブロックされます。トラフィックはこのパスを介して送信されません。PE1はPE3にMACをアドバタイズします。PE3は常にPE1を通じてトラフィックを送受信します。PE3はイーサネット インターフェイス バンドルを介してトラフィックをCE2に送信します。

EVPN シングルアクティブ マルチホーミングの設定

EVPN シングルアクティブ マルチホーミング機能を設定するには、PE1とPE2上で次のタスクを実行します。

EVPN イーサネット セグメントの設定

EVPN イーサネット セグメントを設定するには、次のタスクを実行します。

```
Router# configure
Router(config)# evpn
Router(config-evpn)# timers
Router(config-evpn-timers)# peering 15
Router(config-evpn-timers)# recovery 30
Router(config-evpn-timers)# exit
Router(config-evpn)# interface Bundle-Ether1
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 40.00.00.00.00.00.00.01
Router(config-evpn-ac-es)# load-balancing-mode single-active
Router(config-evpn-ac-es)# bgp route-target 4000.0000.0001
Router(config-evpn-ac-es)# service-carving manual primary 100 secondary 200
Router(config-evpn-ac-es-man)# exit
Router(config-evpn-ac-es)# exit
Router(config-evpn-ac)# mac-flush mvrp
Router(config-evpn-ac)# timers
Router(config-evpn-ac-timers)# peering 15
Router(config-evpn-ac-timers)# recovery 30
Router(config-evpn-ac-timers)# commit
Router(config-evpn-ac-timers)# exit
```

実行コンフィギュレーション

```
configure
evpn
  timers
    peering 15
    recovery 30
  !
  interface Bundle-Ether1
    ethernet-segment
      identifier type 0 40.00.00.00.00.00.00.01
      load-balancing-mode single-active
      bgp route-target 4000.0000.0001
      service-carving manual primary 100 secondary 200
    !
    mac-flush mvrp
    timers
      peering 15
      recovery 30
  !
```


EVPN サービス インスタンス (EVI) パラメータの設定

EVPN サービス インスタンス (EVI) パラメータを定義するには、このタスクを実行します。

```
Router# configure
Router(config)# evpn
Router(config-evpn)# evi 6005
Router(config-evpn-evi)# bgp
Router(config-evpn-evi-bgp)# rd 200:50
Router(config-evpn-evi-bgp)# route-target import 100:6005
Router(config-evpn-evi-bgp)# route-target export 100:6005
Router(config-evpn-evi-bgp)# exit
Router(config-evpn-evi)# advertise-mac
Router(config-evpn-evi)# commit
Router(config-evpn-evi)# exit
```

実行コンフィギュレーション

```
configure
evpn
evi 6005
  bgp
    rd 200:50
    route-target import 100:6005
    route-target export 100:6005
  !
  advertise-mac
!
```

レイヤ2 インターフェイスの設定

レイヤ2 インターフェイスを定義するには、次のタスクを実行します。

```
Router# configure
Router(config)# interface bundle-ether2.1 l2transport
Router(config-subif-l2)# no shutdown
Router(config-subif-l2)# encapsulation dot1q 1
Router(config-subif-l2)# rewrite ingress tag pop 1 symmetric
Router(config-subif-l2)#commit
Router(config-subif-l2)#exit
```

実行コンフィギュレーション

```
configure
interface bundle-ether2.1 l2transport
  no shutdown
  encapsulation dot1q 1
  rewrite ingress tag pop 1 symmetric
!
```

ブリッジドメインの設定

次のステップを実行して PE1 と PE2 上にブリッジドメインを設定します。

```
Router# configure
```

```

Router(config)# l2vpn
Router(config-l2vpn)# bridge group 6005
Router(config-l2vpn-bg)# bridge-domain 6005
Router(config-l2vpn-bg-bd)# interface Bundle-Ether2.1
Router(config-l2vpn-bg-bd-ac)# evi 6005
Router(config-l2vpnbg-bd-evi)# commit
Router(config-l2vpnbg-bd-evi)# exit

```

実行コンフィギュレーション

```

configure
l2vpn
bridge group 6005
bridge-domain 6005
interface Bundle-Ether2.1
evi 6005
!

```

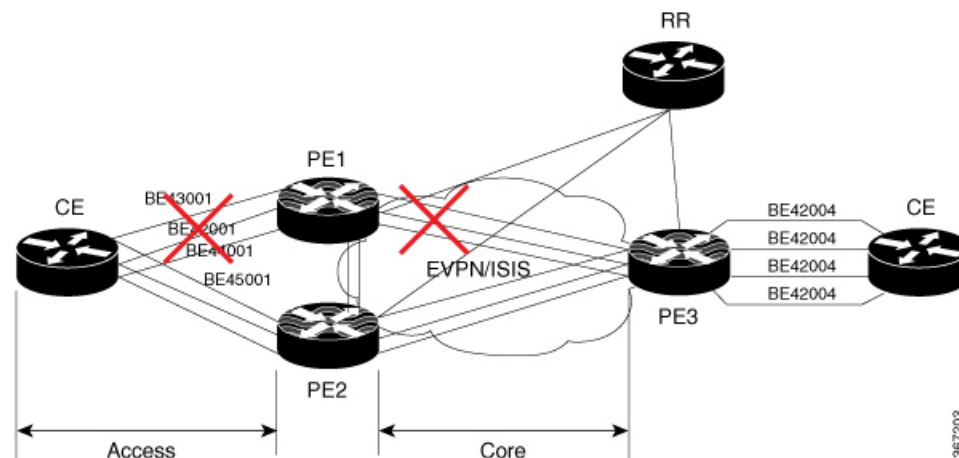
EVPN コア分離保護

EVPN コア分離保護機能を使用すると、コア内のリンク障害をモニタして検出することができます。プロバイダー エッジ (PE) デバイスでコア リンク障害が検出されると、EVPN は、PE のイーサネット セグメント (ES) を停止します。ES は、カスタマー エッジ (CE) デバイスに接続しているアクセス インターフェイスに関連付けられています。

EVPN は、ICCP のコア分離の検出を置き換えるものです。この新機能により、EVPN 環境で ICCP を使用する必要がなくなります。

CE が PE1 および PE2 に接続されているトポロジを考えてみます。PE1、PE2、および PE3 では、MPLS コア ネットワーク上で EVPN が実行されています。コア インターフェイスにはギガビット イーサネットまたはバンドル インターフェイスを使用できます。

図 27: EVPN コア分離保護



PE1 のコア リンクがダウンすると、EVPN はリンク障害を検出し、アクセス ネットワークをダウンさせてコア ネットワークから PE1 ノードを分離します。これにより、CE は PE1 にトラフィックを送信できなくなります。BGP セッションもダウンしているため、BGP は、障害が

発生したPEによってアドバタイズされたすべてのルートを無効にします。これにより、リモート PE2 および PE3 は、L2FIB 内のネクストホップ パスリストと MAC ルートを更新します。PE2 はすべてのトラフィックの転送者になるため、コアネットワークから PE1 を分離します。

すべてのコア インターフェイスと BGP セッションがアップすると、PE1 はイーサネット A-D イーサネットセグメント (ES-EAD) ルートを再度アドバタイズし、サービスカービングをトリガーして、コア ネットワークの一部になります。

EVPN コア分離保護の設定

EVPN グループの配下にコア インターフェイスを設定し、そのグループを、CE に接続された接続回線 (AC) であるイーサネット セグメントに関連付けます。すべてのコア インターフェイスがダウンすると、EVPN は、関連付けられているアクセス インターフェイスをダウンさせます。これにより、CE デバイスは自身のバンドル内でこれらのリンクを使用できなくなります。グループの一部であるすべてのインターフェイスがダウンすると、EVPN はバンドルをダウンさせ、ES-EAD ルートを取り消します。

制約事項

- EVPN の配下には最大 24 のグループを作成できます。
- グループの下には最大 12 のコア インターフェイスを追加できます。
- コア インターフェイスはグループ間で再利用できます。コア インターフェイスは、バンドル インターフェイスにすることができます。
- EVPN グループにはコア インターフェイスのみを含める必要があります。EVPN グループの配下にアクセス インターフェイスを追加しないでください。
- アクセス インターフェイスは、バンドル インターフェイスにしかできません。
- EVPN コアに面するインターフェイスは、物理インターフェイスまたはバンドル メイン インターフェイスのみにする必要があります。サブインターフェイスはサポートされていません。

```
Router# configure
Router(config)# evpn
Router(config-evpn)# group 42001
Router(config-evpn-group)# core interface GigabitEthernet0/2/0/1
Router(config-evpn-group)# core interface GigabitEthernet0/2/0/3
Router(config-evpn-group)# exit
!
Router(config-evpn)# group 43001
Router(config-evpn-group)# core interface GigabitEthernet0/2/0/2
Router(config-evpn-group)# core interface GigabitEthernet0/2/0/4
Router(config-evpn-group)# exit
!
Router# configure
Router(config)# evpn
Router(config-evpn)# interface bundle-Ether 42001
Router(config-evpn-ac)# core-isolation-group 42001
Router(config-evpn-ac)# exit
```

```

!
Router(config-evpn)# interface bundle-Ether 43001
Router(config-evpn-ac)# core-isolation-group 43001
Router(config-evpn-ac)# commit

```

実行コンフィギュレーション

```

configure
evpn
group 42001
  core interface GigabitEthernet0/2/0/1
  core interface GigabitEthernet0/2/0/3
  !
group 43001
  core interface GigabitEthernet0/2/0/2
  core interface GigabitEthernet0/2/0/4
  !
!
configure
evpn
interface bundle-Ether 42001
  core-isolation-group 42001
  !
interface bundle-Ether 43001
  core-isolation-group 43001
  !
!

```

確認

show evpn group コマンドは、evpn グループの完全なリストと、それらに関連付けられているコア インターフェイスおよびアクセス インターフェイスを表示します。各インターフェイスのステータス（アップまたはダウン）も表示されます。アクセスインターフェイスがアップ状態になるには、コア インターフェイスが少なくとも 1 つアップ状態である必要があります。

```

Router# show evpn group /* Lists specific group with core-interfaces and access interface
status */
EVPN Group: 42001
State: Ready
Core Interfaces:
  Bundle-Ethernet110: down
  Bundle-Ethernet111: down
  GigabethEthernet0/2/0/1: up
  GigabethEthernet0/2/0/3: up
  GigabethEthernet0/4/0/8: up
  GigabethEthernet0/4/0/9: up
  GigabethEthernet0/4/0/10: up
Access Interfaces:
  Bundle-Ether42001: up

EVPN Group: 43001
State: Ready
Core Interfaces:
  Bundle-Ethernet110: down
  GigabethEthernet0/2/0/2: up
  GigabethEthernet0/2/0/4: up
  GigabethEthernet0/4/0/9: up

```

```
Access Interfaces:  
Bundle-Ether43001: up
```

EVPN ルーティング ポリシー

EVPN ルーティング ポリシー機能では、アドレスファミリ L2VPN EVPN のルート ポリシー サポートを提供します。この機能は、EVPN ルートフィルタリング機能をルーティングポリシー言語 (RPL) に追加します。フィルタリングはさまざまな EVPN 属性に基づきます。

ピアから受け入れるか、ピアにアドバタイズされる、または1個のルーティングプロトコルから別のプロトコルへ再配布されるときに、ルートを検査し、フィルタリングして、属性を変更するように、ルーティングポリシーがルータに指示します。

この機能により、より粒度が高いルートポリシーの定義を提供するルートポリシー一致基準の EVPN ルートタイプ 1～5 の EVPN ネットワーク層到達可能性情報 (NLRI) 属性を使用してルートポリシーを設定できます。たとえば、ルートポリシーを特定の EVPN ルートタイプのみ適用したり、任意の組み合わせの EVPN NLRI 属性に適用できます。この機能は、ルートポリシーを有効にして EVPN NLRI 属性でフィルタリングすることで、ソリューションの設定および展開に柔軟性をもたらします。

この機能を実装するには、次の概念を理解する必要があります。

- ルーティング ポリシー言語
- ルーティング ポリシー言語の構造
- ルーティング ポリシー言語コンポーネント
- ルーティング ポリシー言語使用方法
- ポリシー定義
- パラメータ化
- ポリシー適用のセマンティック
- ポリシー ステートメント
- 接続点

これらの概念については「[ルーティング ポリシーの実装](#)」を参照してください。

現在、この機能は接続ポイント「イン」または「アウト」の BGP ネイバーでのみサポートされています。ルート ポリシーは BGP ネイバーのインバウンドまたはアウトバウンドのみに適用できます。

EVPN ルート タイプ

EVPN NLRI には次のさまざまなルート タイプがあります。

ルートタイプ1：イーサネット自動検出（AD）ルート

イーサネット（AD）ルートは、EVIごととイーサネットセグメント識別子（ESI）ごとにアドバタイズされます。これらのルートは、イーサネットセグメント（ES）ごとに送信されます。これらはESに属しているEVIのリストを伝送します。ESIフィールドは、CEがシングルホームの場合はゼロに設定されます。

イーサネット A-D ルートタイプ固有の EVPN NLRI は次のフィールドで構成されます。

```

+-----+
|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ドを削減します。

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

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)	

308326

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
!

```

EVPN ELAN での CFM

接続障害管理 (CFM) はサービスレベルの Operations and Maintenance (OAM) プロトコルの 1 つで、VLAN ごとにエンドツーエンドのイーサネットサービスをモニタリングおよびトラブルシューティングするためのツールとなります。これには、予防的な接続モニタリング、障害検証、および障害分離の機能が含まれています。Cisco IOS XR ソフトウェア リリース 6.6.1 では、シングルホーム EVPN エミュレート ローカルエリア ネットワーク (ELAN) サービスに対応した CFM サポートが導入されています。この機能は、ユーザの ELAN サービスをユーザのサービスレベル契約 (SLA) に照らしてモニタするのに役立ちます。これにより、復元力が高く、市場ごとの運用の複雑さが軽減された、高速のレイヤ 2 およびレイヤ 3 サービスが提供されます。

シングルホーム EVPN ELAN サービス対応の CFM は、CFM の連続性チェック、ITU-T Y.1731 準拠の遅延測定メッセージ (DMM)、および合成損失測定 (SLM) の機能をサポートしています。この機能は、物理インターフェイス、サブインターフェイス、バンドルインターフェイスなどの接続回線 (AI) で使用できます。

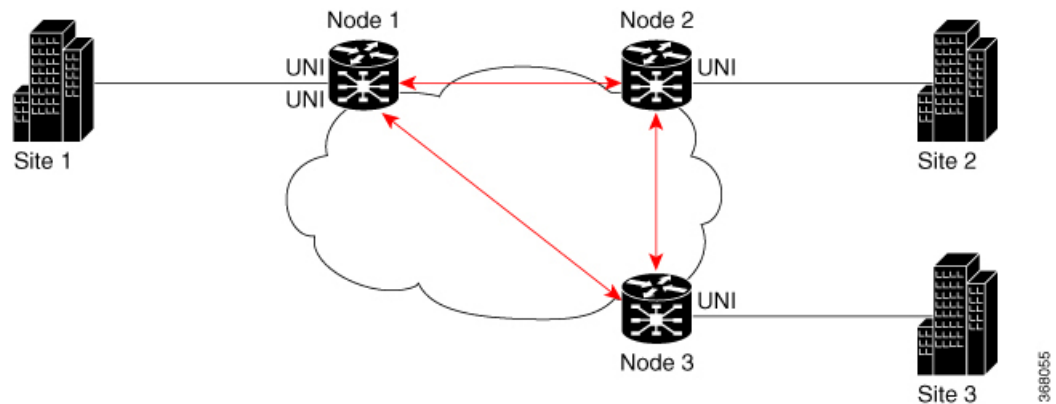
EVPN ELAN での CFM の制約事項

EVPN ELAN での CFM には、次の制限が適用されます。

- シングルホーム EVPN ELAN のみをサポートします。
- アップの MEP のみをサポートします。
- 10 秒以上の CFM タイマー値のみをサポートします。
- ベース ノードごとに最大 20 の EVPN ELAN サービスのみをサポートします。
- EVPN サービスごとに最大 200 のサイトのみをサポートします。
- 損失測定はサポートしていません。
- VPLS を介した CFM はサポートしていません。

EVPN ELAN での CFM の設定

図 28: EVPN ELAN での CFM : フルメッシュトポロジ



このトポロジのノード 1、2、および 3 は、Cisco NCS 5500 シリーズ ルータまたは Cisco NCS 540 シリーズ ルータにすることができます。

EVPN ELAN での CFM の設定には、主に次の作業が伴います。

- CFM サービス連続性チェックの有効化
- MEP クロスチェックの設定
- インターフェイスの CFM のイネーブル化
- SLA プロファイルの設定

EVPN ELAN での CFM の設定例 : フルメッシュトポロジ

```
/* Enabling CFM continuity check */
Router# ethernet cfm
```

```

Router(config-cfm# domain bd-domain level 1 id null
Router(config-cfm-dmn)# service bd-domain bridge group bg-elan bridge-domain bd-elan id
icc-based MC MCMC
Router(config-cfm-dmn-svc)# continuity-check interval 1m
/* Configuring MEP cross-check */
Router(config-cfm-dmn-svc)# mep crosscheck
Router(config-cfm-dmn-svc)# mep-id 1112
Router(config-cfm-dmn-svc)# mep-id 1113
Router(config-cfm-dmn-svc)# commit

```

ノード2とノード3について前述の設定を繰り返し、それぞれの mep-id 値を設定します。ノード2では、ノード1およびノード3のそれぞれの mep-id 値（この例ではそれぞれ 1111 および 1113）を使用して MEP クロスチェックを設定します。ノード3では、ノード1およびノード2のそれぞれの mep-id 値（この例ではそれぞれ 1111 および 1112）を使用して MEP クロスチェックを設定します。

```

/* Enabling CFM on the interface */
Router(config)# interface gigabitEthernet 0/0/0/0.100 12transport
Router(config-subif)# description bg-elan
Router(config-subif)# encapsulation dot1q 100
Router(config-subif)# rewrite ingress tag pop 1 symmetric
Router(config-subif)# mtu 9100
Router(config-subif)# ethernet cfm
Router(config-if-cfm)# mep domain bd-domain service bd-service mep-id 1111
Router(config-if-cfm-mep)# commit

```

ノード2とノード3について前述の設定を繰り返し、それぞれの mep-id 値を設定する必要があります（この例では、ノード2の場合は 1112、ノード3の場合は 1113）。

```

/* Configuring SLA profile */
Router(config)# ethernet sla
Router(config-sla)# profile test-profile1 type cfm-delay-measurement
Router(config-sla-prof)# probe
Router(config-sla-prof-pb)# send burst every 10 seconds packet count 50 interval 100
milliseconds
Router(config-sla-prof-pb)# exit
Router(config-sla-prof)# schedule
Router(config-sla-prof-schedule)# every 3 minutes for 120 seconds
Router(config-sla-prof-schedule)# exit
Router(config-sla-prof)# statistics
Router(config-sla-prof-stat)# measure round-trip-delay
Router(config-sla-prof-stat-cfg)# buckets size 1 probes
Router(config-sla-prof-stat-cfg)# buckets archive 2
Router(config-sla-prof-stat-cfg)# commit

```

同様に、もう1つの sla プロファイル *test-profile2* を設定し、1秒ごとにパケットを送信するようにプローブ設定を設定します。

EVPN ELAN での CFM の実行コンフィギュレーション：フルメッシュトポロジ

ここでは、ノード1の実行コンフィギュレーションを示します。

```

ethernet cfm
domain bd-domain level 1 id null
service bd-domain bridge group bg-elan bridge-domain bd-elan id icc-based MC MCMC
continuity-check interval 1m
mep crosscheck

```

```

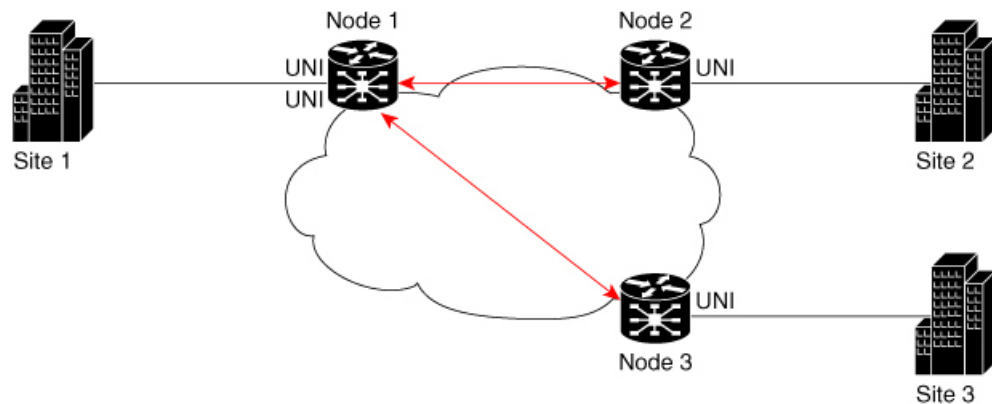
        mep-id 1112
        mep-id 1113
        !
        !
        !
interface GigabitEthernet0/0/0/0.100 l2transport
description bg-elan
encapsulation dot1q 100
rewrite ingress tag pop 1 symmetric
mtu 9100
ethernet cfm
    mep domain bd-domain service bd-service mep-id 1111
    !

ethernet sla
profile test-profile1 type cfm-delay-measurement
probe
    send burst every 10 seconds packet count 50 interval 100 milliseconds
    !
schedule
    every 3 minutes for 120 seconds
    !
statistics
    measure round-trip-delay
    buckets size 1 probes
    buckets archive 2

profile test-profile2 type cfm-delay-measurement
probe
    send packet every 1 seconds
    !
schedule
    every 3 minutes for 120 seconds
    !
statistics
    measure round-trip-delay
    buckets size 1 probes
    buckets archive 5

```

図 29: EVPN ELAN での CFM: ハブアンドスポーク トポロジ



368054

EVPN ELAN での CFM の設定例 : ハブ アンド スポーク トポロジ

ハブ アンド スポーク トポロジの CFM 設定は前述のフル メッシュ トポロジの設定と同じです。ただし、インターフェイスで SLA プロファイル設定について次の追加手順を実行します。

```
/* 1112 and 1113 in this example, are the mep-id values of node 2 and node 3 */
Router(config)#interface gigabitEthernet 0/0/0/0.100 l2transport
Router(config-subif)# ethernet cfm
Router(config-if-cfm)# mep domain bd-domain service bd-service mep-id 1111
Router(config-if-cfm-mep)# sla operation profile test-profile1 target mep-id 1112
Router(config-if-cfm-mep)# sla operation profile test-profile2 target mep-id 1112
Router(config-if-cfm-mep)# sla operation profile test-profile1 target mep-id 1113
Router(config-if-cfm-mep)# sla operation profile test-profile2 target mep-id 1113
Router(config-if-cfm-mep)# commit
```

EVPN ELAN での CFM の実行コンフィギュレーション : ハブ アンド スポーク トポロジ

ここでは、ノード 1 の実行コンフィギュレーションを示します。

```
interface GigabitEthernet0/0/0/0.100 l2transport
description bg-elan
encapsulation dot1q 100
rewrite ingress tag pop 1 symmetric
mtu 9100
ethernet cfm
mep domain bd-domain service bd-service mep-id 1111
sla operation profile test-profile1 target mep-id 1112
sla operation profile test-profile2 target mep-id 1112
sla operation profile test-profile1 target mep-id 1113
sla operation profile test-profile2 target mep-id 1113
!
```

関連項目

[EVPN ELAN での CFM \(198 ページ\)](#)

関連コマンド

- continuity-check
- ethernet cfm
- mep crosscheck
- mep domain
- sla operation



第 9 章

EVPN IRB の設定

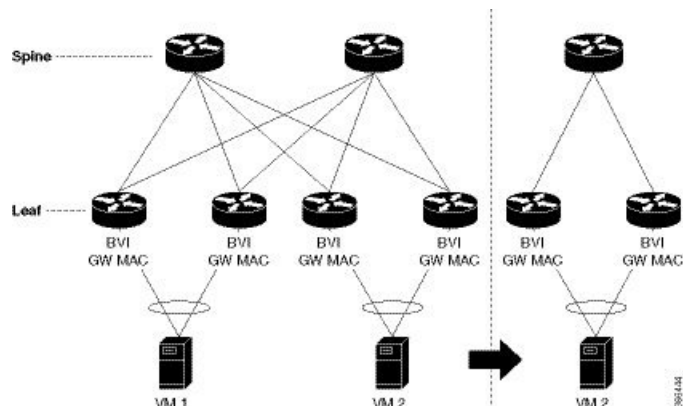
この章では、イーサネット VPN (EVPN) の Integrated Routing and Bridging (IRB) 機能について紹介し、EVPN IRB 機能の設定方法について説明します。

- [EVPN IRB \(203 ページ\)](#)
- [EVPN シングルホーミング アクセス ゲートウェイ \(205 ページ\)](#)
- [EVPN マルチホーミング オールアクティブ \(206 ページ\)](#)
- [手動 ESI 設定を使用した自動 BGP RT の有効化 \(206 ページ\)](#)
- [サポートされている EVPN IRB のシナリオ \(207 ページ\)](#)
- [分散型エニーキャスト ゲートウェイ \(207 ページ\)](#)
- [VM モビリティ サポート \(211 ページ\)](#)
- [重複 IP アドレス検出 \(238 ページ\)](#)
- [EVPN E-Tree \(241 ページ\)](#)
- [IRB での DHCPv4 リレー \(250 ページ\)](#)
- [オールアクティブ マルチホーミング対応 DHCPv4 リレー同期 \(259 ページ\)](#)
- [IRB での DHCPv6 リレー IAPD \(259 ページ\)](#)
- [セッション冗長性を使用したオールアクティブ マルチホーミング対応 DHCPv6 PD 同期 \(263 ページ\)](#)
- [DHCPv6 リレーにおける IAPD ルートの配布と取り消し \(266 ページ\)](#)

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 30 : 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。

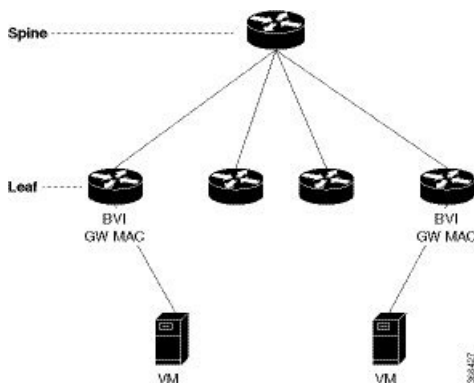
上のトポロジ図では、VM、VM1とVM2が相互に接続されています。VM2が別のスイッチおよび別のサーバに移行する場合、そのVMの現在のMACアドレスとIPアドレスはそのまま保たれます。サブネットが2つのEVPN PE間にストレッチされている場合、同じIRB設定が両方のデバイスに適用されます。

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

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 コアにアダプタイズします。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 ルートもアダプタイズされます。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 デバイスにアダプタイズし、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 を通じてアダプタイズされません。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 31: EVPN シングルホーミング アクセス ゲートウェイ



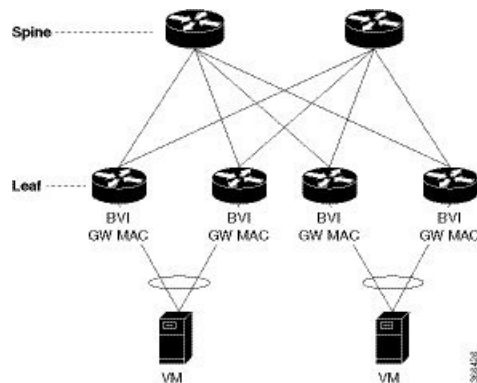
上記は、CE デバイスによる PE デバイス 1 台への接続を許可することによって EVPN シングルホーミング アクセス ゲートウェイがネットワーク接続を有効にするトポロジを示しています。PE デバイスはバンドルインターフェイスまたは物理インターフェイスを通じてイーサネット

トセグメントに接続されます。シングルホーミングにはヌルイーサネットセグメント識別子 (ESI) を使用します。

EVPN マルチホーミング オールアクティブ

EVPN IRB では、EVPN と IP VPN の両方 (VPNv4 と VPNv6 の両方) のアドレスファミリがルータとデータセンターインターコネクト (DCI) ゲートウェイの間で有効になっています。レイヤ 2 (L2) ストレッチが複数のデータセンター (DC) で使用できないときは、VPNv4 ルートまたは VPNv6 ルートを通じてルーティングが確立されます。レイヤ 2 ストレッチが使用できるときは、IP-MAC ルートを ARP で学習して EVPN/BGP に配布する場合にホストルーティングが適用されます。リモートピアゲートウェイでは、これらの IP-MAC EVPN ルートがセカンダリラベルとレイヤ 3 VRF ルートターゲットとともに EVPN ルートタイプ 2 ルートから IP VPN ルーティングテーブルにインポートされます。

図 32: 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ダ (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ド (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。



(注) BVI インターフェイスでカスタムまたはスタティック MAC アドレスが設定されている場合、ワイヤ上の MAC アドレスは設定されているものと異なる場合があります。このことによる動作上または機能上の影響はありません。

サブネット内ユニキャスト データ プレーン

すべての ES と、ローカル EVPN PE からアドバタイズされたすべての EVI、ES および EAD ルートタイプ 2 のルートに対し MAC+IP RT2 を通じて確立されたリモート 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 プロブをトリガーし、ホスト MAC-IP を検出してオーバーレイ上でこのホストのモビリティをトリガーします。

重複 MAC 検出

RFC 7432 に従い、重複 MAC 検出とフリージングがサポートされています。

検出：重複データ検出とリカバリのパラメータは設定可能です。デフォルト設定は、180 秒間に 5 回と重複サイクル 3 回後のルートフリージングです。デフォルト設定では、ホストが 180 秒以内に 5 回移動すると、30 秒間は重複とマークされます。重複状態のホストのルートアドバタイズメントは抑制されます。ホストは 30 秒後に重複状態が解除されます。ホストが重複していると 3 回検出されると、4 回目の重複サイクルで、そのホストは完全に凍結されます。凍結されたホストについては、すべてのルートアドバタイズメントが抑制されます。

マルチホーム ホストでは、MAC をローカルに学習するとは限りませんが、同期を通じて学習されます。重複データ検出はローカルホストとリモート同期ホストの両方でサポートされています。リモート同期ルートは、リモートルートと区別されます。

MAC-IP 処理：MAC ルートが重複しているか、または凍結状態の場合、ルート削除が撤回されることを除き、対応するローカル MAC-IP が更新されます。

重複状態の処理：ホストが重複状態にある場合、ルートアドバタイズメントが抑制されます。ただし、ローカル EVPN-PE のトラフィックがローカルホストに転送されるようにローカルルートはハードウェアでプログラミングされます。

リカバリ：完全に凍結されたホストの凍結解除が可能です。次に、凍結ホストをクリアする推奨手順を示します。

- 重複トラフィックの原因となっているホストをシャットダウンします。

- **clear l2route evpn frozen-mac frozen-flag** コマンドを使用して凍結されたホストをクリアします。

EVPN IRB の設定

```

/* Configure CEF to prefer RIB prefixes over adjacency prefixes.*/

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface Bundle-Ether 3
RP/0/RSP0/CPU0:router(config-if)# lacp system mac 1.1.1
RP/0/RSP0/CPU0:router(config-if)# exit
RP/0/RSP0/CPU0:router(config)# cef adjacency route override rib

/* Configure EVPN L3VRF per DC tenant. */

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# vrf irbl
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 irb1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface bundle-Ether3.1001
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# routed interface BVI100
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-bvi)# split-horizon group core
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-bvi)# evi 10001

```

EVPN IRB の実行コンフィギュレーション

```

/* Configure LACP */

interface Bundle-Ether3
 lACP system mac 1.1.1
!

/* Configure CEF adjacency overwrite. */

cef adjacency route override rib

/* Configure EVPN Layer 3 VRF per DC tenant. */

vrf irb1
address-family ipv4 unicast
 import route-target
  1000:1
!
 export route-target
  1000:1
!

!

/* Configure Layer 2 attachment circuit (AC) from multichassis (MC) bundle interface,
and bridge-group virtual interface (BVI) per bridge domain.*/

interface Bundle-Ether3.1001 l2transport
 encapsulation dot1q 1001
 rewrite ingress tag pop 1 symmetric

```

```

!
interface BVI1001
  host-routing
  vrf irb1
  ipv4 address 10.0.1.1 255.255.255.0
  mac-address 0000.3030.1
!

/* Configure BGP. */

router bgp 3107
  vrf irb1
  rd auto
  address-family ipv4 unicast
  redistribute connected
  redistribute static
!
!

/* Configure EVPN. */

evpn
evi 10001
  bgp
  route-target import 1000:1
  route-target export 1000:1
!
  advertise-mac
  unknown-unicast-suppression
!

/* Configure Layer2 VPN. */

l2vpn
bridge group irb
  bridge-domain irb1
  interface Bundle-Ether3.1001
  !
  routed interface BVI1001
  split-horizon group core
  !
  evi 10001
  !
  !

```

EVPN IRB の確認

マルチホーミングシナリオでの Address Resolution Protocol (ARP) プロトコルエントリおよび同期済みエントリを確認します。EVPN IRB では、マルチホーミングアクティブ-アクティブモードのみがサポートされています。

```
RP/0/RSP0/CPU0:router# show arp vrf evpn1
```

```

-----
0/1/CPU0
-----

```

Address	Age	Hardware Addr	State	Type	Interface
10.1.1.1	-	0010.0001.0001	Interface	ARPA	BVI1
10.1.1.11	02:23:46	1000.0001.0001	Dynamic	ARPA	BVI1
10.1.1.93	-	0000.f65a.357c	EVPN_SYNC	ARPA	BVI1

```

10.1.2.1 - 0011.0112.0001 Interface ARPA BVI2
10.1.2.91 02:24:14 0000.f65a.3570 Dynamic ARPA BVI2
10.1.2.93 02:21:52 0000.f65a.357d Dynamic ARPA BVI2
-----
0/0/CPU0
-----
Address Age Hardware Addr State Type Interface
-----
10.1.1.1 - 0010.0001.0001 Interface ARPA BVI1
10.1.1.11 02:23:46 1000.0001.0001 Dynamic ARPA BVI1
10.1.1.93 - 0000.f65a.357c EVPN_SYNC ARPA BVI1
10.1.2.1 - 0011.0112.0001 Interface ARPA BVI2
10.1.2.91 02:24:14 0000.f65a.3570 Dynamic ARPA BVI2
10.1.2.93 02:21:52 0000.f65a.357d Dynamic ARPA BVI2

```

隣接関係エントリーを確認します。特に、同期済み IPv4 および IP ARP エントリー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ーを確認します。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 0x5000001 0x0 (ptr 0x99fac884) [1], 0x0 (0x0), 0x208
(0x96c58494)
Updated Feb 28 16:06:39.285
Prefix Len 32, traffic index 0, precedence n/a, priority 3
via 172.16.0.1/32, 15 dependencies, recursive [flags 0x6000]
path-idx 0 NHID 0x0 [0x97955380 0x0]
recursion-via-/32
next hop VRF - 'default', table - 0xe0000000
next hop 172.16.0.1/32 via 34034/0/21
next hop 100.0.57.5/32 Te0/0/0/3 labels imposed {ImplNull 24011 24027}
next hop 100.0.67.6/32 Te0/0/0/1 labels imposed {ImplNull 24009 24027}
via 172.16.0.2/32, 11 dependencies, recursive, backup [flags 0x6100]
path-idx 1 NHID 0x0 [0x979554a0 0x0]
recursion-via-/32
next hop VRF - 'default', table - 0xe0000000
next hop 172.16.0.2/32 via 34035/0/21
next hop 100.0.57.5/32 Te0/0/0/3 labels imposed {ImplNull 24012 24031}
next hop 100.0.67.6/32 Te0/0/0/1 labels imposed {ImplNull 24010 24031}

```

次の各項では、サブネットストレッチングの確認方法について説明します。

VRF を確認します。

```

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
    !
  !
!
!

```

モビリティを備えた EVPN IPv6 ホスト

モビリティを備えた EVPN IPv6 ホスト機能を使用すると、IPv4-MPLS コア ネットワークを介して EVPN IPv6 サービスを提供できます。この機能は、オールアクティブのマルチホーミングおよび仮想マシン (VM) またはホストの移動をサポートします。

サービス プロバイダー (SP) は、IPv4 VPN サービスを提供するために、IPv4-MPLS バックボーンによる安定し確立されたコアを使用します。MPLS 経由の IPv6 VPN プロバイダー エッジ トランスポート (プロバイダー エッジ ルータ上の IPv6 (6PE) および VPN プロバイダー エッジ ルータ上の IPv6 (6VPE)) により、SP は、IPv6 コアがなくても IPv4 バックボーンを介して IPv6 VPN サービスを容易に提供できるようになります。プロバイダー エッジ (PE) ルータは、IPv6 到達可能性および IPv6 ラベル配布をアドバタイズするために、MP-iBGP を実行します。6PE の場合、ラベルは接続されたカスタマー エッジ (CE) ルータから学習した IPv6 プレフィックスごとに割り当てられ、6VPE の場合は、プレフィックス単位で、または CE レベル単位と VRF レベル単位でラベルを割り当てるように PE ルータを設定できます。

モビリティ サポート

グローバル VRF では、モビリティはサポートされていません。ただし、同じブリッジ ドメイン内で、ある ES から別の ES にホストを移動することは可能です。ホストは、新しい MAC アドレスと IP アドレスを取得します。ホストは、同じ MAC アドレスに対して複数の IP アドレスを持つことができます。

デフォルト以外の VRF では、モビリティは次の条件でサポートされます。

- 基本的な MAC の移動 : IP アドレスと MAC アドレスは同じままです。同じ IP アドレスと MAC アドレスを使用して、ある ES から別の ES にホストを移動することができます。
- 同じ MAC アドレスで異なる IP アドレス : ホストは新しい IP アドレスを取得します。

- 同じ MAC アドレスで異なる IP アドレス：ホストは新しい MAC アドレスを取得しますが、同じ IP アドレスを保持します。
- 同じ MAC アドレスを持つ複数の IP アドレス：多数の VM が同じ MAC の移動に関与します。

制約事項

- カスタマー VRF では、ホストルーティングが設定されていない場合、MAC-IP アドバタイズメントはゼロ ESI と非ゼロ ESI とで異なります。ホストルーティングが設定されていない場合、非ゼロ ESI の MAC-IP は L3 RT (VRF RT) なしでアドバタイズされます。ゼロ ESI の MAC-IP はアドバタイズされません。次の表に、ESI とホストルーティングに関する MAC-IP アドバタイズメントの動作を示します。

ESI のタイプ	ホストルーティングあり	ホストルーティングなし
非ゼロ ESI の MAC-IP	L3 VRF RT ありでアドバタイズ	L3 VRF RT なしでアドバタイズ
ゼロ ESI の MAC-IP	L3 VRF RT ありでアドバタイズ	アドバタイズされない

- グローバル VRF では、レイヤ 2 ストレッチはサポートされていません。
- グローバル VRF での MAC 移動は、ホストが同じブリッジドメイン内にある場合にのみサポートされます。同じブリッジドメイン内で、ある ES から別の ES にホストを移動することは可能です。
- IP アドレスの重複の検出はサポートされていません。
- ESI ごとに許可される最大リーフ数は 2 です。

モビリティを備えた EVPN IPv6 ホストの設定

モビリティを備えた EVPN IPv6 ホスト機能を設定するには、次のタスクを実行します。

- VRF の設定
- ISIS の設定
- BGP の設定
- AC インターフェイスの設定
- BVI インターフェイスの設定
- EVPN の設定
- L2VPN の設定



(注) デバイスには最大 128K の MAC アドレス エントリを含めることができます。デバイス上のブリッジドメインには最大 65K の MAC アドレス エントリを含めることができます。

```
/* Configure VRF */

Router# configure
Router(config)# vrf cust102
Router(config-vrf)# address-family ipv4 unicast
Router(config-vrf-af)# import route-target 160102:16102
Router(config-vrf-af)# export route-target 160102:16102
Router(config-vrf-af)# exit
!
Router(config-vrf)# address-family ipv6 unicast
Router(config-vrf-af)# import route-target 6160102:16102
Router(config-vrf-af)# export route-target 6160102:16102
Router(config-vrf-af)# commit
!

/* Configure ISIS */

Router# configure
Route(config)# router isis v6
Route(config-isis)# 49.0001.0000.0160.0005.00
Route(config-isis)# nsr
Route(config-isis)# log adjacency changes
Route(config-isis)# lsp-gen-interval maximum-wait 5000 initial-wait 1 secondary-wait
20
Route(config-isis)# lsp-mtu 1468
Route(config-isis)# lsp-refresh-interval 65000
Route(config-isis)# max-lsp-lifetime 65535
Route(config-isis)# address-family ipv4 unicast
Route(config-isis-af)# metric-style wide
Route(config-isis-af)# microloop avoidance protected
Route(config-isis-af)# spf-interval maximum-wait 5000 initial-wait 1 secondary-wait
20
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 Bundle-Ether10
Route(config-isis-if)# point-to-point
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# fast-reroute per-prefix
Route(config-isis-af)# fast-reroute per-prefix ti-lfa
Route(config-isis-af)# metric 10
Route(config-isis-af)# exit
!
Route(config-isis)# interface Bundle-Ether20
Route(config-isis-if)# point-to-point
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# fast-reroute per-prefix
Route(config-isis-af)# fast-reroute per-prefix ti-lfa
Route(config-isis-af)# metric 10
Route(config-isis-af)# exit
!
Route(config-isis)# interface loopback0
```

```

Route(config-isis-if)# passive
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# exit
!
Route(config-isis)# interface loopback10
Route(config-isis-if)# passive
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# prefix-sid index 1605
Route(config-isis-af)# commit
Route(config-isis-af)# exit
!

/* Configure Segment Routing */

Router# configure
Router(config)# segment-routing
Router(config-sr)# global-block 16000 23999
Router(config-sr)# commit

/* Configure BGP */

Router(config)# router bgp 100
Router(config-bgp)# bfd minimum-interval 50
Router(config-bgp)# bfd multiplier 3
Router(config-bgp)# bgp router-id 160.0.0.5
Router(config-bgp)# address-family ipv4 unicast      ---> To support V4 Global VRF
Router(config-bgp-af)# maximum-paths ibgp 10 unequal-cost ---> ECMP
Router(config-bgp-af)# redistribute connected      --> V4 Global VRF
Router(config-bgp-af)# exit
!
Router(config-bgp)# address-family ipv4 unicast      ---> VRF
Router(config-bgp-af)# vrf all
Router(config-bgp-af)# label mode per-vrf
Router(config-bgp-af)# exit
!
Router(config-bgp)# address-family ipv6 unicast      ---> For 6PE
Router(config-bgp-af)# label mode per-vrf
Router(config-bgp-af)# maximum-paths ibgp 8
Router(config-bgp-af)# redistribute static
Router(config-bgp-af)# allocate-label all
Router(config-bgp-af)# exit
!
Router(config-bgp)# address-family vpnv6 unicast      ---> 6 VPE
Router(config-bgp-af)# vrf all
Router(config-bgp-af)# label mode per-vrf
Router(config-bgp-af)# exit
!
Router(config-bgp)# address-family l2vpn evpn      ----> EVPN
Router(config-bgp-af)# bgp implicit-import      ----> Global VRF
Router(config-bgp-af)# exit
!
Router(config-bgp)# neighbor-group evpn-rr
Router(config-bgp-nbr)# remote-as 100
Router(config-bgp-nbr)# bfd fast-detect
Router(config-bgp-nbr)# update-source loopback0
Router(config-bgp-nbr)# address-family ipv4 unicast
Router(config-bgp-nbr-af)# route-policy pass-all in
Router(config-bgp-nbr-af)# route-policy nh-1010 out
Router(config-bgp-nbr-af)# exit
!
Router(config-bgp-nbr)# address-family ipv6 labeled-unicast ----> For 6PE
Router(config-bgp-nbr-af)# route-policy pass-all out
Router(config-bgp-nbr-af)# exit

```

```

!
Router(config-bgp-nbr)# address-family l2vpn evpn
Router(config-bgp-nbr-af)# route-policy pass-all in
Router(config-bgp-nbr-af)# route-policy nh-lol10 out
Router(config-bgp-nbr-af)# advertise vpvv4 unicast re-originated -> For Route Type
5
Router(config-bgp-nbr-af)# advertise vpvv6 unicast re-originated -> For Route Type
5
Router(config-bgp-nbr-af)# exit
!
Router(config-bgp)# neighbor 160.0.0.1
Router(config-bgp-nbr)# use neighbor-group evpn-rr
Router(config-bgp-nbr)# exit
!
Router(config-bgp)# neighbor 160.0.0.2
Router(config-bgp-nbr)# use neighbor-group evpn-rr
Router(config-bgp-nbr)# exit
!
Router(config-bgp)# vrf all
Router(config-bgp-vrf)# rd 1605:102
Router(config-bgp-vrf)# address-family ipv4 unicast
Router(config-bgp-vrf-af)# label mode per-vrf
Router(config-bgp-vrf-af)# maximum-paths ibgp 10 unequal-cost
Router(config-bgp-vrf-af)# redistribute connected ---> Triggers Route Type 5
Router(config-bgp-vrf-af)# exit
!
Router(config-bgp-vrf)# address-family ipv6 unicast
Router(config-bgp-vrf-af)# label mode per-vrf
Router(config-bgp-vrf-af)# maximum-paths ibgp 10 unequal-cost
Router(config-bgp-vrf-af)# redistribute connected
Router(config-bgp-vrf-af)# exit
!

/* Configure AC interface */

Router(config)# interface Bundle-Ether1.102 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 102
Router(config-l2vpn-subif)# rewrite ingress tag pop 1 symmetric
Router(config-l2vpn-subif)# commit
Router(config-l2vpn-subif)# exit

/* Configure BVI interface */

Router(config)# interface BVI100
Router(config-if)# ipv4 address 56.78.100.1 255.255.255.0
Router(config-if)# ipv6 address 56:78:100::1/64
Router(config-if)# mac-address 22.22.22
Router(config-if)# exit
!
Router(config)# interface BVI102
Router(config-if)# host-routing
Router(config-if)# vrf cust102
Router(config-if-vrf)# ipv4 address 56.78.102.1 255.255.255.0
Router(config-if-vrf)# ipv6 address 56:78:100::1/64
Router(config-if-vrf)# ipv6 address 56:78:102::1/64
Router(config-if-vrf)# mac-address 22.22.22
Router(config-if-vrf)# commit

/* Configure CEF */ [Required for dual homing]

Router# configure
Router(config)# cef adjacency route override rib

```

```

/* Configure EVPN, and configure main bundle ethernet segment parameters in EVPN */

Router# configure
Router(config)# evpn
Router(config-evpn)# evi 102
Router(config-evpn-evi)# bgp
Router(config-evpn-evi)# rd 1605:102
Router(config-evpn-evi-bgp)# route-target import 160102:102
Router(config-evpn-evi-bgp)# route-target export 160102:102
Router(config-evpn-evi-bgp)# exit
Router(config-evpn-evi)# advertise-mac
Router(config-evpn-evi)# exit
!
Router(config-evpn)# interface Bundle-Ether1
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 56.56.56.56.56.56.56.01
Router(config-evpn-ac-es)# exit
!
Router(config-evpn)# interface Bundle-Ether2
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 56.56.56.56.56.56.56.02
Router(config-evpn-ac-es)# commit

/* Configure L2VPN */

Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group bg102
Router(config-l2vpn-bg)# bridge-domain bd102
Router(config-l2vpn-bg-bd)# interface Bundle-Ether1.102
Router(config-l2vpn-bg-bd-ac)# exit
!
Router(config-l2vpn-bg-bd)# interface Bundle-Ether2.102
Router(config-l2vpn-bg-bd-ac)# exit
!
Router(config-l2vpn-bg-bd)# interface Bundle-Ether3.102
Router(config-l2vpn-bg-bd-ac)# exit
!
Router(config-l2vpn-bg-bd)# interface Bundle-Ether4.102
Router(config-l2vpn-bg-bd-ac)# exit
!
Router(config-l2vpn-bg-bd)# interface Bundle-Ether5.102
Router(config-l2vpn-bg-bd-ac)# routed interface BVI102
Router(config-l2vpn-bg-bd-bvi)# evi 102
Router(config-l2vpn-bg-bd-bvi-evi)# commit

```

実行コンフィギュレーション

```

/* Configure VRF */

vrf cust102
address-family ipv4 unicast
import route-target
160102:16102
!
export route-target
160102:16102
!
!
address-family ipv6 unicast
import route-target

```

```
6160102:16102
!
export route-target
6160102:16102
!
!
!

/ * Configure ISIS */

router isis v6
net 49.0001.0000.0160.0005.00
nsr
log adjacency changes
lsp-gen-interval maximum-wait 5000 initial-wait 1 secondary-wait 20
lsp-mtu 1468
lsp-refresh-interval 65000
max-lsp-lifetime 65535
address-family ipv4 unicast
metric-style wide
microloop avoidance protected
spf-interval maximum-wait 5000 initial-wait 1 secondary-wait 20
segment-routing mpls sr-prefer
segment-routing prefix-sid-map advertise-local
!
interface Bundle-Ether10
point-to-point
address-family ipv4 unicast
fast-reroute per-prefix
fast-reroute per-prefix ti-lfa
metric 10
!
!
interface Bundle-Ether20
point-to-point
address-family ipv4 unicast
fast-reroute per-prefix
fast-reroute per-prefix ti-lfa
metric 10
!
!
interface Loopback0
passive
address-family ipv4 unicast
!
!
interface Loopback10
passive
address-family ipv4 unicast
prefix-sid index 1605
!
!
!

/ * Configure Segment Routing */

segment-routing
global-block 16000 23999
!

/ * Configure BGP */

router bgp 100
bfd minimum-interval 50
```

```

bfd multiplier 3
bgp router-id 160.0.0.5
address-family ipv4 unicast ---> To support V4 Global VRF
  maximum-paths ibgp 10 unequal-cost ---> ECMP
  redistribute connected --> V4 Global VRF
!
address-family vpnv4 unicast ---> VRF
  vrf all
  label mode per-vrf
!
address-family ipv6 unicast ---> For 6PE
  label mode per-vrf
  maximum-paths ibgp 8
  redistribute connected
  redistribute static
  allocate-label all
!
address-family vpnv6 unicast ---> 6VPE
  vrf all
  label mode per-vrf
!
address-family l2vpn evpn ----> EVPN
bgp implicit-import ----> Global VRF
!

neighbor-group evpn-rr
  remote-as 100
  bfd fast-detect
  update-source Loopback0
  address-family ipv4 unicast
    route-policy pass-all in
    route-policy nh-lo10 out
  !
  address-family ipv6 labeled-unicast ----> For 6PE
  route-policy pass-all out
  !
  address-family l2vpn evpn
  route-policy pass-all in
  route-policy nh-lo10 out
  advertise vpnv4 unicast re-originated ----> For Route Type 5
  advertise vpnv6 unicast re-originated ----> For Route Type 5
  !
!
neighbor 160.0.0.1
use neighbor-group evpn-rr
!
neighbor 160.0.0.2
use neighbor-group evpn-rr
!
vrf cust102
rd 1605:102
address-family ipv4 unicast
  label mode per-vrf
  maximum-paths ibgp 10 unequal-cost
  redistribute connected <----- Triggers Route Type 5
!
address-family ipv6 unicast
  label mode per-vrf
  maximum-paths ibgp 10 unequal-cost
  redistribute connected
!
!

/* Configure AC interface */

```



```
interface Bundle-Ether1.102 l2transport
 encapsulation dot1q 102
 rewrite ingress tag pop 1 symmetric
!
/* Configure BVI interface */
interface BVI100
 ipv4 address 56.78.100.1 255.255.255.0
 ipv6 address 56:78:100::1/64
 mac-address 22.22.22
!
interface BVI102
 host-routing
 vrf cust102
 ipv4 address 56.78.102.1 255.255.255.0
 ipv6 address 56:78:100::1/64
 ipv6 address 56:78:102::1/64
 mac-address 22.22.22
!

/* Configure CEF */ [ Required for Dual homing]
cef adjacency route override rib

/* Configure EVPN */

evpn
 evi 102
  bgp
  rd 1605:102
  route-target import 160102:102
  route-target export 160102:102
  !
  advertise-mac
  !
  !
!
interface Bundle-Ether1
 ethernet-segment
 identifier type 0 56.56.56.56.56.56.56.01
!
!
interface Bundle-Ether2
 ethernet-segment
 identifier type 0 56.56.56.56.56.56.56.02
!
!

/* Configure L2VPN */

l2vpn
 bridge group bg102
 bridge-domain bd102
 interface Bundle-Ether1.102
!
 interface Bundle-Ether2.102
!
 interface Bundle-Ether3.102
!
 interface Bundle-Ether4.102
!
 interface Bundle-Ether5.102
!
```



```
Origin incomplete, metric 0, localpref 100, weight 32768, valid, redistributed, best,
group-best
Received Path ID 0, Local Path ID 0, version 9
mac: 10:11:04:64:f2:7f
```

```
/* Verify Ethernet Segments are peering for Dual homing */
```

```
Router# show evpn ethernet-segment int bundle-Ether 1
```

```
Ethernet Segment Id Interface Nexthops
```

```
-----
0056.5656.5656.5656.5601 BE1 160.5.5.5
                               160.6.6.6
-----
```

```
/* Verify DF election */
```

```
Router# show evpn ethernet-segment int bundle-Ether 1 carving detail
```

```
Legend:
```

```
A - Load-balancing mode and Access Protection incompatible,
B - No Forwarders EVPN-enabled,
C - Backbone Source MAC missing (PBB-EVPN),
RT - ES-Import Route Target missing,
E - ESI missing,
H - Interface handle missing,
I - Name (Interface or Virtual Access) missing,
M - Interface in Down state,
O - BGP End of Download missing,
P - Interface already Access Protected,
Pf - Interface forced single-homed,
R - BGP RID not received,
S - Interface in redundancy standby state,
X - ESI-extracted MAC Conflict
SHG - No local split-horizon-group label allocated
```

```
Ethernet Segment Id Interface Nexthops
```

```
-----
0056.5656.5656.5656.5601 BE1 160.5.5.5
160.6.6.6
ES to BGP Gates : Ready
ES to L2FIB Gates : Ready
Main port :
Interface name : Bundle-Ether1
Interface MAC : 008a.9644.acdd
IfHandle : 0x080004dc
State : Up
Redundancy : Not Defined
ESI type : 0
Value : 56.5656.5656.5656.5601
ES Import RT : 5656.5656.5656 (from ESI)
Source MAC : 0000.0000.0000 (N/A)
Topology :
Operational : MH
Configured : All-active (AApF) (default)
Primary Services : Auto-selection
Secondary Services: Auto-selection
Service Carving Results:
Forwarders : 161
Permanent : 10
EVI:ETag P : 700:1, 701:1, 702:1, 703:1, 704:1, 705:1
EVI:ETag P : 706:1, 707:1, 708:1, 709:1
Elected : 76
EVI E : 100, 102, 104, 106, 108, 110
EVI E : 112, 114, 116, 118, 120, 122,
```

```

EVI E : 124, 126, 128, 130, 132, 134,
EVI E : 136, 138, 140, 142, 144, 146,
EVI E : 148, 150, 152, 154, 156, 158,
EVI E : 160, 162, 164, 166, 168, 170,
EVI E : 172, 174, 176, 178, 180, 182,
EVI E : 184, 186, 188, 190, 192, 194,
EVI E : 196, 198, 200, 202, 204, 206,
EVI E : 208, 210, 212, 214, 216, 218,
EVI E : 220, 222, 224, 226, 228, 230,
EVI E : 232, 234, 236, 238, 240, 242,
EVI E : 244, 246, 248, 250
Not Elected : 75
EVI NE : 101, 103, 105, 107, 109, 111
EVI NE : 113, 115, 117, 119, 121, 123,
EVI NE : 125, 127, 129, 131, 133, 135,
EVI NE : 137, 139, 141, 143, 145, 147,
EVI NE : 149, 151, 153, 155, 157, 159,
EVI NE : 161, 163, 165, 167, 169, 171,
EVI NE : 173, 175, 177, 179, 181, 183,
EVI NE : 185, 187, 189, 191, 193, 195,
EVI NE : 197, 199, 201, 203, 205, 207,
EVI NE : 209, 211, 213, 215, 217, 219,
EVI NE : 221, 223, 225, 227, 229, 231,
EVI NE : 233, 235, 237, 239, 241, 243,
EVI NE : 245, 247, 249
MAC Flushing mode : STP-TCN
Peering timer : 3 sec [not running]
Recovery timer : 30 sec [not running]
Carving timer : 0 sec [not running]
Local SHG label : 68663
Remote SHG labels : 1
68670 : nexthop 160.6.6.6

```

重複 IP アドレス検出

重複 IP アドレス検出機能は、重複する IP アドレスを持つすべてのホストを自動的に検出し、重複する IP アドレスを持つすべての MAC-IP ルートをブロックします。

これにより、意図せずに、または EVPN ファブリック内の悪意によって、重複する IP アドレスが割り当てられたホストから、ネットワークが保護されます。IP アドレスが重複しているホストは、ネットワーク内で不要な変化を引き起こし、同じ IP アドレスを持つホストの一方または両方でトラフィックが損失する原因となります。

システムでは、あるホストから別のホストに MAC アドレスや IP アドレスが移動する際に、それらを追跡することによって、EVPN ホストのモビリティを処理します。2つのホストに同じ IP アドレスが割り当てられている場合、IOS XR システムは両方のホストからの MAC-IP ルートの学習と再学習を維持します。一方のホストから MAC-IP ルートを学習すると、新しく学習したルートの方が以前に他のホストから学習したルートよりも優先されるため、学習のたびに1回の移動としてカウントされます。この動作は、設定されたパラメータに基づいて IP アドレスが重複としてマークされるまで続きます。

どのような場合に IP アドレスを重複としてマークし、異なるホスト間で移動する際に凍結または凍結解除するかは、次のパラメータで決定されます。これらのパラメータは設定可能です。

- **move-interval** : この間隔以内に MAC または IP アドレスが異なるホスト間で特定の回数移動すると、重複または一時的な凍結と見なされます。回数の数値は **move-count** パラメータで指定します。
- **move-count** : **move-interval** で指定した間隔以内に MAC または IP アドレスが異なるホスト間でこの回数移動すると、重複と見なされます。
- **freeze time** : MAC または IP アドレスが重複として検出された後にロックされる時間の長さ。この期間が経過すると、IP アドレスはロック解除され、再学習が許可されます。
- **retry-count** : MAC または IP アドレスが重複として検出された後、永続的に凍結されるまでの、MAC または IP アドレスのロック解除回数。

システムでは、あるホストから別のホスト（別のローカルホストか、リモートのトップオブラック（TOR）の背後にあるホストのどちらか）に IP アドレスが移動した回数を管理しています。**move-interval** パラメータで指定された間隔以内に、**move-count** パラメータで指定された回数だけ移動した IP アドレスは、重複する IP アドレスと見なされます。その IP アドレスを持つ MAC-IP ルートはすべて、**freeze-time** パラメータで指定された時間のあいだ凍結されます。特定の IP アドレスが凍結していることは **syslog** でユーザに通知されます。IP アドレスが凍結されている間、凍結された IP アドレスを持つ新しい MAC-IP ルートまたは既存の MAC-IP ルートに対する更新は、すべて無視されます。

freeze-time が経過すると、対応する MAC-IP ルートが凍結解除され、**move-count** の値がゼロにリセットされます。凍結されていないローカル MAC-IP ルートでは、リモート MAC-IP ルートがプローブモードになっている間、ARP のプローブとフラッシュが開始されます。これにより、重複検出プロセスが再開されます。

また、システムでは、特定の IP アドレスが凍結および凍結解除された回数に関する情報も保持しています。IP アドレスが、**retry-count** 回数の後に重複としてマークされると、ユーザが手動で凍結解除するまで永続的に凍結されます。凍結された MAC、IPv4、および IPv6 アドレスを手動で凍結解除するには、それぞれ次のコマンドを使用します。

- **clear l2route evpn mac** { mac-address } | all [evi evi] frozen-flag
- **clear l2route evpn ipv4** { ipv4-address } | all [evi evi] frozen-flag
- **clear l2route evpn ipv6** { ipv6-address } | all [evi evi] frozen-flag

重複 IP アドレス検出の設定

重複 IP アドレス検出機能を設定するには、次のタスクを実行します。

設定例

```
/* Ipv4 Address Duplicate Detection Configuration */
Router# configure
Router(config)# evpn
Router(config-evpn)# host ipv4-address duplicate-detection
Router(config-evpn-host-ipv4-addr)# move-count 2
Router(config-evpn-host-ipv4-addr)# freeze-time 10
Router(config-evpn-host-ipv4-addr)# retry-count 2
```

```

Router(config-evpn-host-ipv4-addr)# commit

/* Ipv6 Address Duplicate Detection Configuration */
Router# configure
Router(config)# evpn
Router(config-evpn)# host ipv6-address duplicate-detection
Router(config-evpn-host-ipv6-addr)# move-count 2
Router(config-evpn-host-ipv6-addr)# freeze-time 10
Router(config-evpn-host-ipv6-addr)# retry-count 2
Router(config-evpn-host-ipv6-addr)# commit

```

実行コンフィギュレーション

ここでは、重複する IP アドレスを検出するための実行コンフィギュレーションを示します。

```

evpn
 host ipv4-address duplicate-detection
   move-count 2
   freeze-time 10
   retry-count 2
 !
evpn
 host ipv6-address duplicate-detection
   move-count 2
   freeze-time 10
   retry-count 2
 !

```

確認

次に示す show 出力は、重複する IP アドレスの検出パラメータとリカバリパラメータの詳細を示しています。

```

Router#show l2route evpn mac-ip all detail

Flags: (Stt)=Static; (L)=Local; (R)=Remote; (F)=Flood;
(N)=No Redistribution; (Rtr)=Router MAC; (B)=Best Route;
(S)=Peer Sync; (Spl)=Split; (Rcv)=Recd;
(D)=Duplicate MAC; (Z)=Frozen MAC;

Topo ID      Mac Address      IP Address  Prod   Next Hop(s)      Seq No  Flags
Opaque Data  Type             Opaque     Data   Opaque Data Value  -----
-----
-----
33           0022.6730.0001  10.130.0.2  L2VPN  Bundle-Ether6.1300  0       SB 0 12
0x06000000

```

関連項目

- [重複 IP アドレス検出 \(238 ページ\)](#)

関連コマンド

- `evpn host ipv4-address duplicate-detection`

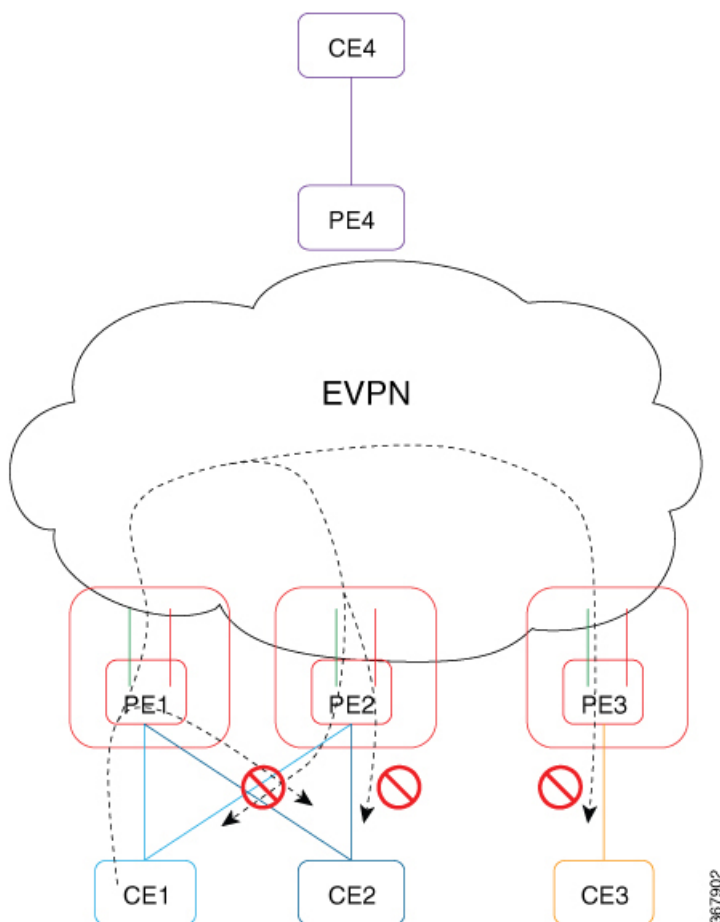
- evpn host ipv6-address duplicate-detection
- show l2route evpn mac-ip all detail

EVPN E-Tree

EVPNE-Tree機能は、MPLS コアを介したルーテッドマルチポイントイーサネットサービスを提供します。EVPNイーサネットツリー (E-Tree) サービスを使用することで、接続回線 (AC) をルートサイトまたはリーフサイトとして定義できます。これにより、ネットワークのロードバランシングやループの回避が容易になります。

次のトポロジでは、PE1、PE2、およびPE3をリーフACと見なし、PE4をルートACと見なしています。ルートACは、他のすべてのACと通信できます。リーフACは、ルートACと通信できますが、L2ユニキャストまたはL2 BUMトラフィックのどちららを使用しても他のリーフACとは通信できません。E-Treeのリーフとして設定されていないPEは、デフォルトでルートと見なされます。この機能では、PE単位でのリーフサイトまたはルートサイトのみがサポートされます。

図 33: EVPN E-Tree



E-Tree リーフは、EVIブリッジドメイン (BD) ごとに設定されます。BDのルートおよびリーフ EVI は、単一のルーテッドターゲット (RT) をエクスポートまたはインポートします。E-Tree リーフが EVI ごとに設定されるため、次のことが導かれます。

- すべての AC がリーフ インジケータを継承します。
- 同じ EVI の AC (リーフ) 間でスプリットホライズン グループが自動的に有効になります。
- 各 PE リーフは、Ethernet Segment per Ethernet Auto Discovery (ES-EAD) ごと、Ethernet Segment Identifier (ESI) ごと、およびリーフ インジケータと E-Tree ラベルを持つ ES-EAD ESI 0 ルートごとに、BGP へのアドバタイズを行います。
- この EVI の下で学習されたすべてのローカル MAC は、E-Tree リーフ インジケータを使用して BGP に再アドバタイズされます。
- PE はそれぞれリモート PE のリストを維持します。



- (注) E-Tree リーフ設定を変更した場合、ローカルに学習された MAC アドレスはすべて消去されます。ローカルに学習された MAC アドレスは、ブリッジポートのサブインターフェイスでの「カプセル化」または「リライト」、あるいは「スプリットホライズングループ」設定が、ブリッジポートの下で変更された場合であっても、すべて消去されます。

ユニキャストのルール

次の表は、ルートおよびリーフでタイプ 2 MAC ルートを受信したときのユニキャストのルールを示しています。

受信した MAC ルート	MAC ルートの処理
ルート EVI (BD) からの非ローカル ESI を持つ MAC アドレス	リモート MAC アドレス。
ルート EVI (BD) からのローカル ESI を持つ MAC アドレス	MAC アドレスの同期、再発信。
リーフ EVI (BD) からの非ローカル ESI を持つ MAC アドレス	リモート MAC アドレス。 リーフ インジケータを持つリモート MAC ルートはドロップされます。

受信した MAC ルート	MAC ルートの処理
リーフ EVI (BD) からの非ローカル ESI を持つ MAC アドレス	MAC アドレスの同期、再発信。MAC アドレスはローカル AC を指し示します。 ローカル AC の障害時に、同期 MAC ルートがリモート MAC ルートになります。リーフ インジケータを持つリモート MAC ルートは、ピアリング PE を指し示すのではなく、ドロップされます。

マルチキャストのルール

マルチキャストは、次の場合にネットワーク内のリーフの検出に使用されます。

- どの EVI が E-Tree リーフとして設定されているかを他のネットワーク PE に示すために、E-Tree 拡張コミュニティを持つ RT-1 ES-EAD ESI-0 ルートが EVI (BD) ごとに送信される場合。
- リーフ EVI (BD) で、E-Tree 拡張コミュニティを持つ RT-1 ES-EAD ESI-0 ルートおよび RT-3 IMCAST ルートを受信した場合。



(注) ローカル EVI (BD) ごとのスプリットホライズングループによって、ローカル AC から AC へのトラフィックフローが阻止されます。

CE1 と CE4 間の通信 (サブネット間)

1. CE1 が、自身のゲートウェイ (IRB インターフェイス) に ARP 要求を送信します。CE1 が、BVI の IP アドレスを解決します。
2. ARP 要求が PE1 のブリッジドメインに到達します。PE1 が、エントリを学習し、フラッシュします。
3. すべてのリモート PE への ARP 要求のうち、プルーニングされたものがドロップされます。これは、すべてのルートのリモート PE およびローカル BVI インターフェイスに複製されます。
4. PE1 の BVI インターフェイスが、自身の BVI IP アドレスと BVI MAC アドレスを使用して、ARP 応答を CE1 に送信します。
5. 同時に、ホストルーティングが設定されているため、PE1 がルートタイプ 2 を使用して EVPN を介して CE1 ホストルートをアドバタイズします。
6. タイプ 2 ルートの受信後、PE に基づいて異なるルールが適用されます。ルートタイプ 2 を受信した後、それぞれの PE の動作は次のようになります。
 1. PE2 : ESI の MAC および IP アドレスがローカル ESI と一致します。MAC アドレスを同期ルートとしてプログラムします。RIB の IP アドレスを、PE1 を指し示すようにプ

プログラムしますが、MAC アドレスは CE1 を指し示します。CE1 へのリンク障害が発生すると、MAC アドレスは、ピアリング PE1 を指し示すのではなく、ハードウェアでドロップ済みとマークされます。

2. PE3 : ESI の MAC および IP アドレスはローカルではありません。ローカル EVI (BD) はリーフであるため、MAC アドレスはハードウェアでドロップ済みとマークされます。RIB の IP アドレスを、PE1 を指し示すようにプログラムします。
 3. PE4 : ESI の MAC および IP アドレスはローカルではありません。ローカル EVI (BD) はルートであるため、MAC をリモートとしてプログラムします。RIB の IP アドレスを、PE1 を指し示すようにプログラムします。
7. PE4 が CE1 を認識します。CE1 と CE4 が相互に通信します。
 8. たとえば、CE4 から着信するルーティング パケットが PE4 に到達します。IP ルックアップが実行されます。PE1 が、ホスト ルート /32 によって最適な宛先として検出されます。PE1 にパケットが転送されます。
 9. PE1 で、IP ルックアップが実行されます。BVI インターフェイスが見つかります。パケットが、ARP によって学習された宛先 MAC アドレスとして、CE1 を使用してカプセル化されます。送信元 MAC アドレスは BVI MAC アドレスのままです。宛先 MAC アドレスのルックアップが、対応するブリッジドメインで実行されます。適切な出力インターフェイスにパケットが転送されます。



(注) CE1 が通信を開始する前に CE4 が CE1 にパケットを送信した場合、パケットがピアリング PE2 に到達する可能性があります。GLEAN の隣接関係が影響を受け、解決するまでトラフィックはドロップされます。エントリを解決するため、PE2 BVI インターフェイスはプローブを開始します。

1. BVI からの ARP プローブが、すべての AC に送信され、EVI にも送信されます (L2 ストレッチ)。
2. PE1 と PE3 が、EVI インターフェイスから ARP プローブを受信し、すべてのローカル AC に複製します。CE1 が ARP 応答を送信します。すべてのリーフ上の IRB が分散型エニークキャスト ゲートウェイで設定されているため、PE1 BVI インターフェイスが応答を受け取ります。

CE1 と CE3 間の通信 (サブネット内)

1. CE1 と CE3 は同じサブネット内にあります。
2. CE1 が、CE3 に ARP 要求を送信します。
3. ARP 要求が PE1 のブリッジドメインに到達します。PE1 が、エントリを学習し、フラッディングします。

4. すべてのリモート PE への ARP 要求のうち、プルーニングされたものがドロップされます。これは、すべてのルートのリモート PE およびローカル BVI インターフェイスに複製されます。
5. CE3 は、CE1 から ARP 要求を受信しません。CE1 は、CE3 と通信しません。
6. CE1 と CE3 をサブネット内で通信させる場合は、ローカルとリモートの両方の PE で、BVI インターフェイスの配下で `local_proxy_arp` を設定する必要があります。

CE1 と CE2 間の通信（サブネット内）

1. CE1 と CE2 は同じサブネット内にあります。
2. CE1 が、CE2 に ARP 要求を送信します。
3. ARP 要求が PE1 のブリッジ ドメインに到達します。PE1 が、エントリを学習し、フラッディングします。
4. すべてのリモート PE への ARP 要求のうち、プルーニングされたものがドロップされます。共通のスプリットホライズングループが原因で、どのローカル AC にも複製されません。
5. CE2 は CE1 から ARP 要求を受信しません。CE1 は CE2 と通信しません。



(注) ローカル CE1 とリモート CE1 間の通信は次のようになります。

- PE1 のローカル CE1 から PE2 のリモート CE1 への BUM トラフィックは、PE2 がプルーニングされているためドロップされます。
- AC 対応 VLAN バンドル機能の場合、PE1 のローカル CE1 から PE1 のローカル CE1 への BUM トラフィックは、ESI フィルタリングによってドロップされます。

EVPN E-Tree の設定

EVPN E-Tree 機能を設定するには、次の作業を実行します。

```
/* Configure EVPN E-Tree service on PE1 and PE2 */

Router# configure
Router(config)# evpn
Router(config-evpn)# evi 1
Router(config-evpn-evi)# etree leaf
```

設定例

```
/* Configure MCLAG on PE1 for dual-home all-active EVPN */

Router# configure
Router(config)# redundancy
```

```

Router(config-redundancy)# ICCP group 1
Router(config-iccp-group)# mlacp node 1
Router(config-iccp-group)# mlacp system mac 000d.0002.0011
Router(config-iccp-group)# mlacp system priority 1
Router(config-iccp-group)# mode singleton
Router(config-iccp-group)# backbone
Router(config-iccp-group-backbone)# interface Bundle-Ether110
!

Router# configure
Router(config)# interface Bundle-Ether1121
Router(config-if)# description DH-F2-1
Router(config-if)# lacp switchover supress-flaps 300
Router(config-if)# mlacp iccp-group 1
Router(config-if)# bundle wait-while 100
Router(config-if)# load-inerval 30

/* Configure MCLAG on PE2 for dual-home all-active EVPN */

Router# configure
Router(config)# redundancy
Router(config-redundancy)# ICCP group 1
Router(config-iccp-group)# mlacp node 2
Router(config-iccp-group)# mlacp system mac 000d.0002.0011
Router(config-iccp-group)# mlacp system priority 1
Router(config-iccp-group)# mode singleton
Router(config-iccp-group)# backbone
Router(config-iccp-group-backbone)# interface Bundle-Ether120
!

Router# configure
Router(config)# interface Bundle-Ether1121
Router(config-if)# description DH-F2-1
Router(config-if)# lacp switchover supress-flaps 300
Router(config-if)# mlacp iccp-group 1
Router(config-if)# bundle wait-while 100
Router(config-if)# load-inerval 30

/* Configure AC interface on PE1 and PE2*/

Router(config)# interface Bundle-Ether1121.1 l2transport
Router(config-l2vpn-subif)# encapsulation dot1q 1
Router(config-l2vpn-subif)# rewrite ingress tag pop 1 symmetric

/* Configure BVI interface on PE1 and PE2 */

Router(config)# interface BVI1
Router(config-if)# host-routing
Router(config-if)# vrf vpn1
Router(config-if-vrf)# ipv4 address 192.0.2.1 255.255.255.0
Router(config-if-vrf)# proxy-arp
Router(config-if-vrf)# local-proxy-arp
Router(config-if-vrf)# 2001:DB8::1/32
Router(config-if-vrf)# mac-address 10.1111.aaaa
Router(config-if-vrf)# load-interval 30

/* Configure the bridge on PE1 and PE2 */

Router(config)# l2vpn
Router(config-l2vpn)# bridge group bgl
Router(config-l2vpn-bg)# bridge-domain bd1
Router(config-l2vpn-bg-bd)# interface Bundle-Ether1121.1
Router(config-l2vpn-bg-bd-ac)# exit
Router(config-l2vpn-bg-bd)# routed interface BVI1

```

```
Router(config-l2vpn-bg-bd-bvi)# exit
Router(config)# evpn
Router(config-evpn)# evi
Router(config-evpn-evi)# commit
```

実行コンフィギュレーション

ここでは、EVPN E-Tree の実行コンフィギュレーションを示します。

```
/* EVPN E-Tree running configuration on PE1 */
redundancy
iccp
  group 1
    mlacp node 1
    mlacp system mac 000d.0002.0011
    mlacp system priority 1
    mode singleton
    backbone
    interface Bundle-Ether110
    !
interface Bundle-Ether1121
description DH-F2-1
lACP switchover suppress-flaps 300
mlacp iccp-group 1
bundle wait-while 100
load-interval 30

!

evpn
evi 1
  etree leaf
  !

l2vpn
bridge group bg1
  bridge-domain bd1
  interface Bundle-Ether1121.1
  routed interface BVI1
  !
  evi 1

interface Bundle-Ether1121.1
l2transport
  encapsulation dot1q 1
  rewrite ingress tag pop 1 symmetric
  !
!
interface BVI1
  host-routing
  vrf vpn1
  ipv4 address 192.0.2.1 255.255.255.0
  proxy-arp
  local-proxy-arp
  ipv6 address 2001:DB8::1/32
  mac-address 10.1111.aaaa
  load-interval 30
  !
!

/* EVPN E-Tree running configuration On PE2 */
redundancy
```

```

iccp
group 1
mlacp node 2
mlacp system mac 000d.0002.0011
mlacp system priority 1
mode singleton
backbone
interface Bundle-Ether120
!
!
interface Bundle-Ether1121
description DH-F2-1
l2transport
l2transport encapsulation dot1q 1
l2transport rewrite ingress tag pop 1 symmetric
mlacp iccp-group 1
bundle wait-while 100
load-interval 30

evpn
evi 1
etree leaf
!
!

l2vpn
bridge group bg1
bridge-domain bd1
interface Bundle-Ether1121.1
routed interface BVI1
!
evi
!
interface Bundle-Ether1121.1
l2transport
l2transport encapsulation dot1q 1
l2transport rewrite ingress tag pop 1 symmetric
!
!
interface BVI1
host-routing
vrf vpn1
ipv4 address 192.0.2.1 255.255.255.0
proxy-arp
local-proxy-arp
ipv6 address 2001:DB8::1/32
mac-address 10.1111.aaaa
load-interval 30
!
!

```

確認

次の項に示す `show` 出力には、EVPN E-Tree の設定の詳細が表示されます。

```

Router#show bgp l2vpn evpn rd 10.0.0.1:0
Route Distinguisher: 10.0.0.1:0
*> [1][10.0.0.1:1][0000.0000.0000.0000.0000][4294967295]/184
      0.0.0.0                                0 i
*> [1][10.0.0.1:2][0000.0000.0000.0000.0000][4294967295]/184
      0.0.0.0                                0 i

```

Each RT-1 ES0 has up to 200 RTs. Two RT-1 ES0 is displayed if you have 250 RTs.

次の出力は、RT-1 ES0 でアドバタイズされたリーフ `excom` を示しています。

```
Router#show bgp l2vpn evpn rd 10.0.0.1:0
[1][10.0.0.1:1][0000.0000.0000.0000][4294967295]/184
Extended community: EVPN E-TREE:0x00:824348 RT:100:1 RT:100:2 RT:100:3 RT:100:4 RT:100:5
RT:100:10 RT:100:11
RT:100:12 RT:100:13 RT:100:14 RT:100:15 RT:100:16 RT:100:17 RT:100:18 RT:100:19 RT:100:20
RT:100:21 RT:100:22 RT:100:23
RT:100:24 RT:100:25 RT:100:26 RT:100:27 RT:100:28 RT:100:29 RT:100:30 RT:100:31 RT:100:32
RT:100:33 RT:100:34 RT:100:35
RT:100:36 RT:100:37 RT:100:38 RT:100:39 RT:100:40 RT:100:41 RT:100:42 RT:100:43 RT:100:44
RT:100:45 RT:100:46 RT:100:47
RT:100:48 RT:100:49 RT:100:50
```

次の出力は、MAC アドバイズメントの RT 2 を示しています。

```
Router#show bgp l2vpn evpn rd 10.0.0.1:1 [2][1][48][0011.1100.0001][0]/104
Paths: (2 available, best #1)
  Advertised to peers (in unique update groups):
    172.16.0.1
  Path #1: Received by speaker 0
  Advertised to peers (in unique update groups):
    172.16.0.1
  Local
    0.0.0.0 from 0.0.0.0 (10.0.0.1)
    Origin IGP, localpref 100, valid, redistributed, best, group-best, import-candidate,
  rib-install
    Received Path ID 0, Local Path ID 1, version 315227
    Extended community: SoO:192.168.0.1:1 EVPN E-TREE:0x01:0 RT:100:1
    EVPN ESI: 0020.0000.0000.0000.1121
```

次の出力は、MAC アドレスと IP アドレスのアドバイズメントにおける 1 つの RT 2 を示しています。

```
Router#show bgp l2vpn evpn rd 10.0.0.1:1 [2][1][48][0011.1100.0001][32][101.0.1.103]/136
Tue Oct 2 16:44:26.755 EDT
BGP routing table entry for [2][1][48][0011.1100.0001][32][101.0.1.103]/136, Route
Distinguisher: 10.0.0.1:1
Versions:
  Process          bRIB/RIB  SendTblVer
  Speaker          313139   313139
  Local Label: 820002
Last Modified: Oct 2 13:26:08.477 for 03:18:18
Paths: (2 available, best #1)
  Advertised to peers (in unique update groups):
    172.16.0.1
  Path #1: Received by speaker 0
  Advertised to peers (in unique update groups):
    172.16.0.1
  Local
    0.0.0.0 from 0.0.0.0 (10.0.0.1)
    Second Label 825164
    Origin IGP, localpref 100, valid, redistributed, best, group-best, import-candidate,
  rib-install
    Received Path ID 0, Local Path ID 1, version 313139
    Extended community: Flags 0xe: SoO:192.168.0.1:1 EVPN E-TREE:0x01:0 RT:100:1
RT:991:1
    EVPN ESI: 0020.0000.0000.0000.1121
```

次の出力は、EVPN における RT-3 包含マルチキャストおよび RT-1 ES0 ルートの集約を示しています。

```

Router#show evpn evi vpn-id 1 inclusive-multicast detail
1          MPLS    0          192.168.0.1
  TEPid   : 0x02000001
  PMSI Type: 0
  Nexthop: 192.168.0.1
  Label   : 810120
  Source  : Remote
  E-Tree: Leaf
1          MPLS    0          10.0.0.1
  TEPid   : 0xffffffff
  PMSI Type: 6
  Nexthop: ::
  Label   : 820120
  Source  : Local
  E-Tree: Leaf
1          MPLS    0          172.16.0.1
  TEPid   : 0x02000003
  PMSI Type: 0
  Nexthop: 172.16.0.1
  Label   : 840120
  Source  : Remote
  E-Tree: Root

```

関連項目

- [EVPN E-Tree \(241 ページ\)](#)

関連コマンド

- etree leaf
- show bgp l2vpn evpn rd

IRB での DHCPv4 リレー

統合ルーティングおよびブリッジング (IRB) での DHCPv4 リレー機能は、EVPN オールアクティブマルチホーミングのシナリオにおいて DHCP のサポートをエンドユーザに提供します。この機能により、トラフィックのフラグディングの削減、ロードシェアリングの増加、トラフィックの最適化、リンクやデバイスの障害時におけるコンバージェンスの高速化、およびデータセンター自動化のシンプル化が実現します。

DHCPv4 リレー エージェントは、エンドユーザ用のアドレス (/32) 割り当てを要求するために、アクセス インターフェイスを介して着信した要求パケットを外部 DHCPv4 サーバに向けて送信します。DHCPv4 リレー エージェントは、DHCPv4 バインディングと、割り当てられたアドレスの各ルート エントリを維持しません。そのため、エンドユーザに対してステートレスとして機能します。

DHCPv4 リレー プロファイルはブリッジグループ仮想インターフェイス (BVI) インターフェイス上で設定されます。BVI インターフェイスは、エンドユーザのルーティング ドメインとブリッジドメインを統合することによってアクセスインターフェイスとして機能します。これにより、レイヤ 2 接続回線 (AC) からの DHCPv4 要求がホスト IPv4 アドレス (/32) の外部 DHCP サーバにリレーされます。

マルチホーミング オールアクティブ EVPN ゲートウェイ

マルチホーミング オールアクティブ EVPN ゲートウェイは、エニーキャスト IP アドレスと MAC アドレスを使用して設定されます。NCS 5500 および NCS 540 デバイスは、集中型の L2 または L3 ゲートウェイを備えています。IRB は、ネイティブ EVPN と MAC ラーニングに基づいて、分散エニーキャスト IP アドレスとエニーキャスト MAC アドレスを使用します。スタティッククライアントは、エニーキャストゲートウェイアドレスを使用して、デフォルトゲートウェイとして設定されます。DHCP クライアントは、BVI インターフェイスを介して IP アドレス割り当てのための DHCP 要求を送信します。L2 アクセスは、シングルホーミングまたはマルチホーミングのどちらにもなり、すべてのアクセスプロトコルが IRB でサポートされるわけではありません。BVI の IP アドレスは、エンドユーザのデフォルトゲートウェイとして機能します。外部 DHCPv4 サーバは、この BVI インターフェイスの IP アドレスをルートオプションのデフォルトゲートウェイとして提供します。インターネットゲートウェイでは EVPN は設定されません。

EVPN IRB ルート配布

EVPN IRB DHCPv4 では、DHCP アプリケーションプロセスと DHCP パケット転送は EVPN IRB L2 および L3 ルーティングとは独立しています。ステートレス DHCP リレーに関するサブスクライバルーティング情報は、ありません。ただし、DHCP クライアントは、L2 および L3 ブリッジングおよびルーティングを行うために、EVPN コアでスタティッククライアントと同様に機能します。DHCP リレーエージェントで **relay information option** コマンドおよび **relay information option vpn** コマンドを設定すると、DHCP リレーエージェントによって DHCP オプション 82 のサブオプション（サブネット選択や VPNID オプションなど）が挿入されます。これらのオプションは、IP アドレスの割り当て時に DHCP サーバによって考慮されます。

DHCPv4 サーバにおけるエンドユーザの IP アドレスの割り当ては、**relay agent information** オプション（リモート ID と回線 ID）に基づいて行われます。DHCP クライアントは L2 AC インターフェイスを使用して、EVPN ブリッジドメインにアクセスし、BVI インターフェイスをデフォルトゲートウェイとして使用します。そのためクライアントは、BVI インターフェイスの同じサブネットの DHCP サーバから IP アドレスを取得する必要があります。

DHCPv4 アプリケーションが **relay-option policy {encapsulate | drop | keep}** コマンドに基づいて BVI インターフェイスを介してアクセス側の DHCPv4 パケットを受信すると、DHCPv4 アプリケーションには、DHCPv4 サーバのオプション 82 リレーエージェント情報、リモート ID、および回線 ID が追加されます。

次の表に、設定されたリレー情報の詳細を得るために DHCPv4 リレー パケットを絞込み属性を示します。この表に記載されている情報は、**relay-option policy {encapsulate | drop | keep}** コマンドの設定に使用します。

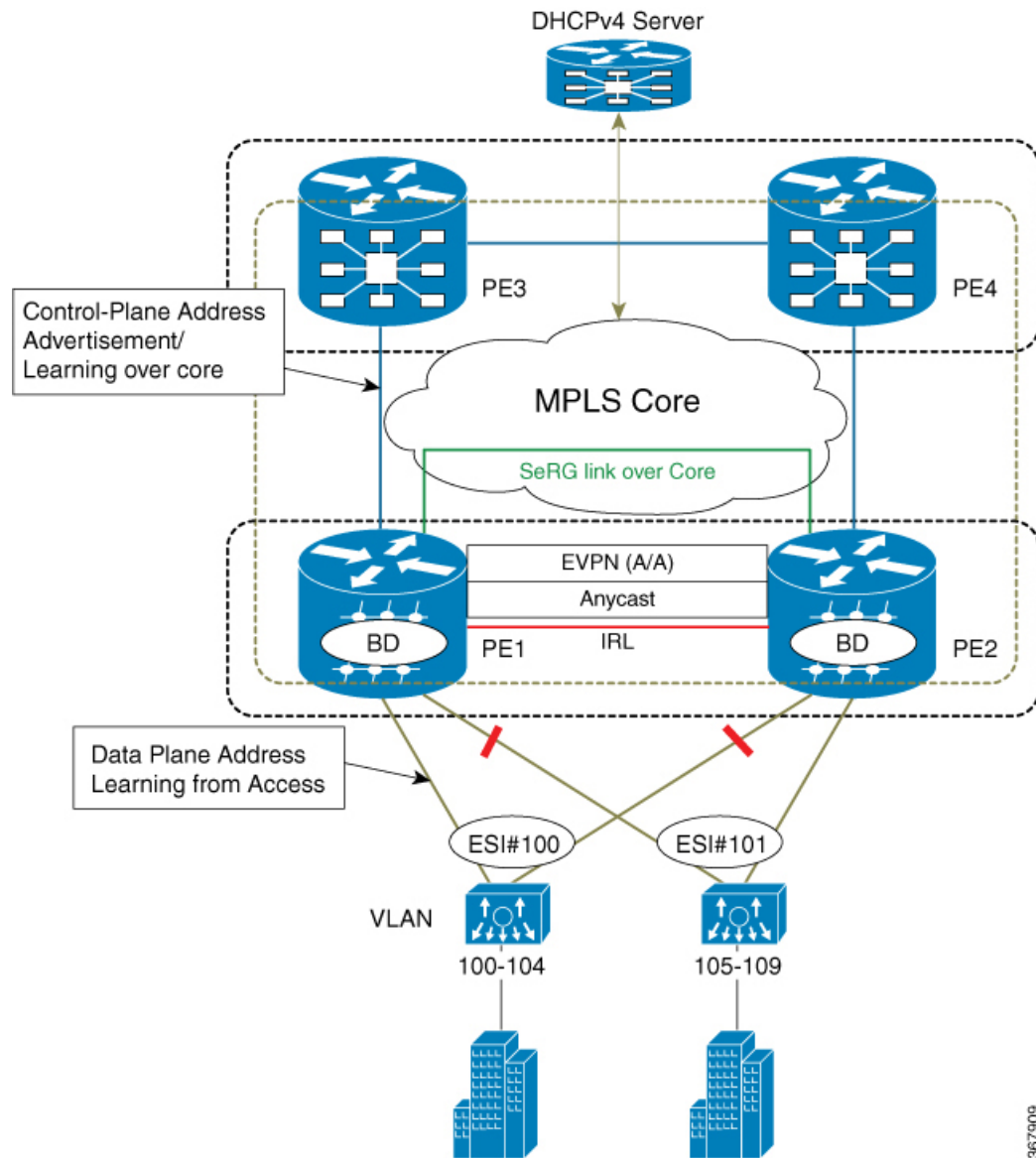
リレーオプションポリシー	DHCPv4 アクセス側パケット	ローカル設定	DHCPv4 リレー パケットの決定
カプセル化	リレー情報なし	リモート ID を持つ DHCPv4 プロファイル 回線 ID を持つ L2 トランスポート AC	リモート ID と回線 ID を持つリレーエージェント

リレーオプションポリシー	DHCPv4 アクセス側パケット	ローカル設定	DHCPv4 リレーパケットの決定
カプセル化	リレー情報 (リモート ID と回線 ID)	リモート ID を持つ DHCPv4 プロファイル 回線 ID を持つ L2 トランスポート AC	リレーエージェント情報をローカル設定 (リモート ID と回線 ID) にオーバーライド
カプセル化	リレー情報なし	リモート ID および VPN 情報を持つ DHCPv4 プロファイル 回線 ID を持つ L2 トランスポート AC	リモート ID、回線 ID、および VPN 情報を持つリレーエージェント
維持	リレー情報 (リモート ID と回線 ID)	設定なし	DHCPv4 リレーエージェントはリレー情報を変更しない
維持	リレー情報 (リモート ID と回線 ID)	リモート ID を持つ DHCPv4 プロファイル 回線 ID を持つ L2 トランスポート AC	DHCPv4 リレーエージェントはリレー情報を変更しない
維持	リレー情報 (リモート ID と回線 ID)	リモート ID および VPN 情報を持つ DHCPv4 プロファイル 回線 ID を持つ L2 トランスポート AC	DHCPv4 リレーエージェントはリレー情報を変更しない
ドロップ	リレー情報 (リモート ID と回線 ID)	設定なし	リレーエージェント情報を除外し、リレーパケットに「None」を追加
ドロップ	リレー情報 (リモート ID と回線 ID)	リモート ID を持つ DHCPv4 プロファイル 回線 ID を持つ L2 トランスポート AC	リレーエージェント情報を除外し、リレーパケットに「None」を追加
ドロップ	リレー情報 (リモート ID と回線 ID)	リモート ID および VPN 情報を持つ DHCPv4 プロファイル 回線 ID を持つ L2 トランスポート AC	リレーエージェント情報を除外し、リレーパケットに「None」を追加

DHCP 要求転送パス

クライアントは、要求をアクセススイッチにブロードキャストし、DH-AA を EVPN PE ルータにブロードキャストします。アクセス スイッチはロード バランシングを行います。アクセス スイッチのロード バランシング設定は、DHCP 要求を送信する DH-AA および DHCP の PE に影響を及ぼします。DHCP 要求は、DHCP リレーで設定されたブリッジドメイン (BD) BVI インターフェイスに到達します。オールアクティブ PE ルータは同じ IP アドレスを使用して設定されているため、BVI IP アドレスを DHCP リレー送信元 IP アドレスとして使用することはできません。DHCPv4 リレーの場合、アクセス (BVI) インターフェイスはリレープロファイルを使用して関連付けられます。デバイス インターセプト パケットは BVI インターフェイスを介して受信され、各リレー プロファイルはゲートウェイ IP アドレス (GIADDR) を使用して定義されます。GIADDR は、DHCPv4 サーバに向けて開始されたリレー パケットの送信元 IP アドレスとして機能します。この GIADDR は、それぞれの BVI インターフェイスのトップ オブ ラック (ToR) 全体で一意です。一意の IPv4 アドレスを持つループバック インターフェイスは、DHCP サーバに到達可能な VRF で設定できます。DHCP リレー送信元アドレスの設定はサポートされていません。

図 34: EVPN オールアクティブ マルチホーミングを行うための DHCPv4 サーバの処理における PON の動作



367909

EVPN オールアクティブ マルチホーミングを行うための DHCPv4 サーバの処理における PON の動作

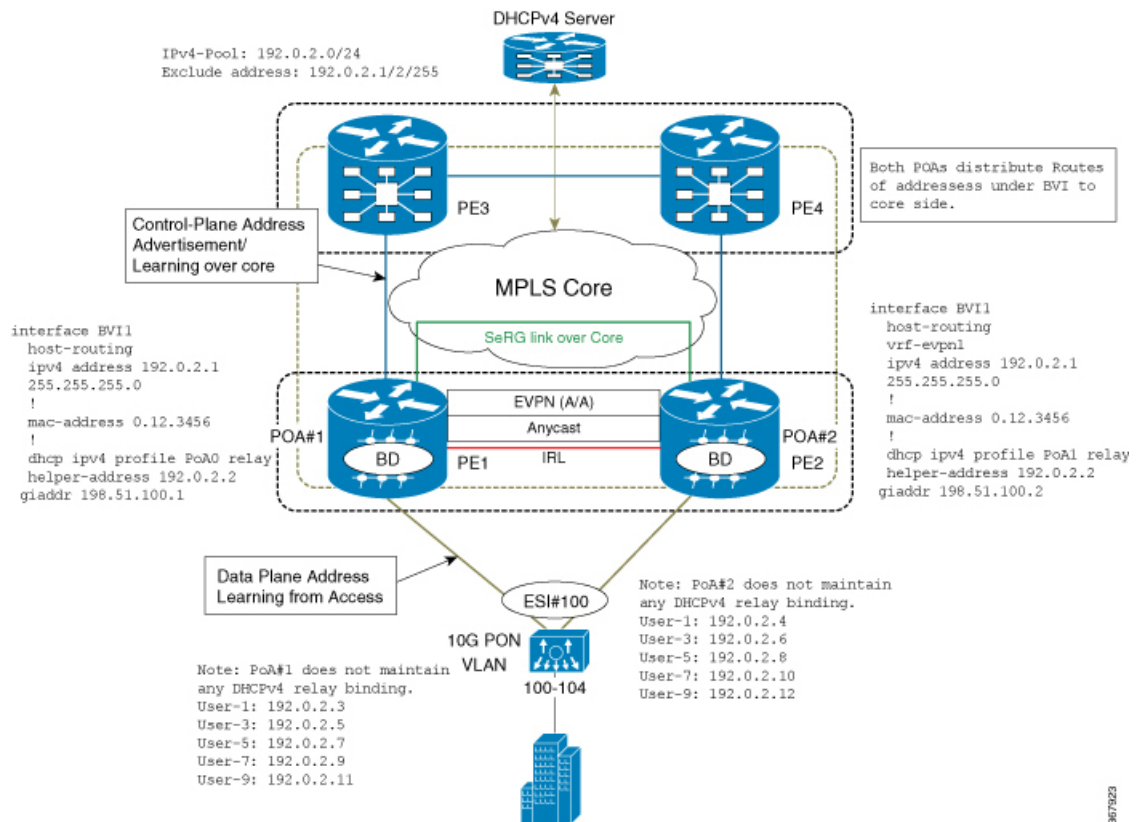
このトポロジでは、PE1 と PE2 はアクセス側のエッジルータです。エッジルータは、ルーティングおよびブリッジングドメインを関連付けて DHCPv4 パケットを処理することにより、BVI インターフェイスを介した CE (10G-OLT) として機能します。CE (L2 OLT、PON、任意の L2 ドメインスイッチ) は、着信した制御パケット (DHCPv4 パケット) を、それぞれの PE に接続されているポートチャネルに向けてハッシュします。CE は、エンドユーザから受信したパケットの 5 つのタプル (src mac、dst mac、src-ip、dst-ip、L4 (tcp/udp) dst/src port) に基づいてハッシュメカニズムを利用し、転送メカニズムを定義します。そのために、デュアルホー

ムのアクティブ-アクティブ モデルにおいて、各 PE への制御パケットのロード バランシング におけるポート チャネルを選択します。

デフォルト VRF での EVPN および DHCPv4 サーバの DHCPv4 リレー処理

EVPN IRB および DHCPv4 サーバを介した DHCPv4 リレーは、同じデフォルト VRF に存在します。DHCPv4 リレー プロファイルは、デフォルト VRF 配下の DHCPv4 アドレスのヘルパー アドレスに関連付けられています。この特定のシナリオでは、PE には、DHCPv4 サーバに向けてリレーされた DHCPv4 パケット内のリレーエージェント情報は追加されません。ただし、DHCPv4 リレー プロファイルは、エニーキャスト IRB アドレス以外の ToR にわたって一意の GIADDR で定義されます。そうしないと、DHCPv4 サーバは、リンクの選択やサブネットの選択を行わないエンド ユーザのアドレス割り当てを実行することが困難になります。VPN 値を 0xFF として VPN 情報が追加されることで、PE にリレーエージェント情報が追加されます。

図 35: デフォルト VRF での EVPN および DHCPv4 サーバの DHCPv4 リレー処理



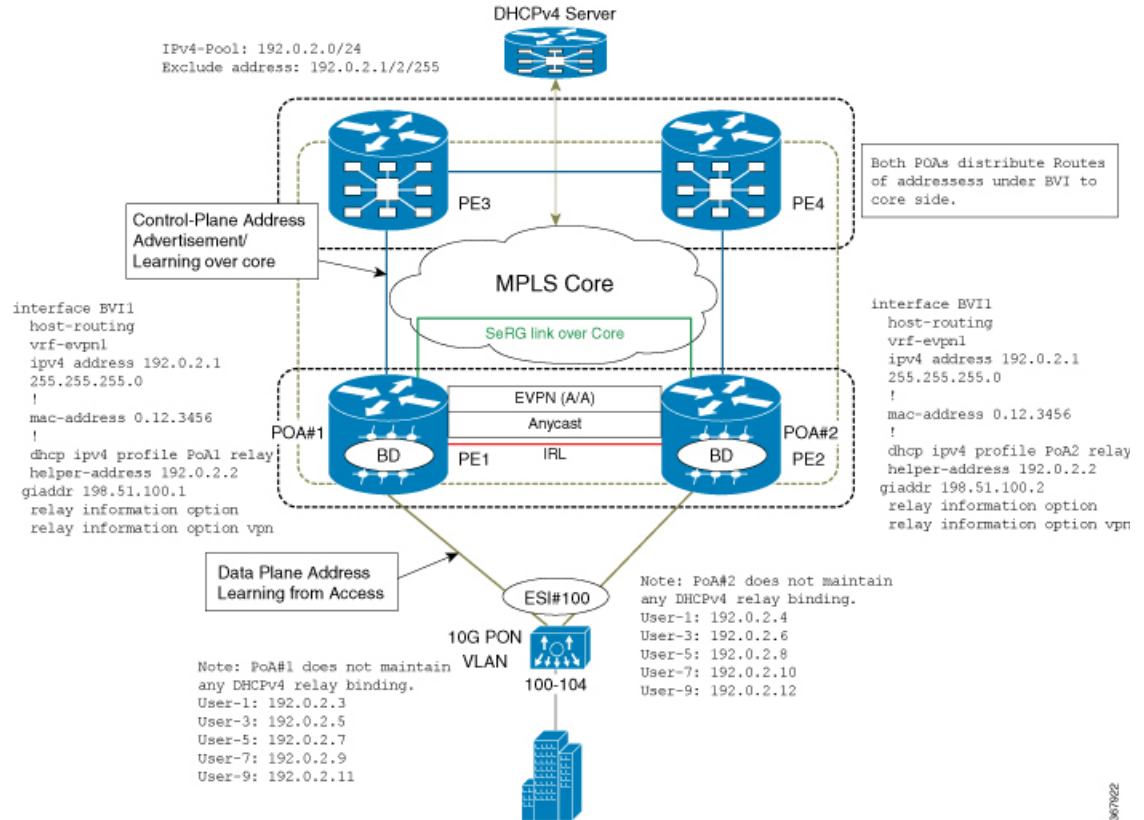
異なる VRF での EVPN および DHCPv4 サーバの DHCPv4 リレー処理

EVPN IRB および DHCPv4 サーバを介した DHCPv4 リレーは、異なる VRF に存在します。または、DHCPv4 サーバに、ToR にわたって一意の GIADDR (エニーキャスト IRB アドレスとは異なる) があります。そうしないと、DHCPv4 サーバは、リンクの選択やサブネットの選択を行わないエンド ユーザのアドレス割り当てを実行することが困難になります。DHCPv4 サーバが、evpn の関連するエニーキャスト IRB アドレスのサブネット プールから確実にアドレス割

り当てを行えるように、DHCPv4 リレー エージェントの ToR が仮想サブネット選択（リンク選択、server-id、vrf-id）を暗に指定する方法があります。それには、DHCPv4 サーバに向けてリレーされたDHCPv4検出および要求パケットに、リレーエージェント情報（オプション82）を追加します。

このトポロジでは、10G PON は、それぞれの接続ポイント（PoA）#1、#2 に向けて均等に DHCP ブロードキャストを配信し、パケットが外部 DHCPv4 サーバにリレーされます。

図 36:異なる VRFでの EVPN および DHCPv4 サーバの DHCPv4 リレー処理



IRB での DHCPv4 リレーの設定

IRB で DHCPv4 リレーを設定するには、次の作業を実行します。

設定例

```

/* PE1 configuration */

Router# configure
Router(config)# interface BVI1
Router(config-if)# host-routing
Router(config-if)# vrf-evpn1
Router(config-if)# ipv4 address 192.0.2.1 255.255.255.0
Router(config-if)# exit
    
```

```

Router(config)# mac-address 0.12.3456
!
Router# configure
Router(config)# dhcp ipv4
Router(config-dhcpv4)# profile PoA1 relay
Router(config-dhcpv4-relay-profile)# helper-address 192.0.2.2 giaddr 198.51.100.1
Router(config-dhcpv4-relay-profile)# relay information option vpn
Router(config-dhcpv4-relay-profile)# relay information option vpn-mode rfc
Router(config-dhcpv4-relay-profile)# commit

/* PE2 configuration */

Router# configure
Router(config)# interface BVI1
Router(config-if)# host-routing
Router(config-if)# vrf-evpn1
Router(config-if)# ipv4 address 192.0.2.1 255.255.255.0
Router(config-if)# exit
Router(config)# mac-address 0.12.3456
!
Router# configure
Router(config)# dhcp ipv4
Router(config-dhcpv4)# profile PoA2 relay
Router(config-dhcpv4-relay-profile)# helper-address 192.0.2.2 giaddr 198.51.100.2
Router(config-dhcpv4-relay-profile)# relay information option vpn
Router(config-dhcpv4-relay-profile)# relay information option vpn-mode rfc
Router(config-dhcpv4-relay-profile)# commit

```

次の例は、リモート ID と回線 ID を持つリレーエージェント情報を追加するための DHCPv4 リレー エージェントの設定を示しています。リモート ID は、BVI インターフェイスの下で関連付けられている DHCPv4 リレープロファイルで設定されます。DHCPv4 は、回線 ID を持つ L2 トランスポート AC を使用して設定されます。

```

Dhcp ipv4
Profile RELAY relay
  Relay information option remote-id format-type ascii cisco
  Relay information policy encapsulate
!

interface BE1.100 relay information option circuit-id format-type hex cisco
!
interface bvi relay RELAY
!

```

実行コンフィギュレーション

ここでは、RB での DHCPv4 リレーの実行コンフィギュレーションを示します。

```

/* PE1 Configuration */
interface BVI1
host-routing
vrf-evpn1
ipv4 address 192.0.2.1 255.255.255.0
!
mac-address 0.12.3456
!
dhcp ipv4 profile PoA1 relay
helper-address 192.0.2.2 giaddr 198.51.100.1
relay information option
relay information option vpn-mode rfc

```

```

/* PE2 Configuration */
interface BVI1
  host-routing
  vrf-evpn1
  ipv4 address 192.0.2.1 255.255.255.0
  !
  mac-address 0.12.3456
  !
  dhcp ipv4 profile PoA2 relay
  helper-address 192.0.2.2 giaddr 198.51.100.2
  relay information option
  relay information option vpn-mode rfc

```

確認

RB での DHCPv4 リレーの設定を確認します。

```

/* Verify DHCPv4 relay statistics
Router# show dhcp vrf default ipv4 relay statistics

```

DHCP IPv4 Relay Statistics for VRF default:

TYPE	RECEIVE	TRANSMIT	DROP
DISCOVER	2000	2000	0
OFFER	2000	2000	0
REQUEST	5500	5500	0
DECLINE	0	0	0
ACK	5500	5500	0
NAK	0	0	0
RELEASE	500	500	0
INFORM	0	0	0
LEASEQUERY	0	0	0
LEASEUNASSIGNED	0	0	0
LEASEUNKNOWN	0	0	0
LEASEACTIVE	0	0	0
BOOTP-REQUEST	0	0	0
BOOTP-REPLY	0	0	0
BOOTP-INVALID	0	0	0

```

/* Verify DHCPv4 relay profile details */
Router# show dhcp ipv4 profile name PoA1 relay

```

```

Profile: PoA1 relay
Helper Addresses:
  192.0.2.2, vrf default, giaddr 198.51.100.1
Remote-Id Format : [ascii | hex]
Remote-Id value : cisco
Information Option: Enabled
Information Option Allow Untrusted: Enabled
Information Option VPN: Enabled
Information Option VPN Mode: RFC
Information Option Policy: Replace

```

関連項目

- [IRB での DHCPv4 リレー \(250 ページ\)](#)

関連コマンド

- show dhcp vrf default ipv4 relay statistics
- show dhcp ipv4 profile name

オールアクティブ マルチホーミング対応 DHCPv4 リレー同期

オールアクティブ マルチホーミング対応 DHCPv4 リレー同期機能は、エンドユーザと DHCPv4 サーバ間で一時的なエンティティを有効にするもので、DHCPv4 バインディングを作成しません。この機能により、エンドユーザ間において接続ポイント (PoA) 全体にわたる DHCP コントロールプレーン パケットの均等な分散がサポートされます。単一ユーザ向けの DHCP 制御パケットはすべて同じ DHCPv4 リレー (PoA) 上に存在します。そのため、エンドユーザは介入や遅延を受けずに IP アドレス割り当てをリリースできます。

マルチプロトコル拡張 BGP セッションが MPLS-SR を介してエッジルータへの PE ルータ間で確立され、学習された MAC-IP 情報が BGP を介してエッジルータに送信されます。MP-BGP は、指定されたイーサネットセグメント識別子 (ESI) とイーサネットタグについて、学習した MAC-IP 情報をルートタイプ 2 を使用してアドバタイズします。エッジルータは、PE1 または PE2 から学習したルートを他の PE に再配布する機能、およびその逆の機能を備えています。このメカニズムにより、MAC IP ルートがエッジルータに配信されます。その結果、個々の PE が完全な MAC IP ルーティング情報を持ちます。

この機能により、双方向トラフィックの転送が保証されます。ハイ アベイラビリティの場合には、ノード (PoA#1 または PoA#2) の障害時、アクセスインターフェイスの障害時、またはコアリンクの障害時に、他の PoA がデータトラフィックを転送します。

IRB での DHCPv6 リレー IAPD

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) の IRB でのリレー Identity Association for Prefix Delegation (IAPD) 機能を使用すると、ユーザがリンク、サブネット、およびサイトアドレッシングの変更を管理できます。この機能により、顧客に自らのネットワーク内での使用を目的としてプレフィックスを割り当てるプロセスが自動化されます。プレフィックス委任は、DHCPv6 プレフィックス委任オプションを使用して、プロバイダーエッジ (PE) デバイスとカスタマーエッジ (CE) デバイスの間で行われます。委任されたプレフィックスが割り当てられたユーザは、プレフィックスをさらにサブネット化してネットワーク内のリンクに割り当てることができます。

DHCPv6 リレーエージェントは、エンドユーザ用の IAPD (::/64 または ::/48) 割り当てを要求するために、アクセスインターフェイスを介して着信したすべての要求パケットを外部 DHCPv6 サーバに向けて送信します。また、DHCPv6 リレーは、DHCPv6 サーバからの応答パケットを受信し、アクセスインターフェイスを介してエンドユーザにパケットを転送します。DHCPv6 リレーは、DHCPv6 PD バインディングと、割り当てられた IAPD の各ルートエントリを維持します。そのため、エンドユーザに対してステートフルとして機能します。DHCPv6 リレー

は、エンドユーザ向けの Internet Assigned Numbers Authority (IANA) アドレス割り当てをサポートしていません。DHCPv6 リレーは、IAPD アドレス割り当てのみをサポートしています。IAPD プレフィックスは、DHCPv6 サーバで設定されているプレフィックス プールに基づきます。

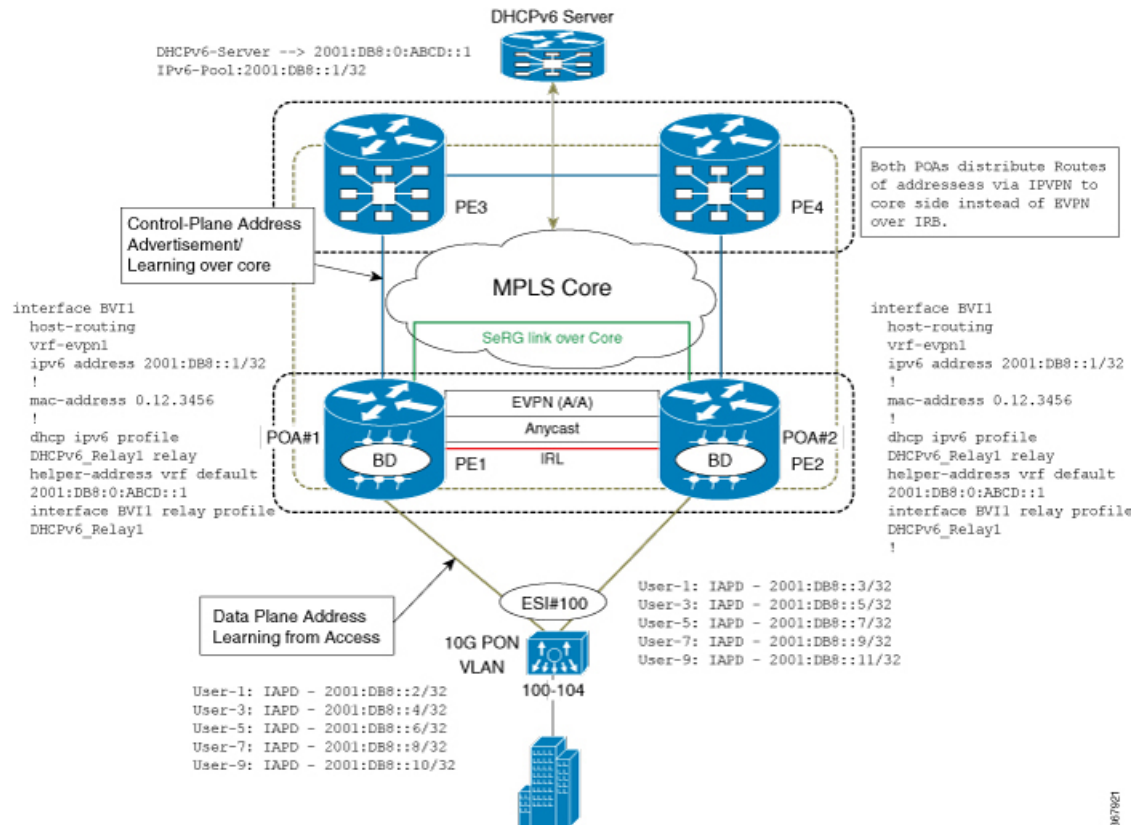
DHCPv6 リレーの場合、アクセス (BVI) インターフェイスはリレー プロファイルと関連付けられます。ToR は、クライアントから受信した DHCPv6 パケットを DHCPv6 サーバに送信するたびに、DHCPv6 サーバ IP アドレスの指定された定義済み VRF に対して最適な送信元 IP アドレスを検出します。ToR は、DHCPv6 サーバに到達するために、VRF ごとに一意の送信元 IP アドレスを維持しています。DHCPv6 リレーには、DHCPv6 ヘルパーアドレスの定義済み VRF のループバック インターフェイスで定義された一意の IPv4 送信元 IP アドレスがあり、MPLS コア ネットワークを介してルーティング可能です。

BVI インターフェイスで設定されたエニーキャスト IP アドレスは、エンドユーザのデフォルトゲートウェイとして機能し、同じサブネット上でアドレス割り当てが行われます。ToR は、MPLS コア ネットワークの IPVPN を介して DHCPv6 サーバに向けて DHCPv6 パケットをリレーするために、一意の送信元 IP アドレスを維持しています。同じ ToR は、外部 DHCPv6 サーバから応答パケットを受信します。DHCPv6 リレー配下における各 ToR の一意の送信元アドレスは、DHCPv6 プロセスにおいて、アクセス インターフェイスおよびリレー パケットを介して受信したパケットのコンテキストを維持するために必要です。このメカニズムは、BVI インターフェイスを介してエンドユーザに応答を送信するのに役に立ちます。

デフォルト VRF での EVPN および DHCPv6 サーバの DHCPv6 リレー処理

EVPN IRB および DHCPv6 サーバを介した DHCPv6 リレーは、同じデフォルト VRF に存在します。DHCPv6 リレー プロファイルは、デフォルト VRF 配下の DHCPv6 アドレスのヘルパーアドレスに関連付けられています。DHCPv4 とは異なり、PE では DHCPv6 リレー パケットにリレー情報オプションが追加されません。

図 37: デフォルト VRF での EVPN および DHCPv6 サーバの DHCPv6 リレー処理



367921

IRB での DHCPv6 リレー IAPD の設定

IRB での DHCPv6 リレー IAPD を設定するには、次の作業を実行します。

設定例

```
/* PE1 configuration */

Router# configure
Router(config)# interface BV11
Router(config-if)# host-routing
Router(config-if)# vrf-evpn1
Router(config-if)# ipv6 address 2001:DB8::1/32
Router(config-if)# exit
Router(config)# mac-address 0.12.3456
!
Router# configure
Router(config)# dhcp ipv6
Router(config-dhcpv6)# profile DHCPv6_Relay1 relay
Router(config-dhcpv6-relay-profile)# helper-address vrf default 2001: DB8:0:ABCD::1
Router(config-dhcpv6-relay-profile)# interface BV11 relay profile DHCPv6_Relay
Router(config-dhcpv6-relay-profile)# commit
```

```

/* PE2 configuration */

Router# configure
Router(config)# interface BVI1
Router(config-if)# host-routing
Router(config-if)# vrf-evpn1
Router(config-if)# ipv6 address 2001:DB8::1/32
Router(config-if)# exit
Router(config)# mac-address 0.12.3456
!
Router# configure
Router(config)# dhcp ipv6
Router(config-dhcpv6)# profile DHCPv6_Relay1 relay
Router(config-dhcpv6-relay-profile)# helper-address vrf default 2001: DB8:0:ABCD::1
Router(config-dhcpv6-relay-profile)# interface BVI1 relay profile DHCPv6_Relay
Router(config-dhcpv6-relay-profile)# commit

```

実行コンフィギュレーション

ここでは、IRB での DHCPv6 リレー IAPD の実行コンフィギュレーションを示します。

```

/* PE1 Configuration */
interface BVI1
  host-routing
  vrf-evpn1
  ipv6 address 2001:DB8::1/32
  !
  mac-address 0.12.3456
  !
  dhcp ipv6 profile DHCPv6_Relay1 relay
  helper-address vrf default 2001: DB8:0:ABCD::1
  interface BVI1 relay profile DHCPv6_Relay1
  !

/* PE2 Configuration *//interface BVI1
  host-routing
  vrf-evpn1
  ipv6 address 2001:DB8::1/32
  !
  mac-address 0.12.3456
  !
  dhcp ipv6 profile DHCPv6_Relay1 relay
  helper-address vrf default 2001: DB8:0:ABCD::1
  interface BVI1 relay profile DHCPv6_Relay1
  !

```

確認

IRB での DHCPv6 リレー IAPD の設定を確認します。

```

/* Verify DHCPv6 relay statistics
Router# show dhcp vrf default ipv6 relay statistics

```

DHCP IPv6 Relay Statistics for VRF default:

TYPE	RECEIVE	TRANSMIT	DROP
DISCOVER	2000	2000	0
OFFER	2000	2000	0
REQUEST	5500	5500	0

DECLINE	0	0	0
ACK	5500	5500	0
NAK	0	0	0
RELEASE	500	500	0
INFORM	0	0	0
LEASEQUERY	0	0	0
LEASEUNASSIGNED	0	0	0
LEASEUNKNOWN	0	0	0
LEASEACTIVE	0	0	0
BOOTP-REQUEST	0	0	0
BOOTP-REPLY	0	0	0
BOOTP-INVALID	0	0	0

関連項目

- [IRB での DHCPv6 リレー IAPD \(259 ページ\)](#)

関連コマンド

- `show dhcp ipv6 relay statistics vrf default`

セッション冗長性を使用したオールアクティブ マルチホーミング対応 DHCPv6 PD 同期

セッション冗長性を使用したオールアクティブ マルチホーミング対応 DHCPv6 PD 同期機能は、制御パケットとデータパケットの両方に対するロードバランシングを提供します。この機能は、スループット（ラインレート）と処理能力に関するデバイスの効率的な利用に役立ちます。

このリリースより前のリリースでは、セッション冗長性（SeRG）のメカニズムは、アクセス障害、コア障害、およびノード/シャーシ障害に対処するためのアクティブ-スタンバイをサポートしていました。これらすべての場合において、1つのアクティブ PoA が、セッションを作成し、PoA 全体にわたって SeRG を使用してバインディング情報を同期する役割を担います。このメカニズムでは、SeRG グループ内の対象のアクセスリンクについて PoA がマスター/スレーブモードであるために、EVPN オールアクティブ マルチホーミングの目的を果たすことができませんでした。この場合、制御パケットを処理し、バインディングを作成し、データパスを転送するためにマスターとして機能するノードが1つだけに制限されます。

SeRG グループ設定を使用したオールアクティブ マルチホーミング対応 DHCPv6 PD 同期を使用すると、マスター/スレーブモードとは異なり、両方の PoAA をアクティブにするように定義できます。また、それぞれの PoA のロールを交換またはネゴシエートする必要はありません。

SeRG では、どのルートタイプでも BGP を介して IAPD プレフィックスルートが配布されることはありません。ルーテッド BVI インターフェイスは DHCPv6 リレーを使用して設定され、エンドユーザーに PD 割り当てを提供します。

個々のマルチホーミング ピア SeRG ロールは ACTIVE のみです。SeRG は、NONE および ACTIVE 以外のロールをサポートしていません。インターフェイスリストを BVI インターフェイスとし

て SeRG 配下に定義し、通常は 1 つまたは複数の BVI インターフェイスを使用します。ただし、L2 トランスポート AC を SeRG インターフェイスリスト配下に定義することは推奨されません。これは、L2 トランスポート AC は L2VPN BD 配下で定義されており、SeRG クライアントの DHCPv6 はこれらの AC 情報を認識しないためです。

SeRG アクティブ-アクティブ モードでは、IPv6-ND 同期は PoA 間で抑制されます。

制約事項

- SeRG はコア リンク障害をサポートしていません。
- SeRG はコアおよびアクセス トラッキング メカニズムをサポートしていません。
- ACTIVE-ACTIVE モードの設定中はバインディングが存在しないことを確認してください。
- 必ずすべての PoA で同じ設定を使用してください。バンドル-イーサ L2 トランスポート AC 設定は、BD と BVI の設定とともに、両側で同じにする必要があります。
- **clear session-redundancy** コマンドは、システムの不整合を回避するために、どのモードでもサポートされていません。
- SeRG アクティブ-アクティブ モードでは、両方の PoA が常にコア リンクを介して到達可能であることを確認してください。コア リンクをアクセスリンクにマッピングする EVPN コア分離機能を設定することをお勧めします。このメカニズムにより、コアリンクがダウンした場合は常に、それぞれのアクセスリンクが削除されることが保証されます。

DHCPv6 PD 同期の設定

SeRG を使用した DHCPv6 PD 同期を設定するには、次の作業を実行します。

設定例

```
/* PoA1 configuration */
Router# configure
Router(config)# session redundancy
Router(config-session-red)# source-interface Loopback0
Router(config-session-red)# group 1
Router(config-session-red-group)# peer 192.0.2.1
Router(config-session-red-group)# mode active-active
Router(config-session-red-group)# interface-list
Router(config-session-red-group-intf)# interface BVI1 id 1
Router(config-session-red-group-intf)# commit

/* PoA2 configuration */
Router# configure
Router(config)# session redundancy
Router(config-session-red)# source-interface Loopback0
Router(config-session-red)# group 1
Router(config-session-red-group)# peer 198.51.100.1
Router(config-session-red-group)# mode active-active
Router(config-session-red-group)# interface-list
```

```
Router(config-session-red-group-intf)# interface BVI1 id 1
Router(config-session-red-group-intf)# commit
```

実行コンフィギュレーション

ここでは、DHCPv6 PD 同期の実行コンフィギュレーションを示します。

```
/* PoA1 Configuration */
session-redundancy
source-interface Loopback0
group 1
  peer 192.0.2.1
  mode active-active
  interface-list
  interface BVI1 id 1
  !
!
!
/* PoA2 Configuration */
session-redundancy
source-interface Loopback0
group 1
  peer 198.51.100.1
  mode active-active
  interface-list
  interface BVI1 id 1
  !
!
!
```

確認

DHCPv6 PD 同期の設定を確認します。

```
/* Verify the session redundancy group */
```

```
Router# show session-redundancy group
Wed Nov 28 16:00:36.559 UTC
Session Redundancy Agent Group Summary
Flags      : E - Enabled, D - Disabled, M - Preferred Master, S - Preferred Slave
            H - Hot Mode, W - Warm Mode, T - Object Tracking Enabled
P/S       : Peer Status
            I - Initialize, Y - Retry, X - Cleanup, T - Connecting
            L - Listening, R- Registered, C - Connected, E - Established
I/F-P Count: Interface or Pool Count
SS Count  : Session Count
```

Node Name	Group ID	Role	Flags	Peer Address	P/S	I/F-P
Count	SS Count	Sync Pending				
0/RP0/CPU0		1	Active	E-H-	120.1.1.1	E
1	1		0			
0/RP0/CPU0		2	Active	E-H-	120.1.1.1	E
1	0		0			
0/RP0/CPU0		3	Active	E-H-	120.1.1.1	E
1	0		0			
0/RP0/CPU0		4	Active	E-H-	120.1.1.1	E
1	0		0			
0/RP0/CPU0		5	Active	E-H-	120.1.1.1	E

```

1          0          0
-----
Session Summary Count(Master/Slave/Active/Total): 0/0/1/1

/* Verify IPv6 relay binding */

Router# show dhcp ipv6 relay binding
Summary:
Total number of clients: 1

IPv6 Prefix: 60:1:1:1::/64 (BVI1)
Client DUID: 000100015bfeb921001094000000
IAID: 0x0
VRF: default
Lifetime: 120 secs (00:02:00)
Expiration: 91 secs (00:01:31)
L2Intf AC: Bundle-Ether1.1
SERG State: SERG-ACTIVE
SERG Intf State: SERG-ACTIVE

```

関連項目

- [セッション冗長性を使用したオールアクティブ マルチホーミング対応 DHCPv6 PD 同期 \(263 ページ\)](#)

関連コマンド

- show session-redundancy group
- show dhcp ipv6 relay binding

DHCPv6 リレーにおける IAPD ルートの配布と取り消し

EVPN マルチホーミング アクティブ-アクティブのシナリオが存在する場合、DHCPv6 リレー エージェントは、接続回線 (AC) および BVI インターフェイスに関連付けられた L2VPN ブリッジ ドメインを介してサポートされ、Identity Association for Prefix Delegation (IAPD) ルートの割り当てが行われます。また、DHCPv6 リレー エージェントは、iBGP を使用して MPLS コア ネットワーク経由でルート配布を実行します。コアからサブスクリバへのトラフィックでは、少数の AC がダウンする可能性があります。すべての AC がダウンするわけではないため、BVI は引き続きアップ状態です。このシナリオでは、ダウンした AC 内のサブスクリバでトラフィック ブロック ホールが生じる可能性があります。トラフィック ブロック ホールが生じる理由は IAPD ルートに関するものです。IAPD ルートは、AC がダウンしても MPLS コア ネットワークについては引き続きアップ状態です。

トラフィック ブロック ホールを防止するため、DHCPv6 リレー エージェントをイネーブルにして、セッションの iBGP を介して MPLS コア ネットワークからの IAPD ルートの取り消しを実行します。ルートの取り消しは、L2VPN ブリッジ ドメインの AC がダウンすると必ず発生します。また、AC がアップ状態に戻るたびに、DHCPv6 リレー エージェントは iBGP を介して IAPD ルートを MPLS コア ネットワークに配布できます。



第 10 章

EVPN 仮想プライベートワイヤサービス (VPWS)

EVPN-VPWS は、ポイントツーポイント サービス用の BGP コントロールプレーン ソリューションです。これにより、PE のペア間で EVPN インスタンスを確立するためのシグナリング およびカプセル化技術が実装されます。EVPN-VPWS には、MAC ルックアップを使用せずに、あるネットワークから別のネットワークにトラフィックを転送する機能があります。VPWS 対応の EVPN により、ポイントツーポイント イーサネット サービスにおいてシングルセグメント およびマルチセグメント PW をシグナリングする必要がなくなります。EVPN-VPWS テクノロジーは、IP および MPLS コアで動作します。IP コアでは BGP がサポートされ、MPLS コアではエンドポイント間でのパケットのスイッチングがサポートされます。

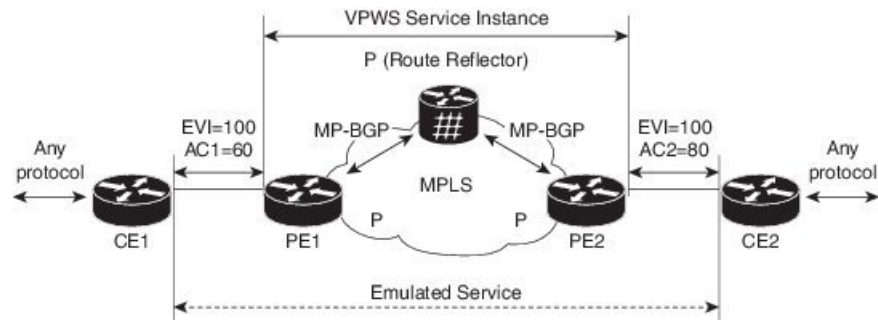
EVPN-VPWS は、シングルホーミングとマルチホーミングの両方をサポートしています。

- [EVPN-VPWS シングル ホーム \(267 ページ\)](#)
- [EVPN-VPWS マルチホーム \(269 ページ\)](#)

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 機能アドバイズメントを使用して、2つのスピーカーが RFC 4760 に従い、EVPN NLRI (AFI 25、SAFI 70) を確実にサポートするようにします。

EVPN VPWS のアーキテクチャでは、PE3 がコントロールプレーンでマルチプロトコル BGP を実行します。次に、EVPN-VPWS 設定を説明する図を示します。



- PE1 上の VPWS サービスには、設定時に指定する次の 3 つの要素が必要です。
 - VPN ID (EVI)
 - ローカル AC 識別子 (AC1)。エミュレートされたサービスのローカルエンドを識別します。
 - リモート AC 識別子 (AC2)。エミュレートされたサービスのリモートエンドを識別します。

PE1 は到達可能性を得るために、MPLS ラベルをローカル AC ごとに割り当てます。

- PE2 上の VPWS サービスは PE1 と同じ方法で設定されます。3 つの同じ要素が必要であり、サービス設定は対称になっている必要があります。

PE2 は到達可能性を得るために、MPLS ラベルをローカル AC ごとに割り当てます。

- PE1 は各ローカルエンドポイント (AC) の EVI イーサネット AD ごとの単一の EVPN を、関連付けられた MPLS ラベルを使用してリモート PE にアドバタイズします。

PE2 は同じタスクを実行します。

- PE2 から EVI EAD ルートごとの EVPN を受け取ると、PE1 はそのローカル L2 RIB にエントリを追加します。PE1 は AC2 に到達するパスのリスト (たとえば、ネクストホップが PE2 の IP アドレスであること) と AC2 の MPLS ラベルを把握しています。

PE2 は同じタスクを実行します。

EVPN-VPWS シングル ホームの設定

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 12vpn 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)# 12vpn
Router(config-12vpn)# xconnect group evpn-vpws
Router(config-12vpn-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
!

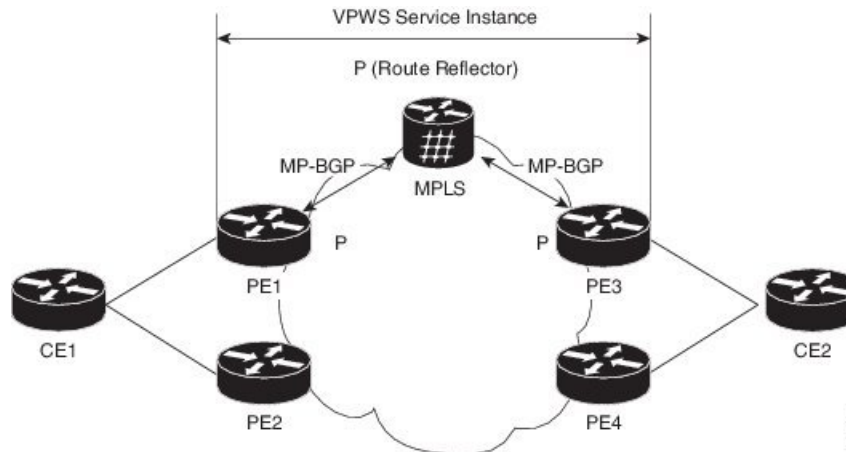
```

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 38: 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 11 章

トラフィック エンジニアリング ポリシー のセグメントルーティングを介した L2VPN サービス

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。送信元デバイスがパスを選択し、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を表す識別子です。

トラフィック エンジニアリング用のセグメントルーティング (SR-TE) は、送信元と宛先のペア間のトンネルを通じて行われます。SR-TE では、送信元ルーティングの概念が使用されません。送信元はパスを計算し、パケットヘッダーでセグメントとしてエンコードします。SR-TE 優先パスでは、各セグメントは、送信元から宛先までのエンドツーエンドのパスであり、プロバイダー コア ネットワークのルータに、IGP によって計算された最短パスではなく指定されたパスに従うように指示します。宛先はトンネルの存在を認識しません。

MPLS LDP の代わりにセグメントルーティングを使用して MPLS L2VPN サービスを転送することで、ネットワークトラフィックのレジリエンスとコンバージェンスが向上します。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、MPLS アーキテクチャに直接適用できます。MPLS データプレーンを使用するセグメントルーティングネットワークでは、LDP またはその他のシグナリングプロトコルは不要です。その代わりに、IGP によってラベル配布が実行されます。ネットワークからプロトコルを排除することでその操作が簡略化し、プロトコルとの対話式操作の必要をなくすことで堅牢性と安定性が向上します。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よくネットワーク帯域幅を利用し、遅延を低減します。

優先トンネルパスの機能により、特定のトラフィックエンジニアリング トンネルパスに疑似回線をマッピングできます。接続回線は、リモート PE ルータの IP アドレス (IGP または LDP を使用して到達可能) ではなく、特定の SR トラフィックエンジニアリング トンネルインターフェイスに相互接続されます。トラフィック エンジニアリング トンネルは、優先トンネルパスを使用して、送信元と宛先の PE ルータ間でトラフィックを転送します。パスが有効で、その設定が SR ポリシーにおけるすべての候補パスの中で最適 (最高値) である場合に、そのパスが SR ポリシーに対して選択されます。

次の L2VPN サービスが SR-TE ポリシーを介してサポートされています。

- 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 L2VPN VPLS または VPWS 優先パス
- SR-TE を使用した EVPN VPWS オンデマンドネクストホップ
- [SR-TE ポリシーを介した EVPN VPWS 優先パス \(274 ページ\)](#)
- [SR-TE ポリシーを介した L2VPN VPLS または VPWS 優先パス \(287 ページ\)](#)
- [SR-TE を使用した EVPN VPWS オンデマンドネクストホップ \(303 ページ\)](#)
- [セグメントルーティングの概要 \(318 ページ\)](#)
- [セグメントルーティングの仕組み \(319 ページ\)](#)
- [セグメントルーティング グローバルブロック \(320 ページ\)](#)

SR-TE ポリシーを介した EVPN VPWS 優先パス

SR-TE ポリシーを介した EVPN VPWS 優先パス機能では、SR-TE ポリシーを使用して、EVPN VPWS 疑似回線 (PW) の2つのエンドポイント間に優先パスを設定できます。SR ポリシーでは、EVPN インスタンス (EVI) ごとにパスを選択できます。この機能はバンドル接続回線 (AC) と物理 AC でサポートされています。

制約事項

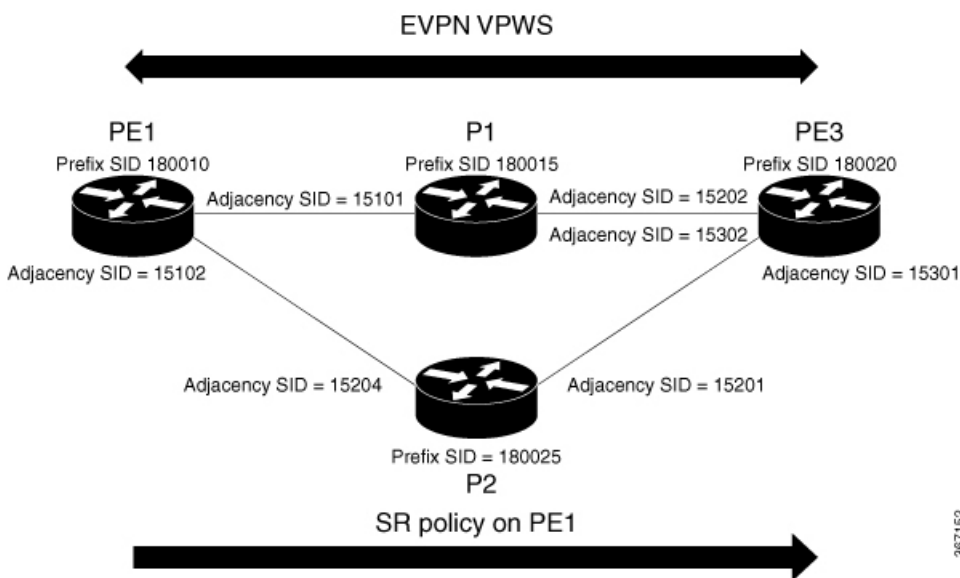
- オンデマンドネクストホップ (ODN) を備えた EVPN VPWS を設定し、優先パスがある EVPN VPWS も同じ PW に設定すると、優先パスが優先されます。
- EVPN VPWS SR ポリシーは EVPN VPWS デュアルホーミングではサポートされていません。
- EVPN はルートがシングルホームネクストホップ用であるかどうかを検証します。そうでない場合は、不適切な SR-TE ポリシーに関するエラーメッセージを発行し、そのポリシーなしで EVPN-VPWS のセットアップを続行します。EVPN は、これがシングルホームかどうかの決定をゼロに設定されている ESI 値に依存します。AC が LACP を実行しているバンドルイーサインターフェイスの場合は、ESI 値を手動でゼロに設定して、自動感知 ESI を上書きする必要があります。これは、EVPN VPWS マルチホーミングがサポートされていないためです。

EVPN デュアルホーミングを無効にするには、バンドルイーサ AC を ESI 値セットをゼロに設定します。

```
evpn
interface Bundle-Ether12
  ethernet-segment
    identifier type 0 00.00.00.00.00.00.00.00
/* Or globally */
Evpn
  ethernet-segment type 1 auto-generation-disable
```


トポロジ

図 39: 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

SR-TE ポリシー機能を介して EVPN VPWS 優先パスを確実に設定するには、次のタスクを実行する必要があります。

- IGP でのプレフィックス SID の設定：次の例は、IS-IS でプレフィックス SID を設定する方法を示しています。
- IGP での隣接関係 SID の設定：次の例は、IS-IS で隣接関係 SID を設定する方法を示しています。
- セグメントリストの設定
- SR-TE ポリシーの設定
- SR-TE ポリシーを介した EVPN VPWS の設定

ISIS でのプレフィックス SID の設定

PE1、P1、P2、および PE3 にプレフィックス SID を設定します。

```

/* Configure Prefix-SID on PE1 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# global-block 180000 200000
Router(config-sr)# exit
!
Router# configure
Route(config)# router isis core
Route(config-isis)# is-type level-2-only
Route(config-isis)# net 49.0002.0330.2000.0031.00
Route(config-isis)# nsr
Route(config-isis)# nsf ietf
Route(config-isis)# log adjacency changes
Route(config-isis)# address-family ipv4 unicast
Route(config-isis-af)# metric-style wide level 2
Route(config-isis-af)# mpls traffic-eng level-2-only
Route(config-isis-af)# mpls traffic-eng router-id 1.1.1.1
Route(config-isis-af)# segment-routing mpls sr-prefer
Route(config-isis-af)# segment-routing prefix-sid-map advertise-local
Route(config-isis-af)# exit
!
Route(config-isis)# interface loopback 0
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# prefix-sid index 180010
Route(config-isis-af)# commit
Route(config-isis-af)# exit

/* Configure Prefix-SID on P1 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# global-block 180000 200000
Router(config-sr)# exit
!
Router# configure
Router(config)# router isis core
Router(config-isis)# is-type level-2-only
Router(config-isis)# net 49.0002.0330.2000.0021.00
Router(config-isis)# nsr
Router(config-isis)# nsf ietf
Router(config-isis)# log adjacency changes
Router(config-isis)# address-family ipv4 unicast
Router(config-isis-af)# metric-style wide level 2
Router(config-isis-af)# mpls traffic-eng level-2-only
Router(config-isis-af)# mpls traffic-eng router-id loopback0
Router(config-isis-af)# segment-routing mpls sr-prefer
Router(config-isis-af)# segment-routing prefix-sid-map advertise-local
Router(config-isis-af)# exit
!
Router(config-isis)# interface loopback 0
Router(config-isis-if)# address-family ipv4 unicast
Router(config-isis-af)# prefix-sid index 180015
Router(config-isis-af)# commit
Router(config-isis-af)# exit

/* Configure Prefix-SID on P2 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# global-block 180000 200000
Router(config-sr)# exit

```

```

!
Router# configure
Route(config)# router isis core
Route(config-isis)# is-type level-2-only
Route(config-isis)# net 49.0002.0330.2000.0022.00
Route(config-isis)# nsr
Route(config-isis)# nsf ietf
Route(config-isis)# log adjacency changes
Route(config-isis)# address-family ipv4 unicast
Route(config-isis-af)# metric-style wide level 2
Route(config-isis-af)# mpls traffic-eng level-2-only
Route(config-isis-af)# mpls traffic-eng router-id loopback0
Route(config-isis-af)# segment-routing mpls sr-prefer
Route(config-isis-af)# segment-routing prefix-sid-map advertise-local
Route(config-isis-af)# exit
!
Route(config-isis)# interface loopback 0
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# prefix-sid index 180025
Route(config-isis-af)# commit
Route(config-isis-af)# exit

/* Configure Prefix-SID on PE3 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# global-block 180000 200000
Router(config-sr)# exit
!
Router# configure
Route(config)# router isis core
Route(config-isis)# is-type level-2-only
Route(config-isis)# net 49.0002.0330.2000.3030.0030.0035.00
Route(config-isis)# address-family ipv4 unicast
Route(config-isis-af)# metric-style wide level 2
Route(config-isis-af)# mpls traffic-eng level-2-only
Route(config-isis-af)# mpls traffic-eng router-id loopback0
Route(config-isis-af)# segment-routing mpls sr-prefer
Route(config-isis-af)# segment-routing prefix-sid-map advertise-local
Route(config-isis-af)# exit
!
Route(config-isis)# interface loopback0
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# prefix-sid index 180020
Route(config-isis-af)# commit
Route(config-isis-af)# exit

```

ISIS での隣接関係 SID の設定

PE1、P1、P2、および PE3 に隣接関係 SID を設定します。

```

/* Configure Adjacency-SID on PE1 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# local-block 15000 15999
!
Router# configure
Route(config)# router isis core
Route(config-isis)# interface Bundle-Ether121

```

```

Route(config-isis-if) # circuit-type level-2-only
Route(config-isis-if) # point-to-point
Route(config-isis-if) # hello-padding disable
Route(config-isis-if) # address-family ipv4 unicast
Route(config-isis-if-af) # adjacency-sid absolute 15101
Route(config-isis-if-af) # exit
!
Router# configure
Route(config) # router isis core
Route(config-isis) # interface TenGigE0/0/1/6
Route(config-isis-if) # circuit-type level-2-only
Route(config-isis-if) # point-to-point
Route(config-isis-if) # hello-padding disable
Route(config-isis-if) # address-family ipv4 unicast
Route(config-isis-if-af) # adjacency-sid absolute 15102
Route(config-isis-if-af) # commit

/* Configure Adjacency-SID on P1 */

Router# configure
Router(config) # segment-routing
Router(config-sr) # local-block 15000 15999
!
Router# configure
Route(config) # router isis core
Route(config-isis) # interface Bundle-Ether121
Route(config-isis-if) # circuit-type level-2-only
Route(config-isis-if) # point-to-point
Route(config-isis-if) # hello-padding disable
Route(config-isis-if) # address-family ipv4 unicast
Route(config-isis-if-af) # metric 20
Route(config-isis-if-af) # adjacency-sid absolute 15200
Route(config-isis-if-af) # commit
!
Router# configure
Route(config) # router isis core
Route(config-isis) # interface TenGigE0/0/0/7
Route(config-isis-if) # circuit-type level-2-only
Route(config-isis-if) # point-to-point
Route(config-isis-if) # hello-padding disable
Route(config-isis-if) # address-family ipv4 unicast
Route(config-isis-if-af) # adjacency-sid absolute 15202
Route(config-isis-if-af) # commit
!
/* Configure Adjacency-SID on P2 */

Router# configure
Router(config) # segment-routing
Router(config-sr) # local-block 15000 15999
!
Router# configure
Route(config) # router isis core
Route(config-isis) # interface TenGigE0/0/0/7
Route(config-isis-if) # circuit-type level-2-only
Route(config-isis-if) # point-to-point
Route(config-isis-if) # hello-padding disable
Route(config-isis-if) # address-family ipv4 unicast
Route(config-isis-if-af) # metric 20
Route(config-isis-if-af) # adjacency-sid absolute 15201
Route(config-isis-if-af) # exit
!
Router# configure
Route(config) # router isis core

```

```

Route(config-isis)# interface TenGigE0/0/0/5
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# metric 20
Route(config-isis-if-af)# adjacency-sid absolute 15204
Route(config-isis-if-af)# commit

/* Configure Adjacency-SID on PE3 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# local-block 15000 15999
!
Router# configure
Route(config)# router isis core
Route(config-isis)# interface TenGigE0/0/0/1
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# adjacency-sid absolute 15301
Route(config-isis-if-af)# exit
!
Router# configure
Route(config)# router isis core
Route(config-isis)# interface TenGigE0/0/0/2
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# adjacency-sid absolute 15302
Route(config-isis-if-af)# commit

```

セグメントリストの設定

```

/* Configure Segment-list on PE1 using prefix-SID */

Router# configure
Router(config)# segment-routing
Router(config-sr)# global-block 180000 200000
Router(config-sr)# traffic-eng
Router(config-sr-te)# logging
Router(config-sr-te-log)# policy status
Router(config-sr-te-log)# exit
!
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# segment-list name pref_sid_to_PE3
Router(config-sr-te-sl)# index 1 mpls label 180020 <-----using prefix-SID
Router(config-sr-te-sl)# exit

/* Configure Segment-list on PE1 using adjacency-SID */

Router# configure
Router(config)# segment-routing
Router(config-sr)# local-block 15000 15999
Router(config-sr)# traffic-eng
Router(config-sr-te)# logging

```

```

Router(config-sr-te-log)# policy status
Router(config-sr-te-log)# exit
!
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# segment-list name pref_adj_sid_to_PE3
Router(config-sr-te-sl)# index 1 mpls label 15101 <-----using
adjacency-SID
Router(config-sr-te-sl)# index 2 mpls label 15202 <-----using
adjacency-SID
Router(config-sr-te-sl)# exit

```

SR-TE ポリシーの設定

```

/* Configure SR-TE Policy */

Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy pref_sid_to_PE3
Router(config-sr-te-policy)# color 9001 end-point ipv4 20.20.20.20
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy)# preference 10
Router(config-sr-te-pp-info)# explicit segment-list pref_sid_to_PE3
Router(config-sr-te-pp-info)# commit
Router(config-sr-te-pp-info)# exit
!
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy pref_adj_sid_to_PE3
Router(config-sr-te-policy)# color 9001 end-point ipv4 20.20.20.20
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy)# preference 200
Router(config-sr-te-pp-info)# explicit segment-list pref_adj_sid_to_PE3
Router(config-sr-te-pp-info)# commit
Router(config-sr-te-pp-info)# exit

/* You can configure multiple preferences for an SR policy. Among the configured
preferences, the largest number takes the highest precedence */

Router# configure
Router(config)# segment-routing
Router(config-sr)# global-block 180000 200000
Router(config-sr)# local-block 15000 15999
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy 1013
Router(config-sr-te-policy)# color 1013 end-point ipv4 2.2.2.2
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy)# preference 100
Router(config-sr-te-pp-info)# explicit segment-list PE1-P1_BE121
Router(config-sr-te-pp-info)# exit
!
Router(config-sr-te-policy)# preference 200
Router(config-sr-te-pp-info)# explicit segment-list PE1-PE3-P1-t0016
Router(config-sr-te-pp-info)# exit
!
Router(config-sr-te-policy)# preference 700 <-----largest number takes the 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



- (注) 自動生成された SR-TE ポリシー名を使用して、L2VPN インスタンスにポリシーをアタッチします。ポリシー名は、ポリシーの色とエンドポイントに基づいて自動生成されます。自動生成されたポリシー名を表示するには、**show segment-routing traffic-eng policy candidate-path name *policy_name*** コマンドを使用します。

```
Router# show segment-routing traffic-eng policy candidate-path name pref_sid_to_PE3

SR-TE policy database
-----
Color: 9001, End-point: 20.20.20.20
Name: srte_c_9001_ep_20.20.20.20

Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# pw-class 1001
Router(config-l2vpn-pwc)# encapsulation mpls
Router(config-l2vpn-pwc-mpls)# preferred-path sr-te policy srte_c_9001_ep_20.20.20.20
fallback disable
Router(config-l2vpn-pwc-mpls)# commit
Router(config-l2vpn-pwc-mpls)# exit
!
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group evpn_vpws
Router(config-l2vpn-xc)# p2p evpn_vpws_1001
Router(config-l2vpn-xc-p2p)# interface tengi0/1/0/1.1001
Router(config-l2vpn-xc-p2p)# neighbor evpn evi 1001 target 10001 source 20001
Router(config-l2vpn-xc-p2p-pw)# pw-class 1001
Router(config-l2vpn-xc-p2p-pw)# commit
Router(config-l2vpn-xc-p2p-pw)# exit

/* If Fallback Enable is configured, which is the default option, and if the SR-policy
is down, then EVPN VPWS will still continue to be UP using the regular IGP path, and not
using the SR-policy */
show l2vpn xconnect detail
EVPN: neighbor 20.20.20.20, PW ID: evi 1001, ac-id 10001, state is up ( established )
Preferred path Inactive : SR TE srte_c_9001_ep_20.20.20.20, Statically configured,
fallback enabled
Tunnel : Down
LSP: Up

/* If Fallback Disable is configured, and if the SR-policy is down, or if it misconfigured
in dual homed mode, then the L2VPN PW will be down */
show l2vpn xconnect detail
EVPN: neighbor 20.20.20.20, PW ID: evi 1001, ac-id 10001, state is down ( local ready )
Preferred path Active : SR TE srte_c_9001_ep_20.20.20.20, Statically configured, fallback
disabled
Tunnel : Down
```

実行コンフィギュレーション

```
/* Configure Prefix-SID in ISIS */
PE1:

configure
  segment-routing
    global-block 180000 200000
!
router isis core
  is-type level-2-only
  net 49.0002.0330.2000.0031.00
  nsr
  nsf ietf
  log adjacency changes
  address-family ipv4 unicast
  metric-style wide level 2
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id 1.1.1.1
  segment-routing mpls sr-prefer
  segment-routing prefix-sid-map advertise-local

interface Loopback0
  address-family ipv4 unicast
  prefix-sid index 180010

P1:

configure
  segment-routing
    global-block 180000 200000

router isis core
  is-type level-2-only
  net 49.0002.0330.2000.0021.00
  nsr
  nsf ietf
  log adjacency changes
  address-family ipv4 unicast
  metric-style wide level 2
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
  segment-routing mpls sr-prefer
  segment-routing prefix-sid-map advertise-local

interface Loopback0
  address-family ipv4 unicast
  prefix-sid index 180015

P2:

configure
  segment-routing
    global-block 180000 200000

router isis core
  is-type level-2-only
  net 49.0002.0330.2000.0022.00
  nsr
  nsf ietf
  log adjacency changes
  address-family ipv4 unicast
```



```
metric-style wide level 2
mpls traffic-eng level-2-only
mpls traffic-eng router-id Loopback0
segment-routing mpls sr-prefer
segment-routing prefix-sid-map advertise-local

interface Loopback0
 address-family ipv4 unicast
  prefix-sid index 180025
```

PE3:

```
configure
 segment-routing
  global-block 180000 200000

router isis core
 is-type level-2-only
 net 49.0002.0330.2000.3030.0030.0035.00
 address-family ipv4 unicast
  metric-style wide level 2
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
  segment-routing mpls sr-prefer
  segment-routing prefix-sid-map advertise-local

interface Loopback0
 address-family ipv4 unicast
  prefix-sid index 180020

/* Configure Adjacency-SID in ISIS */
```

PE1:

```
configure
 segment-routing
  local-block 15000 15999
!

router isis core
!
interface Bundle-Ether121
 circuit-type level-2-only
 point-to-point
 hello-padding disable
 address-family ipv4 unicast
  adjacency-sid absolute 15101

interface TenGigE0/0/1/6
 circuit-type level-2-only
 point-to-point
 hello-padding disable
 address-family ipv4 unicast
  adjacency-sid absolute 15102
```

P1:

```
configure
 segment-routing
  local-block 15000 15999

router isis core
!
interface Bundle-Ether121
```

```
circuit-type level-2-only
point-to-point
hello-padding disable
address-family ipv4 unicast
metric 20
adjacency-sid absolute 15200

interface TenGigE0/0/0/7
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 TenGigE0/0/0/7
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
!
```

SR-TE ポリシーを介した EVPN VPWS 優先パスの確認

```

    preference 700
    explicit segment-list PE1-P1
    !

/* Configure EVPN VPWS over SR-TE policy */
PE1:
configure
l2vpn
pw-class 1001
encapsulation mpls
preferred-path sr-te policy srte_c_9001_ep_20.20.20.20 fallback disable
xconnect group evpn_vpws
p2p evpn_vpws_1001
interface tengi0/1/0/1.1001
neighbor evpn evi 1001 target 10001 source 20001
pw-class 1001
!

```

SR-TE ポリシーを介した EVPN VPWS 優先パスの確認

```

PE1#show segment-routing traffic-eng forwarding policy name pref_sid_to_PE3 detail
Policy          Segment          Outgoing          Outgoing          Next Hop          Bytes
Name            List             Label             Interface          Switched
-----
pref_sid_to_PE3
                                15102             TenGigE0/0/1/6    20.20.20.20       81950960
                                Label Stack (Top -> Bottom): { 15101, 15102 }
                                Path-id: 1, Weight: 0
                                Packets Switched: 787990
Local label: 34555
Packets/Bytes Switched: 1016545/105720680
(!): FRR pure backup

```

```

PE1#show segment-routing traffic-eng policy candidate-path name pref_sid_to_PE3

SR-TE policy database
-----

Color: 9001, End-point: 20.20.20.20
Name: srte_c_9001_ep_20.20.20.20

```

```

PE1#show mpls forwarding tunnels sr-policy name pref_sid_to_PE3
Tunnel          Outgoing          Outgoing          Next Hop          Bytes
Name            Label             Interface          Switched
-----
pref_sid_to_PE3 (SR) 15102 TenGigE0/0/1/6 20.20.20.20       836516512

```

```

PE1#show l2vpn xconnect group evpn_vpws xc-name evpn_vpws_1001 detail
Group evpn_vpws, XC evpn_vpws_1001, state is up; Interworking none
AC: Bundle-Ether12.1001, state is up
Type VLAN; Num Ranges: 1
Outer Tag: 1000
Rewrite Tags: []
VLAN ranges: [1, 1]
MTU 1500; XC ID 0xc0000018; interworking none
Statistics:
  packets: received 642304, sent 642244
  bytes: received 61661184, sent 61655424

```

```
drops: illegal VLAN 0, illegal length 0
EVPN: neighbor 20.20.20.20, PW ID: evi 1001, ac-id 10001, state is up ( established )
XC ID 0xa0000007
Encapsulation MPLS
Source address 10.10.10.10
Encap type Ethernet, control word enabled
Sequencing not set
Preferred path Active : SR TE pref_sid_to_PE3, Statically configured, fallback
disabled
Tunnel : Up
Load Balance Hashing: src-dst-mac
```

関連コマンド

- [adjacency-sid](#)
- [index](#)
- [prefix-sid](#)
- [router isis](#)
- [segment-routing](#)

該当するセグメントルーティング コマンドについては、『*Segment Routing Command Reference for Cisco NCS 5500 Series Routers and Cisco NCS 540 Series Routers*』を参照してください。

関連項目

- [セグメントルーティングの概要 \(318 ページ\)](#)
- [セグメントルーティングの仕組み \(319 ページ\)](#)
- [セグメントルーティング グローバルブロック \(320 ページ\)](#)

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。

制約事項

- SR ポリシーが VPLS 回線の優先パスとして設定されている場合、トラフィックは SR ポリシー パスを通過します。
- PW カウンタは、送受信されたパケットに関する統計情報を使用して更新されます。

SR ポリシーの設定が削除されても、トラフィックの送信が PE 間の通常の LSP パスに戻るため、トラフィックセッションは引き続き機能します。送信されたエンドツーエンドのトラフィックにはドロップはありません。

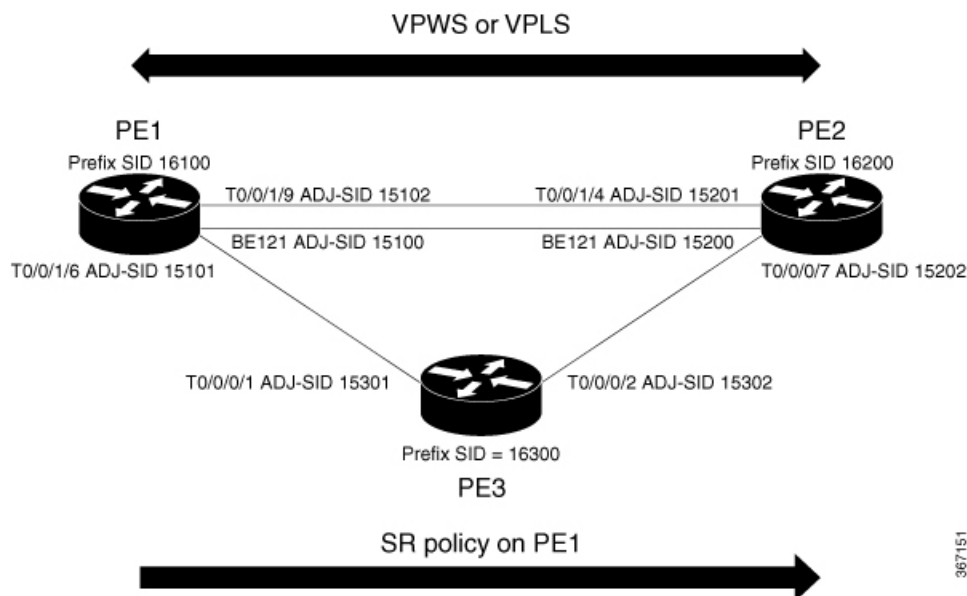
ただし、パケット統計カウンタはリセットされ、ゼロから始まります。

これは、SR ポリシーが削除されると PW も削除され、古い PW に関連付けられている統計情報がクリアされるためです。切り替え後に新しい PW が作成されると、再びカウンタがゼロから始まります。

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

SR-TE ポリシー機能を介して L2VPN VPLS または VPWS 優先パスを設定するには、次のステップを実行します。設定ステップを説明するため、次の図を参考として使用します。

図 40: SR-TE ポリシーを介した L2VPN VPWS および VPLS 優先パス



- IGP でのプレフィックス SID の設定：次の例は、IS-IS でプレフィックス SID を設定する方法を示しています。
- IGP での隣接関係 SID の設定：次の例は、IS-IS で隣接関係 SID を設定する方法を示しています。
- セグメントリストの設定
- SR-TE ポリシーの設定
- SR-TE ポリシーを介した VPLS の設定



(注) デバイスには最大 128K の MAC アドレス エントリを含めることができます。デバイス上のブリッジドメインには最大 64K の MAC アドレス エントリを含めることができます。

- SR-TE ポリシーを介した VPWS の設定

IS-IS でのプレフィックス SID の設定

PE1、PE2、および PE3 にプレフィックス SID を設定します。

```
/* Configure Prefix-SID on PE1 */

Router# configure
Route(config)# router isis core
Route(config-isis)# is-type level-2-only
Route(config-isis)# net 49.0002.0330.2000.0031.00
Route(config-isis)# nsr
Route(config-isis)# nsf ietf
Route(config-isis)# log adjacency changes
Route(config-isis)# address-family ipv4 unicast
Route(config-isis-af)# metric-style wide level 2
Route(config-isis-af)# mpls traffic-eng level-2-only
Route(config-isis-af)# mpls traffic-eng router-id 1.1.1.1
Route(config-isis-af)# segment-routing mpls sr-prefer
Route(config-isis-af)# segment-routing prefix-sid-map advertise-local
Route(config-isis-af)# exit
!
Route(config-isis)# interface loopback 0
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# prefix-sid index 16100
Route(config-isis-af)# commit
Route(config-isis-af)# exit

/* Configure Prefix-SID on PE2 */

Router# configure
Route(config)# router isis core
Route(config-isis)# is-type level-2-only
Route(config-isis)# net 49.0002.0330.2000.0021.00
Route(config-isis)# nsr
Route(config-isis)# nsf ietf
Route(config-isis)# log adjacency changes
Route(config-isis)# address-family ipv4 unicast
Route(config-isis-af)# metric-style wide level 2
Route(config-isis-af)# mpls traffic-eng level-2-only
Route(config-isis-af)# mpls traffic-eng router-id loopback0
Route(config-isis-af)# segment-routing mpls sr-prefer
Route(config-isis-af)# segment-routing prefix-sid-map advertise-local
Route(config-isis-af)# exit
!
Route(config-isis)# interface loopback 0
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# prefix-sid index 16200
Route(config-isis-af)# commit
Route(config-isis-af)# exit
```

```

/* Configure Prefix-SID on PE3 */

Router# configure
Route(config)# router isis core
Route(config-isis)# is-type level-2-only
Route(config-isis)# net 49.0002.0330.2000.3030.0030.0035.00
Route(config-isis)# address-family ipv4 unicast
Route(config-isis-af)# metric-style wide level 2
Route(config-isis-af)# mpls traffic-eng level-2-only
Route(config-isis-af)# mpls traffic-eng router-id loopback0
Route(config-isis-af)# segment-routing mpls sr-prefer
Route(config-isis-af)# segment-routing prefix-sid-map advertise-local
Route(config-isis-af)# exit
!
Route(config-isis)# interface loopback 0
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# prefix-sid index 16300
Route(config-isis-af)# commit
Route(config-isis-af)# exit

```

IS-IS での隣接関係 SID の設定

PE1、PE2、および PE3 に隣接関係 SID を設定します。

```

/* Configure Adjacency-SID on PE1 */

Router# configure
Route(config)# router isis core
Route(config-isis)# interface Bundle-Ether121
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# adjacency-sid absolute 15100
Route(config-isis-if-af)# exit
!
Router# configure
Route(config)# router isis core
Route(config-isis)# interface 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 15101
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 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 TenGigE0/0/0/3
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# adjacency-sid absolute 15201
Route(config-isis-if-af)# exit
!
Router# configure
Route(config)# router isis core
Route(config-isis)# interface TenGigE0/0/0/7
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# adjacency-sid absolute 15202
Route(config-isis-if-af)# commit

/* Configure Adjacency-SID on PE3 */

Router# configure
Route(config)# router isis core
Route(config-isis)# interface TenGigE0/0/0/1
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# adjacency-sid absolute 15301
Route(config-isis-if-af)# exit
!
Router# configure
Route(config)# router isis core
Route(config-isis)# interface TenGigE0/0/0/2
Route(config-isis-if)# circuit-type level-2-only
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-if-af)# adjacency-sid absolute 15302
Route(config-isis-if-af)# commit

```

セグメントリストの設定

PE1、PE2、および PE3 にセグメントリストを設定します。

```

/* Configure segment-list on PE1 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# global-block 16000 23999
Router(config-sr)# local-block 15000 15999

```

```

Router(config-sr)# traffic-eng
Router(config-sr-te)# segment-list segment-list name PE1-PE2
Router(config-sr-te-sl)# index 1 mpls label 16200
Router(config-sr-te-sl)# exit
!
Router(config-sr-te)# segment-list segment-list name PE1-PE3
Router(config-sr-te-sl)# index 1 mpls label 16300
Router(config-sr-te-sl)# exit
!
Router(config-sr-te)# segment-list segment-list name PE1-PE2-PE3
Router(config-sr-te-sl)# index 1 mpls label 16200
Router(config-sr-te-sl)# index 2 mpls label 16300
Router(config-sr-te-sl)# exit
!
Router(config-sr-te)# segment-list segment-list name PE1-PE2_bad
Router(config-sr-te-sl)# index 1 mpls label 16900
Router(config-sr-te-sl)# exit
!
Router(config-sr-te)# segment-list segment-list name PE1-PE3-PE2
Router(config-sr-te-sl)# index 1 mpls label 16300
Router(config-sr-te-sl)# index 2 mpls label 16200
Router(config-sr-te-sl)# exit
!
Router(config-sr-te)# segment-list segment-list name PE1-PE2_BE121
Router(config-sr-te-sl)# index 1 mpls label 15100
Router(config-sr-te-sl)# exit
!
Router(config-sr-te)# segment-list segment-list name PE1-PE3-PE2_link
Router(config-sr-te-sl)# index 1 mpls label 15101
Router(config-sr-te-sl)# index 2 mpls label 15302
Router(config-sr-te-sl)# exit
!
Router(config-sr-te)# segment-list segment-list name PE1-PE3-PE2-t0016
Router(config-sr-te-sl)# index 1 mpls label 15101
Router(config-sr-te-sl)# index 2 mpls label 16200
Router(config-sr-te-sl)# commit

/* Configure segment-list on PE2 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# global-block 16000 23999
Router(config-sr)# local-block 15000 15999
Router(config-sr)# traffic-eng
Router(config-sr-te)# segment-list segment-list name PE2-PE1
Router(config-sr-te-sl)# index 1 mpls label 16100
Router(config-sr-te-sl)# exit
!
Router(config-sr-te)# segment-list segment-list name PE2-PE3-PE1
Router(config-sr-te-sl)# index 1 mpls label 16300
Router(config-sr-te-sl)# index 2 mpls label 16100
Router(config-sr-te-sl)# commit

/* Configure segment-list on PE3 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# global-block 16000 23999
Router(config-sr)# local-block 15000 15999
Router(config-sr)# traffic-eng
Router(config-sr-te)# segment-list segment-list name PE3-PE1
Router(config-sr-te-sl)# index 1 mpls label 16100
Router(config-sr-te-sl)# exit

```

```

!
Router(config-sr-te)# segment-list segment-list name PE3-PE2-PE1
Router(config-sr-te-sl)# index 1 mpls label 16200
Router(config-sr-te-sl)# index 2 mpls label 16100
Router(config-sr-te-sl)# commit

```

SR-TE ポリシーの設定

```

/* Configure SR-TE policy */

Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy 100
Router(config-sr-te-policy)# color 1 end-point ipv4 2.2.2.2
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy)# preference 400
Router(config-sr-te-pp-info)# explicit segment-list PE1-PE3-PE2
Router(config-sr-te-pp-info)# exit
!
Router(config-sr-te-policy)# preference 500 <-----largest number takes the
precedence
Router(config-sr-te-pp-info)# explicit segment-list PE1-PE2
Router(config-sr-te-pp-info)# commit
Router(config-sr-te-pp-info)# exit
!
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy 1013
Router(config-sr-te-policy)# color 1013 end-point ipv4 2.2.2.2
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy)# preference 100
Router(config-sr-te-pp-info)# explicit segment-list PE1-PE2_BE121
Router(config-sr-te-pp-info)# exit
!
Router(config-sr-te-policy)# preference 200
Router(config-sr-te-pp-info)# explicit segment-list PE1-PE3-PE2-t0016
Router(config-sr-te-pp-info)# exit
!
Router(config-sr-te-policy)# preference 500
Router(config-sr-te-pp-info)# explicit segment-list PE1-PE2
Router(config-sr-te-pp-info)# exit
!
Router(config-sr-te-policy)# preference 600
Router(config-sr-te-pp-info)# explicit segment-list PE1-PE3-PE2
Router(config-sr-te-pp-info)# exit
!
Router(config-sr-te-policy)# preference 700
Router(config-sr-te-pp-info)# explicit segment-list PE1-PE3-PE2_link
Router(config-sr-te-pp-info)# commit
!
Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# policy 1300
Router(config-sr-te-policy)# color 1300 end-point ipv4 3.3.3.3
Router(config-sr-te-policy)# candidate-paths
Router(config-sr-te-policy)# preference 100
Router(config-sr-te-pp-info)# explicit segment-list PE1-PE3

```

```
Router(config-sr-te-pp-info)# commit
!
```

SR-TE ポリシーを介した VPLS の設定



- (注) 自動生成された SR-TE ポリシー名を使用して、L2VPN インスタンスにポリシーをアタッチします。ポリシー名は、ポリシーの色とエンドポイントに基づいて自動生成されます。自動生成されたポリシー名を表示するには、**show segment-routing traffic-eng policy candidate-path name *policy_name*** コマンドを使用します。

```
Router# show segment-routing traffic-eng policy candidate-path name 100

SR-TE policy database
-----
Color: 1, End-point: 2.2.2.2
Name: srte_c_1_ep_2.2.2.2

Router# show segment-routing traffic-eng policy candidate-path name 1013

SR-TE policy database
-----
Color: 1013, End-point: 2.2.2.2
Name: srte_c_1013_ep_2.2.2.2

Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# pw-class pw100
Router(config-l2vpn-pwc)# encapsulation mpls
Router(config-l2vpn-pwc-mpls)# preferred-path sr-te policy srte_c_1_ep_2.2.2.2
Router(config-l2vpn-pwc-mpls)# exit
!
Router(config-l2vpn)# pw-class pw1013
Router(config-l2vpn-pwc)# encapsulation mpls
Router(config-l2vpn-pwc-mpls)# preferred-path sr-te policy srte_c_1013_ep_2.2.2.2 fallback
disable
Router(config-l2vpn-pwc-mpls)# exit

/* The default is Fallback Enable. If the SR-policy is down, then L2VPN VPWS/VPLS will
try to be UP using the regular IGP path, and not using the SR policy. If Fallback Disable
is configured, the L2VPN PW will be down when the SR-policy is down. Preferred-path is
the action of pinning down a PW to a SR TE policy */

Router(config)#l2vpn
Router(config-l2vpn)#bridge group bg1
Router(config-l2vpn-bg)#bridge-domain vpls501
Router(config-l2vpn-bg-bd)#interface Bundle-Ether41.501
Router(config-l2vpn-bg-bd-ac)#exit
!
Router(config-l2vpn-bg-bd)#interface TenGigE0/0/0/4
Router(config-l2vpn-bg-bd-ac)#split-horizon group
Router(config-l2vpn-bg-bd-ac)#exit
!
Router(config-l2vpn-bg-bd)#vfi vpls1
Router(config-l2vpn-bg-bd-vfi)#neighbor 2.2.2.2 pw-id 501
Router(config-l2vpn-bg-bd-vfi-pw)#pw-class pw100
Router(config-l2vpn-bg-bd-vfi-pw)#exit
```

```
!
Router(config-l2vpn-bg-bd-vfi)#neighbor 3.3.3.3 pw-id 501
Router(config-l2vpn-bg-bd-vfi-pw)#commit
```

SR-TE ポリシーを介した VPWS の設定



- (注) 自動生成された SR-TE ポリシー名を使用して、L2VPN インスタンスにポリシーをアタッチします。ポリシー名は、ポリシーの色とエンドポイントに基づいて自動生成されます。自動生成されたポリシー名を表示するには、**show segment-routing traffic-eng policy candidate-path name policy_name** コマンドを使用します。

```
Router# show segment-routing traffic-eng policy candidate-path name 1300

SR-TE policy database
-----
Color: 1300, End-point: 3.3.3.3
Name: srte_c_1300_ep_3.3.3.3

Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# pw-class pw1300
Router(config-l2vpn-pwc)# encapsulation mpls
Router(config-l2vpn-pwc-mpls)# load-balancing
Router(config-l2vpn-pwc-mpls-load-bal)# flow-label both
Router(config-l2vpn-pwc-mpls-load-bal)# exit
!
Router(config-l2vpn-pwc-mpls)# preferred-path sr-te policy srte_c_1300_ep_3.3.3.3 fallback
disable
Router(config-l2vpn-pwc-mpls)# exit
!
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group xcon1
Router(config-l2vpn-xc)# p2p vplw1002
Router(config-l2vpn-xc-p2p)# interface TenGigE0/0/0/5
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 TenGigE0/0/0/1

 circuit-type level-2-only
 point-to-point
 hello-padding disable
 address-family ipv4 unicast
 adjacency-sid absolute 15101
!
interface TenGigE0/0/0/2
 circuit-type level-2-only
 point-to-point
 hello-padding disable
 address-family ipv4 unicast
 adjacency-sid absolute 15102

```

```
PE2
router isis core
!
interface Bundle-Ether121
  circuit-type level-2-only
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
  adjacency-sid absolute 15200

interface TenGigE0/0/0/0/4
  circuit-type level-2-only
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
  adjacency-sid absolute 15201

interface TenGigE0/0/0/0/7
  circuit-type level-2-only
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
  adjacency-sid absolute 15202

PE3:
router isis core
!
interface TenGigE0/0/0/1
  circuit-type level-2-only
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
  adjacency-sid absolute 15301
!
!
interface TenGigE0/0/0/2
  circuit-type level-2-only
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
  adjacency-sid absolute 15302

/* Configure segment-list */
PE1:
segment-routing
global-block 16000 23999
local-block 15000 15999
traffic-eng
segment-list name PE1-PE2
  index 1 mpls label 16200
!
segment-list name PE1-PE3
  index 1 mpls label 16300
!
segment-list name PE1-PE2-PE3
  index 1 mpls label 16200
  index 2 mpls label 16300
!
segment-list name PE1-PE2_bad
  index 1 mpls label 16900
!
segment-list name PE1-PE3-PE2
  index 1 mpls label 16300
```

```

    index 2 mpls label 16200
    !
    segment-list name PE1-PE2_BE121
    index 1 mpls label 15100
    !
    segment-list name PE1-PE3-PE2_link
    index 1 mpls label 15101
    index 2 mpls label 15302
    !

    segment-list name PE1-PE3-PE2-t0016
    index 1 mpls label 15101
    index 2 mpls label 16200

PE2:
segment-routing
global-block 16000 23999
local-block 15000 15999
traffic-eng
segment-list name PE2-PE1
index 1 mpls label 16100
!
segment-list name PE2-PE3-PE1
index 1 mpls label 16300
index 2 mpls label 16100

PE3:
segment-routing
global-block 16000 23999
local-block 15000 15999
traffic-eng
segment-list name PE3-PE1
index 1 mpls label 16100
!
segment-list name PE3-PE2-PE1
index 1 mpls label 16200
index 2 mpls label 16100

/* Configure SR-TE policy */

segment-routing
traffic-eng
policy 100
color 1 end-point ipv4 2.2.2.2
candidate-paths
preference 400
explicit segment-list PE1-PE3-PE2
!
preference 500
explicit segment-list PE1-PE2

policy 1013
color 1013 end-point ipv4 2.2.2.2
candidate-paths
preference 100
explicit segment-list PE1-PE2_BE121
!
preference 200
explicit segment-list PE1-PE3-PE2-t0016
!
preference 500
explicit segment-list PE1-PE2
!
preference 600

```



```

        explicit segment-list PE1-PE3-PE2
        !
        preference 700
        explicit segment-list PE1-PE3-PE2_link
        !
policy 1300
  color 1300 end-point ipv4 3.3.3.3
  candidate-paths
  preference 100
  explicit segment-list PE1-PE3
  !

/* Configure VPLS over SR-TE policy
l2vpn
  pw-class pw100
    encapsulation mpls
    preferred-path sr-te policy srte_c_1_ep_2.2.2.2
  pw-class pw1013
    encapsulation mpls
    preferred-path sr-te policy srte_c_1013_ep_2.2.2.2 fallback disable
l2vpn
  bridge group bg1
  bridge-domain vpls501
  interface Bundle-Ether41.501
  !
  interface TenGigE0/0/0/4

    split-horizon group
    !
  vfi vpls1
    neighbor 2.2.2.2 pw-id 501
    pw-class pw100
    !
    neighbor 3.3.3.3 pw-id 501

/*Configure VPWS over SR-TE policy
l2vpn
  pw-class pw1300
    encapsulation mpls
    load-balancing
    flow-label both
    preferred-path sr-te policy srte_c_1300_ep_3.3.3.3 fallback disable

Xconnect group xcon1
  p2p vplw1002
  interface TenGigE0/0/0/5
  neighbor 3.3.3.3 pw-id 1002
  pw-class pw1300

```

SR-TE ポリシー設定を介した L2VPN VPLS または VPWS 優先パスの確認

```

/* The prefix-sid and Adjacency-sid must be in the SR topology */

PE1#show segment-routing traffic-eng ipv4 topology | inc Prefix
Thu Feb  1 20:28:43.343 EST
Prefix SID:
  Prefix 1.1.1.1, label 16100 (regular)
Prefix SID:
  Prefix 3.3.3.3, label 16300 (regular)
Prefix SID:

```

```
Prefix 2.2.2.2, label 16200 (regular)
```

```
PE1#show segment-routing traffic-eng ipv4 topology | inc Adj SID
```

```
Thu Feb 1 20:30:25.760 EST
Adj SID: 61025 (unprotected) 15102 (unprotected)
Adj SID: 61023 (unprotected) 15101 (unprotected)
Adj SID: 65051 (unprotected) 15100 (unprotected)
Adj SID: 41516 (unprotected) 15301 (unprotected)
Adj SID: 41519 (unprotected) 15302 (unprotected)
Adj SID: 46660 (unprotected) 15201 (unprotected)
Adj SID: 24003 (unprotected) 15202 (unprotected)
Adj SID: 46675 (unprotected) 15200 (unprotected)
```

```
PE1# show segment-routing traffic-eng policy candidate-path name 100
```

```
SR-TE policy database
```

```
-----
```

```
Color: 100, End-point: 2.2.2.2
Name: srte_c_1_ep_2.2.2.2
```

```
PE1#show segment-routing traffic-eng policy name 100
```

```
Thu Feb 1 23:16:58.368 EST
```

```
SR-TE policy database
```

```
-----
```

```
Name: 100 (Color: 1, End-point: 2.2.2.2)
```

```
Status:
```

```
Admin: up Operational: up for 05:44:25 (since Feb 1 17:32:34.434)
```

```
Candidate-paths:
```

```
Preference 500:
```

```
Explicit: segment-list PE1-PE2 (active)
```

```
Weight: 0, Metric Type: IGP
```

```
16200 [Prefix-SID, 2.2.2.2]
```

```
Preference 400:
```

```
Explicit: segment-list PE1-PE3-PE2 (inactive)
```

```
Inactive Reason: unresolved first label
```

```
Weight: 0, Metric Type: IGP
```

```
Attributes:
```

```
Binding SID: 27498
```

```
Allocation mode: dynamic
```

```
State: Programmed
```

```
Policy selected: yes
```

```
Forward Class: 0
```

```
PE1#show segment-routing traffic-eng policy name 1013
```

```
Thu Feb 1 21:20:57.439 EST
```

```
SR-TE policy database
```

```
-----
```

```
Name: 1013 (Color: 1013, End-point: 2.2.2.2)
```

```
Status:
```

```
Admin: up Operational: up for 00:06:36 (since Feb 1 21:14:22.057)
```

```
Candidate-paths:
```

```
Preference 700:
```

```
Explicit: segment-list PE1-PE3-PE2_link (active)
```

```
Weight: 0, Metric Type: IGP
```

```
15101 [Adjacency-SID, 13.1.1.1 - 13.1.1.2]
```

```
15302
```

```
Preference 600:
```

```

Explicit: segment-list PE1-PE3-PE2 (inactive)
Inactive Reason:
  Weight: 0, Metric Type: IGP
Preference 500:
  Explicit: segment-list PE1-PE2 (inactive)
  Inactive Reason:
    Weight: 0, Metric Type: IGP
Preference 200:
  Explicit: segment-list PE1-PE3-PE2-t0016 (inactive)
  Inactive Reason: unresolved first label
  Weight: 0, Metric Type: IGP
Preference 100:
  Explicit: segment-list PE1-PE2_BE121 (inactive)
  Inactive Reason: unresolved first label
  Weight: 0, Metric Type: IGP
Attributes:
  Binding SID: 27525
  Allocation mode: dynamic
  State: Programmed
  Policy selected: yes
  Forward Class: 0

PE1#show segment-routing traffic-eng forwarding policy name 100
Thu Feb  1 23:19:28.951 EST
Policy          Segment          Outgoing          Outgoing          Next Hop          Bytes
Name           List             Label             Interface          Switched
-----
100            PE1-PE2          Pop               Te0/0/0/2         12.1.9.2          0
                0                Pop               BE121              121.1.0.2

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           Te0/0/0/1         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          Interface          Switched
-----
1013            (SR) 15302        Te0/0/0/1         13.1.1.2          0

PE1#show l2vpn bridge-domain bd-name vpls501 detail
Sat Feb  3 11:27:35.655 EST
Legend: pp = Partially Programmed.
Bridge group: bg1, bridge-domain: vpls501, id: 250, state: up, ShgId: 0, MSTi: 0
.....
List of VFIs:

```

```

VFI vpls1 (up)
  PW: neighbor 2.2.2.2, PW ID 501, state is up ( established )
  PW class pw100, XC ID 0xa00020d5
  Encapsulation MPLS, protocol LDP
  Source address 1.1.1.1
  PW type Ethernet, control word disabled, interworking none
  Sequencing not set
  Preferred path Active : SR TE 100, Statically configured, fallback disabled
  Tunnel : Up
  PW Status TLV in use
  MPLS          Local                               Remote
  -----
  Label         41042                                       24010
  Group ID      0xfa                                       0x1
  Interface     vpls1                                       vpls1
  MTU           1500                                       1500
  Control word  disabled                                       disabled
  PW type       Ethernet                                       Ethernet
  VCCV CV type  0x2                                       0x2
                (LSP ping verification)           (LSP ping verification)
  VCCV CC type  0x6                                       0x6
                (router alert label)               (router alert label)
                (TTL expiry)                       (TTL expiry)
  -----
  Incoming Status (PW Status TLV):
  Status code: 0x0 (Up) in Notification message
  MIB cpwVcIndex: 2684362965
  Create time: 02/02/2018 16:20:59 (19:06:37 ago)

```

関連コマンド

- [adjacency-sid](#)
- [index](#)
- [prefix-sid](#)
- [router isis](#)
- [segment-routing](#)

該当するセグメントルーティング コマンドについては、『*Segment Routing Command Reference for Cisco NCS 5500, NCS 540 Series Routers, and NCS 560 Series Routers*』を参照してください。

関連項目

- [セグメントルーティングの概要 \(318 ページ\)](#)
- [セグメントルーティングの仕組み \(319 ページ\)](#)
- [セグメントルーティング グローバルブロック \(320 ページ\)](#)

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 (XTC)

パス計算要素 (PCE) は、一連のプロシージャを記述します。これにより、パス計算クライアント (PCC) は PCC から発信されたヘッドエンドトンネルの制御を PCE ピアに報告し、委任します。PCE ピアは、PCC が制御している LSP のパラメータの更新と変更を PCC に要求します。また、PCC を有効にして PCE が計算を開始するとともに、ネットワーク全体の調整を行えるようにします。

制約事項

- 自動プロビジョニングされた TE ポリシーの最大数は 1,000 です。
- EVPN VPWS SR ポリシーは EVPN VPWS デュアル ホーミングではサポートされていません。

EVPN はルートがシングルホームネクストホップ用であるかどうかを検証します。そうでない場合は、不適切な SR-TE ポリシーに関するエラーメッセージを発行し、そのポリシーなしで EVPN-VPWS のセットアップを続行します。EVPN は、これがシングルホームかどうかの決定をゼロに設定されている ESI 値に依存します。AC が LACP を実行しているバンドルイーサインターフェイスの場合は、ESI 値を手動でゼロに設定して、自動感知 ESI を上書きする必要があります。これは、EVPN VPWS マルチホーミングがサポートされていないためです。

EVPN デュアルホーミングを無効にするには、バンドルイーサ AC を ESI 値セットをゼロに設定します。

```

evpn
interface Bundle-Ether12
ethernet-segment
identifier type 0 00.00.00.00.00.00.00.00
/* 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

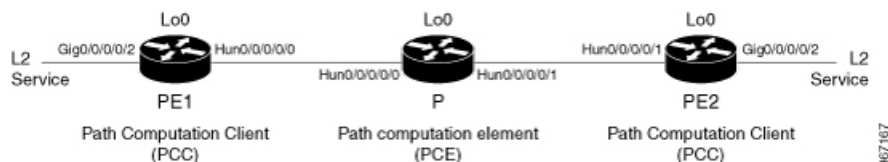
SR-TE を使用して EVPN VPWS オンデマンドネクストホップを設定するには、次のステップを実行します。設定ステップを説明するため、次の図を参考として使用します。

- 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 41: SR-TE を使用した EVPN VPWS オンデマンドネクストホップ



設定例

ISIS でのプレフィックス SID の設定

各ルータがプレフィックスに関連付けられている一意のセグメント識別子を使用するように、ISIS にプレフィックス SID を、コア内にトポロジ独立型ループフリー代替パス (TI-LFA) を設定します。

```
/* Configure Prefix-SID in ISIS and TI-LFA on PE1 */

Router# configure
Route(config)# router isis ring
Route(config-isis)# is-type level-2-only
Route(config-isis)# net 49.0001.1921.6800.1001.00
Route(config-isis)# segment-routing global-block 30100 39100
Route(config-isis)# nsr
Route(config-isis)# distribute link-state
Route(config-isis)# nsf cisco
Route(config-isis)# address-family ipv4 unicast
Route(config-isis-af)# metric-style wide
Route(config-isis-af)# mpls traffic-eng level-1
Route(config-isis-af)# mpls traffic-eng router-id loopback0
Route(config-isis-af)# segment-routing mpls
Route(config-isis-af)# exit
!
Route(config-isis)# interface loopback0
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# prefix-sid index 30101
Route(config-isis-af)# exit
!
Route(config-isis)# interface HundredGigE0/0/0/0
Route(config-isis-if)# circuit-type level-1
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# fast-reroute per-prefix
Route(config-isis-if-af)# fast-reroute per-prefix ti-lfa
Route(config-isis-if-af)# commit

/*Configure Prefix-SID in ISIS and TI-LFA on P router */

Router# configure
Route(config)# router isis ring
Route(config-isis)# net 49.0001.1921.6800.1002.00
Route(config-isis)# segment-routing global-block 30100 39100
Route(config-isis)# nsr
Route(config-isis)# distribute link-state
Route(config-isis)# nsf cisco
Route(config-isis)# address-family ipv4 unicast
Route(config-isis-af)# metric-style wide
Route(config-isis-af)# mpls traffic-eng level-1
Route(config-isis-af)# mpls traffic-eng router-id loopback0
Route(config-isis-af)# segment-routing mpls
Route(config-isis-af)# exit
!
Route(config-isis)# interface loopback0
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# prefix-sid index 30102
Route(config-isis-af)# exit
!
Route(config-isis)# interface HundredGigE0/0/0/0
Route(config-isis-if)# circuit-type level-1
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# fast-reroute per-prefix
Route(config-isis-if-af)# fast-reroute per-prefix ti-lfa
Route(config-isis-if-af)# exit
!
Route(config-isis)# interface HundredGigE0/0/0/1
Route(config-isis-if)# circuit-type level-1
Route(config-isis-if)# point-to-point
```

```

Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# fast-reroute per-prefix
Route(config-isis-if-af)# fast-reroute per-prefix ti-lfa
Route(config-isis-if-af)# commit

/* Configure Prefix-SID in ISIS and TI-LFA on PE2 */

Router# configure
Route(config)# router isis ring
Route(config-isis)# net 49.0001.1921.6800.1003.00
Route(config-isis)# segment-routing global-block 30100 39100
Route(config-isis)# nsr
Route(config-isis)# distribute link-state
Route(config-isis)# nsf cisco
Route(config-isis)# address-family ipv4 unicast
Route(config-isis-af)# metric-style wide
Route(config-isis-af)# mpls traffic-eng level-1
Route(config-isis-af)# mpls traffic-eng router-id loopback0
Route(config-isis-af)# segment-routing mpls
Route(config-isis-af)# exit
!
Route(config-isis)# interface loopback0
Route(config-isis-if)# address-family ipv4 unicast
Route(config-isis-af)# prefix-sid index 30103
Route(config-isis-af)# exit
!
Route(config-isis)# interface HundredGigE0/0/0/1
Route(config-isis-if)# circuit-type level-1
Route(config-isis-if)# point-to-point
Route(config-isis-if)# hello-padding disable
Route(config-isis-if)# fast-reroute per-prefix
Route(config-isis-if-af)# fast-reroute per-prefix ti-lfa
Route(config-isis-if-af)# commit

```

SR-TE の設定

P ルータと PE ルータに SR-TE を設定します。

```

/Configure SR-TE on PE1 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# on-demand color 1
Router(config-sr-te-color)# dynamic mpls
Router(config-sr-te-color-dyn-mpls)# pce
Router(config-sr-te-color-dyn-mpls-pce)# exit
!
Router(config-sr-te)# on-demand color 2
Router(config-sr-te-color)# dynamic mpls
Router(config-sr-te-color-dyn-mpls)# pce
Router(config-sr-te-color-dyn-mpls-pce)# exit
!
Router(config-sr-te)# on-demand color 3
Router(config-sr-te-color)# dynamic mpls
Router(config-sr-te-color-dyn-mpls)# pce
Router(config-sr-te-color-dyn-mpls-pce)# commit

/*Configure SR-TE on P router */
Router# configure
Router(config)# segment-routing

```



```
Router(config-sr)# traffic-eng
Router(config-sr-te)# commit

/Configure SR-TE on PE2 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# on-demand color 11
Router(config-sr-te-color)# dynamic mpls
Router(config-sr-te-color-dyn-mpls)# pce
Router(config-sr-te-color-dyn-mpls-pce)# exit
!
Router(config-sr-te)# on-demand color 12
Router(config-sr-te-color)# dynamic mpls
Router(config-sr-te-color-dyn-mpls)# pce
Router(config-sr-te-color-dyn-mpls-pce)# exit
!
Router(config-sr-te)# on-demand color 13
Router(config-sr-te-color)# dynamic mpls
Router(config-sr-te-color-dyn-mpls)# pce
Router(config-sr-te-color-dyn-mpls-pce)# commit
```

PCE と PCC の設定

P ルータに PCE を、PE1 と PE2 に PCC を設定します。必要に応じて、複数の PCE を設定することもできます。

```
/* Configure PCC on PE1 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# pcc
Router(config-sr-te-pcc)# source-address ipv4 205.1.0.1
Router(config-sr-te-pcc)# pce address ipv4 205.2.0.2
Router(config-sr-te-pcc)# commit

/* Configure PCE on P router */

Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# exit
Router(config)# pce
Router(config-pce)# address ipv4 205.2.0.2
Router(config-pce)# commit

/* Configure PCC on PE2 */

Router# configure
Router(config)# segment-routing
Router(config-sr)# traffic-eng
Router(config-sr-te)# pcc
Router(config-sr-te-pcc)# source-address ipv4 205.3.0.3
Router(config-sr-te-pcc)# pce address ipv4 205.2.0.2
Router(config-sr-te-pcc)# commit
```

SR カラーの設定

PE ルータに SR カラーを設定します。

```
/* Define SR color on PE1 */

Router# configure
Router(config)# extcommunity-set opaque color1
Router(config-ext)# 1
Router(config-ext)# end-set
!
Router(config)# extcommunity-set opaque color2
Router(config-ext)# 2
Router(config-ext)# end-set
!
Router(config)# extcommunity-set opaque color3
Router(config-ext)# 3
Router(config-ext)# end-set
!
/* Define SR color on PE2 */

Router# configure
Router(config)# extcommunity-set opaque color11
Router(config-ext)# 11
Router(config-ext)# end-set
!
Router(config)# extcommunity-set opaque color12
Router(config-ext)# 12
Router(config-ext)# end-set
!
Router(config)# extcommunity-set opaque color13
Router(config-ext)# 13
Router(config-ext)# end-set
!
```

EVPN ルート ポリシーの設定

PE1 と PE2 に EVPN ルート ポリシーを設定します。次に、ルート ポリシー言語を定義し、EVPN ルートを追跡する例を示します。「rd」は PE のアドレスを参照し、L2 サービスのイーサネット仮想インターコネクタとして機能します。

```
/* 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
Router(config-bgp)# bgp router-id 205.1.0.1
Router(config-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
Router(config-bgp)# bgp router-id 205.3.0.3
Router(config-bgp)# bgp graceful-restart
Router(config-bgp)# address-family l2vpn evpn
Router(config-bgp-af)# exit
!
Router(config-bgp)# neighbor 205.1.0.1
Router(config-bgp-nbr)# remote-as 100
Router(config-bgp-nbr)# update-source loopback 0
Router(config-bgp-nbr)# address-family l2vpn evpn
Router(config-bgp-nbr-af)# route-policy evpn_odn_policy in
Router(config-rpl)# commit
```

EVPN VPWS の設定

PE1 と PE2 に EVPN VPWS を設定します。

```

/* Configure EVPN VPWS on PE1 */

Router# configure
Router(config)# interface GigE0/0/0/2.2 l2transport
Router(config-subif)# encapsulation dot1q 1
Router# exit
!
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group evpn_vpws
Router(config-l2vpn-xc)# p2p e1_10
Router(config-l2vpn-xc-p2p)# interface GigE0/0/0/2.2
Router(config-l2vpn-xc-p2p)# neighbor evpn evi 2 target 10 source 10
Router(config-l2vpn-xc-p2p)#commit

/* Configure EVPN VPWS on PE2 */

Router# configure
Router(config)# interface GigE0/0/0/2.4 l2transport
Router(config-subif)# encapsulation dot1q 1
Router# exit
!
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group evpn_vpws
Router(config-l2vpn-xc)# p2p e3_30
Router(config-l2vpn-xc-p2p)# interface GigE0/0/0/2.4
Router(config-l2vpn-xc-p2p)# neighbor evpn evi 2 target 10 source 10
Router(config-l2vpn-xc-p2p)#commit

```

フレキシブルクロスコネクト サービス (FXC) VLAN 非対応の設定

```

/* Configure FXC on PE1 */

Router# configure
Router(config)# interface GigE0/0/0/2.3 l2transport
Router(config-subif)# encapsulation dot1q 3
Router# exit
!
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-unaware evpn_vu
Router(config-l2vpn-fxs-vu)# interface GigE0/0/0/2.3
Router(config-l2vpn-fxs-vu)# neighbor evpn evi 3 target 20
Router(config-l2vpn-fxs-vu)#commit

/* Configure FXC on PE2 */

Router# configure
Router(config)# interface GigE0/0/0/2.3 l2transport
Router(config-subif)# encapsulation dot1q 3
Router# exit
!
Router(config)# l2vpn
Router(config-l2vpn)# flexible-xconnect-service vlan-unaware evpn_vu
Router(config-l2vpn-fxs-vu)# interface GigE0/0/0/2.3
Router(config-l2vpn-fxs-vu)# neighbor evpn evi 3 target 20
Router(config-l2vpn-fxs-vu)#commit

```

実行コンフィギュレーション

```
/* Configure Prefix-SID in ISIS and TI-LFA */
```

PE1:

```
configure
router isis ring
net 49.0001.1921.6800.1001.00
segment-routing global-block 30100 39100
nsr
distribute link-state
nsf cisco
address-family ipv4 unicast
metric-style wide
mpls traffic-eng level-1
mpls traffic-eng router-id Loopback0
segment-routing mpls
!
interface Loopback0
address-family ipv4 unicast
prefix-sid index 30101
!
!
interface HundredGigE0/0/0/0
circuit-type level-1
point-to-point
hello-padding disable
address-family ipv4 unicast
fast-reroute per-prefix
fast-reroute per-prefix ti-lfa
!
!
```

P:

```
configure
router isis ring
net 49.0001.1921.6800.1002.00
segment-routing global-block 30100 39100
nsr
distribute link-state
nsf cisco
address-family ipv4 unicast
metric-style wide
mpls traffic-eng level-1
mpls traffic-eng router-id Loopback0
segment-routing mpls
!
interface Loopback0
address-family ipv4 unicast
prefix-sid index 30102
!
!
interface HundredGigE0/0/0/0
circuit-type level-1
point-to-point
hello-padding disable
address-family ipv4 unicast
fast-reroute per-prefix
fast-reroute per-prefix ti-lfa
!
```

```

!
interface HundredGigE0/0/0/1
  circuit-type level-1
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
    fast-reroute per-prefix
    fast-reroute per-prefix ti-lfa
!

PE2:

configure
router isis ring
  net 49.0001.1921.6800.1003.00
  segment-routing global-block 30100 39100
  nsr
  distribute link-state
  nsf cisco
  address-family ipv4 unicast
    metric-style wide
  mpls traffic-eng level-1
  mpls traffic-eng router-id Loopback0
  segment-routing mpls
!
interface Loopback0
  address-family ipv4 unicast
    prefix-sid index 30103
!
!
interface HundredGigE0/0/0/1
  circuit-type level-1
  point-to-point
  hello-padding disable
  address-family ipv4 unicast
    fast-reroute per-prefix
    fast-reroute per-prefix ti-lfa
!
!

/* Configure SR-TE */

PE1:

configure
  segment-routing
  traffic-eng
    on-demand color 1
    dynamic mpls
    pce
    !
    !
  on-demand color 2
  dynamic mpls
  pce
  !
  !
  on-demand color 3
  dynamic mpls
  pce
  !
P:

```

```
configure
segment-routing
traffic-eng
!

PE2:

configure
segment-routing
traffic-eng
on-demand color 11
dynamic mpls
pce
!
!
on-demand color 12
dynamic mpls
pce
!
!
!
on-demand color 13
dynamic mpls
pce
!

/* Configure PCE and PCC */

PE1:

configure
segment-routing
traffic-eng
pcc
source-address ipv4 205.1.0.1
pce address ipv4 205.2.0.2
!

P:

configure
segment-routing
traffic-eng
pce
address ipv4 205.2.0.2
!

PE2:

configure
segment-routing
traffic-eng
pcc
source-address ipv4 205.3.0.3
pce address ipv4 205.2.0.2
!

/* Configure SR Color */

PE1:

configure
extcommunity-set opaque color1
1
```

```
end-set
!
  extcommunity-set opaque color2
  2
end-set
!
  extcommunity-set opaque color3
  3
end-set
!

PE2:

configure
  extcommunity-set opaque color11
  11
end-set
!
  extcommunity-set opaque color12
  12
end-set
!
  extcommunity-set opaque color13
  13
end-set
!

/* Configure EVPN route policy */

PE1:

configure
  route-policy evpn_odn_policy
  if rd in (205.3.0.3:2) then
    set extcommunity color color1
    set next-hop 205.3.0.3
  elseif rd in (205.3.0.3:3) then
    set extcommunity color color2
    set next-hop 205.3.0.3
  elseif rd in (205.3.0.3:4) then
    set extcommunity color color3
    set next-hop 205.3.0.3
  endif
  pass
end-policy

PE2:

configure
  route-policy evpn_odn_policy
  if rd in (205.1.0.1:2) then
    set extcommunity color color11
    set next-hop 205.1.0.1
  elseif rd in (205.1.0.1:3) then
    set extcommunity color color12
    set next-hop 205.1.0.1
  elseif rd in (205.1.0.1:4) then
    set extcommunity color color13
    set next-hop 205.1.0.1
  endif
  pass
end-policy

/* Configure BGP */
```


PE1:

```
configure
router bgp 100
  bgp router-id 205.1.0.1
  bgp graceful-restart
  address-family l2vpn evpn
  !
neighbor 205.3.0.3
  remote-as 100
  update-source Loopback0
  address-family l2vpn evpn
  route-policy evpn_odn_policy in
  !
```

PE2:

```
configure
router bgp 100
  bgp router-id 205.3.0.3
  bgp graceful-restart
  address-family l2vpn evpn
  !
neighbor 205.1.0.1
  remote-as 100
  update-source Loopback0
  address-family l2vpn evpn
  route-policy evpn_odn_policy in
  !
```

```
/* Configure EVPN VPWS */
```

PE1:

```
configure
interface GigE0/0/0/2.2 l2transport
  encapsulation dot1q 1
  !
l2vpn
xconnect group evpn_vpws
  p2p e1_10
  interface GigE0/0/0/2.2
  neighbor evpn evi 2 target 10 source 10
  !
  !
```

PE2:

```
configure
interface GigE0/0/0/2.4 l2transport
  encapsulation dot1q 1
  !
l2vpn
xconnect group evpn_vpws
  p2p e3_30
  interface GigE0/0/0/2.4
  neighbor evpn evi 2 target 10 source 10
  !
  !
  !
```

```
/* Configure Flexible Cross-connect Service (FXC) */
```

PE1:

```
configure
 interface GigE0/0/0/2.3 l2transport
   encapsulation dot1q 3
 !
l2vpn
 flexible-xconnect-service vlan-unaware evpn_vu
 interface GigE0/0/0/2.3
   neighbor evpn evi 3 target 20
 !
!
```

PE2:

```
configure
 interface GigE0/0/0/2.3 l2transport
   encapsulation dot1q 3
 !
l2vpn
 flexible-xconnect-service vlan-unaware evpn_vu
 interface GigE0/0/0/2.3
   neighbor evpn evi 3 target 20
 !
!
```

SR-TE 設定を使用した EVPN VPWS オン デマンドネクストホップの確認

EVPN ODN 上に設定されている各 L2 サービスに SR-TE ポリシーが自動プロビジョニングされているかを確認します。

```
PE1# show segment-routing traffic-eng policy
```

```
SR-TE policy database
```

```
-----
Name: bgp_AP_1 (Color: 1, End-point: 205.3.0.3)
Status:
  Admin: up Operational: up for 07:16:59 (since Oct  3 16:47:04.541)
Candidate-paths:
  Preference 100:
    Dynamic (pce 205.2.0.2) (active)
      Weight: 0
      30103 [Prefix-SID, 205.3.0.3]
Attributes:
  Binding SID: 68007
  Allocation mode: dynamic
  State: Programmed
  Policy selected: yes
  Forward Class: 0
  Distinguisher: 0
Auto-policy info:
  Creator: BGP
  IPv6 caps enable: no
```

```
PE1#show l2vpn xconnect group evpn_vpws xc-name evpn_vpws_1001 detail
```

```
Group evpn_vpws, XC evpn_vpws_1001, state is up; Interworking none
AC: Bundle-Ether12.1001, state is up
Type VLAN; Num Ranges: 1
Outer Tag: 1000
Rewrite Tags: []
VLAN ranges: [1, 1]
```

```

MTU 1500; XC ID 0xc0000018; interworking none
Statistics:
  packets: received 642304, sent 642244
  bytes: received 61661184, sent 61655424
  drops: illegal VLAN 0, illegal length 0
EVPN: neighbor 20.20.20.20, PW ID: evi 1001, ac-id 10001, state is up ( established )
XC ID 0xa0000007
Encapsulation MPLS
Source address 10.10.10.10
Encap type Ethernet, control word enabled
Sequencing not set
Preferred path Active : SR TE pref_sid_to_PE3, On-Demand, fallback enabled
Tunnel : Up
Load Balance Hashing: src-dst-mac

PE1#show bgp l2vpn evpn route-type 1

BGP router identifier 205.1.0.1, local AS number 100
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0x0 RD version: 0
BGP main routing table version 36
BGP NSR Initial initsync version 25 (Reached)
BGP NSR/ISSU Sync-Group versions 36/0
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 205.1.0.1:2 (default for vrf VPWS:2)
*>i[1][0000.0000.0000.0000.0000][1]/120
205.3.0.3 T:bgp_AP_1
100 0 i

PE1# show evpn evi ead detail

EVI Ethernet Segment Id EtherTag Nexthop Label SRTE IFH
-----
-----
2 0000.0000.0000.0000.0000 1 205.3.0.3 24000 0x5a0
Source: Remote, MPLS

```

関連コマンド

- [adjacency-sid](#)
- [index](#)
- [prefix-sid](#)
- [router isis](#)
- [segment-routing](#)

該当するセグメントルーティングコマンドについては、『*Segment Routing Command Reference for Cisco NCS 5500 Series Routers, Cisco NCS 540 Series Routers, and Cisco NCS 560 Series Routers*』を参照してください。

関連項目

- [セグメントルーティングの概要 \(318 ページ\)](#)
- [セグメントルーティングの仕組み \(319 ページ\)](#)
- [セグメントルーティング グローバルブロック \(320 ページ\)](#)

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」サブモードのみです。

各ルータ (ノード) と各リンク (隣接関係) には関連付けられたセグメント識別子 (SID) があります。ノードセグメント識別子はグローバルに一意であり、IGP で決定されたルータへの最短パスを表します。ネットワーク管理者は各ルータに予約済みブロックからノード ID を割り当てます。一方、隣接関係セグメント ID はローカルで有効なものであり、出力インターフェイスなどの隣接ルータに固有の隣接関係を表します。ルータは、ノード ID の予約済みブロック外の隣接関係識別子を自動的に生成します。MPLS ネットワークでは、セグメント識別子は MPLS ラベルスタック エントリとしてエンコードされます。セグメント ID は指定したパスに沿ってデータを移動します。次の 2 種類のセグメント ID があります。

- **プレフィックス SID** : サービスプロバイダー コア ネットワーク内で IGP が計算した IP アドレスプレフィックスが含まれたセグメント ID。プレフィックス SID はグローバルに一意です。プレフィックスセグメントは、特定のプレフィックスに到達する最短パス (IGP が計算) を表します。ノードセグメントは、ノードのループバックアドレスに結合された特殊なプレフィックスセグメントです。これは、インデックスとしてノード固有の SR グローバルブロック (SRGB) にアドバタイズされます。
- **隣接関係 SID** : ネイバーへのアドバタイジングルータの隣接関係が含まれたセグメント ID。隣接関係 SID は 2 つのルータ間のリンクです。隣接関係 SID は特定のルータに関連しているため、ローカルに一意となっています。

ノードセグメントはマルチホップパスを使用できますが、隣接関係セグメントはワンホップパスです。

セグメント ルーティング グローバル ブロック

セグメント ルーティング グローバル ブロック (SRGB) は、セグメント ルーティングに予約されたラベルの範囲のことです。SRGB は、セグメント ルーティング ノードのローカル プロパティです。MPLS アーキテクチャでは、SRGB はグローバル セグメントに予約済みの一連のローカル ラベルです。セグメント ルーティングでは、各ノードを異なる SRGB で設定できます。そのため、IGP プレフィックス セグメントに関連付けられた絶対 SID はノードごとに変更できます。

SRGB のデフォルト値は 16000 ~ 23999 です。SRGB は、次のように設定できます。

```
Router(config)# router isis 1
Router(config-isis)#segment-routing global-block 45000 55000
```



第 12 章

MACsec を使用した BPDU 透過性の設定

この章では、MACsec 機能での BPDU 透過性について説明します。この機能を使用すると、送信元カスタマー エッジ (CE) デバイスと宛先 CE デバイス間にトンネルを作成し、このトンネルをこれら 2 つの CE 間でのトラフィックの伝送に使用します。

- [MACsec でのレイヤ 2 コントロール プレーンのトンネリング \(321 ページ\)](#)
- [MACsec および MKA の概要 \(321 ページ\)](#)
- [L2CP トンネリング \(322 ページ\)](#)
- [MACsec での L2CP トンネリング \(322 ページ\)](#)
- [設定 \(323 ページ\)](#)

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。インターフェイスが MACsec ポリシーで設定されている場合は、すべての MACsec パケットがパントされるため、2つのカスタマーエッジ (CE) デバイス間で MACsec セッションが確立されます。インターフェイスが MACsec で設定されていない場合は、すべての MACsec パケットがリモート CE にトンネリングされます。MACsec はサブインターフェイスでは設定できません。

CE が MACsec で設定されていて、PE が L2VPN VPWS で設定されている場合、すべての MACsec パケットは VPWS を介してトンネリングされます。

PC のいずれかの CE 接続インターフェイスで MACsec が設定されている場合、このインターフェイス上のすべての MACsec パケットはパントされます。これらのパケットはリモート CE に転送されません。PE のインターフェイスで MACsec が設定されている場合、PE デバイスと CE デバイス間で MACsec セッションは確立されません。

設定

以降の項では、MACsec 機能を使用して BPDU 透過性を設定する手順について説明します。

- MPLS のコアの設定
- L2VPN クロス コネクトの設定
- CE デバイスでの MACsec の設定

L2VPN クロス コネクトの設定

コアに接続するインターフェイス上に IPv4 アドレスを設定します。

```
Router# configure
Router(config)# interface tengige 0/1/0/8/2.1
Router(config-subif)# no shut
Router(config-subif)# ipv4 address 192.0.2.1/24
```

IPv4 ループバック インターフェイスを設定します。

```
Router# configure
Router(config)# interface loopback 0
Router(config)# ipv4 address 10.0.0.1/32
```

IGP として OSPF を設定します。

```
Router# configure
Router(config)# router ospf 100 area 0
Router(config-ospf-ar)# interface Tengige 0/1/0/8/3
Router(config-ospf-ar-if)# exit
Router(config-ospf-ar)# interface loopback 1
```

物理コア インターフェイスに MPLS LDP を設定します。

```
Router(config-ospf-ar)# mpls ldp
Router(config-ldp)# interface TenGigE 0/1/8/3
```

コアに接続するインターフェイス上に IPv4 アドレスを設定します。

```
Router# configure
Router(config)# router bgp 100
Router(config-bgp)# bgp router-id 10.10.10.1
Router(config-bgp)# address-family ipv4 unicast
Router(config-bgp-af)# exit
Router(config-bgp)# address-family l2vpn vpls-vpws
Router(config-bgp-af)# exit
Router(config-bgp)# neighbor 172.16.0.1
Router(config-bgp-nbr)# remote-as 2002
```

```
Router(config-bgp-nbr)# update-source loopback 2
Router(config-bgp-nbr)# address-family l2vpn vpls-vpws
Router(config-bgp-nbr-af)# next-hop-self
```

レイヤ 2 転送として AC を設定し、リモートの疑似回線にパケットを転送します。

```
Router# configure
Router(config)# interface TenGigE 0/1/0/8/2.1 l2transport
Router(config-if)# encaps dot1q 1
```

疑似回線であるネイバーを使用して L2VPN クロスコネクトを設定します。

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# xconnect group g1
Router(config-l2vpn-xc)# p2p g1
Router(config-l2vpn-xc-p2p)# interface TenGigE 0/1/0/2.1
Router(config-l2vpn-xc-p2p)# neighbor 172.16.0.1 pw-id 1
Router(config-l2vpn-xc-p2p-pw)#
```

CE デバイスでの MACsec の設定

```
Router# configure
Router(config)# key chain KC1 macsec
Router(config-kc1-MacSec)# key 5010
Router(config-kc1-MacSec-5010)# key-string password
04795B232C766A6C513A5C4E37582F220F0871781167033124465525017A0C7101 cryptographic-algorithm
aes-128-cmac
Router(config-kc1-MacSec-5010)# lifetime 11:08:00 Aug 08 2017 infinite
Router(config-kc1-MacSec-5010)# commit
!
Router# configure
Router(config)# interface HundredGigE 0/0/0/3
Router(config-if)# macsec psk-keychain KC1
Router(config-if)# commit
```

実行コンフィギュレーション

ここでは、MACsec を使用した BFD 透過性の実行コンフィギュレーションを示します。

```
/* Configuring MPLS core.*/

/* Configure an IPv4 address on an interface that connects to the MPLS core. */

interface tengige 0/1/0/8/3
no shut
ipv4 address 192.0.2.0/24
!

/* Configure an IPv4 loopback interface. */

interface loop 0
ipv4 address 10.0.0.1/32

/* Configure OSPF as IGP. */

router ospf 100 area 0
interface TenGige 0/1/0/8/3
interface loop 0
!
```

```

/* Configure MPLS LDP for the physical core interface. */

mpls ldp
  interface TenGige 0/1/0/8/3
  !
!

/* Configuring L2VPN Xconnect. */

/* Configure an IPv4 address on an interface that connects to the MPLS core. */

router bgp 100
  bgp router-id 192.1.2.22
  address-family ipv4 unicast
  exit
  address-family l2vpn vpls-vpws
  neighbor 172.16.0.1
  remote-as 100
  update-source Loopback2
  address-family l2vpn vpls-vpws
  next-hop-self

/* Configure L2VPN Xconnect with a neighbour which is a pseudowire. */

l2vpn
  xconnect group g1
  p2p g1
  interface tengige 0/1/0/8/2.1
  neighbor 172.16.0.1 pw-id 1

/* Configure MACSec on CE device */
configure
  key chain Kc1 macsec
  key 5010
  key-string password 04795B232C766A6C513A5C4E37582F220F0871781167033124465525017A0C7101
  cryptographic-algorithm aes-128-cmac
  lifetime 11:08:00 Aug 08 2017 infinite
commit
!
configure
  interface HundredGigE0/0/0/3
  macsec psk-keychain Kc1
commit
end

```

確認

次の項に示す show 出力には、MACsec 機能を使用した BPDU 透過性設定の詳細と、それらの設定のステータスが表示されます。

```

/* Verify if IGP on the core is up. */
Router# show ospf neighbor
Group Wed Aug 16 20:32:33.665 UTC
Indicates MADJ interface
# Indicates Neighbor awaiting BFD session up
Neighbors for OSPF 100
Neighbor ID      Pri   State           Dead Time   Address      Interface
172.16.0.1       1     FULL/DR         00:00:30   10.1.1.2    TenGigE0/1/0/8/0
Neighbor is up for 06:05:27Total neighbor count: 1

```

```

/* Verify if the MPLS core is up. */
Router# show mpls ldp neighbor
Wed Aug 16 20:32:38.851 UTC

Peer LDP Identifier: 172.16.0.1:0
  TCP connection: 172.16.0.1:64932 - 172.31.255.254:646
  Graceful Restart: No
  Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 487/523; Downstream-Unsolicited
  Up time: 06:05:24
  LDP Discovery Sources:
    IPv4: (2)
      TenGigE0/1/0/8/0
      Targeted Hello (172.31.255.254 -> 172.16.0.1, active)
    IPv6: (0)
  Addresses bound to this peer:
    IPv4: (8)
      10.0.0.1          10.0.0.2          10.0.0.200        172.16.0.1
      192.168.0.1     172.31.255.255   172.16.0.2        10.255.255.254
    IPv6: (0)

/* Verify if the BGP neighbor is up. */
Router# show bgp neighbor 10.10.10.1
Wed Aug 16 20:32:52.578 UTC

BGP neighbor is 10.10.10.1
  Remote AS 15169, local AS 15169, internal link
  Remote router ID 172.31.255.255
  BGP state = Established, up for 06:03:40
  NSR State: None
  Last read 00:00:34, Last read before reset 00:00:00
  Hold time is 180, keepalive interval is 60 seconds
  Configured hold time: 180, keepalive: 60, min acceptable hold time: 3
  Last write 00:00:34, attempted 19, written 19
  Second last write 00:01:34, attempted 19, written 19
  Last write before reset 00:00:00, attempted 0, written 0
  *****
Connections established 1; dropped 0

/* Verify if the BGP neighbor's next-hop information is valid. */
Router# show cef 10.10.10.1
Wed Aug 16 20:33:18.949 UTC
10.10.10.1/32, version 16, internal 0x1000001 0x0 (ptr 0x8e0ef628) [1], 0x0 (0x8e287bc0),
  0xa20 (0x8e9253e0)
  Updated Aug 16 14:27:15.149
  local adjacency 172.16.0.1
  Prefix Len 32, traffic index 0, precedence n/a, priority 3
  via 172.16.0.1/32, TenGigE0/1/0/8/0, 5 dependencies, weight 0, class 0 [flags 0x0]
  path-idx 0 NHID 0x0 [0x8eb60568 0x8eb60e70]
  next hop 172.16.0.1/32
  local adjacency
  local label 64001          labels imposed {ImplNull}

/* Verify if L2VPN Xconnect is up. */
Router# show l2vpn xconnect
Wed Aug 16 20:47:01.053 UTC
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
       SB = Standby, SR = Standby Ready, (PP) = Partially Programmed

XConnect                Segment 1                Segment 2

```

```

Group      Name      ST      Description      ST      Description      ST
-----
b1         b1         UP      BE100            UP      10.10.10.1      1      UP
-----

/* Note: If L2VPN is down even though the MPLS LDP neighbor is up, check if the AC is
down.
To do this, use the show l2vpn xconnect detail command. */

/* Verify if L2VPN Xconnect is up */
Router# show l2vpn xconnect detail

!
!
AC: Bundle-Ether100, state is up      <<<< This indicates that the AC is up.
Type Ethernet
MTU 1500; XC ID 0xa0000002; interworking none
Statistics:
  packets: received 761470, sent 0
  bytes: received 94326034, sent 0
PW: neighbor 10.10.10.1, PW ID 1, state is up ( established )
PW class not set, XC ID 0xc0000001
Encapsulation MPLS, protocol LDP
Source address 172.16.0.2
PW type Ethernet, control word disabled, interworking none
PW backup disable delay 0 sec
Sequencing not set

!
!
```




第 13 章

参照

ここでは、レイヤ 2 VPN の概要と実装に関する補足情報について説明します。

- [ギガビットイーサネット プロトコル規格 \(329 ページ\)](#)
- [キャリアイーサネットモデルの参照 \(330 ページ\)](#)
- [ギガビットイーサネットおよび10ギガビットイーサネットのデフォルト設定値 \(331 ページ\)](#)
- [リンクバンドルの設定に関する参照 \(333 ページ\)](#)

ギガビットイーサネット プロトコル規格

10 ギガビットイーサネットのアーキテクチャと機能により、サービスプロバイダーは、ルータとポイントオブプレゼンス (POP) 内の他のシステム (コア ルータ、エッジルータ、L2 スイッチ、レイヤ3 (L3) スイッチなど) を相互接続するために設計された、高密度、高帯域幅のネットワークングソリューションを提供でき、その一方でネットワークのスケラビリティおよびパフォーマンスも提供されます。

Cisco NCS 540 シリーズルータのギガビットイーサネットインターフェイスは、次の規格をサポートしています。

- プロトコル規格：
 - IEEE 802.3 物理イーサネット インフラストラクチャ
 - IEEE 802.3ae 10 Gbps イーサネット
- イーサネット規格
 - イーサネット II フレーム構成 (別名 DIX)。
 - IEEE 802.3 フレーム構成には、LLC および LLC/SNAP プロトコルフレーム形式も含まれます。
 - IEEE 802.1q VLAN タギング
 - IEEE 802.1ad プロバイダーブリッジ

詳細については、[キャリアイーサネットモデルの参照 \(330 ページ\)](#) を参照してください。

キャリアイーサネットモデルの参照

この項では、ギガビットイーサネットプロトコル標準の参照について説明します。

IEEE 802.3 物理イーサネット インフラストラクチャ

IEEE 802.3 プロトコル規格では、接続するイーサネットの物理層とデータリンク層の MAC 下位層が定義されています。IEEE 802.3 では、多様な物理メディアで、また多様な速度でキャリア検知多重アクセス/衝突検出 (CSMA/CD) アクセスを使用します。IEEE 802.3 規格は 10 Mbps イーサネットに対応します。IEEE 802.3 規格の拡張では、ギガビットイーサネット、10 ギガビットイーサネット、およびファストイーサネットの実装を規定しています。

IEEE 802.3ae 10 Gbps イーサネット

国際標準化組織の開放型システム間相互接続 (OSI) モデルでは、イーサネットは基本的に L2 プロトコルです。10 ギガビットイーサネットでは、IEEE 802.3 イーサネット MAC プロトコル、IEEE 802.3 イーサネット フレーム形式、および IEEE 802.3 の最小および最大フレーム サイズを使用します。10 Gbps イーサネットは IEEE 802.3ae プロトコル規格に準拠します。

イーサネットモデルに忠実だった 1000BASE-X と 1000BASE-T (ギガビットイーサネット) と同様に、10 ギガビットイーサネットも速度と距離の点でイーサネットが自然に発展した結果です。10 ギガビットイーサネットは全二重方式でファイバのみのテクノロジーなので、低速で半二重方式のイーサネットテクノロジーを定義する CSMA/CD プロトコルを使用した、通信事業者に影響される多重アクセスは必要ありません。他のどの点でも、10 ギガビットイーサネットは元のイーサネットモデルに忠実です。

一般的なイーサネット規格

- IEEE 802.1q VLAN タギング：この規格は、VLAN タギングを定義し、またスイッチ間の従来の VLAN トランッキングも定義します。Cisco NCS 540 シリーズルータは ISL をサポートしていません。
- IEEE 802.1ad プロバイダーブリッジ：この規格は 802.1q のサブセットであり、多くの場合、802.1ad と呼ばれます。Cisco NCS 540 シリーズルータは規格全体には準拠していませんが、規格の機能の大部分はサポートされています。

イーサネット MTU

イーサネットの最大伝送単位 (MTU) は、最大フレームのサイズから 4 バイトのフレームチェックシーケンス (FCS) を引いた値です。この MTU がイーサネットネットワークで伝送できるサイズです。パケットの宛先に到達するまでに経由する各物理ネットワークは、MTU が異なる可能性があります。

Cisco NCS 540 シリーズルータは、2 種類のフレーム転送プロセスをサポートしています。

- IPv4 パケットのフラグメンテーション：このプロセスでは、ネクストホップの物理ネットワークの MTU 内に収まるように、必要に応じて IPv4 パケットが分割されます。



(注) IPv6 はフラグメンテーションをサポートしません。

- MTU の検出プロセスによる最大パケットサイズの決定。このプロセスは、すべての IPv6 デバイスと発信側の IPv4 デバイスに使用できます。このプロセスでは、分割せずに送信できる IPv6 または IPv4 パケットの最大サイズを、発信側の IP デバイスが決定します。最大パケットは、IP 発信元デバイスおよび IP 宛先デバイス間にあるすべてのネットワークの中で、最小 MTU と等値です。このパス内にあるすべてのネットワークの最小 MTU よりもパケットが大きい場合、そのパケットは必要に応じて分割されます。このプロセスによって、発信側のデバイスから大きすぎる IP パケットが送信されなくなります。

標準フレームサイズを超えるフレームの場合、ジャンボフレームのサポートが自動的にイネーブルになります。デフォルト値は標準フレームの場合は 1514、802.1Q タグ付きフレームの場合は 1518 です。これらの数値には、4 バイトの FCS は含まれません。

イーサネットインターフェイスでのフロー制御

10ギガビットイーサネットインターフェイスでのフロー制御は、フロー制御ポーズフレームを定期的に送信する処理で構成されます。この処理は、標準の管理インターフェイスで使用される通常の全二重および半二重のフロー制御とは根本的に異なります。デフォルトでは、入力および出力の両方のフロー制御が Cisco NCS 540 シリーズルータでオフになっています。

ギガビットイーサネットおよび10ギガビットイーサネットのデフォルト設定値

次の表は、ギガビットイーサネットまたは10ギガビットイーサネットのモジュラサービスカードおよびPCの脅威対策PLIMでインターフェイスをイネーブルにしたときに表示される、デフォルトのインターフェイス設定パラメータを示します。



- (注) インターフェイスを管理上のダウン状態にするには、**shutdown** コマンドを使用する必要があります。インターフェイスのデフォルトは **no shutdown** です。ルータにモジュラサービスカードを初めて挿入したときに、プリコンフィギュレーションが行われていない場合、設定マネージャによって **shutdown** 項目が設定に追加されます。この **shutdown** を削除するには、**no shutdown** コマンドを入力します。

表 3: ギガビットイーサネットおよび10ギガビットイーサネット モジュラ サービス カードのデフォルト設定値

パラメータ	設定ファイルのエントリ	デフォルト値	制約事項
フロー制御	flow-control	出力オン、入力オフ	なし
MTU	mtu	1514バイト (通常のフレーム) 1518バイト (802.1Q タグ付きフレーム) 1522バイト (QinQ フレーム)	なし
MAC アドレス	mac address	ハードウェアバインドインアドレス (BIA ²)	L3 のみ
L2 ポート	l2transport	off/L3	L2サブインターフェイスにはL3メイン親インターフェイスが必要です。
出力フィルタリング	Ethernet egress-filter	off	なし
リンク ネゴシエーション	negotiation	off	物理メインインターフェイスのみ
Tunneling Ethertype	tunneling ethertype	0X8100	メインインターフェイスのみで設定されます。サブインターフェイスのみに適用されます。
VLAN タグの一致	encapsulation	メインインターフェイスではすべてのフレーム。サブインターフェイスでは指定されたフレームのみ	encapsulation コマンドはサブインターフェイスのみ

1. 制約事項は L2 メイン インターフェイス、L2 サブインターフェイス、L3 メイン インターフェイス、インターフレックス L2 インターフェイスなどに適用されます。
2. 組み込みのアドレス

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、EtheroKinetic 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。

- グローバルに一意のローカル 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。

