



## Cisco IOS XE Bengaluru 17.6.x (Catalyst 9300 スイッチ) マルチ プロトコルラベルスイッチング (MPLS) コンフィギュレーションガイド

初版 : 2021 年 7 月 31 日

最終更新 : 2023 年 7 月 25 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/](http://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](http://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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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)

© 2021 Cisco Systems, Inc. All rights reserved.



## 目次

---

### 第 1 章

#### MPLS レイヤ 3 VPN の設定 1

##### MPLS レイヤ 3 VPNs 1

MPLS バーチャルプライベート ネットワークの前提条件 1

MPLS バーチャルプライベート ネットワークの制約事項 2

MPLS バーチャルプライベート ネットワークに関する情報 4

MPLS バーチャルプライベート ネットワークの定義 4

MPLS バーチャルプライベート ネットワークの仕組み 5

MPLS バーチャルプライベート ネットワークの主要コンポーネント 5

MPLS バーチャルプライベート ネットワークの利点 6

MPLS バーチャルプライベート ネットワークの設定方法 9

コア ネットワークの設定 9

MPLS バーチャルプライベート ネットワーク カスタマーの接続 10

バーチャルプライベート ネットワークの設定の確認 13

MPLS バーチャルプライベート ネットワーク サイト間の接続の確認 13

MPLS バーチャルプライベート ネットワーク (VPN) の設定例 14

例：RIP を使用した MPLS バーチャルプライベート ネットワークの設定 15

例：スタティック ルートを使用した MPLS バーチャルプライベート ネットワークの設定 16

例：BGP を使用した MPLS バーチャルプライベート ネットワークの設定 17

その他の参考資料 19

MPLS バーチャルプライベート ネットワークの機能履歴 19

---

### 第 2 章

#### eBGP および iBGP マルチパスの設定 21

MPLS-VPN における eBGP および iBGP に対する BGP マルチパス ロード シェアリング 21

MPLS-VPNにおけるeBGPおよびiBGPの両方に対するBGPマルチパスロードシェアリングの前提条件	21
MPLS-VPNにおけるeBGPおよびiBGPの両方に対するBGPマルチパスロードシェアリングの制約事項	22
MPLS-VPNにおけるeBGPおよびiBGPの両方に対するBGPマルチパスロードシェアリングについて	22
eBGPとiBGP間のマルチパスロードシェアリング	22
BGP MPLSネットワークにおけるeBGPおよびiBGPのマルチパスロードシェアリング	23
eBGPおよびiBGPの両方に対するマルチパスロードシェアリングの利点	24
MPLS-VPNにおけるeBGPおよびiBGPの両方に対するBGPマルチパスロードシェアリングの設定方法	24
eBGPおよびiBGPの両方に対するマルチパスロードシェアリングの設定	24
eBGPおよびiBGPの両方に対するマルチパスロードシェアリングの設定の確認	26
MPLS-VPNにおけるeBGPおよびiBGPの両方に対するBGPマルチパスロードシェアリング機能の設定例	26
eBGPおよびiBGPのマルチパスロードシェアリングの設定例	26
MPLS-VPNにおけるeBGPおよびiBGPの両方に対するBGPマルチパスロードシェアリングの機能情報	27
<hr/>	
<b>第 3 章</b>	<b>EIGRP MPLS VPN PE-CE Site of Origin の設定 29</b>
	EIGRP MPLS VPN PE-CE Site of Origin 29
	EIGRP MPLS VPN PE-CE Site of Origin の前提条件 29
	EIGRP MPLS VPN PE-CE Site of Origin の制約事項 30
	EIGRP MPLS VPN PE-CE Site of Origin について 30
	EIGRP MPLS VPN PE-CE Site of Origin サポートの概要 30
	バックドアリンクに対するSite of Originのサポート 30
	Site of Origin 拡張コミュニティとルータとの相互運用 31
	Site of Origin をEIGRPに伝送するBGP VPN ルートの再配布 32
	EIGRP MPLS VPN PE-CE Site of Origin サポート機能の利点 32
	EIGRP MPLS VPN PE-CE Site of Origin サポートの設定方法 32
	Site of Origin 拡張コミュニティの設定 32

SoO 拡張コミュニティの設定の確認	35
EIGRP MPLS VPN PE-CE SoO の設定例	35
Site of Origin 拡張コミュニティの設定例	35
Site of Origin 拡張コミュニティの確認の例	36
EIGRP MPLS VPN PE-CE Site of Origin の機能履歴	37

---

 第 4 章

**Ethernet-over-MPLS (EoMPLS) および疑似回線冗長性の設定 39**

Ethernet-over-MPLS の設定	39
Ethernet-over-MPLS の前提条件	39
Ethernet-over-MPLS の制約事項	40
Ethernet-over-MPLS ポートモードの制約事項	40
EoMPLS VLAN モードの制約事項	40
Ethernet-over-MPLS に関する情報	41
Ethernet-over-MPLS の設定方法	42
Ethernet-over-MPLS ポートモードの設定	42
Ethernet-over-MPLS VLAN モードの設定	45
Ethernet-over-MPLS の設定例	50
疑似回線冗長性の設定	55
疑似回線冗長性の前提条件	55
疑似回線冗長性の制約事項	55
疑似回線冗長性ポートモードの制約事項	55
疑似回線冗長性 VLAN モードの制約事項	56
疑似回線冗長性について	56
疑似回線冗長性の設定方法	57
疑似回線冗長性ポートモードの設定	57
疑似回線冗長性 VLAN モードの設定	62
疑似回線冗長性の設定例	68
Ethernet-over-MPLS および疑似回線冗長性の機能情報	71

---

 第 5 章

**MPLS を介した IPv6 プロバイダー エッジ (6PE) の設定 73**

6PE の前提条件	73
-----------	----

6PE の制約事項	73
6PE について	73
6PE の IPV6 明示的ヌルラベル	74
6PE の設定	75
6PE の IPV6 明示的ヌルラベルの設定	77
6PE の設定例	79
6PE の IPV6 明示的ヌルラベルの設定例	81
MPLS を介した IPv6 プロバイダーエッジ (6PE) の機能履歴	82

## 第 6 章

**MPLS を介した IPv6 VPN プロバイダー エッジ (6VPE) の設定 83**

6VPE の設定	83
6VPE の制約事項	83
6VPE について	83
6VPE の設定例	84
MPLS を介した IPv6 VPN プロバイダーエッジ (6VPE) の機能履歴	88

## 第 7 章

**MPLS VPN InterAS オプションの設定 89**

MPLS VPN InterAS オプションに関する情報	89
自律システムと ASBR	89
MPLS VPN InterAS オプション	90
InterAS オプション B	90
InterAS オプション AB	93
MPLS VPN InterAS オプションの設定方法	97
MPLS VPN InterAS オプション B の設定	97
ネクストホップセルフ方式を使用した InterAS オプション B の設定	97
Redistribute Connected 方式を使用した InterAS オプション B の設定	102
MPLS VPN Inter-AS オプション AB の設定	105
各 VPN カスタマーの ASBR インターフェイスへの VRF の設定	105
ASBR ピア間での MP-BGP セッションの設定	106
Inter-AS 接続を必要とする VPN のルーティング ポリシーの設定	109
Inter-AS オプション A 配置からオプション AB 配置への変更	111

MPLS VPN InterAS オプションの設定の確認	113
MPLS VPN InterAS オプションの設定例	114
InterAS オプション B	114
ネクストホップセルフ方式	114
IGP Redistribute Connected Subnet 方式	120
InterAS オプション AB	126
MPLS VPN InterAS オプションに関するその他の参考資料	130
MPLS VPN InterAS オプションの機能履歴	130

---

## 第 8 章

### MPLS over GRE の設定 133

MPLS over GRE の前提条件	133
GRE を介した MPLS の制約事項	133
MPLS over GRE に関する情報	134
PE-to-PE トンネリング	134
P-to-PE トンネリング	135
P-to-P トンネリング	135
GRE を介した MPLS の設定方法	136
MPLS over GRE トンネルインターフェイスの設定	136
MPLS over GRE の設定例	137
例 : PE-to-PE トンネリング	137
例 : P-to-PE トンネリング	138
例 : P-to-P トンネリング	140
MPLS over GRE に関するその他の参考資料	141
MPLS over GRE の機能情報	141

---

## 第 9 章

### GRE を介した MPLS レイヤ 2 VPN の設定 143

GRE を介した MPLS レイヤ 2 VPN に関する情報	143
トンネリング設定のタイプ	143
PE-to-PE トンネリング	143
P-to-PE トンネリング	144
P-to-P トンネリング	145

GRE を介した MPLS レイヤ 3 VPN の設定方法	145
GRE を介した MPLS レイヤ 2 VPN の設定例	146
例：非 MPLS ネットワークにまたがる GRE トンネルの設定	146
GRE を介した MPLS レイヤ 2 VPN の設定に関するその他の参考資料	147
GRE を介した MPLS レイヤ 2 VPN の設定の機能情報	147

---

**第 10 章**

<b>GRE を介した MPLS レイヤ 3 VPN の設定</b>	<b>149</b>
GRE を介した MPLS レイヤ 3 VPN の前提条件	149
GRE を介した MPLS レイヤ 3 VPN の制約事項	150
GRE を介した MPLS レイヤ 3 VPN に関する情報	150
トンネリング設定のタイプ	150
PE-to-PE トンネリング	150
P-to-PE トンネリング	151
P-to-P トンネリング	152
GRE を介した MPLS レイヤ 3 VPN の設定方法	152
GRE を介した MPLS レイヤ 3 VPN の設定例	153
例：GRE を介した MPLS レイヤ 3 VPN (PE-to-PE トンネリング) の設定	153
例：GRE を介した MPLS レイヤ 3 VPN (P-to-PE トンネリング) の設定	156
GRE を介した MPLS レイヤ 3 VPN の設定の機能情報	159

---

**第 11 章**

<b>MPLS QoS の設定</b>	<b>161</b>
MPLS QoS の前提条件	161
MPLS QoS の制約事項	161
MPLS QoS の概要	162
MPLS QoS の概要	162
MPLS 実験フィールド	163
MPLS EXP の分類とマーキングのメリット	164
MPLS QoS の設定方法	164
MPLS カプセル化パケットの分類	164
最も外側のラベルでの MPLS EXP のマーキング	165
ラベルスイッチドパケットでの MPLS EXP のマーキング	166

条件付きマーキングの設定	167
MPLS EXP の WRED の設定	169
MPLS QoS の設定例	171
例：MPLS カプセル化パケットの分類	171
例：最も外側のラベルでの MPLS EXP のマーキング	172
例：ラベルスイッチドパケットの MPLS EXP のマーキング	172
例：条件付きマーキングの設定	173
例：MPLS EXP の WRED の設定	173
その他の参考資料	174
QoS MPLS EXP の機能履歴	174

---

**第 12 章**

<b>MPLS スタティックラベルの設定</b>	<b>175</b>
MPLS スタティック ラベル	175
MPLS スタティック ラベルの前提条件	175
MPLS スタティック ラベルの制限事項	175
MPLS スタティック ラベルに関する情報	176
MPLS スタティック ラベルの概要	176
MPLS スタティック ラベルの利点	176
MPLS スタティック ラベルの設定方法	176
MPLS スタティック プレフィックス ラベル バインディングの設定	176
MPLS スタティック Prefix/Label バインディングの確認	177
MPLS スタティック ラベルの監視とメンテナンス	178
MPLS スタティック ラベルの設定例	179
例：MPLS スタティック プレフィックス ラベルの設定	179
その他の参考資料	180
MPLS スタティックラベルの機能履歴	181

---

**第 13 章**

<b>MPLS トラフィック エンジニアリングおよび拡張機能の設定</b>	<b>183</b>
MPLS トラフィック エンジニアリングおよび拡張機能の前提条件	183
MPLS トラフィック エンジニアリングおよび拡張機能の制約事項	183
MPLS トラフィック エンジニアリングおよび拡張機能について	184

MPLS トラフィック エンジニアリングおよび拡張機能の概要	184
MPLS トラフィック エンジニアリングの利点	185
MPLS トラフィック エンジニアリングのしくみ	186
トンネルへのトラフィックのマッピング	187
新しいテクノロジーへの IS-IS ネットワークの移行	188
IS-IS ルーティング プロトコルの拡張	188
IS-IS ネットワークを新しいテクノロジーに移行するためのソリューション 1	189
ソリューション 1 での移行アクション	190
IS-IS ネットワークを新しいテクノロジーに移行するためのソリューション 2	190
2 つめのソリューションでの移行アクション	190
TLV コンフィギュレーション コマンド	191
Cisco IOS XE ソフトウェアでの実装	191
MPLS トラフィック エンジニアリングおよび拡張機能の設定方法	192
トンネルをサポートするためのデバイスの設定	192
RSVP ベースのトンネルシグナリングおよび IGP フラッドイングをサポートするためのインターフェイスの設定	193
MPLS トラフィック エンジニアリング用の IS-IS の設定	194
MPLS トラフィック エンジニアリング用の OSPF の設定	195
MPLS トラフィック エンジニアリング トンネルの設定	196
IGP で使用できる MPLS トラフィック エンジニアリング トンネルの設定	198
MPLS トラフィック エンジニアリングおよび拡張機能の設定例	200
例 : IS-IS を使用した MPLS トラフィック エンジニアリングの設定	200
デバイス 1 : MPLS トラフィック エンジニアリングの設定	200
デバイス 1 : IS-IS 設定	201
例 : OSPF を使用した MPLS トラフィック エンジニアリングの設定	201
デバイス 1 : MPLS トラフィック エンジニアリングの設定	201
デバイス 1 : OSPF 設定	201
例 : MPLS トラフィック エンジニアリング トンネルの設定	202
デバイス 1 : ダイナミックパストンネルの設定	202
デバイス 1 : ダイナミックパストンネルの確認	202
デバイス 1 : 明示パスの設定	202

デバイス 1 : 明示パストンネルの設定	202
デバイス 1 : 明示パストンネルの確認	202
例 : トンネル経由の拡張 SPF ルーティングの設定	203
デバイス 1 : IGP 拡張 SPF による考慮の設定	203
デバイス 1 : ルートとトラフィックの確認	203
その他の参考資料	203
MPLS トラフィック エンジニアリングおよび拡張機能の機能履歴	205

---

 第 14 章

<b>MPLS トラフィック エンジニアリング - バンドル インターフェイス サポートの設定</b>	<b>207</b>
MPLS TE - バンドル インターフェイス サポートの前提条件	207
MPLS TE - バンドル インターフェイス サポートの制約事項	208
MPLS TE - バンドル インターフェイス サポートについて	208
Cisco EtherChannel の概要	208
Cisco Gigabit EtherChannel の概要	209
EtherChannel でのロードバランシング	210
MPLS TE - バンドル インターフェイス サポートの設定方法	210
EtherChannel インターフェイスでの MPLS トラフィック エンジニアリングの設定	210
MPLS トラフィック エンジニアリング - バンドル インターフェイス サポートの設定例	211
例 : EtherChannel インターフェイスでの MPLS TE の設定	211
例 : Gigabit EtherChannel での MPLS トラフィック エンジニアリング - バンドル インターフェイス サポートの設定	212
MPLS トラフィック エンジニアリング - バンドル インターフェイス サポートの関連資料	214
MPLS トラフィック エンジニアリング - バンドル インターフェイス サポートの機能情報	214

---

 第 15 章

<b>MPLS トラフィック エンジニアリング (TE) : IP 明示アドレス除外の設定</b>	<b>217</b>
MPLS トラフィック エンジニアリング (TE) - IP 明示アドレス除外の前提条件	217
MPLS トラフィック エンジニアリング (TE) : IP 明示アドレス除外の制約事項	218
MPLS トラフィック エンジニアリング (TE) - IP 明示アドレス除外の概要	218
MPLS トラフィック エンジニアリング	218
シスコ エクスプレス フォワーディング	218
MPLS トラフィック エンジニアリング (TE) - IP 明示アドレス除外の設定方法	219

IP 明示アドレス除外の設定	219
MPLS トラフィック エンジニアリング トンネルの設定	220
MPLS トラフィック エンジニアリング (TE) - IP 明示アドレス除外の設定例	222
例 : IP 明示アドレス除外の設定	222
例 : MPLS トラフィック エンジニアリング トンネルの設定	223
その他の参考資料	223
MPLS トラフィック エンジニアリング (TE) - 明示アドレス除外の機能履歴	224

## 第 16 章

<b>MPLS トラフィック エンジニアリング - LSP 属性の設定</b>	<b>227</b>
MPLS トラフィック エンジニアリング - LSP 属性の前提条件	227
MPLS トラフィック エンジニアリング - LSP 属性の制約事項	227
MPLS トラフィック エンジニアリング - LSP 属性について	228
『MPLS Traffic Engineering—LSP Attributes』	228
MPLS トラフィック エンジニアリング - LSP 属性の利点	228
トラフィック エンジニアリング帯域幅	228
トンネル属性と LSP 属性	229
LSP 属性と LSP 属性リスト	229
LSP 属性リストの管理	230
コンストレイントベース ルーティングとパス オプション選択	230
トンネル再最適化とパス オプション選択	230
帯域幅上書きを使用したパス オプション選択	231
LSP 属性リストを使用する TE トンネルのデフォルトのパス オプション属性	232
MPLS トラフィック エンジニアリング - LSP 属性の設定方法	232
LSP 属性リストの設定	233
LSP 属性リストへの属性の追加	235
例 : LSP 属性リストからの属性の削除	237
LSP 属性リスト内の属性の変更	238
LSP 属性リストの削除	240
LSP 属性リスト内の属性の確認	240
すべての LSP 属性リストの確認	241
LSP 属性リストと MPLS TE トンネルのパス オプションとの関連付け	242

異なる LSP 属性を使用するためのパス オプションの変更	245
MPLS TE トンネルの LSP のパス オプションの削除	248
LSP が正しい属性を使用してシグナリングされていることの確認	250
帯域幅上書きのパス オプションの設定	250
TE トンネルのフォールバック帯域幅パス オプションの設定	250
帯域幅上書きのパス オプションの帯域幅の変更	253
帯域幅上書きのパス オプションの削除	255
LSP が正しい帯域幅を使用してシグナリングされていることの確認	257
MPLS トラフィック エンジニアリング - LSP 属性の設定例	258
LSP 属性リストの設定：例	258
例：LSP 属性リストの設定	258
例：LSP 属性リストへの属性の追加	259
例：LSP 属性リストからの属性の削除	259
例：LSP 属性リスト内の属性の変更	259
例：LSP 属性リストの削除	259
例：LSP 属性リストと TE トンネルのパスオプションとの関連付け	260
例：異なる LSP 属性を使用するためのパスオプションの変更	260
例：MPLS TE トンネルの LSP パスオプションの削除	261
帯域幅上書きのパス オプションの設定：例	261
例：帯域幅上書きのパスオプションの設定	261
TE トンネルのフォールバック帯域幅パス オプションの設定：例	261
例：帯域幅上書きのパスオプションにおける帯域幅の変更	262
例：MPLS TE トンネルの LSP パスオプション帯域幅値の削除	263
その他の参考資料	263
MPLS トラフィック エンジニアリング - LSP 属性の機能情報	264

## 第 17 章

MPLS トラフィック エンジニアリング - トンネル用の設定可能なパス計算メトリックの設定	265
MPLS トラフィック エンジニアリング - トンネル用の設定可能なパス計算メトリックの前提条件	265
MPLS トラフィック エンジニアリング - トンネル用の設定可能なパス計算メトリックの制約事項	266

MPLS トラフィック エンジニアリング - トンネル用の設定可能なパス計算メトリックについて	266
概要	266
利点	267
MPLS トラフィック エンジニアリング - トンネル用の設定可能なパス計算メトリックの設定方法	267
トラフィック エンジニアリング トンネルをサポートするためのプラットフォームの設定	267
MPLS トラフィック エンジニアリング用の IS-IS の設定	268
トラフィック エンジニアリング リンク メトリックの設定	269
MPLS トラフィック エンジニアリング トンネルの設定	270
トンネルパス計算用のメトリック タイプの設定	273
トンネルパス メトリック設定の確認	275
MPLS トラフィック エンジニアリング - トンネル用の設定可能なパス計算メトリックの設定例	275
例：トンネルパス選択のリンク タイプとメトリックの設定	275
例：トンネルパスメトリック設定の確認	278
その他の参考資料	279
MPLS トラフィック エンジニアリング - トンネル用の設定可能なパス計算メトリックに関する機能履歴	280

## 第 18 章

仮想プライベート LAN サービス (VPLS) および VPLS BGP ベースの自動検出の設定	283
VPLS の制約事項	283
VPLS、VPLS BGP ベースの自動検出、および Flow Aware Transport に関する情報	284
VPLS の概要	284
フルメッシュ構成について	284
VPLS BGP ベースの自動検出について	285
Flow Aware Transport 疑似回線について	286
Cisco Catalyst 6000 シリーズ スイッチと Cisco Catalyst 9000 シリーズ スイッチ間の相互運用性	287
VPLS を介した IGMP/MLD スヌーピング	287
VPLS、VPLS BGP ベースの自動検出、および Flow Aware Transport の設定方法	288

CE デバイスへのレイヤ 2 PE デバイスインターフェイスの設定	288
CE デバイスからのタグ付きトラフィックを受け取る PE デバイスの 802.1Q トランクの 設定	288
CE デバイスからのタグなしトラフィックを受け取る PE デバイスの 802.1Q アクセスポート の設定	289
PE デバイスでのレイヤ 2 VLAN インスタンスの設定	290
VPLS の設定	291
Xconnect モードでの VPLS の設定	291
プロトコル CLI モードでの VPLS の設定	294
VPLS BGP ベースの自動検出の設定	302
VPLS BGP ベースの自動検出のイネーブル化	302
VPLS 自動検出を有効にする BGP の設定	303
プロトコル CLI モードでの VPLS BGP ベースの自動検出の設定	306
VPLS および VPLS BGP ベースの自動検出の設定例	309
例：Xconnect モードでの VPLS の設定	309
例：Xconnect モードで設定された VPLS の確認	310
例：テンプレートを使用した VPLS Flow Aware Transport の設定（プロトコル CLI モード）	312
例：VPLS BGP 自動検出の設定	313
例：VPLS BGP 自動検出の確認	314
VPLS および VPLS BGP ベースの自動検出の機能情報	315

## 第 19 章

VPLS の設定：IPv6 ユニキャスト用のルーテッド擬似回線 IRB	317
VPLS の設定に関する制約事項：IPv6 ユニキャスト用ルーテッド擬似回線 IRB	317
VPLS に関する情報：IPv6 ユニキャスト用のルーテッド擬似回線 IRB	317
VPLS について：IPv6 ユニキャスト用のルーテッド擬似回線 IRB	318
集中型 Integrated Routing and Bridging	318
分散型 Integrated Routing and Bridging	319
VPLS でサポートされる機能：IPv6 ユニキャスト用のルーテッド擬似回線 IRB	320
VPLS の設定：IPv6 ユニキャスト用のルーテッド擬似回線 IRB	321
設定例：分散型 IRB	322
VPLS の設定に関する機能情報：IPv6 ユニキャスト用のルーテッド擬似回線 IRB	322

## 第 20 章

<b>MPLS VPN ルート ターゲット書き換えの設定</b>	<b>325</b>
MPLS VPN ルート ターゲット書き換えの前提条件	325
MPLS VPN ルート ターゲット書き換えの制約事項	325
MPLS VPN ルート ターゲット書き換えに関する情報	325
ルート ターゲット置換ポリシー	326
ルート マップおよびルート ターゲットの置換	326
MPLS VPN ルート ターゲット書き換えの設定方法	327
ルート ターゲット置換ポリシーの設定	327
ルート ターゲット置換ポリシーの適用	331
特定の BGP ネイバーへのルート マップの割り当て	331
ルート ターゲット置換ポリシーの確認	334
MPLS VPN ルート ターゲット書き換えの設定例	335
例：ルート ターゲット置換ポリシーの適用	335
例：特定の BGP ネイバーへのルート マップの割り当て	335
MPLS VPN ルートターゲット書き換えの機能履歴	335

## 第 21 章

<b>MPLS VPN-Inter-AS-IPv4 BGP ラベル配布の設定</b>	<b>337</b>
MPLS VPN Inter-AS IPv4 BGP ラベル配布	337
MPLS VPN Inter-AS IPv4 BGP ラベル配布	338
MPLS VPN Inter-AS IPv4 BGP ラベル配布に関する情報	338
MPLS VPN Inter-AS IPv4 BGP ラベル配布の概要	338
BGP ルーティング情報	339
BGP においてルートとともに MPLS ラベルが送信される方法	340
ルートマップを使用したルートのフィルタリング	340
MPLS VPN Inter-AS IPv4 BGP ラベル配布の設定方法	340
IPv4 ルートおよび MPLS ラベルを交換する ASBR の設定	341
VPNv4 ルートを交換するルートリフレクタの設定	343
自律システム内でリモートルートを反映するルートリフレクタの設定	345
ルートマップの作成	348
着信ルート用のルートマップの設定	348

発信ルート用のルートマップの設定	350
ASBR へのルートマップの適用	352
MPLS VPN Inter-AS IPv4 BGP ラベル配布の設定の確認	354
ルートリフレクタ設定の確認	354
CE1 に CE2 のネットワーク到達可能性情報があることの確認	355
PE1 に CE2 のネットワーク層到達可能性情報があることの確認	356
PE2 に CE2 のネットワーク到達可能性情報があることの確認	358
ASBR の設定の確認	359
MPLS VPN Inter-AS IPv4 BGP ラベル配布の設定例	360
BGP を使用して MPLS VPN サービスプロバイダー経由でルートおよび MPLS ラベルを配布する Inter-AS の設定例	361
例：ルートリフレクタ 1 (MPLS VPN サービスプロバイダー)	361
設定例：ASBR1 (MPLS VPN サービスプロバイダー)	363
設定例：ルートリフレクタ 2 (MPLS VPN サービスプロバイダー)	364
設定例：ASBR2 (MPLS VPN サービスプロバイダー)	365
設定例：BGP を使用して非 MPLS VPN サービスプロバイダー経由でルートおよび MPLS ラベルを配布する Inter-AS	366
設定例：ルートリフレクタ 1 (非 MPLS VPN サービスプロバイダー)	367
設定例：ASBR1 (非 MPLS VPN サービスプロバイダー)	368
設定例：ルートリフレクタ 2 (非 MPLS VPN サービスプロバイダー)	370
設定例：ASBR2 (非 MPLS VPN サービスプロバイダー)	371
設定例：ASBR3 (非 MPLS VPN サービスプロバイダー)	372
設定例：ルートリフレクタ 3 (非 MPLS VPN サービスプロバイダー)	373
設定例：ASBR4 (非 MPLS VPN サービスプロバイダー)	374
MPLS VPN Inter-AS IPv4 BGP ラベル配布の設定の機能履歴	376

## 第 22 章

## シームレス MPLS の設定 377

シームレス MPLS に関する情報	377
シームレス MPLS の概要	377
シームレス MPLS のアーキテクチャ	378
シームレス MPLS の設定方法	379

PE ルータでのシームレス MPLS の設定	379
ルータリフレクタでのシームレス MPLS の設定	381
シームレス MPLS の設定例	384
例：PE ルータ 1 でのシームレス MPLS の設定	385
例：ルータリフレクタ 1 でのシームレス MPLS の設定	385
例：PE ルータ 2 でのシームレス MPLS の設定	386
例：ルータリフレクタ 2 でのシームレス MPLS の設定	386
シームレス MPLS の機能履歴	387



# 第 1 章

## MPLS レイヤ 3 VPN の設定

MPLS バーチャルプライベートネットワーク (VPN) は、マルチプロトコルラベルスイッチング (MPLS) プロバイダーコアネットワークによって相互接続された一連のサイトで構成されます。各カスタマーサイトでは、1つ以上のカスタマーエッジ (CE) デバイスが、1つ以上のプロバイダーエッジ (PE) デバイスに接続されます。このモジュールでは、MPLS レイヤ 3 VPN の作成方法について説明します。

- [MPLS レイヤ 3 VPNs \(1 ページ\)](#)

### MPLS レイヤ 3 VPNs

MPLS バーチャルプライベートネットワーク (VPN) は、マルチプロトコルラベルスイッチング (MPLS) プロバイダーコアネットワークによって相互接続された一連のサイトで構成されます。各カスタマーサイトでは、1つ以上のカスタマーエッジ (CE) デバイスが、1つ以上のプロバイダーエッジ (PE) デバイスに接続されます。この章では、MPLS VPN の作成方法について説明します。

### MPLS バーチャルプライベートネットワークの前提条件

- マルチプロトコルラベルスイッチング (MPLS) 、ラベル配布プロトコル (LDP) 、および Cisco Express Forwarding がネットワークにインストールされていることを確認します。
- プロバイダーエッジ (PE) デバイスを含む、コア内のすべてのデバイスは、シスコエクスプレスフォワーディングおよび MPLS 転送をサポートできる必要があります。「MPLS バーチャルプライベートネットワークカスタマーのニーズの評価」を参照してください。
- PE デバイスを含む、コア内のすべてのデバイスで Cisco Express Forwarding を有効にします。Cisco Express Forwarding がイネーブルになっているかどうかを確認する方法については、『Cisco Express Forwarding Configuration Guide』の「Configuring Basic Cisco Express Forwarding」の章を参照してください。
- デバイスをイネーブルにし、サービスの中断時に LDP バインディングおよび MPLS フォワーディングステートを保護するため、`mpls ldp graceful-restart` コマンドを設定する必要があります。スケール設定を使用した高可用性セットアップでの SSO 中のデバイス障害

を回避するために、（フォワーディングステートを保持しない場合でも）このコマンドを設定することを推奨します。

## MPLS バーチャル プライベート ネットワークの制約事項

マルチプロトコル ラベル スイッチング (MPLS) または MPLS バーチャル プライベート ネットワーク (VPN) 環境でスタティックルートを設定する場合は、**ip route** コマンドおよび **ip route vrf** コマンドの一部のバリエーションがサポートされません。スタティック ルートを設定するときは、次の注意事項に従ってください。

### MPLS 環境でサポートされるスタティック ルート

MPLS 環境でスタティックルートを設定する場合、次の **ip route** コマンドがサポートされます。

- **ip route destination-prefix mask interface next-hop-address**

MPLS 環境でスタティックルートを設定し、スタティックな非再帰ルートと特定のアウトバウンドインターフェイスを使用するロードシェアリングを設定する場合、次の **ip route** コマンドがサポートされます。

- **ip route destination-prefix mask interface1 next-hop1**
- **ip route destination-prefix mask interface2 next-hop2**

### TFIB を使用する MPLS 環境でサポートされないスタティック ルート

MPLS 環境でスタティックルートを設定する場合、次の **ip route** コマンドはサポートされません。

- **ip route destination-prefix mask next-hop-address**

MPLS 環境でスタティックルートを設定し、2つのパスでネクストホップに到達できる場所でロードシェアリングを有効にする場合、次の **ip route** コマンドはサポートされません。

- **ip route destination-prefix mask next-hop-address**

MPLS 環境でスタティックルートを設定し、2つのネクストホップで宛先に到達できる場所でロードシェアリングを有効にする場合、次の **ip route** コマンドはサポートされません。

- **ip route destination-prefix mask next-hop1**
- **ip route destination-prefix mask next-hop2**

スタティック ルートを指定する場合は、*interface an next-hop* 引数を使用します。

### MPLS VPN 環境でサポートされるスタティック ルート

次の **ip route vrf** コマンドは、MPLS VPN 環境でスタティックルートを設定し、ネクストホップとインターフェイスが同じ VRF に存在する場合はサポートされません。

- **ip route vrf vrf-name destination-prefix mask next-hop-address**

- **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*
- **ip route vrf** *vrf-name destination-prefix mask interface1 next-hop1*
- **ip route vrf** *vrf-name destination-prefix mask interface2 next-hop2*

MPLS VPN 環境でスタティックルートを設定し、ネクストホップがグローバルルーティングテーブルの MPLS クラウドのグローバルテーブルに存在する場合、次の **ip route vrf** コマンドがサポートされます。たとえば、ネクストホップがインターネットゲートウェイを指している場合は、次のコマンドがサポートされます。

- **ip route vrf** *vrf-name destination-prefix mask next-hop-address global*
- **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address* (このコマンドは、ネクストホップおよびインターフェイスがコアにある場合にサポートされます)。

MPLS VPN 環境でスタティックルートを設定し、スタティックな非再帰ルートと特定のアウトバウンドインターフェイスを使用するロードシェアリングを有効にする場合、次の **ip route** コマンドがサポートされます。

- **ip route** *destination-prefix mask interface1 next-hop1*
- **ip route** *destination-prefix mask interface2 next-hop2*

#### TFIB を使用する MPLS VPN 環境でサポートされないスタティック ルート

MPLS VPN 環境でスタティックルートを設定し、ネクストホップがコア内の MPLS クラウドのグローバルテーブルに存在し、2つのパスでネクストホップに到達できる場所でロードシェアリングを有効にする場合、次の **ip route** コマンドはサポートされません。

- **ip route vrf** *destination-prefix mask next-hop-address global*

MPLS VPN 環境でスタティックルートを設定し、ネクストホップがコア内の MPLS クラウドのグローバルテーブルに存在し、2つのネクストホップで宛先に到達できる場所でロードシェアリングを有効にする場合、次の **ip route** コマンドはサポートされません。

- **ip route vrf** *destination-prefix mask next-hop1 global*
- **ip route vrf** *destination-prefix mask next-hop2 global*

次の **ip route vrf** コマンドは、MPLS VPN 環境でスタティックルートを設定し、ネクストホップとインターフェイスが同じ VRF に存在する場合はサポートされません。

- **ip route vrf** *vrf-name destination-prefix mask next-hop1 vrf-name destination-prefix mask next-hop1*
- **ip route vrf** *vrf-name destination-prefix mask next-hop2*

ネクストホップが CE デバイス上のグローバルテーブルに存在する MPLS VPN 環境でサポートされるスタティック ルート

MPLS VPN 環境でスタティックルートを設定し、ネクストホップがカスタマーエッジ (CE) 側のグローバルテーブルにある場合、次の **ip route vrf** コマンドがサポートされます。たとえ

ば、外部ボーダーゲートウェイプロトコル (EBGP) マルチホップの場合と同様に、宛先プレフィックスが CE デバイスのループバック アドレスである場合は、次のコマンドがサポートされます。

- `ip route vrf vrf-name destination-prefix mask interface next-hop-address`

MPLS VPN 環境でスタティックルートを設定し、ネクストホップが CE 側のグローバルテーブルに存在し、スタティックな非再帰ルートと特定のアウトバウンドインターフェイスを使用するロードシェアリングを有効にする場合、次の `ip route` コマンドがサポートされます。

- `ip route destination-prefix mask interface1 nexthop1`
- `ip route destination-prefix mask interface2 nexthop2`

## MPLS バーチャル プライベート ネットワークに関する情報

この項では、MPLS バーチャルプライベート ネットワークについて説明します。

### MPLS バーチャル プライベート ネットワークの定義

マルチプロトコルラベルスイッチングバーチャルプライベートネットワーク (MPLS VPN) を定義する前に、一般的な VPN を定義する必要があります。VPN の説明を次に示します。

- パブリック インフラストラクチャを介してプライベート ネットワーク サービスを提供する、IP ベースのネットワーク
- インターネットまたはその他のパブリックネットワークやプライベートネットワークを介してプライベートに相互通信できる一連のサイト

通常の VPN は、完全メッシュのトンネル、または相手先固定接続 (PVC) を VPN 内のすべてのサイトに設定することで作成されます。このタイプの VPN は、新しいサイトを追加した場合に VPN 内の各エッジデバイスを変更する必要があるため、維持または拡張が簡単ではありません。

MPLS ベースの VPN は、レイヤ 3 に作成され、ピア モデルに基づきます。ピア モデルによって、サービス プロバイダーおよびカスタマーは、レイヤ 3 のルーティング情報を交換できます。サービス プロバイダーは、カスタマー サイト間でデータをリレーします。このとき、カスタマー側では何をする必要もありません。

MPLS VPN の管理や拡張は、従来の VPN よりも簡単です。新しいサイトが MPLS VPN に追加された場合、更新する必要があるのは、カスタマー サイトにサービスを提供するサービス プロバイダーのエッジデバイスだけです。

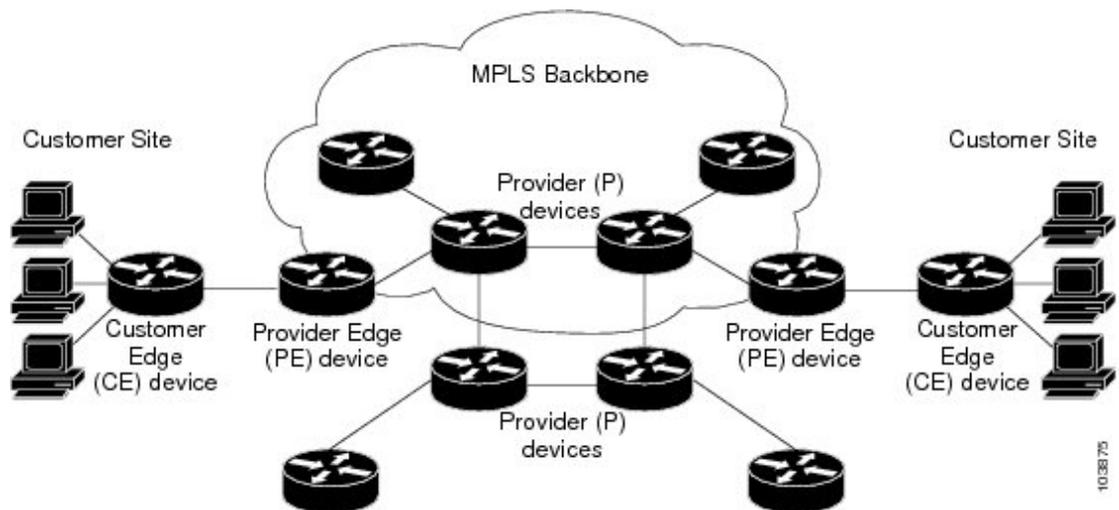
MPLS VPN のさまざまな部分について、次に説明します。

- **プロバイダー (P) デバイス** : プロバイダー ネットワークのコア内のデバイス。P デバイスは MPLS スイッチングを実行し、ルーティングされるパケットに VPN ラベルを付加しません。各ルートの MPLS ラベルは、プロバイダー エッジ (PE) デバイスによって割り当てられます。VPN ラベルは、データ パケットを正しい出力デバイスに誘導するために使用されます。

- PE デバイス：着信パケットが受信されるインターフェイスまたはサブインターフェイスに基づいて、着信パケットに VPN ラベルを付加するデバイス。PE デバイスは、カスタマーエッジ (CE) デバイスに直接接続されます。
- カスタマー (C) デバイス：ISP または企業ネットワークのデバイス。
- CE デバイス：ネットワーク上の PE デバイスに接続する、ISP のネットワーク上のエッジデバイス。CE デバイスは、PE デバイスとインターフェイスする必要があります。

次の図に、基本的な MPLS VPN を示します。

図 1: 基本的 MPLS VPN 用語



## MPLS バーチャルプライベートネットワークの仕組み

マルチプロトコルラベルスイッチングバーチャルプライベートネットワーク (MPLS VPN) 機能は、MPLS ネットワークのエッジでイネーブルになっています。プロバイダーエッジ (PE) デバイスは、次の機能を実行します。

- カスタマーエッジ (CE) デバイスとルーティングアップデートを交換する。
- CE ルーティング情報を VPNv4 ルートに変換する。
- マルチプロトコルボーダーゲートウェイプロトコル (MP-BGP) を介して、他の PE デバイスと VPNv4 ルートを交換する。

ここでは、MPLS VPN の機能について説明します。

## MPLS バーチャルプライベートネットワークの主要コンポーネント

マルチプロトコルラベルスイッチング (MPLS) ベースのバーチャルプライベートネットワーク (VPN) には、次の 3 つの主要コンポーネントがあります。

- **VPN ルート ターゲット コミュニティ**：VPN ルート ターゲット コミュニティは、VPN コミュニティのすべてのメンバのリストです。VPN ルート ターゲットは、各 VPN コミュニティ メンバに設定する必要があります。
- **VPN コミュニティ プロバイダー エッジ (PE) デバイスのマルチプロトコル BGP (MP-BGP) ピアリング**：MP-BGP は、VPN コミュニティのすべてのメンバーに Virtual Route Forwarding (VRF) 到達可能性情報を伝播します。MP-BGP ピアリングは、VPN コミュニティのすべての PE デバイスで設定されている必要があります。
- **MPLS 転送**：MPLS は、VPN サービス プロバイダー ネットワーク上のすべての VPN コミュニティ メンバ間のすべてのトラフィックを転送します。

1 対 1 の関係は、カスタマー サイトと VPNs 間に必ずしも存在する必要はありません。1 つの指定されたサイトを複数の VPN のメンバにできます。ただし、サイトは、1 つの VRF とだけ関連付けることができます。カスタマー サイトの VRF には、そのサイトがメンバとなっている VPN からサイトへの、利用できるすべてのルートが含まれています。

## MPLS バーチャル プライベート ネットワークの利点

マルチプロトコル ラベル スイッチング バーチャル プライベート ネットワーク (MPLS VPN) を使用すると、サービス プロバイダーは、スケーラブルな VPN を展開できます。また、次のような付加価値サービスを提供するための基盤を構築します。

### コネクションレス型サービス

MPLS VPN の重要な技術的メリットとして、コネクションレスであることを挙げるができます。インターネットの成功には、TCP/IP という基礎的な技術が貢献しています。TCP/IP は、パケットを基礎とする、コネクションレス ネットワーク パラダイムに基づいて構築されています。これは、ホスト間の通信を確立するための事前のアクションが不要となり、2 者間の通信が簡単になることを意味します。現在の VPN ソリューションでは、コネクションレス型の IP 環境でプライバシーを確立するために、ネットワーク上でコネクション型ポイントツーポイントのオーバーレイを行っています。VPN がコネクションレス型ネットワーク上で動作しても、VPN では接続の容易さや、コネクションレス型ネットワークで利用できる多様なサービスを活用できません。コネクションレス VPN を作成すると、ネットワーク プライバシーのためのトンネルおよび暗号化が不要となり、その結果、複雑さが大幅に軽減されます。

### 集中型サービス

レイヤ 3 に VPN を構築すると、VPN に代表されるユーザー グループに目的のサービスを配布できます。VPN がサービス プロバイダーに提供する内容は、ユーザーがイントラネット サービスにプライベートに接続するためのメカニズムではありません。VPN では、付加価値サービスを対象のカスタマーに柔軟に提供する方法も提供する必要があります。ユーザーがそれぞれのイントラネットやエクストラネットでサービスをプライベートに使用できるようにするためには、拡張性が重要です。MPLS VPN は、プライベート イントラネットと見なされ、次のような新しい IP サービスを使用できます。

- マルチキャスト

- Quality Of Service (QoS)
- VPN でのテレフォニー サポート
- コンテンツや VPN への Web ホスティングを含む、集中型サービス

カスタマーごとに特化したサービスを、複数組み合わせることでカスタマイズできます。たとえば、IP マルチキャストを低遅延のサービス クラスに組み合わせると、ビデオ会議をイントラネット内で実施できます。

### 拡張性

コネクション型ポイントツーポイントのオーバーレイ、フレームリレー、または ATM 仮想接続 (VC) を使用する VPN を作成する場合、その VPN では、主にスケーラビリティが問題となります。特に、カスタマー サイト間での完全メッシュ接続のないコネクション型 VPN は、最適ではありません。MPLS ベースの VPN では、スケーラビリティの高い VPN ソリューションを活用するために、代わりに、ピアモデルとレイヤ 3 コネクションレス型アーキテクチャを使用します。このピアモデルでは、カスタマー サイトがピアリングする必要があるのは、VPN のメンバであるその他のすべてのカスタマー エッジ (CE) デバイスではなく、1つのプロバイダーエッジ (PE) デバイスだけとなります。コネクションレス型アーキテクチャによって、レイヤ 3 に VPN を作成することができ、トンネルまたは VC を行う必要がなくなります。

MPLS VPN のその他の拡張性の問題は、PE デバイス間の VPN ルートのパーティショニングに起因します。また、コア ネットワークでの PE デバイスとプロバイダー (P) デバイス間での VPN ルートおよび内部ゲートウェイプロトコル (IGP) ルートのさらなるパーティショニングに起因します。

- PE デバイスは、メンバである VPN に対して VPN ルートを維持する必要があります。
- P デバイスでは、VPN ルートを一切維持する必要がありません。

これにより、プロバイダーのコアのスケーラビリティが高まり、いずれのデバイスもスケーラビリティのボトルネックとなりません。

### セキュリティ

MPLS VPN はコネクション型 VPN と同じレベルのセキュリティを提供します。1つの VPN からのパケットが、間違っても別の VPN に送信されることはありません。

セキュリティは、次の領域で提供されます。

- プロバイダーネットワークのエッジでは、お客様から受信したパケットが、正しい VPN に配置されることが保証されます。
- バックボーンでは、VPN トラフィックが常に分離されます。悪意のあるスプーフィング (PE デバイスへのアクセスを取得するための試行) は、ほぼ不可能です。これは、お客様から受信するパケットが IP パケットであるためです。これらの IP パケットは、VPN レベルと一意に識別される特定のインターフェイスまたはサブインターフェイスで受信される必要があります。

### 作成の容易さ

VPN を最大限に活用するには、カスタマーは、新しい VPN とユーザー コミュニティを簡単に作成できる必要があります。MPLS VPN はコネクションレスであるため、特定のポイントツーポイント接続マップまたはトポロジは必要ありません。イントラネットやエクストラネットにサイトを追加して、非公開ユーザー グループを形成できます。この方法で VPN を管理すると、指定された任意のサイトを複数の VPN のメンバにできるため、イントラネットやエクストラネットを構築する場合の柔軟性が最大限に高められます。

### 柔軟なアドレッシング

VPN サービスへのアクセスをより簡単にするために、サービスプロバイダーのお客様は、独自のアドレッシング計画を設計できます。このアドレッシング計画は、他のサービスプロバイダーのお客様のアドレッシング計画から独立させることができます。RFC 1918 に定義されているとおり、多くのお客様はプライベートアドレス空間を使用します。また、イントラネットの接続性を得るために時間と費用をかけてパブリック IP アドレスに変換することは望んでいません。MPLS VPN を使用すると、お客様は、アドレスのパブリックビューとプライベートビューを提供することで、ネットワークアドレス変換 (NAT) を使用することなく現在のアドレス空間を引き続き使用できます。NAT は、重複するアドレス空間を持つ 2 つの VPN が通信する必要がある場合にだけ必要となります。これにより、カスタマーは、パブリック IP ネットワーク上で、独自の未登録プライベートアドレスを使用して自由に通信できます。

### 統合 QoS サポート

QoS は、多くの IP VPN カスタマーにとって重要な要件です。統合 QoS を使用すると、次の 2 つの基本的な VPN 要件に対処できます。

- 予測可能なパフォーマンスおよびポリシーの実装
- MPLS VPN における複数レベルのサービスのサポート

ネットワークトラフィックは、ネットワークのエッジで分類およびラベル付けされます。トラフィックはその後、加入者によって定義されたポリシーに従って集約され、プロバイダーによって実行されて、プロバイダーコア経由で転送されます。その後、破棄確率または遅延ごとに、ネットワークのエッジおよびコアでのトラフィックを異なるクラスに分けることができます。

### 直接的な移行

サービスプロバイダーは、VPN サービスを迅速に展開するために、直接的な移行パスを使用します。MPLS VPN の独自の長所として、IP、ATM、フレームリレー、およびハイブリッドネットワークを含む、複数のネットワークアーキテクチャ上に構築できることを挙げるできます。

CE デバイス上で MPLS をサポートする必要がないため、エンドカスタマーの移行作業は簡単になります。お客様のイントラネットを変更する必要はありません。

## MPLS バーチャル プライベート ネットワークの設定方法

次の項では、MPLS バーチャル プライベート ネットワークを設定する手順について説明します。

### コア ネットワークの設定

次の項では、コアネットワークを設定する手順について説明します。

#### MPLS バーチャル プライベート ネットワーク カスタマーのニーズの評価

マルチプロトコル ラベル スイッチング 仮想プライベート ネットワーク (MPLS VPN) を設定する前に、コア ネットワーク トポロジを識別して、MPLS VPN カスタマーに最適なサービスが提供されるようにする必要があります。コア ネットワーク トポロジを識別するには、次の作業を実行します。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	ネットワークのサイズを識別します。	必要となるデバイスとポートの数を決定するために、次の内容を識別します。 <ul style="list-style-type: none"> <li>サポートする必要があるカスタマーの数</li> <li>カスタマーごとに必要となる VPN の数</li> <li>各 VPN に存在する、仮想ルーティングおよび転送インスタンスの数</li> </ul>
ステップ 2	コアにおけるルーティング プロトコルを識別します。	コア ネットワークで必要なルーティング プロトコルを決定します。
ステップ 3	MPLS VPN ハイ アベイラビリティのサポートが必要かどうかを判断します。	MPLS VPN ノンストップ フォワーディングおよびグレースフルリスタートは、選択デバイスおよび Cisco IOS ソフトウェア リリースでサポートされています。Cisco サポートに問い合わせ、正確な要件およびハードウェア サポートを確認してください。
ステップ 4	MPLS VPN コアで Border Gateway Protocol (BGP) ロードシェアリングおよび冗長パスが必要かどうかを決定します。	設定手順については、『 <i>MPLS Layer 3 VPNs Inter-AS and CSC Configuration Guide</i> 』の「Load Sharing MPLS VPN Traffic」モジュールを参照してください。

## コアにおける MPLS の設定

コアのすべてのデバイスでマルチプロトコルラベルスイッチング (MPLS) をイネーブルにするには、ラベル配布プロトコルとして次のいずれかを設定する必要があります。

- MPLS ラベル配布プロトコル (LDP)。設定については、『*MPLS Label Distribution Protocol Configuration Guide*』の「MPLS Label Distribution Protocol (LDP)」モジュールを参照してください。

## MPLS バーチャルプライベート ネットワーク カスタマーの接続

次の項では、MPLS バーチャルプライベート ネットワーク カスタマーの接続について説明します。

### カスタマーの接続を可能にするための、PE デバイスでの VRF の定義

次の手順を使用して、IPv4 の仮想ルーティングおよび転送 (VRF) 設定を定義します。IPv4 と IPv6 の VRF を定義するには、MPLS レイヤ 3 VPN コンフィギュレーションガイド [英語] の「IPv6 VPN over MPLS」モジュールの「Configuring a Virtual Routing and Forwarding Instance for IPv6」を参照してください。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> enable	特権 EXEC モードを有効にします。  • パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例：  Device# configure terminal	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 3	<b>vrf definition vrf-name</b> 例：  Device(config)# vrf definition vrf1	バーチャルプライベート ネットワーク (VRF) 名を割り当て、VRF コンフィギュレーション モードを開始することにより、Virtual Routing and Forwarding (VPN) ルーティング インスタンスを定義します。  • <i>vrf-name</i> 引数は、VRF に割り当てる名前です。
ステップ 4	<b>rd route-distinguisher</b> 例：	ルーティング テーブルと転送テーブルを作成します。

	コマンドまたはアクション	目的
	<pre>Device(config-vrf)# rd 100:1</pre>	<ul style="list-style-type: none"> <li>• <i>route-distinguisher</i> 引数によって、8 バイトの値が IPv4 プレフィックスに追加され、VPN IPv4 プレフィックスが作成されます。ルート識別子 (RD) は、次のいずれかの形式で入力できます。 <ul style="list-style-type: none"> <li>• 16 ビットの AS 番号 : 32 ビットの番号。101:3 など。</li> <li>• 32 ビットの IP アドレス : 16 ビットの番号。10.0.0.1:1 など。</li> </ul> </li> </ul>
ステップ 5	<p><b>address-family ipv4   ipv6</b></p> <p>例 :</p> <pre>Device(config-vrf)# address-family ipv6</pre>	IPv4 または IPv6 アドレスファミリーモードを開始します。
ステップ 6	<p><b>route-target {import   export   both}</b> <i>route-target-ext-community</i></p> <p>例 :</p> <pre>Device(config-vrf-af)# route-target both 100:1</pre>	<p>VRF 用にルート ターゲット拡張コミュニティを作成します。</p> <ul style="list-style-type: none"> <li>• <b>import</b> キーワードを使用すると、ターゲット VPN 拡張コミュニティからルーティング情報がインポートされます。</li> <li>• <b>export</b> キーワードを使用すると、ルーティング情報がターゲット VPN 拡張コミュニティにエクスポートされます。</li> <li>• <b>both</b> キーワードを使用すると、ターゲット VPN 拡張コミュニティとの間でルーティング情報がインポートおよびエクスポートされます。</li> <li>• <i>route-target-ext-community</i> 引数により、<i>route-target</i> 拡張コミュニティ属性が、インポートやエクスポートの <i>route-target</i> 拡張コミュニティの VRF リストに追加されます。</li> </ul>
ステップ 7	<p><b>exit</b></p> <p>例 :</p> <pre>Device(config-vrf)# exit</pre>	(任意) 終了して、グローバルコンフィギュレーション モードに戻ります。

## 各 VPN カスタマー用の PE デバイスでの VRF インターフェイスの設定

プロバイダー エッジ (PE) デバイス上のインターフェイスまたはサブインターフェイスに仮想ルーティングおよび転送 (VRF) インスタンスを関連付けるには、次の作業を実行します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  Device> enable	特権 EXEC モードを有効にします。  • パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例 :  Device# configure terminal	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 3	<b>interface type number</b> 例 :  Device(config)# interface GigabitEthernet 0/0/1	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。  • <i>type</i> 引数で、設定するインターフェイスのタイプを指定します。  • <i>number</i> 引数には、ポート、コネクタ、またはインターフェイス カード番号を指定します。
ステップ 4	<b>vrf forwarding vrf-name</b> 例 :  Device(config-if)# vrf forwarding vrf1	指定したインターフェイスまたはサブインターフェイスに VRF を関連付けます。  • <i>vrf-name</i> 引数は、VRF に割り当てる名前です。
ステップ 5	<b>end</b> 例 :  Device(config-if)# end	(任意) 終了して、特権 EXEC モードに戻ります。

## PE デバイスと CE デバイス間でのルーティング プロトコルの設定

カスタマー エッジ (CE) デバイスで使用されているのと同じルーティング プロトコルを使用して、プロバイダー エッジ (PE) デバイスを設定します。ボーダー ゲートウェイ プロトコル (BGP)、Routing Information Protocol バージョン 2 (RIPv2)、EIGRP、Open Shortest Path First (OSPF)、または PE デバイスと CE デバイス間のスタティックルートを設定できます。

## バーチャル プライベート ネットワーク の設定の確認

ルート識別子は、Virtual Route Forwarding (VRF) インスタンス用に設定する必要があります。マルチプロトコル ラベル スイッチング (MPLS) は、VRF を伝送するインターフェイスで設定する必要があります。 **show ip vrf** コマンドを使用して、VRF 用に設定されているルート識別子 (RD) とインターフェイスを確認します。

### 手順

---

#### show ip vrf

一連の定義済み VRF インスタンスおよび関連付けられているインターフェイスを表示します。また、この出力では、VRF インスタンスが設定済みルート識別子にマップされます。

---

## MPLS バーチャル プライベート ネットワーク サイト間の接続の確認

ローカルおよびリモートのカスタマー エッジ (CE) デバイスがマルチプロトコル ラベル スイッチング (MPLS) コアを介して通信できることを確認するには、次の作業を実行します。

### MPLS コアを介した CE デバイスから CE デバイスへの IP 接続の確認

### 手順

---

#### ステップ 1 enable

特権 EXEC モードをイネーブルにします。

#### ステップ 2 ping [protocol] {host-name | system-address}

AppleTalk、コネクションレス型モード ネットワーク サービス (CLNS)、IP、Novell、Apollo、Virtual Integrated Network Service (VINES)、DECnet、または Xerox Network Service (XNS) ネットワークでの基本的なネットワーク接続を診断します。 **ping** コマンドを使用して、CE デバイス間の接続を確認します。

#### ステップ 3 trace [protocol] [destination]

パケットがその宛先に送信されるときに取るルートを検出します。 **trace** コマンドは、2つのデバイスが通信できない場合に問題の箇所を分離するのに役立ちます。

#### ステップ 4 show ip route [ip-address [mask] [longer-prefixes]] | protocol [process-id] | [list [access-list-name | access-list-number]

ルーティング テーブルの現在の状態を表示します。 *ip-address* 引数を使用して、CE1 に CE2 へのルートが含まれていることを確認します。CE1 から学習したルートを確認します。CE2 へのルートがリストされていることを確認します。

---

## ローカル CE デバイスとリモート CE デバイスが PE ルーティング テーブルに存在することの確認

## 手順

**ステップ 1 enable**

特権 EXEC モードをイネーブルにします。

**ステップ 2 show ip route vrf vrf-name [prefix]**

Virtual Route Forwarding (VRF) インスタンスに関連付けられている IP ルーティングテーブルを表示します。ローカル カスタマー エッジ (CE) デバイスとリモート カスタマー エッジ (CE) デバイスのループバック アドレスが、プロバイダー エッジ (PE) でデバイスのルーティング テーブルに存在することを確認します。

**ステップ 3 show ip cef vrf vrf-name [ip-prefix]**

VRF に関連付けられている Cisco Express Forwarding 転送テーブルを表示します。次のように、リモート CE デバイスのプレフィックスが、シスコ エクスプレス フォワーディング テーブルに存在することを確認します。

## MPLS バーチャル プライベート ネットワーク (VPN) の設定例

次の項では、MPLS バーチャルプライベート ネットワークを設定する手順について説明します。

## 例：RIP を使用した MPLS バーチャルプライベートネットワークの設定

PE の設定	CE の設定
<pre> vrf vpn1 rd 100:1 route-target export 100:1 route-target import 100:1 ! ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0 ip address 10.0.0.1 255.255.255.255 ! interface GigabitEthernet 1/0/1 vrf forwarding vpn1 ip address 192.0.2.3 255.255.255.0 no cdp enable interface GigabitEthernet 1/0/1 ip address 192.0.2.2 255.255.255.0 mpls label protocol ldp mpls ip ! router rip version 2 timers basic 30 60 60 120 ! address-family ipv4 vrf vpn1 version 2 redistribute bgp 100 metric transparent network 192.0.2.0 distribute-list 20 in no auto-summary exit-address-family ! router bgp 100 no synchronization bgp log-neighbor changes neighbor 10.0.0.3 remote-as 100 neighbor 10.0.0.3 update-source Loopback0 no auto-summary ! address-family vpnv4 neighbor 10.0.0.3 activate neighbor 10.0.0.3 send-community extended  bgp scan-time import 5 exit-address-family ! address-family ipv4 vrf vpn1 redistribute connected redistribute rip no auto-summary no synchronization exit-address-family </pre>	<pre> ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0 ip address 10.0.0.9 255.255.255.255 ! interface GigabitEthernet 1/0/1 ip address 192.0.2.1 255.255.255.0 no cdp enable router rip version 2 timers basic 30 60 60 120 redistribute connected network 10.0.0.0 network 192.0.2.0 no auto-summary </pre>

例：スタティック ルートを使用した MPLS バーチャル プライベート ネットワーク の設定

## 例：スタティック ルートを使用した MPLS バーチャル プライベート ネットワーク の設定

PE の設定	CE の設定
<pre>vrf vpn1  rd 100:1   route-target export 100:1   route-target import 100:1 ! ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0  ip address 10.0.0.1 255.255.255.255 ! interface GigabitEthernet 1/0/1  vrf forwarding vpn1  ip address 192.0.2.3 255.255.255.0  no cdp enable ! interface GigabitEthernet 1/0/1  ip address 192.168.0.1 255.255.0.0  mpls label protocol ldp  mpls ip ! router ospf 100  network 10.0.0. 0.0.0.0 area 100  network 192.168.0.0 255.255.0.0 area 100 ! router bgp 100  no synchronization  bgp log-neighbor changes  neighbor 10.0.0.3 remote-as 100  neighbor 10.0.0.3 update-source Loopback0  no auto-summary ! address-family vpnv4  neighbor 10.0.0.3 activate  neighbor 10.0.0.3 send-community extended  bgp scan-time import 5  exit-address-family ! address-family ipv4 vrf vpn1  redistribute connected  redistribute static  no auto-summary  no synchronization  exit-address-family ! ip route vrf vpn1 10.0.0.9 255.255.255.255 192.0.2.2 ip route vrf vpn1 192.0.2.0 255.255.0.0 192.0.2.2</pre>	<pre>ip cef ! interface Loopback0  ip address 10.0.0.9 255.255.255.255 ! interface GigabitEthernet 1/0/1  ip address 192.0.2.2 255.255.0.0  no cdp enable ! ip route 10.0.0.9 255.255.255.255 192.0.2.3 3 ip route 198.51.100.0 255.255.255.0 192.0.2.3 3</pre>

## 例 : BGP を使用した MPLS バーチャルプライベートネットワークの設定

PE の設定	CE の設定
	<pre>router bgp 5000 bgp log-neighbor-changes neighbor 5.5.5.6 remote-as 5001 neighbor 5.5.5.6 ebgp-multihop 2 neighbor 5.5.5.6 update-source Loopback5 neighbor 35.2.2.2 remote-as 5001 neighbor 35.2.2.2 ebgp-multihop 2 neighbor 35.2.2.2 update-source Loopback1 neighbor 3500::1 remote-as 5001 neighbor 3500::1 ebgp-multihop 2 neighbor 3500::1 update-source Loopback1 ! address-family ipv4   redistribute connected   neighbor 5.5.5.6 activate   neighbor 35.2.2.2 activate   no neighbor 3500::1 activate exit-address-family ! address-family ipv6   redistribute connected   neighbor 3500::1 activate exit-address-family Device-RP(config)#</pre>

例 : BGP を使用した MPLS バージナル プライベート ネットワーク の設定

PE の設定	CE の設定
<pre> router bgp 5001   bgp log-neighbor-changes   bgp graceful-restart   bgp sso route-refresh-enable   bgp refresh max-eor-time 600   redistribute connected   neighbor 102.1.1.1 remote-as 5001   neighbor 102.1.1.1 update-source Loopback1   neighbor 105.1.1.1 remote-as 5001   neighbor 105.1.1.1 update-source Loopback10   neighbor 160.1.1.2 remote-as 5002   !   address-family vpnv4     neighbor 102.1.1.1 activate     neighbor 102.1.1.1 send-community both     neighbor 105.1.1.1 activate     neighbor 105.1.1.1 send-community extended   exit-address-family   !   address-family vpnv6     neighbor 102.1.1.1 activate     neighbor 102.1.1.1 send-community extended      neighbor 105.1.1.1 activate     neighbor 105.1.1.1 send-community extended   exit-address-family   !   address-family ipv4 vrf full     redistribute connected     neighbor 20.1.1.1 remote-as 5000     neighbor 20.1.1.1 ebgp-multihop 2     neighbor 20.1.1.1 update-source Loopback2     neighbor 20.1.1.1 activate     neighbor 20.1.1.1 send-community both   exit-address-family   !   address-family ipv6 vrf full     redistribute connected     neighbor 2000::1 remote-as 5000     neighbor 2000::1 ebgp-multihop 2     neighbor 2000::1 update-source Loopback2     neighbor 2000::1 activate   exit-address-family   !   address-family ipv4 vrf orange     network 87.1.0.0 mask 255.255.252.0     network 87.1.1.0 mask 255.255.255.0     redistribute connected     neighbor 40.1.1.1 remote-as 7000     neighbor 40.1.1.1 ebgp-multihop 2     neighbor 40.1.1.1 update-source Loopback3     neighbor 40.1.1.1 activate     neighbor 40.1.1.1 send-community extended     neighbor 40.1.1.1 route-map orange-lp in     maximum-paths eibgp 2   exit-address-family   !   address-family ipv6 vrf orange     redistribute connected     maximum-paths eibgp 2     neighbor 4000::1 remote-as 7000     neighbor 4000::1 ebgp-multihop 2 </pre>	

PE の設定	CE の設定
<pre>neighbor 4000::1 update-source Loopback3 neighbor 4000::1 activate exit-address-family ! address-family ipv4 vrf sona  redistribute connected  neighbor 160.1.1.2 remote-as 5002  neighbor 160.1.1.2 activate  neighbor 160.1.1.4 remote-as 5003  neighbor 160.1.1.4 activate exit-address-family</pre>	

## その他の参考資料

### 関連資料

関連項目	マニュアルタイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「MPLS コマンド」の項を参照してください。 <i>Command Reference (Catalyst 9300 Series Switches)</i>
Cisco Express Forwarding の設定	『 <i>Cisco Express Forwarding Configuration Guide</i> 』の「Configuring Basic Cisco Express Forwarding」モジュール
LDP の設定	『 <i>MPLS Label Distribution Protocol Configuration Guide</i> 』の「MPLS Label Distribution Protocol (LDP)」モジュール

## MPLS バーチャル プライベート ネットワークの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	MPLS バーチャル プライベート ネットワーク	MPLS バーチャル プライベート ネットワーク (VPN) は、マルチプロトコル ラベル スイッチング (MPLS) プロバイダー コア ネットワークによって相互接続された一連のサイトで構成されます。各カスタマー サイトでは、1つ以上のカスタマーエッジ (CE) デバイスが、1つ以上のプロバイダーエッジ (PE) デバイスに接続されます。
Cisco IOS XE Gibraltar 16.11.1	MPLS レイヤ 3 VPN の BGP PE-CE サポート	プロバイダーエッジ (PE) デバイスとカスタマーエッジ (CE) デバイス間のルーティングプロトコルとしての BGP のサポートが導入されました。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



## 第 2 章

# eBGP および iBGP マルチパスの設定

- MPLS-VPN における eBGP および iBGP に対する BGP マルチパス ロードシェアリング (21 ページ)
- MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロードシェアリングについて (22 ページ)
- MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロードシェアリングの設定方法 (24 ページ)
- MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロードシェアリング機能の設定例 (26 ページ)
- MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロードシェアリングの機能情報 (27 ページ)

## MPLS-VPN における eBGP および iBGP に対する BGP マルチパス ロードシェアリング

eBGP および iBGP に対する BGP マルチパス ロードシェアリング機能によって、マルチプロトコル ラベル スイッチング (MPLS) バーチャルプライベート ネットワーク (VPN) を使用するように設定されたボーダー ゲートウェイ プロトコル (BGP) ネットワークで、外部 BGP (eBGP) パスおよび内部 BGP (iBGP) パスの両方を使用してマルチパス ロード バランシングを設定できます。この機能によって、ロード バランシングの配備能力およびサービス提供能力が向上します。また、この機能は、マルチホーム ネットワークおよびスタブ ネットワークから eBGP パスおよび iBGP パスの両方をインポートするマルチホーム自律システムおよびプロバイダー エッジ (PE) ルータのために役立ちます。

## MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロードシェアリングの前提条件

Cisco Express Forwarding (CEF) または分散型 CEF (dCEF) が、参加するすべてのデバイスでイネーブルになっている必要があります。

## MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロードシェアリングの制約事項

### アドレス ファミリのサポート

この機能は、VPN ルーティング/転送 (VRF) インスタンス単位で設定されます。この機能は IPv4 および IPv6 の VRF アドレス ファミリの両方で設定できます。

### メモリ消費の制約事項

各 BGP マルチパス ルーティング テーブル エントリでは、追加のメモリを使用します。使用できるメモリが少ないデバイスや、特にフル インターネット ルーティング テーブルを送受信するデバイスでは、この機能の使用はお勧めしません。

### パス数の制限

- サポートされるパスの数は、2 つの BGP マルチパスに限定されます。iBGP マルチパス 2 つか、または iBGP マルチパス 1 つと eBGP マルチパス 1 つのいずれかです。
- 等コストルーティングのペアリングが 64 を超える一意のパスである場合、ルートは学習されず、トラフィックはドロップされます。

### サポートされていないコマンド

`ip unnumbered` コマンドは MPLS 設定ではサポートされていません。

## MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロードシェアリングについて

### eBGP と iBGP 間のマルチパス ロードシェアリング

BGP ルーティング プロセスではデフォルトで、1 つのパスをベストパスとしてルーティング 情報ベース (RIB) にインストールします。 `maximum-paths` コマンドを使用すると、マルチパス ロードシェアリングのために複数のパスを RIB にインストールするように BGP を設定できます。BGP は最良パス アルゴリズムを使用して 1 つのマルチパスを最良パスとして選択し、その最良パスを BGP ピアにアドバタイズします。



(注) 設定できるマルチパスのパス数は、`maximum-paths` コマンドリファレンスのページに記載されています。

マルチパス全体でのロードバランシングは CEF によって実行されます。CEF ロードバランシングは、パケット単位のラウンドロビンまたはセッション単位（送信元と宛先のペア）を基準として設定されます。CEF の設定の詳細については、Cisco IOS IP スイッチング コンフィギュレーションガイド [英語]、[IP スイッチング Cisco Express Forwarding コンフィギュレーションガイド \[英語\]](#) を参照してください。MPLS VPN における eBGP および iBGP に対する BGP マルチパス ロードシェアリング機能は、IPv4 VRF アドレスファミリおよび IPv6 VRF アドレスファミリ コンフィギュレーションモードで有効になります。この機能が有効にされると、VRF にインポートされた eBGP パスまたは iBGP パスあるいはその両方でロードバランシングを実行できます。マルチパスの数は VRF 単位で設定されます。別々の VRF マルチパス設定は、固有ルート識別子によって分離されます。

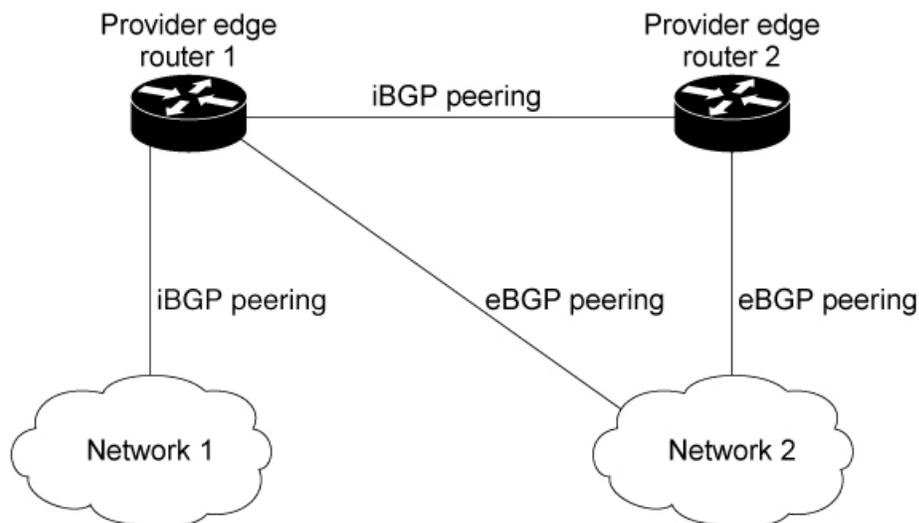


- (注) MPLS VPN における eBGP および iBGP に対する BGP マルチパス ロードシェアリング機能は、設定されたアウトバウンドルーティング ポリシーのパラメータの範囲内で動作します。

## BGP MPLS ネットワークにおける eBGP および iBGP のマルチパス ロードシェアリング

次の図に、2つのリモートネットワークを PE ルータ 1 および PE ルータ 2 に接続したサービスプロバイダー BGP MPLS ネットワークを示します。PE ルータ 1 および PE ルータ 2 には、いずれも VPNv4 ユニキャスト iBGP ピアリングが設定されています。ネットワーク 2 は、PE ルータ 1 および PE ルータ 2 に接続されているマルチホーム ネットワークです。またネットワーク 2 は、ネットワーク 1 とのエクストラネット VPN サービスが設定されています。ネットワーク 1 とネットワーク 2 は両方とも、PE ルータを使用した eBGP ピアリングが設定されています。

図 2: サービスプロバイダー BGP MPLS ネットワーク



355611

PE ルータ 1 には、MPLS VPN における eBGP および iBGP の両方に BGP マルチパス ロードシェアリング機能が設定でき、これによって、iBGP パスと eBGP パスの両方をマルチパスとして選択し、VRF にインポートできます。マルチパスは CEF によって使用され、ロードバランシングが実行されます。ネットワーク 1 からネットワーク 2 に送信される IP トラフィックでは、PE ルータ 1 が eBGP パスを使用してロードシェアリングします。これは、IP トラフィックと iBGP パスが MPLS トラフィックとして送信されるためです。



- (注)
- ローカル CE とローカル PE 間の eBGP セッションはサポートされていません。
  - ローカル PE からリモート CE への eBGP セッションはサポートされています。
  - eiBGP マルチパスは、プレフィックス単位のラベル割り当てモードでのみサポートされません。他のラベル割り当てモードではサポートされません。

## eBGP および iBGP の両方に対するマルチパス ロードシェアリングの利点

MPLS VPN における eBGP および iBGP に対する BGP マルチパス ロードシェアリング機能を使用すると、マルチホーム自律システムおよび PE ルータで、eBGP パスおよび iBGP パスの両方を經由してトラフィックを配信するように設定できます。

## MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロードシェアリングの設定方法

ここでは、次の手順について説明します。

### eBGP および iBGP の両方に対するマルチパス ロードシェアリングの設定

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure { terminal   memory   network }</b> 例：	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。

	コマンドまたはアクション	目的
	Device# <b>configure terminal</b>	
ステップ 3	<b>router bgp as-number</b> 例 : Device(config)# <b>router bgp 40000</b>	ルータ コンフィギュレーション モードを開始して、BGP ルーティング プロセスを作成または設定します。
ステップ 4	<b>neighbor {ip-address   ipv6-address   peer-group-name }</b> 例 : Device(config-router)# <b>neighbor group192</b>	直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。
ステップ 5	<b>address-family ipv4 vrfvrf-name</b> 例 : Device(config-router)# <b>address-family ipv4 vrf RED</b>	ルータをアドレス ファミリ コンフィギュレーション モードにします。  • 別々の VRF マルチパス設定は、固有ルート識別子によって分離されます。
ステップ 6	<b>address-family ipv6 vrfvrf-name</b> 例 : Device(config-router)# <b>address-family ipv6 vrf RED</b>	ルータをアドレス ファミリ コンフィギュレーション モードにします。  • 別々の VRF マルチパス設定は、固有ルート識別子によって分離されます。
ステップ 7	<b>neighbor {ip-address   ipv6-address   peer-group-name } update-source interface-type interface-name</b> 例 : Device(config-router)# <b>neighbor FE80::1234:BFF:FE0E:A471 update-source Gigabitethernet 1/0/0</b>	ピアリングが発生するリンクローカルアドレスを指定します。
ステップ 8	<b>neighbor {ip-address   ipv6-address   peer-group-name } activate</b> 例 : (config-router)# <b>neighbor group192 activate</b>	設定されたアドレス ファミリに対してネイバーまたは受信範囲ピア グループをアクティブにします。
ステップ 9	<b>maximum-paths eibgp [import-number]</b> 例 : (config-router-af)# <b>maximum-paths eibgp 2</b>	ルーティング テーブルにインストールできる平行の iBGP ルートおよび eBGP ルートの数を設定します。

## eBGP および iBGP の両方に対するマルチパス ロードシェアリングの設定の確認

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	<b>show ip bgp neighbors</b> 例： Device# <b>show ip bgp neighbors</b>	ネイバーへの TCP 接続および BGP 接続についての情報を表示します。
ステップ 3	<b>show ip bgp vpnv4 vrf vrf name</b> 例： Device# <b>show ip bgp vpnv4 vrf RED</b>	VPN アドレス情報を BGP テーブルから表示します。このコマンドは、VRF が BGP によって受信されたことを確認するために使用します。
ステップ 4	<b>show ip route vrf vrf-name</b> 例： Device# <b>show ip route vrf RED</b>	VRF インスタンスに関連する IP ルーティング テーブルを表示します。show ip route vrf コマンドは、該当する VRF がルーティング テーブルにあることを確認するために使用します。

## MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロードシェアリング機能の設定例

次に、この機能の設定方法および確認方法の例を示します。

### eBGP および iBGP のマルチパス ロードシェアリングの設定例

次の設定例では、ルータを IPv4 アドレスファミリー モードで設定して、2つの BGP ルート（eBGP または iBGP）をマルチパスとして選択します。

```
Device(config)# router bgp 40000
Device(config-router)# address-family ipv4 vrf RED
Device(config-router-af)# maximum-paths eibgp 2
Device(config-router-af)# end
```

次の設定例では、ルータを IPv6 アドレスファミリ モードで設定して、2つの BGP ルート（eBGP または iBGP）をマルチパスとして選択します。

```
Device(config)#router bgp 40000
Device(config-router)# address-family ipv6 vrf RED
Device(config-router-af)# maximum-paths eibgp 2
Device(config-router-af)# end
```

## MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロードシェアリングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1: MPLS-VPN における eBGP および iBGP の両方に対する BGP マルチパス ロードシェアリングの機能情報

機能名	リリース	機能情報
MPLS-VPN における eBGP および iBGP に対する BGP マルチパス ロードシェアリング	Cisco IOS XE Everest 16.6.1	eBGP および iBGP に対する BGP マルチパス ロードシェアリング機能によって、マルチプロトコルラベルスイッチング (MPLS) バーチャルプライベートネットワーク (VPN) を使用するように設定されたボーダーゲートウェイプロトコル (BGP) ネットワークで、外部 BGP (eBGP) パスおよび内部 BGP (iBGP) パスの両方を使用してマルチパスロードバランシングを設定できます。この機能によって、ロードバランシングの配備能力およびサービス提供能力が向上します。また、この機能は、マルチホームネットワークおよびスタブネットワークから eBGP パスおよび iBGP パスの両方をインポートするマルチホーム自律システムおよびプロバイダーエッジ (PE) ルータのために役立ちます。





## 第 3 章

# EIGRP MPLS VPN PE-CE Site of Origin の設定

- [EIGRP MPLS VPN PE-CE Site of Origin \(29 ページ\)](#)
- [EIGRP MPLS VPN PE-CE Site of Origin について \(30 ページ\)](#)
- [EIGRP MPLS VPN PE-CE Site of Origin サポートの設定方法 \(32 ページ\)](#)
- [EIGRP MPLS VPN PE-CE SoO の設定例 \(35 ページ\)](#)
- [EIGRP MPLS VPN PE-CE Site of Origin の機能履歴 \(37 ページ\)](#)

## EIGRP MPLS VPN PE-CE Site of Origin

EIGRP MPLS VPN PE-CE Site of Origin 機能によって、マルチプロトコル ラベル スイッチング (MPLS) バーチャルプライベート ネットワーク (VPN) トラフィックを、Enhanced Interior Gateway Routing Protocol (EIGRP) ネットワークに対してサイト単位でフィルタリングする機能が追加されます。Site of Origin (SoO) フィルタリングは、インターフェイス レベルで設定され、これを使用して MPLS VPN トラフィックを管理し、複雑で複合的なネットワーク トポロジにおいて過渡的なルーティンググループが発生しないようにします。この機能は、プロバイダーエッジ (PE) とカスタマーエッジ (CE) 間の EIGRP に対する MPLS VPN Support 機能をサポートするために設計されています。EIGRP MPLS VPN をサポートしている PE ルータ上にインストールされている場合、この機能によってバックドアリンクに対するサポートが提供されます。

## EIGRP MPLS VPN PE-CE Site of Origin の前提条件

このドキュメントでは、ネットワーク コア (またはサービス プロバイダー バックボーン) にボーダー ゲートウェイ プロトコル (BGP) が設定されていることを前提にしています。この機能を設定する前に、次のタスクも完了している必要があります。

- この機能は、PE と CE 間の EIGRP に対する MPLS VPN Support 機能をサポートするために導入されており、この機能は、EIGRP MPLS VPN の作成後に設定する必要があります。
- EIGRP MPLS VPN 対応に設定されているすべての PE ルータは、SoO の拡張コミュニティをサポートする Cisco IOS XE Gibraltar 16.11.1 以降のリリースを実行している必要があります。

## EIGRP MPLS VPN PE-CE Site of Origin の制約事項

- VPN サイトがパーティション化されていて、バックドア ルータ インターフェイスで SoO 拡張コミュニティ属性が設定されている場合は、このバックドアリンクを、同じサイトの他のパーティションを起点とするプレフィックスへの代替パスとして使用することはできません。
- VPN サイトごとに、一意の SoO 値を設定する必要があります。同じ VPN サイトをサポートしているすべてのプロバイダー エッジ、およびカスタマー エッジ インターフェイスには (SoO が CE ルータ上に設定されている場合)、同じ値を設定する必要があります。
- `ip unnumbered` コマンドは MPLS 設定ではサポートされていません。

## EIGRP MPLS VPN PE-CE Site of Origin について

ここでは、EIGRP MPLS VPN PE-CE Site of Origin について説明します。

### EIGRP MPLS VPN PE-CE Site of Origin サポートの概要

EIGRP MPLS VPN PE-CE Site of Origin 機能によって、EIGRP から BGP へ、および BGP から EIGRP への再配布に対するサポートが追加されます。SoO 拡張コミュニティは BGP 拡張コミュニティ属性の1つで、これを使用して、あるサイトから生じたルートを特定し、そのプレフィックスが送信元サイトへ再アドバタイズメントされないようにします。SoO 拡張コミュニティは、PE ルータがルートを学習したサイトを一意に識別します。SoO サポートには、EIGRP サイト単位で MPLS VPN トラフィックをフィルタリングする機能があります。SoO のフィルタリングはインターフェイス レベルで設定されており、これを使用して MPLS VPN トラフィックを管理し、(VPN とバックドアリンクの両方が含まれている EIGRP VPN サイトなどの) 複雑で複合的なネットワーク ポロジにおいてルーティンググループが発生しないようにします。

SoO 拡張コミュニティの設定によって、サイト単位で MPLS VPN トラフィックをフィルタリングできます。SoO 拡張コミュニティは、PE ルータ上の着信 BGP ルートマップで設定され、インターフェイスに適用されます。SoO 拡張コミュニティは、より細かくフィルタリングするために、カスタマー サイトのすべての exit ポイントに適用することができますが、VPN サービスを提供する PE ルータから CE ルータへのすべてのインターフェイスに設定する必要があります。

### バックドア リンクに対する Site of Origin のサポート

EIGRP MPLS VPN PE-CE Site of Origin (SoO) 機能によって、バックドア リンクに対するサポートが追加されます。バックドア リンクまたはルートは、リモートサイトとメインサイトとの間の VPN の外部に設定される接続で、たとえば、リモートサイトを企業ネットワークへ接続する WAN 専用線などがあります。バックドア リンクは通常、VPN リンクが停止した、または使用できなくなった場合に EIGRP のサイト間でバックアップルートとして使用されます。

VPN リンクの障害がない場合はバックドア ルータを介したルートが選択されないように、メトリックはバックドア リンク上に設定されます。

SoO 拡張コミュニティは、バックドア ルータのインターフェイス上に定義されます。これはローカル サイト ID を特定するもので、同じサイトをサポートしている PE ルータで使用される値と一致している必要があります。バックドア ルータが、バックドア リンクを介してネイバーから EIGRP アップデート（またはリプライ）を受信すると、ルータは、SoO 値のアップデートを調べます。EIGRP アップデート内の SoO 値がローカルなバックドア インターフェイスの SoO 値と一致している場合、そのルートは拒否され、EIGRP トポロジテーブルには追加されません。このシナリオは通常、受信した EIGRP アップデート内で値が設定されたローカル SoO を備えたルートが他の VPN サイトで学習され、他の VPN サイト内のバックドア ルータによって、バックドア リンクを介してアドバタイズされたときに発生します。バックドア リンクにおける SoO フィルタリングでは、ローカル サイト ID を伝送するルートが含まれている EIGRP アップデートをフィルタリングすることによって、過渡的なルーティング ループが発生しないようにします。

PE ルータ、およびカスタマーサイトのバックドア ルータでこの機能が有効になっており、PE ルータとバックドア ルータの両方で SoO 値が定義されている場合は、PE ルータおよびバックドア ルータは VPN サイト間の統合をサポートします。カスタマーサイトの他のルータでは、ルートがネイバーへ転送されるため、ルートによって伝送される SoO 値を伝搬するだけで見えます。これらのルータは、通常の拡散更新アルゴリズム（DUAL）計算以上は統合に影響を与えず、サポートもしません。

## Site of Origin 拡張コミュニティとルータとの相互運用

SoO 拡張コミュニティを設定すると、EIGRP MPLS VPN PE-CE Site of Origin 機能をサポートしているルータが、各ルートの起点となるサイトを識別できます。この機能が有効になっていると、PE または CE ルータ上の EIGRP ルーティング プロセスは、受信したそれぞれのルートを SoO 拡張コミュニティに対してチェックし、次の条件に基づいてフィルタリングします。

- BGP または CE ルータから受信したルートには、受信側インターフェイス上の SoO 値と一致する SoO 値が含まれている場合：受信側インターフェイス上に設定されている SoO 値と一致する関連 SoO 値とともにルートを受信した場合、そのルートは別の PE ルータまたはバックドアリンクから学習したルートであるため、フィルタリングされます。この動作は、ルーティング ループを回避するために設計されています。
- CE ルータから受信したルートが一致しない SoO 値で設定されている場合：あるルートが、関連付けられている SoO 値とともに受信され、その値が、受信インターフェイス上で設定されている SoO 値と一致しない場合、そのルートは、BGP へ再配布されるように EIGRP トポロジテーブルに追加されます。ルートがすでに EIGRP トポロジテーブルにインストールされているが、別の SoO 値と関連付けられている場合は、そのルートが BGP へ再配布されるときに、トポロジテーブルの SoO 値が使用されます。
- CE ルータから受信したルートに SoO 値が含まれていない場合：受信したルートに SoO 値がない場合、そのルートは EIGRP トポロジテーブルに受け入れられます。ルートが BGP へ再配布される前に、ネクストホップ CE ルータに到達するために使用されるインターフェイスの SoO 値がそのルートに付加されます。

SoO 拡張コミュニティをサポートする BGP および EIGRP ピアがこれらのルートを受信する場合には、関連付けられている SoO 値も受信します。次に、これらの値を、SoO 拡張コミュニティをサポートしている他の BGP および EIGRP ピアへ渡します。このフィルタリングは、過渡的なルートが発信元サイトから再学習されないように、つまり過渡的なルーティンググループが発生しないようにする目的で設計されています。

## Site of Origin を EIGRP に伝送する BGP VPN ルートの再配布

PE ルータ上の EIGRP ルーティングプロセスが、BGP VPN ルートを EIGRP トポロジテーブルへ再配布する場合、EIGRP は、付加された BGP 拡張コミュニティ属性から (SoO 値があれば) SoO 値を抽出し、EIGRP トポロジテーブルへ追加する前に、その SoO 値をルートへ付加します。アップデートを CE ルータへ送信する前に、EIGRP は各ルートについて SoO 値をテストします。インターフェイス上で設定されている SoO 値と一致する SoO 値に関連付けられているルートは、CE ルータに渡される前にフィルタリングされます。EIGRP ルーティングプロセスが、異なる SoO 値に関連付けられているルートを受信すると、その SoO 値は CE ルータに渡され、CE サイトを介して伝送されます。

## EIGRP MPLS VPN PE-CE Site of Origin サポート機能の利点

EIGRP MPLS VPN PE-CE Site of Origin サポート機能の設定によって、サイト単位の VPN フィルタリングが導入されます。これにより、バックドアリンクを備えた MPLS VPN、複数の PE ルータに対してデュアルホーム接続になっている CE ルータ、同じ virtual routing and forwarding (VRF) インスタンス内のさまざまなサイトから CE ルータをサポートしている PE ルータなどの複雑なトポロジに対するサポートが改善されます。

## EIGRP MPLS VPN PE-CE Site of Origin サポートの設定方法

ここでは、EIGRP MPLS VPN PE-CE Site of Origin サポートの設定方法について説明します。

### Site of Origin 拡張コミュニティの設定

SoO 拡張コミュニティの設定によって、サイト単位で MPLS VPN トラフィックをフィルタリングできます。SoO 拡張コミュニティは、PE ルータ上の着信 BGP ルートマップで設定され、インターフェイスに適用されます。SoO 拡張コミュニティは、より細かくフィルタリングするために、カスタマー サイトのすべての exit ポイントに適用することができますが、VPN サービスを提供する PE ルータから CE ルータへのすべてのインターフェイスに設定する必要があります。

#### 始める前に

- ネットワークコア (またはサービス プロバイダー バックボーン) にボーダー ゲートウェイ プロトコル (BGP) が設定されていることを確認する。
- この機能を設定する前に、EIGRP MPLS VPN を設定する。

- EIGRP MPLS VPN をサポートするよう設定されているすべての PE ルータは、SoO 拡張コミュニティをサポートしていること。
- 各 VPN サイトに対して一意の SoO 値を設定すること。各 VPN サイトでは、CE ルータに接続する PE ルータのインターフェイス上で同じ値を使用する必要があります。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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 3	<b>route-map map-name</b> <b>{permit deny} [sequence-number]</b> 例： Device(config)# <b>route-map</b> <b>Site-of-Origin permit 10</b>	ルートマップコンフィギュレーションモードを開始して、ルートマップを作成します。 <ul style="list-style-type: none"> <li>• この手順でルートマップが作成され、SoO 拡張コミュニティが適用されるようになります。</li> </ul>
ステップ 4	<b>set extcommunity</b> <b>sooextended-community-value</b> 例： Device(config-route-map)# <b>set</b> <b>extcommunity soo 100:1</b>	BGP 拡張コミュニティ属性を設定します。 <ul style="list-style-type: none"> <li>• soo キーワードには、Site of Origin 拡張コミュニティ属性を指定します。</li> <li>• extended-community-value 引数には、設定する値を指定します。この値では、次のいずれかの形式を使用できます。               <ul style="list-style-type: none"> <li>• 自律システム番号: ネットワーク番号</li> <li>• IP アドレス: ネットワーク番号</li> </ul> </li> </ul> 自律システム番号とネットワーク番号、または IP アドレスとネットワーク

	コマンドまたはアクション	目的
		番号の区切りにはコロンを使用します。
ステップ 5	<b>exit</b> 例： Device(config-route-map)# <b>exit</b>	ルートマップコンフィギュレーションモードを終了し、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 6	<b>interface type number</b> 例： Device(config)# <b>interface GigabitEthernet 1/0/1</b>	特定のインターフェイスを設定するため、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ます。
ステップ 7	<b>no switchport</b> 例： Device(config-if)# <b>no switchport</b>	インターフェイスをレイヤ 2 ポートとして動作することを停止し、シスコルーテッド (レイヤ 3) ポートにします。
ステップ 8	<b>vrf forwarding vrf-name</b> 例： Device(config-if)# <b>vrf forwarding VRF1</b>	VRF をインターフェイスまたはサブインターフェイスに関連付けます。 <ul style="list-style-type: none"><li>この手順で設定された VRF 名は、プロバイダーエッジとカスタマーエッジ間の EIGRP に対する MPLS VPN Support 機能を備えた EIGRP MPLS VPN に対して作成された VRF 名と一致している必要があります。</li></ul>
ステップ 9	<b>ip vrf sitemap route-map-name</b> 例： Device(config-if)# <b>ip vrf sitemap Site-of-Origin</b>	VRF をインターフェイスまたはサブインターフェイスに関連付けます。 <ul style="list-style-type: none"><li>この手順で設定されたルートマップ名は、手順 3 で、SoO 拡張コミュニティを適用するために作成されたルートマップ名と一致している必要があります。</li></ul>
ステップ 10	<b>ip address ip-address subnet-mask</b> 例： Device(config-if)# <b>ip address 10.0.0.1 255.255.255.255</b>	インターフェイスの IP アドレスを設定します。 <ul style="list-style-type: none"><li>IP アドレスは、VRF フォワーディングをイネーブルにした後で再設定する必要があります。</li></ul>

	コマンドまたはアクション	目的
ステップ 11	<b>end</b> 例 : Device (config-if) # <b>end</b>	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

#### 次のタスク

- バックドアルトが含まれている、複合的な EIGRP MPLS VPN ネットワークトポロジの場合は、次に、バックドアルトに対して「準最適パス」コストコミュニティを設定します。

## SoO 拡張コミュニティの設定の確認

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>show ip bgp vpnv4</b> { <b>all</b>   <b>rd</b> <i>route-distinguisher</i>   <b>vrf</b> <i>vrf-name</i> } [ <i>ip-prefixlength</i> ] 例 : Device# <b>ip bgp vpnv4 vrf SOO-1 20.2.1.1/32</b>	VPN アドレス情報を BGP テーブルから表示します。 <ul style="list-style-type: none"> <li>• <b>show ip bgp vpnv4</b> コマンドと <b>all</b> キーワードを使用して、指定したルートが、SoO 拡張コミュニティ属性で設定されていることを検証します。</li> </ul>

## EIGRP MPLS VPN PE-CE SoO の設定例

ここでは、EIGRP MPLS VPN PE-CE SoO の設定例を紹介します。

### Site of Origin 拡張コミュニティの設定例

次に、グローバル コンフィギュレーション モードで開始し、インターフェイス上で SoO 拡張コミュニティを設定する例を示します。

```
route-map Site-of-Origin permit 10
set extcommunity soo 100:1
exit
```

```
GigabitEthernet1/0/1
vrf forwarding RED
ip vrf sitemap Site-of-Origin
ip address 10.0.0.1 255.255.255.255
end
```

## Site of Origin 拡張コミュニティの確認の例

次の例では、BGP テーブルの VPN アドレス情報を表示し、SoO 拡張コミュニティの設定を確認します。

```
Device# show ip bgp vpnv4 all 10.0.0.1
  BGP routing table entry for 100:1:10.0.0.1/32, version 6
  Paths: (1 available, best #1, no table)
  Advertised to update-groups:
  1
 100 300
192.168.0.2 from 192.168.0.2 (172.16.13.13)
Origin incomplete, localpref 100, valid, external, best
Extended Community: SOO:100:1
```

カスタマー エッジ デバイス show コマンド

```
Device# show ip eigrp topo 20.2.1.1/32
EIGRP-IPv4 Topology Entry for AS(30)/ID(30.0.0.1) for 20.2.1.1/32
  State is Passive, Query origin flag is 1, 2 Successor(s), FD is 131072
  Descriptor Blocks:
 31.1.1.2 (GigabitEthernet1/0/13), from 31.1.1.2, Send flag is 0x0
  Composite metric is (131072/130816), route is External
  Vector metric:
    Minimum bandwidth is 1000000 Kbit
    Total delay is 5020 microseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
    Hop count is 2
    Originating router is 30.0.0.2
  Extended Community: SoO:100:1
  External data:
    AS number of route is 0
    External protocol is Connected, external metric is 0
    Administrator tag is 0 (0x00000000)
```

プロバイダー エッジ デバイス show コマンド

```
Device# show ip eigrp vrf SOO-1 topology 31.1.1.0/24
EIGRP-IPv4 VR(L3VPN) Topology Entry for AS(30)/ID(2.2.2.22)
  Topology(base) TID(0) VRF(SOO-1)
EIGRP-IPv4(30): Topology base(0) entry for 31.1.1.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 1310720
  Descriptor Blocks:
 1.1.1.1, from VPNv4 Sourced, Send flag is 0x0
  Composite metric is (1310720/0), route is Internal (VPNv4 Sourced)
  Vector metric:
    Minimum bandwidth is 1000000 Kbit
    Total delay is 10000000 picoseconds
    Reliability is 255/255
```

```

Load is 1/255
Minimum MTU is 1500
Hop count is 0
Originating router is 1.1.1.11
Extended Community: SoO:100:1

```

## EIGRP MPLS VPN PE-CE Site of Origin の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.6.1	EIGRP MPLS VPN PE-CE Site of Origin	EIGRP MPLS VPN PE-CE Site of Origin 機能によって、マルチプロトコルラベルスイッチング (MPLS) バーチャルプライベート ネットワーク (VPN) トラフィックを、Enhanced Interior Gateway Routing Protocol (EIGRP) ネットワークに対してサイト単位でフィルタリングする機能が追加されます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。





## 第 4 章

# Ethernet-over-MPLS (EoMPLS) および疑似回線冗長性の設定

- [Ethernet-over-MPLS の設定 \(39 ページ\)](#)
- [疑似回線冗長性の設定 \(55 ページ\)](#)
- [Ethernet-over-MPLS および疑似回線冗長性の機能情報 \(71 ページ\)](#)

## Ethernet-over-MPLS の設定

ここでは、Ethernet over Multiprotocol Label Switching (EoMPLS) の設定方法について説明します。

## Ethernet-over-MPLS の前提条件

EoMPLS を設定する前に、ネットワークが次のように設定されていることを確認してください。

- プロバイダーエッジ (PE) デバイスが IP によって相互に到達できるように、コアに IP ルーティングを設定します。
- PE デバイス間にラベルスイッチパス (LSP) が存在するように、コアに MPLS を設定します。
- 接続回線で Xconnect を設定する前に、**no switchport**、**no keepalive**、および **no ip address** コマンドを設定します。
- ロードバランシングの場合、**port-channel load-balance** コマンドの設定は必須です。
- EoMPLS VLAN モードを有効にするには、サブインターフェイスがサポートされている必要があります。
- デバイスをイネーブルにし、サービスの中断時に LDP バインディングおよび MPLS フォワーディングステートを保護するため、**mpls ldp graceful-restart** コマンドを設定する必要があります。スケール設定を使用した高可用性セットアップでの SSO 中のデバイス障害

を回避するために、（フォワーディングステートを保持しない場合でも）このコマンドを設定することを推奨します。

## Ethernet-over-MPLS の制約事項

次の項では、EoMPLS ポートモードおよび EoMPLS VLAN モードの制約事項を示します。

### Ethernet-over-MPLS ポートモードの制約事項

- イーサネット フロー ポイントはサポートされていません。
- Quality of Service (QoS) : お客様の Differentiated Services Code Point (DSCP; DiffServ コードポイント) の再マーキングは、Virtual Private Wire Service (VPWS) および EoMPLS ではサポートされません。
- 明示的 null の仮想回線接続検証 (VCCV) ping はサポートされていません。
- レイヤ 2 プロトコルトンネリング CLI はサポートされていません。
- Flow Aware Transport (FAT) 疑似回線冗長性は、プロトコル CLI モードでのみサポートされています。サポートされているロードバランシングパラメータは、送信元 IP、送信元 MAC アドレス、宛先 IP、および宛先 MAC アドレスです。
- MPLS QoS は、パイプモードと均一モードでのみサポートされています。デフォルトモードはパイプモードです。
- レガシー Xconnect モードとプロトコル CLI (インターフェイス疑似回線設定) モードはどちらもサポートされています。
- Xconnect と MACSec を同じインターフェイスに設定することはできません。
- MACSec は CE デバイスで設定し、Xconnect は PE デバイスで設定する必要があります。
- CE デバイス間で MACSec セッションを使用できる必要があります。
- デフォルトでは、EoMPLS PW は Cisco Discovery Protocol やスパニングツリープロトコル (STP) などのすべてのプロトコルをトンネリングします。EoMPLS PW は L2 プロトコル トンネリング CLI の一環として選択的なプロトコル トンネリングを実行できません。

### EoMPLS VLAN モードの制約事項

- 各 PE デバイスで同じインターワーキングタイプが設定されていない場合、仮想回線は機能しません。
- タグなしトラフィックは、着信トラフィックとしてはサポートされません。
- マルチプレクサ ユーザーネットワーク インターフェイス (MUX UNI) がサポートされていないため、レイヤ 2 サブインターフェイスでは Xconnect モードを有効にできません。

- Xconnect モードは、ポート間トランスポートのメインインターフェイスで有効になっている場合、サブインターフェイスには設定できません。
- FAT は、プロトコル CLI モードでのみ設定できます。
- VLAN モード EoMPLS では、CE デバイスによってクリアされた dot1q で暗号化されたパケットのみが PE デバイスによって処理されます。
- QoS : カスタマー DSCP 再マーキングは VPWS と EoMPLS ではサポートされていません。
- MPLS QoS は、パイプモードと均一モードでサポートされています。デフォルトモードはパイプモードです。
- VLAN モードの EoMPLS では、CE からの Cisco Discovery Protocol パケットは PE で処理されますが、EoMPLS 仮想回線では伝送されません。一方、ポートモードでは、CE からの Cisco Discovery Protocol パケットは仮想回線で伝送されます。
- イーサネットおよび VLAN インターワーキングタイプのみがサポートされています。
- L2 プロトコル トンネリング CLI はサポートされていません。

## Ethernet-over-MPLS に関する情報

EoMPLS は、Any Transport over MPLS (AToM) トランスポートタイプの 1 つです。EoMPLS は、イーサネットプロトコルデータユニット (PDU) を MPLS パケットにカプセル化し、MPLS ネットワーク上で転送することにより機能します。各 PDU は単一パケットとして転送されます。

次のモードがサポートされています。

- ポートモード : ポートのすべてのトラフィックが MPLS ネットワーク上の単一の仮想回線を共有できるようにします。ポートモードは仮想回線タイプ 5 を使用します。
- VLAN モード : MPLS ネットワーク上の単一の仮想回線を介して、送信元 802.1Q VLAN から宛先 802.1Q VLAN にイーサネットトラフィックを転送します。VLAN モードは仮想回線タイプ 5 をデフォルトとして使用します (dot1q タグは転送されません)。ただし、リモート PE がサブインターフェイスベース (VLAN ベース) の EoMPLS の仮想回線タイプ 5 をサポートしていない場合は、仮想回線タイプ 4 (dot1 タグを転送) を使用します。

EoMPLS ポートモードと EoMPLS VLAN モード間のインターワーキング : EoMPLS ポートモードがローカル PE で設定され、EoMPLS VLAN モードがリモート PE で設定されている場合、カスタマーエッジ (CE) レイヤ 2 スイッチポートインターフェイスは、ポートモード側で access として設定する必要があります。また、スパンニングツリープロトコルは、CE デバイスの VLAN モード側で無効にする必要があります。

PE 間のすべての中間リンクの最大伝送ユニット (MTU) が、入力 PE で受信される最大のレイヤ 2 パケットを伝達できる必要があります。

Cisco IOS XE Bengaluru 17.6.1 リリース以降、ポートモードの Ethernet-over-MPLS 疑似回線を介して Link Aggregation Control Protocol (LACP) および Port Aggregation Protocol (PAgP) パケットを転送できるようになります。

## Ethernet-over-MPLS の設定方法

EoMPLS は、ポートモードまたは VLAN モードで設定できます。

### Ethernet-over-MPLS ポートモードの設定

EoMPLS ポートモードは、Xconnect モードまたはプロトコル CLI 方式のいずれかを使用して設定できます。

#### Xconnect モード

Xconnect モードで EoMPLS ポートモードを設定するには、次の手順を実行します。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  Device> <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例 :  Device# <b>configure terminal</b>	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 3	<b>interface interface-id</b> 例 :  Device(config)# <b>interface TenGigabitEthernet1/0/36</b>	トランクとして設定するインターフェイスを定義し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 4	<b>no switchport</b> 例 :  Device(config-if)# <b>no switchport</b>	物理ポートに限り、レイヤ 3 モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	<b>no ip address</b> 例：  Device(config-if) # <b>no ip address</b>	物理ポートに割り当てられている IP アドレスがないことを確認します。
ステップ 6	<b>no keepalive</b> 例：  Device(config-if) # <b>no keepalive</b>	デバイスがキープアライブ メッセージを送信しないことを確認します。
ステップ 7	<b>xconnect peer-device-id vc-id encapsulation mpls</b> 例：  Device(config-if) # <b>xconnect 10.1.1.1 962 encapsulation mpls</b>	接続回線を疑似回線仮想回線 (VC) にバインドします。このコマンドの構文は、その他のレイヤ 2 トランスポートの場合と同じです。
ステップ 8	<b>end</b> 例：  Device(config-if) # <b>end</b>	インターフェイスコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

## プロトコル CLI 方式

プロトコル CLI モードで EoMPLS ポートモードを設定するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例：  Device# <b>configure terminal</b>	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。

	コマンドまたはアクション	目的
ステップ 3	<b>port-channel load-balance dst-ip</b> 例：  Device(config)# <b>port-channel load-balance dst-ip</b>	負荷分散方式を宛先 IP アドレスに設定します。
ステップ 4	<b>interface interface-id</b> 例：  Device(config)# <b>interface TenGigabitEthernet1/0/21</b>	トランクとして設定するインターフェイスを定義し、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ます。
ステップ 5	<b>no switchport</b> 例：  Device(config-if)# <b>no switchport</b>	物理ポートに限り、レイヤ 3 モードを開始します。
ステップ 6	<b>no ip address</b> 例：  Device(config-if)# <b>no ip address</b>	物理ポートに割り当てられている IP アドレスがないことを確認します。
ステップ 7	<b>no keepalive</b> 例：  Device(config-if)# <b>no keepalive</b>	デバイスがキープアライブメッセージを送信しないことを確認します。
ステップ 8	<b>exit</b> 例：  Device(config-if)# <b>exit</b>	インターフェイス コンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 9	<b>interface pseudowire number</b> 例：  Device(config)# <b>interface pseudowire 17</b>	指定した値で疑似回線インターフェイスを確立して、疑似回線コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 10	<b>encapsulation mpls</b> 例 :  Device(config-if) # <b>encapsulation mpls</b>	トンネリング カプセル化を指定します。
ステップ 11	<b>neighbor peer-ip-addr vc-id</b> 例 :  Device(config-if) # <b>neighbor 10.10.0.10 17</b>	レイヤ 2 VPN (L2VPN) 疑似回線のピア IP アドレスと仮想回線 (VC) ID を指定します。
ステップ 12	<b>l2vpn xconnect context context-name</b> 例 :  Device(config-if) # <b>l2vpn xconnect context vpws17</b>	L2VPN クロスコネク トコンテキストを作成して、Xconnect コンテキスト コンフィギュレーションモードを開始します。
ステップ 13	<b>member interface-id</b> 例 :  Device(config-if-xconn) # <b>member TenGigabitEthernet1/0/21</b>	L2VPN クロスコネク トを形成するインターフェイスを指定します。
ステップ 14	<b>member pseudowire number</b> 例 :  Device(config-if-xconn) # <b>member pseudowire 17</b>	L2VPN クロスコネク トを形成する疑似回線インターフェイスを指定します。
ステップ 15	<b>end</b> 例 :  Device(config-if-xconn) # <b>end</b>	Xconnect インターフェイス コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

## Ethernet-over-MPLS VLAN モードの設定

EoMPLS VLAN モードは、Xconnect モードまたはプロトコル CLI 方式のいずれかを使用して設定できます。

## Xconnect モード

Xconnect モードで EoMPLS VLAN モードを設定するには、次の手順を実行します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  Device# <b>configure terminal</b>	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 3	<b>interface interface-id</b> 例：  Device(config)# <b>interface TenGigabitEthernet1/0/36</b>	トランクとして設定するインターフェイスを定義し、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ます。
ステップ 4	<b>no switchport</b> 例：  Device(config-if)# <b>no switchport</b>	物理ポートに限り、レイヤ 3 モードを開始します。
ステップ 5	<b>no ip address</b> 例：  Device(config-if)# <b>no ip address</b>	物理ポートに割り当てられている IP アドレスがないことを確認します。
ステップ 6	<b>no keepalive</b> 例：  Device(config-if)# <b>no keepalive</b>	デバイスがキープアライブメッセージを送信しないことを確認します。
ステップ 7	<b>exit</b> 例：	インターフェイス コンフィギュレーションモードを終了し、グローバルコ

	コマンドまたはアクション	目的
	Device(config-if) # <b>exit</b>	ンフィギュレーションモードに戻ります。
ステップ 8	<b>interface interface-id.subinterface</b> 例 : Device(config) # <b>interface TenGigabitEthernet1/0/36.1105</b>	設定するサブインターフェイスを定義して、サブ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ます。
ステップ 9	<b>encapsulation dot1Q vlan-id</b> 例 : Device(config-subif) # <b>encapsulation dot1Q 1105</b>	サブインターフェイス上で、トラフィックの IEEE 802.1Q カプセル化をイネーブルにします。
ステップ 10	<b>xconnect peer-ip-addr vc-id encapsulation mpls</b> 例 : Device(config-subif) # <b>xconnect 10.0.0.1 1105 encapsulation mpls</b>	接続回線を疑似接続 VC にバインドします。このコマンドの構文は、その他のレイヤ 2 トランスポートの場合と同じです。
ステップ 11	<b>end</b> 例 : Device(config-subif-xconn) # <b>end</b>	特権 EXEC モードに戻ります。

## プロトコル CLI 方式

プロトコル CLI モードで EoMPLS VLAN モードを設定するには、次の手順を実行します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例 :	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。

	コマンドまたはアクション	目的
	Device# <b>configure terminal</b>	
ステップ 3	<b>port-channel load-balance dst-ip</b> 例：  Device(config)# <b>port-channel load-balance dst-ip</b>	負荷分散方式を宛先 IP アドレスに設定します。
ステップ 4	<b>interface interface-id</b> 例：  Device(config)# <b>interface TenGigabitEthernet1/0/36</b>	トランクとして設定するインターフェイスを定義し、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ます。
ステップ 5	<b>no switchport</b> 例：  Device(config-if)# <b>no switchport</b>	物理ポートに限り、レイヤ 3 モードを開始します。
ステップ 6	<b>no ip address</b> 例：  Device(config-if)# <b>no ip address</b>	物理ポートに割り当てられている IP アドレスがないことを確認します。
ステップ 7	<b>no keepalive</b> 例：  Device(config-if)# <b>no keepalive</b>	デバイスがキープアライブメッセージを送信しないことを確認します。
ステップ 8	<b>exit</b> 例：  Device(config-if)# <b>exit</b>	インターフェイス コンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 9	<b>interface interface-id.subinterface</b> 例：  Device(config)# <b>interface</b>	設定するサブインターフェイスを定義して、サブ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ます。

	コマンドまたはアクション	目的
	<code>TenGigabitEthernet1/0/36.1105</code>	
ステップ 10	<b>encapsulation dot1Q</b> <i>vlan-id</i> 例 :  Device (config-subif) # <b>encapsulation dot1Q 1105</b>	サブインターフェイス上で、トラフィックの IEEE 802.1Q カプセル化をイネーブルにします。
ステップ 11	<b>exit</b> 例 :  Device (config-subif) # <b>exit</b>	サブインターフェイス コンフィギュレーションモードを終了し、インターフェイス コンフィギュレーションモードに戻ります。
ステップ 12	<b>interface pseudowire</b> <i>number</i> 例 :  Device (config) # <b>interface pseudowire 17</b>	指定した値で疑似回線インターフェイスを確立して、疑似回線コンフィギュレーションモードを開始します。
ステップ 13	<b>encapsulation mpls</b> 例 :  Device (config-if) # <b>encapsulation mpls</b>	トンネリング カプセル化を指定します。
ステップ 14	<b>neighbor peer-ip-addr vc-id</b> 例 :  Device (config-if) # <b>neighbor 10.10.0.10 17</b>	L2VPN 疑似回線のピア IP アドレスと VC ID 値を指定します。
ステップ 15	<b>l2vpn xconnect context</b> <i>context-name</i> 例 :  Device (config-if) # <b>l2vpn xconnect context vpws17</b>	L2VPN クロスコネク トコンテキストを作成して、Xconnect コンテキストコンフィギュレーションモードを開始します。
ステップ 16	<b>member interface-id.subinterface</b> 例 :	L2VPN クロスコネク トを形成するサブインターフェイスを指定します。

	コマンドまたはアクション	目的
	<pre>Device(config-if-xconn)# member TenGigabitEthernet1/0/36.1105</pre>	
ステップ 17	<b>member pseudowire number</b> 例 : <pre>Device(config-if-xconn)# member pseudowire 17</pre>	L2VPN クロスコネクトを形成する疑似回線インターフェイスを指定します。
ステップ 18	<b>end</b> 例 : <pre>Device(config-if-xconn)# end</pre>	Xconnect コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。

## Ethernet-over-MPLS の設定例

図 3: EoMPLS トポロジ

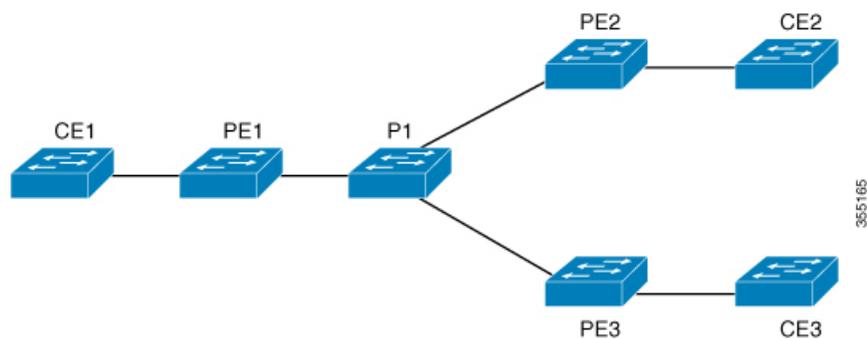


表 2: EoMPLS ポートモードの設定

PE の設定	CE の設定
<pre> mpls ip mpls label protocol ldp mpls ldp graceful-restart mpls ldp router-id loopback 1 force interface Loopback1 ip address 10.1.1.1 255.255.255.255 ip ospf 100 area 0 router ospf 100 router-id 10.1.1.1 nsf system mtu 9198 port-channel load-balance dst-ip ! interface gigabitethernet 2/0/39 no switchport no ip address no keepalive ! interface pseudowire101 encapsulation mpls neighbor 10.10.10.10 101 load-balance flow ip dst-ip load-balance flow-label both l2vpn xconnect context pw101 member pseudowire101 member gigabitethernet 2/0/39 ! interface tengigabitethernet 3/0/10 switchport trunk allowed vlan 142 switchport mode trunk channel-group 42 mode active ! interface Port-channel42 switchport trunk allowed vlan 142 switchport mode trunk ! interface Vlan142 ip address 10.11.11.11 255.255.255.0  ip ospf 100 area 0 mpls ip mpls label protocol ldp ! </pre>	<pre> interface gigabitethernet 1/0/33 switchport trunk allowed vlan 912 switchport mode trunk spanning-tree portfast trunk ! interface Vlan912 ip address 10.91.2.3 255.255.255.0 ! </pre>

表 3: EoMPLS VLAN モードの設定

PE の設定	CE の設定
<pre>interface tengigabitethernet 1/0/36 no switchport no ip address no keepalive exit ! interface tengigabitethernet 1/0/36.1105 encapsulation dot1Q 1105 exit ! interface pseudowire1105 encapsulation mpls neighbor 10.10.0.10 1105 exit ! l2vpn xconnect context vme1105 member tengigabitethernet 1/0/36.1105 member pseudowire1105 end !</pre>	<pre>interface fortygigabitethernet 1/9 switchport switchport mode trunk switchport trunk allowed vlan 1105  mtu 9216 end !</pre>

表 4: EoMPLS ポートモードと EoMPLS VLAN モードの設定間のインターワーキング

PE の設定 : ポートモード	CE の設定 : ポートモード
<pre>interface tengigabitethernet 1/0/37 no switchport no ip address no keepalive exit ! interface pseudowire1105 encapsulation mpls neighbor 10.11.11.11 1105 exit ! l2vpn xconnect context vme1105 member tengigabitethernet 1/0/37 member pseudowire1105 end !</pre>	<pre>interface fortygigabitethernet1/10 switchport switchport mode access switchport access vlan 1105 end  no spanning-tree vlan 1105 !</pre>

PE の設定 : VLAN モード	CE の設定 : VLAN モード
<pre>interface tengigabitethernet 1/0/36 no switchport no ip address no keepalive exit ! interface tengigabitethernet 1/0/36.1105  encapsulation dot1Q 1105 exit ! interface pseudowire1105 encapsulation mpls neighbor 10.10.0.10 1105 exit ! l2vpn xconnect context vm1105 member tengigabitethernet 1/0/36.1105 member pseudowire1105 end !</pre>	<pre>interface fortygigabitethernet 1/9 switchport switchport mode trunk switchport trunk allowed vlan 1105  mtu 9216 end  no spanning-tree vlan 1105 !</pre>

EoMPLS ポートモードと EoMPLS VLAN モード間のインターワーキングのもう 1 つのシナリオは、両方の CE デバイスで次のコマンドを設定することです。

- **switchport mode trunk**
- **switchport trunk allowed vlan *vlan-id***
- **spanning-tree vlan *vlan-id***

送信されたトラフィックが二重 VLAN タグ付きでない場合、データトラフィックは両方の CE デバイスで STP を無効化することで流れます。

次に、**show mpls l2 vc vcid *vc-id* detail** コマンドの出力例を示します。

```
Device# show mpls l2 vc vcid 1105 detail
Local interface: TenGigabitEthernet1/0/36.1105 up, line protocol up, Eth VLAN 1105 up
Interworking type is Ethernet
Destination address: 10.0.0.1, VC ID: 1105, VC status: up
Output interface: Po10, imposed label stack {33 10041}
Preferred path: not configured
Default path: active
Next hop: 10.10.0.1
Create time: 00:04:09, last status change time: 00:02:13
Last label FSM state change time: 00:02:12
Signaling protocol: LDP, peer 10.0.0.1:0 up
Targeted Hello: 10.0.0.10(LDP Id) -> 10.0.0.1, LDP is UP
Graceful restart: configured and enabled
Non stop routing: not configured and not enabled
Status TLV support (local/remote) : enabled/supported
LDP route watch : enabled
Label/status state machine : established, LruRru
Last local dataplane status rcvd: No fault
Last BFD dataplane status rcvd: Not sent
Last BFD peer monitor status rcvd: No fault
Last local AC circuit status rcvd: No fault
Last local AC circuit status sent: No fault
```

```

Last local PW i/f circ status rcvd: No fault
Last local LDP TLV      status sent: No fault
Last remote LDP TLV    status rcvd: No fault
Last remote LDP ADJ    status rcvd: No fault
MPLS VC labels: local 124, remote 10041
Group ID: local 336, remote 352
MTU: local 9198, remote 9198
Remote interface description:
MAC Withdraw: sent:1, received:0
Sequencing: receive disabled, send disabled
Control Word: On (configured: autosense)
SSO Descriptor: 10.0.0.1/1105, local label: 124
Dataplane:
  SSM segment/switch IDs: 9465983/446574 (used), PWID: 109
VC statistics:
  transit packet totals: receive 0, send 0
  transit byte totals:   receive 0, send 0
  transit packet drops:  receive 0, seq error 0, send 0

```

次に、**show l2vpn atom vc vcid vc-id detail** コマンドの出力例を示します。

```

Device# show l2vpn atom vc vcid 1105 detail
pseudowire100109 is up, VC status is up PW type: Ethernet
Create time: 00:04:17, last status change time: 00:02:22
Last label FSM state change time: 00:02:20
Destination address: 10.0.0.1 VC ID: 1105
Output interface: Po10, imposed label stack {33 10041}
Preferred path: not configured
Default path: active
Next hop: 10.10.0.1
Member of xconnect service TenGigabitEthernet1/0/36.1105-1105, group right
Associated member TenGigabitEthernet1/0/36.1105 is up, status is up
Interworking type is Ethernet
Service id: 0x1f000037
Signaling protocol: LDP, peer 10.0.0.1:0 up
Targeted Hello: 10.0.0.10(LDP Id) -> 10.0.0.1, LDP is UP
Graceful restart: configured and enabled
Non stop routing: not configured and not enabled
PWid FEC (128), VC ID: 1105
Status TLV support (local/remote)      : enabled/supported
  LDP route watch                       : enabled
  Label/status state machine            : established, LruRru
  Local dataplane status received       : No fault
  BFD dataplane status received        : Not sent
  BFD peer monitor status received      : No fault
  Status received from access circuit   : No fault
  Status sent to access circuit         : No fault
  Status received from pseudowire i/f   : No fault
  Status sent to network peer          : No fault
  Status received from network peer     : No fault
  Adjacency status of remote peer      : No fault
Sequencing: receive disabled, send disabled
Bindings
Parameter      Local                               Remote
-----
Label          124                                       10041
Group ID       336                                       352
Interface
MTU            9198                                       9198
Control word on (configured: autosense)  on
PW type        Ethernet                               Ethernet
VCCV CV type   0x02                                       0x02
               LSPV [2]                               LSPV [2]
VCCV CC type   0x06                                       0x06

```

```

RA [2], TTL [3]
Status TLV enabled RA [2], TTL [3] supported
SSO Descriptor: 10.0.0.1/1105, local label: 124
Dataplane:
SSM segment/switch IDs: 9465983/446574 (used), PWID: 109
Rx Counters
0 input transit packets, 0 bytes
0 drops, 0 seq err
0 MAC withdraw
Tx Counters
0 output transit packets, 0 bytes
0 drops
1 MAC withdraw

```

次に、**show mpls forwarding-table** コマンドの出力例を示します。

```

Device# show mpls forwarding-table 10.0.0.1

```

Local Label	Outgoing Label	Prefix or Tunnel Id	Bytes Switched	Outgoing interface	Next Hop
2049	33	10.0.0.1/32	38540	Hu2/0/30/2.1	10.0.0.2
	33	10.0.0.1/32	112236	Hu2/0/30/2.2	10.0.0.6
	33	10.0.0.1/32	46188	Hu2/0/30/2.3	10.0.0.8

## 疑似回線冗長性の設定

ここでは、疑似回線の冗長性を設定する方法について説明します。

### 疑似回線冗長性の前提条件

- 接続回線で Xconnect モードを設定する前に、**no switchport**、**no keepalive**、および **no ip address** コマンドを設定します。
- ロードバランシングの場合、**port-channel load-balance** コマンドを設定します。
- 疑似回線冗長性 VLAN モードを有効にするには、サブインターフェイスがサポートされている必要があります。

### 疑似回線冗長性の制約事項

ここでは、疑似回線冗長性ポートモードおよび疑似回線冗長性 VLAN モードの制約事項について説明します。

#### 疑似回線冗長性ポートモードの制約事項

- Ethernet Flow Point (EFP) および Internet Group Management Protocol (IGMP) スヌーピングはサポートされません。
- コアネットワークでの ECMP ロードバランシングのフローラベルは、カスタマーの送信元 IP、宛先 IP、送信元 MAC、および宛先 MAC に基づきます。

- MPLS QoS は、パイプおよび均一モードでサポートされています。デフォルトモードはパイプモードです。
- QoS : カスタマー DSCP 再マーキングは VPWS と EoMPLS ではサポートされていません。
- 明示的 null の VCCV ping はサポートされていません。
- **ip unnumbered** コマンドは MPLS 設定ではサポートされていません。
- 複数のバックアップ疑似回線はサポートされていません。
- PW 冗長グループのスイッチオーバーはサポートされていません。

## 疑似回線冗長性 VLAN モードの制約事項

- 各 PE デバイスで同じインターワーキングタイプが設定されていない場合、仮想回線は機能しません。
- タグなしトラフィックは、着信トラフィックとしてはサポートされません。
- マルチプレクサ ユーザーネットワーク インターフェイス (MUX UNI) がサポートされていないため、レイヤ 2 サブインターフェイスでは Xconnect モードを有効にできません。
- Xconnect モードは、ポート間トランスポートのメインインターフェイスで有効になっている場合、サブインターフェイスには設定できません。
- Flow Aware Transport (FAT) は、プロトコル CLI モードでのみ設定できます。
- MACsec は、疑似回線冗長性 VLAN モードではサポートされません。
- QoS : カスタマー DSCP 再マーキングは VPWS と疑似回線冗長性ではサポートされていません。
- MPLS QoS は、パイプモードと均一モードでのみサポートされています。デフォルトモードはパイプモードです。
- VLAN モードの類似回線冗長性では、CE からの Cisco Discovery Protocol パケットは PE で処理されますが、類似回線冗長性の仮想回線では伝送されません。一方、ポートモードでは、CE からの Cisco Discovery Protocol パケットは仮想回線で伝送されます。
- イーサネットおよび VLAN インターワーキングタイプのみがサポートされています。
- L2 プロトコル トンネリング CLI はサポートされていません。

## 疑似回線冗長性について

L2VPN 疑似回線冗長性機能を使用すると、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 デバイスで発生した障害、または PE デバイスと CE デバイス間のリンクで発生した障害から回復できます。

PE 間のすべての中間リンクの最大伝送ユニット (MTU) が、入力 PE で受信される最大のレイヤ 2 パケットを伝達できる必要があります。

疑似回線冗長性は、Xconnect とプロトコル CLI 方式の両方を使用して設定できます。

## 疑似回線冗長性の設定方法

疑似回線冗長性は、ポートモードまたは VLAN モードで設定できます。

### 疑似回線冗長性ポートモードの設定

疑似回線冗長性ポートモードは、Xconnect モードまたはプロトコル CLI 方式のいずれかを使用して設定できます。

#### Xconnect モード

Xconnect モードで疑似回線冗長性ポートモードを設定するには、次の手順を実行します。



(注) ロードバランスを有効にするには、「Ethernet-over-MPLSの設定方法」セクションの Xconnect モードの手順から該当する **load-balance** コマンドを使用します。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例 : Device# <b>configure terminal</b>	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 3	<b>interface interface-id</b> 例 : Device(config)# <b>interface GigabitEthernet1/0/44</b>	トランクとして設定するインターフェイスを定義し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 4	<b>no switchport</b> 例 :	物理ポートに限り、レイヤ 3 モードを開始します。

	コマンドまたはアクション	目的
	Device(config-if)# <b>no switchport</b>	
ステップ 5	<b>no ip address</b> 例： Device(config-if)# <b>no ip address</b>	物理ポートに割り当てられている IP アドレスがないことを確認します。
ステップ 6	<b>no keepalive</b> 例： Device(config-if)# <b>no keepalive</b>	デバイスがキープアライブメッセージを送信しないことを確認します。
ステップ 7	<b>xconnect peer-device-id vc-id encapsulation mpls</b> 例： Device(config-if)# <b>xconnect 10.1.1.1 117 encapsulation mpls</b>	接続回線を疑似接続 VC にバインドします。このコマンドの構文は、その他のレイヤ 2 トランスポートの場合と同じです。
ステップ 8	<b>backup peer peer-router-ip-addr vcid vc-id [ priority value ]</b> 例： Device(config-if)# <b>backup peer 10.11.11.11 118 priority 9</b>	疑似回線 VC の冗長ピアを指定します。
ステップ 9	<b>end</b> 例： Device(config)# <b>end</b>	インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

## プロトコル CLI 方式

プロトコル CLI モードで疑似回線冗長性ポートモードを設定するには、次の手順を実行します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  Device# <b>configure terminal</b>	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 3	<b>port-channel load-balance dst-ip</b> 例：  Device(config)# <b>port-channel load-balance dst-ip</b>	負荷分散方式を宛先 IP アドレスに設定します。
ステップ 4	<b>interface interface-id</b> 例：  Device(config)# <b>interface TenGigabitEthernet1/0/36</b>	トランクとして設定するインターフェイスを定義し、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ます。
ステップ 5	<b>no switchport</b> 例：  Device(config-if)# <b>no switchport</b>	物理ポートに限り、レイヤ 3 モードを開始します。
ステップ 6	<b>no ip address</b> 例：  Device(config-if)# <b>no ip address</b>	物理ポートに割り当てられている IP アドレスがないことを確認します。
ステップ 7	<b>no keepalive</b> 例：  Device(config-if)# <b>no keepalive</b>	デバイスがキープアライブメッセージを送信しないことを確認します。

	コマンドまたはアクション	目的
ステップ 8	<b>exit</b> 例 :  Device(config-if) # <b>exit</b>	インターフェイス コンフィギュレーション モードを終了します。
ステップ 9	<b>interface pseudowire number-active</b> 例 :  Device(config) # <b>interface pseudowire 17</b>	指定した値でアクティブ状態の疑似回線インターフェイスを確立して、疑似回線コンフィギュレーションモードを開始します。
ステップ 10	<b>encapsulation mpls</b> 例 :  Device(config-if) # <b>encapsulation mpls</b>	トンネリング カプセル化を指定します。
ステップ 11	<b>neighbor active-peer-ip-addr vc-id</b> 例 :  Device(config-if) # <b>neighbor 10.10.0.10 17</b>	L2VPN 疑似回線のアクティブ状態のピア IP アドレスと VC ID 値を指定します。
ステップ 12	<b>exit</b> 例 :  Device(config-if) # <b>exit</b>	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 13	<b>interface pseudowire number-standby</b> 例 :  Device(config) # <b>interface pseudowire 18</b>	指定した値でスタンバイ状態の疑似回線インターフェイスを確立して、疑似回線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	<b>encapsulation mpls</b> 例 :  Device(config-if) # <b>encapsulation mpls</b>	トンネリング カプセル化を指定します。

	コマンドまたはアクション	目的
ステップ 15	<b>neighbor standby-peer-ip-addr vc-id</b> 例 : Device(config-if)# <b>neighbor 10.10.0.11 18</b>	L2VPN 疑似回線のスタンバイ状態のピア IP アドレスと VC ID 値を指定します。
ステップ 16	<b>l2vpn xconnect context context-name</b> 例 : Device(config-if)# <b>l2vpn xconnect context vpws17</b>	L2VPN クロスコネクトコンテキストを作成し、VLAN モードの EoMPLS 接続回線をアクティブ状態およびスタンバイ状態の疑似回線インターフェイスに接続します。
ステップ 17	<b>member interface-id</b> 例 : Device(config-if-xconn)# <b>member TenGigabitEthernet1/0/36</b>	L2VPN クロスコネクトを形成するインターフェイスを指定します。
ステップ 18	<b>member pseudowire number-active group group-name [priority value]</b> 例 : Device(config-if-xconn)# <b>member pseudowire 17 group pwr10</b>	L2VPN クロスコネクトを形成するアクティブ状態の疑似回線インターフェイスを指定します。
ステップ 19	<b>member pseudowire number-standby group group-name [priority value]</b> 例 : Device(config-if-xconn)# <b>member pseudowire 18 group pwr10 priority 6</b>	L2VPN クロスコネクトを形成するスタンバイ状態の疑似回線インターフェイスを指定します。
ステップ 20	<b>end</b> 例 : Device(config-if-xconn)# <b>end</b>	Xconnect コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。

## 疑似回線冗長性 VLAN モードの設定

疑似回線冗長性 VLAN モードは、Xconnect モードまたはプロトコル CLI 方式のいずれかを使用して設定できます。

### Xconnect モード

Xconnect モードで疑似回線冗長性 VLAN モードを設定するには、次の手順を実行します。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  Device# <b>configure terminal</b>	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 3	<b>interface interface-id</b> 例：  Device(config)# <b>interface TenGigabitEthernet1/0/36</b>	トランクとして設定するインターフェイスを定義し、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ます。
ステップ 4	<b>no switchport</b> 例：  Device(config-if)# <b>no switchport</b>	物理ポートに限り、レイヤ 3 モードを開始します。
ステップ 5	<b>no ip address</b> 例：  Device(config-if)# <b>no ip address</b>	物理ポートに割り当てられている IP アドレスがないことを確認します。
ステップ 6	<b>no keepalive</b> 例：  Device(config-if)# <b>no keepalive</b>	デバイスがキープアライブメッセージを送信しないことを確認します。

	コマンドまたはアクション	目的
ステップ 7	<b>exit</b> 例 : Device (config-if) # <b>exit</b>	インターフェイス コンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 8	<b>interface interface-id.subinterface</b> 例 : Device (config) # <b>interface TenGigabitEthernet1/0/36.1105</b>	設定するサブインターフェイスを定義して、サブ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ます。
ステップ 9	<b>encapsulation dot1Q vlan-id</b> 例 : Device (config-subif) # <b>encapsulation dot1Q 1105</b>	サブインターフェイス上で、トラフィックの IEEE 802.1Q カプセル化をイネーブルにします。
ステップ 10	<b>xconnect peer-ip-addr vc-id encapsulation mpls</b> 例 : Device (config-subif) # <b>xconnect 10.0.0.1 1105 encapsulation mpls</b>	接続回線を疑似接続 VC にバインドします。このコマンドの構文は、その他のレイヤ 2 トランスポートの場合と同じです。
ステップ 11	<b>backup peer peer-ip-addr vc-id [priority value]</b> 例 : Device (config-subif-xconn) # <b>backup peer 10.10.10.10 1105 priority 8</b>	疑似回線 VC の冗長ピアを指定します。
ステップ 12	<b>end</b> 例 : Device (config-subif-xconn) # <b>end</b>	Xconnect コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。

## プロトコル CLI 方式

プロトコル CLI モードで疑似回線冗長性 VLAN モードを設定するには、次の手順を実行します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  Device# <b>configure terminal</b>	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 3	<b>port-channel load-balance dst-ip</b> 例：  Device(config)# <b>port-channel load-balance dst-ip</b>	負荷分散方式を宛先 IP アドレスに設定します。
ステップ 4	<b>interface interface-id</b> 例：  Device(config)# <b>interface TenGigabitEthernet1/0/36</b>	トランクとして設定するインターフェイスを定義し、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ます。
ステップ 5	<b>no switchport</b> 例：  Device(config-if)# <b>no switchport</b>	物理ポートに限り、レイヤ 3 モードを開始します。
ステップ 6	<b>no ip address</b> 例：  Device(config-if)# <b>no ip address</b>	物理ポートに割り当てられている IP アドレスがないことを確認します。

	コマンドまたはアクション	目的
ステップ 7	<b>no keepalive</b> 例 :  Device (config-if) # <b>no keepalive</b>	デバイスがキープアライブメッセージを送信しないことを確認します。
ステップ 8	<b>exit</b> 例 :  Device (config-if) # <b>exit</b>	インターフェイス コンフィギュレーション モードを終了します。
ステップ 9	<b>interface interface-id.subinterface</b> 例 :  Device (config) # <b>interface TenGigabitEthernet1/0/36.1105</b>	設定するサブインターフェイスを定義して、サブ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ます。
ステップ 10	<b>encapsulation dot1Q vlan-id</b> 例 :  Device (config-subif) # <b>encapsulation dot1Q 1105</b>	サブインターフェイス上で、トラフィックの IEEE 802.1Q カプセル化をイネーブルにします。
ステップ 11	<b>exit</b> 例 :  Device (config-subif) # <b>exit</b>	サブインターフェイス コンフィギュレーションモードを終了します。
ステップ 12	<b>interface pseudowire number-active</b> 例 :  Device (config) # <b>interface pseudowire 17</b>	指定した値でアクティブ状態の疑似回線インターフェイスを確立して、疑似回線コンフィギュレーションモードを開始します。
ステップ 13	<b>encapsulation mpls</b> 例 :  Device (config-if) # <b>encapsulation mpls</b>	トンネリング カプセル化を指定します。

	コマンドまたはアクション	目的
ステップ 14	<b>neighbor active-peer-ip-addr vc-id</b> 例 :  Device(config-if) # <b>neighbor 10.10.0.10 17</b>	レイヤ 2 VPN (L2VPN) 疑似回線のアクティブなピア IP アドレスと仮想回線 (VC) ID を指定します。
ステップ 15	<b>exit</b> 例 :  Device(config-if) # <b>exit</b>	インターフェイス設定モードを終了します。
ステップ 16	<b>interface pseudowire number-standby</b> 例 :  Device(config) # <b>interface pseudowire 18</b>	指定した値でスタンバイ状態の疑似回線インターフェイスを確立して、疑似回線コンフィギュレーションモードを開始します。
ステップ 17	<b>encapsulation mpls</b> 例 :  Device(config-if) # <b>encapsulation mpls</b>	トンネリング カプセル化を指定します。
ステップ 18	<b>neighbor standby-peer-ip-addr vc-id</b> 例 :  Device(config-if) # <b>neighbor 10.10.0.11 18</b>	L2VPN 疑似回線のスタンバイ状態のピア IP アドレスと VC ID 値を指定します。
ステップ 19	<b>l2vpn xconnect context context-name</b> 例 :  Device(config-if) # <b>l2vpn xconnect context vpws17</b>	L2VPN クロスコネクトコンテキストを作成し、VLAN モードの EoMPLS 接続回線をアクティブ状態およびスタンバイ状態の疑似回線インターフェイスに接続します。
ステップ 20	<b>member interface-id.subinterface</b> 例 :	L2VPN クロスコネクトを形成するインターフェイスを指定します。

	コマンドまたはアクション	目的
	Device(config-if-xconn)# <b>member TenGigabitEthernet1/0/36.1105</b>	
ステップ 21	<b>member pseudowire number-active group group-name [priority value]</b> 例 :  Device(config-if-xconn)# <b>member pseudowire 17 group pwr10</b>	L2VPN クロスコネクトを形成するアクティブ状態の疑似回線インターフェイスを指定します。
ステップ 22	<b>member pseudowire number-standby group group-name [priority value]</b> 例 :  Device(config-if-xconn)# <b>member pseudowire 18 group pwr10 priority 6</b>	L2VPN クロスコネクトを形成するスタンバイ状態の疑似回線インターフェイスを指定します。
ステップ 23	<b>end</b> 例 :  Device(config-if-xconn)# <b>end</b>	Xconnect コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。

## 疑似回線冗長性の設定例

表 5: 疑似回線冗長性ポートモードの設定

PE の設定	CE の設定
<pre> mpls ip mpls label protocol ldp mpls ldp graceful-restart mpls ldp router-id loopback 1 force ! interface Loopback1 ip address 10.1.1.1 255.255.255.255 ip ospf 100 area 0 router ospf 100 router-id 10.1.1.1 nsf ! interface gigabitethernet 2/0/39 no switchport no ip address no keepalive ! interface pseudowire101 encapsulation mpls neighbor 10.10.10.10 101 ! interface pseudowire102 encapsulation mpls neighbor 10.10.10.11 101 l2vpn xconnect context pw101 member pseudowire101 group pwgrp1 priority 1 member pseudowire102 group pwgrp1 priority 15  member GigabitEthernet2/0/39 ! interface tengigabitethernet 3/0/10 switchport trunk allowed vlan 142 switchport mode trunk channel-group 42 mode active ! interface Port-channel42 switchport trunk allowed vlan 142 switchport mode trunk ! interface Vlan142 ip address 10.11.11.11 255.255.255.0 ip ospf 100 area 0 mpls ip mpls label protocol ldp ! </pre>	<pre> interface gigabitethernet 1/0/33 switchport trunk allowed vlan 912 switchport mode trunk spanning-tree portfast trunk ! interface Vlan912 ip address 10.91.2.3 255.255.255.0 ! </pre>

表 6: 疑似回線冗長 VLAN モードの設定

PE の設定	CE の設定
<pre> interface tengigabitethernet 1/0/36   no switchport   no ip address   no keepalive exit ! interface tengigabitethernet 1/0/36.1105   encapsulation dot1Q 1105   exit ! interface pseudowire1105   encapsulation mpls   neighbor 10.10.0.10 1105 exit ! interface pseudowire1106   encapsulation mpls   neighbor 10.10.0.11 1106 ! l2vpn xconnect context vme1105   member tengigabitethernet 1/0/36.1105   member pseudowire1105 group pwr10   member pseudowire1106 group pwr10 priority 6 end ! </pre>	<pre> interface fortygigabitethernet 1/9   switchport   switchport mode trunk   switchport trunk allowed vlan 1105    mtu 9216 end ! </pre>

次に、**show mpls l2 vc vcid vc-id detail** コマンドの出力例を示します。

```

Device# show mpls l2 vc vcid 1105 detail
Local interface: TenGigabitEthernet1/0/36.1105 up, line protocol up, Eth VLAN 1105 up
  Interworking type is Ethernet
  Destination address: 10.11.11.11, VC ID: 1105, VC status: standby
    Output interface: Po10, imposed label stack {1616}
    Preferred path: not configured
    Default path: active
    Next hop: 10.10.0.1
  Create time: 00:04:09, last status change time: 00:02:13
  Last label FSM state change time: 00:02:15
  Signaling protocol: LDP, peer 10.11.11.11:0 up
  Targeted Hello: 10.10.0.10(LDP Id) -> 10.11.11.11, LDP is UP
  Graceful restart: configured and enabled
  Non stop routing: not configured and not enabled
  Status TLV support (local/remote)   : enabled/supported
    LDP route watch                   : enabled
    Label/status state machine        : established, LrdRru
    Last local dataplane status rcvd: No fault
    Last BFD dataplane status rcvd: Not sent
    Last BFD peer monitor status rcvd: No fault
    Last local AC circuit status rcvd: DOWN(standby)
    Last local AC circuit status sent: No fault
    Last local PW i/f circ status rcvd: No fault
    Last local LDP TLV status sent: DOWN(standby)
    Last remote LDP TLV status rcvd: No fault
    Last remote LDP ADJ status rcvd: No fault
  MPLS VC labels: local 125, remote 1616
  Group ID: local 336, remote 0

```

```

MTU: local 9198, remote 9198
Remote interface description:
MAC Withdraw: sent:1, received:0
Sequencing: receive disabled, send disabled
Control Word: On (configured: autosense)
SSO Descriptor: 10.11.11.11/1105, local label: 125
Dataplane:
  SSM segment/switch IDs: 96143/450671 (used), PWID: 110
VC statistics:
  transit packet totals: receive 0, send 0
  transit byte totals:  receive 0, send 0
  transit packet drops:  receive 0, seq error 0, send 0

```

次に、**show l2vpn atom vc vcid vc-id detail** コマンドの出力例を示します。

```

Device# show l2vpn atom vc vcid 1105 detail
pseudowire100110 is up, VC status is standby PW type: Ethernet
  Create time: 00:04:17, last status change time: 00:02:22
  Last label FSM state change time: 00:02:24
  Destination address: 10.11.11.11 VC ID: 1105
  Output interface: Po10, imposed label stack {1616}
  Preferred path: not configured
  Default path: active
  Next hop: 10.0.0.1
Member of xconnect service TenGigabitEthernet1/0/36.1105-1105, group right
  Associated member TenGigabitEthernet1/0/36.1105 is up, status is up
  Interworking type is Ethernet
  Service id: 0x1f000037
Signaling protocol: LDP, peer 10.11.11.11:0 up
  Targeted Hello: 10.0.0.10(LDP Id) -> 10.11.11.11, LDP is UP
  Graceful restart: configured and enabled
  Non stop routing: not configured and not enabled
  PWid FEC (128), VC ID: 1105
  Status TLV support (local/remote)           : enabled/supported
    LDP route watch                           : enabled
    Label/status state machine                 : established, LrdRru
    Local dataplane status received           : No fault
    BFD dataplane status received             : Not sent
    BFD peer monitor status received          : No fault
    Status received from access circuit       : DOWN(standby)
    Status sent to access circuit             : No fault
    Status received from pseudowire i/f       : No fault
    Status sent to network peer               : DOWN(standby)
    Status received from network peer         : No fault
    Adjacency status of remote peer          : No fault
Sequencing: receive disabled, send disabled
Bindings
  Parameter      Local      Remote
  -----
  Label          125          1616
  Group ID       336          0
  Interface
  MTU            9198         9198
  Control word on (configured: autosense)    on
  PW type        Ethernet
  VCCV CV type  0x02         0x02
                LSPV [2]
                LSPV [2]
  VCCV CC type  0x06         0x02
                RA [2], TTL [3]
                RA [2]
  Status TLV     enabled      supported
SSO Descriptor: 10.11.11.11/1105, local label: 125
Dataplane:
  SSM segment/switch IDs: 96143/450671 (used), PWID: 110
Rx Counters

```

```

0 input transit packets, 0 bytes
0 drops, 0 seq err
0 MAC withdraw
Tx Counters
0 output transit packets, 0 bytes
0 drops
1 MAC withdraw

```

次に、`show mpls l2transport vc vc-id` コマンドの出力例を示します。

```
Device# show mpls l2transport vc 101
```

Local intf	Local circuit	Dest address	VC ID	Status
TenGigabitEthernet1/0/36.1105	Eth VLAN 1105	10.0.0.1	1105	UP
TenGigabitEthernet1/0/36.1105	Eth VLAN 1105	10.11.11.11	1105	STANDBY

## Ethernet-over-MPLS および疑似回線冗長性の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレーンで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 7: Ethernet-over-MPLS および疑似回線冗長性の機能情報

機能名	リリース	機能情報
Ethernet-over-MPLS および疑似回線冗長性	Cisco IOS XE Everest 16.6.1	この機能が導入されました。 ポートモードのサポートが導入されました。
Ethernet over MPLS および疑似回線冗長性	Cisco IOS XE Gibraltar 16.12.1	VLAN モードのサポートが導入されました。
Macsec over EoMPLS	Cisco IOS XE Amsterdam 17.1.1	VLAN モード EoMPLS の場合、CE デバイスで <code>macsec dot1q-in-clear 1</code> コマンドによって設定されたパケットのみが PE デバイスで処理されます。
Ethernet over MPLS 疑似回線を介した LACP および PAgP パケット転送	Cisco IOS XE Gibraltar 17.6.1	ポートモードの Ethernet-over-MPLS 疑似回線を介して Link Aggregation Control Protocol (LACP) および Port Aggregation Protocol (PAgP) パケットを転送できるようになりました。





## 第 5 章

# MPLS を介した IPv6 プロバイダー エッジ (6PE) の設定

- [6PE の前提条件 \(73 ページ\)](#)
- [6PE の制約事項 \(73 ページ\)](#)
- [6PE について \(73 ページ\)](#)
- [6PE の IPV6 明示的ヌルラベル \(74 ページ\)](#)
- [6PE の設定 \(75 ページ\)](#)
- [6PE の IPV6 明示的ヌルラベルの設定 \(77 ページ\)](#)
- [6PE の設定例 \(79 ページ\)](#)
- [6PE の IPV6 明示的ヌルラベルの設定例 \(81 ページ\)](#)
- [MPLS を介した IPv6 プロバイダーエッジ \(6PE\) の機能履歴 \(82 ページ\)](#)

## 6PE の前提条件

PE-CE IGP IPv6 ルートをコア BGP に再配布し、また、コア BGP を PE-CE IGP IPv6 ルートに再配布します。

## 6PE の制約事項

eBGP は CE-PE としてサポートされていません。スタティック ルート、OSPFv3、ISIS、RIPv2 は CE-PE としてサポートされています。

## 6PE について

6PE は、IPv4 MPLS を介してグローバル IPv6 到達可能性を提供する技術です。これにより、他のすべてのデバイスに対して 1 つの共有ルーティング テーブルを使用できるようになります。6PE を使用することで、IPv6 ドメインは IPv4 を介して相互に通信できるようになります。

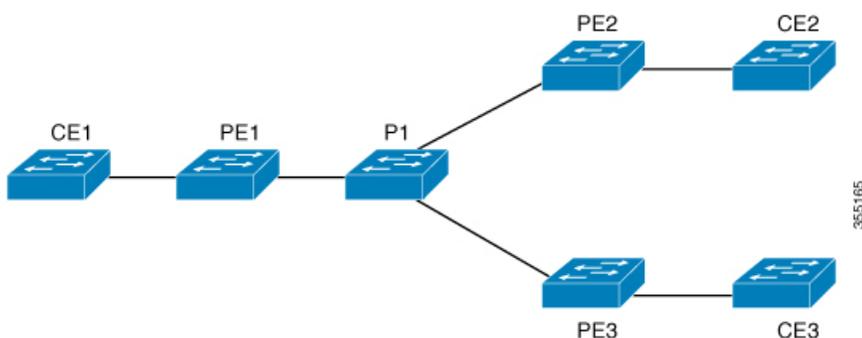
IPv6 ドメインごとに1つの IPv4 アドレスのみが必要であり、明示的にトンネルを設定する必要はありません。

6PE 実装時は、プロバイダー エッジルータが 6PE をサポートするようにアップグレードされますが、残りのコア ネットワークに影響することはありません (IPv6 非対応)。転送が IP ヘッダー自体ではなくラベルに基づいて行われるため、この実装にはコアルータの再設定は必要ありません。これにより、IPv6 の導入を費用効率性の高い戦略で実現できます。マルチプロトコルボーダーゲートウェイプロトコル (mp-iBGP) の拡張機能を使用して PE ルータによって IPv6 到達可能性情報が交換されます。

6PE は PE ルータの IPv4 ネットワーク設定の mp-iBGP に基づき、アドバタイズする各 IPv6 アドレス プレフィックスの MPLS の他に IPv6 到達可能性情報を交換します。PE ルータは、IPv4 と IPv6 の両方を実行するデュアルスタックとして設定され、IPv4 マッピング IPv6 アドレスを使用して IPv6 プレフィックスの到達可能性情報を交換します。6PE および 6VPE プレフィックスについて PE ルータがアドバタイズするネクストホップは、この場合も IPv4 L3 VPN ルートに使用される IPv4 アドレスです。値 `::FFFF:` が IPv4 ネクストホップの先頭に追加されます。これは、IPv4 マッピングの IPv6 アドレスです。

次の図に 6PE トポロジを示します。

図 4: 6PE トポロジ



## 6PE の IPv6 明示的ヌルラベル

ヌルラベルは、最後から2番目のラベルスイッチルータ (LSR) と出力 LSR の間で使用されるラベルです。

Cisco IOS XE Bengaluru 17.6.1 リリース以降、IPv6 明示的ヌルラベルを VPN ラベルとして使用して、MPLS コアを介して IPv6 到達可能性情報を交換できるようになります。IPv6 明示的ヌルラベルの値は 2 です。ヌルラベルでは、ラベルの転送にボーダーゲートウェイプロトコル (BGP) は使用されません。ヌルラベルを使用すると、BGP ラベルは使用されないため、より多くの IPv6 プレフィックスをサポートできます。

アドレスファミリ コンフィギュレーションモードで `label mode [explicit-null | all-explicit-null]` コマンドを使用して、IPv6 明示的ヌルラベルを設定できます。

`explicit-null` または `all-explicit-null` ラベルを選択できます。

- **explicit-null** ラベル：直接接続方式により BGP ラベル付きユニキャストネイバーに送信される IPv6 プレフィックス用。
- **all-explicit-null** ラベル：BGP ラベル付きユニキャストネイバーに送信されるすべての IPv6 プレフィックス用。

## 6PE の設定

6PE を設定する PE ルータが IPv4 クラウドおよび IPv6 クラウドの両方に参加していることを確認します。

PE ルータ上で実行する BGP は、他の PE で実行する BGP と (IPv4) ネイバー関係を確立する必要があります。その後、IPv6 テーブルから学習した IPv6 プレフィックスをそれらのネイバーにアドバタイズする必要があります。BGP がアドバタイズした IPv6 プレフィックスには、アドバタイズメントのネクストホップアドレスとして IPv4 エンコードの IPv6 アドレスが自動的に設定されます。

6PE を設定するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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 3	<b>ipv6 unicast-routing</b> 例： Device(config)# <b>ipv6 unicast-routing</b>	IPv6 ユニキャストデータグラムの転送を有効にします。
ステップ 4	<b>router bgp as-number</b> 例： Device(config)# <b>router bgp 65001</b>	ルータが存在する自律システム (AS) を識別する番号を入力します。  <i>as-number</i> : 自律システム番号。2 バイトの番号の範囲は 1 ~ 65535 です。4 バイトの番号の範囲は 1.0 ~ 65535.65535 です。

	コマンドまたはアクション	目的
ステップ 5	<b>bgp router-id interface interface-id</b> 例 : <pre>Device(config-router)# bgp router-id interface Loopback1</pre>	ローカル ボーダー ゲートウェイ プロトコル (BGP) ルーティングプロセスの固定ルータ ID を設定します。
ステップ 6	<b>bgp log-neighbor-changes</b> 例 : <pre>Device(config-router)# bgp log-neighbor-changes</pre>	BGP ネイバーリセットのロギングを有効にします。
ステップ 7	<b>bgp graceful-restart</b> 例 : <pre>Device(config-router)# bgp graceful-restart</pre>	すべての Border Gateway Protocol (BGP) ネイバーで BGP グレースフルリスタート機能をグローバルで有効にします。
ステップ 8	<b>neighbor { ip-address   ipv6-address   peer-group-name } remote-as as-number</b> 例 : <pre>Device(config-router)# neighbor 33.33.33.33 remote-as 65001</pre>	BGP ネイバーテーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。 <ul style="list-style-type: none"> <li>• <i>ip-address</i> : ルーティング情報を交換するピアルータの IP アドレス。</li> <li>• <i>ipv6-address</i> : ルーティング情報を交換するピアルータの IPv6 アドレス。</li> <li>• <i>peer-group-name</i> : BGP ピアグループの名前。</li> <li>• <i>remote-as</i> : リモート自律システムを指定します。</li> <li>• <i>as-number</i> : ネイバーが属する自律システムの 1 ~ 65535 の範囲内の番号。</li> </ul>
ステップ 9	<b>neighbor { ip-address   ipv6-address   peer-group-name } update-source interface-type interface-number</b> 例 : <pre>Device(config-router)# neighbor 33.33.33.33 update-source Loopback1</pre>	BGP セッションが TCP 接続の動作インターフェイスを使用できるように設定します。

	コマンドまたはアクション	目的
ステップ 10	<b>address-family ipv6</b> 例 :  Device (config-router) # <b>address-family ipv6</b>	標準 IPv6 アドレス プレフィックスを使用する BGP などのルーティングセッションを設定するために、アドレスファミリ コンフィギュレーションモードを開始します。
ステップ 11	<b>redistribute protocol as-number match { internal   external 1   external 2</b> 例 :  Device (config-router-af) # <b>redistribute ospf 11 match internal external 1</b>	ルートを 1 つのルーティング ドメインから他のルーティング ドメインに再配布します。
ステップ 12	<b>neighbor { ip-address   ipv6-address   peer-group-name } activate</b> 例 :  Device (config-router-af) # <b>neighbor 33.33.33.33 activate</b>	BGP ネイバーとの情報交換を有効にします。
ステップ 13	<b>neighbor { ip-address   ipv6-address   peer-group-name } send-label</b> 例 :  Device (config-router-af) # <b>neighbor 33.33.33.33 send-label</b>	隣接 BGP ルータに BGP ルートを含む MPLS ラベルを送信します。
ステップ 14	<b>exit-address-family</b> 例 :  Device (config-router-af) # <b>exit-address-family</b>	BGP アドレス ファミリ サブモードを終了します。
ステップ 15	<b>end</b> 例 :  Device (config) # <b>end</b>	特権 EXEC モードに戻ります。

## 6PE の IPV6 明示的ヌルラベルの設定

6PE の IPV6 明示的ヌルラベルを設定するには、次の手順を実行します。

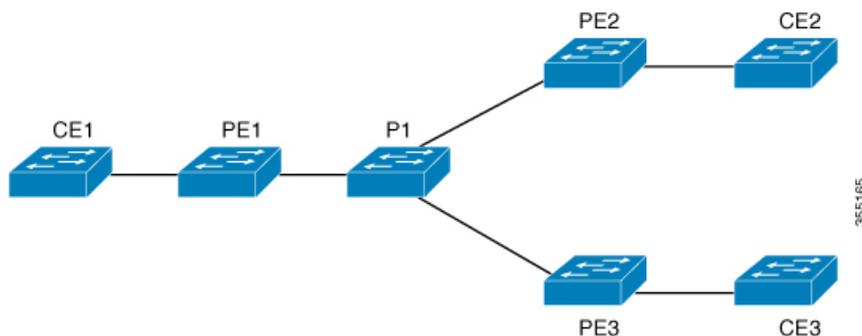
## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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 3	<b>ipv6 unicast-routing</b> 例： Device(config)# <b>ipv6 unicast-routing</b>	IPv6 ユニキャストデータグラムの転送を有効にします。
ステップ 4	<b>router bgp as-number</b> 例： Device(config)# <b>router bgp 65001</b>	ルータが存在する自律システム (AS) を識別する番号を入力します。  <i>as-number</i> : 自律システム番号。2 バイトの番号の範囲は 1 ~ 65535 です。4 バイトの番号の範囲は 1.0 ~ 65535.65535 です。
ステップ 5	<b>address-family ipv6</b> 例： Device(config-router)# <b>address-family ipv6</b>	標準 IPv6 アドレス プレフィックスを使用する BGP などのルーティングセッションを設定するために、アドレスファミリ 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	<b>label mode</b> [ <b>explicit-null</b>   <b>all-explicit-null</b> ] 例： Device(config-router-af)# <b>label mode explicit-null</b>	IPv6 明示的ヌルラベルの設定  <ul style="list-style-type: none"> <li>• <b>explicit-null</b> ラベル：直接接続方式により BGP ラベル付きユニキャストネイバーに送信される IPv6 プレフィックス用。</li> <li>• <b>all-explicit-null</b> ラベル：BGP ラベル付きユニキャストネイバーに送信されるすべての IPv6 プレフィックス用。</li> </ul>
ステップ 7	<b>neighbor { ip-address   ipv6-address   peer-group-name } activate</b> 例：	BGP ネイバーとの情報交換を有効にします。

	コマンドまたはアクション	目的
	Device(config-router-af)# <b>neighbor 33.33.33.33 activate</b>	
ステップ 8	<b>neighbor { ip-address   ipv6-address   peer-group-name } send-label</b> 例 : Device(config-router-af)# <b>neighbor 33.33.33.33 send-label</b>	隣接 BGP ルータに BGP ルートを含む MPLS ラベルを送信します。
ステップ 9	<b>exit-address-family</b> 例 : Device(config-router-af)# <b>exit-address-family</b>	BGP アドレス ファミリ サブモードを終了します。
ステップ 10	<b>end</b> 例 : Device(config)# <b>end</b>	特権 EXEC モードに戻ります。

## 6PE の設定例

図 5: 6PE トポロジ



## PE の設定

```

router ospfv3 11
ip routing
ipv6 unicast-routing
address-family ipv6 unicast
redistribute bgp 65001
exit-address-family
!
router bgp 65001
bgp router-id interface Loopback1
bgp log-neighbor-changes
bgp graceful-restart
neighbor 33.33.33.33 remote-as 65001
neighbor 33.33.33.33 update-source Loopback1
!
address-family ipv4
neighbor 33.33.33.33 activate
!
address-family ipv6
redistribute ospf 11 match internal external 1 external 2 include-connected
neighbor 33.33.33.33 activate
neighbor 33.33.33.33 send-label
neighbor 33.33.33.33 send-community extended
!

```

次に、**show bgp ipv6 unicast summary** の出力例を示します。

```

BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 34, main routing table version 34
4 network entries using 1088 bytes of memory
4 path entries using 608 bytes of memory
4/4 BGP path/bestpath attribute entries using 1120 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2816 total bytes of memory
BGP activity 6/2 prefixes, 16/12 paths, scan interval 60 secs

```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down
2.2.2.2	4	100	21	21	34	0	0	
00:04:57	2							

```

sh ipv route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

      B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
      IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP
external
      ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr -
Redirect
      RL - RPL, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
      OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

```

```

    la - LISP alt, lr - LISP site-registrations, ld - LISP dyn-eid
1A - LISP away
C  10:1:1:2::/64 [0/0]
    via Vlan4, directly connected
L  10:1:1:2::1/128 [0/0]
    via Vlan4, receive
LC 11:11:11:11::11/128 [0/0]
    via Loopback1, receive
B  30:1:1:2::/64 [200/0]
    via 33.33.33.33%default, indirectly connected
B  40:1:1:2::/64 [200/0]
    via 44.44.44.44%default, indirectly connected

```

次に、**show bgp ipv6 unicast** コマンドの出力例を示します。

```

BGP table version is 112, local router ID is 11.11.11.11
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
                r RIB-failure, S Stale, m multipath, b backup-path, f
RT-Filter,
                x best-external, a additional-path, c RIB-compressed,
                t secondary path,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

```

	Network	Next Hop	Metric	LocPrf	Weight	Path
*>	10:1:1:2::/64	::		0		32768 ?
*>i	30:1:1:2::/64	::FFFF:33.33.33.33		0	100	0 ?
*>i	40:1:1:2::/64	::FFFF:44.44.44.44		0	100	0 ?
*>i	173:1:1:2::/64	::FFFF:33.33.33.33		2	100	0 ?

次に、**show ipv6 cef 40:1:1:2::0/64 detail** コマンドの出力例を示します。

```

40:1:1:2::/64, epoch 6, flags [rib defined all labels]
recursive via 44.44.44.44 label 67
nexthop 1.20.4.2 Port-channel103 label 99-(local:147)

```

## 6PE の IPV6 明示的ヌルラベルの設定例

次の例では、IPV6 explicit-null ラベルの設定方法を示します。

```

Device(config)# router bgp 1
Device(config-router)# address-family ipv6
Device(config-router-af)#label mode explicit-null
Device(config-router-af)# neighbor 33.33.33.33 activate
Device(config-router-af)# neighbor 33.33.33.33 send-label

```

次の例では、IPV6 all-explicit-null ラベルの設定方法を示します。

```

Device(config)# router bgp 1
Device(config-router)# address-family ipv6
Device(config-router-af)# label mode all-explicit-null
Device(config-router-af)# neighbor 33.33.33.33 activate
Device(config-router-af)# neighbor 33.33.33.33 send-label

```

## MPLS を介した IPv6 プロバイダー エッジ (6PE) の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.6.1	MPLS を介した IPv6 プロバイダー エッジ (6PE)	MPLS を介した IPv6 プロバイダー エッジ (6PE) は、IPv4 MPLS を介したグローバル IPv6 到達可能性を提供し、他のすべてのデバイスに 1 つの共有ルーティングテーブルを提供します。
Cisco IOS XE Bengaluru 17.6.1	6PE の IPV6 明示的ヌルラベル	IPv6 明示的ヌルラベルを VPN ラベルとして使用して、MPLS コアを介して IPv6 到達可能性情報を交換できます。ラベルの値は 2 です。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



## 第 6 章

# MPLS を介した IPv6 VPN プロバイダーエッジ (6VPE) の設定

- [6VPE の設定 \(83 ページ\)](#)

## 6VPE の設定

次の項では、スイッチでの 6VPE の設定について説明します。

## 6VPE の制約事項

- Inter-AS および Carrier Supporting Carrier (CSC) はサポートされていません。
- VRF ルートリーキングはサポートされていません。
- eBGP は CE-PE としてサポートされていません。
- EIGRP、OSPFv3、RIP、ISIS、スタティックルートは、CE-PE としてサポートされていません。
- サポートされている MPLS ラベル割り当てモードは VRF 単位とプレフィックス単位です。プレフィックス単位がデフォルトのモードです。
- IP フラグメンテーションは、レイヤ 3 VPN の Per-Prefix モードではサポートされていません。
- DHCPv6 は、ポート単位の信頼が有効になっている 6VPE トポロジではサポートされません。

## 6VPE について

6VPE は IPv4 バックボーンを使用して VPN IPv6 サービスを提供するメカニズムです。使用可能な IPv4 MPLS バックボーンを利用することで、MPLS コア内でのデュアルスタッキングが不要になります。つまり、運用コストを削減し、6PE アプローチのセキュリティ上の制限に対処

します。6VPE は、通常の IPv4 MPLS-VPN プロバイダー エッジ とほぼ同じですが、VRF 内に IPv6 サポート が追加されています。これは、VPN メンバー デバイス 用に、論理的に分割されたルーティング テーブル エントリ を提供します。

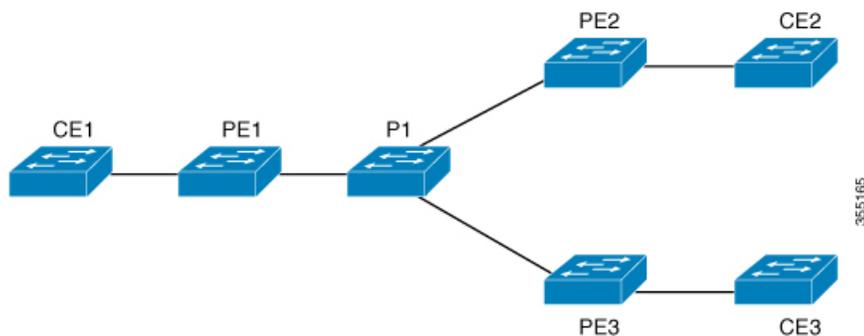
### MPLS ベースの 6VPE ネットワークのコンポーネント

- VPN ルート ターゲット コミュニティ : VPN コミュニティのその他すべてのメンバのリスト。
- VPN コミュニティ PE ルータのマルチプロトコル BGP (MP-BGP) ピアリング : VPN コミュニティのすべてのメンバに VRF 到達可能性情報を伝播します。
- MPLS 転送 : VPN サービスプロバイダー ネットワークのすべての VPN コミュニティメンバ間にすべてのトラフィックを転送します。

MPLS VPN モデルでは共通のルーティング テーブルを共有するサイトの集合として VPN が定義されます。カスタマー サイトは 1 つ以上のインターフェイスでサービス プロバイダー ネットワークに接続され、サービス プロバイダーは、VRF テーブルと呼ばれる VPN ルーティング テーブルと各インターフェイスを関連付けます。

## 6VPE の設定例

図 6: 6VPE トポロジ



## PE の設定

## PE の設定

```

vrf definition 6VPE-1
 rd 65001:11
 route-target export 1:1
 route-target import 1:1
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
 !
interface TenGigabitEthernet1/0/38
 no switchport
 vrf forwarding 6VPE-1
 ip address 10.3.1.1 255.255.255.0
 ip ospf 2 area 0
 ipv6 address 10:111:111:111::1/64
 ipv6 enable
 ospfv3 1 ipv6 area 0
 !
router ospf 2 vrf 6VPE-1
 router-id 1.1.11.11
 redistribute bgp 65001 subnets
 !
router ospfv3 1
 nsr
 graceful-restart
 !
address-family ipv6 unicast vrf 6VPE-1
 redistribute bgp 65001
 exit-address-family
 !
router bgp 65001
 bgp router-id interface Loopback1
 bgp log-neighbor-changes
 bgp graceful-restart
 neighbor 33.33.33.33 remote-as 65001
 neighbor 33.33.33.33 update-source Loopback1
 !
 address-family ipv4 vrf 6VPE-1
 redistribute ospf 2 match internal external 1 external 2
 exit-address-family
 address-family ipv6 vrf 6VPE-1
 redistribute ospf 1 match internal external 1 external 2 include-connected
 exit-address-family
 !
address-family vpnv4
 neighbor 33.33.33.33 activate
 neighbor 33.33.33.33 send-community both
 neighbor 44.44.44.44 activate
 neighbor 44.44.44.44 send-community both
 neighbor 55.55.55.55 activate
 neighbor 55.55.55.55 send-community both
 exit-address-family
 !
address-family vpnv6
 neighbor 33.33.33.33 activate
 neighbor 33.33.33.33 send-community both
 neighbor 44.44.44.44 activate
 neighbor 44.44.44.44 send-community both
 neighbor 55.55.55.55 activate

```

**PE の設定**

```
neighbor 55.55.55.55 send-community both
exit-address-family
!
```

次に、**show mpls forwarding-table vrf** の出力例を示します。

```
Local Outgoing Prefix Bytes Label Outgoing Next Hop
Label Label or Tunnel Id Switched interface
29 No Label A:A:A:565::/64[V] \ 0 aggregate/VRF601
32 No Label A:B5:1:5::/64[V] 2474160 V1601 FE80::200:7BFF:FE62:2636
33 No Label A:B5:1:4::/64[V] 2477978 V1601 FE80::200:7BFF:FE62:2636
35 No Label A:B5:1:3::/64[V] 2477442 V1601 FE80::200:7BFF:FE62:2636
36 No Label A:B5:1:2::/64[V] 2476906 V1601 FE80::200:7BFF:FE62:2636
37 No Label A:B5:1:1::/64[V] 2476370 V1601 FE80::200:7BFF:FE62:2636
```

次に、**show vrf counter** コマンドの出力例を示します。

```
Maximum number of VRFs supported: 256
Maximum number of IPv4 VRFs supported: 256
Maximum number of IPv6 VRFs supported: 256
Maximum number of platform iVRFs supported: 10
Current number of VRFs: 127
Current number of IPv4 VRFs: 6
Current number of IPv6 VRFs: 127
Current number of VRFs in delete state: 0
Current number of platform iVRFs: 1
```

次に、**show ipv6 route vrf** コマンドの出力例を示します。

```
IPv6 Routing Table - VRF1 - 8 entries Codes: C - Connected, L - Local,
S - Static, U - Per-user Static route B - BGP, R - RIP, I1 - ISIS L1,
I2 - ISIS L2 IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX -
EIGRP external ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr
- Redirect RL - RPL, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext
1 OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2 la -
LISP alt, lr - LISP site-registrations, ld - LISP dyn-eid la - LISP
away
```

```
B 1:1:1:1::1/128 [200/1] via 1.1.1.11%default, indirectly connected
O 2:2:2:2::2/128 [110/1] via FE80::A2E0:AFF:FE30:3E40,
TenGigabitEthernet1/0/7
B 3:3:3:3::3/128 [200/1] via 3.3.3.33%default, indirectly connected
B 10:1:1:1::/64 [200/0] via 1.1.1.11%default, indirectly connected
C 10:2:2:2::/64 [0/0] via TenGigabitEthernet1/0/7, directly connected
L 10:2:2:2::1/128 [0/0] via TenGigabitEthernet1/0/7, receive
B 10:3:3:3::/64 [200/0] via 3.3.3.33%default, indirectly connected
L FF00::/8 [0/0] via Null0, receive
```

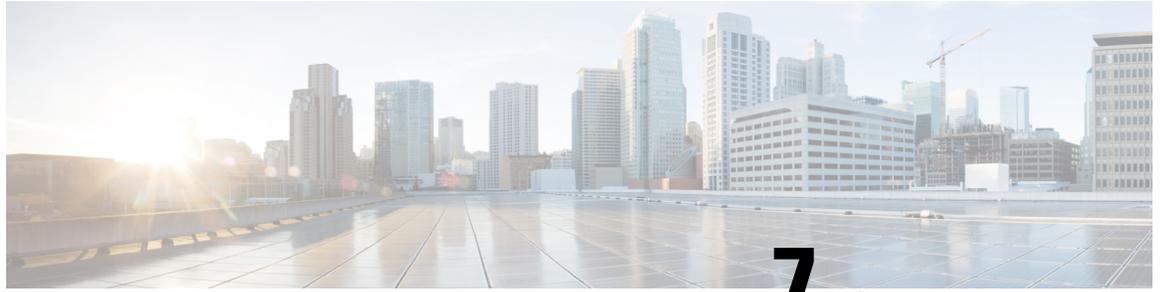
## MPLS を介した IPv6 VPN プロバイダーエッジ (6VPE) の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.6.1	MPLS を介した IPv6 VPN プロバイダーエッジ (6VPE)	MPLS を介した IPv6 VPN プロバイダーエッジ (6VPE) は IPv4 バックボーンを使用して VPN IPv6 サービスを提供するメカニズムです。使用可能な IPv4 MPLS バックボーンを利用することで、MPLS コア内でのデュアルスタッキングが不要になります。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



## 第 7 章

# MPLS VPN InterAS オプションの設定

- [MPLS VPN InterAS オプションに関する情報 \(89 ページ\)](#)
- [MPLS VPN InterAS オプションの設定方法 \(97 ページ\)](#)
- [MPLS VPN InterAS オプションの設定の確認 \(113 ページ\)](#)
- [MPLS VPN InterAS オプションの設定例 \(114 ページ\)](#)
- [MPLS VPN InterAS オプションに関するその他の参考資料 \(130 ページ\)](#)
- [MPLS VPN InterAS オプションの機能履歴 \(130 ページ\)](#)

## MPLS VPN InterAS オプションに関する情報

MPLS VPN InterAS オプション機能は、異なる MPLS VPN サービスプロバイダー間で VPN を相互接続するさまざまな方法を提供します。これにより、お客様のサイトを複数のキャリアネットワーク（自律システム）に存在させ、サイト間でのシームレスな VPN 接続が可能になります。

### 自律システムと ASBR

自律システム（AS）とは、共通のシステム管理グループによって管理され、単一の明確に定義されたプロトコルを使用している単一のネットワークまたはネットワークのグループのことです。多くの場合、VPN は異なる地理的領域の異なる AS に拡張されます。一部の VPN は、複数のサービスプロバイダーにまたがって拡張する必要があり、それらはオーバーラッピング VPN と呼ばれます。VPN の複雑さや場所に関係なく、AS 間の接続はお客様に対してシームレスである必要があります。

自律システム境界ルータ（ASBR）は、複数のルーティングプロトコルを使用して設定された AS 内のデバイスであり、外部ルーティングプロトコル（eBGP など）またはスタティックルートを使用するか、あるいは両方を使用して、他の ASBR とルーティング情報を交換します。

異なるサービスプロバイダーからの個別の自律システムは、VPN IP アドレスの形式で情報を交換することによって通信し、次のプロトコルを使用してルーティング情報を共有します。

- AS 内では、ルーティング情報は iBGP を使用して共有されます。

iBGP は、各 VPN および各 AS 内の IP プレフィックスのネットワーク層情報を配布します。

- 自律システム間では、ルーティング情報は eBGP を使用して共有されます。

eBGP を使用することで、サービスプロバイダーは別の自律システム間でのルーティング情報のループフリー交換を保証するインタードメインルーティングシステムを設定できます。eBGP の主な機能は、自律システムのルートに関する情報を含む、自律システム間のネットワーク到達可能性情報を交換することです。自律システムは、eBGP ボーダーエッジルータを使用してラベルスイッチング情報を含むルートを配布します。各ボーダーエッジルータでは、ネクストホップおよび MPLS ラベルが書き換えられます。

MPLS VPN InterAS オプションの設定はサポートされており、プロバイダー間 VPN を含めることができます。これは、異なるボーダーエッジルータで接続されている2つ以上の自律システムで構成される MPLS VPN です。自律システムでは eBGP を使用してルートが交換されます。iBGP やルーティング情報は自律システム間で交換されません。

## MPLS VPN InterAS オプション

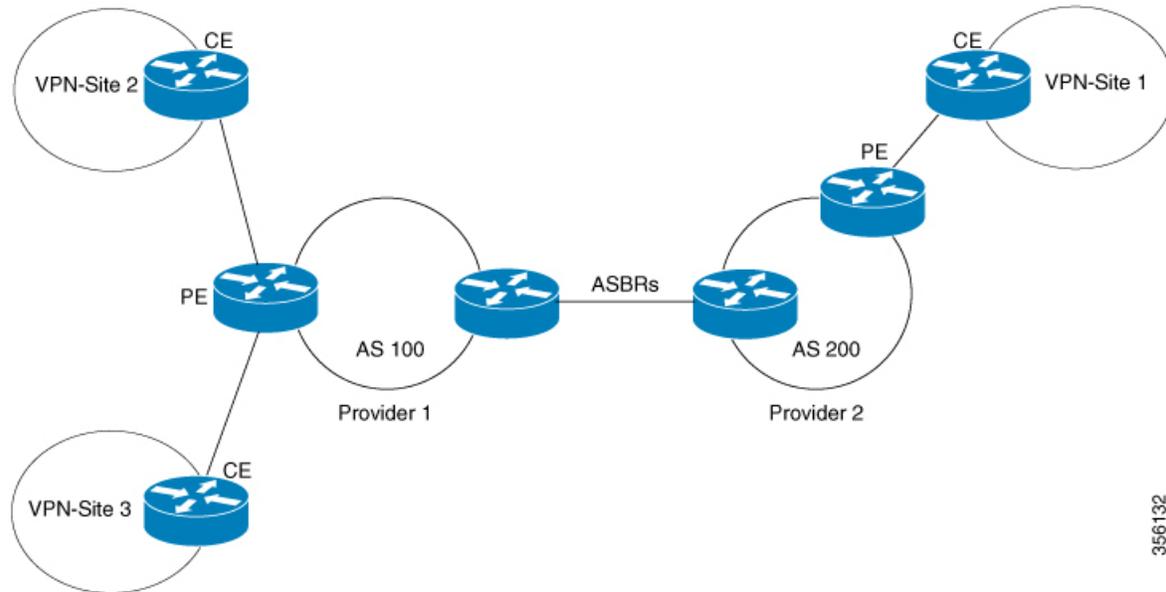
RFC4364 で定義されている次のオプションは、異なる自律システム間の MPLS VPN 接続を提供します。

- InterAS オプション B：このオプションは、ASBR 間の VPNv4 ルート配布を提供します。
- InterAS オプション AB：このオプションは、InterAS オプション A ネットワークと InterAS オプション B ネットワークの最良の機能を組み合わせたものです。MPLS VPN サービスプロバイダーは、さまざまな自律システムを相互接続して VPN サービスを提供できます。

### InterAS オプション B

InterAS オプション B ネットワークでは、ASBR ポートは、MPLS トラフィックを受信できる1つ以上のインターフェイスによって接続されます。このオプションを使用すると、ASBR は eBGP セッションを使用して相互にピアリングします。ASBR は PE ルータとしても機能し、AS 内のすべての PE ルータとピアリングします。ASBR は VRF を保持しませんが、他の AS に渡す必要がある PE ルータからの VPNv4 ルートのすべてまたはサブセットを保持します。VPNv4 ルートは、route-distinguisher を使用して ASBR で一意に維持され、ルートターゲットを使用してフィルタリングされます。ASBR は、eBGP を使用して VPNv4 ルートと VPN ラベルを交換します。

図 7: InterAS オプション B のトポロジ



ASBR 間で VPNv4 ルートのネクストホップを配布するための 2 つの方法がサポートされています。2 つの ASBR を接続するリンクで LDP または IGP を有効にする必要はありません。ASBR 上の直接接続されたインターフェイス間の MP-eBGP セッションにより、インターフェイスはラベル付きパケットを転送できます。直接接続された BGP ピアに対してこの MPLS 転送を保証するには、ASBR に接続するインターフェイスで `mpls bgp forwarding` コマンドを設定する必要があります。このコマンドは、直接接続されたインターフェイスの IOS に実装されています。最大 200 の BGP ネイバーを設定できます。

- ネクストホップセルフ方式：ネクストホップを他の ASBR から学習したすべての VPNv4 ルートのローカル ASBR のネクストホップに変更します。
- Redistribute Connected Subnet 方式：`redistribute connected subnets` コマンドを使用して、リモート ASBR のネクストホップアドレスをローカル IGP に再配布します。つまり、VPNv4 ルートがローカル AS に再配布されても、ネクストホップは変更されません。

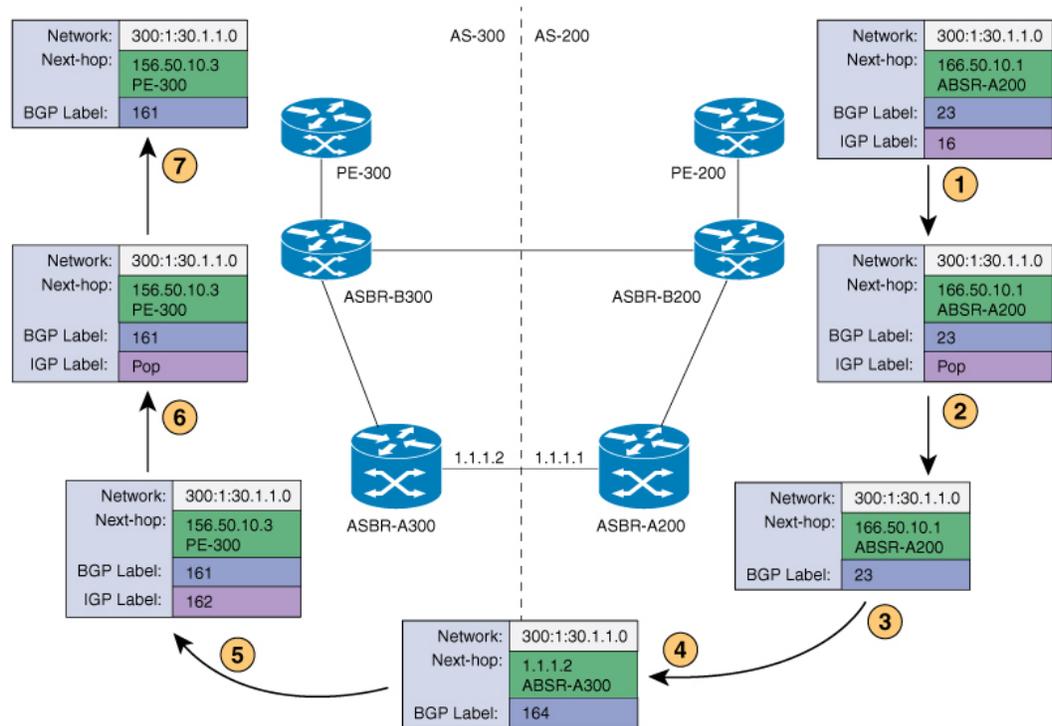


(注) 等コストパス（リモート AS への ECMP）が複数ある場合は、ASBR 上のリモートループバックに対する MPLS スタティック ラベル バインディングを設定する必要があります。そのように設定しないと、パケットが損失する場合があります。

次に説明するラベルスイッチパス転送の項では、AS200 はネクストホップセルフ方式で設定されており、AS300 は Redistribute Subnet 方式で設定されています。

## ネクストホップセルフ方式

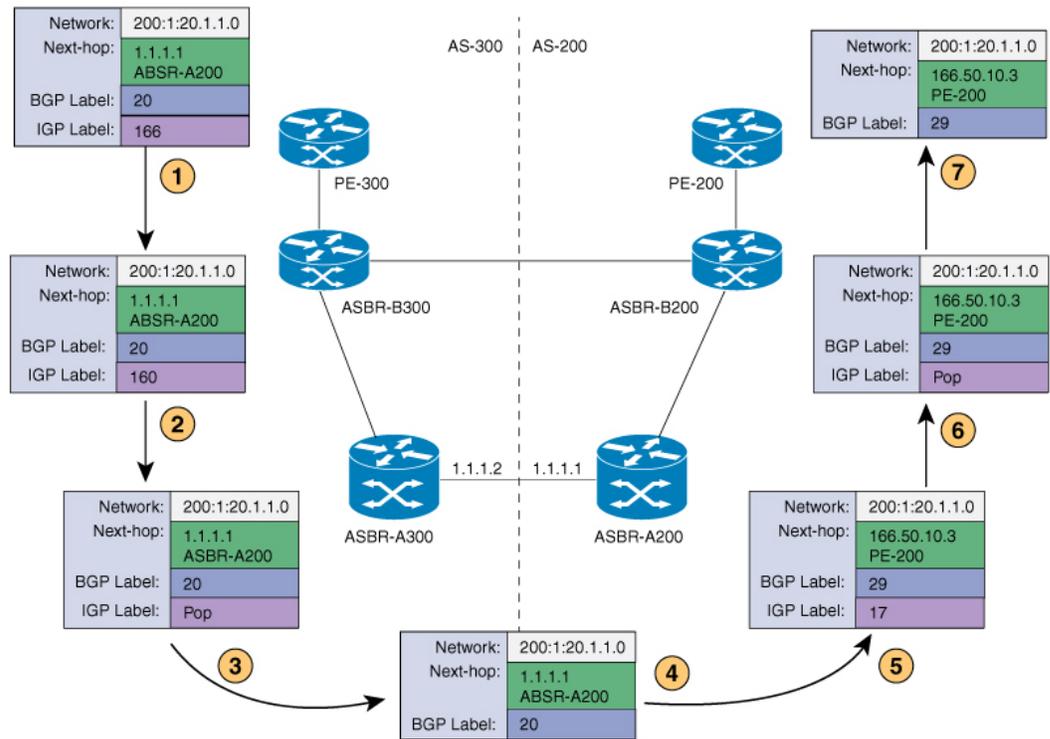
次の図に、ネクストホップセルフ方式のラベル転送パスを示します。パケットが AS 200 の PE-200 から AS 300 の PE-300 に到達するときに、ラベルがスタックにプッシュ、スワップ、およびポップされます。ステップ 5 で、ASBR-A300 はラベル付きフレームを受信し、ラベル 164 をラベル 161 に置き換え、IGP ラベル 162 をラベルスタックにプッシュします。



356133

## Redistribute Connected Subnet 方式

次の図に、Redistribute Connected Subnet 方式のラベル転送パスを示します。パケットが AS 300 の PE-300 から AS 200 の PE-200 に移動するときに、ラベルがスタックにプッシュ、スワップ、およびポップされます。ステップ 5 で、ASBR-A200 は BGP ラベル 20 のフレームを受信し、ラベル 29 と交換し、ラベル 17 をプッシュします。



356134

## InterAS オプション AB

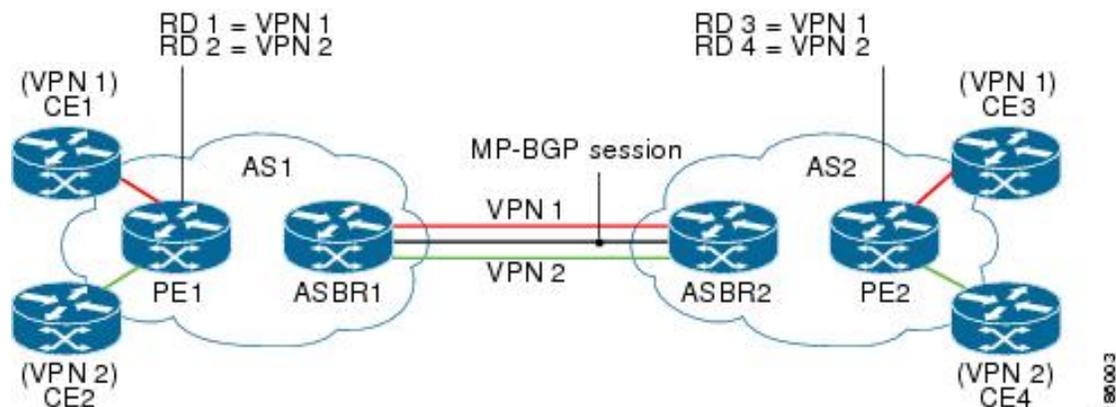
MPLS VPN サービスプロバイダーは、さまざまな自律システムを相互接続して、複数の VPN カスタマーにサービスを提供する必要があります。MPLS VPN InterAS オプション AB 機能を使用すると、グローバルルーティングテーブル内の単一の MP-BGP セッションを使用してさまざまな自律システムを相互接続し、コントロールプレーントラフィックを送信できます。この MP-BGP セッションでは、2つの ASBR 間で、各 VRF インスタンスの VPN プレフィックスがシグナリングされます。このトラフィックは、IP または MPLS です。

VPN トラフィックは VRF 固有のインターフェイスを経由する IP トラフィックであるため、2つの ASBR 間で MPLS BGP 転送または LDP を設定する必要はありません。

InterAS オプション AB 機能には、サービスプロバイダーにとって次の利点があります。

- ASBR ピア間の IP QoS 機能を維持し、カスタマー SLA を実現できます。
- データプレーントラフィックは、セキュリティ上の目的で VRF ごとに分離されます。
- SVI にポリシーを付加することで、専用の QoS ポリシーを各 VRF に適用できます。

## ルート配布およびパケット転送



次の属性は、上の図に示されているサンプル InterAS オプション AB ネットワークのトポロジを示しています。

- CE1 と CE3 は VPN 1 に属しています。
- CE2 と CE4 は VPN 2 に属しています。
- PE1 では、VPN 1 (VRF 1) にルート識別子 1 (RD 1) を、VPN 2 (VRF 2) に RD 2 を使用しています。
- PE2 は、VPN 1 (VRF 1) に RD 3 を、VPN 2 (VRF 2) に RD 4 を使用しています。
- ASBR1 では、VRF 1 が RD 5 に、VRF 2 が RD 6 にプロビジョニングされています。
- ASBR2 では、VRF 1 が RD 7 に、VRF 2 が RD 8 にプロビジョニングされています。
- ASBR1 と ASBR2 との間には 3 つのリンクがあります。
  - VRF 1
  - VRF 2
  - MP-BGP セッション

## VPN 1 のルート配布

ルート識別子 (RD) は、各ルートにどの VPN が属しているかを識別するためにルートに付加される識別子です。各ルーティングインスタンスには、一意な RD 自律システムが関連付けられている必要があります。RD は、VPN の周囲に境界を設置して、異なる VPN で同じ IP アドレスプレフィックスを使用してもこれらの IP アドレスプレフィックスが重複しないようにするために使用されます。RD 文は、インスタンスタイプが VRF である場合は必須です。

次のプロセスは、上記の図の VPN 1 のルート配布プロセスを示しています。このプロセスで使用されているプレフィックス「N」は、VPN の IP アドレスを示しています。

## ASBR1

- CE1 は、プレフィックス N を PE1 にアドバタイズします。

- PE1 は、VPN プレフィックス RD 1:N を ASBR1 に MP-iBGP 経由でアドバタイズします。
- ASBR1 は、プレフィックスを VPN 1 にインポートして、プレフィックス RD 5:N を作成します。
- ASBR1 は、インポートしたプレフィックス RD 5:N を ASBR2 にアドバタイズします。ASBR1 は、自身をプレフィックス RD 5:N のネクストホップとして設定し、このプレフィックスとともにシグナリングされるローカルラベルを割り当てます。
- ASBR1 は、最初に受信した RT ではなく、VRF に設定されたエクスポート RT を使用してルートをアドバタイズします。デフォルトで、ASBR1 はソースプレフィックス RD 1:N を ASBR2 にアドバタイズしません。このプレフィックスは、オプション AB VRF にインポートされるプレフィックスであるため、アドバタイズされません。

#### ASBR2

- ASBR2 は、プレフィックス RD 5:N を受信して、RD 7:N として VPN 1 にインポートします。
- ASBR2 は、最初に受信した RT ではなく、VRF に設定されたエクスポート RT を使用してルートをアドバタイズします。
- プレフィックスのインポート時に、ASBR2 は RD 7:N のネクストホップを VRF 1 の ASBR1 インターフェイス IP アドレスに設定します。ネクストホップテーブル ID も VRF 1 に設定されます。RD 7:N 用の MPLS 転送エントリをインストールする場合、デフォルトでは ASBR2 は転送プロセスで発信ラベルをインストールしません。これにより、ASBR 間のトラフィックを IP にすることができます。
- ASBR2 は、インポートしたプレフィックス RD 7:N を PE2 にアドバタイズします。ASBR2 は、自身をこのプレフィックスのネクストホップとして設定し、このプレフィックスとともにシグナリングされるローカルラベルも割り当てます。デフォルトで、ASBR2 はソースプレフィックス RD 5:N を PE2 にアドバタイズしません。このプレフィックスは、オプション AB VRF にインポートされるプレフィックスであるため、アドバタイズされません。
- PE2 は、RD 7:N を RD 3:N として VRF 1 にインポートします。

#### VPN 1 のパケット転送

次のパケット転送プロセスは、オプション A のシナリオと同様に動作します。ASBR は VPN の終端となることによって PE と同様に動作し、トラフィックを標準 IP パケットとして VPN ラベルなしで次の PE に転送します。その後、次の PE で VPN プロセスが繰り返されます。したがって、各 PE デバイスは隣接 PE デバイスを CE デバイスとして扱い、各自律システムでのルート再配布には標準的なレイヤ 3 MPLS VPN メカニズムが使用されます。つまり、各 PE は、外部 BGP (eBGP) を使用して相互にラベルなし IPv4 アドレスを配布します。

- CE3 は、N 宛てのパケットを PE2 に送信します。

- PE2 は、ASBR2 によって割り当てられた VPN ラベル、およびパケットを ASBR2 にトンネリングするために必要な内部ゲートウェイプロトコル (IGP) ラベルでパケットをカプセル化します。
- パケットは、VPN ラベルが付いた状態で ASBR2 に到達します。ASBR2 は VPN ラベルを削除し、パケットを IP として ASBR1 の VRF 1 インターフェイスに送信します。
- IP パケットが、ASBR1 の VRF 1 インターフェイスに到達します。ASBR1 は、PE1 によって割り当てられた VPN ラベル、およびパケットを PE1 にトンネリングするために必要な IGP ラベルでパケットをカプセル化します。
- パケットは、VPN ラベルが付いた状態で PE1 に到達します。PE1 は VPN ラベルを削除して、IP パケットを CE1 に転送します。

## VPN 2 のルート配布

次の情報は、上記の図の VPN 2 のルート配布プロセスを示しています。

### ASBR1

- CE2 は、プレフィックス N を PE1 にアドバタイズします。N は VPN IP アドレスです。
- PE1 は、VPN プレフィックス RD 2:N を ASBR1 に MP-iBGP 経由でアドバタイズします。
- ASBR1 は、プレフィックスを VPN 2 にインポートして、プレフィックス RD 6:N を作成します。
- ASBR1 は、インポートしたプレフィックス RD 6:N を ASBR2 にアドバタイズします。ASBR2 は、自身をこのプレフィックスのネクストホップとして設定し、このプレフィックスとともにシグナリングされるローカルラベルも割り当てます。デフォルトで、ASBR1 はソースプレフィックス RD 2:N を ASBR2 にアドバタイズしません。このプレフィックスは、オプション AB VRF にインポートされるプレフィックスであるため、アドバタイズされません。

### ASBR2

- ASBR2 は、プレフィックス RD 6:N を受信して、RD 8:N として VPN 2 にインポートします。
- プレフィックスのインポート時に、ASBR2 は RD 8:N のネクストホップを VRF 2 の ASBR1 インターフェイスアドレスに設定します。ネクストホップテーブル ID も VRF 2 の ID に設定されます。RD 8:N 用の MPLS 転送エントリをインストールする場合、デフォルトでは ASBR2 は転送プロセスで発信ラベルをインストールしません。これにより、ASBR 間のトラフィックを IP にすることができます。
- ASBR2 は、インポートしたプレフィックス RD 8:N を PE2 にアドバタイズします。ASBR2 は、自身をこのプレフィックスのネクストホップとして設定し、このプレフィックスとともにシグナリングされるローカルラベルも割り当てます。デフォルトで、ASBR2 はソースプレフィックス RD 6:N を PE2 にアドバタイズしません。このプレフィックスは、オプション AB VRF にインポートされるプレフィックスであるため、アドバタイズされません。

- PE2 は、RD 8:N を RD 4:N として VRF 2 にインポートします。

## MPLS VPN InterAS オプションの設定方法

次の項では、MPLS VPN InterAS オプションの設定方法について説明します。

### MPLS VPN InterAS オプション B の設定

ここでは、ネクストホップセルフ方式と Redistribute Connected 方式を使用して interAS オプション B を設定する方法について説明します。

#### ネクストホップセルフ方式を使用した InterAS オプション B の設定

ネクストホップセルフ方式を使用して ASBR で InterAS オプション B を設定するには、次の手順を実行します。

##### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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 3	<b>router ospf process-id</b> 例： Device(config)# <b>router ospf 1</b>	OSPF ルーティングプロセスを設定し、プロセス番号を割り当てます。
ステップ 4	<b>router-id ip-address</b> 例： Device(config)# <b>router-id 4.1.1.1</b>	固定ルータ ID を指定します。
ステップ 5	<b>nsr</b> 例： Device(config-router)# <b>nsr</b>	OSPF ノンストップルーティング (NSR) を設定します。

	コマンドまたはアクション	目的
ステップ 6	<b>nsf</b> 例 :  Device(config-router)# <b>nsf</b>	OSPF ノンストップ フォワーディング (NSF) を設定します。
ステップ 7	<b>redistribute bgp</b> <i>autonomous-system-number</i> 例 :  Device(config-router)# <b>redistribute bgp 200</b>	BGP 自律システムからルートを OSPF ルーティングプロセスに再配布します。
ステップ 8	<b>passive-interface interface-type</b> <i>interface-number</i> 例 :  Device(config-router)# <b>passive-interface GigabitEthernet 1/0/10</b> Device(config-router)# <b>passive-interface Tunnel0</b>	インターフェイスの Open Shortest Path First (OSPF) ルーティングアップデートを無効にします。
ステップ 9	<b>network ip-address wildcard-mask aread</b> <i>area-id</i> 例 :  Device(config-router)# <b>network 4.1.1.0 0.0.0.0.255 area 0</b>	OSPF を実行するインターフェイスを定義し、そのインターフェイスに対するエリア ID を定義します。
ステップ 10	<b>exit</b> 例 :  Device(config-router)# <b>exit</b>	ルータ コンフィギュレーションモードを終了します。
ステップ 11	<b>router bgp autonomous-system-number</b> 例 :  Device(config)# <b>router bgp 200</b>	BGP ルーティングプロセスを設定します。
ステップ 12	<b>bgp router-id ip-address</b> 例 :  Device(config-router)# <b>bgp router-id 4.1.1.1</b>	BGP ルーティングプロセスの固定ルータ ID を設定します。
ステップ 13	<b>bgp log-neighbor changes</b> 例 :	BGP ネイバーリセットのロギングを有効にします。

	コマンドまたはアクション	目的
	Device(config-router)# <b>bgp log-neighbor changes</b>	
ステップ 14	<b>no bgp default ipv4-unicast</b> 例 : Device(config-router)# <b>no bgp default ipv4-unicast</b>	アドレスファミリー IPv4 のルーティング情報のアドバタイズメントを無効にします。
ステップ 15	<b>no bgp default route-target filter</b> 例 : Device(config-router)# <b>no bgp default route-target filter</b>	BGP の route-target コミュニティフィルタリングを無効にします。
ステップ 16	<b>neighbor ip-address remote-as as-number</b> 例 : Device(config-router)# <b>neighbor 4.1.1.3 remote-as 200</b>	エントリを BGP ネイバーテーブルに設定します。
ステップ 17	<b>neighbor ip-address update-source interface-type interface-number</b> 例 : Device(config-router)# <b>neighbor 4.1.1.3 update-source Loopback0</b>	Cisco IOS ソフトウェアで、BGP セッションによる TCP 接続の特定の動作インターフェイスを使用できるようになります。
ステップ 18	<b>neighbor ip-address remote-as as-number</b> 例 : Device(config-router)# <b>neighbor 4.1.1.3 remote-as 300</b>	エントリを BGP ネイバーテーブルに設定します。
ステップ 19	<b>address-family ipv4</b> 例 : Device(config-router)# <b>address-family ipv4</b>	標準 IP バージョン 4 アドレスプレフィックスを使用する BGP ルーティングセッションを設定するために、アドレスファミリー コンフィギュレーションモードを開始します。
ステップ 20	<b>neighbor ip-address activate</b> 例 : Device(config-router-af)# <b>neighbor 10.32.1.2 activate</b>	BGP ネイバーとの情報交換を有効にします。

	コマンドまたはアクション	目的
ステップ 21	<b>neighbor ip-address send-label</b> 例 :  Device(config-router-af) # <b>neighbor 10.32.1.2 send-label</b>	隣接 BGP ルータに BGP ルートを含む MPLS ラベルを送信します。
ステップ 22	<b>exit address-family</b> 例 :  Device(config-router-af) # <b>exit address-family</b>	BGP アドレス ファミリ サブモードを終了します。
ステップ 23	<b>address-family vpnv4</b> 例 :  Device(config-router) # <b>address-family vpnv4</b>	アドレス ファミリ コンフィギュレーションモードでデバイスを設定して、標準 VPNv4 アドレスプレフィックスを使用する、BGP などのルーティングセッションを設定します。
ステップ 24	<b>neighbor ip-address activate</b> 例 :  Device(config-router-af) # <b>neighbor 4.1.1.3 activate</b>	BGP ネイバーとの情報交換を有効にします。
ステップ 25	<b>neighbor ip-address send-community extended</b> 例 :  Device(config-router-af) # <b>neighbor 4.1.1.3 send-community extended</b>	コミュニティ属性が BGP ネイバーに送信されるように指定します。
ステップ 26	<b>neighbor ip-address next-hop-self</b> 例 :  Device(config-router-af) # <b>neighbor 4.1.1.3 next-hop-self</b>	ルータを BGP スピーキングネイバーのネクストホップとして設定します。これは、ネクストホップセルフ方式を実装するコマンドです。
ステップ 27	<b>neighbor ip-address activate</b> 例 :  Device(config-router-af) # <b>neighbor 10.30.1.2 activate</b>	BGP ネイバーとの情報交換を有効にします。
ステップ 28	<b>neighbor ip-address send-community extended</b> 例 :	コミュニティ属性が BGP ネイバーに送信されるように指定します。

	コマンドまたはアクション	目的
	Device(config-router-af)# <b>neighbor 10.30.1.2 send-community extended</b>	
ステップ 29	<b>exit address-family</b> 例 : Device(config-router-af)# <b>exit address-family</b>	BGP アドレス ファミリ サブモードを終了します。
ステップ 30	<b>bgp router-id ip-address</b> 例 : Device(config-router)# <b>bgp router-id 4.1.1.3</b>	BGP ルーティングプロセスの固定ルータ ID を設定します。
ステップ 31	<b>bgp log-neighbor changes</b> 例 : Device(config-router)# <b>bgp log-neighbor changes</b>	BGP ネイバーリセットのロギングを有効にします。
ステップ 32	<b>neighbor ip-address remote-as as-number</b> 例 : Device(config-router)# <b>neighbor 4.1.1.1 remote-as 200</b>	エントリを BGP ネイバーテーブルに設定します。
ステップ 33	<b>neighbor ip-address update-source interface-type interface-number</b> 例 : Device(config-router)# <b>neighbor 4.1.1.1 update-source Loopback0</b>	Cisco IOS ソフトウェアで、BGP セッションによる TCP 接続の特定の動作インターフェイスを使用できるようになります。
ステップ 34	<b>address-family vpnv4</b> 例 : Device(config-router)# <b>address-family vpnv4</b>	アドレス ファミリ コンフィギュレーションモードでデバイスを設定して、標準 VPNv4 アドレスプレフィックスを使用する、BGP などのルーティングセッションを設定します。
ステップ 35	<b>neighbor ip-address activate</b> 例 : Device(config-router-af)# <b>neighbor 4.1.1.1 activate</b>	BGP ネイバーとの情報交換を有効にします。

## Redistribute Connected 方式を使用した InterAS オプション B の設定

	コマンドまたはアクション	目的
ステップ 36	<b>neighbor ip-address send-community extended</b> 例 : Device(config-router-af)# <b>neighbor 4.1.1.1 send-community extended</b>	コミュニティ属性が BGP ネイバーに送信されるように指定します。
ステップ 37	<b>exit address-family</b> 例 : Device(config-router-af)# <b>exit address-family</b>	BGP アドレス ファミリ サブモードを終了します。

## Redistribute Connected 方式を使用した InterAS オプション B の設定

Redistribute Connected 方式を使用して ASBR で InterAS オプション B を設定するには、次の手順を実行します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b> 例 : Device# <b>configure terminal</b>	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 3	<b>router ospf process-id</b> 例 : Device(config)# <b>router ospf 1</b>	OSPF ルーティングプロセスを設定し、プロセス番号を割り当てます。
ステップ 4	<b>router-id ip-address</b> 例 : Device(config)# <b>router-id 5.1.1.1</b>	固定ルータ ID を指定します。
ステップ 5	<b>nsr</b> 例 :	OSPF ノンストップルーティング (NSR) を設定します。

	コマンドまたはアクション	目的
	Device(config-router)# <b>nsr</b>	
ステップ 6	<b>nsf</b> 例：  Device(config-router)# <b>nsf</b>	OSPF ノンストップ フォワーディング (NSF) を設定します。
ステップ 7	<b>redistribute connected</b> 例：  Device(config-router)# <b>redistribute connected</b>	リモート ASBR のネクストホップアドレスをローカル IGP に再配布します。これは、Redistribute Connected 方式を実装するコマンドです。
ステップ 8	<b>passive-interface interface-type interface-number</b> 例：  Device(config-router)# <b>passive-interface GigabitEthernet 1/0/10</b> Device(config-router)# <b>passive-interface Tunnel0</b>	インターフェイスの Open Shortest Path First (OSPF) ルーティングアップデートを無効にします。
ステップ 9	<b>network ip-address wildcard-mask area-id</b> 例：  Device(config-router)# <b>network 5.1.1.0 0.0.0.0.255 area 0</b>	OSPF を実行するインターフェイスを定義し、そのインターフェイスに対するエリア ID を定義します。
ステップ 10	<b>exit</b> 例：  Device(config-router)# <b>exit</b>	ルータ コンフィギュレーションモードを終了します。
ステップ 11	<b>router bgp autonomous-system-number</b> 例：  Device(config)# <b>router bgp 300</b>	BGP ルーティングプロセスを設定します。
ステップ 12	<b>bgp router-id ip-address</b> 例：  Device(config-router)# <b>bgp router-id 5.1.1.1</b>	BGP ルーティングプロセスの固定ルータ ID を設定します。
ステップ 13	<b>bgp log-neighbor changes</b> 例：	BGP ネイバーリセットのロギングを有効にします。

	コマンドまたはアクション	目的
	Device(config-router)# <b>bgp log-neighbor changes</b>	
ステップ 14	<b>no bgp default ipv4-unicast</b> 例 : Device(config-router)# <b>no bgp default ipv4-unicast</b>	アドレスファミリー IPv4 のルーティング情報のアドバタイズメントを無効にします。
ステップ 15	<b>no bgp default route-target filter</b> 例 : Device(config-router)# <b>no bgp default route-target filter</b>	BGP の route-target コミュニティフィルタリングを無効にします。
ステップ 16	<b>neighbor ip-address remote-as as-number</b> 例 : Device(config-router)# <b>neighbor 5.1.1.3 remote-as 300</b>	エントリを BGP ネイバーテーブルに設定します。
ステップ 17	<b>neighbor ip-address update-source interface-type interface-number</b> 例 : Device(config-router)# <b>neighbor 4.1.1.3 update-source Loopback0</b>	Cisco IOS ソフトウェアで、BGP セッションによる TCP 接続の特定の動作インターフェイスを使用できるようになります。
ステップ 18	<b>neighbor ip-address remote-as as-number</b> 例 : Device(config-router)# <b>neighbor 10.30.1.2 remote-as 200</b>	エントリを BGP ネイバーテーブルに設定します。
ステップ 19	<b>address-family vpv4</b> 例 : Device(config-router)# <b>address-family vpv4</b>	アドレスファミリー コンフィギュレーションモードでデバイスを設定して、標準 VPNv4 アドレスプレフィックスを使用する、BGP などのルーティングセッションを設定します。
ステップ 20	<b>neighbor ip-address activate</b> 例 : Device(config-router-af)# <b>neighbor 5.1.1.3 activate</b>	BGP ネイバーとの情報交換を有効にします。

	コマンドまたはアクション	目的
ステップ 21	<b>neighbor ip-address send-community extended</b>  例 :  Device (config-router-af) # <b>neighbor 5.1.1.3 send-community extended</b>	コミュニティ属性が BGP ネイバーに送信されるように指定します。
ステップ 22	<b>neighbor ip-address activate</b>  例 :  Device (config-router-af) # <b>neighbor 10.30.1.1 activate</b>	BGP ネイバーとの情報交換を有効にします。
ステップ 23	<b>neighbor ip-address send-community extended</b>  例 :  Device (config-router-af) # <b>neighbor 10.30.1.2 send-community extended</b>	コミュニティ属性が BGP ネイバーに送信されるように指定します。
ステップ 24	<b>exit address-family</b>  例 :  Device (config-router-af) # <b>exit address-family</b>	BGP アドレス ファミリ サブモードを終了します。
ステップ 25	<b>mpls ldp router-id interface-id [force]</b>  例 :  Device (config-router) # <b>mpls ldp router-id Loopback0 force</b>	LDP ルータ ID を決定する優先インターフェイスを指定します。

## MPLS VPN Inter-AS オプション AB の設定

次の項では、MPLS VPN において ASBR で InterAS オプション AB 機能を設定する方法について説明します。

### 各 VPN カスタマーの ASBR インターフェイスへの VRF の設定

次の手順を実行して、各 VPN カスタマーの ASBR インターフェイスに VRF を設定し、それらの VPN が InterAS オプション AB ネットワークを介して接続できるようにします。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"><li>パスワードを入力します（要求された場合）。</li></ul>
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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 3	<b>interface type number</b> 例： Device(config)# <b>interface gigabitethernet 1/0/1</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<b>ip vrf forwarding vrf-name</b> 例： Device(config-if)# <b>ip vrf forwarding vpn1</b>	指定したインターフェイスに VRF を関連付けます。 <ul style="list-style-type: none"><li>vrf-name 引数は、VRF に割り当てる名前です。</li></ul>
ステップ 5	<b>end</b> 例： Device(config-if)# <b>end</b>	(任意) 終了して、特権 EXEC モードに戻ります。

## ASBR ピア間での MP-BGP セッションの設定

BGP では、IPv4 以外のアドレスファミリのサポートを定義する BGP マルチプロトコル拡張（RFC 2283、Multiprotocol Extensions for BGP-4 を参照）を使用して、PE デバイス間の VPN-IPv4 プレフィックスの到達可能性情報を伝播します。この拡張を使用すると、指定された VPN のルートが、その VPN の他のメンバによってのみ学習されるようになり、VPN のメンバ間の相互通信が可能になります。

この項の次の手順に従って、ASBR で MP-BGP セッションを設定します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"><li>パスワードを入力します（要求された場合）。</li></ul>
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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 3	<b>router bgp as-number</b> 例： Device(config)# <b>router bgp 100</b>	BGP ルーティング プロセスを設定し、デバイスでルータ コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"><li>as-number 引数は、デバイスを他の BGP デバイスに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0～65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512～65535 です。</li></ul>
ステップ 4	<b>neighbor {ip-address peer-group-name} remote-as as-number</b> 例： Device(config-router)# <b>neighbor 192.168.0.1 remote-as 200</b>	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリーを追加します。 <ul style="list-style-type: none"><li>ip-address 引数には、ネイバーの IP アドレスを指定します。</li><li>peer-group-name 引数には、BGP ピア グループの名前を指定します。</li><li>as-number 引数には、ネイバーが属している自律システムを指定します。</li></ul>
ステップ 5	<b>address-family vpnv4 [unicast]</b> 例： Device(config-router)# <b>address-family vpnv4</b>	アドレス ファミリ コンフィギュレーション モードを開始して、標準 VPNv4 アドレス プレフィックスを使用する、BGP などのルーティング セッションを設定します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>unicast キーワードでは、IPv4 ユニキャストアドレスプレフィックスを指定します。</li> </ul>
ステップ 6	<b>neighbor</b> {ip-address   peer-group-name} <b>activate</b>  例： Device(config-router-af) # <b>neighbor</b> <b>192.168.0.1 activate</b>	ネイバー デバイスとの情報交換を有効にします。 <ul style="list-style-type: none"> <li>ip-address 引数には、ネイバーの IP アドレスを指定します。</li> <li>peer-group-name 引数には、BGP ピアグループの名前を指定します。</li> </ul>
ステップ 7	<b>neighbor</b> {ip-address   peer-group-name} <b>inter-as-hybrid</b>  例： Device(config-router-af) # <b>neighbor</b> <b>192.168.0.1 inter-as-hybrid</b>	eBGP ピアデバイス (ASBR) を Inter-AS オプション AB ピアとして設定します。 <ul style="list-style-type: none"> <li>ip-address 引数には、ネイバーの IP アドレスを指定します。</li> <li>peer-group-name 引数には、BGP ピアグループの名前を指定します。</li> <li>プレフィックスがオプション AB VRF にインポートされると、インポートされたパスがこのピアにアドバタイズされます。</li> <li>プレフィックスをこのピアから受信し、オプション AB VRF にインポートすると、インポートされたパスが iBGP ピアにアドバタイズされます。</li> </ul> <p>(注) アドバタイズされたルートには、VRF で設定された RT があります。アドバタイズされたルートには、元の RT はありません。</p>
ステップ 8	<b>exit-address-family</b>  例： Device(config-router) # <b>exit-address-family</b>	アドレス ファミリ コンフィギュレーション モードを終了します。

## Inter-AS 接続を必要とする VPN のルーティング ポリシーの設定

適切なルーティング ポリシーおよびオプション AB 設定を設定して、ASBR ピア間で Inter-AS 接続が必要な VPN の VRF を設定するには、この項の手順を使用します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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 3	<b>vrf definition vrf-name</b> 例： Device(config)# <b>vrf definition vpn1</b>	VRF 名を割り当て、VRF コンフィギュレーション モードを開始することにより、VPN ルーティング インスタンスを定義します。  • <i>vrf-name</i> 引数は、VRF に割り当てる名前です。
ステップ 4	<b>rd route-distinguisher</b> 例： Device(config-vrf)# <b>rd 100:1</b>	ルーティング テーブルと転送テーブルを作成します。  • <i>route-distinguisher</i> 引数によって、8 バイトの値が IPv4 プレフィックスに追加され、VPN IPv4 プレフィックスが作成されます。RD は、次のいずれかの形式で入力できます。  • 16 ビット自律システム番号： 101:3 などの 32 ビット数値  • 32 ビット IP アドレス： 192.168.122.15:1 などの 16 ビット数値
ステップ 5	<b>address-family ipv4</b> 例： Device(config-vrf)# <b>address-family ipv4</b>	VRF アドレス ファミリ コンフィギュレーション モードを開始して、VRF のアドレス ファミリを指定します。  • <b>ipv4</b> キーワードは、VRF の IPv4 アドレスファミリを指定します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• 16 ビット自律システム番号 : 101:3 などの 32 ビット数値</li> <li>• 32 ビット IP アドレス : 192.168.122.15:1 などの 16 ビット数値</li> </ul>
ステップ 6	<code>route-target {import export both} route-target-ext-community</code> 例 : <pre>Device(config-vrf-af)# route-target import 100:1</pre>	VRF 用にルート ターゲット 拡張 コミュニティを作成します。 <ul style="list-style-type: none"> <li>• <b>import</b> キーワードを使用すると、ターゲット VPN 拡張コミュニティからルーティング情報がインポートされます。</li> <li>• <b>export</b> キーワードを使用すると、ルーティング情報がターゲット VPN 拡張コミュニティにエクスポートされます。</li> <li>• <b>both</b> キーワードを使用すると、ターゲット VPN 拡張コミュニティとの間でルーティング情報がインポートおよびエクスポートされます。</li> <li>• <code>route-target-ext-community</code> 引数により、<code>route-target</code> 拡張コミュニティ属性が、インポート、エクスポート、または両方（インポートとエクスポート）の <code>route-target</code> 拡張コミュニティの VRF リストに追加されます。</li> </ul>
ステップ 7	<code>inter-as-hybrid</code> 例 : <pre>Device(config-vrf-af)# inter-as-hybrid</pre>	VRF をオプション AB VRF として指定します。これには次のような効果があります。 <ul style="list-style-type: none"> <li>• この VRF にインポートされるルートは、オプション AB ピアと VPNv4 iBGP ピアにアダプタイズできます。</li> <li>• オプション AB ピアからルートを受信し、そのルートが VRF にインポートされると、そのルートのネク</li> </ul>

	コマンドまたはアクション	目的
		ストホップテーブル ID が VRF のテーブル ID に設定されます。
ステップ 8	<b>inter-as-hybrid</b> [next-hopip-address] 例 : Device (config-vrf-af) # <b>inter-as-hybrid</b> <b>next-hop 192.168.1.0</b>	(任意) VRF にインポートされ、オプション AB ピアから受信したパスに設定するネクスト ホップ IP アドレスを指定します。  • ネクスト ホップ コンテキストも、これらのパスをインポートした VRF に設定されます。
ステップ 9	<b>end</b> 例 : Device (config-vrf-af) # <b>end</b>	(任意) 終了して、特権 EXEC モードに戻ります。

## Inter-AS オプション A 配置からオプション AB 配置への変更

オプション A 配置では、VRF インスタンスは ASBR デバイス間ではバックツーバック接続であり、異なる自律システムの PE デバイス間では直接接続です。PE デバイスは複数の物理または論理インターフェイスによって接続され、各インターフェイスは (VRF インスタンスを介して) 特定の VPN に関連付けられています。

オプション AB 配置では、グローバル ルーティング テーブル内の単一の MP-BGP セッションを使用してさまざまな自律システムが相互接続され、コントロールプレーントラフィックが伝送されます。

MPLS VPN Inter-AS オプション A 配置からオプション AB 配置へ変更するには、次の手順を実行します。

1. ASBR で MP-BGP セッションを設定します。特定の VPN のルートとその VPN の他のメンバのみが学習でき、VPN のメンバが相互に通信できるように、BGP マルチプロトコル拡張を使用して IPv4 以外のアドレス ファミリのサポートが定義されます。
2. オプション A からのアップグレードが必要な VRF を特定し、**inter-as-hybrid** コマンドを使用してそれらの VRF をオプション AB に対して設定します。
3. eBGP (ピア ASBR) ネイバーの設定を削除するには、この項の次の手順に従います。
4. 追加 eBGP (ピア ASBR) ネイバーの設定を削除するには、次の手順のステップをすべて繰り返します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"><li>パスワードを入力します（要求された場合）。</li></ul>
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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 3	<b>router bgp as-number</b> 例： Device(config)# <b>router bgp 100</b>	BGP ルーティング プロセスを設定し、デバイスでルータ コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"><li><i>as-number</i> 引数は、デバイスを他の BGP デバイスに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。有効な番号は 0～65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512～65535 です。</li></ul>
ステップ 4	<b>address-family ipv4 vrf vrf-name</b> 例： Device(config-router)# <b>address-family ipv4 vrf vpn4</b>	特定の VPN のルートとその VPN の他のメンバのみが学習でき、VPN のメンバが相互に通信できるように、ASBR の MP-BGP セッションで識別される各 VRF を設定します。 <ul style="list-style-type: none"><li>アドレス ファミリ コンフィギュレーション モードを開始して、VRF のアドレスファミリを指定します。</li></ul>
ステップ 5	<b>no neighbor {ip-address   peer-group-name}</b> 例： Device(config-router-af)# <b>no neighbor 192.168.0.1</b>	ネイバー eBGP (ASBR) デバイスとの情報交換のための設定が削除されます。 <ul style="list-style-type: none"><li><i>ip-address</i> 引数には、ネイバーの IP アドレスを指定します。</li></ul>
ステップ 6	<b>exit-address-family</b> 例：	アドレス ファミリ コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
	Device (config-router-af) # <b>exit-address-family</b>	
ステップ 7	<b>end</b>  例 : Device (config-router-af) # <b>end</b>	特権 EXEC モードに戻ります。

## MPLS VPN InterAS オプションの設定の確認

InterAS オプション B の設定情報を確認するには、次のいずれかの作業を行います。

コマンド	目的
<b>ping ip-address source interface-type</b>	デバイスのアクセシビリティをチェックします。ループバック インターフェイスを使用して CE1 と CE2 間の接続を確認するには、このコマンドを使用します。
<b>show bgp vpnv4 unicast labels</b>	着信および発信 BGP ラベルを表示します。
<b>show mpls forwarding-table</b>	MPLS ラベル転送情報ベースの内容を表示します。
<b>show ip bgp</b>	BGP ルーティングテーブル内のエントリを表示します。
<b>show { ip   ipv6 } bgp [ vrf vrf-name ]</b>	VRF での BGP に関する情報を表示します。
<b>show ip route [ ip-address [ mask ] ] [ protocol ] vrf vrf-name</b>	ルーティング テーブルの現在の状態を表示します。ip-address 引数を使用して、CE1 に CE2 へのルートが含まれていることを確認します。CE1 から学習したルートを確認します。CE2 へのルートがリストされていることを確認します。
<b>show { ip   ipv6 } route vrf vrf-name</b>	VRF に関連付けられた IP ルーティング テーブルを表示します。ローカル CE ルータとリモート CE ルータのループバックアドレスが、PE ルータのルーティングテーブルに存在することを確認します。
<b>show running-config bgp</b>	BGP の実行コンフィギュレーションを表示します。
<b>show running-config vrf vrf-name</b>	VRF の実行コンフィギュレーションを表示します。

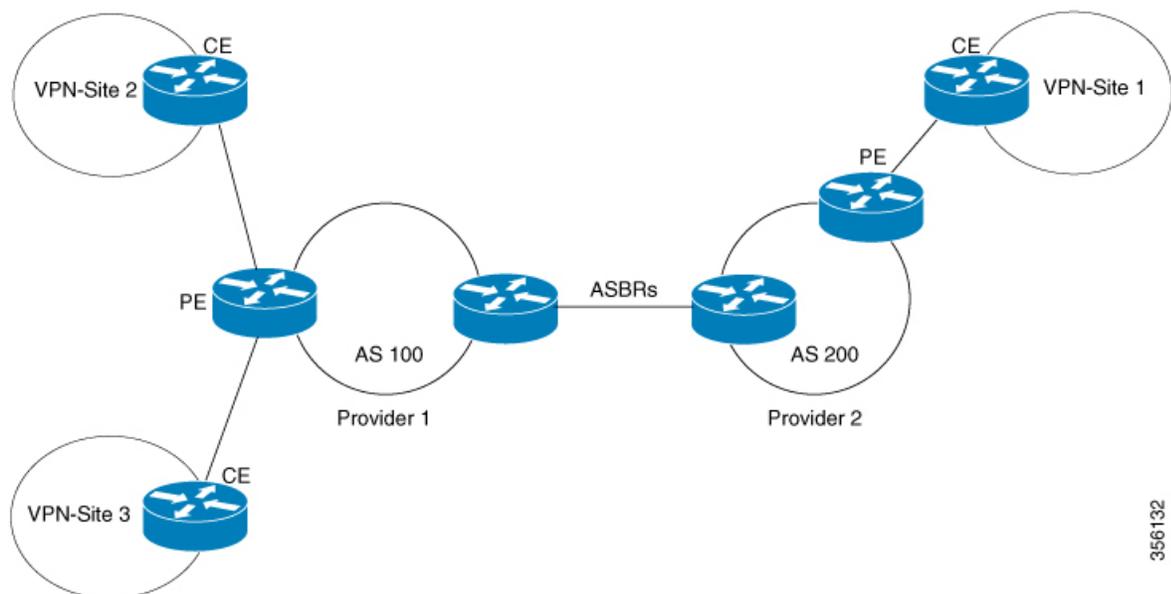
コマンド	目的
<code>show vrf vrf-name interface interface-type interface-id</code>	VRF に対して設定されるルート識別子 (RD) およびインターフェイスを検証します。
<code>trace destination [ vrf vrf-name ]</code>	パケットがその宛先に送信されるときに取るルートを検出します。 <b>trace</b> コマンドは、2つのルータが通信できない場合に問題の箇所を分離するのに役立ちます。

## MPLS VPN InterAS オプションの設定例

### InterAS オプション B

#### ネクストホップセルフ方式

図 8: ネクストホップセルフ方式を使用した **InterAS** オプション **B** のトポロジ



356132

## PE1 - P1 - ASBR1 の設定

PE1	P1	ASBR1
	<pre> interface Loopback0 ip address 4.1.1.2 255.255.255.255 ip ospf 1 area 0 interface GigabitEthernet1/0/4 no switchport ip address 10.10.1.2 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp ! interface GigabitEthernet1/0/23 no switchport ip address 10.20.1.1 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp </pre>	<pre> interface Loopback0 ip address 4.1.1.1 255.255.255.255 ip ospf 1 area 0 interface GigabitEthernet1/0/10 no switchport ip address 10.30.1.1 255.255.255.0 mpls bgp forwarding interface GigabitEthernet1/0/23 no switchport ip address 10.20.1.2 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp router ospf 1 router-id 4.1.1.1 nsr nsf redistribute bgp 200 passive-interface GigabitEthernet1/0/10 passive-interface Tunnel0 network 4.1.1.0 0.0.0.255 area 0 router bgp 200 bgp router-id 4.1.1.1 bgp log-neighbor-changes no bgp default ipv4-unicast no bgp default route-target filter neighbor 4.1.1.3 remote-as 200 neighbor 4.1.1.3 update-source Loopback0 neighbor 10.30.1.2 remote-as 300 ! address-family ipv4 neighbor 10.30.1.2 activate neighbor 10.30.1.2 send-label exit-address-family ! address-family vpnv4 neighbor 4.1.1.3 activate neighbor 4.1.1.3 send-community extended neighbor 4.1.1.3 next-hop-self neighbor 10.30.1.2 activate neighbor 10.30.1.2 send-community extended exit-address-family </pre>

PE1	P1	ASBR1
<pre> vrf definition Mgmt-vrf ! address-family ipv4 exit-address-family ! address-family ipv6 exit-address-family ! vrf definition vrf1 rd 200:1 route-target export 200:1 route-target import 200:1 route-target import 300:1 ! address-family ipv4 exit-address-family interface Loopback0 ip address 4.1.1.3 255.255.255.255 ip ospf 1 area 0 ! interface Loopback1 vrf forwarding vrf1 ip address 192.1.1.1 255.255.255.255 ip ospf 200 area 0 ! interface GigabitEthernet2/0/4 no switchport ip address 10.10.1.1 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp interface GigabitEthernet2/0/9 description to-IXIA-1:p8 no switchport vrf forwarding vrf1 ip address 192.2.1.1 255.255.255.0 ip ospf 200 area 0 router ospf 200 vrf vrf1 router-id 192.1.1.1 nsr nsf redistribute connected redistribute bgp 200 network 192.1.1.1 0.0.0.0 area 0 network 192.2.1.0 0.0.0.255 area 0 router ospf 1 router-id 4.1.1.3 nsr nsf redistribute connected router bgp 200 bgp router-id 4.1.1.3 bgp log-neighbor-changes neighbor 4.1.1.1 remote-as </pre>		

PE1	P1	ASBR1
<pre>200 neighbor 4.1.1.1 update-source Loopback0 ! address-family vpnv4 neighbor 4.1.1.1 activate neighbor 4.1.1.1 send-community extended exit-address-family ! address-family ipv4 vrf vrf1 redistribute connected redistribute ospf 200 maximum-paths ibgp 4 exit-address-family</pre>		

## ASBR2 – P2 – PE2 の設定

表 8:

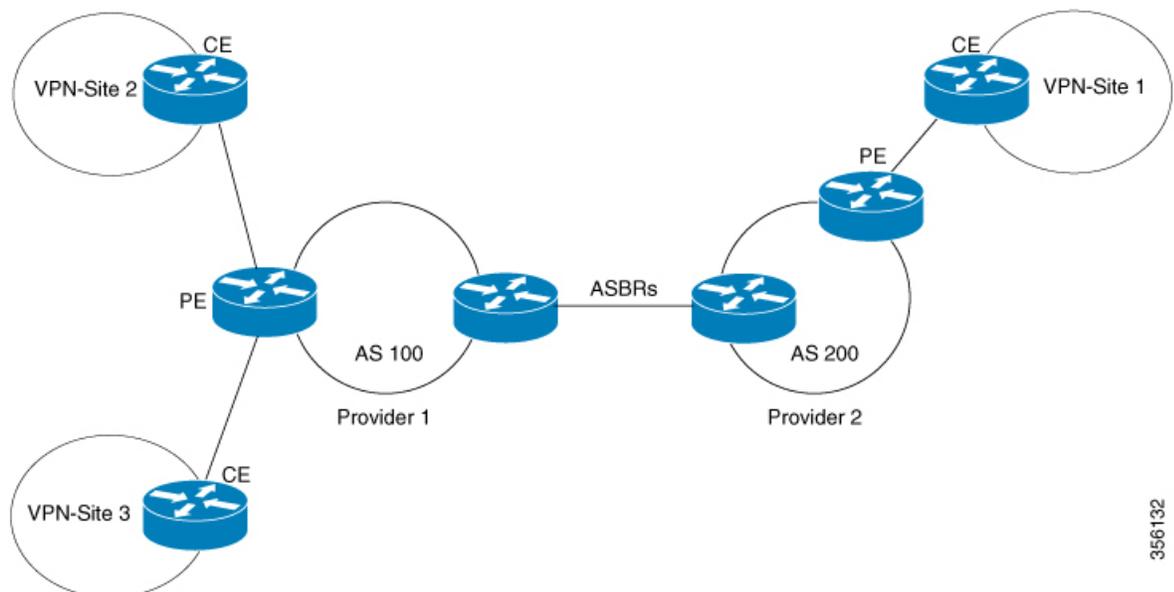
PE2	P2	ASBR2
	<pre> interface Loopback0 ip address 5.1.1.2 255.255.255.255 ip ospf 1 area 0 interface GigabitEthernet1/0/1 no switchport ip address 10.50.1.1 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp interface GigabitEthernet2/0/3 no switchport ip address 10.40.1.2 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp </pre>	<pre> interface Loopback0 ip address 5.1.1.1 255.255.255.255 ip ospf 1 area 0 ! interface GigabitEthernet1/0/37 no switchport ip address 10.30.1.2 255.255.255.0 mpls bgp forwarding interface GigabitEthernet1/0/47 no switchport ip address 10.40.1.1 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp router ospf 1 router-id 5.1.1.1 nsr nsf passive-interface GigabitEthernet1/0/37 passive-interface Tunnel0 network 5.1.1.0 0.0.0.255 area 0 ! router bgp 300 bgp router-id 5.1.1.1 bgp log-neighbor-changes no bgp default ipv4-unicast no bgp default route-target filter neighbor 5.1.1.3 remote-as 300 neighbor 5.1.1.3 update-source Loopback0 neighbor 10.30.1.1 remote-as 200 ! address-family ipv4 neighbor 10.30.1.1 activate neighbor 10.30.1.1 send-label exit-address-family ! address-family vpnv4 neighbor 5.1.1.3 activate neighbor 5.1.1.3 send-community extended neighbor 5.1.1.3 next-hop-self neighbor 10.30.1.1 activate neighbor 10.30.1.1 send-community extended exit-address-family </pre>

PE2	P2	ASBR2
<pre> vrf definition vrf1 rd 300:1 route-target export 300:1 route-target import 300:1 route-target import 200:1 ! address-family ipv4 exit-address-family interface Loopback0 ip address 5.1.1.3 255.255.255.255 ip ospf 1 area 0 ! interface Loopback1 vrf forwarding vrf1 ip address 193.1.1.1 255.255.255.255 ip ospf 300 area 0 interface GigabitEthernet1/0/1 no switchport ip address 10.50.1.2 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp ! interface GigabitEthernet1/0/2 no switchport vrf forwarding vrf1 ip address 193.2.1.1 255.255.255.0 ip ospf 300 area 0 router ospf 300 vrf vrf1 router-id 193.1.1.1 nsr nsf redistribute connected redistribute bgp 300 network 193.1.1.1 0.0.0.0 area 0 network 193.2.1.0 0.0.0.255 area 0 ! router ospf 1 router-id 5.1.1.3 nsr nsf redistribute connected router bgp 300 bgp router-id 5.1.1.3 bgp log-neighbor-changes neighbor 5.1.1.1 remote-as 300 neighbor 5.1.1.1 update-source Loopback0 ! address-family ipv4 neighbor 5.1.1.1 activate neighbor 5.1.1.1 send-label exit-address-family </pre>		

PE2	P2	ASBR2
<pre> ! address-family vpnv4 neighbor 5.1.1.1 activate neighbor 5.1.1.1 send-community extended exit-address-family ! address-family ipv4 vrf vrf1 redistribute connected redistribute ospf 300 maximum-paths ibgp 4 exit-address-family </pre>		

## IGP Redistribute Connected Subnet 方式

図 9: Redistribute Connected Subnet 方式を使用した InterAS オプション B のトポロジ



356132

## PE1 - P1 - ASBR1 の設定

PE1	P1	ASBR1
	<pre>interface Loopback0 ip address 4.1.1.2 255.255.255.255 ip ospf 1 area 0 interface GigabitEthernet1/0/4 no switchport ip address 10.10.1.2 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp ! interface GigabitEthernet1/0/23 no switchport ip address 10.20.1.1 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp</pre>	<pre>router ospf 1 router-id 4.1.1.1 nsr nsf redistribute connected passive-interface GigabitEthernet1/0/10 passive-interface Tunnel0 network 4.1.1.0 0.0.0.255 area 0 router bgp 200 bgp router-id 4.1.1.1 bgp log-neighbor-changes no bgp default ipv4-unicast no bgp default route-target filter neighbor 4.1.1.3 remote-as 200 neighbor 4.1.1.3 update-source Loopback0 neighbor 10.30.1.2 remote-as 300 ! address-family vpnv4 neighbor 4.1.1.3 activate neighbor 4.1.1.3 send-community extended neighbor 10.30.1.2 activate neighbor 10.30.1.2 send-community extended exit-address-family mpls ldp router-id Loopback0 force</pre>

## IGP Redistribute Connected Subnet 方式

PE1	P1	ASBR1
<pre> vrf definition Mgmt-vrf ! address-family ipv4 exit-address-family ! address-family ipv6 exit-address-family ! vrf definition vrf1 rd 200:1 route-target export 200:1 route-target import 200:1 route-target import 300:1 ! address-family ipv4 exit-address-family interface Loopback0 ip address 4.1.1.3 255.255.255.255 ip ospf 1 area 0 ! interface Loopback1 vrf forwarding vrf1 ip address 192.1.1.1 255.255.255.255 ip ospf 200 area 0 ! interface GigabitEthernet2/0/4 no switchport ip address 10.10.1.1 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp interface GigabitEthernet2/0/9 description to-IXIA-1:p8 no switchport vrf forwarding vrf1 ip address 192.2.1.1 255.255.255.0 ip ospf 200 area 0 router ospf 200 vrf vrf1 router-id 192.1.1.1 nsr nsf redistribute connected redistribute bgp 200 network 192.1.1.1 0.0.0.0 area 0 network 192.2.1.0 0.0.0.255 area 0 router ospf 1 router-id 4.1.1.3 nsr nsf redistribute connected router bgp 200 bgp router-id 4.1.1.3 bgp log-neighbor-changes neighbor 4.1.1.1 remote-as </pre>		

PE1	P1	ASBR1
<pre>200 neighbor 4.1.1.1 update-source Loopback0 ! address-family vpnv4 neighbor 4.1.1.1 activate neighbor 4.1.1.1 send-community extended exit-address-family ! address-family ipv4 vrf vrf1 redistribute connected redistribute ospf 200 maximum-paths ibgp 4 exit-address-family</pre>		

## ASBR2 – P2 – PE2 の設定

PE2	P2	ASBR2
	<pre> interface Loopback0 ip address 5.1.1.2 255.255.255.255 ip ospf 1 area 0 interface GigabitEthernet1/0/1 no switchport ip address 10.50.1.1 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp interface GigabitEthernet2/0/3 no switchport ip address 10.40.1.2 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp </pre>	<pre> router ospf 1 router-id 5.1.1.1 nsr nsf redistribute connected passive-interface GigabitEthernet1/0/10 passive-interface Tunnel0 network 5.1.1.0 0.0.0.255 area 0 router bgp 300 bgp router-id 5.1.1.1 bgp log-neighbor-changes no bgp default ipv4-unicast no bgp default route-target filter neighbor 5.1.1.3 remote-as 300 neighbor 5.1.1.3 update-source Loopback0 neighbor 10.30.1.1 remote-as 200 ! address-family vpnv4 neighbor 5.1.1.3 activate neighbor 5.1.1.3 send-community extended neighbor 10.30.1.1 activate neighbor 10.30.1.1 send-community extended exit-address-family mpls ldp router-id Loopback0 force </pre>

PE2	P2	ASBR2
<pre> vrf definition vrf1 rd 300:1 route-target export 300:1 route-target import 300:1 route-target import 200:1 ! address-family ipv4 exit-address-family interface Loopback0 ip address 5.1.1.3 255.255.255.255 ip ospf 1 area 0 ! interface Loopback1 vrf forwarding vrf1 ip address 193.1.1.1 255.255.255.255 ip ospf 300 area 0 interface GigabitEthernet1/0/1 no switchport ip address 10.50.1.2 255.255.255.0 ip ospf 1 area 0 mpls ip mpls label protocol ldp ! interface GigabitEthernet1/0/2 no switchport vrf forwarding vrf1 ip address 193.2.1.1 255.255.255.0 ip ospf 300 area 0 router ospf 300 vrf vrf1 router-id 193.1.1.1 nsr nsf redistribute connected redistribute bgp 300 network 193.1.1.1 0.0.0.0 area 0 network 193.2.1.0 0.0.0.255 area 0 ! router ospf 1 router-id 5.1.1.3 nsr nsf redistribute connected router bgp 300 bgp router-id 5.1.1.3 bgp log-neighbor-changes neighbor 5.1.1.1 remote-as 300 neighbor 5.1.1.1 update-source Loopback0 ! address-family ipv4 neighbor 5.1.1.1 activate neighbor 5.1.1.1 send-label </pre>		

PE2	P2	ASBR2
<pre> exit-address-family ! address-family vpnv4 neighbor 5.1.1.1 activate neighbor 5.1.1.1 send-community extended exit-address-family ! address-family ipv4 vrf vrf1 redistribute connected redistribute ospf 300 maximum-paths ibgp 4 exit-address-family </pre>		

## InterAS オプション AB

次に、各デバイスのトポロジと設定を表示する例を示します。

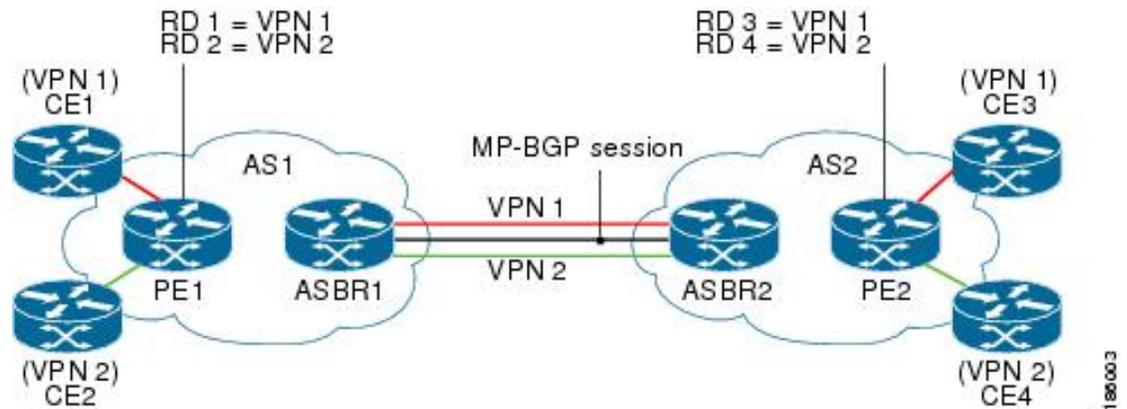


表 9:

PE1 の設定	P1 の設定	ASBR1 の設定	ASBR2 の設定	PE2 の設定
	<pre> interface Loopback0 ip address 2.2.2.2 255.255.255.255 ! interface TenGigabitEthernet1/1  ip address 10.1.1.2 255.255.255.0 mpls ip ! interface TenGigabitEthernet1/2  no ip address ! interface TenGigabitEthernet1/3  ip address 20.1.1.1 255.255.255.0 mpls ip ! router ospf 1 router-id 2.2.2.2  network 2.2.2.2 0.0.0.0 area 0 network 10.1.1.0 0.0.0.255 area 0 network 20.1.1.0 0.0.0.255 area 0 ! </pre>			

PE1 の設定	P1 の設定	ASBR1 の設定	ASBR2 の設定	PE2 の設定
<pre> ip vrf cust-1 rd 100:1 route-target export 100:1 route-target import 100:1 ! ip vrf cust-2 rd 100:2 route-target export 100:2 route-target import 100:2 ! interface Loopback0 ip address 1.1.1.1 255.255.255.255 ! interface Loopback1 ip address 11.11.11.11 255.255.255.255 ! interface Loopback2 ip address 12.12.12.12 255.255.255.255 ! ! interface HundredGigE1/0/1/1 no switchport ip address 10.1.1.1 255.255.255.0 mpls ip ! ! interface HundredGigE1/0/1/4 no switchport no ip address ! interface HundredGigE1/0/1/4.100 encapsulation dot1Q 100 ip vrf forwarding cust-1 ip address 11.1.1.1 255.255.255.0 ! interface HundredGigE1/0/1/4.101 encapsulation </pre>		<pre> ip vrf cust-1 rd 100:10001 route-target export 100:1 route-target import 100:1 route-target import 200:1 inter-as-hybrid next-hop 160.1.1.2 ! ip vrf cust-2 rd 100:20001 route-target export 100:2 route-target import 100:2 route-target import 200:2 inter-as-hybrid next-hop 170.1.1.2 ! ! interface Loopback0 ip address 3.3.3.3 255.255.255.255 ! ! interface TwentyFiveGigE1/0/3 no switchport ip address 20.1.1.2 255.255.255.0 mpls ip ! ! interface TwentyFiveGigE1/0/10.10 encapsulation dot1Q 10 ip address 150.1.1.1 255.255.255.0 mpls bgp forwarding ! interface TwentyFiveGigE1/0/10.20 encapsulation dot1Q 20 ip vrf forwarding cust-1 ip address 160.1.1.1 255.255.255.0 </pre>	<pre> ip vrf cust-1 rd 200:10001 route-target export 200:1 route-target import 200:1 route-target import 100:1 inter-as-hybrid next-hop 160.1.1.1 ! ip vrf cust-2 rd 200:20001 route-target export 200:2 route-target import 200:2 route-target import 100:2 inter-as-hybrid next-hop 170.1.1.1 ! ! interface Loopback0 ip address 4.4.4.4 255.255.255.255 ! ! interface TwentyFiveGigE1/0/2 no switchport ip address 30.1.1.1 255.255.255.0 mpls ip ! ! interface TwentyFiveGigE1/0/10.10 encapsulation dot1Q 10 ip address 150.1.1.2 255.255.255.0 mpls bgp forwarding ! interface TwentyFiveGigE1/0/10.20 encapsulation dot1Q 20 ip vrf forwarding cust-1 ip address 160.1.1.1 255.255.255.0 </pre>	<pre> ip vrf cust-1 rd 200:1 route-target export 200:1 route-target import 200:1 route-target import 100:1 ! ip vrf cust-2 rd 200:2 route-target export 200:2 route-target import 200:2 route-target import 100:2 ! interface Loopback0 ip address 5.5.5.5 255.255.255.255 ! interface Loopback1 ip address 55.55.55.55 255.255.255.255 ! interface Loopback2 ip address 56.56.56.56 255.255.255.255 ! ! interface HundredGigE1/0/1/1.200 encapsulation dot1Q 200 ip vrf forwarding cust-1 ip address 55.1.1.1 255.255.255.0 ! interface HundredGigE1/0/1/1.201 encapsulation dot1Q 201 ip vrf forwarding cust-2 ip address 56.1.1.1 255.255.255.0 ! interface HundredGigE1/0/1/1.3 no switchport ip address </pre>

PE1 の設定	P1 の設定	ASBR1 の設定	ASBR2 の設定	PE2 の設定
<pre> dot1Q 101 ip vrf forwarding   cust-2 ip address   12.1.1.1   255.255.255.0 ! router ospf 2 vrf   cust-1 router-id   11.11.11.11 network 11.1.1.0   0.0.0.255 area 0 network   11.11.11.11   0.0.0.0 area 0 ! router ospf 3 vrf   cust-2 router-id   12.12.12.12 network 12.1.1.0   0.0.0.255 area 0 network   12.12.12.12   0.0.0.0 area 0 ! router ospf 1 router-id 1.1.1.1  network 1.1.1.1   0.0.0.0   area 0 network 10.1.1.0   0.0.0.255 area 0 ! router bgp 100 bgp router-id   1.1.1.1 bgp log-neighbor-   changes neighbor 3.3.3.3   remote-as 100 neighbor 3.3.3.3   update-   source Loopback0 ! address-family   vpv4 neighbor 3.3.3.3   activate neighbor 3.3.3.3   send-   community   extended   exit-address-family ! address-family   ipv4 vrf cust-1   redistribute   connected </pre>		<pre> ! interface   TwentyFiveGigE1/0/10.30 ! encapsulation   dot1Q 30 ip vrf forwarding   cust-2 ip address   170.1.1.1   255.255.255.0 ! router ospf 1 router-id 3.3.3.3 network 3.3.3.3   0.0.0.0 area 0 network 20.1.1.0   0.0.0.255 area 0 ! router bgp 100 bgp router-id   3.3.3.3 bgp log-neighbor-   changes neighbor 1.1.1.1   remote-   as 100 neighbor   150.1.1.2   remote-as 200 ! address-family   ipv4   redistribute   connected neighbor 1.1.1.1   activate neighbor   150.1.1.2   activate   exit-address-family ! address-family   vpv4 neighbor 1.1.1.1   activate neighbor 1.1.1.1   send-   community both neighbor   150.1.1.2   activate neighbor   150.1.1.2   send-   community both neighbor   150.1.1.2   inter- as-hybrid   exit-address-family ! address-family   ipv4 </pre>	<pre> 160.1.1.2 255.255.255.0 ! interface   TwentyFiveGigE1/0/10.30 ! encapsulation   dot1Q 30 ip vrf forwarding   cust-2 ip address   170.1.1.2   255.255.255.0 ! router ospf 1 router-id 4.4.4.4 network 4.4.4.4   0.0.0.0   area 0 network 30.1.1.0   0.0.0.255   area 0 ! router bgp 200 bgp router-id   4.4.4.4 bgp log-neighbor-   changes neighbor 5.5.5.5   remote-   as 200 neighbor   150.1.1.1   remote-as 100 ! address-family   ipv4 neighbor 5.5.5.5   activate neighbor   150.1.1.1   activate   exit-address-family ! address-family   vpv4 neighbor 5.5.5.5   activate neighbor 5.5.5.5   send-community   both neighbor   150.1.1.1   activate neighbor   150.1.1.1   send-community   both neighbor   150.1.1.1   inter-as-hybrid ! exit-address-family </pre>	<pre> 30.1.1.2 255.255.255.0 mpls ip ! router ospf 2 vrf   cust-1 router-id   55.55.55.55 network 55.1.1.0   0.0.0.255   area 0 network   55.55.55.55   0.0.0.0   area 0 ! router ospf 3 vrf   cust-2 router-id   56.56.56.56 network 56.1.1.0   0.0.0.255 area 0 network   56.56.56.56   0.0.0.0 area 0 ! router ospf 1 router-id 5.5.5.5 network 5.5.5.5   0.0.0.0   area 0 network 30.1.1.0   0.0.0.255   area 0 ! router bgp 200 bgp router-id   5.5.5.5 bgp   log-neighbor-changes neighbor 4.4.4.4   remote-as 200 neighbor 4.4.4.4   update-source   Loopback0 ! address-family   vpv4 neighbor 4.4.4.4   activate neighbor 4.4.4.4   send-community   extended   exit-address-family ! address-family   ipv4 vrf cust-1   redistribute   connected   redistribute ospf   2   maximum-paths </pre>

PE1 の設定	P1 の設定	ASBR1 の設定	ASBR2 の設定	PE2 の設定
<pre> redistribute ospf  2 maximum-paths ibgp 4 exit-address-family ! address-family ipv4 vrf cust-2 redistribute connected redistribute ospf  3 maximum-paths ibgp 4 exit-address-family </pre>		<pre> vrf cust-1 redistribute connected exit-address-family ! address-family ipv4 vrf cust-2 redistribute connected exit-address-family ! </pre>	<pre> ! address-family ipv4 vrf cust-1 redistribute connected exit-address-family ! address-family ipv4 vrf cust-2 redistribute connected exit-address-family ! </pre>	<pre> ibgp 4 exit-address-family ! address-family ipv4 vrf cust-2 redistribute connected redistribute ospf  3 maximum-paths ibgp 4 exit-address-family ! </pre>

## MPLS VPN InterAS オプションに関するその他の参考資料

### 関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「MPLS コマンド」の項を参照してください。 <i>Command Reference (Catalyst 9300 Series Switches)</i>

## MPLS VPN InterAS オプションの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Gibraltar 16.11.1	MPLS VPN InterAS オプション B	InterAS オプションは、iBGP および eBGP ピアリングを使用して、異なる AS 内の VPN が相互に通信できるようにします。InterAS オプション B ネットワークでは、ASBR ポートは、MPLS トラフィックを受信できる 1 つ以上のインターフェイスによって接続されます。

リリース	機能	機能情報
Cisco IOS XE Amsterdam 17.3.1	MPLS VPN InterAS オプション AB	MPLS VPN InterAS オプション AB では、ルータ上でグローバルに有効になっている単一のマルチプロトコルボーダー ゲートウェイ プロトコル (MP-BGP) セッションを使用して、異なる自律システムを相互接続できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。





## 第 8 章

# MPLS over GRE の設定

- [MPLS over GRE の前提条件](#) (133 ページ)
- [GRE を介した MPLS の制約事項](#) (133 ページ)
- [MPLS over GRE に関する情報](#) (134 ページ)
- [GRE を介した MPLS の設定方法](#) (136 ページ)
- [MPLS over GRE の設定例](#) (137 ページ)
- [MPLS over GRE に関するその他の参考資料](#) (141 ページ)
- [MPLS over GRE の機能情報](#) (141 ページ)

## MPLS over GRE の前提条件

次のルーティングプロトコルが正しく設定され、動作していることを確認します。

- ラベル配布プロトコル (LDP) : MPLS ラベル配布の場合。
- コアデバイス P1-P2 間のルーティングプロトコル (ISIS または OSPF)
- PE1-P1 と PE2-P2 間の MPLS
- 入力トラフィックは MPLS ネットワークから IP コアに入り、出力トラフィックは IP コアを出て MPLS ネットワークに入るため、プロトコル境界を通過するときに QoS グループ値を使用して QoS ポリシーを定義することをお勧めします。

## GRE を介した MPLS の制約事項

- GRE トンネリング :
  - L2VPN over mGRE および L3VPN over mGRE はサポートされていません。
  - トンネル送信元は、ループバックインターフェイスまたはレイヤ3インターフェイスにのみできます。これらのインターフェイスは、物理インターフェイスまたは EtherChannel のいずれかです。

- トンネルインターフェイスは、スタティックルート、Enhanced Interior Gateway Routing Protocol (EIGRP)、および Open Shortest Path First (OSPF) ルーティングプロトコルをサポートしています。
- GRE オプション：シーケンシング、チェックサム、およびソースルートはサポートされていません。
- IPv6 Generic Routing Encapsulation (GRE) はサポートされていません。
- Carrier Supporting Carrier (CSC) はサポートされていません。
- トンネルの送信元をサブインターフェイスにすることはできません。

## MPLS over GRE に関する情報

MPLS over GRE 機能は、非 MPLS ネットワーク経由でマルチプロトコル ラベル スイッチング (MPLS) パケットのトンネリングを行うためのメカニズムを提供します。この機能を使用すると、非 MPLS ネットワーク間の Generic Routing Encapsulation (GRE) トンネルを作成できます。MPLS パケットは、GRE トンネルパケット内でカプセル化され、カプセル化されたパケットは、GRE トンネルを経由して非 MPLS ネットワークを通ります。GRE トンネルパケットを非 MPLS ネットワークの反対側で受信すると、GRE トンネルパケットヘッダーが削除され、内部の MPLS パケットが最終的な宛先に転送されます。GRE トンネルのエンドポイント間のコアネットワークは ISIS または OSPF ルーティングプロトコルを使用しますが、GRE トンネルは OSPF または EIGRP を使用します。

## PE-to-PE トンネリング

プロバイダーエッジ間 (PE-to-PE) トンネリング設定によって、非 MPLS ネットワーク間の複数のカスタマーネットワークをスケーラブルな方法で接続できます。この設定を使用して、複数のカスタマーネットワーク宛のトラフィックは、単一の Generic Routing Encapsulation (GRE) トンネルから多重化されます。



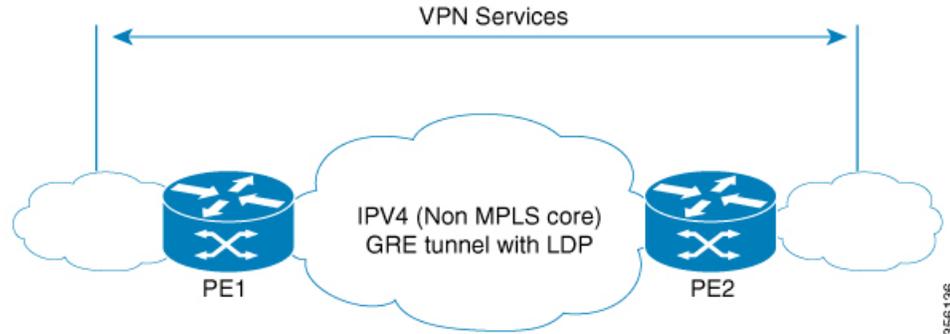
(注) 類似したスケーラブルではない代替方法は、別個の GRE トンネルから各カスタマーネットワークに接続することです (たとえば、1つのカスタマー ネットワークを各 GRE トンネルに接続します)。

非 MPLS ネットワークのいずれかの側にある PE デバイスは、(非 MPLS ネットワーク内で動作している) ルーティングプロトコルを使用して、非 MPLS ネットワークのもう一方の側にある PE デバイスについて学習します。PE デバイス間に確立された学習ルートは、メインまたはデフォルトのルーティングテーブルに格納されます。

反対方向の PE デバイスは、OSPF または EIGRP を使用して、PE デバイスの背後にあるカスタマーネットワークに関連付けられたルートについて学習します。これらの学習ルートは、非 MPLS ネットワークには認識されません。

次の図は、非 MPLS ネットワークにまたがる GRE トンネルを介した、ある PE デバイスから別の PE デバイスへのエンドツーエンド IP コアを示しています。

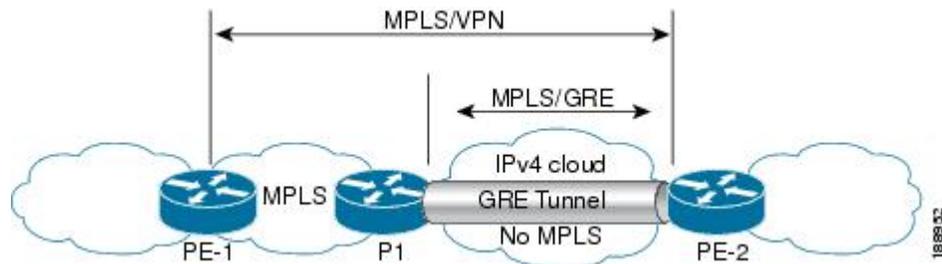
図 10: PE-to-PE トンネリング



## P-to-PE トンネリング

Provider-to-Provider Edge (P-to-PE) トンネリング設定によって、非マルチプロトコルラベルスイッチング (MPLS) ネットワークで PE デバイス (P1) を MPLS セグメント (PE-2) に接続できます。この設定では、非 MPLS ネットワークの一方の側宛の MPLS トラフィックは、単一の Generic Routing Encapsulation (GRE) トンネル経由で送信されます。

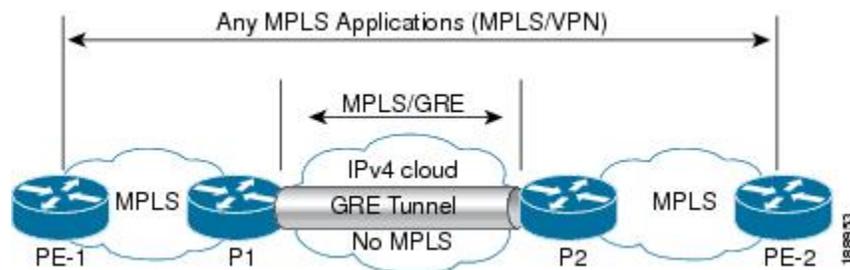
図 11: P-to-PE トンネリング



## P-to-P トンネリング

下図に示すように、Provider-to-Provider (P-to-P) 設定によって、非マルチプロトコルラベルスイッチング (MPLS) ネットワークで 2 つの MPLS セグメント (P1 から P2) を接続できます。この設定では、非 MPLS ネットワークの一方の側宛の MPLS トラフィックは、単一の Generic Routing Encapsulation (GRE) トンネル経由で送信されます。

図 12: P-to-P トンネリング



## GRE を介した MPLS の設定方法

次の項では、GRE を介した MPLS のさまざまな設定手順について説明します。

### MPLS over GRE トンネル インターフェイスの設定

MPLS over GRE 機能を設定するには、非 MPLS ネットワークにまたがる GRE トンネルを作成する必要があります。次の手順は、GRE トンネルの両方の終端にあるデバイスで実行する必要があります。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# configure terminal	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 3	<b>interface tunnel <i>tunnel-number</i></b> 例： Device(config)# interface tunnel 1	トンネル インターフェイスを作成します。続いて、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<b>ip address <i>ip-address mask</i></b> 例： Device(config-if)# ip address 10.0.0.1 255.255.255.0	トンネル インターフェイスに IP アドレスを割り当てます。

	コマンドまたはアクション	目的
ステップ 5	<b>tunnel source</b> <i>source-address</i> 例 :  Device(config-if)# tunnel source 10.1.1.1	トンネル送信元 IP アドレスを指定します。
ステップ 6	<b>tunnel destination</b> <i>destination-address</i> 例 :  Device(config-if)# tunnel destination 10.1.1.2	トンネル宛先 IP アドレスを指定します。
ステップ 7	<b>mpls ip</b> 例 :  Device(config-if)# mpls ip	トンネルの物理インターフェイスでマルチプロトコル ラベル スイッチング (MPLS) を有効にします。
ステップ 8	<b>end</b> 例 :  Device(config-if)# end	特権 EXEC モードに戻ります。

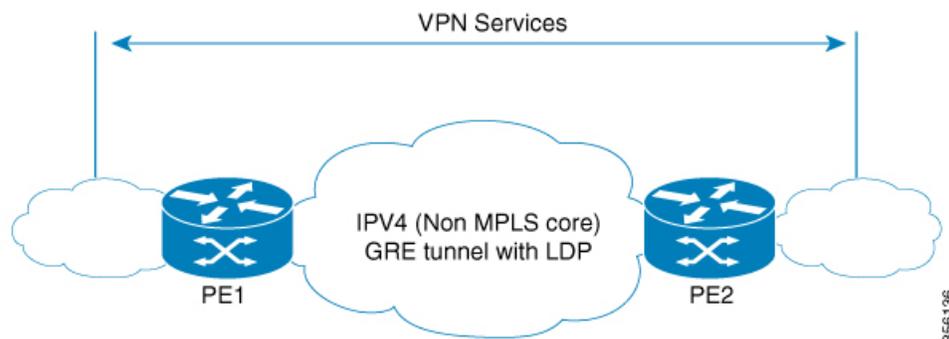
## MPLS over GRE の設定例

次の項では、GRE を介した MPLS のさまざまな設定例について説明します。

### 例 : PE-to-PE トンネリング

次に、2つのプロバイダーエッジ (PE) デバイスでの基本的な MPLS 設定を示します。PE-to-PE トンネリングは、GRE トンネルを使用して非 MPLS ネットワーク経由でトラフィックを送信します。

図 13: PE-to-PE トンネリングのトポロジ



356136

### PE1 の設定

```
!  
mpls ip  
!  
interface loopback 10  
ip address 11.2.2.2 255.255.255.255  
ip router isis  
!  
interface GigabitEthernet 1/1/1  
ip address 1.1.1.1 255.255.255.0  
ip router isis  
!  
interface Tunnel 1  
ip address 10.0.0.1 255.255.255.0  
ip ospf 1 are 0  
tunnel source 11.2.2.2  
tunnel destination 11.1.1.1  
mpls ip  
!  
interface Vlan701  
ip address 65.1.1.1 255.255.255.0  
ip ospf 1 area 0  
!
```

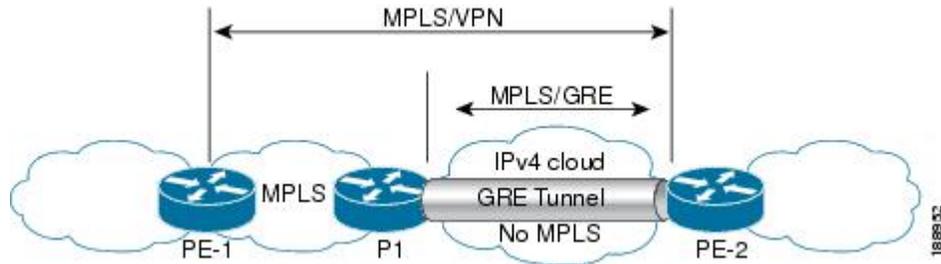
### PE2 の設定

```
!  
mpls ip  
!  
interface loopback 10  
ip address 11.1.1.1 255.255.255.255  
ip router isis  
!  
interface GigabitEthernet 1/1/1  
ip address 2.1.1.1 255.255.255.0  
ip router isis  
!  
interface Tunnel 1  
ip address 10.0.0.2 255.255.255.0  
ip ospf 1 are 0  
tunnel source 11.1.1.1  
tunnel destination 11.2.2.2  
mpls ip  
!  
interface Vlan701  
ip address 75.1.1.1 255.255.255.0  
ip ospf 1 area 0  
!
```

## 例 : P-to-PE トンネリング

次に、2つのプロバイダー (P) デバイス (P-to-PE トンネリング) での基本的な MPLS 設定を示します。P-to-PE トンネリングでは、GRE トンネルを使用して非 MPLS ネットワーク経由でトラフィックが送信されます。

図 14: P-to-PE トンネリングのトポロジ



### PE1 の設定

```
!
mpls ip
!
interface GigabitEthernet 1/1/1
ip address 3.1.1.2 255.255.255.0
ip ospf 1 are 0
mpls ip
!
interface Vlan701
ip address 75.1.1.1 255.255.255.0
ip ospf 1 area 0
!
```

### P1 の設定

```
!
mpls ip
!
interface loopback 10
ip address 11.2.2.2 255.255.255.255
ip router isis
!
interface GigabitEthernet 1/1/1
ip address 1.1.1.1 255.255.255.0
ip router isis
!
interface GigabitEthernet 1/1/2
ip address 3.1.1.1 255.255.255.0
ip ospf 1 are 0
mpls ip
!
interface Tunnel 1
ip address 10.0.0.1 255.255.255.0
ip ospf 1 are 0
tunnel source 11.2.2.2
tunnel destination 11.1.1.1
mpls ip
!
```

### PE2 の設定

```
!
mpls ip
!
```

## 例 : P-to-P トンネリング

```

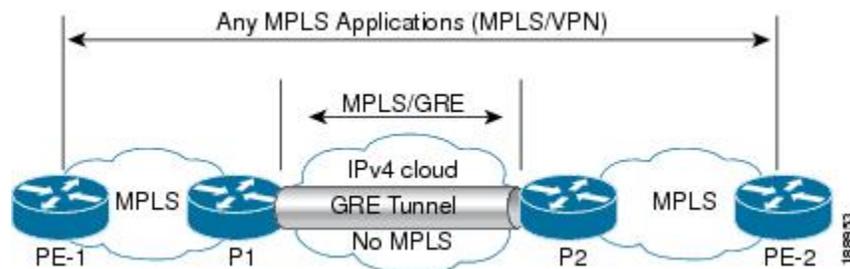
interface loopback 10
ip address 11.1.1.1 255.255.255.255
ip router isis
!
interface GigabitEthernet 1/1/1
ip address 2.2.1.1 255.255.255.0
ip router isis
!
interface Tunnel 1
ip address 10.0.0.2 255.255.255.0
ip ospf 1 are 0
tunnel source 11.1.1.1
tunnel destination 11.2.2.2
mpls ip
!
interface Vlan701
ip address 75.1.1.1 255.255.255.0
ip ospf 1 area 0
!

```

## 例 : P-to-P トンネリング

次に、2つのプロバイダー (P) デバイス (P-to-PE トンネリング) での基本的な MPLS 設定の例を示します。P-to-PE トンネリングでは、GRE トンネルを使用して非 MPLS ネットワーク経由でトラフィックが送信されます。

図 15: P-to-P トンネリングのトポロジ



## P1 の設定

```

!
interface Loopback10
ip address 10.1.1.1 255.255.255.255
ip router isis
!
interface Tunnel10
ip address 10.10.10.1 255.255.255.252
ip ospf 1 area 0
mpls ip
tunnel source 10.1.1.1
tunnel destination 10.2.1.1

```

## P2 の設定

```

!
interface Tunnel10

```

```
ip address 10.10.10.2 255.255.255.252
ip ospf 1 area 0
mpls ip
tunnel source 10.2.1.1
tunnel destination 10.1.1.1
!
interface Loopback10
ip address 10.2.1.1 255.255.255.255
ip router isis
```

## MPLS over GRE に関するその他の参考資料

### 関連資料

関連項目	マニュアルタイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	の「MPLS コマンド」の項を参照してください。 <i>Command Reference (Catalyst 9300 Series Switches)</i>

## MPLS over GRE の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、[www.cisco.com/go/cfn](http://www.cisco.com/go/cfn) に移動します。Cisco.com のアカウントは必要ありません。

表 10: MPLS over GRE の機能情報

機能名	リリース	変更内容
MPLS over GRE	Cisco IOS XE Gibraltar 16.11.1	<p>GRE を介した MPLS 機能は、Generic Routing Encapsulation (GRE) トンネルを作成することで、非 MPLS ネットワーク経由でマルチプロトコル ラベル スイッチング (MPLS) パケットのトンネリングを行うためのメカニズムを提供します。MPLS パケットは、GRE トンネル パケット内でカプセル化され、カプセル化されたパケットは、GRE トンネルを経由して非 MPLS ネットワークを通ります。GRE トンネル パケットを非 MPLS ネットワークの反対側で受信すると、GRE トンネル パケット ヘッダーが削除され、内部の MPLS パケットが最終的な宛先に転送されます。</p>



## 第 9 章

# GRE を介した MPLS レイヤ 2 VPN の設定

- [GRE を介した MPLS レイヤ 2 VPN に関する情報 \(143 ページ\)](#)
- [GRE を介した MPLS レイヤ 3 VPN の設定方法 \(145 ページ\)](#)
- [GRE を介した MPLS レイヤ 2 VPN の設定例 \(146 ページ\)](#)
- [GRE を介した MPLS レイヤ 2 VPN の設定に関するその他の参考資料 \(147 ページ\)](#)
- [GRE を介した MPLS レイヤ 2 VPN の設定の機能情報 \(147 ページ\)](#)

## GRE を介した MPLS レイヤ 2 VPN に関する情報

GRE を介した MPLS レイヤ 2 VPN 機能は、非 MPLS ネットワーク経由でマルチプロトコルラベルスイッチング (MPLS) パケットのトンネリングを行うためのメカニズムを提供します。この機能を使用すると、非 MPLS ネットワーク間の Generic Routing Encapsulation (GRE) トンネルを作成できます。MPLS パケットは、GRE トンネルパケット内でカプセル化され、カプセル化されたパケットは、GRE トンネルを経由して非 MPLS ネットワークを通ります。GRE トンネルパケットを非 MPLS ネットワークの反対側で受信すると、GRE トンネルパケットヘッダーが削除され、内部の MPLS パケットが最終的な宛先に転送されます。

GRE を介した MPLS レイヤ 2 VPN を設定するには、仮想プライベート LAN サービス (VPLS) または EoMPLS (Ethernet over MPLS) を設定する必要があります。

## トンネリング設定のタイプ

次の項では、サポートされているさまざまなタイプのトンネリング設定について説明します。

### PE-to-PE トンネリング

プロバイダーエッジ間 (PE-to-PE) トンネリング設定によって、非 MPLS ネットワーク間の複数のカスタマーネットワークをスケーラブルな方法で接続できます。この設定を使用して、複数のカスタマーネットワーク宛のトラフィックは、単一の GRE トンネルから多重化されます。

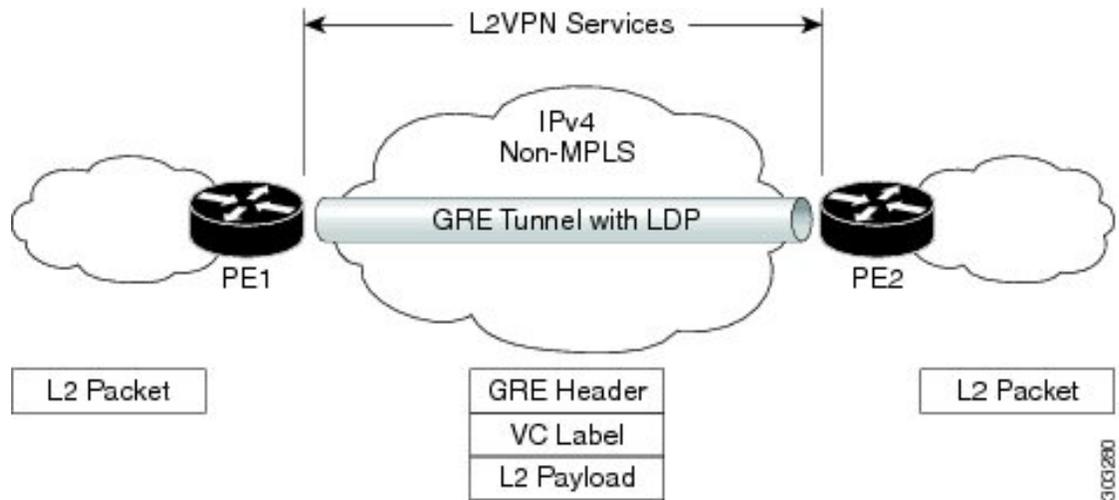
非 MPLS ネットワークのいずれかの側にある PE デバイスは、(非 MPLS ネットワーク内で動作している) ルーティングプロトコルを使用して、非 MPLS ネットワークのもう一方の側に

ある PE デバイスについて学習します。PE デバイス間に確立された学習ルートは、メインまたはデフォルトのルーティング テーブルに格納されます。

反対方向の PE デバイスは、ボーダー ゲートウェイ プロトコル (BGP) を使用して、PE デバイスの背後にあるカスタマーネットワークに関連付けられたルートについて学習します。これらの学習ルートは、非 MPLS ネットワークには認識されません。

図 16: PE-to-PE トンネリング (144 ページ) は、非 MPLS ネットワークにまたがる GRE トンネルを介した、PE デバイス間のエンドツーエンド IP コアを示しています。

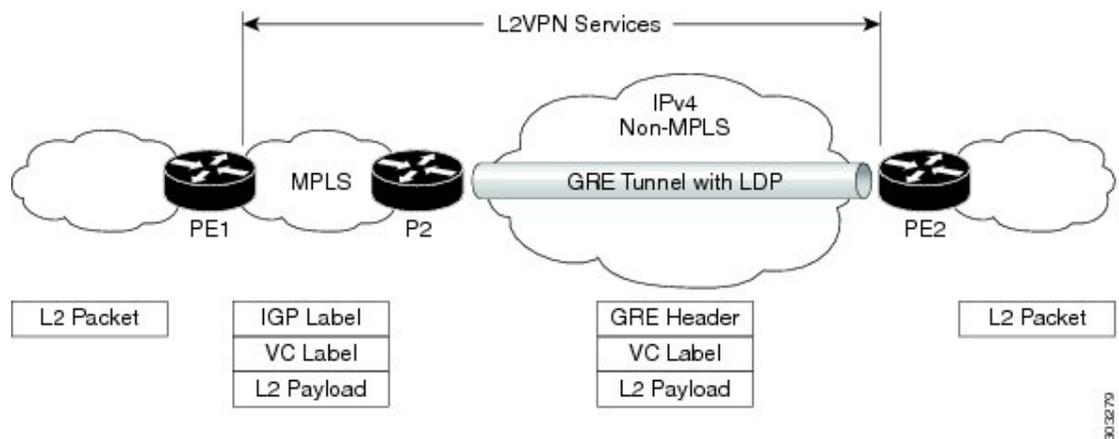
図 16: PE-to-PE トンネリング



## P-to-PE トンネリング

図 17: P-to-PE トンネリング (144 ページ) に、非 MPLS ネットワーク上で 2 つの MPLS セグメント (P2 から PE2) を接続する方法を示します。この設定では、非 MPLS ネットワークの一方の側宛の MPLS トラフィックは、単一の GRE トンネル経由で送信されます。

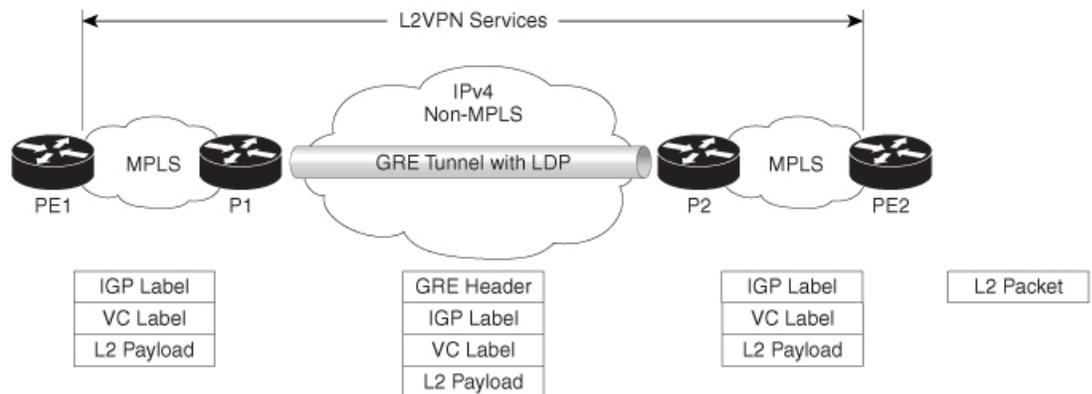
図 17: P-to-PE トンネリング



## P-to-P トンネリング

図 18: P-to-P トンネリング (145 ページ) に、非 MPLS ネットワーク上で 2 つの MPLS セグメント (P1 ~ P2) を接続する方法を示します。この設定では、非 MPLS ネットワークの一方の側宛の MPLS トラフィックは、単一の GRE トンネル経由で送信されます。

図 18: P-to-P トンネリング



356234

## GRE を介した MPLS レイヤ 3 VPN の設定方法

GRE を介した MPLS 機能を設定するには、非 MPLS ネットワークにまたがる GRE トンネルを作成する必要があります。GRE トンネルの両端にあるデバイスで、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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 3	<b>interface tunnel tunnel-number</b> 例： Device(config)# <b>interface tunnel 1</b>	トンネル インターフェイスを作成します。続いて、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<b>ip address ip-address mask</b> 例： Device(config-if)# <b>ip address 10.0.0.1 255.255.255.0</b>	トンネル インターフェイスに IP アドレスを割り当てます。

	コマンドまたはアクション	目的
ステップ 5	<b>tunnel source</b> <i>source-address</i> 例： Device(config-if)# <b>tunnel source</b> 10.1.1.1	トンネルの送信元 IP アドレスを設定します。
ステップ 6	<b>tunnel destination</b> <i>destination-address</i> 例： Device(config-if)# <b>tunnel destination</b> 10.1.1.2	トンネルの宛先 IP アドレスを設定します。
ステップ 7	<b>mpls ip</b> 例： Device(config-if)# <b>mpls ip</b>	トンネルの物理インターフェイスでの MPLS を有効にします。
ステップ 8	<b>end</b> 例： Device(config-if)# <b>end</b>	特権 EXEC モードに戻ります。

## GRE を介した MPLS レイヤ 2 VPN の設定例

次の項では、GRE を介した MPLS レイヤ 2 VPN の設定例を示します。

### 例：非 MPLS ネットワークにまたがる GRE トンネルの設定

次に、非 MPLS ネットワークにまたがる汎用的な GRE トンネルの設定例を示します。

次に、PE1 デバイスのトンネルの設定例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface Tunnel 1
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# tunnel source 10.0.0.1
Device(config-if)# tunnel destination 10.0.0.2
Device(config-if)# ip ospf 1 area 0
Device(config-if)# mpls ip
```

次に、PE2 デバイスのトンネルの設定例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface Tunnel 1
Device(config-if)# ip address 10.1.1.2 255.255.255.0
Device(config-if)# tunnel source 10.0.0.2
Device(config-if)# tunnel destination 10.0.0.1
Device(config-if)# ip ospf 1 area 0
Device(config-if)# mpls ip
```

## GRE を介した MPLS レイヤ 2 VPN の設定に関するその他の参考資料

### 関連資料

関連項目	マニュアルタイトル
VPLS の設定	詳細については、「VPLSに関する情報」を参照してください。
Ethernet-over-MPLS (EoMPLS) および疑似回線冗長性 (PWR) の設定	詳細については、次を参照してください。 <a href="#">Ethernet-over-MPLS の設定方法 (42 ページ)</a>

## GRE を介した MPLS レイヤ 2 VPN の設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 11: GRE を介した MPLS レイヤ 2 VPN の設定に関する機能情報

機能名	リリース	機能情報
GRE を介した MPLS レイヤ 2 VPN	Cisco IOS XE Gibraltar 16.12.1	GRE を介した MPLS レイヤ 2 VPN 機能は、非 MPLS ネットワーク経由で MPLS パケットのトンネリングを行うためのメカニズムを提供します。





## 第 10 章

# GRE を介した MPLS レイヤ 3 VPN の設定

- [GRE を介した MPLS レイヤ 3 VPN の前提条件](#) (149 ページ)
- [GRE を介した MPLS レイヤ 3 VPN の制約事項](#) (150 ページ)
- [GRE を介した MPLS レイヤ 3 VPN に関する情報](#) (150 ページ)
- [GRE を介した MPLS レイヤ 3 VPN の設定方法](#) (152 ページ)
- [GRE を介した MPLS レイヤ 3 VPN の設定例](#) (153 ページ)
- [GRE を介した MPLS レイヤ 3 VPN の設定の機能情報](#) (159 ページ)

## GRE を介した MPLS レイヤ 3 VPN の前提条件

- マルチプロトコル ラベル スイッチング (MPLS) バーチャルプライベート ネットワーク (VPN) が設定されていることを確認します。
- 次のルーティングプロトコルが設定されていることを確認します。
  - Label Distribution Protocol (LDP; ラベル配布プロトコル) : MPLS ラベル配布の場合。
  - マルチプロトコル ボーダー ゲートウェイ プロトコル (MP-BGP) : VPN ルートとラベル配布の場合。
- プロトコル境界を横断する QoS ポリシーを定義するには、Quality of Service (QoS) グループ値を使用することを推奨します。入力トラフィックは MPLS ネットワークから IP コアに入り、出力トラフィックは IP コアを出て MPLS ネットワークに入るため、QoS グループ値が必要です。
- Generic Routing Encapsulation (GRE) トンネルを設定する前に、IP アドレスを指定してループバック インターフェイス (Virtual Routing Forwarding (VRF) に接続されていない) インターフェイスを設定します。IPv4 アドレスを持つこのダミー ループバック インターフェイスは、IPv4 転送用に内部で作成されたトンネル インターフェイスを有効にします。VRF に接続されておらず IPv4 アドレスが設定されているインターフェイスがシステムに 1 つ以上ある場合は、ループバック インターフェイスを設定する必要はありません。

## GRE を介した MPLS レイヤ 3 VPN の制約事項

GRE を介した MPLS レイヤ 3 VPN 機能では、次のものはサポートされません。

- トンネルインターフェイスに設定されている QoS サービスポリシー



(注) トンネルインターフェイスに設定されている QoS サービスポリシーはサポートされませんが、物理インターフェイスまたはサブインターフェイスに設定されている QoS サービスポリシーはサポートされます。

- シーケンシング、チェックサム、およびソースルートなどの GRE オプション
- IPv6 GRE の設定
- Carrier Supporting Carrier (CSC) などの拡張機能

## GRE を介した MPLS レイヤ 3 VPN に関する情報

GRE を介した MPLS レイヤ 3 VPN 機能は、非 MPLS ネットワーク経由で MPLS パケットのトンネリングを行うためのメカニズムを提供します。この機能を使用すると、非 MPLS ネットワーク間の GRE トンネルを作成できます。MPLS パケットは、GRE トンネルパケット内でカプセル化され、カプセル化されたパケットは、GRE トンネルを経由して非 MPLS ネットワークを通ります。GRE トンネルパケットを非 MPLS ネットワークの反対側で受信すると、GRE トンネルパケットヘッダーが削除され、内部の MPLS パケットが最終的な宛先に転送されます。

### トンネリング設定のタイプ

次の項では、サポートされているさまざまなタイプのトンネリング設定について説明します。

#### PE-to-PE トンネリング

プロバイダーエッジ間 (PE-to-PE) トンネリング設定によって、非 MPLS ネットワーク間の複数のカスタマーネットワークをスケーラブルな方法で接続できます。この設定を使用して、複数のカスタマーネットワーク宛のトラフィックは、単一の GRE トンネルから多重化されます。

**図 19: PE-to-PE トンネリング (151 ページ)** に示すように、PE デバイスは、VRF 番号を非 MPLS ネットワークの各側にあるカスタマーエッジ (CE) デバイスに割り当てます。

PE デバイスは、ボーダーゲートウェイプロトコル (BGP)、Open Shortest Path First (OSPF)、または Routing Information Protocol (RIP) などのルーティングプロトコルを、CE デバイスの

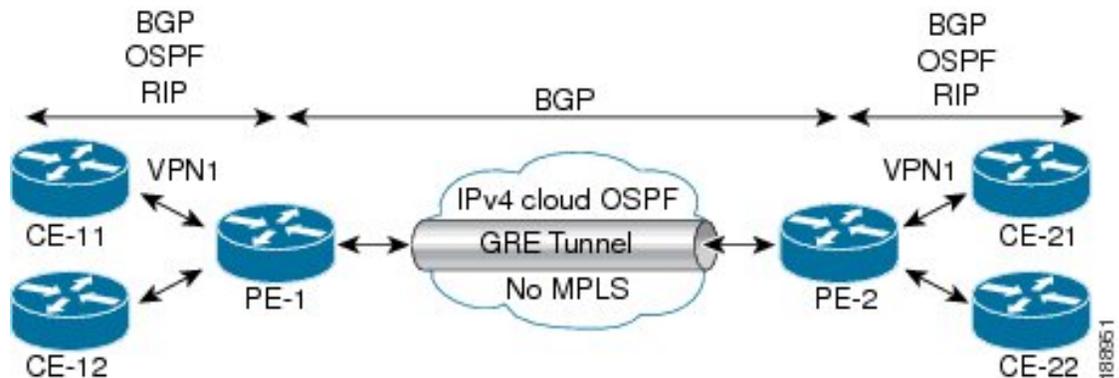
背後にある IP ネットワークを学習するために使用します。CE デバイスの背後にある IP ネットワークへのルートは、関連する CE デバイスの VRF ルーティングテーブルに格納されます。

非 MPLS ネットワークの一方の側にある PE デバイスは（非 MPLS ネットワーク内で動作している）ルーティングプロトコルを使用して、非 MPLS ネットワークのもう一方の側にある PE デバイスについて学習します。PE デバイス間に確立された学習ルートは、メインまたはデフォルトのルーティングテーブルに格納されます。

反対方向の PE デバイスは、BGP を使用して、PE デバイスの背後にあるカスタマーネットワークに関連付けられたルートについて学習します。これらの学習ルートは、非 MPLS ネットワークには認識されません。

図 19: PE-to-PE トンネリング (151 ページ) は、非 MPLS ネットワークにまたがる GRE トンネル経由で BGP ネイバー（反対方向の PE デバイス）へのスタティックルートを定義する BGP を示しています。BGP ネイバーによって学習されたルートには GRE トンネルのネクストホップが含まれているため、すべてのカスタマーネットワークトラフィックが GRE トンネルを使用して送信されます。

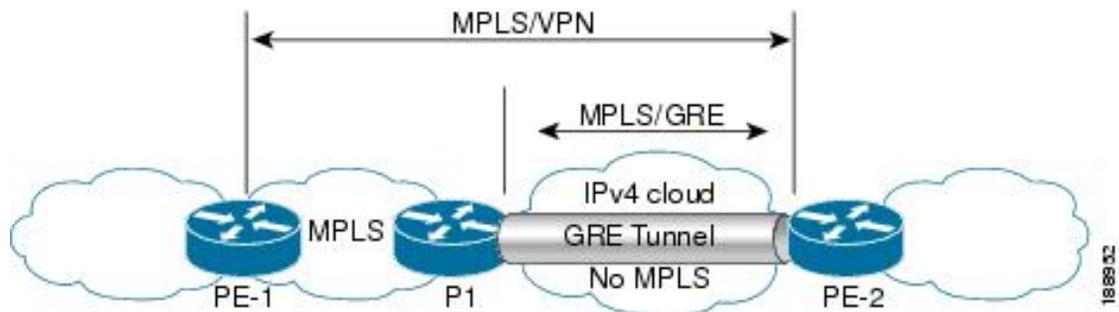
図 19: PE-to-PE トンネリング



## P-to-PE トンネリング

図 20: P-to-PE トンネリング (151 ページ) に、非 MPLS ネットワーク上で 2 つの MPLS セグメント (P2 から PE2) を接続する方法を示します。この設定では、非 MPLS ネットワークの一方の側宛の MPLS トラフィックは、単一の GRE トンネル経由で送信されます。

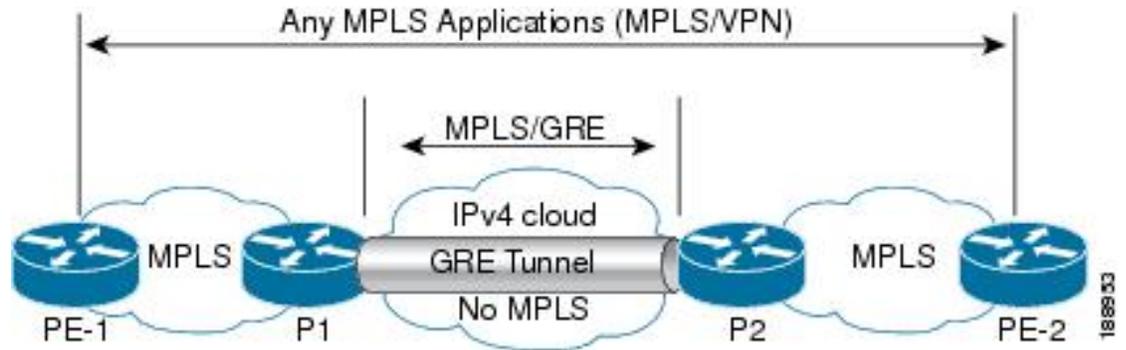
図 20: P-to-PE トンネリング



## P-to-P トンネリング

図 21 : P-to-P トンネリング (152 ページ) に、非 MPLS ネットワーク上で 2 つの MPLS セグメント (P1 ~ P2) を接続する方法を示します。この設定では、非 MPLS ネットワークの一方の側宛の MPLS トラフィックは、単一の GRE トンネル経由で送信されます。

図 21 : P-to-P トンネリング



## GRE を介した MPLS レイヤ 3 VPN の設定方法

GRE を介した MPLS 機能を設定するには、非 MPLS ネットワークにまたがる GRE トンネルを作成する必要があります。GRE トンネルの両端にあるデバイスで、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例 : Device# <b>configure terminal</b>	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 3	<b>interface tunnel tunnel-number</b> 例 : Device(config)# <b>interface tunnel 1</b>	トンネル インターフェイスを作成します。続いて、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<b>ip address ip-address mask</b> 例 : Device(config-if)# <b>ip address 10.0.0.1 255.255.255.0</b>	トンネル インターフェイスに IP アドレスを割り当てます。

	コマンドまたはアクション	目的
ステップ 5	<b>tunnel source</b> <i>source-address</i> 例： Device(config-if)# <b>tunnel source</b> 10.1.1.1	トンネルの送信元 IP アドレスを設定します。
ステップ 6	<b>tunnel destination</b> <i>destination-address</i> 例： Device(config-if)# <b>tunnel destination</b> 10.1.1.2	トンネルの宛先 IP アドレスを設定します。
ステップ 7	<b>mpls ip</b> 例： Device(config-if)# <b>mpls ip</b>	トンネルの物理インターフェイスでの MPLS を有効にします。
ステップ 8	<b>end</b> 例： Device(config-if)# <b>end</b>	特権 EXEC モードに戻ります。

## GRE を介した MPLS レイヤ 3 VPN の設定例

次の項では、GRE を介した MPLS レイヤ 3 VPN のさまざまな設定例を示します。

### 例：GRE を介した MPLS レイヤ 3 VPN（PE-to-PE トンネリング）の設定

次に、PE1 から PE2 へのレイヤ 3 VPN および GRE トンネルを設定する例を示します（[図 19: PE-to-PE トンネリング（151 ページ）](#) を参照）。

次に、PE1 にループバック インターフェイスを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface Loopback10
Device(config-if)# ip address 209.165.200.225 255.255.255.255
Device(config-if)# end
```

次に、PE2 にループバック インターフェイスを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface Loopback3
Device(config-if)# ip address 209.165.202.129 255.255.255.255
Device(config-if)# end
```

次に、PE1 の IGP でループバックをアドバタイズする例を示します。

```
Device> enable
Device# configure terminal
```

## 例：GRE を介した MPLS レイヤ 3 VPN (PE-to-PE トンネリング) の設定

```
Device(config)# router ospf 10
Device(config-router)# router-id 198.51.100.10
Device(config-router)# end
```

次に、GRE トンネルを設定し、トンネルで異なる IGP インスタンスを設定し、PE1 のトンネルで MPLS を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface Tunnel13
Device(config-if)# ip address 203.0.113.200 255.255.255.248
Device(config-if)# ip ospf 11 area 0
Device(config-if)# mpls ip
Device(config-if)# tunnel source 209.165.200.225
Device(config-if)# tunnel destination 209.165.202.129
Device(config-if)# end
```

次に、GRE トンネルを設定し、トンネルで異なる IGP インスタンスを設定し、PE2 のトンネルで MPLS を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface Tunnel131
Device(config-if)# ip address 203.0.113.201 255.255.255.248
Device(config-if)# ip ospf 11 area 0
Device(config-if)# mpls ip
Device(config-if)# tunnel source 209.165.202.129
Device(config-if)# tunnel destination 209.165.200.225
Device(config-if)# end
```

次に、トンネルに設定された IGP インスタンスで BGP の PE1 ループバック IP をアドバタイズする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# router ospf 11
Device(config-router)# router-id 198.51.100.11
Device(config-router)# network 192.0.1.1 0.0.0.0 area 0
Device(config-router)# end
```

次に、トンネルに設定された IGP インスタンスで BGP の PE2 ループバック IP をアドバタイズする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# router ospf 11
Device(config-router)# router-id 203.0.113.201
Device(config-router)# network 192.0.1.1 0.0.0.0 area 0
Device(config-router)# end
```

次に、CE1 が接続されている PE1 に VRF を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# vrf definition vrf-1
Device (config-vrf)# rd 1:1
Device (config-vrf)# address-family ipv4
Device (config-vrf-af)# route-target import 1:2
Device (config-vrf-af)# route-target export 1:1
Device(config-vrf)# end
```

次に、CE2 が接続されている PE2 に VRF を設定する例を示します。

```
Device> enable
Device# configure terminal
Device (config)# vrf definition vrf-1
Device (config-vrf)# rd 2:2
Device (config-vrf)# address-family ipv4
Device (config-vrf-af)# route-target import 1:1
Device (config-vrf-af)# route-target export 1:2
Device (config-vrf)# end
```

次に、PE1-CE1 インターフェイスを設定する例を示します。

```
Device> enable
Device# configure terminal
Device (config)# int po14.1
Device (config-subif)# encapsulation dot1Q 10
Device (config-subif)# vrf forwarding vrf-1
Device (config-subif)# ip address 14.2.1.1 255.255.255.0
Device (config-subif)# end
```

次に、PE2-CE2 インターフェイスを設定する例を示します。

```
Device> enable
Device# configure terminal
Device (config)# int po24.1
Device (config-subif)# encapsulation dot1Q 10
Device (config-subif)# vrf forwarding vrf-1
Device (config-subif)# ip address 24.2.1.1 255.255.255.0
Device (config-subif)# end
```

次に、PE1-CE1 外部ボーダー ゲートウェイ プロトコル (EBGP) を設定する例を示します。

```
Device> enable
Device# configure terminal
Device (config)# router bgp 65040
Device (config-router)# address-family ipv4 vrf vrf-1
Device (config-router-af)# neighbor 14.2.1.2 remote-as 65041
Device (config-router-af)# neighbor 14.2.1.2 activate
Device (config-router-af)# exit-address-family
Device (config-router)# end
```

次に、PE2-CE2 EBGP を設定する例を示します。

```
Device> enable
Device# configure terminal
Device (config)# router bgp 65040
Device (config-router)# address-family ipv4 vrf vrf-1
Device (config-router-af)# neighbor 24.2.1.2 remote-as 65041
Device (config-router-af)# neighbor 24.2.1.2 activate
Device (config-router-af)# exit-address-family
Device (config-router)# end
```

次に、PE1 に PE1-PE2 MP-BGP を設定する例を示します。

```
Device> enable
Device# configure terminal
Device (config)# router bgp 65040
Device (config-router)# neighbor 192.0.2.1 remote-as 65040
Device (config-router)# neighbor 192.0.2.1 update-source Loopback0
Device (config-router)# address-family ipv4
Device (config-router-af)# neighbor 192.0.2.1 activate
Device (config-router-af)# exit
Device (config-router)# address-family vpnv4
Device (config-router-af)# neighbor 192.0.2.1 activate
```

## 例：GRE を介した MPLS レイヤ 3 VPN (P-to-PE トンネリング) の設定

```
Device (config-router-af)# neighbor 192.0.2.1 send-community both
Device (config-router-af)# exit
Device (config-router)# end
```

## 例：GRE を介した MPLS レイヤ 3 VPN (P-to-PE トンネリング) の設定

次に、PE デバイス (PE1 と PE2) および MPLS セグメント (P1) でレイヤ 3 VPN を設定し、PE1 から P1、PE2 への GRE トンネルを設定する例を示します (図 20: P-to-PE トンネリング (151 ページ) を参照)。

次に、PE1 の GRE トンネルにループバック インターフェイスを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface Loopback4
Device(config-if)# ip address 209.165.200.230 255.255.255.255
Device(config-if)# end
```

次に、P1 の GRE トンネルにループバック インターフェイスを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface Loopback100
Device(config-if)# ip address 209.165.200.235 255.255.255.255
Device(config-if)# end
```

次に、PE1-P1 からインターフェイスを設定し、IGP を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface Port-channel11
Device(config-if)# no switchport
Device(config-if)# ip address 209.165.201.1 255.255.255.248
Device(config-if)# ip ospf 10 area 0
Device(config-if)# end
```

次に、P1-PE1 からインターフェイスを設定し、IGP を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface Port-channel1
Device(config-if)# no switchport
Device(config-if)# ip address 209.165.201.2 255.255.255.248
Device(config-if)# ip broadcast-address 209.165.201.31
Device(config-if)# ip ospf 10 area 0
Device(config-if)# end
```

次に、PE1 の IGP でループバックをアドバタイズする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# router ospf 10
Device(config-router)# router-id 198.51.100.10
Device(config-router)# network 209.165.200.230 0.0.0.0 area 0
Device(config-router)# end
```

次に、P1 の IGP でループバックをアドバタイズする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# router ospf 10
Device(config-router)# router-id 198.51.100.20
Device(config-router)# network 209.165.200.235 0.0.0.0 area 0
Device(config-router)# end
```

次に、GRE トンネルを設定し、トンネルで IGP インスタンスを設定し、PE1 のトンネルで MPLS を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface Tunnel111
Device(config-if)# ip address 209.165.202.140 255.255.255.248
Device(config-if)# ip ospf 11 area 0
Device(config-if)# mpls ip
Device(config-if)# tunnel source 209.165.200.230
Device(config-if)# tunnel destination 209.165.200.235
Device(config-if)# end
```

次に、GRE トンネルを設定し、トンネルで IGP インスタンスを設定し、P1 のトンネルで MPLS を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface Tunnel111
Device(config-if)# ip address 209.165.202.141 255.255.255.248
Device(config-if)# ip ospf 11 area 0
Device(config-if)# mpls ip
Device(config-if)# tunnel source 209.165.200.235
Device(config-if)# tunnel destination 209.165.200.230
Device(config-if)# end
```

次に、PE1 上のトンネルの IGP インスタンスで BGP の PE ループバック IP をアドバタイズする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface Tunnel111
Device(config)# router ospf 11
Device(config-router)# router-id 198.51.100.11
Device(config-router)# network 192.0.1.1 0.0.0.0 area 0
Device(config-router)# end
```

次に、PE2-P1 からインターフェイスを設定し、IGP および MPLS を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface Port-channel12
Device(config-if)# no switchport
Device(config-if)# ip address 209.165.201.1 255.255.255.248
Device(config-if)# ip ospf 11 area 0
Device(config-if)# mpls ip
Device(config-if)# end
```

次に、P1-PE2 からインターフェイスを設定し、IGP を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface Port-channel12
Device(config-if)# no switchport
Device(config-if)# ip address 209.165.201.2 255.255.255.248
```

## 例：GRE を介した MPLS レイヤ 3 VPN (P-to-PE トンネリング) の設定

```
Device(config-if)# ip ospf 11 area 0
Device(config-if)# mpls ip
Device(config-if)# end
```

次に、CE1 が接続されている PE1 で VRF を作成する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# vrf definition vrf-1
Device (config-vrf)# rd 1:1
Device (config-vrf)# address-family ipv4
Device (config-vrf-af)# route-target import 1:2
Device (config-vrf-af)# route-target export 1:1
Device (config-vrf-af)# exit
Device (config-vrf)# end
```

次に、CE2 が接続されている PE2 で VRF を作成する例を示します。

```
Device> enable
Device# configure terminal
Device (config)# vrf definition vrf-1
Device (config-vrf)# rd 2:2
Device (config-vrf)# address-family ipv4
Device (config-vrf-af)# route-target import 1:1
Device (config-vrf-af)# route-target export 1:2
Device (config-vrf-af)# exit
Device (config-vrf)# end
```

次に、PE1-CE1 インターフェイスを設定する例を示します。

```
Device> enable
Device# configure terminal
Device (config)# int po14.1
Device (config-subif)# encapsulation dot1Q 10
Device (config-subif)# vrf forwarding vrf-1
Device (config-subif)# ip address 14.2.1.1 255.255.255.0
Device (config-subif)# exit
Device (config)# end
```

次に、PE2-CE2 インターフェイスを設定する例を示します。

```
Device> enable
Device# configure terminal
Device (config)# int po24.1
Device (config-subif)# encapsulation dot1Q 10
Device (config-subif)# vrf forwarding vrf-1
Device (config-subif)# ip address 24.2.1.1 255.255.255.0
Device (config-subif)# exit
Device (config)# end
```

次に、PE1-CE1 EBGP を設定する例を示します。

```
Device> enable
Device# configure terminal
Device (config)# router bgp 65040
Device (config-router)# address-family ipv4 vrf vrf-1
Device (config-router-af)# neighbor 14.2.1.2 remote-as 65041
Device (config-router-af)# neighbor 14.2.1.2 activate
Device (config-router-af)# exit-address-family
Device (config-router)# end
```

次に、PE2-CE2 EBGP を設定する例を示します。

```
Device> enable
Device# configure terminal
```

```
Device (config)# router bgp 65040
Device (config-router)# address-family ipv4 vrf vrf-1
Device (config-router-af)# neighbor 24.2.1.2 remote-as 65041
Device (config-router-af)# neighbor 24.2.1.2 activate
Device (config-router-af)# exit-address-family
Device (config-router)# end
```

次に、PE1 に PE1-PE2 MP-BGP を設定する例を示します。

```
Device> enable
Device# configure terminal
Device (config)# router bgp 65040
Device (config-router)# neighbor 192.0.2.1 remote-as 65040
Device (config-router)# neighbor 192.0.2.1 update-source Loopback0
Device (config-router)# address-family ipv4
Device (config-router-af)# neighbor 192.0.2.1 activate
Device (config-router-af)# exit
Device (config-router)# address-family vpnv4
Device (config-router-af)# neighbor 192.0.2.1 activate
Device (config-router-af)# neighbor 192.0.2.1 send-community both
Device (config-router-af)# exit
Device (config-router)# end
```

次に、PE2 に PE2-PE1 MP-BGP を設定する例を示します。

```
Device> enable
Device# configure terminal
Device (config)# router bgp 65040
Device (config-router)# neighbor 192.0.1.1 remote-as 65040
Device (config-router)# neighbor 192.0.1.1 update-source Loopback0
Device (config-router)# address-family ipv4
Device (config-router-af)# neighbor 192.0.1.1 activate
Device (config-router-af)# exit
Device (config-router)# address-family vpnv4
Device (config-router-af)# neighbor 192.0.1.1 activate
Device (config-router-af)# neighbor 192.0.1.1 send-community both
Device (config-router-af)# exit
Device (config-router)# end
```

## GRE を介した MPLS レイヤ 3 VPN の設定の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレーンで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 12: GRE を介した MPLS レイヤ 3 VPN の設定に関する機能情報

機能名	リリース	機能情報
GRE を介した MPLS レイヤ 3 VPN	Cisco IOS XE Gibraltar 16.12.1	GRE を介した MPLS レイヤ 3 VPN 機能は、非 MPLS ネットワーク経由で MPLS パケットのトンネリングを行うためのメカニズムを提供します。





# 第 11 章

## MPLS QoS の設定

- [MPLS QoS の前提条件](#) (161 ページ)
- [MPLS QoS の制約事項](#) (161 ページ)
- [MPLS QoS の概要](#) (162 ページ)
- [MPLS QoS の設定方法](#) (164 ページ)
- [MPLS QoS の設定例](#) (171 ページ)
- [その他の参考資料](#) (174 ページ)
- [QoS MPLS EXP の機能履歴](#) (174 ページ)

### MPLS QoS の前提条件

- スイッチはマルチプロトコルラベルスイッチング (MPLS) のプロバイダーエッジ (PE) またはプロバイダー (P) ルータとして設定する必要があります。この設定には、有効なラベルプロトコルと基礎となる IP ルーティングプロトコルの設定を含めることができます。

### MPLS QoS の制約事項

- MPLS の分類とマーキングは、運用可能な MPLS ネットワーク内でのみ実行できます。
- パケットが入力で IP タイプ オブ サービス (ToS) またはサービス クラス (CoS) によって分類された場合は、出力で MPLS EXP によって再分類できません (インポジションケース)。ただし、パケットが入力で MPLS によって分類された場合は、出力で IP ToS、CoS、または Quality of Service (QoS) グループによって再分類できます (ディスポジションケース)。
- プロトコルの境界を越えてトラフィックに QoS を適用するには、QoS グループを使用します。入力トラフィックを分類し、QoS グループに割り当てることができます。その後、出力で QoS グループを使用して分類し、QoS を適用することができます。

- パケットが MPLS でカプセル化されている場合は、IP などの他のプロトコルの MPLS ペイロードをチェックして分類またはマーキングすることはできません。MPLS EXP マーキングのみが MPLS によってカプセル化されたパケットに影響します。
- ショートパイプモードは、MPLS ネットワーク経由のパケット転送に対してはサポートされていません。ユニフォームモードとパイプモードのいずれかのモードを使用してパケットを転送できます。

## MPLS QoS の概要

ここでは、MPLS QoS について詳しく説明します。

### MPLS QoS の概要

ネットワーク管理者は MPLS QoS 機能を使用することで、差別化したサービスを MPLS ネットワーク上で提供できます。送信対象の IP パケットごとに適用する CoS を指定することによって、さまざまなネットワーク要件を満たすことができます。各パケットのヘッダーに IP precedence ビットを設定することによって、IP パケットに対して異なるサービスクラスを確立できます。MPLS ネットワークでの分類、再マーキング、およびキューイングは、MPLS EXP ビットを介して実行されます。MPLS ネットワークでは、パケットが MPLS EXP フィールドのマーキングによって区別され、重み付けランダム早期検出 (WRED) の設定に応じて適切に処理されます。

MPLS パケットの MPLS EXP フィールドでは、次のことができます。

- **トラフィックの分類**

分類プロセスでマーキングするトラフィックが選択されます。分類は、トラフィックを複数の優先順位レベル、つまり、サービスクラスに分割することによりこのプロセスを実施します。トラフィック分類は、クラスベースの QoS プロビジョニングのプライマリ コンポーネントです。詳細については、『Classifying Network Traffic』を参照してください。

- **トラフィックのポリシングとマーキング**

ポリシングでは、設定されたレートを上回るトラフィックが廃棄されるか、別のドロップレベルにマーキングされます。トラフィックのマーキングは、パケットフローを特定してそれらを区別する方法です。パケットマーキングを利用すれば、ネットワークを複数の優先プライオリティ レベルまたはサービスクラスに分割することができます。詳細については、『Marking Network Traffic』を参照してください。

- **Queueing**

キューイングは、トラフィックの輻輳の防止に役立ちます。これには、プライオリティレベル キューイング、重み付けテールドロップ (WTD)、スケジューリング、シェーピング、および重み付けランダム早期検出 (WRED) 機能が含まれます。

## MPLS 実験フィールド

MPLS Experimental ビット (EXP) フィールドは、ノードからパケットに付加される QoS 処理 (Per-Hop Behavior) を定義するために使用可能な MPLS ヘッダー内の 3 ビット フィールドです。IP ネットワークでは、DiffServ コード ポイント (DSCP) (6 ビット フィールド) でクラスとドロップ優先順位が定義されます。EXP ビットは、IP DSCP でエンコードされた情報の一部を伝達するためにも、ドロップ優先順位をエンコードするためにも使用できます。

デフォルトで、Cisco IOS ソフトウェアは、IP パケットの DSCP または IP precedence の上位 3 ビットを MPLS ヘッダー内の EXP フィールドにコピーします。このアクションは、MPLS ヘッダーが初めて IP パケットに付加されたときに実行されます。ただし、DSCP または IP precedence と EXP ビットとの間のマッピングを定義することによって、EXP フィールドを設定することもできます。このマッピングは、**set mpls experimental** コマンドまたは **police** コマンドを使用して設定されます。詳細については、「MPLS EXP の分類とマーキングの方法」を参照してください。



- (注) **set ip dscp** により設定されたポリシーマップは、プロバイダーエッジデバイスではサポートされません。MPLS ラベルインポジションノードのポリシーアクションは、**set mpls experimental imposition** 値に基づく必要があります。ただし、入力インターフェイスと出力インターフェイスの両方がレイヤ 3 ポートである場合、アクション **set ip dscp** が指定されたポリシーマップはサポートされます。

MPLS EXP マーキング操作を実行するには、テーブルマップを使用します。入力ポリシー内の別のトラフィック クラスに QoS グループを割り当て、テーブルマップを使用して QoS グループを出力ポリシー内の DSCP および EXP マーキングに変換することをお勧めします。

ネットワーク経由で伝送されるパケットの IP precedence フィールド値をサービスプロバイダーが変更したくない場合は、MPLS EXP フィールド値を使用して IP パケットを分類してマーキングできます。

MPLS EXP フィールド用の複数の値を選択することにより、ネットワーク輻輳が発生した場合に重大なパケットが優先されるようにそのようなパケットをマーキングすることができます。

WRED はネットワーク トラフィックを監視し、共通ネットワークおよびインターネットワークのボトルネックで輻輳を回避します。WRED は、インターフェイスが輻輳状態になると、優先順位の低いトラフィックを選択的に破棄できます。この機能により、サービスクラスごとに異なるパフォーマンス特性を提供することもできます。

MPLS ネットワーク上でパケットを転送する方法は 2 つあります。

均一モード：パケット転送の均一モードは、QoS の 1 つのレイヤで動作します。入力側のプロバイダーエッジが、着信 IP パケットの DSCP 情報を、インポーズされたラベルの MPLS EXP ビットにコピーし、IP プレシデンスビットが MPLS EXP フィールドにマッピングされます。EXP ビットは、コアを通過する際に、ネットワークの中間デバイスで変更される場合と変更されない場合があります。出力側のプロバイダーエッジが、EXP ビットを新しく公開された IP パケットの DSCP ビットにコピーします。

パイプモード：パケット転送のパイプモードは、QoS の2つのレイヤで動作します。データの元の QoS。コアを通過しても変更されません。コアごとの QoS。元の IP パケットの QoS とは別の QoS です。DSCP 情報は、パケットが MPLS ネットワークを通過するときに保存および格納されます。MPLS EXP ラベルは入力時に PE によって適用されますが、IP プレシデンスビットは保存されません。出力では、元の IP プレシデンス値が保持されます。

## MPLS EXP の分類とマーキングのメリット

QoS EXP Matching 機能を使用すると、マルチプロトコル ラベル スイッチング (MPLS) Experimental ビット (EXP ビット) フィールドを変更することで、ネットワークトラフィックを分類、マーキング、およびキューイングできます。ネットワーク経路で伝送されるパケットの IP precedence フィールド値をサービス プロバイダーが変更したくない場合は、MPLS EXP フィールド値を使用して IP パケットを分類してマーキングできます。

MPLS EXP フィールド用の複数の値を選択することにより、ネットワーク輻輳が発生した場合に重大なパケットが優先されるようにそのようなパケットをマーキングすることができます。

## MPLS QoS の設定方法

この項では、MPLS QoS の設定方法について説明します。

### MPLS カプセル化パケットの分類

**match mpls experimental topmost** コマンドを使用すれば、MPLS ドメイン内のパケット EXP 値に基づくトラフィック クラスを定義できます。これらのクラスは、**police** コマンドを使用して EXP トラフィックをマーキングするサービス ポリシーを定義するために使用できます。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： <code>Device&gt; enable</code>	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： <code>Device# configure terminal</code>	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 3	<b>class-map [match-all   match-any]</b> <i>class-map-name</i> 例：	トラフィックを指定したクラスにマッチングするために使用するクラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	<code>Device(config)# class-map exp3</code>	クラス マップ名を入力します。
ステップ 4	<b>match mpls experimental topmost</b> <i>mpls-exp-value</i> 例 : <code>Device(config-cmap)# match mpls experimental topmost 3</code>	一致基準を指定します。 (注) <b>match mpls experimental topmost</b> コマンドは、最上位ラベルヘッダー内の EXP 値に基づいてトラフィックを分類します。
ステップ 5	<b>end</b> 例 : <code>Device(config-cmap)# end</code>	(任意) 特権 EXEC モードに戻ります。

## 最も外側のラベルでの MPLS EXP のマーキング

インポートされたラベル エントリの MPLS EXP フィールドの値を設定するには、次の作業を実行します。

### 始める前に

インポジションでの MPLS パケットのマーキングが IP ToS または CoS フィールドに基づく入力分類で使用されます。



- (注)
- IP インポジション マーキングでは、デフォルトで、IP precedence 値が MPLS EXP 値にコピーされます。
  - プロバイダーエッジのイーグレスポリシーは、入力時の再マーキングポリシーがある場合にのみ、MPLS EXP クラスの一致により機能します。入力時のプロバイダーエッジは IP インターフェイスであり、デフォルトでは DSCP 値のみが信頼されています。入力時の再マーキングポリシーを設定しない場合、キューイングのラベルは MPLS EXP 値ではなく DSCP 値に基づいて生成されます。ただし、中継プロバイダールータは MPLS インターフェイス上で動作するため、入力時の再マーキングポリシーを設定しなくても機能します。
  - **set mpls experimental imposition** コマンドは、新しいまたは追加の MPLS ラベルが追加されたパケットに対してのみ機能します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# configure terminal	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 3	<b>policy-map policy-map-name</b> 例： Device(config)# policy-map mark-up-exp-2	作成されるポリシー マップの名前を指定し、ポリシー マップ コンフィギュレーション モードを開始します。 ポリシー マップ名を入力します。
ステップ 4	<b>class class-map-name</b> 例： Device(config-pmap)# class prec012	トラフィックを指定したクラスにマッチングするために使用するクラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。 クラス マップ名を入力します。
ステップ 5	<b>set mpls experimental imposition mpls-exp-value</b> 例： Device(config-pmap-c)# set mpls experimental imposition 2	上部のラベルの MPLS EXP フィールドの値を設定します。
ステップ 6	<b>end</b> 例： Device(config-pmap-c)# end	(任意) 特権 EXEC モードに戻ります。

## ラベルスイッチドパケットでの MPLS EXP のマーキング



(注) **set mpls experimental topmost** コマンドは、MPLS トラフィックの最も外側のラベルに EXP をマークします。入力ポリシーでのこのマーキングにより、出力ポリシーに MPLS EXP 値に基づく分類を含める必要があります。

ラベルスイッチドパケットでの MPLS EXP フィールドを設定するには、次の作業を実行します。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# configure terminal	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 3	<b>policy-map <i>policy-map-name</i></b> 例： Device(config)# policy-map mark-up-exp-2	作成されるポリシー マップの名前を指定し、ポリシー マップ コンフィギュレーション モードを開始します。 ポリシー マップ名を入力します。
ステップ 4	<b>class <i>class-map-name</i></b> 例： Device(config-pmap)# class-map exp012	トラフィックを指定したクラスにマッチングするために使用するクラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。 クラス マップ名を入力します。
ステップ 5	<b>set mpls experimental topmost <i>mpls-exp-value</i></b> 例： Device(config-pmap-c)# set mpls experimental topmost 2	出力インターフェイスの最上位ラベルの MPLS EXP フィールド値を設定します。
ステップ 6	<b>end</b> 例： Device(config-pmap-c)# end	(任意) 特権 EXEC モードに戻ります。

## 条件付きマーキングの設定

すべてのインポートされたラベルに MPLS EXP フィールドの値を条件付きで設定するには、次の作業を実行します。

始める前に



- (注) **set-mpls-exp-topmost-transmit** アクションは、MPLS カプセル化パケットにのみ影響します。  
**set-mpls-exp-imposition-transmit** アクションは、パケットに追加されたすべての新しいラベルに影響します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> enable	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  Device# configure terminal	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 3	<b>policy-map policy-map-name</b> 例：  Device(config)# policy-map ip2tag	作成されるポリシー マップの名前を指定し、ポリシー マップ コンフィギュレーション モードを開始します。  • ポリシー マップ名を入力します。
ステップ 4	<b>class class-map-name</b> 例：  Device(config-pmap)# class iptcp	トラフィックと指定されたクラスを照合するために使用するクラス マップを作成し、ポリシー マップ クラス コンフィギュレーション モードを開始します。  • クラス マップ名を入力します。
ステップ 5	<b>police cir bps bc pir bps be</b> 例：  Device(config-pmap-c)# police cir 1000000 pir 2000000	分類するトラフィック用のポリサーを定義し、ポリシー マップ クラス ポリシング 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	<b>conform-action transmit</b> 例：  Device(config-pmap-c-police)# conform-action transmit 3	ポリサーで指定された値に適合するパケットに対して実行するアクションを定義します。  • この例では、パケットが認定情報 レート (cir) に適合する場合または 適合バースト (bc) サイズ以内の場合

	コマンドまたはアクション	目的
		合に、MPLSEXP フィールドが3に設定されます。
ステップ 7	<b>exceed-action</b> <b>set-mpls-exp-topmost-transmit exp table</b> <i>table-map-name</i>  例 :  <pre>Device(config-pmap-c-police)# exceed-action set-mpls-exp-topmost-transmit exp table dscp2exp</pre>	ポリサーで指定された値を上回るパケットに対して実行するアクションを定義します。
ステップ 8	<b>violate-action drop</b>  例 :  <pre>Device(config-pmap-c-police)# violate-action drop</pre>	レートが最大情報レート (pir) を超えており、bc と be の範囲外のパケットに対して実行するアクションを定義します。 <ul style="list-style-type: none"> <li>違反アクションを指定する前に、超過アクションを指定する必要があります。</li> <li>この例では、パケットレートが pir レートを超えており、bc と be の範囲外の場合に、パケットがドロップされます。</li> </ul>
ステップ 9	<b>end</b>  例 :  <pre>Device(config-pmap-c-police)# end</pre>	(任意) 特権 EXEC モードに戻ります。

## MPLS EXP の WRED の設定

次の手順を実行して、MPLS EXP の WRED を有効にします。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例 : <pre>Device&gt; enable</pre>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>パスワードを入力します (要求された場合)。</li> </ul>

	コマンドまたはアクション	目的
ステップ 2	<b>configure terminal</b> 例：  Device# configure terminal	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 3	<b>policy-map policy-map-name</b> 例：  Device(config)# policy-map wred_exp	作成されるポリシー マップの名前を指定し、ポリシー マップ コンフィギュレーション モードを開始します。  • ポリシー マップ名を入力します。
ステップ 4	<b>class class-map-name</b> 例：  Device(config-pmap)# class exp	トラフィックを指定したクラスにマッチングするために使用するクラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。  • クラス マップ名を入力します。
ステップ 5	<b>bandwidth {kbps remainingpercentage percentpercentage}</b> 例：  Device(config-pmap-c)# bandwidth percent 30	ポリシーマップに属しているクラスに割り当てる帯域幅またはトラフィックシェーピングを指定します。
ステップ 6	<del>random-detect {exp-value percent min-threshold max-threshold}</del> 例：  Device(config-pmap-c)# random-detect mpls-exp- based	パケットのドロップ確率を計算する際には MPLS EXP 値を使用するように WRED を設定します。
ステップ 7	<b>random-detect exp-value percent min-threshold max-threshold</b> 例：  Device(config-pmap-c)# random-detect exp 1 10 20 Device(config-pmap-c)# random-detect exp 2 30 40 Device(config-pmap-c)# random-detect exp 2 40 80	MPLS EXP 値、最小しきい値と最大しきい値をパーセンテージで指定します。
ステップ 8	<b>end</b> 例：  Device(config-pmap-c-police)# end	(任意) 特権 EXEC モードに戻ります。

# MPLS QoS の設定例

ここでは、MPLS QoS の設定例を紹介します。

## 例：MPLS カプセル化パケットの分類

### MPLS EXP クラス マップの定義

次の例では、MPLS 実験値 3 を含むパケットと一致する exp3 という名前のクラスマップを定義する方法を示します。

```
Device(config)# class-map exp3
Device(config-cmap)# match mpls experimental topmost 3
Device(config-cmap)# exit
```

### ポリシー マップの定義とポリシー マップの入カインターフェイスへの適用

次の例では、上の例でポリシーマップを定義するために作成したクラスマップを使用する方法を示します。また、この例では、入力トラフィックの物理インターフェイスにポリシーマップを適用する方法も示します。

```
Device(config)# policy-map change-exp-3-to-2
Device(config-pmap)# class exp3
Device(config-pmap-c)# set mpls experimental topmost 2
Device(config-pmap)# exit
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# service-policy input change-exp-3-to-2
Device(config-if)# exit
```

### ポリシー マップの定義とポリシー マップの出カインターフェイスへの適用

次の例では、上の例でポリシーマップを定義するために作成したクラスマップを使用します。また、この例では、出力トラフィックの物理インターフェイスにポリシーマップを適用します。

```
Device(config)# policy-map WAN-out
Device(config-pmap)# class exp3
Device(config-pmap-c)# shape average 10000000
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# service-policy output WAN-out
Device(config-if)# exit
```

## 例：最も外側のラベルでの MPLS EXP のマーキング

### MPLS EXP インポジション ポリシー マップの定義

次の例では、転送されたパケットの IP precedence 値に基づいて MPLS EXP インポジション値を 2 に設定するポリシー マップを定義します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# class-map prec012
Device(config-cmap)# match ip prec 0 1 2
Device(config-cmap)# exit
Device(config)# policy-map mark-up-exp-2
Device(config-pmap)# class prec012
Device(config-pmap-c)# set mpls experimental imposition 2
Device(config-pmap-c)# exit
Device(config-pmap)# exit
```

### MPLS EXP インポジション ポリシー マップをメイン インターフェイスに適用する

次に、ポリシー マップをギガビットイーサネット インターフェイス 0/0/0 に適用する例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# service-policy input mark-up-exp-2
Device(config-if)# exit
```

## 例：ラベルスイッチドパケットの MPLS EXP のマーキング

### MPLS EXP ラベル スイッチド パケット ポリシー マップの定義

次の例では、転送されたパケットの MPLS EXP 値に基づいて MPLS EXP 最上位値を 2 に設定するポリシー マップを定義する方法を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# class-map exp012
Device(config-cmap)# match mpls experimental topmost 0 1 2
Device(config-cmap)# exit
Device(config-cmap)# policy-map mark-up-exp-2
Device(config-pmap)# class exp012
Device(config-pmap-c)# set mpls experimental topmost 2
Device(config-pmap-c)# exit
Device(config-pmap)# exit
```

### メイン インターフェイスへの MPLS EXP ラベル スイッチド パケット ポリシー マップの適用

次に、ポリシー マップのメイン インターフェイスへの適用例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# service-policy input mark-up-exp-2
Device(config-if)# exit
```

## 例：条件付きマーキングの設定

次の例では、**ip2tag** ポリシーマップに含まれる **iptcp** クラス用のポリサーを作成し、そのポリシーマップをギガビットイーサネットインターフェイスに適用する方法を示します。

```
Device(config)# policy-map ip2tag
Device(config-pmap)# class iptcp
Device(config-pmap-c)# police cir 1000000 pir 2000000
Device(config-pmap-c-police)# conform-action transmit
Device(config-pmap-c-police)# exceed-action set-mpls-exp-imposition-transmit 2
Device(config-pmap-c-police)# violate-action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit
Device(config-pmap)# exit
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# service-policy input ip2tag
```

## 例：MPLS EXP の WRED の設定

次に、MPLS EXP の WRED をイネーブルにする例を示します。

```
Device# configure terminal
Device(config)# policy-map wred_exp
Device(config-pmap-c)# bandwidth percent 30
Device(config-pmap-c)# random-detect mpls-exp-based
Device(config-pmap-c)# random-detect exp 1 10 20
Device(config-pmap-c)# random-detect exp 2 30 40
Device(config-pmap-c)# random-detect exp 2 40 80
```

### WRED のしきい値ラベルの表示

**show policy-map policy-map-name** コマンドを使用して、MPLS EXP の WRED 設定を確認します。

次の出力例には、WRED のしきい値ラベルが表示されています。

```
Device# show policy-map wred_exp
Policy Map wred_exp
Class exp
bandwidth 30 (%)
percent-based wred, exponential weight 9
exp    min-threshold    max-threshold
-----
0      -                    -
1      10                   20
2      30                   40
```

3	40	80
4	-	-
5	-	-
6	-	-
7	-	-

## その他の参考資料

### 関連資料

関連項目	マニュアル タイトル
QoS コマンド	『Cisco IOS Quality of Service Solutions Command Reference』

## QoS MPLS EXP の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたりリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	QoS MPLS EXP	QoS EXP Matching 機能を使用すると、マルチプロトコルラベルスイッチング (MPLS) Experimental ビット (EXP ビット) フィールドを変更することで、ネットワークトラフィックを分類、マーキング、およびキューイングできます。
Cisco IOS XE Amsterdam 17.3.1	MPLS QoS - WRED	MPLS Quality of Service (QoS) で重み付けランダム早期検出 (WRED) がサポートされるようになりました。この機能は、MPLS 試験ビットを使用してパケットの廃棄確率を計算するように WRED を設定します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



## 第 12 章

# MPLS スタティックラベルの設定

- [MPLS スタティック ラベル \(175 ページ\)](#)

## MPLS スタティック ラベル

このマニュアルでは、Cisco MPLS スタティック ラベル機能について説明します。MPLS スタティックラベル機能は、ラベルと IPv4 プレフィックス間のバインディングを静的に設定できるようにします。

## MPLS スタティック ラベルの前提条件

MPLS スタティックラベルを有効にするには、次の Cisco IOS 機能がネットワークでサポートされている必要があります。

- マルチプロトコル ラベル スイッチング (MPLS)
- Cisco Express Forwarding; シスコ エクスプレス フォワーディング

## MPLS スタティック ラベルの制限事項

- MPLS VPN のプロバイダーエッジ (PE) ルータには、ラベルをカスタマー ネットワーク プレフィックス (VPN IPv4 プレフィックス) にスタティックにバインドするためのメカニズムは存在しません。
- MPLS スタティッククロスコネクトはサポートされていません。
- MPLS スタティックラベルはラベル制御非同期転送モード (lc-atm) ではサポートされていません。
- MPLS スタティック バインディングは、ローカルプレフィックスではサポートされません。
- VRF 対応スタティックラベルはサポートされていません。

## MPLS スタティックラベルに関する情報

### MPLS スタティックラベルの概要

一般的に、ラベルスイッチングルータ（LSR）は、ラベルスイッチパケットに使用するラベルを動的に学習します。これは、次のようなラベル配布プロトコルによって行われます。

- ラベルをネットワークアドレスにバインドするために使用される Internet Engineering Task Force (IETF) 標準である、Label Distribution Protocol (LDP; ラベル配布プロトコル)
- トラフィック エンジニアリング (TE) のラベル配布に使用されるリソース予約プロトコル (RSVP)
- マルチプロトコルラベルスイッチング (MPLS) バーチャルプライベートネットワーク (VPN) のラベル配布に使用されるボーダーゲートウェイプロトコル (BGP)

学習したラベルをパケットのラベルスイッチングに使用するために、LSR はそのラベルをラベル転送情報ベース (LFIB) にインストールします。

MPLS スタティックラベル機能は、ラベルと IPv4 プレフィックス間のバインディングを静的に設定できるようにします。

### MPLS スタティックラベルの利点

#### ラベルと IPv4 プレフィックス間のスタティックバインディング

ラベルと IPv4 プレフィックス間のスタティックバインディングを設定して、LDP ラベル配布を実装しないネイバルルータ経由の MPLS ホップバイホップ転送をサポートできます。

## MPLS スタティックラベルの設定方法

### MPLS スタティックプレフィックスラベルバインディングの設定

MPLS スタティック Prefix/Label バインディングを設定するには、グローバルコンフィギュレーションモードで次のコマンドを使用します。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> enable	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：	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。

	コマンドまたはアクション	目的
	Device# configure terminal	
ステップ 3	<b>mpls label range</b> <i>min-label max-label</i> [ <b>static</b> <i>min-static-label max-static-label</i> ] 例 : Device(config)# mpls label range 200 100000 static 16 199	MPLS スタティック ラベル機能で使用するラベルの範囲を指定します。 (デフォルトではスタティック割り当て用に予約されたラベルはありません)。
ステップ 4	<b>mpls static binding ipv4</b> <i>prefix mask</i> [ <b>input</b>   <b>output</b> <i>nexthop</i> ] <i>label</i> 例 : Device(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 55	IPv4 プレフィックスに対するラベルのスタティック バインディングを指定します。 指定したバインディングは、ルーティングの要求時に自動的に MPLS 転送テーブルにインストールされます。

## MPLS スタティック Prefix/Label バインディングの確認

MPLS スタティック Prefix/Label バインディングの設定を確認するには、次の手順を実行します。

### 手順

**ステップ 1** **show mpls label range** コマンドを入力します。出力には、新しいラベル範囲はリロードが行われるまで有効にならないことが示されます。

例 :

```
Device# show mpls label range

Downstream label pool: Min/Max label: 16/983039
  [Configured range for next reload: Min/Max label: 200/100000]
Range for static labels: Min/Max/Number: 16/199
```

リロード後に実行される **show mpls label range** コマンドの次の出力には、新しいラベル範囲が有効になっていることが示されます。

例 :

```
Device# show mpls label range

Downstream label pool: Min/Max label: 200/100000
Range for static labels: Min/Max/Number: 16/199
```

**ステップ 2** 設定されたスタティック Prefix/Label バインディングを表示するには、**show mpls static binding ipv4** コマンドを入力します。

例 :

```
Device# show mpls static binding ipv4
10.17.17.17/32: Incoming label: 251 (in LIB)
  Outgoing labels:
    10.0.0.1          18
10.18.18.18/32: Incoming label: 201 (in LIB)
  Outgoing labels:
10.0.0.1 implicit-null
```

**ステップ3** MPLS 転送で現在使用されているスタティック Prefix/Label バインディングを確認するには、**show mpls forwarding-table** コマンドを使用します。

例：

```
Device# show mpls forwarding-table
Local  Outgoing  Prefix          Bytes tag  Outgoing  Next Hop
tag    tag or VC  or Tunnel Id   switched  interface
201    Pop tag    10.18.18.18/32  0         PO1/1/0   point2point
      2/35      10.18.18.18/32  0         AT4/1/0.1 point2point
251    18         10.17.17.17/32  0         PO1/1/0   point2point
```

## MPLS スタティックラベルの監視とメンテナンス

MPLS スタティックラベルを監視およびメンテナンスするには、次のコマンドを1つ以上使用します。

手順

	コマンドまたはアクション	目的
ステップ1	<b>enable</b> 例：  Devie> enable	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ2	<b>show mpls forwarding-table</b> 例：  Device# show mpls forwarding-table	MPLS LFIB の内容を表示します。
ステップ3	<b>show mpls label range</b> 例：  Device# show mpls label range	スタティックラベル範囲に関する情報が表示されます。
ステップ4	<b>show mpls static binding ipv4</b> 例：  Device# show mpls static binding ipv4	設定されているスタティック Prefix/Label バインディングに関する情報を表示します。

## MPLS スタティック ラベルの設定例

### 例 : MPLS スタティック プレフィックス ラベルの設定

次の出力では、動的に割り当てられたラベル 16 ~ 983039 から 200 ~ 100000 に使用される範囲が **mpls label range** コマンドによって再設定されます。また、16 ~ 199 のスタティックラベル範囲が設定されます。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# mpls label range 200 100000 static 16 199
% Label range changes take effect at the next reload.
Router(config)# end
```

次の出力では、新しいラベルの範囲はリロードが発生するまで適用されないことが **show mpls label range** コマンドによって示されています。

```
Device# show mpls label range

Downstream label pool: Min/Max label: 16/983039
  [Configured range for next reload: Min/Max label: 200/100000]
Range for static labels: Min/Max/Number: 16/199
```

次の出力では、リロード後に実行される **show mpls label range** コマンドによって、新しいラベルの範囲が有効になっていることが示されています。

```
Device# show mpls label range

Downstream label pool: Min/Max label: 200/100000
Range for static labels: Min/Max/Number: 16/199
```

次の出力では、**mpls static binding ipv4** コマンドによってスタティック Prefix/Label バインディングが設定されています。さまざまなプレフィックスの着信（ローカル）と発信（リモート）のラベルも設定されています。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 55
Device(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 output 10.0.0.66 2607
Device(config)# mpls static binding ipv4 10.6.0.0 255.255.0.0 input 17
Device(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 output 10.13.0.8 explicit-null
Device(config)# end
```

次の出力では、**show mpls static binding ipv4** コマンドによってスタティック Prefix/Label バインディングが表示されています。

```
Device# show mpls static binding ipv4

10.0.0.0/8: Incoming label: none;
  Outgoing labels:
10.13.0.8          explicit-null
10.0.0.0/8: Incoming label: 55 (in LIB)
  Outgoing labels:
    10.0.0.66          2607
```

10.66.0.0/16: Incoming label: 17 (in LIB)  
Outgoing labels: None

## その他の参考資料

### 関連資料

関連項目	マニュアル タイトル
MPLS コマンド	『 <i>Multiprotocol Label Switching Command Reference</i> 』

### 標準

標準	タイトル
この機能がサポートする新しい規格または変更された規格はありません。既存の規格のサポートは、この機能によって変更されていません。	--

### MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャセットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

## シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## MPLS スタティックラベルの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	MPLS スタティックラベル	MPLS スタティックラベル機能は、ラベルと IPv4 プレフィックス間のバインディングを静的に設定できるようにします。 次のコマンドが導入または変更されました。 <b>debug mpls static binding、mpls label range、mpls static binding ipv4、show mpls label range、show mpls static binding ipv4</b>

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。





## 第 13 章

# MPLS トラフィック エンジニアリングおよび拡張機能の設定

- [MPLS トラフィック エンジニアリングおよび拡張機能の前提条件 \(183 ページ\)](#)
- [MPLS トラフィック エンジニアリングおよび拡張機能の制約事項 \(183 ページ\)](#)
- [MPLS トラフィック エンジニアリングおよび拡張機能について \(184 ページ\)](#)
- [MPLS トラフィック エンジニアリングおよび拡張機能の設定方法 \(192 ページ\)](#)
- [MPLS トラフィック エンジニアリングおよび拡張機能の設定例 \(200 ページ\)](#)
- [その他の参考資料 \(203 ページ\)](#)
- [MPLS トラフィック エンジニアリングおよび拡張機能の機能履歴 \(205 ページ\)](#)

## MPLS トラフィック エンジニアリングおよび拡張機能の前提条件

MPLS TE を有効にする前に、ネットワークが次の Cisco IOS 機能をサポートしていることを確認します。

- Multiprotocol Label Switching : マルチプロトコル ラベル スイッチング
- IP シスコ エクスプレス フォワーディング
- Intermediate System-to-Intermediate System (IS-IS) または Open Shortest Path First (OSPF)

## MPLS トラフィック エンジニアリングおよび拡張機能の制約事項

- MPLS TE 高速再ルーティングはサポートされていません。

- MPLS TE は、1つの IGP プロセスまたはインスタンスのみをサポートします。複数の IGP プロセスまたはインスタンスはサポートされず、複数の IGP プロセスまたはインスタンスでは MPLS TE を設定できません。
- MPLS TE 機能では、番号なし IP アドレスリンクを介したルーティングおよびシグナリングはサポートされていません。このため、このようなリンク上には、この機能を設定しないでください。
- 明示パスを指定するとき、転送アドレス（トラフィックを次のルータに転送するインターフェイスのアドレス）をネクストホップアドレスとして指定すると、明示パスが使用されない場合があります。転送アドレスを使用すると、そのエントリをパス計算のルーズホップとして扱うことができます。受信アドレス（送信側ルータからのトラフィックを受信するインターフェイスのアドレス）をネクストホップアドレスとして使用することを推奨します。

次の例では、スイッチ S3 からスイッチ S1 にトラフィックが送信されます。スイッチ S1 とルータ S2 の間で a,b および x,y とマーク付けされたパスはパラレルパスです。

```
S1 (a) ---- (b) S2 (c) -- (d) S3
      (x) ---- (y)
```

転送アドレス（アドレス d および b）を使用して S3 から S1 への明示パスを設定すると、トンネルは明示パスの代わりにパラレルパス（x,y）を介してトラフィックを再ルーティングする場合があります。明示パスがトンネルによって必ず使用されるようにするには、次の例に示すように、**next-address** コマンドの一部として受信アドレスを指定します。

```
ip explicit-path name path1
  next-address (c)
  next-address (a)
```

## MPLS トラフィック エンジニアリングおよび拡張機能について

続くセクションでは、MPLS TE および拡張機能について説明します。

## MPLS トラフィック エンジニアリングおよび拡張機能の概要

MPLS は、レイヤ 2 テクノロジーとレイヤ 3 テクノロジーを統合したものです。従来のレイヤ 2 機能をレイヤ 3 で使用可能にすることで、MPLS はトラフィック エンジニアリングを可能にしています。したがって、レイヤ 2 ネットワークの上にレイヤ 3 ネットワークを重ねることによってのみ可能になる機能を、1 層のネットワーク内で実現できます。

トラフィック エンジニアリングは、サービスプロバイダーと ISP バックボーンに不可欠です。このようなバックボーンは、伝送容量の大量使用をサポートしている必要があります。また、リンク障害やノード障害に耐えられるように、復元力が高いネットワークである必要があります。

MPLS トラフィック エンジニアリングによって、統合型のトラフィック エンジニアリングが可能になります。MPLSを使用すると、レイヤ3にトラフィック エンジニアリング機能が統合され、バックボーンの容量とトポロジによる制約を前提に、IPトラフィックのルーティングが最適化されます。

MPLS トラフィック エンジニアリングでは、次の機能がサポートされています。

- パケットを適切なトラフィックフローに自動的にマッピングするように、IS-ISやOSPFなどの標準的な内部ゲートウェイプロトコル（IGP）を拡張します。
- トランスポートトラフィックはMPLS転送を使用してネットワーク全体に伝送されます。
- ネットワーク全体のトラフィックフローのルートを決めます。その決定は、トラフィックフローに必要なリソースおよびネットワークで使用可能なリソースに基づいています。
- 制約ベースルーティングを使用します。制約ベースルーティングでは、トラフィックフローのパスはそのフローのリソース要件（制約）を満たす最短パスになります。MPLS トラフィック エンジニアリングでは、トラフィック フローには、帯域幅要件、メディア要件、プライオリティ（他のフローのプライオリティと比較）などがあります。
- トポロジが変更されたことによって発生した新しい制約に対応することによって、リンク障害またはノード障害から回復します。
- マルチホップ ラベルスイッチドパス（LSP）を通過する MPLS 転送を使用して、パケットを転送します。
- 次のようなバックボーントポロジでLSPのルーティングおよびシグナリング機能を使用します。
  - そのバックボーントポロジと使用可能なリソースを認識している。
  - バックボーン上のLSPのルートを決めるとき、リンク帯域幅とトラフィックフローのサイズが考慮される。
  - 複数のプライマリパスがオフラインで事前に計算されている場合も、障害に対するバックボーンの復元力を高めるダイナミック適応メカニズムが備えられている。
  - IGP（IS-ISまたはOSPF）最短パス優先（SPF）計算の拡張機能が備えられており、どのトラフィックをどのLSPを介して送信するかが自動的に計算される。

## MPLS トラフィック エンジニアリングの利点

WAN 接続は、ISP 予算において高価な項目です。トラフィック エンジニアリングにより、ISP はネットワークトラフィックをルーティングして、スルーブットと遅延の観点でユーザに最善のサービスを提供できるようになります。トラフィック エンジニアリングでは、サービスプロバイダーの効率を高めることによって、ネットワークのコストを削減します。

現在、一部のISPは、オーバーレイモデルを基礎としてサービスを提供しています。このモデルでは、送信施設はレイヤ2スイッチングによって管理されます。ルータはフルメッシュの仮想トポロジだけを認識し、ほとんどの宛先が1ホップ離れて出現します。明示的なレイヤ2転

送レイヤを使用する場合、トラフィックが使用可能な帯域幅を使用する方法を正確に制御できません。ただし、オーバーレイモデルには、数多くのデメリットがあります。MPLS トラフィック エンジニアリングでは、個別のネットワークを稼働させることも、スケーラブルでない完全メッシュのルータ相互接続を使用することもなく、オーバーレイ モデルのトラフィック エンジニアリングの利点が得られます。

## MPLS トラフィック エンジニアリングのしくみ

MPLS TE では、RSVP を使用して、バックボーン上で LSP を自動的に確立および維持します。LSP で使用されるパスは、LSP リソース要件とネットワークリソース（帯域幅など）によって決まります。

使用可能なリソースは、リンクステートベースの IGP に対する拡張機能を使用してフラッドイングされます。

トラフィック エンジニアリング トンネルは、必要なリソースと使用可能なリソースの調和に基づいて LSP ヘッドで計算されます（制約ベースルーティング）。IGP は、これらの LSP にトラフィックを自動的にルーティングします。通常、MPLS TE バックボーンを通過するパケットは、入力ポイントと出力ポイントを接続する単一の LSP 上を伝送されます。

MPLS トラフィック エンジニアリングは、次の Cisco IOS メカニズムに基づいて構築されています。

- IP トンネル インターフェイス

レイヤ 2 の観点では、MPLS トンネル インターフェイスは LSP のヘッドを表します。これは、帯域幅要件、メディア要件、プライオリティなどの一連のリソース要件を使用して設定されます。

レイヤ 3 の観点では、LSP トンネル インターフェイスはトンネル宛先への単一方向仮想リンクのヘッドエンドです。

- MPLS トラフィック エンジニアリング パス計算モジュール

この計算モジュールは LSP ヘッドで動作します。このモジュールは、LSP で使用するパスを決定します。パス計算では、フラッドイングされたトポロジおよびリソース情報を含むリンクステート データベースが使用されます。

- トラフィック エンジニアリング拡張を備えた RSVP

RSVP は各 LSP ホップで動作し、計算されたパスに基づいて LSP のシグナリングおよび維持のために使用されます。

- MPLS トラフィック エンジニアリング リンク管理モジュール

このモジュールは、各 LSP ホップで動作します。RSVP シグナリングメッセージに対するリンクコールアドミッションを実行し、フラッドイングされるトポロジおよびリソース情報のブックキーピングを行います。

- リンクステート IGP（トラフィック エンジニアリング拡張機能を備えた IS-IS または OSPF）

これらのIGPは、リンク管理モジュールからトポロジおよびリソース情報をグローバルにフラiddiingするために使用されます。

- リンクステート IGP (IS-IS または OSPF) で使用される SPF 計算の拡張

IGPは、トンネル宛先に基づいて適切なLSPトンネルにトラフィックを自動的にルーティングします。また、スタティックルートを使用して、LSPトンネルにトラフィックを誘導することもできます。

- ラベルスイッチング フォワーディング

この転送メカニズムは、レイヤ2と類似の機能をルータに提供し、RSVPシグナリングによって確立されたLSPの複数のホップを経由してトラフィックを誘導できるようにします。

バックボーンのエンジニアリングを行う方法の1つは、すべての入力デバイスからすべての出力デバイスまでのトンネルのメッシュを定義することです。MPLS TEパス計算モジュールおよびシグナリングモジュールは、これらのトンネルのLSPで使用されるパスを、リソースの可用性とネットワークの動的な状態に基づいて決定します。入力デバイスで動作するIGPは、どの出力デバイスにどのトラフィックを送信するかを決定し、入力から出力へのトンネルにそのトラフィックを誘導します。

入力デバイスから出力デバイスへのフローが大きいため、単一のリンクに収まらなくなる可能性があります。また、このフローは単一のトンネルでは伝送できません。こうしたシナリオでは、特定の入力および出力の間に複数のトンネルを設定し、それらの間でフローの負荷が分担されるようにすることができます。

## トンネルへのトラフィックのマッピング

このセクションでは、トラフィックがトンネルにどのようにマッピングされるかについて説明します。従来のホップバイホップリンクステートルーティングプロトコルがMPLS TE機能とどのように相互作用するかについて説明します。このセクションでは、最短パス優先 (SPF) アルゴリズム (Dijkstra アルゴリズムとも呼ばれることもある) がどのように拡張されるかについて説明します。この拡張により、リンクステートIGPは、MPLSトラフィックエンジニアリングが確立するトンネルを介してトラフィックを自動的に転送できます。

統合IS-ISまたはOSPFなどのリンクステートプロトコルでは、SPFアルゴリズムを使用して、ネットワーク内のヘッドエンドノードからすべてのノードへの最短パスツリーを計算します。ルーティングテーブルは、この最短パスツリーを基に作成されます。ルーティングテーブルには、宛先と先頭ホップに関する情報のセットが順番に格納されています。ルータで通常のホップバイホップルーティングが実行されている場合、最初のホップはルータに接続された物理インターフェイス上に存在します。

新しいトラフィック エンジニアリング アルゴリズムでは、ネットワーク内の1つまたは複数のノードへの明示ルートを計算します。送信元ルータは、これらの明示ルートを論理インターフェイスとして認識します。このマニュアルの中では、これらの明示ルートはLSPによって表され、トラフィック エンジニアリング トンネル (TE トンネル) と呼ばれます。

次の各項では、リンクステート IGP がこれらのショートカットをどのように使用し、これらの TE トンネルを指すルートルーティング テーブルにどのようにインストールするかについて説明します。これらのトンネルは明示ルートを使用します。TE トンネルで使用されるパスは、トンネルのヘッドエンドルータによって制御されます。エラーがない場合、TE トンネルはループしないことが保証されていますが、ルータが TE トンネルの使用方法に同意している必要があります。このようにしない場合、トラフィックは複数のトンネルでループする可能性があります。

MPLS TE トンネルの明示パスを指定する場合、明示パス内にネクストホップルータのリンクアドレスまたはノードアドレスを指定できます。リンクアドレスとノードアドレスを混在させて指定することもできます。リンクアドレスとノードアドレスを混在させて指定する場合でも制約はありません。

## 新しいテクノロジーへの IS-IS ネットワークの移行

RFC 1142 で規定されている IS-IS には、MPLS TE の拡張が含まれています。IS-IS 上で MPLS トラフィック エンジニアリングを実行したり、これらの他の拡張を利用したりするには、この新しいテクノロジーに IS-IS ネットワークを移行する必要があります。このセクションでは、これらの拡張について説明します。ここでは、既存の IS-IS ネットワークを標準的な ISO 10589 プロトコルから RFC 1142 で規定されている IS-IS のバージョンに移行する 2 つの方法を示します。既存の IS-IS ネットワーク上で MPLS TE を実行するには、RFC 1142 で規定されている IS-IS のバージョンへの移行が必要です。ただし、OSPF 上で MPLS TE を実行する場合は、同様のネットワークの移行は不要です。

## IS-IS ルーティング プロトコルの拡張

IS-IS ルーティング プロトコルの拡張は、次の目的に使用できます。

- リンク メトリックの 6 ビット制限を削除します。
- エリア間 IP ルートを許可します。
- IS-IS でトラフィック エンジニアリング用に異なる種類の情報を伝送できるようにします。今後、さらに拡張が必要になる場合があります。

これらの目的に役立つように、次の 2 つの新しいタイプ、長さ、値 (TLV) オブジェクトが定義されています。

- TLV 22 はリンク (厳密には隣接) を表します。これは、ISO 10589 (TLV 2) の「IS ネイバー オプション」と同じ目的に役立ちます。
- TLV 135 は到達可能な IP プレフィックスを表します。これは、RFC 1195 (TLV 128 および 130) の IP ネイバー オプションに似ています。



(注) これら 2 つの TLV (22 および 135) は簡略化して「新スタイルの TLV」と呼ばれます。TLV 2、128、および 130 は「旧スタイルの TLV」と呼ばれます。

新しい TLV には両方とも固定長部分があり、それに任意のサブ TLV が続きます。これらの新しい TLV のメトリック領域は 6 ビットから 24 または 32 ビットに拡張されています。サブ TLV では、リンクおよびプレフィックスに新しいプロパティを追加できます。トラフィック エンジニアリングは、この機能を使用してリンクに新しいプロパティを追加できる最初のテクノロジーです。

## IS-IS ネットワークを新しいテクノロジーに移行するためのソリューション 1

旧スタイルの TLV を新スタイルの TLV に移行する場合、同じ情報を 2 回（旧スタイルの TLV で 1 回と新スタイルの TLV で 1 回）アドバタイズできます。この操作により、すべてのデバイスでアドバタイズ内容が認識されます。

このアプローチを使用した場合、次の 3 つのデメリットがあります。

- **LSP のサイズ**：移行中、LSP は元のサイズの約 2 倍に増大します。このことは、大規模な LSP データベース（LSPDB）を使用するネットワークで問題になる場合があります。次の理由により、LSP データベースが大きくなる場合があります。
  - 多数のデバイスがあるため LSP が増大する。
  - ルータごとに、数多くのネイバーまたは IP プレフィックスが存在する。多くの情報をアドバタイズするデバイスにより、LSP がフラグメント化されます。
- **予測不可能な結果**：大規模なネットワークでは、このアプローチによって予測不可能な結果が生じることがあります。大規模なネットワークを移行する場合、LSP フラッディングおよび SPF スケーリングに関する制限が強制されます。
- **あいまいさ**：デバイスが旧スタイルの TLV と新スタイルの TLV で異なる情報を検出すると、デバイスでどのような処理を実行するかが不明確になる可能性があります。
  - ネットワークが不安定になる何らかの特別な状況が発生することがある。このとき、いずれかの実装がどの程度状況に対応できるかを試してはならない。
  - トラフィック エンジニアリング拡張機能によって、LSP が頻繁に再フラッディングされるようになる可能性がある。

このような問題の大部分は、次の項目を使用して簡単に解決できます。

- LSP 内の旧スタイルの TLV と新スタイルの TLV のすべての情報
- 最も小さいリンクメトリックを持つ隣接（隣接が複数回アドバタイズされる場合）

同じ情報を 2 回アドバタイズする主な利点として、新スタイルの TLV がネットワーク内のすべてのデバイスによって認識される前に、ネットワーク管理者が新スタイルの TLV を使用できることを挙げることができます。

## ソリューション1での移行アクション

旧スタイルの TLV を使用する IS-IS を新スタイルの TLV に移行する場合は、次のアクションを実行します。

- すべてのデバイスが古いソフトウェアを実行している場合、旧スタイルの TLV だけをアドバタイズおよび使用します。
- 一部のデバイスを新しいソフトウェアにアップグレードします。
- 旧スタイルの TLV と新スタイルの TLV の両方をアドバタイズするように、新しいソフトウェアを使用する一部のデバイスを設定します。これらのルータでは、両方のスタイルの TLV を受け入れます。旧スタイルの TLV だけを引き続きアドバタイズおよび使用するように、（古いソフトウェアを使用する）他のデバイスを設定します。
- ネットワークの一部でトラフィック エンジニアリングをテストします。
- ネットワーク全体を移行する必要がある場合は、両方のスタイルの TLV をアドバタイズして受け入れるように、残りのすべてのデバイスをアップグレードおよび設定します。
- 新スタイルの TLV だけをアドバタイズして受け入れるように、すべてのデバイスを設定します。
- 63 よりも大きいメトリックを設定します。

## IS-IS ネットワークを新しいテクノロジーに移行するためのソリューション2

デバイスは同時に1つのスタイルの TLV だけをアドバタイズしますが、移行時には両方のスタイルの TLV を認識できます。このアプローチには、主に次の2つの利点があります。

- LSP は、移行時にほぼ同じサイズになります。
- 1つの LSP 内で同じ情報が2回アドバタイズされると、あいまいさがなくなります。

この方法は、より広いメトリックを使用する（つまり、IS-IS を実行しているルータで新スタイルの TLV だけを生成して受け入れるようにする）ように、ネットワーク全体（またはエリア全体）を移行する場合に役立ちます。

この方法のデメリットとして、いずれかのデバイスが新スタイルの TLV のアドバタイズを開始するには、すべてのデバイスが新スタイルの TLV を認識している必要があることを挙げることができます。この方法は、2つめの問題、つまり、ネットワーク管理者がトラフィック エンジニアリング用に新スタイルの TLV を使用し、一部のデバイスが旧スタイルの TLV だけを認識できる場合の問題の解決には役立ちません。

## 2つめのソリューションでの移行アクション

2つめのソリューションを使用する場合は、次のアクションを実行できます。

- すべてのデバイスが古いソフトウェアを実行している場合、旧スタイルの TLV だけをアダプタイズおよび使用します。
- すべてのデバイスを新しいソフトウェアにアップグレードします。
- 旧スタイルの TLV をアダプタイズするが、両方のスタイルの TLV を受け入れるように、すべてのデバイスを 1 つずつ設定します。
- 新スタイルの TLV をアダプタイズするが、両方のスタイルの TLV を受け入れるように、すべてのデバイスを 1 つずつ設定します。
- 新スタイルの TLV だけをアダプタイズして受け入れるように、すべてのデバイスを 1 つずつ設定します。
- 63 よりも大きいメトリックを設定します。

## TLV コンフィギュレーション コマンド

**metric-style** コマンドを使用して、デバイスに受け入れられる TLV のタイプを設定できます。デバイスが IS-IS コンフィギュレーションモードの場合、**metric-style** コマンドで次のキーワードを設定できます。

- **metric-style narrow** : デバイスが旧スタイルの TLV だけを生成して受け入れるようにします。
- **metric-style transition** : デバイスが旧スタイルと新スタイル両方の TLV を生成して受け入れるようにします。
- **metric-style wide** : デバイスが新スタイルの TLV だけを生成して受け入れるようにします。

**metric-style** コマンドを使用する場合、次の移行スキームのいずれかを使用できます。

- narrow > transition > wide
- narrow > narrow transition > wide transition > wide

## Cisco IOS XE ソフトウェアでの実装

Cisco IOS XE では両方の移行ソリューションを導入できます。それぞれの環境に適したソリューションを選択してください。テストネットワークにはソリューション1が適しています（「[IS-IS ネットワークを新しいテクノロジーに移行するためのソリューション 1 \(189 ページ\)](#)」を参照）。どちらのソリューションでも完全移行を行えますが、手順と設定はソリューション1の方が簡単です。移行中に LSP データベースのサイズが急激に増加する恐れがある大規模なネットワークでは、ソリューション2を使用してください（「[IS-IS ネットワークを新しいテクノロジーに移行するためのソリューション 2 \(190 ページ\)](#)」を参照）。

# MPLS トラフィック エンジニアリングおよび拡張機能の設定方法

続くセクションでは、MPLS トラフィック エンジニアリングおよび拡張機能の設定手順について説明します。

## トンネルをサポートするためのデバイスの設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例：  Device# <b>configure terminal</b>	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 3	<b>ip cef</b> 例：  Device(config)# <b>ip cef</b>	標準的なシスコ エクスプレス フォワーディング動作をイネーブルにします。
ステップ 4	<b>mpls traffic-eng tunnels</b> 例：  Device(config)# <b>mpls traffic-eng tunnels</b>	デバイスで MPLS トラフィック エンジニアリング トンネルをイネーブルにします。
ステップ 5	<b>exit</b> 例：  Device(config)# <b>exit</b>	特権 EXEC モードに戻ります。

## RSVP ベースのトンネル シグナリングおよび IGP フラッドイングをサポートするためのインターフェイスの設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例 :  Device# <b>configure terminal</b>	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 3	<b>interface type slot / subslot / port [ subinterface-number]</b> 例 :  Device (config)# <b>interface Port-channel 114</b>	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<b>mpls traffic-eng tunnels</b> 例 :  Device (config-if)# <b>mpls traffic-eng tunnels</b>	インターフェイスで MPLS トラフィック エンジニアリング トンネルをイネーブルにします。
ステップ 5	<b>ip rsvp bandwidth bandwidth</b> 例 :  Device (config-if)# <b>ip rsvp bandwidth 1000</b>	インターフェイスで RSVP をイネーブルにし、予約する帯域幅の量を指定します。
ステップ 6	<b>exit</b> 例 :  Device (config-if)# <b>exit</b>	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 7	<b>exit</b> 例 :  Device (config)# <b>exit</b>	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

## MPLS トラフィック エンジニアリング用の IS-IS の設定



(注) MPLS トラフィック エンジニアリングは、1つの IGP プロセスまたはインスタンスのみをサポートします。複数の IGP プロセスまたはインスタンスはサポートされていません。MPLS トラフィック エンジニアリングを複数の IGP プロセスまたはインスタンスで設定することはできません。

MPLS トラフィック エンジニアリング用に IS-IS を設定するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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 3	<b>router isis</b> 例： Device(config)# <b>router isis</b>	IS-IS ルーティングをイネーブルにし、IS-IS プロセスを指定します。デバイスはコンフィギュレーション モードになります。
ステップ 4	<b>mpls traffic-eng level</b> 例： Device(config-router)# <b>mpls traffic-eng level-1</b>	IS-IS レベル 1 で MPLS トラフィック エンジニアリングをオンにします。
ステップ 5	<b>mpls traffic-eng level</b> 例： Device(config-router)# <b>mpls traffic-eng level-2</b>	IS-IS レベル 2 で MPLS トラフィック エンジニアリングをオンにします。
ステップ 6	<b>mpls traffic-eng router-id type number</b> 例： Device(config-router)# <b>mpls traffic-eng router-id loopback 0</b>	ノードのトラフィック エンジニアリング ルータ識別子が、インターフェイス loopback0 に関連付けられている IP アドレスになるように指定します。

	コマンドまたはアクション	目的
ステップ 7	<b>metric-style wide</b> 例 : Device(config-router)# <b>metric-style wide</b>	新スタイルのタイプ、長さ、値 (TLV) オブジェクトだけを生成して受け入れるようにルータを設定します。

## MPLS トラフィック エンジニアリング用の OSPF の設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例 : Device# <b>configure terminal</b>	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 3	<b>router ospf process-id</b> 例 : Device(config)# <b>router ospf 200</b>	IP 用の OSPF ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> <li>• <i>process-id</i> 引数の値は、OSPF ルーティング プロセスの内部で使用される識別パラメータです。ローカルで割り当てられ、任意の正の整数を使用できます。OSPF ルーティング プロセスごとに固有の値を割り当てます。</li> </ul>
ステップ 4	<b>mpls traffic-eng area number</b> 例 : Device(config-router)# <b>mpls traffic-eng area 0</b>	指定された OSPF エリアに対して MPLS TE をオンにします。
ステップ 5	<b>mpls traffic-eng router-id loopback0</b> 例 : Device(config-router)# <b>mpls traffic-eng router-id loopback0</b>	ノードの TE ルータ識別子が、インターフェイス loopback0 に関連付けられている IP アドレスになるように指定します。

	コマンドまたはアクション	目的
ステップ 6	<b>exit</b> 例：  Device(config-router)# <b>exit</b>	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	<b>exit</b> 例：  Device(config)# <b>exit</b>	特権 EXEC モードに戻ります。

## MPLS トラフィック エンジニアリング トンネルの設定

MPLS TE トンネルの優先明示パスを設定するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例：  Device# <b>configure terminal</b>	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 3	<b>interface tunnel number</b> 例：  Device(config)# <b>interface Tunnel0</b>	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。  • <i>number</i> 引数はトンネルの番号です。
ステップ 4	<b>ip unnumbered type number</b> 例：  Device(config-if)# <b>ip unnumbered loopback0</b>	明示的な IP アドレスをインターフェイスに割り当てずにインターフェイス上の IP 処理をイネーブルにします。  • <i>type</i> 引数および <i>number</i> 引数では、ルータに IP アドレスが割り当てられている別のインターフェイスのタイプと番号を指定します。番号付けされていない別のインターフェイスは指定できません。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>MPLS トラフィック エンジニアリング トンネル インターフェイスは単一方向リンクを表すため、番号なしにする必要があります。</li> </ul>
ステップ 5	<b>tunnel destination</b> <i>ip-address</i> 例 : <pre>Device(config-if)# tunnel destination 192.168.4.4</pre>	トンネル インターフェイスの宛先を指定します。 <ul style="list-style-type: none"> <li><i>ip-address</i> 引数では、宛先デバイスの MPLS トラフィック エンジニアリング ルータ ID を指定する必要があります。</li> </ul>
ステップ 6	<b>tunnel mode mpls traffic-eng</b> 例 : <pre>Device(config-if)# tunnel mode mpls traffic-eng</pre>	トンネル カプセル化モードを MPLS トラフィック エンジニアリング に設定します。
ステップ 7	<b>tunnel mpls traffic-eng bandwidth</b> <i>bandwidth</i> 例 : <pre>Device(config-if)# tunnel mpls traffic-eng bandwidth 250</pre>	MPLS トラフィック エンジニアリング トンネルの帯域幅を設定します。 <ul style="list-style-type: none"> <li><i>bandwidth</i> 引数は、MPLS トラフィック エンジニアリング トンネルで確保する kbps 単位の数値です。範囲は 1 ~ 4294967295 です。</li> </ul> (注) トンネルに自動帯域幅が設定されている場合は、 <b>tunnel mpls traffic-eng bandwidth</b> コマンドを使用して、トンネルの初期帯域幅を設定します。
ステップ 8	<b>tunnel mpls traffic-eng path-option</b> <i>number</i> {dynamic   explicit {name <i>path-name</i>   identifier <i>path-number</i> }} [lockdown] 例 : <pre>Device(config-if)# tunnel mpls traffic-eng path-option 10 explicit identifier 321</pre>	指定した IP 明示パス、またはトラフィック エンジニアリング トポロジ データベースからダイナミックに計算されたパスを使用するように、トンネルを設定します。 <ul style="list-style-type: none"> <li><i>number</i> 引数は、このパス オプションの優先度です。複数のパス オプションを設定する場合、より低い数値のオプションが優先されます。有効値は 1 ~ 1000 です。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>dynamic</b> キーワードは、LSP のパスがダイナミックに計算されることを示します。</li> <li>• <b>explicit</b> キーワードは、LSP のパスが IP 明示パスの場合に指定します。</li> <li>• <b>name path-name</b> のキーワードと引数のペアは、トンネルがこのオプションで使用する IP 明示パスのパス名です。</li> <li>• <b>identifier path-number</b> のキーワードと引数のペアは、トンネルがこのオプションで使用する IP 明示パスのパス番号です。有効な範囲は 1 ~ 65535 です。</li> <li>• <b>lockdown</b> キーワードは、LSP を再最適化できないようにする場合に指定します。</li> </ul> <p>(注) 明示パスが現在使用可能でない場合は、ダイナミックパスが使用されます。</p>
ステップ 9	<b>exit</b> 例 : Device(config-if) # <b>exit</b>	インターフェイスコンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。

## IGP で使用できる MPLS トラフィック エンジニアリング トンネルの設定

IGP で使用できる MPLS TE トンネルを設定するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。

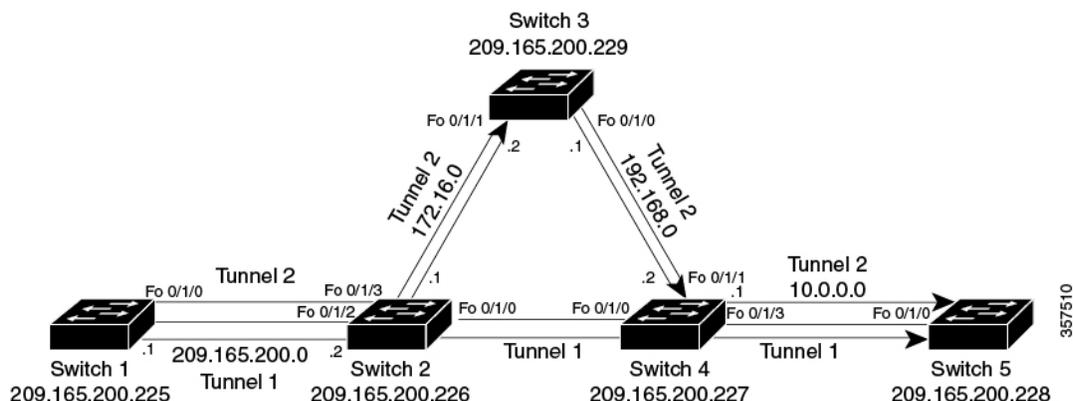
	コマンドまたはアクション	目的
ステップ 2	<b>configure terminal</b> 例 :  Device# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	<b>interface tunnel number</b> 例 :  Device(config)# <b>interface tunnel10</b>	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<b>ip unnumbered type number</b> 例 :  Device(config-if)# <b>ip unnumbered loopback 0</b>	トンネル インターフェイスに IP アドレスを割り当てます。  MPLS トラフィック エンジニアリング トンネル インターフェイスは単一方向リンクを表すため、番号なしにする必要があります。
ステップ 5	<b>tunnel destination ip-address</b> 例 :  Device(config-if)# <b>tunnel destination 10.20.1.1</b>	トンネルの宛先を指定します。  <i>ip-address</i> キーワードは、ホスト宛先の IP アドレス（ドット付き 10 進表記）です。
ステップ 6	<b>tunnel mode mpls traffic-eng</b> 例 :  Device(config-if)# <b>tunnel mode mpls traffic-eng</b>	トンネル カプセル化モードを MPLS トラフィック エンジニアリングに設定します。
ステップ 7	<b>tunnel mpls traffic-eng bandwidth bandwidth</b> 例 :  Device(config-if)# <b>tunnel mpls traffic-eng bandwidth 1000</b>	MPLS トラフィック エンジニアリング トンネルの帯域幅を設定します。
ステップ 8	<b>tunnel mpls traffic-eng path-option number {dynamic   explicit {name path-name}   identifier path-number} [lockdown]</b> 例 :  Device(config-if)# <b>tunnel mpls traffic-eng path-option 1 explicit identifier 1</b>	指定した IP 明示パス、またはトラフィック エンジニアリング トポロジ データベースからダイナミックに計算されたパスを使用するように、トンネルを設定します。  明示パスが現在使用できない場合は、ダイナミックパスが使用されます。

	コマンドまたはアクション	目的
ステップ 9	<b>exit</b>  例：  Device(config-if)# <b>exit</b>	インターフェイスコンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。

## MPLS トラフィック エンジニアリングおよび拡張機能の設定例

次の図は、MPLS トポロジの例を示しています。この例では、ポイントツーポイントの発信インターフェイスを指定しています。続く各セクションでは、MPLS トラフィック エンジニアリング、および図 3 に示す基本的なトンネル設定を実装するときに入力するコンフィギュレーションコマンドの例を示します。

図 22: MPLS トラフィック エンジニアリング トンネルの設定例



### 例：IS-IS を使用した MPLS トラフィック エンジニアリングの設定

次に、MPLS TE を設定し、IS-IS ルーティングをイネーブルにするときに入力するコマンドの例を示します（図 1 を参照）。



(注) ネットワークのトラフィック エンジニアリング対象部分にあるすべてのルータで次のコマンドを入力します。

#### デバイス 1：MPLS トラフィック エンジニアリングの設定

MPLS トラフィック エンジニアリングを設定するには、次のコマンドを入力します。

```
ip cef
mpls traffic-eng tunnels
interface loopback 0
ip address 10.0.0.0 255.255.255.254
ip router isis
interface Fo 1/0/0
ip address 209.165.200.1 255.255.0.0
ip router isis
mpls traffic-eng tunnels
ip rsvp bandwidth 1000
```

## デバイス 1 : IS-IS 設定

IS-IS ルーティングをイネーブルにするには、次のコマンドを入力します。

```
router isis
network 47.0000.0011.0011.00
is-type level-1
metric-style wide
mpls traffic-eng router-id loopback0
mpls traffic-eng level-1
```

## 例 : OSPF を使用した MPLS トラフィック エンジニアリングの設定

次に、MPLS トラフィック エンジニアリングを設定し、OSPF ルーティングをイネーブルにするときに入力するコマンドの例を示します (図 1 を参照)。



- (注) ネットワークのトラフィック エンジニアリング対象部分にあるすべてのルータで次のコマンドを入力します。

## デバイス 1 : MPLS トラフィック エンジニアリングの設定

MPLS トラフィック エンジニアリングを設定するには、次のコマンドを入力します。

```
ip cef
mpls traffic-eng tunnels
interface loopback 0
ip address 209.165.200.225 255.255.255.255
interface Fo 1/0/0
ip address 209.165.200.1 255.255.0.0
mpls traffic-eng tunnels
ip rsvp bandwidth 1000
```

## デバイス 1 : OSPF 設定

OSPF をイネーブルにするには、次のコマンドを入力します。

```
router ospf 0
network 209.165.200.0.0.0.255.255 area 0
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
```

## 例：MPLS トラフィック エンジニアリング トンネルの設定

次に、ダイナミックパストンネルとそのトンネルの明示パスを設定する例を示します。MPLS トラフィック エンジニアリング トンネルを設定する前に、指定のルータ（この場合、ルータ 1）で適切なグローバルコマンドおよびインターフェイスコマンドを入力します。

### デバイス 1：ダイナミックパストンネルの設定

ダイナミックパスを使用するようにトンネルを設定するには、次のコマンドを入力します。

```
interface tunnel1
ip unnumbered loopback 0
tunnel destination 209.165.200.228
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng bandwidth 100
tunnel mpls traffic-eng priority 1 1
tunnel mpls traffic-eng path-option 1 dynamic
```

### デバイス 1：ダイナミックパストンネルの確認

トンネルがアップ状態になっていることを確認するには、次のコマンドを入力します。

```
show mpls traffic-eng tunnels
show ip interface tunnel1
```

### デバイス 1：明示パスの設定

明示パスを設定するには、次のコマンドを入力します。

```
ip explicit-path identifier 1
next-address 209.165.200.1
next-address 172.16.0.1
next-address 192.168.0.1
next-address 10.0.0.1
```

### デバイス 1：明示パストンネルの設定

明示パスを使用するようにトンネルを設定するには、次のコマンドを入力します。

```
interface tunnel2
ip unnumbered loopback 0
tunnel destination 209.165.200.228
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng bandwidth 100
tunnel mpls traffic-eng priority 1 1
tunnel mpls traffic-eng path-option 1 explicit identifier 1
```

### デバイス 1：明示パストンネルの確認

トンネルがアップ状態になっていることを確認するには、次のコマンドを入力します。

```
show mpls traffic-eng tunnels
show ip interface tunnel2
```

## 例：トンネル経由の拡張 SPF ルーティングの設定

ここでは、IGP での拡張 SPF 計算でトンネルが考慮されるようにして、適切なネットワークプレフィックスに対するトンネル経由のルートを実インストールするコマンドを示します。

### デバイス 1：IGP 拡張 SPF による考慮の設定

IGP が拡張最短パス優先（SPF）計算でトンネル（トンネルがアップ状態の場合）を使用するように指定するには、次のコマンドを入力します。

```
interface tunnell
 tunnel mpls traffic-eng autoroute announce
```

### デバイス 1：ルートとトラフィックの確認

トンネルがアップ状態になっており、トラフィックがトンネル経由でルーティングされていることを確認するには、次のコマンドを入力します。

```
#show mpls traffic-eng tunnels tu12001 brief
Signalling Summary:
LSP Tunnels Process: running
Passive LSP Listener: running
RSVP Process: running
Forwarding: enabled
auto-tunnel:
p2p Disabled (0), id-range:62336-64335

Periodic reoptimization: every 3600 seconds, next in 694 seconds
Periodic FRR Promotion: Not Running
Periodic auto-bw collection: every 300 seconds, next in 94 seconds
SR tunnel max label push: 2 primary path labels (2 repair path labels)
TUNNEL NAME DESTINATION UP IF DOWN IF STATE/PROT
tu12001 2.2.2.2 - Po114 up/up
```

## その他の参考資料

ここでは、MPLS トラフィック エンジニアリングおよび拡張機能に関する関連資料について説明します。

### 関連資料

関連項目	マニュアルタイトル
IS-IS コマンド	『Cisco IOS IP Routing Protocols Command Reference』
OSPF コマンド	『Cisco IOS IP Routing Protocols Command Reference』
MPLS TE コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』
RSVP コマンド	『Cisco IOS Quality of Service Solutions Command Reference』

## MIB

MIB	MIB のリンク
なし	<p>選択したプラットフォーム、Cisco IOS ソフトウェア リリース、およびフィーチャセットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFC

RFC	タイトル
1142	『IS-IS』
1195	『Use of OSI IS-IS for Routing in TCP/IP and Dual Environments』
2205	『Resource ReSerVation Protocol (RSVP)』
2328	『OSPF Version 2』
2370	『The OSPF Opaque LSA Option』

## シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<p><a href="http://www.cisco.com/en/US/support/index.html">http://www.cisco.com/en/US/support/index.html</a></p>

# MPLS トラフィック エンジニアリングおよび拡張機能の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Bengaluru 17.6.1	MPLS トラフィック エンジニアリングおよび拡張機能	マルチプロトコル ラベル スイッチング (MPLS) には、レイヤ 2 テクノロジーとレイヤ 3 テクノロジーが統合されています。従来のレイヤ 2 機能をレイヤ 3 で使用可能にすることで、MPLS はトラフィック エンジニアリングを可能にしています。したがって、1 層のネットワーク内で、今までレイヤ 2 ネットワークの上にレイヤ 3 ネットワークを重ねることによって初めて実現できていた機能を提案できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、<https://cfmng.cisco.com/> にアクセスします。





## 第 14 章

# MPLS トラフィック エンジニアリング - バンドル インターフェイス サポート の 設定

- [MPLS TE - バンドル インターフェイス サポート の 前提条件 \(207 ページ\)](#)
- [MPLS TE - バンドル インターフェイス サポート の 制約事項 \(208 ページ\)](#)
- [MPLS TE - バンドル インターフェイス サポート について \(208 ページ\)](#)
- [MPLS TE - バンドル インターフェイス サポート の 設定方法 \(210 ページ\)](#)
- [MPLS トラフィック エンジニアリング - バンドル インターフェイス サポート の 設定例 \(211 ページ\)](#)
- [MPLS トラフィック エンジニアリング - バンドル インターフェイス サポート の 関連資料 \(214 ページ\)](#)
- [MPLS トラフィック エンジニアリング - バンドル インターフェイス サポート の 機能情報 \(214 ページ\)](#)

## MPLS TE - バンドル インターフェイス サポート の 前提条件

- マルチプロトコル ラベル スイッチング (MPLS) トラフィック エンジニアリング (TE) トンネルを設定してください。
- グローバル コンフィギュレーション モードで、Cisco Express Forwarding (CEF) をイネーブルにしてください。
- Resource Reservation Protocol (RSVP) 機能をイネーブルにしてください。
- EtherChannel を設定してください。
- Gigabit EtherChannel を設定してください。

## MPLS TE - バンドル インターフェイス サポート の制約事項

- スイッチ 仮想 インターフェイス (SVI) を介した トラフィック エンジニアリング は、SVI が 1 つの ポイント ツー ポイント インターフェイス として 機能する 複数の リンク の バンドル で 構成 されていない 限り サポート され ません。
- また、バンドル インターフェイス に 有効な IP アドレス が 設定 されて いて、メンバー リンク には IP アドレス が 設定 されていない ことが 条件 となります。

## MPLS TE - バンドル インターフェイス サポート について

MPLS トラフィック エンジニアリング - バンドル インターフェイス サポート 機能 を 使用 すると、バンドル インターフェイス (EtherChannel および Gigabit EtherChannel (GEC)) を 介して マルチプロトコル ラベル スイッチング (MPLS) トラフィック エンジニアリング (TE) トンネル を イネーブル に する ことが できます。

リソース 予約 プロトコル (RSVP) により、メンバー リンク が 追加 または 削除 された 場合 や、リンク が アクティブ または 非アクティブ に なった 場合 に 発生 する 帯域幅 変更 が TE に 通知 され ます。TE は 内部 ゲートウェイ プロトコル (IGP) フラッドイング を 介して、ネットワーク 内の 他の ノード に 通知 します。デフォルト では、TE ラベル スイッチ ドパス (LSP) が 利用 できる 帯域幅 は、インターフェイス 帯域幅 の 75% です。バンドル インターフェイス で RSVP コマンド を 使用 すると、TE LSP が 利用 できる グローバル な 帯域幅 の 割合 を 変更 できます。帯域 予約 と プリエンブション は サポート されて います。

ここでは、MPLS トラフィック エンジニアリング の バンドル インターフェイス サポート について 説明 します。

## Cisco EtherChannel の概要

Cisco EtherChannel テクノロジー は、標準 ベース の 802.3 全二重 形式 ファスト イーサネット に 基づいて 構築 され、キャンパス ネットワーク バックボーン に 信頼性 の 高い、高速 な ソリューション を 提供 します。EtherChannel テクノロジー は、Fast EtherChannel 接続、Gigabit EtherChannel 接続、10 Gigabit EtherChannel 接続 において、それぞれ 最大 800 Mbps、8 Gbps、または 80 Gbps の 集約 帯域幅 を 提供 すること により、キャンパス に スケーラブル な 帯域幅 を 提供 します。これらの 接続 速度 は それぞれ、使用 されている リンク の 速度 (100 Mbps、1 Gbps、10 Gbps) に 合わせて 異なる 場合 があります。帯域幅 を 必要 と する 環境 では、EtherChannel テクノロジー を 使用 すること で トラフィック を 集約 し、オーバーサブスクリプション を 最小限 に 抑え、効果的 な リンク 復元 メカニズム を 実装 することが できます。

## Cisco EtherChannel の利点

Cisco EtherChannel テクノロジーを使用すると、単独のリンクを使用するイーサネットテクノロジーに比べて、サーバ、ルータ、およびスイッチ間の帯域幅を拡張することができます。

Cisco EtherChannel テクノロジーには段階的に帯域幅を拡張できるという利点があり、その他にも次の利点があります。

- **標準規格に基づく設計**：Cisco EtherChannel テクノロジーは、複数の全二重ポイントツーポイントリンクをグループ化することにより、IEEE 802.3 対応イーサネット上で動作するように設計されています。EtherChannel テクノロジーでは、全二重の自動ネゴシエーションと自動検知を行うために IEEE 802.3 のメカニズムが必要に応じて使用されます。
- **柔軟に拡張できる帯域幅**：Cisco EtherChannel テクノロジーでは、集約するリンクの速度に応じて、100 Mbps、1 Gbps、または 10 Gbps の倍数単位で帯域幅集約が行われます。たとえば、全二重ファストイーサネットリンクのペアで構成される EtherChannel テクノロジーを展開することで、ワイヤリング クローゼットとデータセンターの間で 400 Mbps 以上の帯域幅を提供することができます。データセンターでは、サーバとネットワーク バックボーンの間で最大 800 Mbps の帯域幅を提供することができ、帯域幅を段階的に拡張することができます。
- **ロード バランシング**：Cisco EtherChannel テクノロジーはいくつかのファストイーサネットリンクで構成され、これらのリンク間のトラフィックをロードバランシングできます。ユニキャスト、ブロードキャスト、およびマルチキャストトラフィックはリンク全体に均等に分散され、その結果パフォーマンスが向上し、冗長性のあるパラレルパスが実現します。いずれかのリンクに障害が発生すると、トラフィックはユーザの介入なしにチャンネル内の残りのリンクにリダイレクトされ、パケットの損失は最小限に抑えられます。
- **復元力と迅速なコンバージェンス**：いずれかのリンクに障害が発生した場合、Cisco EtherChannel テクノロジーは残りのリンクの間で負荷を再分散することにより、自動リカバリを行います。リンクに障害が発生すると、Cisco EtherChannel テクノロジーは障害が発生したリンクから残りのリンクに 1 秒以内にトラフィックをリダイレクトします。このコンバージェンスはエンドユーザに影響することなく実行され、ホストのプロトコル タイマーの時間切れやセッションの切断などは発生しません。

## Cisco Gigabit EtherChannel の概要

Cisco Gigabit EtherChannel (GEC) は、ギガビット/秒 (Gbps) 単位の転送レートを誇る高性能イーサネットテクノロジーです。Gigabit EtherChannel は、個々のギガビットイーサネットリンク (Gigabit Ethernet および 10 Gigabit Ethernet) を 1 つの論理リンクにバンドルすることにより、最大 8 つの物理リンクの集約帯域幅を提供します。各 EtherChannel のすべての LAN ポートが同じ速度に設定され、レイヤ 2 LAN ポートまたはレイヤ 3 LAN ポートのどちらか一方として設定されている必要があります。EtherChannel 内の 1 つのリンクに到達したインバウンドブロードキャストおよびマルチキャストパケットは、EtherChannel 内の別のリンクに戻されることはありません。

## EtherChannel でのロードバランシング

ロードバランシングは、TE に使用できる実際の帯域幅に影響します。マルチリンク ロードバランシングでは、パケット単位のロードバランシング方式が使用されます。バンドル インターフェイスの帯域幅をすべて利用できます。EtherChannel ロードバランシングには、トラフィック パターンとロードバランシングの設定に応じて、さまざまなロードバランシング方式があります。TE に使用可能な合計帯域幅は 1 つのメンバー リンクの帯域幅までに制限される場合があります。

## MPLS TE - バンドル インターフェイス サポート の設定方法

ここでは、MPLS トラフィック エンジニアリングのバンドル インターフェイス サポート の設定方法について説明します。

### EtherChannel インターフェイスでの MPLS トラフィック エンジニアリングの設定

EtherChannel インターフェイスで MPLS トラフィック エンジニアリングを設定するには、次の手順を実行します。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例 : Device# <b>configure terminal</b>	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 3	<b>interface type number [name-tag]</b> 例 : Device(config)# <b>interface port-channel 1</b>	EtherChannel バンドルを作成し、バンドルにグループ番号を割り当て、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<b>ip address ip-address mask [secondary]</b> 例 :	EtherChannel グループの IP アドレスを指定します。

	コマンドまたはアクション	目的
	Device(config-if) # <b>ip address 10.0.0.4 255.255.255.0</b>	
ステップ 5	<b>mpls traffic-eng tunnels</b>  例 :  Device(config-if) # <b>mpls traffic-eng tunnels</b>	インターフェイスの MPLS TE トンネル シグナリングをイネーブルにします。  • シグナリングをイネーブルにする前に、デバイスで MPLS TE トンネルはイネーブルにする必要があります。
ステップ 6	<b>ip rsvp bandwidth [interface-kbps] [single-flow-kbps]</b>  例 :  Device(config-if) # <b>ip rsvp bandwidth 100</b>	インターフェイスで IP 用の RSVP をイネーブルにし、RSVP 帯域幅プールで利用できるインターフェイスの合計帯域幅の割合を指定します。
ステップ 7	<b>end</b>  例 :  Device(config-if) # <b>end</b>	インターフェイスコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

## MPLS トラフィック エンジニアリング - バンドル インターフェイス サポートの設定例

ここでは、MPLS トラフィック エンジニアリング - バンドル インターフェイス サポートの設定例を紹介します。

### 例 : EtherChannel インターフェイスでの MPLS TE の設定

次に、EtherChannel インターフェイスで MPLS TE を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface port-channel 1
Device(config-if)# ip address 10.0.0.4 255.255.255.0
Device(config-if)# mpls traffic-eng tunnels
Device(config-if)# ip rsvp bandwidth 100
Device(config-if)# end
```

## 例 : Gigabit EtherChannel での MPLS トラフィック エンジニアリング-バンドルインターフェイス サポートの設定

次の例は、シスコデバイス上の GEC で MPLS トラフィック エンジニアリング-バンドルインターフェイス サポートをイネーブルにする方法を示しています。

```

Device> enable
Device# configure terminal

! Enable global MPLS TE on routers
Device(config)# router ospf 100
Device(config-router)# network 10.0.0.1 0.0.0.255 area 0
Device(config-router)# mpls traffic-eng area 0
Device(config-router)# mpls traffic-eng router-id Loopback 0
Device(config-router)# exit

! Configure GEC interface and enable MPLS TE and RSVP on interface
Device(config)# interface Port-channel 1
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# mpls traffic-eng tunnels
Device(config-if)# ip rsvp bandwidth
Device(config-if)# exit

! Define explicit path
Device(config)# ip explicit-path name primary enable
Device(cfg-ip-expl-path)# next-address 172.12.1.2
Device(cfg-ip-expl-path)# next-address 172.23.1.2
Device(cfg-ip-expl-path)# next-address 172.34.1.2
Device(cfg-ip-expl-path)# next-address 10.4.4.4
Device(cfg-ip-expl-path)# exit

! Configure primary tunnel on head-end device
Device(config)# interface Tunnel 14
Device(config-if)# ip unnumbered Loopback 0
Device(config-if)# tunnel mode mpls traffic-eng
Device(config-if)# tunnel destination 10.10.10.0
Device(config-if)# tunnel mpls traffic-eng autoroute announce
Device(config-if)# tunnel mpls traffic-eng path-option 10 explicit name primary
Device(config-if)# exit

! Configure GEC interface
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# no ip address
Device(config-if)# channel-group 1 mode active
Device(config-if)# exit

! Configure GEC interface
Device(config)# interface GigabitEthernet 0/0/2
Device(config-if)# no ip address
Device(config-if)# channel-group 1 mode active
Device(config-if)# exit

```

**show mpls traffic-eng tunnels** コマンドの出力には、1 つのトンネルに関する情報、またはデバイス上で設定されているすべてのトンネルに関する 1 行の情報が表示されます。

```
Device# show mpls traffic-eng tunnels tunnel 14
```

```

Name: Cat9k_t14                               (Tunnel10) Destination: 10.4.4.4
Status:
  Admin: up           Oper: up           Path: valid           Signalling: connected
  path option 1, type explicit toR4overR3R3 (Basis for Setup, path weight 3)

Config Parameters:
  Bandwidth: 0           kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 0 [0] bw-based
  auto-bw: disabled
Active Path Option Parameters:
  State: explicit path option 1 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

  InLabel : -
  OutLabel : Port-channell, 1608
  Next Hop : 172.16.1.2
  RSVP Signalling Info:
    Src 10.1.1.1, Dst 10.4.4.4, Tun_Id 14, Tun_Instance 35
  RSVP Path Info:
    My Address: 172.12.1.1
    Explicit Route: 172.12.1.2 172.23.1.1 172.23.1.2 172.34.1.1
                    172.34.1.2 10.4.4.4

History:
  Tunnel:
    Time since created: 17 hours
    Time since path change: 18 minutes, 22 seconds
    Number of LSP IDs (Tun_Instances) used: 35
  Current LSP: [ID: 35]
    Uptime: 18 minutes, 22 seconds
    Selection: reoptimization
  Prior LSP: [ID: 32]
    ID: path option unknown
    Removal Trigger: signalling shutdown

```

Device# **show mpls traffic-eng tunnels brief**

show mpls traffic-eng tunnels brief

Signalling Summary:

```

LSP Tunnels Process:           running
Passive LSP Listener:         running
RSVP Process:                 running
Forwarding:                   enabled
Periodic reoptimization:      every 3600 seconds, next in 3299 seconds
Periodic FRR Promotion:       Not Running
Periodic auto-bw collection:   every 300 seconds, next in 299 seconds

```

P2P TUNNELS/LSPs:

TUNNEL NAME	DESTINATION	UP IF	DOWN IF	STATE/PROT^M
Cat9k_t14	10.4.1.1		-	Po12 up/up

On Mid Router:

P2P TUNNELS/LSPs:

TUNNEL NAME	DESTINATION	UP IF	DOWN IF	STATE/PROT
Cat9k_t14	10.4.1.1		Po12	Po23 up/up
Cat9k_t23	10.2.1.1		Po25	- up/up

## MPLS トラフィック エンジニアリング-バンドルインターフェイス サポートの関連資料

### 関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	<a href="#">『Cisco IOS Master Commands List, All Releases』</a>
MPLS トラフィック エンジニアリング コマンド	<a href="#">『Cisco IOS Multiprotocol Label Switching Command Reference』</a>
IPv6 コマンド	<a href="#">『IPv6 Command Reference』</a>

### シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## MPLS トラフィック エンジニアリング-バンドルインターフェイス サポートの機能情報

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Bengaluru 17.6.1	MPLS トラフィック エンジニアリング - バンドル インターフェイス サポート	MPLS トラフィック エンジニアリング - バンドル インターフェイス サポート機能を使用すると、バンドル インターフェイス (EtherChannel、Gigabit EtherChannel (GEC)) を介して MPLS トラフィック エンジニアリング トンネルをイネーブルにすることができます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、<https://cfngng.cisco.com/>にアクセスします。





## 第 15 章

# MPLS トラフィック エンジニアリング (TE) : IP 明示アドレス除外の設定

- [MPLS トラフィック エンジニアリング \(TE\) - IP 明示アドレス除外の前提条件 \(217 ページ\)](#)
- [MPLS トラフィック エンジニアリング \(TE\) : IP 明示アドレス除外の制約事項 \(218 ページ\)](#)
- [MPLS トラフィック エンジニアリング \(TE\) - IP 明示アドレス除外の概要 \(218 ページ\)](#)
- [MPLS トラフィック エンジニアリング \(TE\) - IP 明示アドレス除外の設定方法 \(219 ページ\)](#)
- [MPLS トラフィック エンジニアリング \(TE\) - IP 明示アドレス除外の設定例 \(222 ページ\)](#)
- [その他の参考資料 \(223 ページ\)](#)
- [MPLS トラフィック エンジニアリング \(TE\) - 明示アドレス除外の機能履歴 \(224 ページ\)](#)

## MPLS トラフィック エンジニアリング (TE) - IP 明示アドレス除外の前提条件

IP 明示アドレス除外をサポートするには、ネットワークで次の Cisco IOS 機能がサポートされている必要があります。

- MPLS
- IP シスコ エクスプレス フォワーディング
- Intermediate System-to-Intermediate System (IS-IS) または Open Shortest Path First (OSPF)

# MPLS トラフィック エンジニアリング (TE) : IP 明示アドレス除外の制約事項

MPLS TE は、**exclude-address** コマンドで設定されたすべての除外アドレスか、**next-address** コマンドで設定されたすべての包含アドレスのいずれか（両方の組み合わせではない）で構成された IP 明示パスを受け入れます。

## MPLS トラフィック エンジニアリング (TE) - IP 明示アドレス除外の概要

MPLS トラフィック エンジニアリング (TE) - IP 明示アドレス除外機能は、マルチプロトコル ラベル スイッチング (MPLS) の TE ラベル スイッチド パス (LSP) のパスからリンクまたは ノードを除外する手段を提供します。

この機能を有効にするには、**ip explicit-path** コマンドを使用します。このコマンドにより、IP 明示パスを作成し、パスを指定するためのコンフィギュレーション サブモードを開始できます。この機能により、サブモードコマンドに、パスから除外するアドレスを指定するための **exclude-address** コマンドが追加されます。

MPLS TE LSP の除外アドレスが、フラッドイングされたリンクを識別している場合、Constraint-based Shortest Path First (CSPF) ルーティング アルゴリズムでは、LSP のパスの計算時にそのリンクが考慮されません。除外アドレスが、フラッドイングされた MPLS TE ルータ ID を指定している場合、CSPF ルーティング アルゴリズムでは、LSP のパスがデバイス ID で識別されるノードを経由することが許可されません。

## MPLS トラフィック エンジニアリング

MPLS は、インターネット技術特別調査委員会 (IETF) により指定されたフレームワークであり、ネットワークを介するトラフィックフローの効率的な指定、ルーティング、フォワーディング、およびスイッチングを可能にします。

トラフィック エンジニアリング (TE) は、ハイプライオリティのトラフィックに常に十分な帯域幅が確保されるように、帯域割り当てを調整するプロセスです。

MPLS TE では、上流のデバイスが特定のトラフィックストリームのネットワークトンネルを作成してから、そのトンネルに使用可能な帯域幅を修正します。

## シスコ エクスプレス フォワーディング

Cisco Express Forwarding は、デバイス内部の高度なレイヤ 3 スイッチングテクノロジーです。これにより、Cisco デバイスが入力インターフェイスから出力インターフェイスにパケットを転送するときに使用する最速の方法が定義されます。**ip cef** コマンドを使用すると、Cisco Express

Forwarding がグローバルに有効になります。 **ip route-cache cef** コマンドを使用すると、インターフェイス上で Cisco Express Forwarding が有効になります。

## MPLS トラフィック エンジニアリング (TE) - IP 明示アドレス除外の設定方法

ここでは、MPLS トラフィック エンジニアリング (TE) - IP 明示アドレス除外のさまざまな設定手順について説明します。

### IP 明示アドレス除外の設定

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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 3	<b>ip explicit-path {name path-name   identifier number} [enable   disable]</b> 例： Device(config)# <b>ip explicit-path name OmitR12</b>	明示パスの名前または番号を指定し、パスをイネーブルにして、明示パス コンフィギュレーション モードに切り替えます。
ステップ 4	<b>exclude-address ip-address</b> 例： Device(cfg-ip-expl-path)# <b>exclude-address 10.12.12.12</b>	指定したリンクまたはノードを、コンストレイントベースの SPF による考慮から除外します。  • <i>ip-address</i> は、ノードのリンク アドレスまたはルータ ID です。
ステップ 5	<b>exit</b> 例： Device(cfg-ip-expl-path)# <b>exit</b>	明示パス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	<b>exit</b> 例 :  Device(config)# <b>exit</b>	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	<b>show ip explicit-path</b> 例 :  Device# <b>show ip explicit-path</b>	設定した IP 明示パスの情報を表示します。

## MPLS トラフィック エンジニアリング トンネルの設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  Device> <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例 :  Device# <b>configure terminal</b>	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 3	<b>interface tunnel number</b> 例 :  Device(config)# <b>interface tunnel11</b>	インターフェイスタイプを設定し、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ます。
ステップ 4	<b>ip unnumbered loopback0</b> 例 :  Device(config-if)# <b>ip unnumbered loopback0</b>	トンネルインターフェイスに IP アドレスを割り当てます。  <ul style="list-style-type: none"> <li>MPLS トラフィック エンジニアリングトンネルインターフェイスは単一方向リンクを表すため、番号なしにする必要があります。</li> </ul>
ステップ 5	<b>tunnel destination ip-address</b> 例 :  Device(config-if)# <b>tunnel destination 10.11.11.11</b>	トンネルの宛先を指定します。  <ul style="list-style-type: none"> <li>トンネルの宛先は、宛先デバイスの MPLS トラフィック エンジニアリング ルータ ID にする必要があります。</li> </ul>

	コマンドまたはアクション	目的
ステップ 6	<b>tunnel mode mpls traffic-eng</b> 例 : <pre>Device(config-if)# tunnel mode mpls traffic-eng</pre>	トンネルカプセル化モードを MPLS トラフィック エンジニアリング に設定します。
ステップ 7	<b>tunnel mpls traffic-eng bandwidth bandwidth</b> 例 : <pre>Device(config-if)# tunnel mpls traffic-eng bandwidth 100</pre>	MPLS トラフィック エンジニアリング トンネルの帯域幅を設定します。
ステップ 8	<b>tunnel mpls traffic-eng path-option number {dynamic   explicit {name path-name   ID path-number}} [lockdown]</b> 例 : <pre>Device(config-if)# tunnel mpls traffic-eng path-option 2 dynamic</pre>	<p>指定した IP 明示パス、またはトラフィック エンジニアリング トポロジ データベースからダイナミックに計算されたパスを使用するように、トンネルを設定します。</p> <ul style="list-style-type: none"> <li>明示パスが使用可能でない場合は、ダイナミックパスが使用されます。</li> </ul> <p>(注) 除外アドレスを指定するパスオプションを設定するには、(dynamic キーワードではなく) explicit キーワードを指定し、「<a href="#">IP 明示アドレス除外の設定 (219 ページ)</a>」の項の手順に従って設定した IP 明示パスを指定します。</p>
ステップ 9	<b>exit</b> 例 : <pre>Device(config-if)# exit</pre>	インターフェイス コンフィギュレーション モードを終了します。
ステップ 10	<b>exit</b> 例 : <pre>Device(config)# exit</pre>	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 11	<b>show mpls traffic eng tunnels</b> 例 : Device# <b>show mpls traffic eng tunnels</b>	トンネルの情報（トンネルが動作中であれば現在のトンネルパスを含む）を表示します。 <ul style="list-style-type: none"> <li>• コマンド出力を参照すると、トンネルの構築に使用されたパスを判断できます。<b>exclude-address</b> コマンドを入力した場合、指定したリンクまたはノードは表示されません。</li> </ul>

## MPLS トラフィック エンジニアリング (TE) - IP 明示アドレス除外の設定例

ここでは、MPLS トラフィックエンジニアリング (TE) - IP 明示アドレス除外の設定例を紹介します。

### 例 : IP 明示アドレス除外の設定

次に、2つのパス オプションを使用して MPLS TE トンネルを設定する例を示します。1つは除外アドレスを使用した優先的な明示パスで、もう1つはバックアップのダイナミックパスです。

OmitR12 という名前の IP 明示パスを設定します。これにより、ルータ ID が 10.12.12.12 のルータが除外されます。

```
ip explicit-path name OmitR12
exclude-address 10.12.12.12
Explicit Path name OmitR12:
1: exclude-address 10.12.12.12
exit
```

明示パスの設定を確認するには、**show ip explicit-path** コマンドを使用します。

```
show ip explicit-paths name OmitR12
PATH OmitR12 (loose source route, path complete, generation 3)
1: exclude-address 10.12.12.12
```



- (注) ネットワーク内の LSR (ノード) のルータ ID がわかっている必要があります。この例では、その 10.12.12.12 がルータ ID です。この ID がわからない場合、指定したアドレスがリンク ID の IP アドレスかルータ ID の IP アドレスかが不明になります。

## 例 : MPLS トラフィック エンジニアリング トンネルの設定

次の例では、トンネル 11 を 2 つのオプションで設定します。優先されるパスオプションは IP 明示パスである **OmitR2** です。

```
interface tunne l11
ip unnumbered loopback0
tunnel destination 10.11.11.11
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 1 explicit name OmitR12
tunnel mpls traffic-eng path-option 2 dynamic
```



- (注) この他にも、TE トンネルのプロパティ（帯域幅やプライオリティなど）を設定するためのコマンドがあります。これらのコマンドの詳細については、『*Cisco IOS IP Switching Services Configuration Guide*』を参照してください。

## その他の参考資料

ここでは、MPLS トラフィック エンジニアリング (TE) - IP 明示アドレス除外機能の関連資料について説明します。

### 関連資料

関連項目	マニュアルタイトル
Cisco IOS コマンド	<a href="#">『Cisco IOS Master Commands List, All Releases』</a>
MPLS コマンド	<a href="#">『Cisco IOS Multiprotocol Label Switching Command Reference』</a>
MPLS 設定情報	<a href="#">『Cisco IOS XE Multiprotocol Label Switching Configuration Guide』</a>

### 標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

## MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS ソフトウェアリリース、およびフィーチャセットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

## シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<a href="http://www.cisco.com/en/US/support/index.html">http://www.cisco.com/en/US/support/index.html</a>

## MPLS トラフィック エンジニアリング (TE) - 明示アドレス除外の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Bengaluru 17.6.1	MPLS トラフィック エンジニアリング (TE) - IP 明示アドレス除外	MPLS トラフィック エンジニアリング (TE) - IP 明示アドレス除外機能は、マルチプロトコル ラベル スイッチング (MPLS) の TE ラベルスイッチドパス (LSP) からリンクまたはノードを除外する手段を提供します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、<https://cfmng.cisco.com/> にアクセスします。





## 第 16 章

# MPLS トラフィック エンジニアリング - LSP 属性の設定

- [MPLS トラフィック エンジニアリング - LSP 属性の前提条件 \(227 ページ\)](#)
- [MPLS トラフィック エンジニアリング - LSP 属性の制約事項 \(227 ページ\)](#)
- [MPLS トラフィック エンジニアリング - LSP 属性について \(228 ページ\)](#)
- [MPLS トラフィック エンジニアリング - LSP 属性の設定方法 \(232 ページ\)](#)
- [MPLS トラフィック エンジニアリング - LSP 属性の設定例 \(258 ページ\)](#)
- [その他の参考資料 \(263 ページ\)](#)
- [MPLS トラフィック エンジニアリング - LSP 属性の機能情報 \(264 ページ\)](#)

## MPLS トラフィック エンジニアリング - LSP 属性の前提条件

MPLS トラフィック エンジニアリング - LSP 属性機能では、LSP 属性リストまたは帯域幅上書きのパスオプション機能を設定する前に MPLS TE トンネルを設定する必要があります。

## MPLS トラフィック エンジニアリング - LSP 属性の制約事項

- 異なるプライオリティのパスオプション間での再最適化はサポートされていません。
- LSP 属性リスト機能では、パスオプションの優先順位を設定する際、トンネルやトンネルで使用される他のパスオプションに設定されている優先順位と一致させる必要があります。

# MPLS トラフィック エンジニアリング - LSP 属性について

ここでは、MPLS トラフィック エンジニアリング - LSP 属性について説明します。

## 『MPLS Traffic Engineering—LSP Attributes』

このマニュアルでは、マルチプロトコル ラベル スイッチング (MPLS) トラフィック エンジニアリング (TE) トンネルに関連付けられたパス オプションのラベル スイッチドパス (LSP) 属性の設定方法について説明します。

MPLS トラフィック エンジニアリング - LSP 属性機能は、MPLS TE 機能の拡張版であり、LSP 属性リスト機能と帯域幅上書きのパス オプション機能を備えています。これらの機能によって、MPLS TE トンネルパス オプションの LSP 属性を柔軟に設定できるようになります。LSP 属性リストを使用すると、TE トンネルのパス オプションに対して複数の LSP 属性を適用できます。必要な LSP 属性が帯域幅だけである場合、帯域幅上書きのパス オプションを設定できます。

## MPLS トラフィック エンジニアリング - LSP 属性の利点

MPLS トラフィック エンジニアリング - LSP 属性機能は、LSP 属性リスト機能と帯域幅上書きのパス オプション機能を提供します。これらの機能には、次の利点があります。

- LSP 属性リスト機能によって、TE トンネルの複数の LSP 固有のパス オプションの値を設定できる。
- 1 つ以上の TE トンネルで、LSP 属性リストを参照することによって特定のパス オプションを指定できる。
- LSP 属性リストによって、MPLS TE ユーザ インターフェイスがより柔軟で使いやすくなり、拡張と管理が簡単になる。
- 帯域幅上書きのパス オプション機能によって、TE トンネルが帯域幅の制約を緩和できるパス オプションに一時的にフォールバックできる単一のコマンドが提供される。

## トラフィック エンジニアリング帯域幅

MPLS トラフィック エンジニアリングを使用すると、IP トラフィックの制約ベースのルーティング (CBR) が可能になります。CBR によって満たされる制約の 1 つに、選択されたパスにおける必要な帯域幅の可用性があります。通常の TE トンネル帯域幅は、グローバルプールと呼ばれます。サブプール帯域幅は、グローバルプールの一部です。サブプール帯域幅は、使用中以外はグローバルプールから予約されません。そのため、サブプールトンネルでは、サブプール以外のトンネルよりも高いプライオリティが必要となります。

LSP 属性帯域幅パス オプションは、グローバルプール（デフォルト）またはサブプールの帯域幅を使用するように設定できます。パス オプションの帯域幅値は任意の有効な値に設定でき、プールはトンネルに設定されているプールと同じものである必要はありません。



(注) **bandwidth [global] kbps** コマンドを使用してパスオプションの帯域幅を設定する場合は、すべてサブプールの帯域幅を使用するか、またはすべてグローバルプールの帯域幅を使用してください。

LSP 属性リスト機能または帯域幅上書きのパス オプション機能を使用すると、ダイナミックパスオプションと明示パスオプションの両方で帯域幅を設定できます。これらの機能をイネーブルにするコマンドは、両方同時に使用することはできません。帯域幅がパスオプションに設定する必要がある唯一の LSP 属性である場合は、機能をイネーブルにするコマンドを使用します。帯域幅の制約が緩和される複数のパスオプションを設定する場合、これが最も簡単な方法です。インターフェイス コンフィギュレーション モードで **tunnel mpls traffic-eng path-option** コマンドに **bandwidth** キーワードを入力すると、そのパスオプションに対しては LSP 属性リストを設定できなくなります。

## トンネル属性と LSP 属性

Cisco IOS XE トンネリング インターフェイスには、MPLS TE に関連した数多くのパラメータがあります。通常、これらのパラメータは、インターフェイス コンフィギュレーション モードで **tunnel mpls traffic-eng** コマンドを使用して設定します。これらのコマンドの多くは、トンネルのロードシェアリング係数などの、トンネル固有のプロパティを決定します。これらのコマンドでは、トンネルによって使用されている特定の LSP には関連しないパラメータが設定されます。ただし、一部のトンネリングパラメータは、トンネルが使用する LSP に適用されます。LSP 固有のプロパティは、LSP 属性リストを使用して設定できます。

## LSP 属性と LSP 属性リスト

LSP 属性リストには、TE トンネルに設定できる各 LSP 固有のパラメータの値を含めることができます。LSP 属性リストは、**mpls traffic-eng lsp attributes string** コマンドを使用して設定します。ここで、*string* は属性リストを示しています。指定できる LSP 属性には、次のものがあります。

- LSP を構成するリンクの属性フラグ (**affinity** コマンド)
- グローバルプールまたはサブプールの LSP 帯域幅 (**bandwidth** コマンド)
- LSP の再最適化のディセーブル化 (**lockdown** コマンド)
- LSP プライオリティ (**priority** コマンド)
- LSP で使用されるルートの記録 (**record-route** コマンド)

## LSP 属性リストの管理

MPLS トラフィック エンジニアリング - LSP 属性機能には、LSP 属性リストを管理するためのコマンドも用意されています。次を実行できます。

- すべての属性リストエントリの再リスト (**list** コマンド)
- リストからの特定の属性の削除 (**noattribute** コマンド)

**exit** コマンドを使用すると、LSP 属性コンフィギュレーションサブモードを終了して、グローバルコンフィギュレーションモードに戻ります。

要件に応じて、異なるパス オプションに対して、異なる属性のセットを持つ LSP 属性リストを設定できます。また、LSP 属性リストは、同じ LSP 属性を使用する複数の TE トンネルを設定するための簡単な方法でもあります。つまり、同じ LSP 属性リストを参照して、1 つ以上の TE トンネルの LSP 固有のパラメータを設定できます。

## コンストレイントベース ルーティングとパス オプション選択

MPLS トラフィック エンジニアリングでは、Resource Reservation Protocol (RSVP) を使用して、バックボーン上で LSP を自動的に確立および維持します。LSP で使用されるパスは、LSP リソース要件とネットワーク リソース（帯域幅など）によって決まります。トラフィック エンジニアリングトンネルは、必要なリソースと使用可能なリソースの調和に基づいて LSP ヘッドで計算されます（コンストレイントベース ルーティング）。

帯域幅上書きのパス オプション機能がない場合、TE トンネルでは、ダイナミック パス オプションまたは明示パス オプションに基づいて、優先度順に LSP が確立されます。ただし、TE トンネルに設定された帯域幅などの属性によって、LSP パス オプションが制約を満たす場合にだけ LSP の設定が許可されます。設定されたパス オプションを満たすパスが見つからない場合、トンネルは設定されません。

帯域幅上書きのパス オプション機能によって、TE トンネルインターフェイスに設定された帯域幅を上書きできるフォールバック パス オプションが提供されます。たとえば、帯域幅をゼロ (0) に設定したパス オプションを設定すると、コンストレイントベース ルーティングの計算で適用される帯域幅の制約を効果的に除去することができます。

## トンネル再最適化とパス オプション選択

再最適化は、トラフィック エンジニアリング トンネルを持つデバイスで、LSP が確立されているトンネルを調査し、より適切な LSP が利用できるかどうかを取得するときに発生します。より適切な LSP が利用可能である場合、デバイスでは、より適切な LSP をシグナリングします。シグナリングに成功すると、デバイスでは古い LSP がより適切な新しい LSP に置き換えられます。

再最適化は、タイマー、**mpls traffic-eng reoptimize** コマンドの発行、またはトンネルの再シグナリングが必要となる設定変更によってトリガーできます。たとえば、MPLS 自動帯域幅機能では、タイマーを使用して、帯域幅パス オプション属性に基づいた再最適化の頻度が設定されます。帯域幅上書きのパス オプション機能を使用すると、TE トンネルインターフェイスに設

定された帯域幅と、特定のパス オプションに設定された帯域幅を切り替えることができます。これにより、TE トンネルにおける LSP のシグナリングの成功率が高まります。

パス オプションに帯域幅上書きが設定されている場合、トラフィック エンジニアリング ソフトウェアは 30 秒ごとに帯域幅を再最適化してトンネルに設定された帯域幅の再設定を試みま  
す（「帯域幅上書きのパス オプションの設定」を参照）。

LSP 属性リストで **lockdown** コマンドを使用して、LSP の再最適化をディセーブルにできます。**tunnel mpls traffic-eng path-option** コマンドを使用して、**lockdown** コマンドを含む LSP 属性リストをパス オプションに適用できます。



- (注) **bandwidth [global] kpbs** コマンドを使用してパス オプションの帯域幅を設定する場合は、すべてサブプールの帯域幅を使用するか、またはすべてグローバルプールの帯域幅を使用してください。サブプールの帯域幅とサブプール以外の帯域幅を混合しないでください。混合すると、あとでパス オプションが再最適化されません。

## 帯域幅上書きを使用したパス オプション選択

帯域幅上書きのパス オプション機能を使用すると、特定のパス オプションの帯域幅パラメータを設定できます。この設定には、**tunnel mpls traffic-eng path-option** コマンドの **bandwidth** キーワードを使用します。帯域幅が設定されたパス オプションを使用して LSP がシグナリングされる場合、トンネルに対して設定された帯域幅ではなく、パス オプションに関連付けられた帯域幅がシグナリングされます。

また、この機能を使用すると、トンネルのヘッドエンドで LSP の確立に失敗するたびに発生する帯域幅の制約を緩和できるように複数のパス オプションを設定することもできます。

次の設定では、**tunnel mpls traffic-eng bandwidth** コマンドを使用してトンネルの帯域幅を設定し、3 つの **tunnel mpls traffic-eng path-option** コマンドを使用して LSP のシグナリングパス オプションを定義しています。

```
tunnel mpls traffic-eng bandwidth 1000
tunnel mpls traffic-eng path-option 1 explicit name path1
tunnel mpls traffic-eng path-option 2 explicit name path2 bandwidth 500
tunnel mpls traffic-eng path-option 3 dynamic bandwidth 0
```

デバイスでは、次のように優先度順に LSP のパス オプションが選択されます。

- デバイスでは、パス オプションを使用して、パス オプション 1 から LSP のシグナリングが試みられます。

**path-option 1** には帯域幅が設定されていないため、デバイスでは、トンネルインターフェイスに設定された 1000 kbps の帯域幅を使用して LSP のシグナリングが試みられます。

- ネットワークで 1000 kbps の帯域幅を利用できない場合、デバイスは、**path-option 2** を使用して LSP の確立を試みます。

path-option 2 には、500 kbps の帯域幅が設定されています。これにより、トンネルインターフェイスに設定されている元の 1000 kbps の帯域幅の制約が緩和されます。

- 500 kbps が利用できない場合、デバイスは、path-option 3 を使用して LSP の確立を試みません。

path-option 3 はダイナミックとして設定されており、帯域幅は 0 です。宛先までの IP パスが存在し、他のすべてのトンネル制約が満たされる場合、デバイスで LSP が確立されます。

## LSP 属性リストを使用する TE トンネルのデフォルトのパス オプション属性

TE トンネルのパス オプション属性の値は、次のように決定されます。

- パス オプションによって参照される LSP 属性リストの値は、トンネルインターフェイスに設定された値よりも優先されます。
- LSP 属性リストに属性が指定されていない場合、トンネル設定の属性が使用されます。LSP 属性リストにはデフォルト値が設定されていません。
- トンネルに属性が設定されていない場合、デバイスでは、次のようにトンネルのデフォルト値が使用されます。

```
{affinity= affinity 0 mask 0,
bandwidth= bandwidth 0,
lockdown= no lockdown,
priority= priority 7 7,
record-route= no record-route
.
.
.
}
```

## MPLS トラフィック エンジニアリング - LSP 属性の設定方法

ここでは、MPLS トラフィック エンジニアリング - LSP 属性の設定について説明します。

## LSP 属性リストの設定

パス オプションに適用する必要な属性を持つラベル スイッチド パス (LSP) 属性リストを設定するには、次の作業を実行します。要件に応じて、異なるパスオプションに対して、異なる属性のセットを持つ LSP 属性リストを設定できます。LSP 属性リストによって、MPLS TE トンネル パス オプションの設定において、柔軟で使いやすく、拡張と管理が簡単なユーザ インターフェイスが提供されます。

また、LSP 属性リストは、同じ LSP 属性を使用する複数の TE トンネルを設定するための簡単な方法でもあります。つまり、同じ LSP 属性リストを参照して、1 つ以上の TE トンネルの LSP 固有のパラメータを設定できます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例：  Device# <b>configure terminal</b>	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 3	<b>mpls traffic-eng lsp attributes string</b> 例：  Device(config)# <b>mpls traffic-eng lsp attributes 1</b>	LSP 属性リストを設定し、LSP 属性コンフィギュレーションモードを開始します。  • <i>string</i> 引数では、特定の LSP 属性リストを指定します。
ステップ 4	<b>affinity value [mask value]</b> 例：  Device(config-lsp-attr)# <b>affinity 0 mask 0</b>	(任意) LSP を構成するリンクの属性フラグを指定します。  • <i>value</i> 引数では、LSP を構成するリンクに必要な値を指定します。各ビットの値は 0 または 1 です。  • <b>mask value</b> キーワードと引数の組み合わせは、どの属性値をチェックする必要があるかを示します。  • マスクのビットが 0 の場合、そのビットに対応するリンクの属性値は関連しません。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• マスクのビットが 1 の場合、そのリンクの属性値と、そのビットに対応する LSP の必要なアフィニティは一致する必要があります。</li> </ul>
ステップ 5	<b>bandwidth [global] kbps</b> 例 : <pre>Device(config-lsp-attr) # bandwidth 5000</pre>	(任意) LSP 帯域幅を指定します。 <ul style="list-style-type: none"> <li>• <b>global</b> キーワードは、グローバルプールパス オプションを示します。</li> <li>• <b>kbps</b> 引数は、パス オプションで確保する kbps の数値です。範囲は 1 ~ 4294967295 です。</li> </ul>
ステップ 6	<b>list</b> 例 : <pre>Device(config-lsp-attr) # list</pre>	(任意) LSP 属性リストの内容を表示します。
ステップ 7	<b>lockdown</b> 例 : <pre>Device(config-lsp-attr) # lockdown</pre>	(任意) LSP の再最適化をディセーブルにします。
ステップ 8	<b>priority setup-priority [hold-priority]</b> 例 : <pre>Device(config-lsp-attr) # priority 1 1</pre>	(任意) LSP プライオリティを指定します。 <ul style="list-style-type: none"> <li>• <b>setup-priority</b> 引数は、LSP のシグナリング時に既存のどの LSP よりも優先的に取得できるかを決定するために使用します。有効な値は 0 ~ 7 であり、数字が小さいほど優先順位は高くなります。したがって、設定プライオリティが 0 の LSP は、プライオリティが 0 以外のどの LSP よりも優先的に取得されます。</li> <li>• <b>hold-priority</b> 引数は LSP と関連付けられて、シグナリングされている他の LSP の方を優先的に取得する必要があるかどうかを決定しま</li> </ul>

	コマンドまたはアクション	目的
		す。有効な値は 0～7 であり、数字が小さいほど優先順位は高くなります。
ステップ 9	<b>record-route</b> 例： Device(config-lsp-attr)# <b>record-route</b>	(任意) LSP によって使用されるルートを記録します。
ステップ 10	<b>no sub-command</b> 例： Device(config-lsp-attr)# <b>no record-route</b>	(任意) LSP 属性リストから特定の属性を削除します。  • <i>sub-command</i> 引数には、属性リストから削除する LSP 属性を指定します。
ステップ 11	<b>exit</b> 例： Device(config-lsp-attr)# <b>exit</b>	(任意) LSP 属性コンフィギュレーション モードを終了します。
ステップ 12	<b>end</b> 例： Device(config)# <b>end</b>	(任意) 終了して、特権 EXEC モードに戻ります。

## LSP 属性リストへの属性の追加

LSP 属性リストに属性を追加するには、次の作業を実行します。LSP 属性リストによって、柔軟で使いやすく、いつでも MPLS TE トンネル トラフィックの要件に合うように拡張または変更可能なユーザ インターフェイスが提供されます。LSP 属性コンフィギュレーション モードは、特定の LSP 属性リストを表示したり、必要なパス オプション属性を追加または変更したりするために使用します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	<b>configure terminal</b> 例 :  Device# <b>configure terminal</b>	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 3	<b>mpls traffic-eng lsp attributes string</b> 例 :  Device(config)# <b>mpls traffic-eng lsp attributes 1</b>	LSP 属性リストを設定し、LSP 属性コンフィギュレーション モードを開始します。  <ul style="list-style-type: none"> <li>• <i>string</i> 引数では、特定の LSP 属性リストを指定します。</li> </ul>
ステップ 4	<b>affinity value [maskvalue]</b> 例 :  Device(config-lsp-attr)# <b>affinity 0 mask 0</b>	(任意) LSP を構成するリンクの属性フラグを指定します。  <ul style="list-style-type: none"> <li>• <i>value</i> 引数では、LSP を構成するリンクに必要な値を指定します。各ビットの値は 0 または 1 です。</li> <li>• <i>maskvalue</i> キーワードと引数の組み合わせは、どの属性値をチェックする必要があるかを示します。               <ul style="list-style-type: none"> <li>• マスクのビットが 0 の場合、そのビットに対応するリンクの属性値は関連しません。</li> <li>• マスクのビットが 1 の場合、そのリンクの属性値と、そのビットに対応する LSP の必要なアフィニティは一致する必要があります。</li> </ul> </li> </ul>
ステップ 5	<b>bandwidth [ global] kbps</b> 例 :  Device(config-lsp-attr)# <b>bandwidth 1000</b>	LSP 帯域幅を指定します。  <ul style="list-style-type: none"> <li>• <b>global</b> キーワードは、グローバル プール パス オプションを示します。</li> <li>• <i>kbps</i> 引数は、パス オプションで確保する kbps の数値です。範囲は 1 ~ 4294967295 です。</li> </ul>
ステップ 6	<b>priority setup-priority [hold-priority]</b> 例 :	LSP プライオリティを指定します。  <ul style="list-style-type: none"> <li>• <i>setup-priority</i> 引数は、LSP のシグナリング時に既存のどの LSP よりも</li> </ul>

	コマンドまたはアクション	目的
	Device(config-lsp-attr)# <b>priority 2 2</b>	優先的に取得できるかを決定するために使用します。有効な値は0～7であり、数字が小さいほど優先順位は高くなります。したがって、設定プライオリティが0のLSPは、プライオリティが0以外のどのLSPよりも優先的に取得されます。  <ul style="list-style-type: none"> <li>• <i>hold-priority</i> 引数はLSPと関連付けられて、シグナリングされている他のLSPの方を優先的に取得する必要があるかどうかを決定します。有効な値は0～7であり、数字が小さいほど優先順位は高くなります。</li> </ul>
ステップ7	<b>list</b> 例：  Device(config-lsp-attr)# <b>list</b>	(任意) LSP属性リストの内容を表示します。  <ul style="list-style-type: none"> <li>• 属性リストに追加されたパスオプション属性を表示する場合に<b>list</b>コマンドを使用します。</li> </ul>
ステップ8	<b>exit</b> 例：  Device(config-lsp-attr)# <b>exit</b>	(任意) LSP属性コンフィギュレーションモードを終了します。
ステップ9	<b>end</b> 例：  Device(config)# <b>end</b>	(任意) 終了して、特権 EXEC モードに戻ります。

## 例：LSP 属性リストからの属性の削除

次に、文字列 'simple' で識別される LSP 属性リストから priority 属性を削除する例を示します。

```
Device(config)# mpls traffic-eng lsp attributes simple
Device(config-lsp-attr)# priority 1 1
Device(config-lsp-attr)# list
LIST simple
 priority 1 1
!
Device(config-lsp-attr)# no priority
Device(config-lsp-attr)# list
LIST simple
!
Device(config-lsp-attr)# exit
```

## LSP 属性リスト内の属性の変更

LSP 属性リスト内の属性を変更するには、次の作業を実行します。LSP 属性リストによって、いつでも MPLS TE トンネルトラフィックの要件に合うように拡張または変更可能な、柔軟なユーザ インターフェイスが提供されます。LSP 属性コンフィギュレーション モードは、特定の LSP 属性リストを表示したり、必要なパス オプション属性を変更したりするために使用します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例：  Device# <b>configure terminal</b>	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 3	<b>mpls traffic-eng lsp attributes string</b> 例：  Device(config)# <b>mpls traffic-eng lsp attributes 1</b>	LSP 属性リストを設定し、LSP 属性コンフィギュレーション モードを開始します。  • <i>string</i> 引数では、特定の LSP 属性リストを指定します。
ステップ 4	<b>affinity value [maskvalue]</b> 例：  Device(config-lsp-attr)# <b>affinity 1 mask 1</b>	LSP を構成するリンクの属性フラグを指定します。  • <i>value</i> 引数は、LSP を構成するリンクに必要な値です。各ビットの値は 0 または 1 です。  • <i>maskvalue</i> キーワードと引数の組み合わせは、どの属性値をチェックする必要があるかを示します。  • マスクのビットが 0 の場合、そのビットに対応するリンクの属性値は関連しません。  • マスクのビットが 1 の場合、そのリンクの属性値と、そのビットに対応するトンネルの必要なアフィニティは一致する必要があります。

	コマンドまたはアクション	目的
ステップ 5	<b>list</b> 例 : <pre>Device(config-lsp-attr)# list</pre>	(任意) LSP 属性リストの内容を表示します。 <ul style="list-style-type: none"> <li>属性リストに設定されたパスオプション属性を表示する場合に <b>list</b> コマンドを使用します。</li> </ul>
ステップ 6	<b>affinity value [maskvalue]</b> 例 : <pre>Device(config-lsp-attr)# affinity 0 mask 0</pre>	LSP を構成するリンクの属性フラグを指定します。 <ul style="list-style-type: none"> <li><b>value</b> 引数は、LSP を構成するリンクに必要な値です。各ビットの値は 0 または 1 です。</li> <li><b>maskvalue</b> キーワードと引数の組み合わせは、どの属性値をチェックする必要があるかを示します。               <ul style="list-style-type: none"> <li>マスクのビットが 0 の場合、そのビットに対応するリンクの属性値は関連しません。</li> <li>マスクのビットが 1 の場合、そのリンクの属性値と、そのビットに対応するトンネルの必要なアフィニティは一致する必要があります。</li> </ul> </li> </ul>
ステップ 7	<b>list</b> 例 : <pre>Device(config-lsp-attr)# list</pre>	(任意) LSP 属性リストの内容を表示します。 <ul style="list-style-type: none"> <li>属性リストでパスオプション属性が変更されたことを確認する場合に <b>list</b> コマンドを使用します。</li> </ul>
ステップ 8	<b>exit</b> 例 : <pre>Device(config-lsp-attr)# exit</pre>	(任意) LSP 属性コンフィギュレーションモードを終了します。
ステップ 9	<b>end</b> 例 : <pre>Device(config)# end</pre>	(任意) 終了して、特権 EXEC モードに戻ります。

## LSP 属性リストの削除

LSP 属性リストを削除するには、次の作業を実行します。この作業は、MPLS TE トンネルの LSP 属性リストに指定された LSP 属性パス オプションが不要になった場合に実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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 3	<b>no mpls traffic-eng lsp attributes string</b> 例： Device(config)# <b>no mpls traffic-eng lsp attributes 1</b>	デバイス設定から指定した LSP 属性リストを削除します。  • <i>string</i> 引数は、削除する特定の LSP 属性リストを示します。
ステップ 4	<b>end</b> 例： Device(config)# <b>end</b>	(任意) 終了して、特権 EXEC モードに戻ります。
ステップ 5	<b>show mpls traffic-eng lsp attributes [string]</b> 例： Device# <b>show mpls traffic-eng lsp attributes</b>	(任意) 設定した LSP 属性リストに関する情報を表示します。  • ルータから LSP 属性リストが削除されたことを確認する場合に、 <b>show mpls traffic-eng lsp attributes</b> コマンドを使用します。

## LSP 属性リスト内の属性の確認

LSP 属性リスト内の属性を確認するには、次の手順を実行します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例 :  Device# <b>configure terminal</b>	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 3	<b>mpls traffic-eng lsp attributes string list</b> 例 :  Device(config)# <b>mpls traffic-eng lsp attributes 1 list</b>	LSP 属性コンフィギュレーション モードを開始します。特定の LSP 属性リストの内容を確認します。
ステップ 4	<b>exit</b> 例 :  Device(config-lsp-attr)# <b>exit</b>	LSP 属性コンフィギュレーション モードを終了します。
ステップ 5	<b>end</b> 例 :  Device(config)# <b>exit</b>	特権 EXEC モードに戻ります。

## すべての LSP 属性リストの確認

設定されているすべての LSP 属性リストを確認するには、次の作業を実行します。次の作業を実行し、すべての LSP 属性リストを表示して、設定した属性リストが動作していることを確認します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	<b>show mpls traffic-eng lsp attributes <i>string</i> [details]</b> 例 : <pre>Device# show mpls traffic-eng lsp attributes</pre>	設定されているすべての LSP 属性のリストを表示します。
ステップ 3	<b>show running-config   begin <i>text-string</i></b> 例 : <pre>Device# show running-config   begin mpls traffic-eng lsp</pre>	設定されているすべての LSP 属性リストが想定どおりであることを確認します。 <b>mpls traffic-eng lsp <i>text-string</i></b> を指定して <b>begin</b> コマンド修飾子を使用すると、コンフィギュレーションファイル内の LSP 属性情報を検索されます。
ステップ 4	<b>exit</b> 例 : <pre>Device# exit</pre>	ユーザー EXEC モードに戻ります。

## LSP 属性リストと MPLS TE トンネルのパス オプションとの関連付け

LSP 属性リストと MPLS TE トンネルのパス オプションを関連付けるには、次の作業を実行します。この作業は、設定した LSP 属性リストを MPLS TE トンネルのパス オプションに適用する場合に必要です。

要件に応じて、異なるパス オプションに対して、異なる属性のセットを持つ LSP 属性リストを設定できます。また、LSP 属性リストは、同じ LSP 属性を使用する複数の TE トンネルを設定するための簡単な方法でもあります。つまり、同じ LSP 属性リストを参照して、1つ以上の TE トンネルの LSP 固有のパラメータを設定できます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : <pre>Device&gt; enable</pre>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例 : <pre>Device# configure terminal</pre>	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。

	コマンドまたはアクション	目的
ステップ 3	<b>interface</b> <i>type number</i> 例 : Device(config)# <b>interface tunnel 1</b>	インターフェイスタイプを設定し、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ます。 <ul style="list-style-type: none"> <li>• <i>type</i> 引数は、設定するインターフェイスのタイプです。</li> <li>• <i>number</i> 引数は、作成または設定するトンネルインターフェイスの番号です。</li> </ul>
ステップ 4	<b>tunnel destination</b> { <i>hostname</i>   <i>ip-address</i> } 例 : Device(config-if)# <b>tunnel destination 10.10.10.12</b>	このパス オプションのトンネルの宛先を指定します。 <ul style="list-style-type: none"> <li>• <i>hostname</i> 引数は、ホスト宛先の名前です。</li> <li>• <i>ip-address</i> 引数は、10 進の 4 分割ドット表記で表した、ホスト宛先の IP アドレスです。</li> </ul>
ステップ 5	<b>tunnel mode mpls traffic-eng</b> 例 : Device(config-if)# <b>tunnel mode mpls traffic-eng</b>	MPLS TE のトンネルのカプセル化モードを設定します。
ステップ 6	<b>tunnel mpls traffic-eng autoroute announce</b> 例 : Device(config-if)# <b>tunnel mpls traffic-eng autoroute announce</b>	IGP における拡張 Shortest Path First (SPF) の計算において、(トンネルがアップの場合に) トンネルを使用する必要があることを指定します。
ステップ 7	<b>tunnel mpls traffic-eng bandwidth</b> [[ <i>global</i> ] <i>bandwidth</i> ] 例 : Device(config-if)# <b>tunnel mpls traffic-eng bandwidth 1000</b>	MPLS TE トンネルに必要な帯域幅を設定し、その帯域幅をサブプールまたはグローバル プールに割り当てます。 <ul style="list-style-type: none"> <li>• <b>global</b> キーワードは、グローバルプールトンネルを示します。</li> <li>• <i>kbps</i> 引数は、MPLS TE トンネルで確保する kbps 単位の帯域幅です。範囲は 1 ~ 4294967295 です。</li> </ul>

	コマンドまたはアクション	目的
ステップ 8	<p><b>tunnel mpls traffic-eng priority</b> <i>setup-priority</i> [<i>hold-priority</i>]</p> <p>例 :</p> <pre>Device(config-if)# tunnel mpls traffic-eng priority 1 1</pre>	<p>どの既存のトンネルを優先的に取得するかをシステムが決定する場合に使用されるプライオリティを設定します。</p> <ul style="list-style-type: none"> <li>• <i>setup-priority</i> 引数は、このトンネルでの LSP のシグナリング時に既存のどのトンネルよりも優先的に取得できるかを決定するために使用されるプライオリティです。</li> </ul> <p>有効な値の範囲は 0 ~ 7 です。値が小さいほど、プライオリティが高いことを示します。設定プライオリティが 0 の LSP は、プライオリティが 0 以外のどの LSP よりも優先的に取得されません。</p> <ul style="list-style-type: none"> <li>• <i>hold-priority</i> 引数は、このトンネルの LSP と関連付けられた、シグナリングされている他の LSP の方を優先的に取得する必要があるかどうかを決定するためのプライオリティです。</li> </ul> <p>有効な値は 0 ~ 7 であり、数字が小さいほど優先順位は高くなります。</p>
ステップ 9	<p><b>tunnel mpls traffic-eng path-option</b> <i>number</i> {<b>dynamic</b>   <b>explicit</b> {<i>name</i> <i>path-name</i>   <i>path-number</i>} [<i>verbatim</i>]}} [<i>attributes string</i>] [<i>bandwidth</i> [ <i>global</i>] <i>kbps</i>] [<i>lockdown</i>]</p> <p>例 :</p> <pre>Device(config-if)# tunnel mpls traffic-eng path-option 1 dynamic attributes 1</pre>	<p>LSP 属性リストを追加して、MPLS TE トンネルのパスオプションの LSP 関連パラメータを指定します。</p> <ul style="list-style-type: none"> <li>• <i>number</i> 引数は、パスオプションを示します。</li> <li>• <b>dynamic</b> キーワードは、パスオプションがダイナミックに計算されることを示します (ルータによって最良パスが計算されます)。</li> <li>• <b>explicit</b> キーワードは、パスオプションが指定されていることを示します。パスの IP アドレスを指定します。</li> <li>• <b>name</b> <i>path-name</i> のキーワードと引数の組み合わせは、明示パスオプションの名前を示します。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <i>path-number</i> 引数は、明示パス オプションの番号を示します。</li> <li>• <b>verbatim</b> キーワードを指定すると、トポロジデータベース検証がバイパスされます。</li> </ul> <p>(注) <b>verbatim</b> キーワードは、明示パスオプションでだけ使用できます。</p> <ul style="list-style-type: none"> <li>• <b>attributes</b> <i>string</i> のキーワードと引数の組み合わせは、LSP のパスオプションを指定する属性リストを示します。</li> <li>• <b>bandwidth</b> キーワードは、LSP の帯域幅を指定します。</li> <li>• <b>global</b> キーワードは、グローバルプールパス オプションを示します。</li> <li>• <i>kbps</i> 引数は、パス オプションで確保する kbps の数値です。範囲は 1 ~ 4294967295 です。</li> <li>• <b>lockdown</b> キーワードを指定すると、LSP の再最適化がディセーブルになります。</li> </ul>
ステップ 10	<b>end</b> 例 :  Device (config-if) # <b>end</b>	(任意) 終了して、特権 EXEC モードに戻ります。

## 異なる LSP 属性を使用するためのパス オプションの変更

パス オプションを変更して異なる LSP 属性リストを使用するには、次の作業を実行します。

要件に応じて、異なるパス オプションに対して異なる属性のセットを持つ LSP 属性リストを設定したり、パス オプションに関連付けられた属性のセットを変更したりできます。パスオプションを変更して異なる LSP 属性リストを使用するには、**tunnel mpls traffic-eng path-option number dynamic attributes string** コマンドをインターフェイス コンフィギュレーション モードで使用します。**attributes** および *string* のキーワードと引数は、指定したパスオプションの新しい LSP 属性リストを示します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例 :  Device# <b>configure terminal</b>	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 3	<b>interface type number</b> 例 :  Device(config)# <b>interface tunnel 1</b>	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。  <ul style="list-style-type: none"> <li>• <i>type</i> 引数は、設定するインターフェイスのタイプです。</li> <li>• <i>number</i> 引数は、作成または設定するトンネルインターフェイスの番号です。</li> </ul>
ステップ 4	<b>tunnel destination {hostname   ip-address}</b> 例 :  Device(config-if)# <b>tunnel destination 10.10.10.12</b>	このパス オプションのトンネルの宛先を指定します。  <ul style="list-style-type: none"> <li>• <i>hostname</i> 引数は、ホスト宛先の名前です。</li> <li>• <i>ip-address</i> 引数は、10 進の 4 分割ドット表記で表した、ホスト宛先の IP アドレスです。</li> </ul>
ステップ 5	<b>tunnel mpls traffic-eng path-option number {dynamic   explicit} {namepath-name   path-number} [verbatim] [attributesstring] [bandwidth [global] kbps] [lockdown]</b> 例 :  Device(config-if)# <b>tunnel mpls traffic-eng path-option 1 dynamic attributes 1</b>	LSP 属性リストを追加して、MPLS TE トンネルのパス オプションの LSP 関連パラメータを指定します。  <ul style="list-style-type: none"> <li>• <i>number</i> 引数は、パス オプションを示します。</li> <li>• <b>dynamic</b> キーワードは、パスオプションがダイナミックに計算されることを示します (ルータによって最良パスが計算されます)。</li> <li>• <b>explicit</b> キーワードは、パスオプションが指定されていることを示し</li> </ul>

	コマンドまたはアクション	目的
		<p>ます。パスの IP アドレスを指定します。</p> <ul style="list-style-type: none"> <li>• <b>namepath-name</b> のキーワードと引数の組み合わせは、明示パスオプションの名前を示します。</li> <li>• <b>path-number</b> 引数は、明示パス オプションの番号を示します。</li> <li>• <b>verbatim</b> キーワードを指定すると、トポロジデータベース検証がバイパスされます。</li> </ul> <p>(注) <b>verbatim</b> キーワードは、明示パスオプションでだけ使用できます。</p> <ul style="list-style-type: none"> <li>• <b>attributesstring</b> のキーワードと引数の組み合わせは、LSP のパスオプションを指定する属性リストを示します。</li> <li>• <b>bandwidth</b> キーワードは、LSP の帯域幅を指定します。</li> <li>• <b>global</b> キーワードは、グローバル プール パス オプションを示します。</li> <li>• <b>kpbs</b> 引数は、パス オプションで確保する kbps の数値です。範囲は 1 ~ 4294967295 です。</li> <li>• <b>lockdown</b> キーワードを指定すると、LSP の再最適化がディセーブルになります。</li> </ul>
ステップ 6	<p><b>end</b></p> <p>例 :</p> <pre>Device(config-if) # end</pre>	<p>(任意) 終了して、特権 EXEC モードに戻ります。</p>

## MPLS TE トンネルの LSP のパス オプションの削除

MPLS TE トンネルの LSP のパス オプションを削除するには、次の作業を実行します。MPLS TE トンネルのトラフィック要件が変更された場合は、次の作業を実行して LSP のパス オプションを削除します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例 :  Device# <b>configure terminal</b>	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 3	<b>interface type number</b> 例 :  Device(config)# <b>interface tunnel 1</b>	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。  <ul style="list-style-type: none"> <li>• <i>type</i> 引数は、設定するインターフェイスのタイプです。</li> <li>• <i>number</i> 引数は、作成または設定するトンネルインターフェイスの番号です。</li> </ul>
ステップ 4	<b>tunnel destination {hostname   ip-address}</b> 例 :  Device(config-if)# <b>tunnel destination 10.10.10.12</b>	このパス オプションのトンネルの宛先を指定します。  <ul style="list-style-type: none"> <li>• <i>hostname</i> 引数は、ホスト宛先の名前です。</li> <li>• <i>ip-address</i> 引数は、10 進の 4 分割ドット表記で表した、ホスト宛先の IP アドレスです。</li> </ul>
ステップ 5	<b>no tunnel mpls traffic-eng path-option number {dynamic   explicit {namepath-name   path-number} [verbatim]} [attributesstring] [bandwidth [global] kbps] [lockdown]</b> 例 :	MPLS TE トンネルのパス オプションの LSP 関連パラメータを指定する LSP 属性リストを削除します。  <ul style="list-style-type: none"> <li>• <i>number</i> 引数は、パス オプションを示します。</li> </ul>

	コマンドまたはアクション	目的
	<pre>Device(config-if)# no tunnel mpls traffic-eng path-option 1 dynamic attributes 1</pre>	<ul style="list-style-type: none"> <li>• <b>dynamic</b> キーワードは、パスオプションがダイナミックに計算されることを示します (ルータによって最良パスが計算されます)。</li> <li>• <b>explicit</b> キーワードは、パスオプションが指定されていることを示します。パスの IP アドレスを指定します。</li> <li>• <b>namepath-name</b> のキーワードと引数の組み合わせは、明示パスオプションの名前を示します。</li> <li>• <b>path-number</b> 引数は、明示パスオプションの番号を示します。</li> <li>• <b>verbatim</b> キーワードを指定すると、トポロジデータベース検証がバイパスされます。</li> </ul> <p>(注) <b>verbatim</b> キーワードは、明示パスオプションでだけ使用できます。</p> <ul style="list-style-type: none"> <li>• <b>attributesstring</b> のキーワードと引数の組み合わせは、LSP のパスオプションを指定する属性リストを示します。</li> <li>• <b>bandwidth</b> キーワードは、LSP の帯域幅を指定します。</li> <li>• <b>global</b> キーワードは、グローバルプールパスオプションを示します。</li> <li>• <b>kbps</b> 引数は、パスオプションで確保する kbps の数値です。範囲は 1 ~ 4294967295 です。</li> <li>• <b>lockdown</b> キーワードを指定すると、LSP の再最適化がディセーブルになります。</li> </ul>
ステップ 6	<pre>end</pre> <p>例 :</p>	(任意) 終了して、特権 EXEC モードに戻ります。

LSP が正しい属性を使用してシグナリングされていることの確認

	コマンドまたはアクション	目的
	Device(config-if)# <b>end</b>	

## LSP が正しい属性を使用してシグナリングされていることの確認

指定したトンネルで LSP が正しい属性を使用してシグナリングされていることを確認するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>show mpls traffic-eng tunnels tunnel-interface [brief]</b> 例： Device# <b>show mpls traffic-eng tunnels tunnel1</b>	指定したトンネルで LSP が正しい属性を使用してシグナリングされていることを確認します。
ステップ 3	<b>exit</b> 例： Device# <b>exit</b>	このコマンドを使用して、ユーザ EXEC モードに戻ります。次に例を示します。

## 帯域幅上書きのパス オプションの設定

ここでは、帯域幅上書きのパスオプションを設定するための手順について説明します。



(注) path-option パラメータとして帯域幅を設定すると、path-option パラメータとして LSP 属性リストを設定することはできなくなります。

## TE トンネルのフォールバック帯域幅パス オプションの設定

TE トンネルのフォールバック帯域幅パスオプションを設定するには、次の作業を実行します。次の作業を実行して、トンネルのヘッドエンドで LSP の確立に失敗するたびに帯域幅の制約が緩和されるパス オプションを設定します。

帯域幅上書きのパス オプション機能を設定することにより、パス オプションにおける帯域幅の制約を一時的に緩和して、TE トンネルで LSP が設定される確率を高めることができます。TE トンネルで帯域幅上書きのパス オプションが使用されている場合、トラフィック エンジニアリング ソフトウェアでは、帯域幅が元々設定されているより適したパス オプションが使用されるように、30秒ごとにトンネルの再最適化が試みられます。帯域幅上書きのパス オプション機能は帯域幅の制約を一時的に緩和することを目的として設計されています。すべてのトラフィック エンジニアリング トンネルの再最適化を即時に実行する場合は、**mpls traffic-eng reoptimize** コマンドを使用できます。また、帯域幅上書きに **lockdown** コマンドを設定して、自動再最適化を防止できます。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例：  Device# <b>configure terminal</b>	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 3	<b>interface type number</b> 例：  Device(config)# <b>interface tunnel 1</b>	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> <li>• <i>type</i> 引数は、設定するインターフェイスのタイプです。</li> <li>• <i>number</i> 引数は、作成または設定するトンネルインターフェイスの番号です。</li> </ul>
ステップ 4	<b>tunnel destination {hostname   ip-address}</b> 例：  Device(config-if)# <b>tunnel destination 10.10.10.12</b>	このパス オプションのトンネルの宛先を指定します。 <ul style="list-style-type: none"> <li>• <i>hostname</i> 引数は、ホスト宛先の名前です。</li> <li>• <i>ip-address</i> 引数は、10 進の 4 分割ドット表記で表した、ホスト宛先の IP アドレスです。</li> </ul>
ステップ 5	<b>tunnel mpls traffic-eng path-option number {dynamic   explicit {name path-name   path-number} [verbatim]}</b>	帯域幅上書きのパス オプションを追加して、MPLS TE トンネルのパス オプ

コマンドまたはアクション	目的
<p>[<i>attributes string</i>] [<i>bandwidth [ global] kbps</i>] [<i>lockdown</i>]</p> <p>例 :</p> <pre>Device(config-if)# tunnel mpls traffic-eng path-option 1 dynamic bandwidth 500</pre>	<p>シヨンに帯域幅フォールバックを指定します。</p> <ul style="list-style-type: none"> <li>• <i>number</i> 引数は、パス オプションを示します。</li> <li>• <b>dynamic</b> キーワードは、パスオプションが動的に計算されることを示します (ルータによって最良パスが計算されます)。</li> <li>• <b>explicit</b> キーワードは、パスオプションが指定されていることを示します。パスの IP アドレスを指定します。</li> <li>• <i>namepath-name</i> のキーワードと引数の組み合わせは、明示パスオプションの名前を示します。</li> <li>• <i>path-number</i> 引数は、明示パスオプションの番号を示します。</li> <li>• <b>verbatim</b> キーワードを指定すると、トポロジデータベース検証がバイパスされます。</li> </ul> <p>(注)      <b>verbatim</b> キーワードは、明示パスオプションでだけ使用できます。</p> <ul style="list-style-type: none"> <li>• <i>attributesstring</i> のキーワードと引数の組み合わせは、LSP のパスオプションを指定する属性リストを示します。</li> <li>• <b>bandwidth</b> キーワードは、LSP の帯域幅を指定します。</li> <li>• <b>global</b> キーワードは、グローバルプールパス オプションを示します。</li> <li>• <i>kbps</i> 引数は、パス オプションで確保する kbps の数値です。範囲は 1 ~ 4294967295 です。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>lockdown</b> キーワードを指定すると、LSPの再最適化がディセーブルになります。</li> </ul>
ステップ 6	<b>end</b> 例： Device(config-if) # <b>end</b>	(任意) 終了して、特権 EXEC モードに戻ります。

## 帯域幅上書きのパス オプションの帯域幅の変更

帯域幅上書きのパスオプションの帯域幅を変更するには、次の作業を実行します。トンネルのヘッドエンドで LSP が確実に確立されるようにするために、パス オプションの帯域幅の制約をさらに緩和または変更する必要がある場合があります。

帯域幅上書きのパスオプション機能は帯域幅の制約を一時的に緩和することを目的として設計されています。すべてのトラフィック エンジニアリング トンネルの再最適化を即時に実行する場合は、**mpls traffic-eng reoptimize** コマンドを使用できます。また、帯域幅上書きに **lockdown** コマンドを設定して、自動再最適化を防止できます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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 3	<b>interface type number</b> 例： Device(config)# <b>interface tunnel 1</b>	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> <li>• <i>type</i> 引数は、設定するインターフェイスのタイプです。</li> <li>• <i>number</i> 引数は、作成または設定するトンネル インターフェイスの番号です。</li> </ul>

	コマンドまたはアクション	目的
ステップ 4	<p><b>tunnel destination</b> {hostname   ip-address}</p> <p>例 :</p> <pre>Device(config-if)# tunnel destination 10.10.10.12</pre>	<p>このパス オプションのトンネルの宛先を指定します。</p> <ul style="list-style-type: none"> <li>• <i>hostname</i> 引数は、ホスト宛先の名前です。</li> <li>• <i>ip-address</i> 引数は、10 進の 4 分割ドット表記で表した、ホスト宛先の IP アドレスです。</li> </ul>
ステップ 5	<p><b>tunnel mpls traffic-eng path-option</b> number {dynamic   explicit} {name path-name   path-number} [verbatim] [attributes string] [bandwidth [global] kbps] [lockdown]</p> <p>例 :</p> <pre>Device(config-if)# tunnel mpls traffic-eng path-option 2 dynamic bandwidth 500</pre> <p>例 :</p>	<p>帯域幅上書きのパス オプションを追加して、MPLS TE トンネルのパス オプションに帯域幅フォールバックを指定します。</p> <ul style="list-style-type: none"> <li>• <i>number</i> 引数は、パス オプションを示します。</li> <li>• <b>dynamic</b> キーワードは、パスオプションがダイナミックに計算されることを示します (ルータによって最良パスが計算されます)。</li> <li>• <b>explicit</b> キーワードは、パスオプションが指定されていることを示します。パスの IP アドレスを指定します。</li> <li>• <i>namepath-name</i> のキーワードと引数の組み合わせは、明示パスオプションの名前を示します。</li> <li>• <i>path-number</i> 引数は、明示パスオプションの番号を示します。</li> <li>• <b>verbatim</b> キーワードを指定すると、トポロジデータベース検証がバイパスされます。</li> </ul> <p>(注) <b>verbatim</b> キーワードは、明示パスオプションでだけ使用できます。</p> <ul style="list-style-type: none"> <li>• <i>attributesstring</i> のキーワードと引数の組み合わせは、LSP のパスオプションを指定する属性リストを示します。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>bandwidth</b> キーワードは、LSP の帯域幅を指定します。</li> <li>• <b>global</b> キーワードは、グローバル プール パス オプションを示します。</li> <li>• <b>kbps</b> 引数は、パス オプションで確保する kbps の数値です。範囲は 1 ~ 4294967295 です。</li> <li>• <b>lockdown</b> キーワードを指定すると、LSP の再最適化がディセーブルになります。</li> </ul>
ステップ 6	<b>end</b> 例 : Device(config-if) # <b>end</b>	(任意) 終了して、特権 EXEC モードに戻ります。
ステップ 7	<b>show mpls traffic-eng tunnels tunnel-interface [brief]</b> 例 : Device# <b>show mpls traffic-eng tunnels tunnel1</b>	(任意) トンネルの情報を表示します。 <ul style="list-style-type: none"> <li>• Use the <b>showmplstraffic-engtunnels</b> command to verify which bandwidth path option is in use by the LSP.</li> </ul>

## 帯域幅上書きのパス オプションの削除

帯域幅上書きのパス オプションの帯域幅を削除するには、次の作業を実行します。帯域幅上書きのパス オプション機能は帯域幅の制約を一時的に緩和することを目的として設計されています。次の作業を実行して、帯域幅の上書きが不要な場合にこれを削除します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例 : Device# <b>configure terminal</b>	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。

	コマンドまたはアクション	目的
ステップ 3	<b>interface tunnel number</b> 例 :  Device(config)# <b>interface tunnel 1</b>	トンネル インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。  <ul style="list-style-type: none"> <li>• <b>number</b> 引数は、作成または設定するトンネル インターフェイスの番号です。</li> </ul>
ステップ 4	<b>tunnel destination {hostname   ip-address}</b> 例 :  Device(config-if)# <b>tunnel destination 10.10.10.12</b>	このパス オプションのトンネルの宛先を指定します。  <ul style="list-style-type: none"> <li>• <b>hostname</b> 引数は、ホスト宛先の名前です。</li> <li>• <b>ip-address</b> 引数は、10 進の 4 分割ドット表記で表した、ホスト宛先の IP アドレスです。</li> </ul>
ステップ 5	<b>no tunnel mpls traffic-eng path-option number {dynamic   explicit {name path-name   path-number} [verbatim]} [attributes string] [bandwidth [ global] kbps] [lockdown]</b> 例 :  Device(config-if)# <b>no tunnel mpls traffic-eng path-option 2 dynamic bandwidth 500</b>	MPLS TE トンネルのパス オプションの帯域幅フォールバックを指定する帯域幅上書きのパス オプションを削除します。  <ul style="list-style-type: none"> <li>• <b>number</b> 引数は、パス オプションを示します。</li> <li>• <b>dynamic</b> キーワードは、パスオプションがダイナミックに計算されることを示します (ルータによって最良パスが計算されます)。</li> <li>• <b>explicit</b> キーワードは、パスオプションが指定されていることを示します。パスの IP アドレスを指定します。</li> <li>• <b>name path-name</b> のキーワードと引数の組み合わせは、明示パスオプションの名前を示します。</li> <li>• <b>path-number</b> 引数は、明示パスオプションの番号を示します。</li> <li>• <b>verbatim</b> キーワードを指定すると、トポロジデータベース検証がバイパスされます。</li> </ul>

	コマンドまたはアクション	目的
		<p>(注) <b>verbatim</b> キーワードは、明示パスオプションでだけ使用できます。</p> <ul style="list-style-type: none"> <li>• <b>attributes string</b> のキーワードと引数の組み合わせは、LSP のパスオプションを指定する属性リストを示します。</li> <li>• <b>bandwidth</b> キーワードは、LSP の帯域幅を指定します。</li> <li>• <b>global</b> キーワードは、グローバルプールパスオプションを示します。</li> <li>• <b>kbps</b> 引数は、パスオプションで確保する kbps の数値です。範囲は 1 ~ 4294967295 です。</li> <li>• <b>lockdown</b> キーワードを指定すると、LSP の再最適化がディセーブルになります。</li> </ul>
ステップ 6	<b>end</b> 例 : Device(config-if) # <b>end</b>	(任意) 終了して、特権 EXEC モードに戻ります。
ステップ 7	<b>show mpls traffic-eng tunnels tunnel-interface [brief]</b> 例 : Device# <b>show mpls traffic-eng tunnels tunnell</b>	(任意) トンネルの情報を表示します。 <ul style="list-style-type: none"> <li>• どの帯域幅パスオプションが LSP で使用されているかを確認する場合に <b>show mpls traffic-eng tunnels</b> コマンドを使用します。</li> </ul>

## LSP が正しい帯域幅を使用してシグナリングされていることの確認

LSP が正しい帯域幅を使用してシグナリングされていることを確認するには、次の手順を実行します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>show mpls traffic-eng tunnels tunnel-interface [brief]</b> 例 :  Device# <b>show mpls traffic-eng tunnels tunnel21</b>	<p>LSP が正しい帯域幅を使用してシグナリングされていること、およびトンネルに設定されている帯域幅が上書きされていることを確認します。</p> <p>帯域幅の上書きがアクティブにシグナリングされている場合は、<b>show mpls traffic-eng tunnel</b> コマンドによって Active Path Option Parameters という見出しの下に帯域幅の上書き情報が表示されます。この例では、帯域幅の上書き (BandwidthOverride) がイネーブルになっており、トンネルが path-option 2 を使用してシグナリングされていることが示されています。シグナリングされている帯域幅は 500 です。これは、パス オプション 2 に設定されている値であり、トンネル インターフェイスに設定されている 1000 kbps の帯域幅が上書きされています。</p>
ステップ 3	<b>exit</b> 例 :  Device# <b>exit</b>	このコマンドを使用して、ユーザ EXEC モードに戻ります。次に例を示します。

## MPLS トラフィック エンジニアリング - LSP 属性の設定例

ここでは、MPLS トラフィック エンジニアリング - LSP 属性の設定例を紹介します。

### LSP 属性リストの設定 : 例

#### 例 : LSP 属性リストの設定

次の例は、番号 1 で識別される LSP 属性リストでアフィニティおよび帯域幅の LSP 関連の属性を設定する方法を示しています。

```
Device(config)# mpls traffic-eng lsp attributes 1
Device(config-lsp-attr)# affinity 7 mask 7
Device(config-lsp-attr)# bandwidth 1000
Device(config-lsp-attr)# exit
```

## 例：LSP 属性リストへの属性の追加

次に、番号 1 で識別される LSP 属性リストに priority 属性を追加する例を示します。

```
Device(config)# mpls traffic-eng lsp attributes 1
Device(config-lsp-attr)# affinity 7 mask 7
Device(config-lsp-attr)# bandwidth 1000
Device(config-lsp-attr)# priority 1 1
Device(config-lsp-attr)# exit
```

## 例：LSP 属性リストからの属性の削除

次に、文字列 'simple' で識別される LSP 属性リストから priority 属性を削除する例を示します。

```
Device(config)# mpls traffic-eng lsp attributes simple
Device(config-lsp-attr)# priority 1 1
Device(config-lsp-attr)# list
LIST simple
  priority 1 1
!
Device(config-lsp-attr)# no priority
Device(config-lsp-attr)# list
LIST simple
!
Device(config-lsp-attr)# exit
```

## 例：LSP 属性リスト内の属性の変更

次の例は、番号 5 で識別される LSP 属性リスト内の帯域幅を変更する方法を示しています。

```
Device(config)# mpls traffic-eng lsp attributes 5
Device(config-lsp-attr)# bandwidth 1000
Device(config-lsp-attr)# priority 1 1
Device(config-lsp-attr)# list
LIST 5
  bandwidth 1000
  priority 1 1
Device(config-lsp-attr)# bandwidth 500
Device(config-lsp-attr)# list
LIST 5
  bandwidth 500
  priority 1 1
Device(config-lsp-attr)# exit
```

## 例：LSP 属性リストの削除

次の例では、番号 1 で識別される LSP 属性リストを削除する方法を示します。

```
Device(config)# mpls traffic-eng lsp attributes 1
Device(config-lsp-attr)# affinity 7 mask 7
```

例：LSP 属性リストと TE トンネルのパスオプションとの関連付け

```
Device(config-lsp-attr)# bandwidth 1000
Device(config-lsp-attr)# priority 1 1

Device(config-lsp-attr)# exit
!
Device(config)# no mpls traffic-eng lsp attributes 1
```

## 例：LSP 属性リストと TE トンネルのパスオプションとの関連付け

次の例は、番号 3 で識別される LSP 属性リストをパスオプション 1 に関連付けています。

```
Device(config)# mpls traffic-eng lsp attributes 3
Device(config-lsp-attr)# bandwidth 1000
Device(config-lsp-attr)# priority 2 2
Device(config-lsp-attr)# exit
!
!
Device(config)# interface Tunnel 1
Device(config-if)# ip unnumbered FastEthernet1/0/1
Device(config-if)# tunnel destination 10.112.0.12
Device(config-if)# tunnel mode mpls traffic-eng
Device(config-if)# tunnel mpls traffic-eng affinity 1
Device(config-if)# tunnel mpls traffic-eng bandwidth 5000
Device(config-if)# tunnel mpls traffic-eng path-option 1 dynamic attributes 3
```

この設定では、LSP は次の属性を持ちます。

```
{bandwidth = 1000
 priority = 2 2
 affinity 1
 reroute enabled.
}
```

パス オプションによって参照される LSP 属性リストは、トンネル インターフェイスに設定された値よりも優先されます。

## 例：異なる LSP 属性を使用するためのパスオプションの変更

次に、パスオプション 1 を変更して、番号 1 で識別される LSP 属性リストを使用する例を示します。

```
Device(config)# mpls traffic-eng lsp attributes 1
Device(config-lsp-attr)# affinity 7 mask 7
Device(config-lsp-attr)# bandwidth 500
Device(config-lsp-attr)# priority 1 1
Device(config-lsp-attr)# exit
Device(config)# mpls traffic-eng lsp attributes 2
Device(config-lsp-attr)# bandwidth 1000
Device(config-lsp-attr)# priority 1 1
Device(config-lsp-attr)# exit
Device(config)# interface Tunnel 1
Device(config-if)# ip unnumbered FastEthernet1/0/1
Device(config-if)# tunnel destination 10.112.0.12
Device(config-if)# tunnel mode mpls traffic-eng
Device(config-if)# tunnel mpls traffic-eng affinity 1
Device(config-if)# tunnel mpls traffic-eng bandwidth 5000
Device(config-if)# tunnel mpls traffic-eng path-option 1 dynamic attributes 1
```

この設定では、LSP は次の属性を持ちます。

```
{affinity = 7 mask = 7
 bandwidth = 500
 priority = 1 1
}
```

## 例：MPLS TE トンネルの LSP パスオプションの削除

次に、TE トンネルの LSP のパスオプション 1 を削除する例を示します。

```
Device(config)# interface Tunnel 1
Device(config-if)# ip unnumbered FastEthernet1/0/1
Device(config-if)# tunnel destination 10.112.0.12
Device(config-if)# tunnel mode mpls traffic-eng
Device(config-if)# tunnel mpls traffic-eng affinity 1
Device(config-if)# tunnel mpls traffic-eng bandwidth 5000
Device(config-if)# tunnel mpls traffic-eng path-option 1 explicit path1 attributes 1
Device(config-if)# tunnel mpls traffic-eng path-option 2 explicit path2 attributes 2
!
!
Device(config-if)# no tunnel mpls traffic-eng path-option 1 explicit path1 attributes 1
```

## 帯域幅上書きのパス オプションの設定：例

### 例：帯域幅上書きのパスオプションの設定

次に、パス オプションを設定して帯域幅を上書きする例を示します。

```
Device(config-if)# tunnel mpls traffic-eng path-option 3 explicit name path1 ?
attributes Specify an LSP attribute list
bandwidth override the bandwidth configured on the tunnel
lockdown not a candidate for reoptimization
<cr>
Device(config-if)# tunnel mpls traffic-eng path-option 3 explicit name path1 bandwidth
?
<0-4294967295> bandwidth requirement in kbps
Device(config-if)# tunnel mpls traffic-eng path-option 3 explicit name path1 bandwidth
500 ?
lockdown not a candidate for reoptimization
<cr>
```



(注) path-option パラメータとして帯域幅を設定すると、path-option パラメータとして LSP 属性リストを設定することはできなくなります。

## TE トンネルのフォールバック帯域幅パス オプションの設定：例

次に、**tunnel mpls traffic-eng path-option** コマンドを使用して複数のパスオプションを設定する例を示します。

```
interface Tunnel 1
```

## 例：帯域幅上書きのパスオプションにおける帯域幅の変更

```

ip unnumbered Loopback0
tunnel destination 10.10.10.12
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 1 1
tunnel mpls traffic-eng bandwidth 1000
tunnel mpls traffic-eng path-option 1 explicit name path1
tunnel mpls traffic-eng path-option 2 explicit name path2 bandwidth 500
tunnel mpls traffic-eng path-option 3 dynamic bandwidth 0
end

```

デバイスでは、次のように優先度順に LSP のパス オプションが選択されます。

- デバイスでは、パス オプションを使用して、path-option 1 から LSP のシグナリングが試みられます。

path-option 1 には帯域幅が設定されていないため、デバイスでは、トンネルインターフェイスに設定された 1000 kbps の帯域幅を使用して LSP のシグナリングが試みられます。

- ネットワークで 1000 kbps の帯域幅を利用できない場合、デバイスは、path-option 2 を使用して LSP の確立を試みます。

path-option 2 には、500 kbps の帯域幅が設定されています。これにより、トンネルインターフェイスに設定されている元の 1000 kbps の帯域幅の制約が緩和されます。

- 500 kbps が利用できない場合、デバイスは、path-option 3 を使用して LSP の確立を試みます。

path-option 3 はダイナミックとして設定されており、帯域幅は 0 です。宛先までの IP パスが存在し、他のすべてのトンネル制約が満たされる場合、デバイスで LSP が確立されます。

## 例：帯域幅上書きのパスオプションにおける帯域幅の変更

次の例は、帯域幅上書きのパスオプションの帯域幅を変更する方法を示しています。path-option 3 が帯域幅 100 kbps の明示パスに変更されています。また、path-option 4 が帯域幅 0 に設定されています。

```

interface Tunnel 1
ip unnumbered Loopback0
tunnel destination 10.10.10.12
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 1 1
tunnel mpls traffic-eng bandwidth 1000
tunnel mpls traffic-eng path-option 1 explicit name path1
tunnel mpls traffic-eng path-option 2 explicit name path2 bandwidth 500
tunnel mpls traffic-eng path-option 3 dynamic bandwidth 0
!
!
Device(config)# tunnel mpls traffic-eng path-option 3 explicit name path3 bandwidth 100
Device(config)# tunnel mpls traffic-eng path-option 4 dynamic bandwidth 0

```

## 例：MPLS TE トンネルの LSP パスオプション帯域幅値の削除

次の例は、MPLS TE トンネルの LSP のパス オプション 3 の帯域幅を削除する方法を示しています。

```
interface Tunnel 1
 ip unnumbered Loopback0
 tunnel destination 10.10.10.12
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 1 explicit name path1
 tunnel mpls traffic-eng path-option 2 explicit name path2 bandwidth 500
 tunnel mpls traffic-eng path-option 3 explicit name path3 bandwidth 100
 tunnel mpls traffic-eng path-option 4 dynamic bandwidth 0
!
Router(config)# no tunnel mpls traffic-eng path-option 3 explicit name path3 bandwidth
100
```

## その他の参考資料

### 関連資料

関連項目	マニュアルタイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
MPLS トラフィック エンジニアリング コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』

### シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

# MPLS トラフィック エンジニアリング - LSP 属性の機能情報

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Bengaluru 17.6.1	MPLS トラフィック エンジニアリング LSP 属性	MPLS トラフィック エンジニアリング - LSP 属性機能は、MPLS TE 機能の拡張版であり、LSP 属性リスト機能と帯域幅上書きのパスオプション機能を備えています。これらの機能によって、MPLS TE トンネルパス オプションの LSP 属性を柔軟に設定できるようになります。LSP 属性リストを使用すると、TE トンネルのパス オプションに対して複数の LSP 属性を適用できます。必要な LSP 属性が帯域幅だけである場合、帯域幅上書きのパス オプションを設定できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、<https://cfngn.cisco.com/> にアクセスします。



## 第 17 章

# MPLS トラフィック エンジニアリング - トンネル用の設定可能なパス計算メトリックの設定

- [MPLS トラフィック エンジニアリング - トンネル用の設定可能なパス計算メトリックの前提条件 \(265 ページ\)](#)
- [MPLS トラフィック エンジニアリング - トンネル用の設定可能なパス計算メトリックの制約事項 \(266 ページ\)](#)
- [MPLS トラフィック エンジニアリング - トンネル用の設定可能なパス計算メトリックについて \(266 ページ\)](#)
- [MPLS トラフィック エンジニアリング - トンネル用の設定可能なパス計算メトリックの設定方法 \(267 ページ\)](#)
- [MPLS トラフィック エンジニアリング - トンネル用の設定可能なパス計算メトリックの設定例 \(275 ページ\)](#)
- [その他の参考資料 \(279 ページ\)](#)
- [MPLS トラフィック エンジニアリング - トンネル用の設定可能なパス計算メトリックに関する機能履歴 \(280 ページ\)](#)

## MPLS トラフィック エンジニアリング - トンネル用の設定可能なパス計算メトリックの前提条件

トンネルパス計算のメトリックを設定する前に、ネットワークで次の Cisco IOS XE 機能がサポートされている必要があります。

- マルチプロトコルラベルスイッチング (MPLS) トラフィック エンジニアリング トンネル
- IP シスコ エクスプレス フォワーディング
- Open Shortest Path First (OSPF) または Intermediate System-to-Intermediate System (IS-IS)

## MPLS トラフィック エンジニアリング - トンネル用の設定可能なパス計算メトリックの制約事項

- 明示的に設定しないかぎり、特定のリンクのTEリンクメトリックはIGPリンクメトリックになります。TEリンクメトリックを使用してコスト/距離以外のリンクプロパティを表す場合、**mpls traffic-eng administrative-weight** コマンドを使用して、TEトンネルに使用できるすべてのネットワークリンクに対して、そのプロパティを表すTEリンクメトリックを設定する必要があります。このようにしない場合は、トンネルによって予期しないパスが使用されることがあります。
- MPLS トラフィック エンジニアリングは、1つのIGPプロセスまたはインスタンスのみをサポートします。複数のIGPプロセスまたはインスタンスはサポートされないため、MPLS トラフィック エンジニアリングを複数のIGPプロセスまたはインスタンスで設定しないでください。

## MPLS トラフィック エンジニアリング - トンネル用の設定可能なパス計算メトリックについて

ここでは、MPLS トラフィック エンジニアリングのトンネル用の設定可能なパス計算メトリックについて説明します。

### 概要

MPLS トラフィック エンジニアリング - トンネルの設定可能なパス計算メトリック機能を使用すると、トラフィック エンジニアリング (TE) トンネルのパス計算で使用されるメトリックをトンネル単位で制御できます。

ネットワークでMPLS TEが設定されると、すべてのリンクに関して2種類のメトリック（通常のIGP（OSPFまたはIS-IS）リンクメトリックとTEリンクメトリック）が内部ゲートウェイプロトコル（IGP）によりフラッドイングされます。IGPは、通常宛先ネットワークのルートを計算するときと同じ方法で、IGPリンクメトリックを使用します。

次のいずれかのメトリックに基づいて各トンネルのパス計算を行うように指定することができます。

- IGP リンク メトリック。
- TE リンク メトリック。特定のアプリケーションのニーズを表すように設定できます。たとえば、TEリンクメトリックは、リンク伝搬遅延を表すように設定できます。

## 利点

トラフィック エンジニアリング (TE) トンネルを使用して2つのタイプのトラフィックを伝送する場合、トンネルの設定可能なパス計算メトリック機能を使用して、各タイプのトラフィックの要件に合わせてトンネルのパス選択を調整できます。

たとえば、(低遅延が要求される) 音声トラフィックの伝送に特定のトンネルを使用し、データの伝送には他のトンネルを使用するとします。この状況では、TE リンク メトリックを使用してリンク遅延を表し、次の作業を実行できます。

- パス計算のリンク遅延を表すように設定された TE リンク メトリックを使用するように音声伝送トンネルを設定します。
- パス計算に IGP メトリックを使用するようにデータ伝送トンネルを設定します。

# MPLS トラフィック エンジニアリング - トンネル用の設定可能なパス計算メトリックの設定方法

ここでは、MPLS トラフィック エンジニアリングのトンネル用の設定可能なパス計算メトリックを設定する手順について説明します。

## トラフィックエンジニアリングトンネルをサポートするためのプラットフォームの設定

トラフィック エンジニアリング トンネルをサポートするためのプラットフォームを設定するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例 : Device# <b>configure terminal</b>	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 3	<b>ip cef distributed</b> 例 :	分散型シスコ エクスプレス フォワーディング動作をイネーブルにします。

	コマンドまたはアクション	目的
	Device(config)# <b>ip cef distributed</b>	
ステップ 4	<b>mpls traffic-eng tunnels</b> 例 : Device(config)# <b>mpls traffic-eng tunnels</b>	デバイスで MPLS トラフィック エンジニアリング トンネル機能をイネーブルにします。
ステップ 5	<b>exit</b> 例 : Device(config)# <b>exit</b>	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

## MPLS トラフィック エンジニアリング用の IS-IS の設定



- (注) MPLS トラフィック エンジニアリングは、1つの IGP プロセスまたはインスタンスのみをサポートします。複数の IGP プロセスまたはインスタンスはサポートされていません。MPLS トラフィック エンジニアリングを複数の IGP プロセスまたはインスタンスで設定することはできません。

MPLS トラフィック エンジニアリング用に IS-IS を設定するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例 : Device# <b>configure terminal</b>	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 3	<b>router isis</b> 例 : Device(config)# <b>router isis</b>	IS-IS ルーティングをイネーブルにし、IS-IS プロセスを指定します。デバイスはコンフィギュレーション モードになります。

	コマンドまたはアクション	目的
ステップ 4	<b>mpls traffic-eng level</b> 例： Device (config-router) # <b>mpls traffic-eng level-1</b>	IS-IS レベル 1 で MPLS トラフィック エンジニアリングをオンにします。
ステップ 5	<b>mpls traffic-eng level</b> 例： Device (config-router) # <b>mpls traffic-eng level-2</b>	IS-IS レベル 2 で MPLS トラフィック エンジニアリングをオンにします。
ステップ 6	<b>mpls traffic-eng router-id type number</b> 例： Device (config-router) # <b>mpls traffic-eng router-id loopback 0</b>	ノードのトラフィック エンジニアリング ルータ識別子が、インターフェイス loopback0 に関連付けられている IP アドレスになるように指定します。
ステップ 7	<b>metric-style wide</b> 例： Device (config-router) # <b>metric-style wide</b>	新スタイルのタイプ、長さ、値 (TLV) オブジェクトだけを生成して受け入れるようにルータを設定します。

## トラフィック エンジニアリング リンク メトリックの設定

明示的に設定しないかぎり、TE リンク メトリックは IGP リンク メトリックになります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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 3	<b>interface type slot / subslot / port [subinterface-number]</b> 例： Device (config)# <b>interface port channel 20</b>	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。  • <i>type</i> 引数は、設定するインターフェイスのタイプです。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <i>slot</i> 引数はシャーシのスロット番号です。</li> <li>• <i>/subslot</i> キーワードと引数のペアは、SPA がインストールされている SIP のセカンダリスロット番号です。スラッシュ (/) が必要です。</li> <li>• <i>/port</i> キーワードと引数のペアは、ポートまたはインターフェイスの番号です。スラッシュ (/) が必要です。</li> <li>• <i>.subinterface-number</i> キーワードと引数のペアは、サブインターフェイスの番号で、範囲は 1 ~ 4294967293 です。ピリオド (.) の前の番号は、このサブインターフェイスが属する番号と一致する必要があります。</li> </ul>
ステップ 4	<b>mpls traffic-eng administrative-weight weight</b> 例 : Device(config-if)# <b>mpls traffic-eng administrative-weight 20</b>	リンクの IGP 管理上の重み (コスト) を無効にします。 <ul style="list-style-type: none"> <li>• <i>weight</i> 引数はリンクのコストです。</li> </ul>
ステップ 5	<b>exit</b> 例 : Device(config-if)# <b>exit</b>	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 6	<b>exit</b> 例 : Device(config)# <b>exit</b>	グローバル コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

## MPLS トラフィック エンジニアリング トンネルの設定

MPLS TE トンネルの優先明示パスを設定するには、次の手順を実行します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  Device> <b>enable</b>	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例 :  Device# <b>configure terminal</b>	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 3	<b>interface tunnel number</b> 例 :  Device(config)# <b>interface Tunnel0</b>	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。  • <i>number</i> 引数はトンネルの番号です。
ステップ 4	<b>ip unnumbered type number</b> 例 :  Device(config-if)# <b>ip unnumbered loopback0</b>	明示的な IP アドレスをインターフェイスに割り当てずにインターフェイス上の IP 処理をイネーブルにします。  • <i>type</i> 引数および <i>number</i> 引数では、ルータに IP アドレスが割り当てられている別のインターフェイスのタイプと番号を指定します。番号付けされていない別のインターフェイスは指定できません。  • MPLS トラフィック エンジニアリング トンネル インターフェイスは単一方向リンクを表すため、番号なしにする必要があります。
ステップ 5	<b>tunnel destination ip-address</b> 例 :  Device(config-if)# <b>tunnel destination 192.168.4.4</b>	トンネル インターフェイスの宛先を指定します。  • <i>ip-address</i> 引数では、宛先デバイスの MPLS トラフィック エンジニアリング ルータ ID を指定する必要があります。

	コマンドまたはアクション	目的
ステップ 6	<b>tunnel mode mpls traffic-eng</b> 例 : <pre>Device(config-if)# tunnel mode mpls traffic-eng</pre>	トンネル カプセル化モードを MPLS トラフィック エンジニアリングに設定します。
ステップ 7	<b>tunnel mpls traffic-eng bandwidth bandwidth</b> 例 : <pre>Device(config-if)# tunnel mpls traffic-eng bandwidth 250</pre>	MPLS トラフィック エンジニアリング トンネルの帯域幅を設定します。 <ul style="list-style-type: none"> <li>• <b>bandwidth</b> 引数は、MPLS トラフィック エンジニアリング トンネルで確保する kbps 単位の数値です。範囲は 1 ~ 4294967295 です。</li> </ul> (注) トンネルに自動帯域幅が設定されている場合は、 <b>tunnel mpls traffic-eng bandwidth</b> コマンドを使用して、トンネルの初期帯域幅を設定します。
ステップ 8	<b>tunnel mpls traffic-eng path-option number {dynamic   explicit {name path-name   identifier path-number}} [lockdown]</b> 例 : <pre>Device(config-if)# tunnel mpls traffic-eng path-option 10 explicit identifier 321</pre>	指定した IP 明示パス、またはトラフィック エンジニアリング トポロジデータベースからダイナミックに計算されたパスを使用するように、トンネルを設定します。 <ul style="list-style-type: none"> <li>• <b>number</b> 引数は、このパス オプションの優先度です。複数のパス オプションを設定する場合、より低い数値のオプションが優先されます。有効値は 1 ~ 1000 です。</li> <li>• <b>dynamic</b> キーワードは、LSP のパスがダイナミックに計算されることを示します。</li> <li>• <b>explicit</b> キーワードは、LSP のパスが IP 明示パスの場合に指定します。</li> <li>• <b>name path-name</b> のキーワードと引数のペアは、トンネルがこのオプションで使用する IP 明示パスのパス名です。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>identifier path-number</b> のキーワードと引数のペアは、トンネルがこのオプションで使用する IP 明示パスのパス番号です。有効な範囲は 1 ~ 65535 です。</li> <li>• <b>lockdown</b> キーワードは、LSP を再最適化できないようにする場合に指定します。</li> </ul> <p>(注) 明示パスが現在使用可能でない場合は、ダイナミックパスが使用されます。</p>
ステップ 9	<b>exit</b> 例 : Device(config-if) # <b>exit</b>	インターフェイスコンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。

## トンネルパス計算用のメトリック タイプの設定

明示的に設定されていない限り、TE リンクメトリックタイプはトンネルパスの計算に使用されません。使用するメトリックタイプを制御するための2つのコマンドがあります。インターフェイス コンフィギュレーション コマンドでは、特定の TE トンネルに使用するメトリックタイプを指定します。グローバル コンフィギュレーション コマンドでは、インターフェイス コンフィギュレーションコマンドでメトリックタイプが指定されていないTE トンネルに使用するメトリックタイプを指定します。



(注) どちらのパス選択メトリック コマンドも入力しない場合は、トラフィック エンジニアリング (TE) メトリックが使用されます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例 :	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。

	コマンドまたはアクション	目的
	Device# <code>configure terminal</code>	
ステップ 3	<b>interface tunnel number</b> 例 : Device(config)# <code>interface Tunnel0</code>	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> <li>• <b>number</b> 引数はトンネルのポート番号です。</li> </ul>
ステップ 4	<b>tunnel mpls traffic-eng path-selection metric {igp   te}</b> 例 : Device(config-if)# <code>tunnel mpls traffic-eng path-selection metric igp</code>	トンネルのパス計算に使用するメトリック タイプを指定します。 <ul style="list-style-type: none"> <li>• <b>igp</b> キーワードは、内部ゲートウェイ プロトコル (IGP) メトリックを使用する場合に指定します。</li> <li>• <b>te</b> キーワードは、トラフィック エンジニアリング (TE) メトリックを使用する場合に指定します。これがデフォルトです。</li> </ul>
ステップ 5	<b>exit</b> 例 : Device(config-if)# <code>exit</code>	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
ステップ 6	<b>mpls traffic-eng path-selection metric {igp   te}</b> 例 : Device(config)# <code>mpls traffic-eng path-selection metric igp</code>	特定のトンネルに対してメトリック タイプが明示的に設定されていない場合に使用するメトリック タイプを指定します。 <ul style="list-style-type: none"> <li>• <b>igp</b> キーワードは、内部ゲートウェイ プロトコル (IGP) メトリックを使用する場合に指定します。</li> <li>• <b>te</b> キーワードは、トラフィック エンジニアリング (TE) メトリックを使用する場合に指定します。これがデフォルトです。</li> </ul>
ステップ 7	<b>exit</b> 例 : Device(config)# <code>exit</code>	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

## トンネルパスメトリック設定の確認

トンネルパスメトリックの設定を確認するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	<b>show mpls traffic-eng topology</b> 例： Device# <b>show mpls traffic-eng topology</b>	各リンクの TE および IGP メトリックを表示し、ネットワークにリンクメトリックが正しく設定されていることを確認します。
ステップ 3	<b>show mpls traffic-eng tunnels</b> 例： Device# <b>show mpls traffic-eng tunnels</b>	トンネルパス計算に使用されるリンクメトリックを表示し、各トンネルに必要なリンクメトリックが使用されていることを確認します。
ステップ 4	<b>exit</b> 例： Device# <b>exit</b>	ユーザ EXEC モードに戻ります。

## MPLS トラフィック エンジニアリング - トンネル用の設定可能なパス計算メトリックの設定例

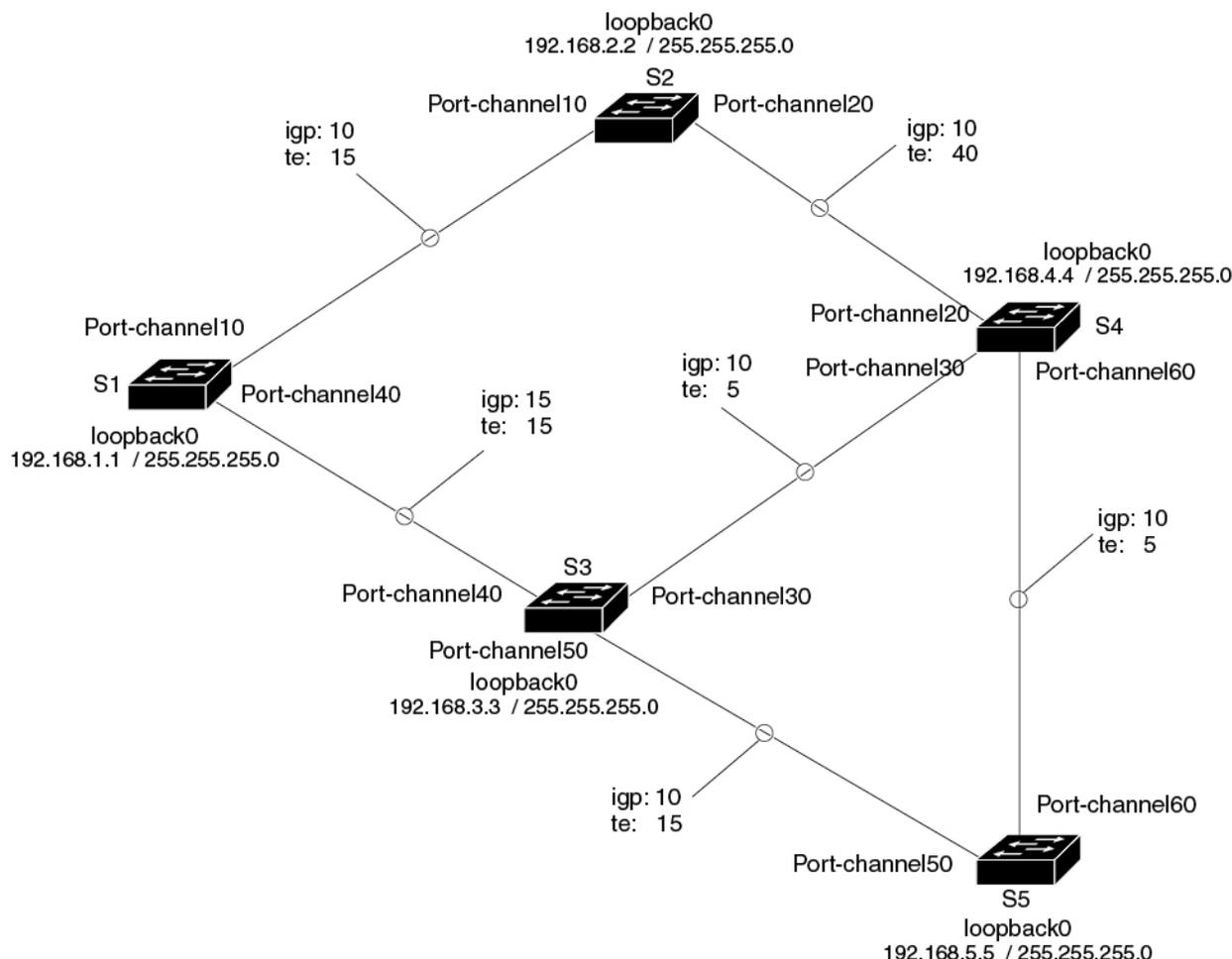
ここでは、トンネル用の設定可能なパス計算メトリックの設定例を紹介します。

### 例：トンネルパス選択のリンクタイプとメトリックの設定

ここでは、トンネルのパス選択に使用するリンクメトリックタイプの設定方法、およびリンクメトリック自体の設定方法を示します。ここで使用されているコンフィギュレーションコマンドでは、パス計算用のメトリックタイプの指定、およびリンクへのメトリックの割り当てに重点を置いています。例のシナリオを完全に設定するには、追加のコマンドが必要です。たとえば、トラフィックエンジニアリング用の IGP コマンドや、トラフィックエンジニアリングをイネーブルにして使用可能な帯域幅を割り当てるためのリンクインターフェイスコマンドが必要となります。

ここに示す例では、下の図に示す単純なネットワークテクノロジーがサポートされています。

図 23: ネットワーク トポロジ



上の図では、次のように設定されています。

- Tunnel1 と Tunnel2 は、S1（ヘッドエンド）から S4（テールエンド）まで伸びています。
- Tunnel3 は S1 から S5 に実行されます。
- Tunnel1 と Tunnel3 のパス計算では、リンク遅延を表すメトリックを使用する必要があります。これらのトンネルでは音声トラフィックを伝送するためです。
- Tunnel2 のパス計算では、IGP メトリックを使用する必要があります。これは、MPLS TE が遅延要件なしでデータトラフィックを伝送するためです。

次に、各デバイスの設定の一部を示します。これらの設定は、リンクメトリック、およびトンネルパス計算でのそのリンクメトリックの使用に関連しています。リンク遅延を表す TE メトリックは、各デバイスのネットワークリンクに対して設定する必要があります。また、S1 には 3 つのトンネルを設定する必要があります。

これらの設定では、Tunnel1 ではパス S1-S3-S4、Tunnel2 ではパス S1-S2-S4、Tunnel3 ではパス S1-S3-S4-S5 が強制的に使用されるようにしています（リンクの帯域幅がトンネルに対応するのに十分であることを前提とした場合）。

### S1 Configuration

次の例は、上の図に示されている Tunnel1、Tunnel2、および Tunnel3 のトンネルのヘッドエンド (S1) を設定する方法を示しています。

```
interface port channel 40
mpls traffic-eng administrative-weight 15      !TE metric different from IGP metric
interface port channel 10
mpls traffic-eng administrative-weight 15      !TE metric different from IGP metric
interface Tunnel1                               !Tunnel1 uses TE metric (default)
                                              !for path selection

ip unnumbered loopback0
tunnel destination 192.168.4.4 255.255.255.0
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng bandwidth 1000
tunnel mpls traffic-eng path-option 1 dynamic
interface Tunnel2                               !Tunnel2 uses IGP metric
                                              !for path selection

ip unnumbered loopback0
tunnel destination 192.168.4.4 255.255.255.0
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng bandwidth 1000
tunnel mpls traffic-eng path-option 1 dynamic
tunnel mpls traffic-eng path-selection-metric igp !Use IGP cost for path selection.
interface Tunnel3                               !Tunnel3 uses TE metric (default)
                                              !for path selection

ip unnumbered loopback0
tunnel destination 192.168.5.5 255.255.255.0
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng bandwidth 1000
tunnel mpls traffic-eng path-option 1 dynamic
```

### S2 Configuration

次の例は、上の図に示されている S2 の設定方法を示しています。

```
interface port channel 10
mpls traffic-eng administrative-weight 15      !TE metric different from IGP metric
interface port channle 20
mpls traffic-eng administrative-weight 40      !TE metric different from IGP metric
```

### S3 Configuration

次の例は、上の図に示されている S3 の設定方法を示しています。

```
interface port channel 40
mpls traffic-eng administrative-weight 15      !TE metric different from IGP metric
interface port channel 50
mpls traffic-eng administrative-weight 15      !TE metric different from IGP metric
interface port channel 30
mpls traffic-eng administrative-weight 5       !TE metric different from IGP metric
```

### S4 Configuration

次の例は、上の図に示されている R4 の設定方法を示しています。

```

interface port channel 20
mpls traffic-eng administrative-weight 15      !TE metric different from IGP metric
interface port channel 30
mpls traffic-eng administrative-weight 15      !TE metric different from IGP metric
interface port channel 60
mpls traffic-eng administrative-weight 5       !TE metric different from IGP metric

```

### S5 Configuration

次の例は、上の図に示されている S5 の設定方法を示しています。

```

interface port channel 50
mpls traffic-eng administrative-weight 15      !TE metric different from IGP metric
interface port channel 60
mpls traffic-eng administrative-weight 5       !TE metric different from IGP metric

```

## 例：トンネルパスメトリック設定の確認

次に、トンネルパスメトリックの設定を確認する例を示します。

次に、**show mpls traffic-eng topology** コマンドの出力例を示します。このコマンドにより、各リンクの TE および IGP メトリックが表示されます。

```

Device# show mpls traffic-eng topology
My_System_id: 1440.0000.0044.00 (isis level-1)
IGP Id: 0090.0000.0009.00, MPLS TE Id:192.168.9.9 Router Node (isis level-1)
  link[0 ]:Nbr IGP Id: 0090.0000.0009.03, gen:7
    frag_id 0, Intf Address:10.0.0.99
    TE metric:100, IGP metric:48, attribute_flags:0x0    !!Note TE and IGP metrics
    physical_bw: 10000 (kbps), max_reservable_bw_global: 0 (kbps)
    max_reservable_bw_sub: 0 (kbps)
  .
  .
  .
  link[1 ]:Nbr IGP Id: 0055.0000.0055.00, gen:7
    frag_id 0, Intf Address:10.205.0.9, Nbr Intf Address:10.205.0.55
    TE metric:120, IGP metric:10, attribute_flags:0x0    !!Note TE and IGP metrics
    physical_bw: 155000 (kbps), max_reservable_bw_global: 500000 (kbps)
    max_reservable_bw_sub: 0 (kbps)

```

次に、**show mpls traffic-eng tunnels** コマンドの出力例を示します。このコマンドにより、トンネルパスの計算に使用されるリンクメトリックが表示されます。

```

Device# show mpls traffic-eng tunnels
Name: te3640-17-c_t221 (Tunnel22) Destination: 192.168.100.22
Status:
  Admin: up      Oper: up      Path: valid      Signalling: connected
  path option 1, type dynamic (Basis for Setup, path weight 10)
Config Parameters:
  Bandwidth: 400 kps (Global)  Priority: 1 1  Affinity: 0x0/0xFFFF
  Metric Type: IGP                                     !!Note metric type

```

```

AutoRoute: enabled LockDown: disabled Loadshare: 0 bw-based
auto-bw: disabled(0/115) 0 Bandwidth Requested: 0
.
.
.
Name: te3640-17-c_t222 (Tunnel133) Destination: 192.168.100.22
Status:
Admin: up Oper: up Path: valid Signalling: connected
path option 1, type dynamic (Basis for Setup, path weight 10)
Config Parameters:
Bandwidth: 200 kbps (Global) Priority: 1 1 Affinity: 0x0/0xFFFF
Metric Type: TE !!Note metric type
AutoRoute: enabled LockDown: disabled Loadshare: 0 bw-based
auto-bw: disabled(0/115) 0 Bandwidth Requested: 0
.
.
.

```

## その他の参考資料

### 関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『 <a href="#">Cisco IOS Master Commands List, All Releases</a> 』
IS-IS および OSPF の設定作業	『 <a href="#">Cisco IOS XE IP Routing Protocols Configuration Guide</a> 』
IS-IS および OSPF コマンド	『 <a href="#">Cisco IOS IP Routing Protocols Command Reference</a> 』
MPLS および MPLS TE の設定作業	『 <a href="#">Cisco IOS XE Multiprotocol Label Switching Configuration Guide</a> 』
MPLS TE コマンド	『 <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a> 』
トンネルの設定作業	<ul style="list-style-type: none"> <li>『<a href="#">Cisco IOS XE Interface and Hardware Component Configuration Guide</a>』</li> <li>『<a href="#">Cisco IOS XE Multiprotocol Label Switching Configuration Guide</a>』</li> </ul>
トンネル コンフィギュレーション コマンド	<ul style="list-style-type: none"> <li>『<a href="#">Cisco IOS Interface and Hardware Component Command Reference</a>』</li> <li>『<a href="#">Cisco IOS XE Multiprotocol Label Switching Command Reference</a>』</li> </ul>

## シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## MPLS トラフィック エンジニアリング - トンネル用の設定可能なパス計算メトリックに関する機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Bengaluru 17.6.1	MPLS トラフィック エンジニアリング - トンネルの設定可能なパス計算メトリック	MPLS トラフィック エンジニアリング - トンネルの設定可能なパス計算メトリック機能を使用すると、トラフィック エンジニアリング (TE) トンネルのパス計算で使用されるメトリックをトンネル単位で制御できます。特定のトンネルを使用して低遅延が要求される音声トラフィックを伝送し、他のトンネルを使用してデータを伝送します。TE リンク メトリックを使用すると、リンク遅延を表し、パス計算用に音声トラフィック伝送トンネルを設定し、パス計算に Interior Gateway Protocol (IGP) メトリックを使用するようにデータ伝送トンネルを設定できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、<https://cfmng.cisco.com/>にアクセスします。





## 第 18 章

# 仮想プライベート LAN サービス (VPLS) および VPLS BGP ベースの自動検出の設定

- [VPLS の制約事項 \(283 ページ\)](#)
- [VPLS、VPLS BGP ベースの自動検出、および Flow Aware Transport に関する情報 \(284 ページ\)](#)
- [VPLS、VPLS BGP ベースの自動検出、および Flow Aware Transport の設定方法 \(288 ページ\)](#)
- [VPLS および VPLS BGP ベースの自動検出の設定例 \(309 ページ\)](#)
- [VPLS および VPLS BGP ベースの自動検出の機能情報 \(315 ページ\)](#)

## VPLS の制約事項

- レイヤ 2 プロトコルトネリングの設定はサポートされていません。
- Integrated Routing and Bridging (IRB) の設定はサポートされていません。
- 明示的 null の仮想回線接続検証 (VCCV) ping はサポートされていません。
- スイッチは、ハブとしてではなく、階層型仮想プライベート LAN サービス (VPLS) でスポークとして設定されている場合にのみサポートされます。
- レイヤ 2 VPN インターワーキング機能はサポートされていません。
- **ip unnumbered** コマンドは、マルチプロトコル ラベル スイッチング (MPLS) 構成ではサポートされていません。
- フラッドトラフィックの場合、仮想回線 (VC) 統計情報は、**show mpls l2 vc vcid detail** コマンドの出力に表示されません。
- 接続回線では、Dot1q トンネル構成はサポートされていません。

# VPLS、VPLS BGP ベースの自動検出、および Flow Aware Transport に関する情報

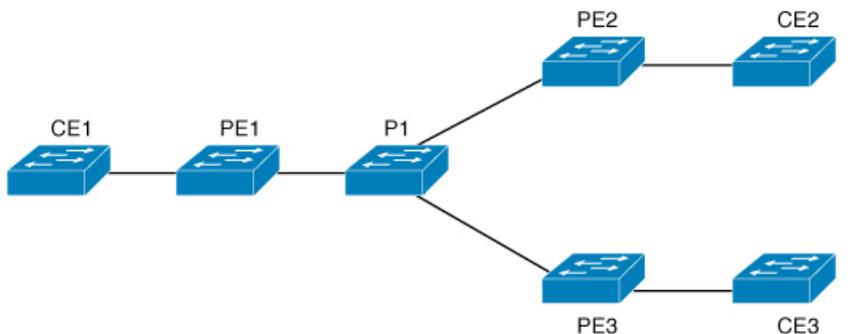
次の項では、VPLS、VPLS BGP ベースの自動検出、および Flow Aware Transport について説明します。

## VPLS の概要

VPLSにより、企業は、サービスプロバイダーから提供されるインフラストラクチャを介して、複数サイトからのイーサネットベースの LAN をまとめてリンクできます。企業の側からは、サービスプロバイダーのパブリックネットワークは、1つの大きなイーサネット LAN のように見えます。サービスプロバイダーからすると、VPLSは、大規模な設備投資なしで、既存のネットワーク上に収益を生み出す新たなサービスを導入するチャンスになります。オペレータは、ネットワークでの機器の運用年数を延長できます。

VPLSはプロバイダーコアを使用して複数の接続回線をまとめ、複数の接続回線間の仮想ブリッジをシミュレートします。VPLS のトポロジは、カスタマーからは認識されません。すべてのカスタマーエッジ (CE) デバイスは、プロバイダーコアによってエミュレートされた論理ブリッジに接続されているように見えます。

図 24: VPLS トポロジ



## フルメッシュ構成について

フルメッシュ構成では、VPLSに参加するすべてのプロバイダーエッジ (PE) デバイス間でトンネルラベルスイッチパス (LSP) のフルメッシュが必要です。フルメッシュ構成では、シグナリングのオーバーヘッドと、PE デバイス上でプロビジョニング対象の VC に対するパケット複製の要件が多くなります。

フルメッシュ構成の場合、参加している各 PE デバイスに仮想転送インスタンス (VFI) が必要です。VFI には、VPLS ドメインの VPN ID、そのドメインの他の PE デバイスのアドレス、トンネルシグナリングのタイプ、各ピア PE デバイスのカプセル化のメカニズムが含まれます。

VPLS インスタンスは、エミュレート VC の相互接続によって形成される一連の VFI を構成します。VPLS インスタンスは、パケット交換ネットワーク上の論理ブリッジを形成します。VPLS インスタンスには、一意の VPN ID が割り当てられます。

PE デバイスは、VFI を使用して、エミュレートされた VC から VPLS インスタンスの他のすべての PE デバイスまでのフルメッシュ LSP を確立します。PE デバイスは、Cisco IOS CLI を使用して、スタティック設定を通じた VPLS インスタンスのメンバーシップを取得します。

フルメッシュ構成では、PE デバイスが単一のブロードキャストドメインを維持できます。そのため、接続回線でブロードキャスト、マルチキャスト、または未知のユニキャストパケットを受信すると、PE デバイスは、他のすべての接続回線およびエミュレート回線のパケットを、その VPLS インスタンスに参加している他のすべての CE デバイスへに送信します。CE デバイスでは、VPLS インスタンスを、エミュレート LAN として認識します。

プロバイダーコアでのパケットループの問題を回避するために、PE デバイスは、エミュレート VC に「スプリットホライズン」の原則を適用します。スプリットホライズンの原則により、エミュレート VC でパケットを受信したパケットは、他のいずれのエミュレート VC にも転送されなくなります。

VFI を定義したら、CE デバイスへの接続回線にバインドする必要があります。

パケット転送の判断は、特定の VPLS ドメインのレイヤ 2 VFI を検索することによって行われます。

特定の PE デバイスの VPLS インスタンスは、特定の物理または論理ポートに着信するイーサネットフレームを受信し、イーサネットスイッチによる動作同様に、MAC アドレステーブルに入力します。PE デバイスは、この MAC アドレスを使用して、リモートサイトにある別の PE デバイスに配布するために、このようなフレームを適切な LSP に切り替えます。

MAC アドレスが MAC アドレステーブルにない場合、PE デバイスは、イーサネットフレームを複製し、イーサネットフレームが入力された入力ポートを除く、その VPLS インスタンスに関連付けられたすべての論理ポートにフラッドします。PE デバイスは、特定のポートでパケットを受信したときに MAC アドレステーブルを更新し、一定期間使用されていないアドレスを削除します。

## VPLS BGP ベースの自動検出について

VPLS 自動検出を使用すると、各 PE デバイスで、同じ VPLS ドメインの一部である他の PE デバイスを検出できます。VPLS 自動検出は、PE デバイスが VPLS ドメインに追加、またはドメインから削除されたタイミングも追跡します。VPLS 自動検出を有効にすると、VPLS ドメインを手動で設定したり、PE デバイスが追加または削除されたときに設定を維持したりする必要がなくなります。VPLS 自動検出は、ボーダー ゲートウェイ プロトコル (BGP) を使用して、VPLS メンバーを検出し、VPLS ドメイン内の擬似回線 (PW) をセットアップおよび解除します。

BGP では、エンドポイントプロビジョニング情報を保存する際にレイヤ 2 VPN ルーティング情報ベース (RIB) が使用されます。これは、レイヤ 2 VFI が設定されるたびにアップデートされます。プレフィックスおよびパス情報はレイヤ 2 VPN データベースに保存され、ベストパスが BGP により決定されるようになります。BGP により、更新メッセージですべての BGP ネ

イパーにエンドポイントプロビジョニング情報が配布される場合、レイヤ2VPNベースのサービスをサポートするために、このエンドポイント情報を使用して疑似回線メッシュが設定されます。

BGP 自動検出のメカニズムにより、VPLS 機能に必要な不可欠なレイヤ2VPNサービスの設定が簡易化されます。VPLSは、高速イーサネットを使用した堅牢でスケーラブルなIP MPLSネットワークによる大規模なLANとして、地理的に分散した拠点間を接続することで柔軟なサービスの展開を実現します。

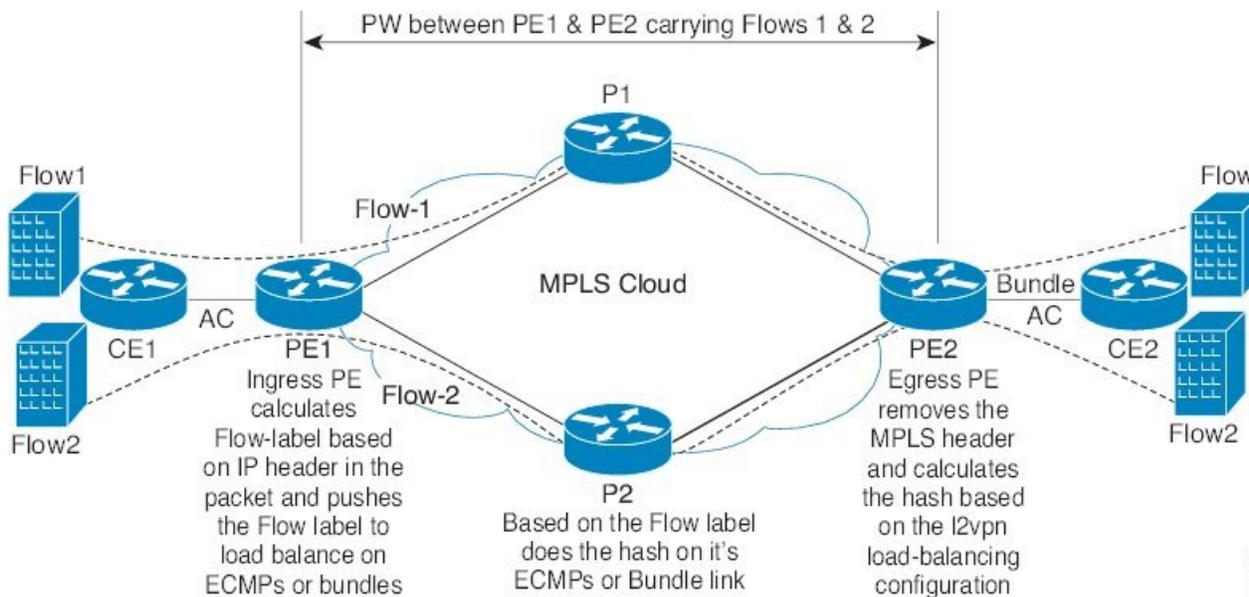
## Flow Aware Transport 疑似回線について

デバイスは通常、ラベルスタックの最低ラベル（特定の疑似回線のすべてのフローに対して同じラベル）に基づいてトラフィックをロードバランスします。このとき、非対称ロードバランシングが発生することがあります。このコンテキストでは、フローは同じ送信元/宛先ペアを持つパケットのシーケンスを示します。パケットは、送信元プロバイダーエッジ (PE) デバイスから宛先 PE デバイスに転送されます。

Flow Aware Transport PW は、PW 内の個々のフローを識別する機能を提供します。また、それらのフローを使用してトラフィックをロードバランスする機能をデバイスに提供します。Equal Cost Multipath (ECMP; 等コストマルチパス) が使用されている場合、Flow Aware Transport PW はコア内のトラフィックのロードバランスに使用されます。PW に伝送される個々のパケットフローに基づいてフローラベルが作成され、最低ラベルとしてパケットに挿入されます。デバイスは、フローラベルをロードバランシングに使用でき、コア内のECMPパスまたはリンクがバンドルされたパスでより適切なトラフィックの分配が行われます。

図 25 : Flow Aware Transport PW と、ECMP およびバンドルされたリンクへ分配される 2つのフローに、Flow Aware Transport PW と、ECMP およびバンドルされたリンクへ分配される 2つのフローの例を示します。

図 25 : Flow Aware Transport PW と、ECMP およびバンドルされたリンクへ分配される 2つのフロー



追加のラベルは、仮想回線 (VC) のフロー情報を含むスタック (フローラベルと呼ばれる) に追加されます。フローラベルは、PW 内のフローを区別する一意の ID で、送信元/宛先 MAC アドレスと送信元/宛先 IP アドレスから取得されます。フローラベルにはラベルスタック (EOS) ビットセットの末尾が含まれ、VC ラベルの後ろや、コントロールワード (存在する場合) の前に挿入されます。入力 PE は、フローラベルを計算し、転送します。Flow Aware Transport PW コンフィギュレーションは、フローラベルを有効にします。出力 PE は、決定が行われないように、フローラベルを廃棄します。

すべてのコアデバイスが、Flow Aware Transport PW でフローラベルに基づいてロードバランシングを実行します。これにより、ECMP とリンクバンドルへのフローの分配が可能になります。

Flow Aware Transport PW は、ポートチャネルロードバランシングアルゴリズムのみに基づいて動作します。

## Cisco Catalyst 6000 シリーズ スイッチと Cisco Catalyst 9000 シリーズ スイッチ間の相互運用性

次の項では、Cisco Catalyst 6000 シリーズ スイッチと Cisco Catalyst 9000 シリーズ スイッチ間でフローラベルを送受信できるようにする方法について説明します。

Flow Aware Transport PW (Advanced VPLS を使用) で設定された Cisco Catalyst 6000 シリーズ スイッチでは、フローラベルのネゴシエーションはサポートされていません。Cisco Catalyst 6000 シリーズ スイッチが Cisco Catalyst 9000 シリーズ スイッチなどのリモート PE デバイスと相互運用可能な場合、Cisco Catalyst 9000 シリーズ スイッチはデータトラフィックのフローラベルを送受信できません。Cisco Catalyst 9000 シリーズ スイッチで **load-balance flow-label both static** コマンドを設定すると、Cisco Catalyst 6000 シリーズ スイッチがフローラベルのネゴシエーションをサポートしていない場合でも、Cisco Catalyst 9000 シリーズ スイッチでフローラベルを送受信できます。

次に、フローラベルの送受信を有効にする設定例を示します。

```
Device> enable
Device# configure terminal
Device(config)# template type pseudowire mpls
Device(config-template)# encapsulation mpls
Device(config-template)# load-balance flow ip dst-ip
Device(config-template)# load-balance flow-label both static
Device(config-template)# end
```

## VPLS を介した IGMP/MLD スヌーピング

Cisco IOS XE Bengaluru 17.6.1 のリリースから、VPLS を介した MLD スヌーピングがサポートされるようになりました。VPLS を介した IGMP スヌーピングのサポートが Cisco IOS XE Amsterdam 17.1.1 のリリースで導入されました。

VPLS を介した IGMP/MLD スヌーピングを有効にすると、リモートプロバイダーエッジ (PE) デバイスから IGMP/MLD レポートを受信する疑似回線でトラフィックが転送されます。IGMP/MLD クエリとレポートは、すべての疑似回線にフラッディングされます。

MLD スヌーピングはデフォルトでは有効になっていないため、グローバルレベルで設定する必要があります。

IGMP スヌーピングは、デフォルトではグローバルレベルで有効になっています。

MLD スヌーピングの詳細については、「IPv6 MLDスヌーピングの設定に関する情報」を参照してください。

IGMP スヌーピングについては、「IGMP スヌーピング」を参照してください。

## VPLS、VPLS BGP ベースの自動検出、および Flow Aware Transport の設定方法

次の項では、VPLS、VPLS BGP ベースの自動検出、および Flow Aware Transport に関する設定情報について説明します。

### CE デバイスへのレイヤ 2 PE デバイスインターフェイスの設定

CE デバイスへのレイヤ 2 PE デバイスインターフェイスを設定する必要があります。次の項では、VPLS を設定する前に完了する必要があるさまざまな設定作業について説明します。

### CE デバイスからのタグ付きトラフィックを受け取る PE デバイスの 802.1Q トランクの設定

PE デバイスで 802.1Q トランクを設定するには、次の手順を実行します。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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 3	<b>interface interface-id</b> 例： Device(config)# <b>interface TenGigabitEthernet1/0/24</b>	トランクとして設定するインターフェイスを定義し、インターフェイスコンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	<b>no ip address <i>ip_address mask</i> [secondary]</b> 例 : Device(config-if) # <b>no ip address</b>	IP 処理をディセーブルにして、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	<b>switchport</b> 例 : Device(config-if) # <b>switchport</b>	レイヤ 2 スイッチドインターフェイスのスイッチング特性を変更します。
ステップ 6	<b>switchport trunk encapsulation dot1q</b> 例 : Device(config-if) # <b>switchport trunk encapsulation dot1q</b>	スイッチ ポートのカプセル化形式を 802.1Q に設定します。
ステップ 7	<b>switchport trunk allow vlan <i>vlan_ID</i></b> 例 : Device(config-if) # <b>switchport trunk allow vlan 2129</b>	許可 VLAN のリストを設定します。
ステップ 8	<b>switchport mode trunk</b> 例 : Device(config-if) # <b>switchport mode trunk</b>	トランキング VLAN レイヤ 2 インターフェイスへのインターフェイスを設定します。
ステップ 9	<b>end</b> 例 : Device(config-if) # <b>end</b>	特権 EXEC モードに戻ります。

## CE デバイスからのタグなしトラフィックを受け取る PE デバイスの 802.1Q アクセスポートの設定

PE デバイスで 802.1Q アクセスポートを設定するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。

## PE デバイスでのレイヤ 2 VLAN インスタンスの設定

	コマンドまたはアクション	目的
ステップ 2	<b>configure terminal</b> 例 :  Device# <b>configure terminal</b>	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 3	<b>interface interface-id</b> 例 :  Device(config)# <b>interface TenGigabitEthernet1/0/24</b>	トランクとして設定するインターフェイスを定義し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 4	<b>no ip address ip_address mask [secondary ]</b> 例 :  Device(config-if)# <b>no ip address</b>	IP 処理をディセーブルにします。
ステップ 5	<b>switchport</b> 例 :  Device(config-if)# <b>switchport</b>	レイヤ 2 スイッチドインターフェイスのスイッチング特性を変更します。
ステップ 6	<b>switchport mode access</b> 例 :  Device(config-if)# <b>switchport mode access</b>	インターフェイスタイプを、非トランキング、タグなし、シングル VLAN レイヤ 2 インターフェイスとして設定します。
ステップ 7	<b>switchport access vlan vlan_ID</b> 例 :  Device(config-if)# <b>switchport access vlan 2129</b>	インターフェイスがアクセス モードのときに VLAN を設定します。
ステップ 8	<b>end</b> 例 :  Device(config-if)# <b>end</b>	特権 EXEC モードに戻ります。

## PE デバイスでのレイヤ 2 VLAN インスタンスの設定

PE デバイスにレイヤ 2 VLAN インターフェイスを設定すると、VLAN データベースへの PE デバイス上のレイヤ 2 VLAN インスタンスで、VPLS と VLAN 間のマッピングを設定できます。

PE デバイスでレイヤ 2 VLAN インスタンスを設定するには、次の手順を実行します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例 : Device# <b>configure terminal</b>	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 3	<b>vlan vlan-id</b> 例 : Device (config)# <b>vlan 2129</b>	特定の VLAN を設定します。
ステップ 4	<b>interface vlan vlan-id</b> 例 : Device (config-vlan)# <b>interface vlan 2129</b>	この VLAN にインターフェイスを設定します。
ステップ 5	<b>end</b> 例 : Device (config-vlan)# <b>end</b>	特権 EXEC モードに戻ります。

## VPLS の設定

VPLS は、Xconnect モードまたはプロトコル CLI 方式を使用して設定できます。次の項では、VPLS の設定方法について説明します。

### Xconnect モードでの VPLS の設定

次の項では、Xconnect モードでの VPLS の設定について説明します。

#### PE デバイス上での MPLS の設定

PE デバイスで MPLS を設定するには、次の手順を実行します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例 : Device# <b>configure terminal</b>	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 3	<b>mpls ip</b> 例 : Device(config)# <b>mpls ip</b>	MPLS ホップバイホップ転送を設定します。
ステップ 4	<b>mpls label protocol ldp</b> 例 : Device(config)# <b>mpls label protocol ldp</b>	プラットフォームの Label Distribution Protocol (LDP; ラベル配布プロトコル) を指定します。
ステップ 5	<b>mpls ldp logging neighbor-changes</b> 例 : Device(config)# <b>mpls ldp logging neighbor-changes</b>	(任意) ネイバーの変更の記録を指定します。
ステップ 6	<b>end</b> 例 : Device(config)# <b>end</b>	特権 EXEC モードに戻ります。

## PE デバイスでの VFI の設定

VFI によって VPLS ドメインの VPN ID、そのドメインの他の PE デバイスのアドレス、トンネルのシグナリングのタイプ、各ピアデバイスのカプセル化のメカニズムが指定されます。

PE デバイスで VFI および関連する VC を設定するには、次の手順を実行します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	Device> <b>enable</b>	パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例 : Device# <b>configure terminal</b>	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 3	<b>l2 vfi vfi-name manual</b> 例 : Device(config)# <b>l2 vfi 2129 manual</b>	レイヤ 2 VFI 手動コンフィギュレーション モードをイネーブルにします。
ステップ 4	<b>vpn id vpn-id</b> 例 : Device(config-vfi)# <b>vpn id 2129</b>	VPLS ドメインの VPN ID を設定します。このレイヤ 2 Virtual Routing Forwarding (VRF) にバインドされたエミュレート VC でシグナリングにこの VPN ID が使用されます。  (注) <i>vpn-id</i> は <i>vlan-id</i> と同じです。
ステップ 5	<b>neighbor router-id {encapsulation mpls}</b> 例 : Device(config-vfi)# <b>neighbor remote-router-id encapsulation mpls</b>	リモートピアリングルータ ID と、エミュレート VC をセットアップするために使用されるトンネルカプセル化タイプまたは疑似回線 (PW) プロパティを指定します。
ステップ 6	<b>end</b> 例 : Device(config-vfi)# <b>end</b>	特権 EXEC モードに戻ります。

#### PE デバイスでの VFI への接続回線の関連付け

VFI を定義したら、1 つ以上の接続回線に関連付ける必要があります。

接続回線を VFI に関連付けるには、次の手順を実行します。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :	特権 EXEC モードを有効にします。  パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
	Device> <b>enable</b>	
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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 3	<b>interface vlan <i>vlan-id</i></b> 例： Device(config)# <b>interface vlan 2129</b>	動的なスイッチ仮想インターフェイス (SVI) を作成するか、使用します。  (注) <i>vlan-id</i> は <i>vpn-id</i> と同じです。
ステップ 4	<b>no ip address</b> 例： Device(config-if)# <b>no ip address</b>	IP 処理をディセーブルにします。(IP アドレスを設定する場合は、VLAN のレイヤ 3 インターフェイスを設定できません)。
ステップ 5	<b>xconnect vfi <i>vfi-name</i></b> 例： Device(config-if)# <b>xconnect vfi 2129</b>	VLAP ポートにバインドするレイヤ 2 VFI を指定します。
ステップ 6	<b>end</b> 例： Device(config-if)# <b>end</b>	特権 EXEC モードに戻ります。

## プロトコル CLI モードでの VPLS の設定

次の項では、プロトコル CLI モードでの VPLS の設定について説明します。

### プロトコル CLI モードでの VPLS の設定

プロトコル CLI モードで VPLS を設定するには、次の手順を実行します。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。  パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
ステップ 2	<b>configure terminal</b> 例 :  Device# <b>configure terminal</b>	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 3	<b>l2vpn vfi context vfi-name</b> 例 :  Device(config)# <b>l2vpn vfi context vpls1</b>	レイヤ 2 VPN VFI コンテキストを確立して、レイヤ 2 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 4	<b>vpn id vpn-id</b> 例 :  Device(config-vfi)# <b>vpn id 10</b>	VPLS ドメインの VPN ID を設定します。
ステップ 5	<b>member ip-address encapsulation mpls</b> 例 :  Device(config-vfi)# <b>member 2.2.2.2 encapsulation mpls</b>	ポイントツーポイントレイヤ 2 VPN VFI 接続を形成するデバイスを指定します。
ステップ 6	<b>exit</b> 例 :  Device(config-vfi)# <b>exit</b>	特権 EXEC モードに戻ります。
ステップ 7	次のいずれかを選択します。  • <b>vlan configuration vlan-id</b> • <b>interface vlan vlan-id</b> 例 :  Device(config)# <b>vlan configuration 100</b> OR Device(config)# <b>interface vlan 100</b>	VLAN または インターフェイスに適用する設定を適用し、VLAN または インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	<b>member vfi vfi-name</b> 例 :  Device(config-vlan-config)# <b>member vfi vpls1</b>	VFI インスタンスを VLAN または インターフェイスにバインドします。
ステップ 9	<b>end</b> 例 :  Device(config-vlan-config)# <b>end</b>	特権 EXEC モードに戻ります。

## 疑似回線インターフェイスを使用した VPLS Flow Aware Transport の設定 (プロトコル CLI モード)

疑似回線インターフェイスを使用して VPLS Flow Aware Transport を設定するには、次の手順を実行します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードを有効にします。  パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例：  Device# <b>configure terminal</b>	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 3	<b>interface pseudowire number</b> 例：  Device(config)# <b>interface pseudowire 1001</b>	指定した名前で PW を確立して、疑似回線インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<b>encapsulation mpls</b> 例：  Device(config-if)# <b>encapsulation mpls</b>	トンネリングカプセル化を MPLS として指定します。
ステップ 5	<b>neighbor peer-address vcid-value</b> 例：  Device(config-if)# <b>neighbor 10.1.1.200 200</b>	レイヤ 2 VPN PW のピア IP アドレスと VC ID 値を指定します。
ステップ 6	<b>load-balance flow</b> 例：  Device(config-if)# <b>load-balance flow</b>	ロードバランシングがフロー単位で実行されるように、PW 機能を使用したロードバランシングを有効にします。
ステップ 7	<b>load-balance flow-label</b> 例：  Device(config-if)# <b>load-balance flow-label both</b>	MPLS PW 機能の Flow Aware Transport を有効にして、フローラベルの使用方法を指定します。
ステップ 8	<b>exit</b> 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	Device(config-if)# <b>exit</b>	
ステップ 9	<b>l2vpn vfi context vfi-name</b> 例 : Device(config)# <b>l2vpn vfi context vpls1</b>	レイヤ 2 VPN VFI コンテキストを確立して、レイヤ 2 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 10	<b>vpn id vpn-id</b> 例 : Device(config-vfi)# <b>vpn id 10</b>	VPLS ドメインの VPN ID を設定します。
ステップ 11	<b>member pseudowire number</b> 例 : Device(config-vfi)# <b>member pseudowire 1001</b>	疑似回線インターフェイスを VFI のメンバーとして追加します。
ステップ 12	<b>exit</b> 例 : Device(config-vfi)# <b>exit</b>	特権 EXEC モードに戻ります。
ステップ 13	次のいずれかを選択します。 <ul style="list-style-type: none"><li>• <b>vlan configuration vlan-id</b></li><li>• <b>interface vlan vlan-id</b></li></ul> 例 : Device(config)# <b>vlan configuration 100</b> OR Device(config)# <b>interface vlan 100</b>	VLAN またはインターフェイスに適用する設定を適用し、VLAN または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ます。
ステップ 14	<b>member vfi vfi-name</b> 例 : Device(config-vlan-config)# <b>member vfi vpls1</b>	VFI インスタンスを VLAN またはインターフェイスにバインドします。
ステップ 15	<b>end</b> 例 : Device(config-vlan-config)# <b>end</b>	特権 EXEC モードに戻ります。

## テンプレートを使用した VPLS Flow Aware Transport の設定 (プロトコル CLI モード)

テンプレートを使用して VPLS Flow Aware Transport を設定すると、複数の PW が同じ設定を共有できます。

テンプレートを使用して VPLS Flow Aware Transport を設定するには、次の手順を実行します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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 3	<b>template type pseudowire [template-name]</b> 例： Device(config)# <b>template type pseudowire mpls</b>	レイヤ 2 PW の名前を指定し、擬似回線テンプレートコンフィギュレーションモードを開始します。
ステップ 4	<b>encapsulation mpls</b> 例： Device(config-template)# <b>encapsulation mpls</b>	トンネリングカプセル化を MPLS として指定します。
ステップ 5	<b>load-balance flow</b> 例： Device(config-template)# <b>load-balance flow</b>	ロードバランシングがフロー単位で実行されるように、PW 機能を使用したロードバランシングを有効にします。
ステップ 6	<b>load-balance flow-label</b> 例： Device(config-template)# <b>load-balance flow-label both</b>	MPLS PW 機能の Flow Aware Transport を有効にして、フローラベルの使用方法を指定します。
ステップ 7	<b>exit</b> 例： Device(config-template)# <b>exit</b>	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 8	<b>l2vpn vfi context</b> <i>vfi-name</i> 例 : Device (config) # <b>l2vpn vfi context vpls1</b>	レイヤ 2 VPN VFI コンテキストを確立して、レイヤ 2 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 9	<b>vpn id</b> <i>vpn-id</i> 例 : Device (config-vfi) # <b>vpn id 10</b>	VPLS ドメインの VPN ID を設定します。
ステップ 10	<b>member ip-address template</b> <i>template-name</i> 例 : Device (config-vfi) # <b>member 102.102.102.102 template mpls</b>	ポイントツーポイントレイヤ 2 VPN VFI 接続を形成するデバイスを指定します。 <ul style="list-style-type: none"> <li>• <b>ip-address</b> : VFI ネイバーの IP アドレス。</li> <li>• <b>template-name</b> : テンプレート方式としてテンプレート名 <b>mpls</b> を指定します。 <b>template</b></li> </ul>
ステップ 11	<b>exit</b> 例 : Device (config-vfi) # <b>exit</b>	特権 EXEC モードに戻ります。
ステップ 12	次のいずれかを選択します。 <ul style="list-style-type: none"> <li>• <b>vlan configuration</b> <i>vlan-id</i></li> <li>• <b>interface vlan</b> <i>vlan-id</i></li> </ul> 例 : Device (config) # <b>vlan configuration 100</b> OR Device (config) # <b>interface vlan 100</b>	VLAN またはインターフェイスに適用する設定を適用し、VLAN またはインターフェイス コンフィギュレーション モードを開始します。
ステップ 13	<b>member vfi</b> <i>vfi-name</i> 例 : Device (config-vlan-config) # <b>member vfi vpls1</b>	VFI インスタンスを VLAN またはインターフェイスにバインドします。
ステップ 14	<b>end</b> 例 :	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	Device (config-vlan-config) # <b>end</b>	

### 疑似回線とテンプレートを使用した VPLS Flow Aware Transport の設定 (プロトコル CLI モード)

PW とテンプレートの両方を使用して VPLS Flow Aware Transport を設定するには、次の手順を実行します。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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 3	<b>template type pseudowire [template-name]</b> 例： Device (config) # <b>template type pseudowire mpls</b>	レイヤ 2 PW の名前を指定し、疑似回線テンプレートコンフィギュレーションモードを開始します。
ステップ 4	<b>encapsulation mpls</b> 例： Device (config-template) # <b>encapsulation mpls</b>	トンネリングカプセル化を MPLS として指定します。
ステップ 5	<b>load-balance flow</b> 例： Device (config-template) # <b>load-balance flow</b>	ロードバランシングがフロー単位で行われるように、PW 機能を使用したロードバランシングを有効にします。
ステップ 6	<b>load-balance flow-label</b> 例： Device (config-template) # <b>load-balance flow-label both</b>	MPLS PW 機能の Flow Aware Transport を有効にして、フローラベルの使用方法を指定します。
ステップ 7	<b>exit</b> 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	Device (config-template) # <b>exit</b>	
ステップ 8	<b>interface pseudowire number</b> 例 : Device (config) # <b>interface pseudowire 1001</b>	指定した名前 で PW を確立して、疑似回線 インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	<b>source template type pseudowire [template-name]</b> 例 : Device (config-if) # <b>source template type pseudowire mpls</b>	mpls という名前 のタイプ 疑似回線 のソース テンプレート を設定 します。
ステップ 10	<b>neighbor peer-address vcid-value</b> 例 : Device (config-if) # <b>neighbor 10.1.1.200 200</b>	レイヤ 2 VPN PW のピア IP アドレス と VC ID 値 を指定 します。
ステップ 11	<b>exit</b> 例 : Device (config-if) # <b>exit</b>	特権 EXEC モード に戻ります。
ステップ 12	<b>l2vpn vfi context vfi-name</b> 例 : Device (config) # <b>l2vpn vfi context vpls1</b>	レイヤ 2 VPN VFI コンテキスト を確立して、レイヤ 2 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 13	<b>vpn id vpn-id</b> 例 : Device (config-vfi) # <b>vpn id 10</b>	VPLS ドメイン の VPN ID を設定 します。
ステップ 14	<b>member pseudowire number</b> 例 : Device (config-vfi) # <b>member pseudowire 1001</b>	疑似回線 インターフェイス を VFI のメンバー として追加 します。
ステップ 15	<b>exit</b> 例 : Device (config-vfi) # <b>exit</b>	特権 EXEC モード に戻ります。

	コマンドまたはアクション	目的
ステップ 16	次のいずれかを選択します。 <ul style="list-style-type: none"> <li>• <b>vlan configuration</b> <i>vlan-id</i></li> <li>• <b>interface vlan</b> <i>vlan-id</i></li> </ul> 例：  Device(config)# <b>vlan configuration</b> <b>100</b> OR Device(config)# <b>interface vlan</b> <b>100</b>	VLAN またはインターフェイスに適用する設定を適用し、VLAN または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ます。
ステップ 17	<b>member vfi</b> <i>vfi-name</i> 例：  Device(config-vlan-config)# <b>member vfi</b> <b>vpls1</b>	VFI インスタンスを VLAN またはインターフェイスにバインドします。
ステップ 18	<b>end</b> 例：  Device(config-vlan-config)# <b>end</b>	特権 EXEC モードに戻ります。

## VPLS BGP ベースの自動検出の設定

次の項では、VPLS BGP ベースの自動検出の設定方法について説明します。

### VPLS BGP ベースの自動検出のイネーブル化

VPLS BGP ベースの自動検出を有効にするには、次の手順を実行します。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードを有効にします。  パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  Device# <b>configure terminal</b>	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。

	コマンドまたはアクション	目的
ステップ 3	<b>l2 vfi vfi-name autodiscovery</b> 例 :  Device(config)# <b>l2 vfi 2128 autodiscovery</b>	PE デバイス上で VPLS 自動検出を有効にして、L2 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 4	<b>vpn id vpn-id</b> 例 :  Device(config-vfi)# <b>vpn id 2128</b>	VPLS ドメインの VPN ID を設定します。
ステップ 5	<b>end</b> 例 :  Device(config-vfi)# <b>end</b>	特権 EXEC モードに戻ります。

## VPLS 自動検出を有効にする BGP の設定

VPLS 自動検出を有効にするように BGP を設定するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  Device> <b>enable</b>	特権 EXEC モードを有効にします。  パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例 :  Device# <b>configure terminal</b>	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 3	<b>router bgp autonomous-system-number</b> 例 :  Device(config)# <b>router bgp 1000</b>	指定したルーティングプロセスのルータ コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
ステップ 4	<p><b>no bgp default ipv4-unicast</b></p> <p>例 :</p> <pre>Device(config-router)# no bgp default ipv4-unicast</pre>	<p>BGP ルーティングプロセスで使用される IPv4 ユニキャストアドレスファミリを無効にします。</p> <p>(注) IPv4 ユニキャストアドレスファミリのルーティング情報は、<b>neighbor remote-as router</b> コマンドを使用して設定された各 BGP ルーティングセッションに対して、デフォルトでアドバタイズされます。ただし、<b>neighbor remote-as</b> コマンドを設定する前に、<b>no bgp default ipv4-unicast</b> コマンドを設定した場合は除きます。既存のネイバー コンフィギュレーションは影響されません。</p>
ステップ 5	<p><b>bgp log-neighbor-changes</b></p> <p>例 :</p> <pre>Device(config-router)# bgp log-neighbor-changes</pre>	<p>BGP ネイバー リセットのロギングを有効にします。</p>
ステップ 6	<p><b>neighbor remote-as { ip-address   peer-group-name } remote-as autonomous-system-number</b></p> <p>例 :</p> <pre>Device(config-router)# neighbor 44.254.44.44 remote-as 1000</pre>	<p>指定された自律システム内のネイバーの IP アドレスまたはピア グループ名を、ローカル デバイスの IPv4 マルチプロトコル BGP ネイバー テーブルに追加します。</p> <ul style="list-style-type: none"> <li>• <i>autonomous-system-number</i> 引数が、<b>router bgp</b> コマンドで指定された自律システム番号と一致する場合、ネイバーは内部ネイバーになります。</li> <li>• <i>autonomous-system-number</i> 引数が、<b>router bgp</b> コマンドで指定された自律システム番号と一致しない場合、ネイバーは外部ネイバーになります。</li> </ul>

	コマンドまたはアクション	目的
ステップ 7	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>update-source</b> <i>interface-type</i> <i>interface-number</i> 例 : <pre>Device(config-router)# neighbor 44.254.44.44 update-source Loopback300</pre>	(任意) ルーティングテーブルアップデートを受信するための特定のソースまたはインターフェイスを選択するようにデバイスを設定します。
ステップ 8	他の BGP ネイバーを設定する場合は、ステップ 6 と 7 を繰り返します。	インターフェイス コンフィギュレーション モードを終了します。
ステップ 9	<b>address-family</b> <i>l2vpn</i> [ <i>vpls</i> ] 例 : <pre>Device(config-router)# address-family l2vpn vpls</pre>	レイヤ 2 VPN アドレスファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。  オプションの <b>vpls</b> キーワードは、VPLS エンドポイントプロビジョニング情報が BGP ピアに配布されるように指定します。
ステップ 10	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>activate</b> 例 : <pre>Device(config-router-af)# neighbor 44.254.44.44 activate</pre>	BGP ネイバーとの情報交換を有効にします。
ステップ 11	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>send-community</b> { <b>both</b>   <b>standard</b>   <b>extended</b> } 例 : <pre>Device(config-router-af)# neighbor 44.254.44.44 send-community both</pre>	コミュニティ属性が BGP ネイバーに送信されるように指定します。
ステップ 12	ステップ 10 と 11 を繰り返して、L2VPN アドレスファミリ内の他の BGP ネイバーをアクティブにします。	
ステップ 13	<b>exit-address-family</b> 例 : <pre>Device(config-router-af)#</pre>	アドレス ファミリ コンフィギュレーション モードを終了し、ルータ コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
	<code>exit-address-family</code>	
ステップ 14	<code>end</code> 例 :  Device(config-router)# <code>end</code>	ルータ コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。

## プロトコル CLI モードでの VPLS BGP ベースの自動検出の設定

次の項では、プロトコル CLI モードでの VPLS BGP ベースの自動検出の設定について説明します。

### プロトコル CLI モードでの VPLS BGP ベースの自動検出の設定

プロトコル CLI モードで VPLS BGP ベースの自動検出を設定するには、次の手順を実行します。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code> 例 :  Device> <code>enable</code>	特権 EXEC モードを有効にします。  パスワードを入力します (要求された場合)。
ステップ 2	<code>configure terminal</code> 例 :  Device# <code>configure terminal</code>	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 3	<code>l2vpn vfi context vfi-name</code> 例 :  Device(config)# <code>l2vpn vfi context vpls1</code>	レイヤ 2 VPN VFI コンテキストを確立して、レイヤ 2 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 4	<code>vpn id vpn-id</code> 例 :  Device(config-vfi)# <code>vpn id 10</code>	VPLS ドメインの VPN ID を設定します。
ステップ 5	<code>autodiscovery bgp signaling ldp</code> 例 :	BGP シグナリングと LDP シグナリングを有効にします。

	コマンドまたはアクション	目的
	Device (config-vfi) # <b>autodiscovery bgp signaling ldp</b>	
ステップ 6	<b>exit</b> 例 : Device (config-vfi-autodiscovery) # <b>exit</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>exit</b> 例 : Device (config-vfi) # <b>exit</b>	特権 EXEC モードに戻ります。
ステップ 8	次のいずれかを選択します。 <ul style="list-style-type: none"> <li>• <b>vlan configuration <i>vlan-id</i></b></li> <li>• <b>interface vlan <i>vlan-id</i></b></li> </ul> 例 : Device (config) # <b>vlan configuration 100</b> OR Device (config) # <b>interface vlan 100</b>	VLAN またはインターフェイスに適用する設定を適用し、VLAN またはインターフェイス コンフィギュレーションモードを開始します。
ステップ 9	<b>member vfi <i>vfi-name</i></b> 例 : Device (config-vlan-config) # <b>member vfi vpls1</b>	VFI インスタンスを VLAN またはインターフェイスにバインドします。
ステップ 10	<b>end</b> 例 : Device (config-vlan-config) # <b>end</b>	特権 EXEC モードに戻ります。

テンプレートを使用した VPLS BGP ベースの自動検出 Flow Aware Transport の設定 (プロトコル CLI モード)

テンプレートを使用して VPLS BGP ベースの自動検出 Flow Aware Transport を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
	Device> <b>enable</b>	
ステップ 2	<b>configure terminal</b> 例 :  Device# <b>configure terminal</b>	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 3	<b>template type pseudowire [template-name]</b> 例 :  Device(config)# <b>template type pseudowire mpls</b>	レイヤ 2 PW の名前を指定し、擬似回線テンプレートコンフィギュレーション モードを開始します。
ステップ 4	<b>encapsulation mpls</b> 例 :  Device(config-template)# <b>encapsulation mpls</b>	トンネリングカプセル化を MPLS として指定します。
ステップ 5	<b>load-balance flow</b> 例 :  Device(config-template)# <b>load-balance flow</b>	ロードバランシングがフロー単位で実行されるように、PW 機能を使用した Any Transport over MPLS (AToM) ロードバランシング機能を有効にします。
ステップ 6	<b>load-balance flow-label</b> 例 :  Device(config-template)# <b>load-balance flow-label both</b>	MPLS PW 機能の Flow Aware Transport を有効にして、フローラベルの使用方法を指定します。
ステップ 7	<b>exit</b> 例 :  Device(config-template)# <b>exit</b>	特権 EXEC モードに戻ります。
ステップ 8	<b>l2vpn vfi context vfi-name</b> 例 :  Device(config)# <b>l2vpn vfi context vpls1</b>	レイヤ 2 VPN VFI コンテキストを確立して、レイヤ 2 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 9	<b>vpn id vpn-id</b> 例 :  Device(config-vfi)# <b>vpn id 10</b>	VPLS ドメインの VPN ID を設定します。

	コマンドまたはアクション	目的
ステップ 10	<b>autodiscovery bgp signaling ldp template</b> <i>name</i> 例 : Device (config-vfi) # <b>autodiscovery bgp signaling ldp template mpls</b>	BGP シグナリングと LDP シグナリングを有効にします。
ステップ 11	<b>exit</b> 例 : Device (config-vfi) # <b>exit</b>	特権 EXEC モードに戻ります。
ステップ 12	次のいずれかを選択します。 <ul style="list-style-type: none"> <li>• <b>vlan configuration</b> <i>vlan-id</i></li> <li>• <b>interface vlan</b> <i>vlan-id</i></li> </ul> 例 : Device (config) # <b>vlan configuration 100</b> OR Device (config) # <b>interface vlan 100</b>	VLAN またはインターフェイスに適用する設定を適用し、VLAN またはインターフェイス コンフィギュレーションモードを開始します。
ステップ 13	<b>member vfi</b> <i>vfi-name</i> 例 : Device (config-vlan-config) # <b>member vfi vpls1</b>	VFI インスタンスを VLAN またはインターフェイスにバインドします。
ステップ 14	<b>end</b> 例 : Device (config-vlan-config) # <b>end</b>	特権 EXEC モードに戻ります。

## VPLS および VPLS BGP ベースの自動検出の設定例

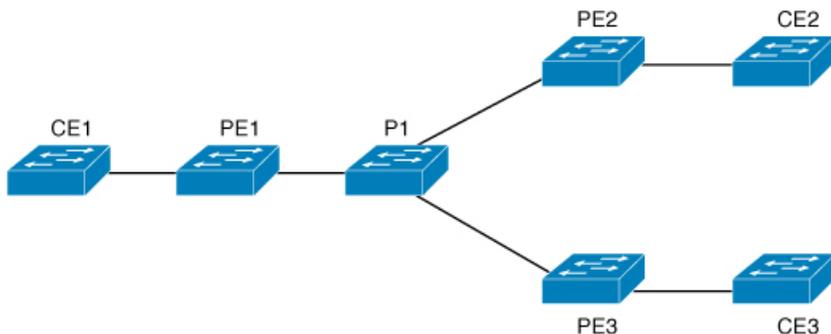
この項では、VPLS および VPLS BGP ベースの自動検出の設定例を示します。

### 例 : Xconnect モードでの VPLS の設定

次に、PE1 および PE2 デバイスで VPLS を設定する例を示します。

例 : Xconnect モードで設定されたVPLSの確認

図 26: VPLS トポロジ



## PE1 の設定

```

Device> enable
Device# configure terminal
Device(config)# pseudowire-class vpls2129
Device(config-if)# encapsulation mpls
Device(config-if)# exit
Device(config)# 12 vfi 2129 manual
Device(config-vfi)# vpn id 2129
Device(config-vfi)# neighbor 44.254.44.44 pw-class vpls2129
Device(config-vfi)# neighbor 188.98.89.98 pw-class vpls2129
Device(config-vfi)# exit
Device(config)# interface TenGigabitEthernet1/0/24
Device(config-if)# switchport trunk allowed vlan 2129
Device(config-if)# switchport mode trunk
Device(config-if)# exit
Device(config)# interface vlan 2129
Device(config-vlan-config)# no ip address
Device(config-vlan-config)# xconnect vfi 2129
    
```

## 例 : Xconnect モードで設定されたVPLSの確認

次に、**show mpls 12transport vc detail** コマンドの出力例を示します。このコマンドの出力には、仮想回線に関する情報が表示されます。

```

Device# show mpls 12transport vc detail
Local interface: VFI 2129 vfi up
Interworking type is Ethernet
Destination address: 44.254.44.44, VC ID: 2129, VC status: up
Output interface: Gi1/0/9, imposed label stack {18 17}
Preferred path: not configured
Default path: active
Next hop: 177.77.177.2
Create time: 19:09:33, last status change time: 09:24:14
Last label FSM state change time: 09:24:14
Signaling protocol: LDP, peer 44.254.44.44:0 up
Targeted Hello: 1.1.1.72 (LDP Id) -> 44.254.44.44, LDP is UP
Graceful restart: configured and enabled
Non stop routing: not configured and not enabled
    
```

```

Status TLV support (local/remote) : enabled/supported
LDP route watch                   : enabled
Label/status state machine        : established, LruRru
Last local dataplane status rcvd: No fault
Last BFD dataplane status rcvd: Not sent
Last BFD peer monitor status rcvd: No fault
Last local AC circuit status rcvd: No fault
Last local AC circuit status sent: No fault
Last local PW i/f circ status rcvd: No fault
Last local LDP TLV status sent: No fault
Last remote LDP TLV status rcvd: No fault
Last remote LDP ADJ status rcvd: No fault
MPLS VC labels: local 512, remote 17
Group ID: local n/a, remote 0
MTU: local 1500, remote 1500
Remote interface description:
Sequencing: receive disabled, send disabled
Control Word: Off
SSO Descriptor: 44.254.44.44/2129, local label: 512
Dataplane:
SSM segment/switch IDs: 20498/20492 (used), PWID: 2
VC statistics:
transit packet totals: receive 0, send 0
transit byte totals: receive 0, send 0
transit packet drops: receive 0, seq error 0, send 0

```

次に、**show l2vpn atom vc** コマンドの出力例を示します。このコマンドの出力には、ATM over MPLS が VC に設定されていることが示されます。

```

Device# show l2vpn atom vc detail

pseudowire100005 is up, VC status is up PW type: Ethernet
Create time: 19:25:56, last status change time: 09:40:37
Last label FSM state change time: 09:40:37
Destination address: 44.254.44.44 VC ID: 2129
Output interface: Gi1/0/9, imposed label stack {18 17}
Preferred path: not configured
Default path: active
Next hop: 177.77.177.2
Member of vfi service 2129
Bridge-Domain id: 2129
Service id: 0x32000003
Signaling protocol: LDP, peer 44.254.44.44:0 up
Targeted Hello: 1.1.1.72(LDP Id) -> 44.254.44.44, LDP is UP
Graceful restart: configured and enabled
Non stop routing: not configured and not enabled
Pwid FEC (128), VC ID: 2129
Status TLV support (local/remote) : enabled/supported
LDP route watch                   : enabled
Label/status state machine        : established, LruRru
Local dataplane status received   : No fault
BFD dataplane status received    : Not sent
BFD peer monitor status received  : No fault
Status received from access circuit : No fault
Status sent to access circuit     : No fault
Status received from pseudowire i/f : No fault
Status sent to network peer       : No fault
Status received from network peer  : No fault
Adjacency status of remote peer   : No fault
Sequencing: receive disabled, send disabled
Bindings

```

例：テンプレートを使用した VPLS Flow Aware Transport の設定 (プロトコル CLI モード)

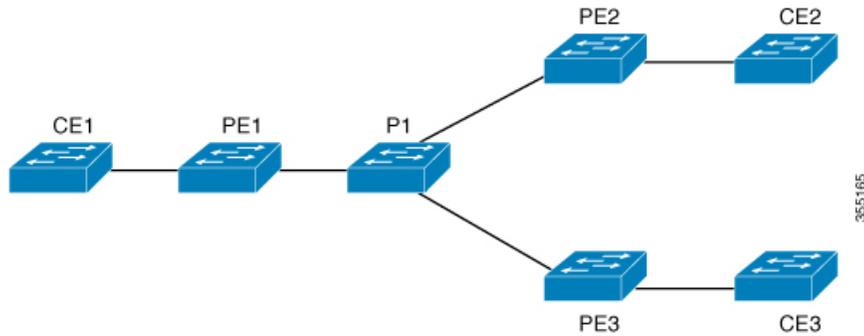
```

Parameter      Local                               Remote
-----
Label          512                                  17
Group ID       n/a                                  0
Interface
MTU            1500                                 1500
Control word   off                                  off
PW type        Ethernet                             Ethernet
VCCV CV type   0x02                                 0x02
                LSPV [2]                             LSPV [2]
VCCV CC type   0x06                                 0x06
                RA [2], TTL [3]                             RA [2], TTL [3]
Status TLV     enabled                               supported
SSO Descriptor: 44.254.44.44/2129, local label: 512
Dataplane:
  SSM segment/switch IDs: 20498/20492 (used), PWID: 2
Rx Counters
  0 input transit packets, 0 bytes
  0 drops, 0 seq err
Tx Counters
  0 output transit packets, 0 bytes
  0 drops
    
```

## 例：テンプレートを使用した VPLS Flow Aware Transport の設定 (プロトコル CLI モード)

次に、PE1 および PE2 デバイスで VPLS を設定する例を示します。

図 27: VPLS トポロジ



**PE1 の設定**

```
Device> enable
Device# configure terminal
Device(config)# template type pseudowire mpls
Device(config-template)# encapsulation mpls
Device(config-template)# load-balance flow ip dst-ip
Device(config-template)# load-balance flow-label both
Device(config-template)# exit
Device(config)# interface Loopback0
Device(config-if)# ip address 1.1.1.30 255.255.255.255
Device(config-if)# ip ospf 1 area 0
Device(config-if)# exit
Device(config)# interface TwentyFiveGigE1/0/9
Device(config-if)# no switchport
Device(config-if)# ip address 80.0.0.30 255.255.255.0
Device(config-if)# ip ospf 1 area 0
Device(config-if)# mpls ip
Device(config-if)# exit
Device(config)# l2vpn vfi context foo
Device(config-vfi)# vpn id 2129
Device(config-vfi)# member 1.1.1.20 template mpls
Device(config-vfi)# exit
Device(config)# interface TwentyFiveGigE1/0/2
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 100
Device(config-if)# exit
Device(config)# interface vlan 100
Device(config-vlan-config)# member vfi foo
Device(config-vlan-config)# end
```

**例 : VPLS BGP 自動検出の設定**

次に、PE デバイスで VPLS を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# router bgp 1000
Device(config-router)# bgp log-neighbor-changes
Device(config-router)# bgp graceful-restart
Device(config-router)# neighbor 44.254.44.44 remote-as 1000
Device(config-router)# neighbor 44.254.44.44 update-source Loopback300
Device(config-router)# address-family l2vpn vpls
Device(config-router-af)# neighbor 44.254.44.44 activate
Device(config-router-af)# neighbor 44.254.44.44 send-community both
Device(config-router-af)# exit-address-family
Device(config-router-af)# end
Device(config)# l2 vfi 2128 autodiscovery
Device(config-vfi)# vpn id 2128
Device(config-vfi)# exit
Device(config)# interface vlan 2128
Device(config-vlan-config)# no ip address
Device(config-vlan-config)# xconnect vfi 2128
!
```

## 例 : VPLS BGP 自動検出の確認

次に、**show platform software fed sw 1 matm macTable vlan 2000** コマンドの出力例を示します。

```
Device# show platform software fed sw 1 matm macTable vlan 2000

VLAN  MAC                Type      Seq#  macHandle          siHandle          diHandle
      *a_time *e_time  ports
2000  2852.6134.05c8      0X8002    0      0xffbba312c8      0xffbb9ef938     0x5154
      0          0      Vlan2000
2000  0000.0078.9012      0X1       32627  0xffbb665ec8      0xffbb60b198     0xffbb653f98
      300      278448  Port-channel11
2000  2852.6134.0000      0X1       32651  0xffba15e1a8      0xff454c2328     0xffbb653f98
      300      63      Port-channel11
2000  0000.0012.3456      0X2000001 32655  0xffba15c508      0xff44f9ec98     0x0
      300      1      2000:33.33.33.33

Total Mac number of addresses:: 4
*a_time=aging_time(secs) *e_time=total_elapsed_time(secs)
Type:
MAT_DYNAMIC_ADDR      0x1      MAT_STATIC_ADDR      0x2
MAT_CPU_ADDR          0x4      MAT_DISCARD_ADDR     0x8
MAT_ALL_VLANS         0x10     MAT_NO_FORWARD        0x20
MAT_IPMULT_ADDR       0x40     MAT_RESYNC            0x80
MAT_DO_NOT_AGE        0x100    MAT_SECURE_ADDR       0x200
MAT_NO_PORT           0x400    MAT_DROP_ADDR         0x800
MAT_DUP_ADDR          0x1000   MAT_NULL_DESTINATION  0x2000
MAT_DOT1X_ADDR        0x4000   MAT_ROUTER_ADDR       0x8000
MAT_WIRELESS_ADDR     0x10000  MAT_SECURE_CFG_ADDR   0x20000
MAT_OPO_DATA_PRESENT  0x40000  MAT_WIRED_TUNNEL_ADDR 0x80000
MAT_DLR_ADDR          0x100000 MAT_MRP_ADDR          0x200000
MAT_MSRR_ADDR         0x400000 MAT_LISP_LOCAL_ADDR   0x800000
MAT_LISP_REMOTE_ADDR  0x1000000 MAT_VPLS_ADDR         0x2000000
```

次に、**show bgp l2vpn vpls all** コマンドの出力例を示します。

```
Device# show bgp l2vpn vpls all

BGP table version is 6, local router ID is 222.5.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
               t secondary path,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 1000:2128
*> 1000:2128:1.1.1.72/96
      0.0.0.0          32768 ?
*>i 1000:2128:44.254.44.44/96
      44.254.44.44          0 100 0 ?
```

## VPLS および VPLS BGP ベースの自動検出の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 13: VPLS および VPLS BGP ベースの自動検出の機能情報

機能名	リリース	機能情報
VPLS および VPLS BGP ベースの自動検出の設定	Cisco IOS XE Everest 16.5.1a	VPLSにより、企業は、サービスプロバイダーから提供されるインフラストラクチャを介して、複数サイトからのイーサネットベースのLANをまとめてリンクできます。  VPLS自動検出を使用すると、各 PE デバイスで、同じ VPLS ドメインの一部である他の PE デバイスを検出できます。
VPLS レイヤ2 スヌーピング : IGMP (IPv4)	Cisco IOS XE Amsterdam 17.1.1	IGMP スヌーピングは、VPLS が設定されたネットワークでサポートされます。
VPLS を介した MLD スヌーピング	Cisco IOS XE Bengaluru 17.6.1	VPLS を介した MLD スヌーピングのサポートが導入されました。これにより、リモートプロバイダーエッジ (PE) デバイスから IGMP/MLD レポートを受信する疑似回線でトラフィックを転送できるようになります。





## 第 19 章

# VPLS の設定 : IPv6 ユニキャスト用のルーテッド擬似回線 IRB

VPLS : IPv6 ユニキャスト用ルーテッド擬似回線 IRB 機能を使用すると、ルータを使用する代わりにスイッチインターフェイスでトラフィックをルーティングできます。

- [VPLS の設定に関する制約事項 : IPv6 ユニキャスト用ルーテッド擬似回線 IRB \(317 ページ\)](#)
- [VPLS に関する情報 : IPv6 ユニキャスト用のルーテッド擬似回線 IRB \(317 ページ\)](#)
- [VPLS の設定 : IPv6 ユニキャスト用のルーテッド擬似回線 IRB \(321 ページ\)](#)
- [設定例 : 分散型 IRB \(322 ページ\)](#)
- [VPLS の設定に関する機能情報 : IPv6 ユニキャスト用のルーテッド擬似回線 IRB \(322 ページ\)](#)

## VPLS の設定に関する制約事項 : IPv6 ユニキャスト用ルーテッド擬似回線 IRB

- この機能は、マルチキャストルーティングプロトコルで設定されたドメインではサポートされません。
- この機能は、IPv6 アドレスファミリではサポートされていません。
- VPLS over GRE は、Integrated Routing and Bridging (IRB) ではサポートされていません。

## VPLS に関する情報 : IPv6 ユニキャスト用のルーテッド擬似回線 IRB

次の項では、VPLS : IPv6 ユニキャスト用ルーテッド擬似回線 IRB について説明します。

## VPLS について : IPv6 ユニキャスト用のルーテッド擬似回線 IRB

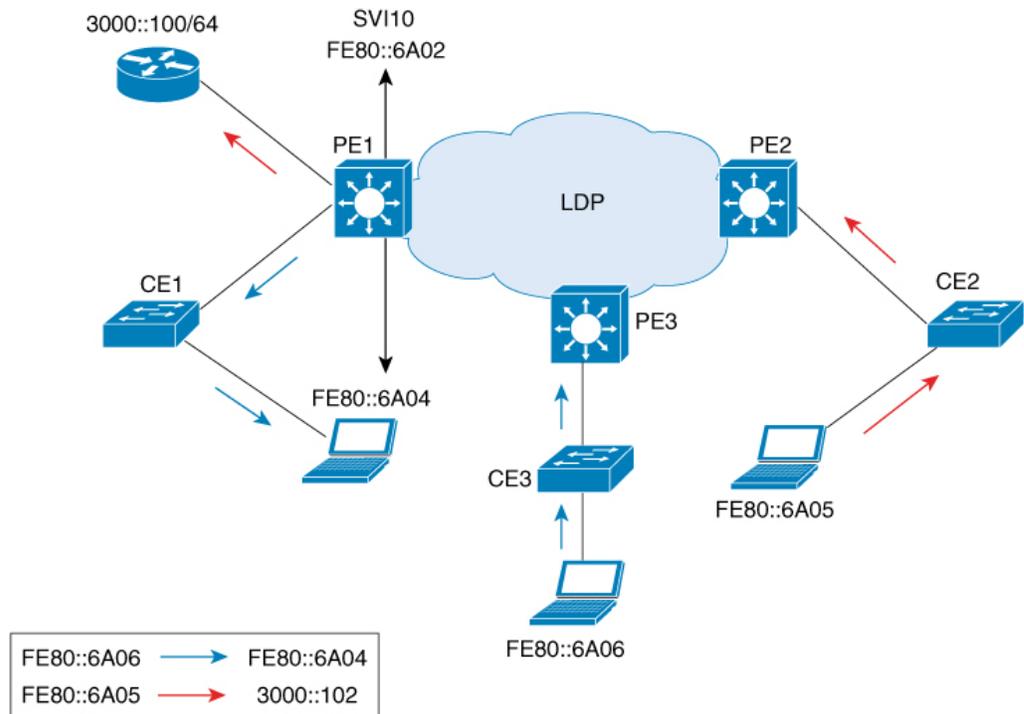
VPLS : IPv6 ユニキャスト用ルーテッド擬似回線 IRB 機能により、仮想プライベート LAN サービス (VPLS) マルチポイント プロバイダー エッジ (PE) デバイス インターフェイスで、PE デバイス間の擬似回線 (PW) 接続用のレイヤ 2 フレームのスイッチとともにレイヤ 3 トラフィックをルーティングできます。インターフェイス間でのフレームのルーティング機能は、同じデバイス上のレイヤ 3 ネットワーク (VPN または グローバル) への PW の終了、またはレイヤ 2 トンネルを介したレイヤ 3 フレームのトンネリング (VPLS) には影響しません。

## 集中型 Integrated Routing and Bridging

集中型 Integrated Routing and Bridging (IRB) では、PE デバイスの 1 つのインターフェイスだけがドメイン内で IRB で設定されます。PE デバイスに接続されているすべてのホストデバイスは、この IRB インターフェイス IP アドレスをゲートウェイとして設定されます。

次の図は、集中型 IRB で設定されたドメインを示しています。図は、IRB が PE デバイス (PE1) インターフェイスで設定されていることを示しています。カスタマーエッジ (CE1) デバイス (CE1、CE2、および CE3) に接続されているすべてのホストは、ゲートウェイとして IRB インターフェイス IPv6 アドレス (FE80::6A02) を使用して設定されます。このシナリオでは、レイヤ 3 ルータ (3000::100/64) 宛ての packets でのみレイヤ 3 packets の書き換えが行われます。これは、これらのインターフェイスまたはルータが PE1 デバイスから到達可能であるためです。すべてのホストは、同じブリッジドメイン (FE80:6A0x) の一部であるため、レイヤ 2 でのみ通信します。

図 28 : 集中型 IRB



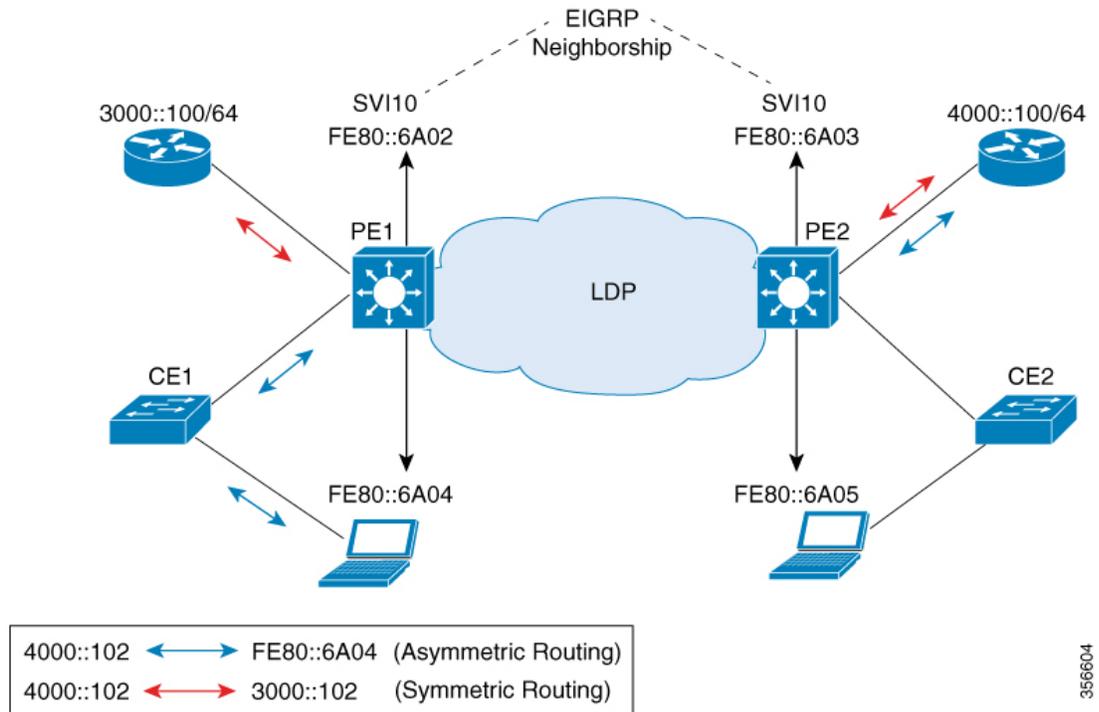
356603

## 分散型 Integrated Routing and Bridging

分散型 IRB では、すべての PE デバイスのすべてのインターフェイスがドメイン内の IRB で設定されます。PE デバイスで有効になっているルーティングプロトコルにより、PE デバイス間でルートを学習できます。

次の図は、分散型 IRB で設定されたドメインを示しています。Enhanced Interior Gateway Routing Protocol (EIGRP) は、ルータ (3000::100/64 および 4000::100/64) がルートを交換できるように、PE デバイス (PE1 および PE2) のインターフェイスに設定されます。CE デバイスに接続されているホストは、ローカル IRB インターフェイスの IP アドレスをゲートウェイとして設定されます。たとえば、ホスト FE80::6A04 は、IRB インターフェイス IPv6 アドレス FE80::6A02 をゲートウェイとして設定され、ホスト FE80::6A05 は IRB インターフェイス IPv6 アドレス FE80::6A03 をゲートウェイとして設定されます。このシナリオでは、着信トラフィックがスイッチ仮想インターフェイス (SVI) を経由する場合、同じブリッジドメイン (FE80::6A0x) 下の IRB インターフェイス間で関係が形成されるため、MPLS ネットワークを介して SVI から発信トラフィックに到達することもできます。

図 29:分散型 IRB



上記の図では、PE2を介して到達可能なルータインターフェイス宛でのトラフィックがPE1に着信する場合、ルーティングはゲートウェイの設定に基づいてPE（つまりPE2）の出力で行われます。このようなシナリオでは、PE2に到達するパケットは、常に、送信元MACをホストMACとして持ち、ゲートウェイMAC（エージングタイム後にエージアウトする）は持ちません。ゲートウェイMACがエージアウトすると、逆方向のトラフィックでフラッディングが発生します。したがって、非対称ルーティングの場合は、VPLSドメイン内のPE間でフラッディングが発生しないように、MACエージングタイムよりも小さいtimer値を使用して、**ipv6 nd cache expire refresh** コマンドと **ipv6 nd cache expire timer refresh** コマンドの両方を設定することを推奨します。

このシナリオ（CE1からトラフィックが着信するシナリオ）では、入力インターフェイスと出力インターフェイスの両方がPE1の転送パイプラインのSVIを指します。これは予期された動作ですが、ICMPリダイレクトメッセージが生成されます。したがって、分散型IRBの場合にICMPリダイレクトメッセージが生成されないように、インターフェイスコンフィギュレーションモードでSVIに **no ip redirects** コマンドを設定することを推奨します。

## VPLSでサポートされる機能 : IPv6ユニキャスト用のルーテッド擬似回線 IRB

VPLSで設定されたインターフェイスでサポートされている機能は次のとおりです。IPv6ユニキャスト機能のルーテッド擬似回線 IRB :

- IPv6 ユニキャスト ルーティング プロトコル
- VPN ルーティングおよび転送 (VRF)
- DHCP リレー
- Address Resolution Protocol (ARP) タイムアウト
- Internet Control Message Protocol (ICMP) リダイレクトメッセージのブロッキング

## VPLS の設定 : IPv6 ユニキャスト用のルーテッド擬似回線 IRB

VPLS : IPv6 ユニキャスト機能用ルーテッド擬似回線 IRB を設定するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例 : Device# <b>configure terminal</b>	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 3	<b>interface vlan <i>vlan-id</i></b> 例 : Device(config)# <b>interface vlan 100</b>	VLAN インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<b>xconnect vfi <i>vfi-name</i></b> 例 : Device(config-if)# <b>xconnect vfi VFI100</b>	VLAP ポートにバインドするレイヤ 2 VFI を指定します。
ステップ 5	<b>ipv6 address <i>ip-address</i></b> 例 : Device(config-if)# <b>ipv6 address 4000::100/64</b>	インターフェイスに IPv6 アドレスを割り当てます。

## 設定例 : 分散型 IRB

次に、分散型 IRB を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# template type pseudowire VPLS
Device(config-template)# encapsulation mpls
Device(config-template)# l2vpn vfi context VPLS
Device(config-template)# vpn id 10
Device(config-template)# member pseudowire1
Device(config-if)# end

Device(config)# interface pseudowire1
Device(config-if)# source template type pseudowire VPLS
Device(config-if)# encapsulation mpls
Device(config-if)# signaling protocol ldp
Device(config-if)# neighbor 3000::102
Device(config-if)# end

Device(config)# interface Vlan10
Device(config-if)# ipv6 address 4000::100/64
Device(config-if)# no ip redirects
Device(config-if)# member vfi VPLS
Device(config-if)# end
```

## VPLS の設定に関する機能情報 : IPv6 ユニキャスト用のルーテッド擬似回線 IRB

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能名	機能情報
Cisco IOS XE Amsterdam 17.3.x	VPLS : IPv6 ユニキャスト用ルーテッド擬似回線 IRB	VPLS : IPv6 ユニキャスト用ルーテッド擬似回線 IRB 機能を使用すると、ルータを使用する代わりにスイッチインターフェイスでトラフィックをルーティングできます。  この機能のサポートは、Cisco Catalyst 9300 シリーズスイッチの 9300 スイッチモデルでのみ導入されました。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。





## 第 20 章

# MPLS VPN ルート ターゲット書き換えの設定

- [MPLS VPN ルート ターゲット書き換えの前提条件 \(325 ページ\)](#)
- [MPLS VPN ルート ターゲット書き換えの制約事項 \(325 ページ\)](#)
- [MPLS VPN ルート ターゲット書き換えに関する情報 \(325 ページ\)](#)
- [MPLS VPN ルート ターゲット書き換えの設定方法 \(327 ページ\)](#)
- [MPLS VPN ルート ターゲット書き換えの設定例 \(335 ページ\)](#)
- [MPLS VPN ルートターゲット書き換えの機能履歴 \(335 ページ\)](#)

## MPLS VPN ルート ターゲット書き換えの前提条件

- マルチプロトコル ラベル スイッチング (MPLS) バーチャルプライベート ネットワーク (VPN) の設定方法を知っている必要があります。
- 自律システム (AS) 向けに RT 置換ポリシーおよびターゲット デバイスを識別する必要があります。

## MPLS VPN ルート ターゲット書き換えの制約事項

ルート ターゲットの書き換えは、単一 AS トポロジにのみ実装できます。

`ip unnumbered` コマンドは MPLS 設定ではサポートされていません。

## MPLS VPN ルート ターゲット書き換えに関する情報

この項では、MPLS VPN ルートターゲット書き換えについて説明します。

## ルート ターゲット置換ポリシー

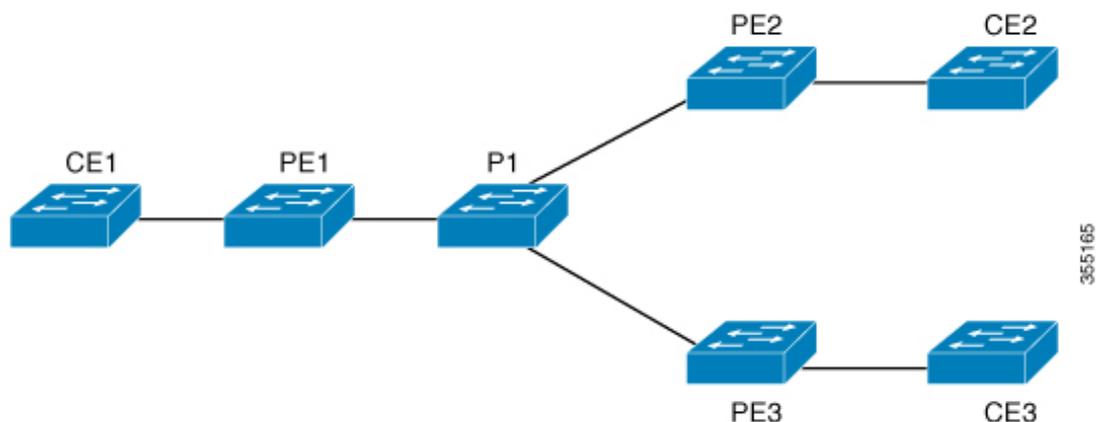
ピアのルーティング ポリシーには、インバウンドまたはアウトバウンドのルーティング テーブルアップデートに影響する可能性のある設定がすべて含まれています。インバウンドおよびアウトバウンドの Border Gateway Protocol (BGP) アップデートに対してルート ターゲットの置換を有効にすると、MPLS VPN ルート ターゲット書き換え機能がルーティング テーブルアップデートに影響する可能性があります。BGP バーチャルプライベート ネットワーク IP バージョン4 (VPNv4) のアップデートでは、ルートターゲットが拡張コミュニティ属性として送信されます。ルートターゲット拡張コミュニティ属性を使用して、一連のサイト、および設定されたルート ターゲットを使用するルートを受信できる VPN ルーティングおよび転送 (VRF) インスタンスが識別されます。

MPLS VPN ルート ターゲットの書き換え機能は、プロバイダー エッジ (PE) デバイスで設定できます。

次の図に、マルチプロトコル ラベル スイッチング (MPLS) VPN の単一自律システム トポロジ内の PE デバイスでルート ターゲットを置換する例を示します。この例には、次の設定が含まれています。

- PE1 は、VRF カスタマー A の RT 65000:1 をインポートおよびエクスポートして、RT 65000:1 のすべてのインバウンド VPNv4 プレフィックスを RT 65000:2 に書き換えるように設定されています。
- PE2 は、VRF カスタマー B の RT 65000:2 をインポートおよびエクスポートして、RT 65000:2 のすべてのインバウンド VPNv4 プレフィックスを RT 65000:1 に書き換えるように設定されています。

図 30: 単一の MPLS VPN 自律システム トポロジのプロバイダー エッジ (PE) デバイスでのルート ターゲットの置換



## ルート マップおよびルート ターゲットの置換

MPLS VPN ルート ターゲット書き換え機能によって Border Gateway Protocol (BGP) インバウンド/アウトバウンドルートマップ機能が拡張され、ルートターゲットの置換がイネーブルになります。ルートマップ コンフィギュレーション モードで入力した `set extcomm-list delete` コ

マンドを使用すると、拡張コミュニティリストに基づいてルートターゲット拡張コミュニティ属性を削除できます。

## MPLS VPN ルート ターゲット書き換えの設定方法

次の項では、MPLS VPN ルートターゲット書き換えの設定手順について説明します。

### ルート ターゲット置換ポリシーの設定

インターネットワークにルート ターゲット (RT) 置換ポリシーを設定するには、次の作業を実行します。

RT  $x$  を RT  $y$  に書き換えるようにプロバイダー エッジ (PE) を設定したとき、その PE に RT  $x$  をインポートする仮想ルーティングおよび転送 (VRF) インスタンスが設定されている場合は、RT  $x$  に加えて RT  $y$  をインポートする VRF も設定する必要があります。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> enable	特権 EXEC モードを有効にします。  • パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例：  Device# configure terminal	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 3	<b>ip extcommunity-list</b> { <i>standard-list-number</i>   <i>expanded-list-number</i> } { <b>permit</b>   <b>deny</b> } [ <i>regular-expression</i> ] [ <b>rt</b>   <b>soo</b> <i>extended-community-value</i> ] 例：  Device(config)# ip extcommunity-list 1 permit rt 65000:2	拡張コミュニティ アクセス リストを作成し、リストへのアクセスを制御します。  • <i>standard-list-number</i> 引数は 1 ~ 99 の整数で、拡張コミュニティの 1 つまたは複数の許可グループまたは拒否グループを指定します。  • <i>expanded-list-number</i> 引数は 100 ~ 500 の整数で、拡張コミュニティの 1 つまたは複数の許可グループまたは拒否グループを指定します。拡張リストには正規表現を設定できませんが、標準リストには設定できません。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>permit</b> キーワードを指定すると、条件が一致した場合にアクセスが許可されます。</li> <li>• <b>deny</b> キーワードを指定すると、条件が一致した場合にアクセスが拒否されます。</li> <li>• <i>regular-expression</i> 引数には、マッチングを行う入カストリングパターンを指定します。拡張された拡張コミュニティリストを使用してルートターゲットのマッチングを行う場合は、正規表現にパターン RT: を追加します。</li> <li>• <b>rt</b> キーワードには、ルートターゲット拡張コミュニティ属性を指定します。<b>rt</b> キーワードは標準拡張コミュニティリストにのみ設定できます。拡張された拡張コミュニティリストには設定できません。</li> <li>• <b>soo</b> キーワードには、Site of Origin (SOO) 拡張コミュニティ属性を指定します。<b>soo</b> キーワードは標準拡張コミュニティリストだけに設定できます。拡張された拡張コミュニティリストには設定できません。</li> <li>• <i>extended-community-value</i> 引数には、ルートターゲットまたは Site of Origin を指定します。この値には次の組み合わせのいずれかを指定できます。 <ul style="list-style-type: none"> <li>• <code>autonomous-system-number:network-number</code></li> <li>• <code>ip-address:network-number</code></li> </ul> </li> </ul> <p>自律システム番号とネットワーク番号、または IP アドレスとネットワーク番号の区切りにはコロンを使用します。</p>
ステップ 4	<b>route-map</b> <i>map-name</i> [ <b>permit</b>   <b>deny</b> ] [ <i>sequence-number</i> ] 例 :	ルーティング プロトコル間でルートを再配布する条件を定義するか、ポリシールーティングをイネーブルにしてルート

	コマンドまたはアクション	目的
	<pre>Device(config)# route-map rtrewrite permit 10</pre>	<p>マップ コンフィギュレーション モードを開始します。</p> <ul style="list-style-type: none"> <li>• <i>map-name</i> 引数では、ルートマップに意味のある名前を定義します。 <b>redistribute</b> ルータ コンフィギュレーション コマンドはこの名前を使用して、このルートマップを参照します。複数のルート マップで同じマップ名を共有できます。</li> <li>• このルートマップの一致基準が満たされた場合、<b>permit</b> キーワードが指定されていると、設定アクションに従ってルートが再配布されます。ポリシー ルーティングの場合、パケットはポリシーに従ってルーティングされます。</li> </ul> <p>一致基準が満たされなかった場合、<b>permit</b> キーワードが指定されていると、同じマップタグを持つ次のルートマップがテストされます。あるルートが、同じ名前を共有するルート マップセットの一致基準のいずれをも満たさない場合、そのセットによる再配布は行われません。</p> <p>デフォルトは <b>permit</b> キーワードです。</p> <ul style="list-style-type: none"> <li>• ルートマップの一致基準が満たされた場合でも、<b>deny</b> キーワードが指定されているとルートは再配布されません。ポリシー ルーティングの場合、パケットはポリシーに従ってルーティングされません。また、同じマップ タグ名を共有するルート マップは、これ以上検証されません。パケットがポリシー ルーティングの対象にならない場合、通常の転送アルゴリズムが使用されます。</li> <li>• <i>sequence-number</i> 引数は、同じ名前を設定済みのルートマップのリストにおける新しいルートマップの位置を示す番号です。このコマンドの</li> </ul>

	コマンドまたはアクション	目的
		<b>no</b> 形式を指定すると、ルートマップの位置が削除されます。
ステップ 5	<b>match extcommunity</b> { <i>standard-list-number</i>   <i>expanded-list-number</i> } 例 : <pre>Device(config-route-map)# match extcommunity 1</pre> 例 : <pre>Device(config-route-map)# match extcommunity 101</pre>	Border Gateway Protocol (BGP) 拡張コミュニティ リスト属性とマッチングします。 <ul style="list-style-type: none"> <li>• <i>standard-list-number</i> 引数は 1 ~ 99 の番号で、拡張コミュニティ属性の 1 つまたは複数の許可グループまたは拒否グループを指定します。</li> <li>• <i>expanded-list-number</i> 引数は 100 ~ 500 の番号で、拡張コミュニティ属性の 1 つまたは複数の許可グループまたは拒否グループを指定します。</li> </ul>
ステップ 6	<b>set extcomm-list</b> <i>extended-community-list-number delete</i> 例 : <pre>Device(config-route-map)# set extcomm-list 1 delete</pre>	インバウンドまたはアウトバウンド BGP バーチャルプライベート ネットワークバージョン 4 (VPNv4) アップデートの拡張コミュニティ属性からルートターゲットを削除します。 <ul style="list-style-type: none"> <li>• <i>extended-community-list-number</i> 引数には、拡張コミュニティ リスト番号を指定します。</li> </ul>
ステップ 7	<b>set extcommunity</b> { <b>rt</b> <i>extended-community-value</i> [ <b>additive</b> ]   <b>soo</b> <i>extended-community-value</i> } 例 : <pre>Device(config-route-map)# set extcommunity rt 65000:1 additive</pre>	BGP 拡張コミュニティ属性を設定します。 <ul style="list-style-type: none"> <li>• <b>rt</b> キーワードには、ルートターゲット拡張コミュニティ属性を指定します。</li> <li>• <b>soo</b> キーワードには、Site of Origin 拡張コミュニティ属性を指定します。</li> <li>• <i>extended-community-value</i> 引数には、設定値を指定します。この値には次の組み合わせのいずれかを指定できます。               <ul style="list-style-type: none"> <li>• <i>autonomous-system-number</i><i>network-number</i></li> <li>• <i>ip-address:network-number</i></li> </ul> </li> </ul>

	コマンドまたはアクション	目的
		自律システム番号とネットワーク番号、または IP アドレスとネットワーク番号の区切りにはコロンを使用します。 <ul style="list-style-type: none"> <li>• <b>additive</b> キーワードを指定すると、既存のルートターゲットを置換することなく、既存のルートターゲットリストにルートターゲットが追加されます。</li> </ul>
ステップ 8	<b>end</b> 例 : Device(config-route-map)# end	(任意) 特権 EXEC モードに戻ります。
ステップ 9	<b>show route-map map-name</b> 例 : Device# show route-map extmap	(任意) マッチングと設定されたエントリが正しいことを確認します。 <ul style="list-style-type: none"> <li>• <i>map-name</i> 引数には、特定のルートマップの名前を指定します。</li> </ul>

## ルート ターゲット置換ポリシーの適用

ネットワークにルート ターゲット置換ポリシーを適用するには、次の作業を実行します。

### 特定の BGP ネイバーへのルート マップの割り当て

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>configure terminal</b> 例 : Device# configure terminal	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 3	<b>router bgp as-number</b> 例 : Device(config)# router bgp 100	Border Gateway Protocol (BGP) ルーティングプロセスを設定し、デバイスでルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <i>as-number</i> 引数は、デバイスを他の BGP デバイスに対して識別し、転送するルーティング情報にタグを設定する自律システムの番号を示します。</li> </ul> <p>指定できる範囲は0～65535です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512～65535です。</p>
ステップ 4	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>  例 :  <pre>Device(config-router)# neighbor 172.10.0.2 remote-as 200</pre>	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。 <ul style="list-style-type: none"> <li>• <i>ip-address</i> 引数には、ネイバーの IP アドレスを指定します。</li> <li>• <i>peer-group-name</i> 引数には、BGP ピア グループの名前を指定します。</li> <li>• <i>as-number</i> 引数には、ネイバーが属している自律システムを指定します。</li> </ul>
ステップ 5	<b>address-family</b> <i>vpn4</i> [ <b>unicast</b> ]  例 :  <pre>Device(config-router)# address-family vpn4</pre>	アドレス ファミリ コンフィギュレーションモードを開始して、標準バージョン 4 (VPNv4) アドレスプレフィックスを使用する、BGP などのルーティングセッションを設定します。 <ul style="list-style-type: none"> <li>• <b>unicast</b> キーワード (任意) は、VPNv4 ユニキャストアドレスプレフィックスを指定します。</li> </ul>
ステップ 6	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>activate</b>  例 :  <pre>Device(config-router-af)# neighbor 172.16.0.2 activate</pre>	ネイバー BGP デバイスとの情報交換を有効にします。 <ul style="list-style-type: none"> <li>• <i>ip-address</i> 引数には、ネイバーの IP アドレスを指定します。</li> <li>• <i>peer-group-name</i> 引数には、BGP ピア グループの名前を指定します。</li> </ul>

	コマンドまたはアクション	目的
ステップ 7	<p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>}  <b>send-community</b> [<b>both</b>   <b>extended</b>   <b>standard</b>]</p> <p>例 :</p> <pre>Device(config-router-af)# neighbor 172.16.0.2 send-community extended</pre>	<p>コミュニティ属性が BGP ネイバーに送信されるように指定します。</p> <ul style="list-style-type: none"> <li>• <i>ip-address</i> 引数には、BGP 対応ネイバーの IP アドレスを指定します。</li> <li>• <i>peer-group-name</i> 引数には、BGP ピア グループの名前を指定します。</li> <li>• <b>both</b> キーワードを指定すると、標準および拡張コミュニティ属性が送信されます。</li> <li>• <b>extended</b> キーワードを指定すると、拡張コミュニティ属性が送信されます。</li> <li>• <b>standard</b> キーワードを指定すると、標準コミュニティ属性が送信されます。</li> </ul>
ステップ 8	<p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>}  <b>route-map</b> <i>map-name</i> {<b>in</b>   <b>out</b>}</p> <p>例 :</p> <pre>Device(config-router-af)# neighbor 172.16.0.2 route-map extmap in</pre>	<p>着信ルートまたは発信ルートにルートマップを適用します。</p> <ul style="list-style-type: none"> <li>• <i>ip-address</i> 引数には、ネイバーの IP アドレスを指定します。</li> <li>• <i>peer-group-name</i> 引数には、BGP ピア グループまたはマルチプロトコルピア グループの名前を指定します。</li> <li>• <i>map-name</i> 引数には、ルートマップの名前を指定します。</li> <li>• <b>in</b> キーワードを指定すると、着信ルートにルートマップが適用されます。</li> <li>• <b>out</b> キーワードを指定すると、発信ルートにルートマップが適用されます。</li> </ul>
ステップ 9	<p><b>end</b></p> <p>例 :</p> <pre>Device(config-router-af)# end</pre>	<p>(任意) 特権 EXEC モードに戻ります。</p>

## ルートターゲット置換ポリシーの確認

### 手順

---

#### ステップ1 enable

特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。

例：

```
Device> enable
Device#
```

#### ステップ2 show ip bgp vpnv4 vrf vrf-name

指定したルートターゲット（RT）拡張コミュニティ属性を持つバーチャルプライベートネットワークバージョン4（VPNv4）が適切な RT 拡張コミュニティ属性で置換されることを確認して、プロバイダーエッジ（PE）デバイスが書き換えられた RT 拡張コミュニティ属性を受け取ることを確認します。

PE1 でルートターゲットの置換を確認するには、次のコマンドを入力します。

例：

```
Device# show ip bgp vpnv4 vrf Customer_A 192.168.1.1/32 internal
BGP routing table entry for 65000:1:192.168.1.1/32, version 6901
Paths: (1 available, best #1, table Customer_A)
  Advertised to update-groups:
    5
  Refresh Epoch 1
  650002
    3.3.3.3 (metric 3) (via default) from 3.3.3.3 (55.5.4.1)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:65000:1
      mpls labels in/out nolabel/3025
      rx pathid: 0, tx pathid: 0x0
      net: 0xFFB0A72E38, path: 0xFFB0E6A370, pathext: 0xFFB0E5D970
      flags: net: 0x0, path: 0x7, pathext: 0x181
```

#### ステップ3 exit

ユーザー EXEC モードに戻ります。

例：

```
Device# exit
Device>
```

---

# MPLS VPN ルート ターゲット書き換えの設定例

次の項では、MPLS VPN ルートターゲット書き換えの設定例について説明します。

## 例：ルート ターゲット置換ポリシーの適用

### 例：特定の BGP ネイバーへのルート マップの割り当て

次に、Border Gateway Protocol (BGP) ネイバーにルート マップ `extmap` を関連付ける例を示します。BGP インバウンドルートマップは、着信アップデートのルートターゲット (RT) を置換するように設定されています。

```
router bgp 1
address-family vpnv4
neighbor 2.2.2.2 route-map rtrewrite in
```

次に、アウトバウンド BGP ネイバーに同じルートマップを関連付ける例を示します。このルートマップは、発信アップデートの RT を置換するように設定されています。

```
router bgp 1
address-family vpnv4
neighbor 2.2.2.2 route-map rtrewrite out
```

# MPLS VPN ルートターゲット書き換えの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.6.1	MPLS VPN ルート ターゲット書き換え	インバウンドおよびアウトバウンドの Border Gateway Protocol (BGP) アップデートに対してルートターゲットの置換を有効にすると、MPLS VPN ルートターゲット書き換え機能がルーティングテーブルアップデートに影響する可能性があります。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。





## 第 21 章

# MPLS VPN-Inter-AS-IPv4 BGP ラベル配布の設定

- [MPLS VPN Inter-AS IPv4 BGP ラベル配布 \(337 ページ\)](#)
- [MPLS VPN Inter-AS IPv4 BGP ラベル配布 \(338 ページ\)](#)
- [MPLS VPN Inter-AS IPv4 BGP ラベル配布に関する情報 \(338 ページ\)](#)
- [MPLS VPN Inter-AS IPv4 BGP ラベル配布の設定方法 \(340 ページ\)](#)
- [ルートマップの作成 \(348 ページ\)](#)
- [MPLS VPN Inter-AS IPv4 BGP ラベル配布の設定の確認 \(354 ページ\)](#)
- [MPLS VPN Inter-AS IPv4 BGP ラベル配布の設定例 \(360 ページ\)](#)
- [MPLS VPN Inter-AS IPv4 BGP ラベル配布の設定の機能履歴 \(376 ページ\)](#)

## MPLS VPN Inter-AS IPv4 BGP ラベル配布

この機能を使用すると、バーチャルプライベートネットワーク (VPN) サービスプロバイダーネットワークを設定できます。このネットワークでは、自律システム境界ルータ (ASBR) が、プロバイダーエッジ (PE) ルータのマルチプロトコル ラベル スイッチング (MPLS) ラベル付きの IPv4 ルートを交換します。ルートリフレクタ (RR) は、マルチホップ、マルチプロトコル外部ボーダーゲートウェイプロトコル (EBGP) を使用して VPNv4 ルートを交換します。この設定では、ASBR にすべての VPNv4 ルートを格納する必要がなくなります。ルートリフレクタを使用して VPNv4 ルートを格納し、PE ルータに転送すると、拡張性が向上します。

MPLS VPN—Inter-AS—IPv4 BGP ラベル配布機能には、次の利点があります。

- ルートリフレクタを使用して VPNv4 ルートを格納すると拡張性が向上する：この設定は、ASBR がすべての VPNv4 ルートを保持し、VPNv4 ラベルに基づいてルートを転送する設定よりも拡張性が優れています。この設定では、ルートリフレクタが VPNv4 ルートを保持することで、ネットワーク境界での設定が簡素化されます。
- 非 VPN コアネットワークが VPN トラフィックの中継ネットワークとして機能できる：非 MPLS VPN サービスプロバイダーを介して、MPLS ラベル付きの IPv4 ルートを転送できます。

- 隣接 LSR 間の他のラベル配布プロトコルが不要になる：隣接する 2 つのラベルスイッチルータ (LSR) が BGP ピアでもある場合、BGP で MPLS ラベルの配布を実行できます。これら 2 つの LSR 間で、他のラベル配布プロトコルは必要ありません。
- 自律システム (AS) の境界を越えた IPv4 ルートのロードバランシングを可能にする EBGP マルチパスのサポートが含まれています。

## MPLS VPN Inter-AS IPv4 BGP ラベル配布

この機能には、次の制約事項があります。

- EBGP マルチホップが設定されたネットワークでは、非隣接デバイス間にラベルスイッチパス (LSP) を設定する必要があります (RFC 3107)。
- PE デバイスでは、BGP ラベル配布をサポートするイメージを実行する必要があります。実行できない場合は、PE デバイス間で EBGP を実行できません。
- ASBR 上の Point-to-Point Protocol (PPP) カプセル化は、この機能ではサポートされていません。
- BGP スピーカーを接続する物理インターフェイスは、Cisco Express Forwarding (CEF) または分散型 CEF と MPLS をサポートしている必要があります。

## MPLS VPN Inter-AS IPv4 BGP ラベル配布に関する情報

MPLS VPN Inter-AS IPv4 BGP ラベル配布を設定するには、次の情報が必要です。

### MPLS VPN Inter-AS IPv4 BGP ラベル配布の概要

この機能を使用すると、VPN サービス プロバイダー ネットワークを設定して、MPLS ラベル付き IPv4 ルートを交換できます。次のように VPN サービス プロバイダー ネットワークを設定できます。

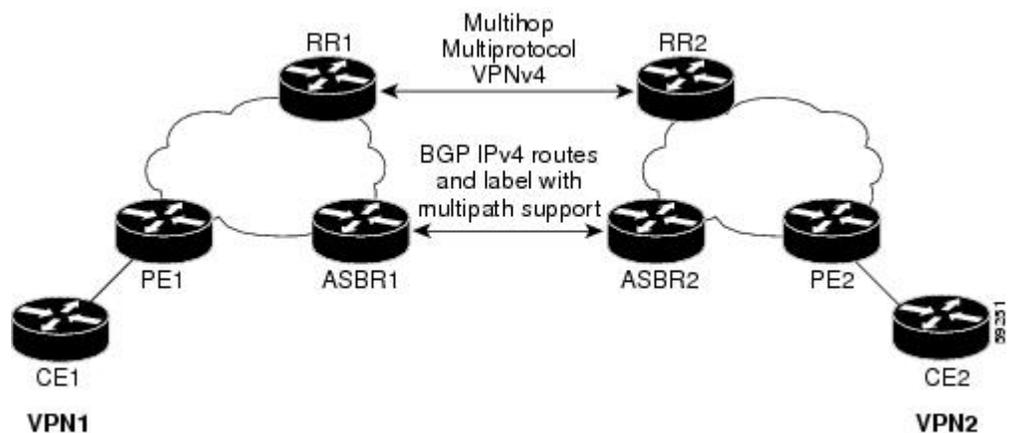
- ルートリフレクタは、マルチホップ、マルチプロトコル EBGP を使用して VPNv4 ルートを交換します。この設定では、自律システムをまたがってネクストホップ情報および VPN ラベルが維持されます。
- ローカル PE ルータ (図 1 の PE1 など) は、リモート PE ルータ (PE2) のルートおよびラベル情報を認識する必要があります。この情報は、次のいずれかの方法で PE ルータおよび ASBR 間で交換できます。
  - 内部ゲートウェイ プロトコル (IGP) と Label Distribution Protocol (LDP; ラベル配布プロトコル) : ASBR は、EBGP から学習した IPv4 ルートおよび MPLS ラベルを IGP や LDP に再配布できます。その逆も可能です。

- 内部ボーダー ゲートウェイ プロトコル (IBGP) IPv4 ラベル配布 : ASBR および PE ルータは、直接 IBGP セッションを使用して、VPNv4 と IPv4 ルートおよび MPLS ラベルを交換できます。

または、ルート リフレクタが、ASBR から学習した IPv4 ルートおよび MPLS ラベルを VPN の PE ルータに反映できます。これは、ASBR が IPv4 ルートおよび MPLS ラベルをルートリフレクタと交換できるようにすることで実現されます。ルートリフレクタは、VPNv4 ルートも VPN の PE ルータに反映します (最初の箇条書き項目を参照)。たとえば、VPN1 では、RR1 は、学習した VPNv4 ルート、および ASBR1 から学習した IPv4 ルートと MPLS ラベルを PE1 に反映します。ルートリフレクタを使用して VPNv4 ルートを格納し、それらのルートを PE ルータおよび ASBR 経由で転送することで、スケーラブルな構成が可能になります。

- ASBR は、EBGP を使用して PE ルータの IPv4 ルートと MPLS ラベルを交換します。これにより、CSC 境界全体のロードバランシングが可能になります。

図 31 : EBGP および IBGP を使用してルートと MPLS ラベルを配布する VPN



## BGP ルーティング情報

BGP ルーティング情報には、次の項目が含まれています。

- 宛先の IP アドレスであるネットワーク番号 (プレフィックス)。
- 自律システム (AS) パス : ルートがローカルルータに到達するために通過する他の AS のリスト。リスト内の最初の自律システムがローカルルータに最も近いシステムです。リスト内の最後の自律システムはローカルルータから最も遠いシステムであり、通常は、ルートの始点となる自律システムです。
- ネクスト ホップなどの、自律システム パスについての他の情報を提供するパス属性。

## BGP においてルートとともに MPLS ラベルが送信される方法

BGP (EBGP および IBGP) でルートを配布する場合、そのルートにマッピングされている MPLS ラベルも配布できます。ルートの MPLS ラベルマッピング情報は、そのルートに関する情報を含む BGP 更新メッセージによって伝送されます。ネクストホップが変わらない場合は、ラベルも維持されます。

両方の BGP ルータで **neighbor send-label** コマンドを発行すると、ルートとともに MPLS ラベルを送信できることがルータ間で相互にアドバタイズされます。ルータ間で MPLS ラベルを送信可能であると正常にネゴシエーションされると、それらのルータからのすべての発信 BGP アップデートに MPLS ラベルが追加されます。

## ルートマップを使用したルートのフィルタリング

両方のルータが MPLS ラベルを使用してルートを配布するように設定されている場合、すべてのルートがマルチプロトコル拡張を使用して符号化され、すべてのルートに MPLS ラベルが付いています。ルートマップを使用して、ルータ間の MPLS ラベルの配布を制御できます。ルートマップで指定できるルートは次のとおりです。

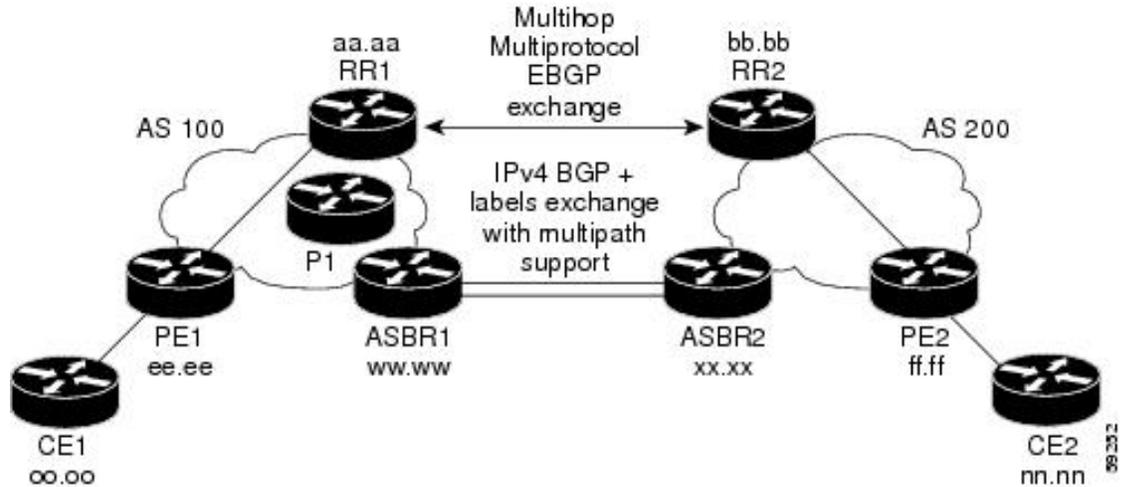
- MPLS ラベルを配布するルータの場合、MPLS ラベルを使用して配布するルートを指定できます。
- MPLS ラベルを受信するルータの場合、受け入れるルートおよび BGP テーブルにインストールするルートを指定できます。

## MPLS VPN Inter-AS IPv4 BGP ラベル配布の設定方法

以下の図は、次の設定を示しています。

- この設定は、2つの VPN で構成されています。
- ASBR は、MPLS ラベル付きの IPv4 ルートを交換します。
- ルートリフレクタは、マルチホップ MPLS EBGP を使用して VPNv4 ルートを交換します。
- ルートリフレクタは、その自律システム内の他のルータに IPv4 ルートおよび VPN4 ルートを反映します。

図 32: IPv4 ルートおよび MPLS ラベルを交換する 2つの VPN サービス プロバイダーの設定



## IPv4 ルートおよび MPLS ラベルを交換する ASBR の設定

次のタスクを実行して、ASBR を設定し、MPLS ラベル付きの BGP ルートを配布できるようにします。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"><li>パスワードを入力します (要求された場合)。</li></ul>
ステップ 2	<b>configure terminal</b> 例 : Device# configure terminal	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 3	<b>router bgp as-number</b> 例 : Device(config)# router bgp 100	ルータ コンフィギュレーションモードを開始します。 <ul style="list-style-type: none"><li><b>as-number</b> : 他の BGP ルータに対するルータを指定し、同時に渡されるルーティング情報のタギングをする自律システムの番号。有効値の範囲は 1 ~ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ~ 65535 です。</li></ul>

	コマンドまたはアクション	目的
ステップ 4	<p><b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i></p> <p>例 :</p> <pre>Device(config)# neighbor 209.165.201.2 remote-as 200</pre>	<p>BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。</p> <ul style="list-style-type: none"> <li>• <i>ip-address</i> 引数には、ネイバーの IP アドレスを指定します。</li> <li>• <i>peer-group-name</i> 引数には、BGP ピアグループの名前を指定します。</li> <li>• <i>as-number</i> 引数には、ネイバーが属している自律システムを指定します。</li> </ul>
ステップ 5	<p><b>address-family ipv4</b> [ <b>multicast</b>   <b>unicast</b>   <b>vrf</b> <i>vrf-name</i> ]</p> <p>例 :</p> <pre>Device(config-router)# address-family ipv4</pre>	<p>標準 IPv4 アドレス プレフィックスを使用する BGP などのルーティングセッションを設定するために、アドレスファミリ コンフィギュレーションモードを開始します。</p> <ul style="list-style-type: none"> <li>• <b>multicast</b> キーワードでは、IPv4 マルチキャストアドレスプレフィックスを指定します。</li> <li>• <b>unicast</b> キーワードでは、IPv4 ユニキャストアドレスプレフィックスを指定します。</li> <li>• <b>vrf</b> <i>vrf-name</i> キーワードおよび引数では、後続の IPv4 アドレスファミリ コンフィギュレーションモードコマンドに関連付ける VPN ルーティングおよび転送 (VRF) インスタンスの名前を指定します。</li> </ul>
ステップ 6	<p><b>maximum-paths</b> <i>number-paths</i></p> <p>例 :</p> <pre>Device(config-router)# maximum-paths 2</pre>	<p>(任意) IP ルーティングプロトコルがサポートできる並列ルートの最大数を制御します。</p> <p><i>number-paths</i> 引数には、IP ルーティングプロトコルがルーティングテーブルにインストールするパラレルルートの最大数を 1 ~ 6 の範囲で指定します。</p>
ステップ 7	<p><b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>activate</b></p> <p>例 :</p>	<p>ネイバールータとの情報交換をイネーブルにします。</p>

	コマンドまたはアクション	目的
	Device (config-router-af) # neighbor 209.165.201.2 activate	<ul style="list-style-type: none"> <li>• ip-address 引数には、ネイバーの IP アドレスを指定します。</li> <li>• peer-group-name 引数には、BGP ピアグループの名前を指定します。</li> </ul>
ステップ 8	<b>neighbor ip-address send-label</b> 例： Device (config-router-af) # neighbor 10.0.0.1 send-label	BGP ルートとともに MPLS ラベルをネイバー BGP ルータに送信できるように BGP ルータを設定します。 <ul style="list-style-type: none"> <li>• ip-address 引数には、ネイバー ルータの IP アドレスを指定します。</li> </ul>
ステップ 9	<b>exit-address-family</b> 例： Device (config-router-af) # exit-address-family	アドレスファミリサブモードを終了します。
ステップ 10	<b>end</b> 例： Device (config-router-af) # end	(任意) 終了して、特権 EXEC モードに戻ります。

## VPNv4 ルートを交換するルータリフレクタの設定

### 始める前に

ルータリフレクタでマルチホップ、マルチプロトコル EBGp を使用して VPNv4 ルートを交換できるようにするには、次の手順を実行します。

また、この手順では、自律システム間でネクストホップ情報および VPN ラベルが維持されるように指定します。この手順では、例として RR1 を使用します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>configure terminal</b> 例： Device# configure terminal	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。

	コマンドまたはアクション	目的
ステップ 3	<b>router bgp <i>as-number</i></b> 例 : Device(config)# router bgp 100	ルータ コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> <li>• <b>as-number</b> : 他の BGP ルータに対するルータを指定し、同時に渡されるルーティング情報のタギングをする自律システムの番号。有効値の範囲は 1 ~ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ~ 65535 です。</li> </ul> 自律システム番号によって、他の自律システム内のルータで RR1 が特定されます。
ステップ 4	<b>neighbor {<i>ip-address</i>   <i>peer-group-name</i>} remote-as <i>as-number</i></b> 例 : Device(config)# neighbor 192.0.2.1 remote-as 200	BGP ネイバーテーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。 <ul style="list-style-type: none"> <li>• <b>ip-address</b> 引数には、ネイバーの IP アドレスを指定します。</li> <li>• <b>peer-group-name</b> 引数には、BGP ピアグループの名前を指定します。</li> <li>• <b>as-number</b> 引数には、ネイバーが属している自律システムを指定します。</li> </ul>
ステップ 5	<b>address-family vpnv4 [unicast]</b> 例 : Device(config-router)# address-family vpnv4	アドレス ファミリ コンフィギュレーションモードを開始して、標準仮想プライベートネットワークバージョン 4 (VPNv4) アドレスプレフィックスを使用する、BGP などのルーティングセッションを設定します。 <ul style="list-style-type: none"> <li>• <b>unicast</b> キーワード (任意) は、VPNv4 ユニキャストアドレスプレフィックスを指定します。</li> </ul>
ステップ 6	<b>neighbor {<i>ip-address</i>   <i>peer-group-name</i>} ebgp-multihop [<i>tth</i>]</b> 例 : Device(config-router-af)# neighbor 192.0.2.1 ebgp-multihop 255	直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <i>ip-address</i> 引数には、BGP 対応ネイバーの IP アドレスを指定します。</li> <li>• <i>peer-group-name</i> 引数には、BGP ピアグループの名前を指定します。</li> <li>• <i>ttl</i> 引数には、1 ~ 255 ホップの範囲の存続可能時間を指定します。</li> </ul>
ステップ 7	<b>neighbor {ip-address peer-group-name} activate</b> 例 : <pre>Device(config-router-af)# neighbor 192.0.2.1 activate</pre>	ネイバールータとの情報交換をイネーブルにします。 <ul style="list-style-type: none"> <li>• <i>ip-address</i> 引数には、ネイバーの IP アドレスを指定します。</li> <li>• <i>peer-group-name</i> 引数には、BGP ピアグループの名前を指定します。</li> </ul>
ステップ 8	<b>neighbor {ip-address peer-group-name} next-hop unchanged</b> 例 : <pre>Device(config-router-af)# neighbor 10.0.0.2 next-hop unchanged</pre>	外部 BGP (EBGP) マルチホップピアで、ネクストホップを変更せずに伝播できるようにします。 <ul style="list-style-type: none"> <li>• <i>ip-address</i> 引数には、ネクストホップの IP アドレスを指定します。</li> <li>• <i>peer-group-name</i> 引数には、ネクストホップである BGP ピアグループの名前を指定します。</li> </ul>
ステップ 9	<b>exit-address-family</b> 例 : <pre>Device(config-router-af)# exit-address-family</pre>	アドレスファミリサブモードを終了します。
ステップ 10	<b>end</b> 例 : <pre>Device(config-router-af)# end</pre>	(任意) 終了して、特権 EXEC モードに戻ります。

## 自律システム内でリモートルートを反映するルートルフレクタの設定

RR が ASBR から学習した IPv4 ルートおよびラベルを自律システム内の PE ルータに反映できるようにするには、次の手順を実行します。

これは、ASBR および PE ルータを RR のルートルリフレクタ クライアントにすることによって実現されます。また、この手順では、RR で VPNv4 ルートを反映できるようにする方法についても説明します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b> 例： Device# configure terminal	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 3	<b>router bgp as-number</b> 例： Device(config)# router bgp 100	ルータ コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> <li><b>as-number</b>：他の BGP ルータに対するルータを指定し、同時に渡されるルーティング情報のタギングをする自律システムの番号。有効値の範囲は 1 ～ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ～ 65535 です。</li> </ul> 自律システム番号によって、他の自律システム内のルータで RR1 が特定されます。
ステップ 4	<b>address-family ipv4</b> <b>[multicast   unicast   vrfvrf-name ]</b> 例： Device(config-router)# address-family ipv4	標準 IPv4 アドレス プレフィックスを使用する BGP などのルーティングセッションを設定するために、アドレスファミリ コンフィギュレーションモードを開始します。 <ul style="list-style-type: none"> <li><b>multicast</b> キーワードでは、IPv4 マルチキャストアドレスプレフィックスを指定します。</li> <li><b>unicast</b> キーワードでは、IPv4 ユニキャストアドレスプレフィックスを指定します。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>vrf vrf-name キーワードおよび引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VPN ルーティングおよび転送 (VRF) インスタンスの名前を指定します。</li> </ul>
ステップ 5	<b>neighbor {ip-address   peer-group-name} activate</b>  例 : <pre>Device(config-router-af)# neighbor 203.0.113.1 activate</pre>	ネイバルータとの情報交換をイネーブルにします。 <ul style="list-style-type: none"> <li>ip-address 引数には、ネイバーの IP アドレスを指定します。</li> <li>peer-group-name 引数には、BGP ピアグループの名前を指定します。</li> </ul>
ステップ 6	<b>neighbor ip-address route-reflector-client</b>  例 : <pre>Device(config-router-af)# neighbor 203.0.113.1 route-reflector-client</pre>	ルータを BGP ルートルフレクタとして設定し、指定したネイバーをそのクライアントとして設定します。 <ul style="list-style-type: none"> <li>ip-address 引数には、クライアントとして識別される BGP ネイバーの IP アドレスを指定します。</li> </ul>
ステップ 7	<b>neighbor ip-address send-label</b>  例 : <pre>Device(config-router-af)# neighbor 203.0.113.1 send-label</pre>	BGP ルートとともに MPLS ラベルをネイバー BGP ルータに送信できるように BGP ルータを設定します。 <ul style="list-style-type: none"> <li>ip-address 引数には、ネイバルータの IP アドレスを指定します。</li> </ul>
ステップ 8	<b>exit-address-family</b>  例 : <pre>Device(config-router-af)# exit-address-family</pre>	アドレスファミリサブモードを終了します。
ステップ 9	<b>address-family vpnv4 [unicast]</b>  例 : <pre>Device(config-router)# address-family vpnv4</pre>	アドレスファミリ コンフィギュレーションモードを開始して、標準 VPNv4 アドレスプレフィックスを使用する、BGP などのルーティングセッションを設定します。 <ul style="list-style-type: none"> <li>unicast キーワード (任意) は、VPNv4 ユニキャストアドレスプレフィックスを指定します。</li> </ul>

	コマンドまたはアクション	目的
ステップ 10	<b>neighbor {ip-address peer-group-name} activate</b>  例： Device(config-router-af)# neighbor 203.0.113.1 activate	ネイバルータとの情報交換をイネーブルにします。  <ul style="list-style-type: none"> <li>• <i>ip-address</i> 引数には、ネイバーの IP アドレスを指定します。</li> <li>• <i>peer-group-name</i> 引数には、BGP ピアグループの名前を指定します。</li> </ul>
ステップ 11	<b>neighbor ip-address route-reflector-client</b>  例： Device(config-router-af)# neighbor 203.0.113.1 route-reflector-client	RR がネイバルータに IBGP ルートを渡せるようにします。
ステップ 12	<b>exit-address-family</b>  例： Device(config-router-af)# exit-address-family	アドレスファミリサブモードを終了します。
ステップ 13	<b>end</b>  例： Device(config-router-af)# end	(任意) 終了して、特権 EXEC モードに戻ります。

## ルートマップの作成

ルートマップを使用すると、MPLS ラベルを使用して配布するルートを指定できます。また、ルータが受信し、BGP テーブルに追加する MPLS ラベル付きのルートを指定することもできます。

ルートマップはアクセスリストと連動します。ルートをアクセスリストに入力し、ルートマップを設定するときにアクセスリストを指定します。

次の手順を実行すると、ASBR 使用して、ルートマップで指定されているルートとともに MPLS ラベルを送信できます。また、ASBR はルートマップで指定されたルートのみを受け入れません。

## 着信ルート用のルートマップの設定

着信ルートをフィルタリングするルートマップを作成するには、次の作業を実行します。アクセスリストを作成し、ルータで受け入れて BGP テーブルに追加させるルートを指定します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b> 例 : Device# configure terminal	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 3	<b>router bgp as-number</b> 例 : Device(config)# router bgp 100	ルータ コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> <li><b>as-number</b> : 他の BGP ルータに対するルータを指定し、同時に渡されるルーティング情報のタグgingをする自律システムの番号。有効値の範囲は 1 ~ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ~ 65535 です。</li> </ul> 自律システム番号によって、他の自律システム内のルータで RR1 が特定されます。
ステップ 4	<b>route-map route-map name [permit   deny] [sequence-number]</b> 例 : Device(config-router)# route-map IN permit 11	指定した名前で作成します。 <ul style="list-style-type: none"> <li><b>permit</b> キーワードを指定すると、すべての条件が満たされた場合にアクションが実行されます。</li> <li><b>deny</b> キーワードを指定すると、すべての条件が満たされた場合にアクションが実行されません。</li> <li><b>sequence-number</b> 引数を指定すると、ルートマップに優先順位付けできます。複数のルートマップが存在し、それらにプライオリティを設定する場合、それぞれに番号を割り当てます。最初に最も低い番号のルートマップが実装され、次に2番めに低</li> </ul>

	コマンドまたはアクション	目的
		い番号のルートマップが実装され、それ以降も同様です。
ステップ 5	<b>match ip address</b> <code>{access-list-number   access-list-name}</code> <code>[...access-list-number   ...access-list-name]</code> 例： <pre>Device(config-route-map)# match ip address 2</pre>	標準アクセスリストまたは拡張アクセスリストで許可された宛先ネットワーク番号アドレスを含むすべてのルートを配するか、またはパケットに対してポリシールーティングを実行します。 <ul style="list-style-type: none"> <li>• <code>access-list-number</code> 引数は、標準アクセスリストまたは拡張アクセスリストの番号です。1～199の整数を指定できます。</li> <li>• <code>access-list-name</code> 引数は、標準アクセスリストまたは拡張アクセスリストの名前です。1～199の整数を指定できます。</li> </ul>
ステップ 6	<b>match mpls-label</b> 例： <pre>Device(config-route-map)# match mpls-label</pre>	ルートがルートマップで指定された条件を満たす場合、MPLS ラベルを含むルートが再配布されます。
ステップ 7	<b>end</b> 例： <pre>Device(config-router-af)# end</pre>	(任意) 終了して、特権 EXEC モードに戻ります。

## 発信ルート用のルートマップの設定

発信ルートをフィルタリングするルートマップを作成するには、次の作業を実行します。アクセスリストを作成し、MPLS ラベルを使用してルータに配布させるルートを指定します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： <pre>Device&gt; enable</pre>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b> 例：	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。

	コマンドまたはアクション	目的
	Device# configure terminal	
ステップ 3	<b>router bgp <i>as-number</i></b> 例 : Device(config)# router bgp 100	ルータ コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> <li>• <b>as-number</b> : 他の BGP ルータに対するルータを指定し、同時に渡されるルーティング情報のタギングをする自律システムの番号。有効値の範囲は 1 ~ 65535 です。内部ネットワークで使用できるプライベート自律システム番号の範囲は、64512 ~ 65535 です。</li> <li>AS 番号によって、他の自律システム内のルータへの RR1 が特定されます。</li> </ul>
ステップ 4	<b>route-map <i>route-map name</i></b> <b>[<i>permit</i>   <i>deny</i>] [<i>sequence-number</i>]</b> 例 : Device(config-router)# route-map OUT permit 10	指定した名前でもルートマップを作成します。 <ul style="list-style-type: none"> <li>• <b>permit</b> キーワードを指定すると、すべての条件が満たされた場合にアクションが実行されます。</li> <li>• <b>deny</b> キーワードを指定すると、すべての条件が満たされた場合にアクションが実行されません。</li> <li>• <b>sequence-number</b> 引数を指定すると、ルートマップに優先順位付けできます。複数のルートマップが存在し、それらにプライオリティを設定する場合、それぞれに番号を割り当てます。最初に最も低い番号のルートマップが実装され、次に2番めに低い番号のルートマップが実装され、それ以降も同様です。</li> </ul>
ステップ 5	<b>match ip address</b> <b>{<i>access-list-number</i>   <i>access-list-name</i>}</b> <b>[...<i>access-list-number</i>   ...<i>access-list-name</i>]</b> 例 : Device(config-route-map)# match 10.0.0.2 1	標準アクセスリストまたは拡張アクセスリストで許可された宛先ネットワーク番号アドレスを含むすべてのルートを配するか、またはパケットに対してポリシールーティングを実行します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <code>access-list-number</code> 引数は、標準アクセスリストまたは拡張アクセスリストの番号です。1～199の整数を指定できます。</li> <li>• <code>access-list-name</code> 引数は、標準アクセスリストまたは拡張アクセスリストの名前です。1～199の整数を指定できます。</li> </ul>
ステップ 6	<b>set mpls-label</b> 例： <pre>Device(config-route-map)# set mpls-label</pre>	ルートがルートマップで指定された条件を満たす場合、MPLS ラベルを使用してルートを配布できるようにします。
ステップ 7	<b>end</b> 例： <pre>Device(config-router-af)# end</pre>	(任意) 終了して、特権 EXEC モードに戻ります。

## ASBR へのルートマップの適用

ASBR でルートマップを使用できるようにするには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： <pre>Device&gt; enable</pre>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>configure terminal</b> 例： <pre>Device# configure terminal</pre>	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 3	<b>router bgp as-number</b> 例： <pre>Device(config)# router bgp 100</pre>	ルータ コンフィギュレーション モードを開始します。 <ul style="list-style-type: none"> <li>• <code>as-number</code> : 他の BGP ルータに対するルータを指定し、同時に渡されるルーティング情報のタギングをする自律システムの番号。有効値の範囲は1～65535です。内部ネットワー</li> </ul>

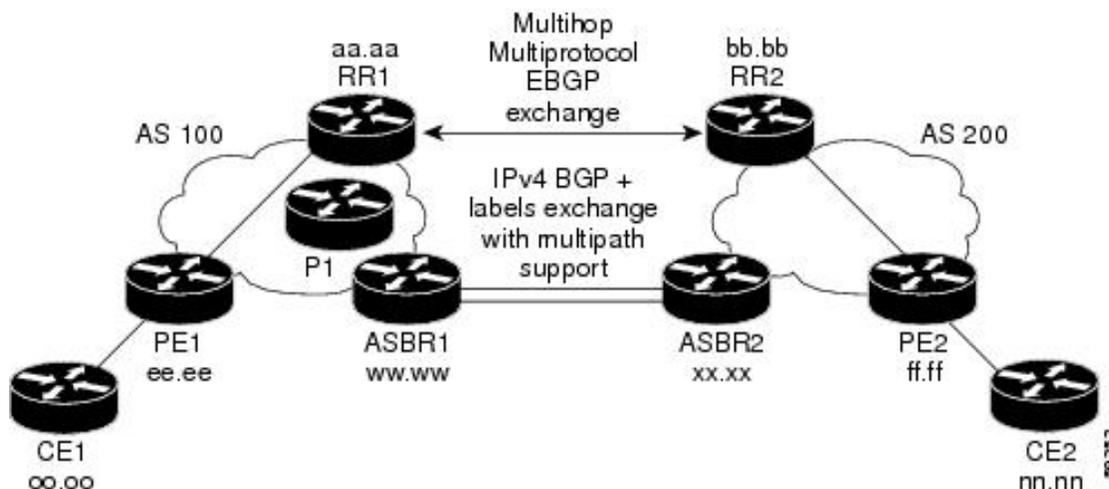
	コマンドまたはアクション	目的
		<p>クで使用できるプライベート自律システム番号の範囲は、64512 ~ 65535 です。</p> <p>自律システム番号によって、他の自律システム内のルータで RR1 が特定されます。</p>
ステップ 4	<p><b>address-family ipv4</b> [ <b>multicast</b>   <b>unicast</b>   <b>vrf vrf-name</b> ]</p> <p>例 :</p> <pre>Device(config-router)# address-family ipv4</pre>	<p>標準 IPv4 アドレス プレフィックスを使用する BGP などのルーティングセッションを設定するために、アドレスファミリー コンフィギュレーション モードを開始します。</p> <ul style="list-style-type: none"> <li>• <b>multicast</b> キーワードでは、IPv4 マルチキャスト アドレス プレフィックスを指定します。</li> <li>• <b>unicast</b> キーワードでは、IPv4 ユニキャスト アドレス プレフィックスを指定します。</li> <li>• <b>vrf vrf-name</b> キーワードおよび引数では、後続の IPv4 アドレス ファミリ コンフィギュレーション モード コマンドに関連付ける VPN ルーティングおよび転送 (VRF) インスタンスの名前を指定します。</li> </ul>
ステップ 5	<p><b>neighbor ip-address route-map route-map-name out</b></p> <p>例 :</p> <pre>Device(config-router-af)# neighbor 209.165.200.225 route-map OUT out</pre>	<p>着信ルートにルートマップを適用します。</p> <ul style="list-style-type: none"> <li>• <b>ip-address</b> 引数では、ルートマップを適用するルート指定します。</li> <li>• <b>route-map-name</b> 引数では、ルートマップの名前を指定します。</li> <li>• <b>out</b> キーワードでは、発信ルートにルートマップを適用します。</li> </ul>
ステップ 6	<p><b>neighbor ip-address send-label</b></p> <p>例 :</p> <pre>Device(config-router-af)# neighbor 209.165.200.225 send-label</pre>	<p>ルートとともに MPLS ラベルを送信するルータの機能をアドバタイズします。</p> <ul style="list-style-type: none"> <li>• <b>ip-address</b> 引数では、ルートとともに MPLS ラベルを送信できるルータを指定します。</li> </ul>

	コマンドまたはアクション	目的
ステップ 7	<b>exit-address-family</b> 例： Device(config-router-af) # exit-address-family	アドレスファミリーサブモードを終了します。
ステップ 8	<b>end</b> 例： Device(config-router-af) # end	(任意) 終了して、特権 EXEC モードに戻ります。

## MPLS VPN Inter-AS IPv4 BGP ラベル配布の設定の確認

設定については、次の図を参照してください。

図 33: IPv4 ルートおよび MPLS ラベルを交換する 2 つの VPN サービス プロバイダーの設定



ルートリフレクタを使用して VPNv4 ルートを配布し、ASBR を使用して IPv4 ラベルを配布する場合は、次の手順に従って設定を確認します。

### ルートリフレクタ設定の確認

ルートリフレクタ設定を確認するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	Device> enable	<ul style="list-style-type: none"> <li>パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>show ip bgp vpnv4 {all   rd route-distinguisher   vrf vrf-name} [summary] [labels]</b> 例： Device# show ip bgp vpnv4 all summary 例： Device# show ip bgp vpnv4 all labels	（任意）BGP テーブルからの VPN アドレス情報を表示します。 <ul style="list-style-type: none"> <li>ルータリフレクタ間にマルチホップ、マルチプロトコル、EBGP セッションが存在し、ルータリフレクタ間で VPNv4 ルートが交換されていることを確認するには、all キーワードと summary キーワードを指定して、<b>show ip bgp vpnv4</b> コマンドを使用します。</li> <li>コマンド出力の最後の 2 行に、次の情報が表示されます。               <ul style="list-style-type: none"> <li>プレフィックスが PE1 から学習されて RR2 に渡されていること。</li> <li>プレフィックスが RR2 から学習されて PE1 に渡されていること。</li> </ul> </li> <li>ルータリフレクタ間で VPNv4 ラベル情報が交換されていることを確認するには、all キーワードと labels キーワードを指定して、<b>show ip bgp vpnv4</b> コマンドを使用します。</li> </ul>
ステップ 3	<b>disable</b> 例： Device# disable	（任意）終了して、ユーザー EXEC モードに戻ります。

## CE1 に CE2 のネットワーク到達可能性情報があることの確認

ルータ CE1 がルータ CE2 の NLRI を持っていることを確認するには、次の作業を実行します。

## PE1 に CE2 のネットワーク層到達可能性情報があることの確認

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>show ip route</b> [ip-address [mask] [longer prefixes]]   [protocol [process-id]]   [list access-list-number   access-list-name] 例： Device# show ip route 209.165.201.1	ルーティング テーブルの現在の状態を表示します。  • ip-address 引数を指定して <b>show ip route</b> コマンドを使用して、CE1 に CE2 へのルートが含まれていることを確認します。  • <b>show ip route</b> コマンドを使用して、CE1 が学習したルートを確認します。CE2 へのルートがリストされていることを確認します。
ステップ 3	<b>disable</b> 例： Device# disable	(任意) 終了して、ユーザー EXEC モードに戻ります。

## PE1 に CE2 のネットワーク層到達可能性情報があることの確認

ルータ PE1 がルータ CE2 の NLRI を持っていることを確認するには、次の作業を実行します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>show ip route vrf</b> vrf-name [connected] [protocols [as-number] [tag] [output-modifiers]] [list number [output-modifiers]] [profile] [static [output-modifiers]] [summary [output-modifiers]] [supernets-only [output-modifiers]] [traffic engineering [output-modifiers]]	(任意) VRF に関連付けられている IP ルーティングテーブルを表示します。  • <b>show ip route vrf</b> コマンドを使用して、ルータ PE1 がルータ CE2 (nn.nn.nn.nn) からルートを学習していることを確認します。

	コマンドまたはアクション	目的
	例 : <pre>Device# show ip route vrf vpn1 209.165.201.1</pre>	
ステップ 3	<b>show ip bgp vpnv4</b> { <b>all</b>   <b>rd</b> <i>route-distinguisher</i>   <b>vrf</b> <i>vrf-name</i> } <i>{ip-prefix/length</i> <b>[longer-prefixes]</b> <i>[output-modifiers]</i> ] <i>[network-address</i> <b>[mask]</b> <b>[longer-prefixes]</b> <i>[output-modifiers]</i> ] <b>[cidr-only]</b> <i>[community]</i> <b>[community-list]</b> <b>[dampened-paths]</b> <b>[filter-list]</b> <b>[flap-statistics]</b> <b>[inconsistent-as]</b> <b>[neighbors]</b> <b>[path</b> <i>[line]</i> <b>]</b> <b>[peer-group]</b> <b>[quote-regexp]</b> <b>[regexp]</b> <b>[summary]</b> <b>[tags]</b>	(任意) BGP テーブルからの VPN アドレス情報を表示します。  <ul style="list-style-type: none"> <li>ルータ PE2 がルータ CE2 の BGP ネクストホップであることを確認するには、<b>vrf</b> または <b>all</b> キーワード指定して <b>show ip bgp vpnv4</b> コマンドを使用します。</li> </ul>
ステップ 4	<b>show ip cef</b> [ <b>vrf</b> <i>vrf-name</i> ] <i>[network</i> <i>[mask]</i> ] <b>[longer-prefixes]</b> <b>[detail]</b>	(任意) 転送情報ベース (FIB) のエントリを表示するか、または FIB のサマリーを表示します。  <ul style="list-style-type: none"> <li><b>show ip cef</b> コマンドを使用して、Cisco Express Forwarding (CEF) エントリが正しいことを確認します。</li> </ul>
ステップ 5	<b>show mpls forwarding-table</b> [ <i>{network</i> <i>{mask length}</i>   <b>labels</b> <i>label</i> [- <i>label</i> ]   <b>interface</b> <i>interface</i>   <b>next-hop</b> <i>address</i>   <b>lsp-tunnel</b> <i>[tunnel-id]</i> }] <b>[detail]</b>	(任意) MPLS 転送情報ベース (LFIB) の内容を表示します。  <ul style="list-style-type: none"> <li><b>show mpls forwarding-table</b> コマンドを使用して、BGP ネクストホップルータ (自律システム境界) の IGP ラベルを確認します。</li> </ul>
ステップ 6	<b>show ip bgp</b> <i>[network]</i> <i>[network-mask]</i> <b>[longer-prefixes]</b>	(任意) BGP ルーティング テーブルのエントリを表示します。  <ul style="list-style-type: none"> <li><b>show ip bgp</b> コマンドを使用して、リモート出力 PE ルータ (PE2) のラベルを確認します。</li> </ul>
ステップ 7	<b>show ip bgp vpnv4</b> { <b>all</b>   <b>rd</b> <i>route-distinguisher</i>   <b>vrf</b> <i>vrf-name</i> } <b>[summary]</b> <b>[labels]</b>	(任意) BGP テーブルからの VPN アドレス情報を表示します。

## PE2にCE2のネットワーク到達可能性情報があることの確認

	コマンドまたはアクション	目的
	例： Device# show ip bgp vpnv4 all labels	<ul style="list-style-type: none"> <li>PE2 からアドバタイズされた CE2 の VPN ラベルを確認するには、<b>show ip bgp vpnv4 all summary</b> コマンドを使用します。</li> </ul>
ステップ 8	<b>disable</b> 例： Device# disable	(任意) 終了して、ユーザー EXEC モードに戻ります。

## PE2にCE2のネットワーク到達可能性情報があることの確認

PE2 が CE2 にアクセスできることを確認するには、次の作業を実行します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>show ip route vrf vrf-name [connected] [protocol [as-number] [tag] [output-modifiers] ] [list number [output-modifiers] ] [profile [static [output-modifiers] ] [summary [output-modifiers] ] [supernets-only [output-modifiers] ] [traffic-engineering [output-modifiers] ] ]</b> 例： Device# show ip route vrf vpn1 209.165.201.1	(任意) VRF に関連付けられている IP ルーティングテーブルを表示します。 <ul style="list-style-type: none"> <li>CE2 の VPN ルーティングおよび転送テーブルを確認するには、<b>show ip route vrf</b> コマンドを使用します。出力にはネクストホップ情報が表示されます。</li> </ul>
ステップ 3	<b>show mpls forwarding-table [vrf vpn-name] [ {network {mask   length }   labels label [-label]   interface interface   next-hop address   lsp-tunnel [tunnel-id] } ] [detail]</b> 例： Device# show mpls forwarding-table vrf vpn1 209.165.201.1	(任意) LFIB の内容を表示します。 <ul style="list-style-type: none"> <li>CE2 の VPN ルーティングおよび転送テーブルを確認するには、<b>vrf</b> キーワードを指定して <b>show mpls forwarding-table</b> コマンドを使用します。出力に、CE2 のラベルと発信インターフェイスが表示されます。</li> </ul>

	コマンドまたはアクション	目的
ステップ 4	<b>show ip bgp vpnv4</b> { <b>all</b>   <b>rd</b> <i>route-distinguisher</i>   <b>vrf</b> <i>vrf-name</i> } <b>[summary]</b> <b>[labels]</b>  例： Device# show ip bgp vpnv4 all labels	(任意) BGP テーブルからの VPN アドレス情報を表示します。  <ul style="list-style-type: none"> <li>マルチプロトコル BGP テーブル内の CE2 の VPN ラベルを確認するには、<b>all</b> および <b>labels</b> キーワードを指定して <b>show ip bgp vpnv4</b> コマンドを使用します。</li> </ul>
ステップ 5	<b>show ip cef</b> [ <b>vrf</b> <i>vrf-name</i> ] [ <i>network</i> <i>[mask]</i> ] [ <b>longer-prefixes</b> ] [ <b>detail</b> ]  例： Device# show ip cef <vrf-name> 209.165.201.1	(任意) 転送情報ベース (FIB) のエントリを表示するか、または FIB のサマリーを表示します。  <ul style="list-style-type: none"> <li>CE2 の CEF エントリを確認するには、<b>show ip cef</b> コマンドを使用します。コマンド出力に、CE2 のローカルラベルと発信インターフェイスが表示されます。</li> </ul>
ステップ 6	<b>disable</b>  例： Device# disable	(任意) 終了して、ユーザー EXEC モードに戻ります。

## ASBR の設定の確認

ASBR 間で、ルート マップの指定に従って MPLS ラベル付きの IPv4 ルートまたはラベルなしの IPv4 ルートが交換されていることを確認するには、次の作業を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例： Device> enable	特権 EXEC モードを有効にします。  <ul style="list-style-type: none"> <li>パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>show ip bgp</b> <b>[network]</b> [ <i>network-mask</i> ] [ <b>longer-prefixes</b> ]  例： Device# show ip bgp 209.165.202.129  例：	(任意) BGP ルーティング テーブルのエントリを表示します。  <ul style="list-style-type: none"> <li><b>show ip bgp</b> コマンドを使用して、次のことを確認します。</li> </ul>

	コマンドまたはアクション	目的
	Device# show ip bgp 192.0.2.1	<ul style="list-style-type: none"> <li>ASBR1 が ASBR2 から PE2 の MPLS ラベルを受信していること。</li> <li>ASBR1 がラベルなしの RR2 の ASBR2 IPv4 ルートを受信していること。コマンド出力に MPLS ラベル情報が表示されない場合、MPLS ラベルなしでルートが受信されています。</li> <li>ASBR2 が ASBR1 に PE2 の MPLS ラベルを配布していること。</li> <li>ASBR2 が ASBR1 に RR2 のラベルを配布していないこと。</li> </ul>
ステップ 3	<b>show ip cef [vrf vrf-name] [network [mask]] [longer-prefixes] [detail]</b> 例 : Device# show ip cef 209.165.202.129 例 : Device# show ip cef 192.0.2.1	(任意) 転送情報ベース (FIB) のエントリを表示するか、または FIB のサマリーを表示します。 <ul style="list-style-type: none"> <li>ASBR1 および ASBR2 から <b>show ip cef</b> コマンドを使用して、次のことを確認します。               <ul style="list-style-type: none"> <li>PE2 の CEF エントリが正しいこと。</li> <li>RR2 の CEF エントリが正しいこと。</li> </ul> </li> </ul>
ステップ 4	<b>disable</b> 例 : Device# disable	(任意) 終了して、ユーザー EXEC モードに戻ります。

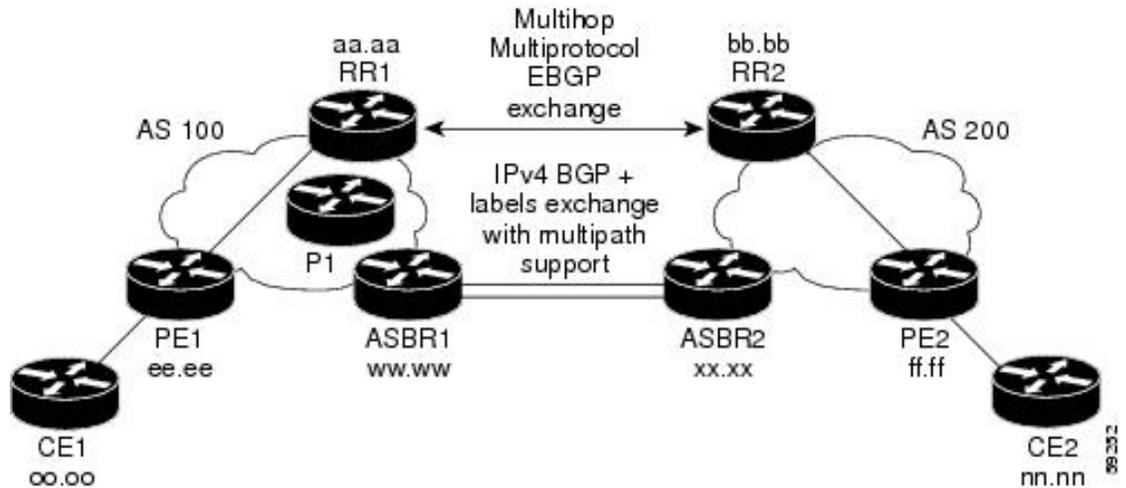
## MPLS VPN Inter-AS IPv4 BGP ラベル配布の設定例

MPLS VPN Inter-AS IPv4 BGP ラベル配布機能の設定例には、次のものがあります。

## BGP を使用して MPLS VPN サービスプロバイダー経由でルートおよび MPLS ラベルを配布する Inter-AS の設定例

次の図に、2つの MPLS VPN サービスプロバイダーを示します。サービスプロバイダーは、ルータリフレクタ間で VPNv4 ルートを配布します。サービスプロバイダーは、ASBR 間で MPLS ラベル付きの IPv4 ルートを配布します。

図 34: MPLS VPN サービスプロバイダー間での IPv4 ルートと MPLS ラベルの配布



設定例では、リモートの RR と PE からローカルの RR と PE に、VPNv4 ルートおよび MPLS ラベル付きの IPv4 ルートを配布するために使用できる次の 2 つの技術を示しています。

- 自律システム 100 は、RR を使用して、リモート RR から学習した VPNv4 ルートを配布します。また、RR は、IPv4 ラベルを使用して、ASBR1 から学習したリモート PE アドレスとラベルを配布します。
- 自律システム 200 では、ASBR2 が学習した IPv4 ルートが IGP に再配布されます。

この項では、次の設定例を示します。

### 例：ルータリフレクタ 1 (MPLS VPN サービスプロバイダー)

RR1 の設定例では、次のことが指定されています。

- RR1 は、マルチプロトコル、マルチホップ EBGP を使用して、RR2 と VPNv4 ルートを交換します。
- VPNv4 ネクストホップ情報および VPN ラベルは、自律システム間で保存されます。
- RR1 から PE1 に次の内容が反映されます。
  - RR2 から学習した VPNv4 ルート
  - ASBR1 から学習した IPv4 ルートおよび MPLS ラベル

例：ルータリフレクタ 1 (MPLS VPN サービスプロバイダー)

```

ip subnet-zero
ip cef
!
interface Loopback0
 ip address 10.0.0.1 255.255.255.255
 no ip directed-broadcast
!
interface Serial1/2
 ip address 209.165.201.8 255.0.0.0
 no ip directed-broadcast
 clockrate 124061
!
router ospf 10
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 network 10.0.0.1 0.0.0.0 area 100
 network 209.165.201.9 0.255.255.255 area 100
!
router bgp 100
 bgp cluster-id 1
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor 203.0.113.1 remote-as 100
 neighbor 203.0.113.1 update-source Loopback0
 neighbor 209.165.200.225 remote-as 100
 neighbor 209.165.200.225 update-source Loopback0
 neighbor 192.0.2.1 remote-as 200
 neighbor 192.0.2.1 ebgp-multihop 255
 neighbor 192.0.2.1 update-source Loopback0
 no auto-summary
!
address-family ipv4
 neighbor 203.0.113.1 activate
 neighbor 203.0.113.1 route-reflector-client                !IPv4+labels session to PE1

 neighbor 203.0.113.1 send-label
 neighbor 209.165.200.225 activate
 neighbor 209.165.200.225 route-reflector-client            !IPv4+labels session
to ASBR1
 neighbor 209.165.200.225 send-label
 no neighbor 192.0.2.1 activate
 no auto-summary
 no synchronization
 exit-address-family
!
address-family vpv4
 neighbor 203.0.113.1 activate
 neighbor 203.0.113.1 route-reflector-client                !VPNv4 session with PE1
 neighbor 203.0.113.1 send-community extended
 neighbor 192.0.2.1 activate
 neighbor 192.0.2.1 next-hop-unchanged                    !MH-VPNv4 session with RR2
 neighbor 192.0.2.1 send-community extended                !with next hop unchanged

 exit-address-family
!
ip default-gateway 3.3.0.1
no ip classless
!
snmp-server engineID local 00000009020000D0584B25C0
snmp-server community public RO
snmp-server community write RW
no snmp-server ifindex persist
snmp-server packetsize 2048

```

```
!
end
```

## 設定例 : ASBR1 (MPLS VPN サービスプロバイダー)

ASBR1 は、ASBR2 と IPv4 ルートおよび MPLS ラベルを交換します。

この例では、ASBR1 で、次のルートマップを使用してルートがフィルタリングされています。

- OUT というルート マップでは、ASBR1 において、PE1 ルート (ee.ee) はラベルを付けて配布し、RR1 ルート (aa.aa) はラベルを付けずに配布する必要があることが指定されています。
- IN というルート マップでは、ASBR1 にラベル付きの PE2 ルート (ff.ff) とラベルなしの RR2 ルート (bb.bb) を受け入れさせるように指定しています。

```
ip subnet-zero
mpls label protocol tdp
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet0/2
 ip address 209.165.201.6 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
!
interface Ethernet0/3
 ip address 209.165.201.18 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
 mpls label protocol ldp
 mpls ip
!router ospf 10
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 passive-interface Ethernet0/2
 network 209.165.200.225 0.0.0.0 area 100
 network 209.165.201.9 0.255.255.255 area 100

router bgp 100
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor 10.0.0.1 remote-as 100
 neighbor 10.0.0.1 update-source Loopback0
 neighbor 209.165.201.2 remote-as 200
 no auto-summary
!
address-family ipv4
 redistribute ospf 10
 neighbor 10.0.0.1 activate
 neighbor 10.0.0.1 send-label
 neighbor 209.165.201.2 activate
 neighbor 209.165.201.2 advertisement-interval 5
 neighbor 209.165.201.2 send-label
 neighbor 209.165.201.2 route-map IN in
 neighbor 209.165.201.2 route-map OUT out
```

! Redistributing IGP into BGP  
! so that PE1 & RR1 loopbacks  
! get into the BGP table

! accepting routes in route map IN.  
! distributing routes in route map OUT.

## 設定例：ルータリフレクタ 2 (MPLS VPN サービスプロバイダー)

```

neighbor 209.165.201.3 activate
neighbor 209.165.201.3 advertisement-interval 5
neighbor 209.165.201.3 send-label
neighbor 209.165.201.3 route-map IN in          ! accepting routes in route map IN.
neighbor 209.165.201.3 route-map OUT out       ! distributing routes in route map OUT.
no auto-summary
no synchronization
exit-address-family
!
ip default-gateway 3.3.0.1
ip classless
!
access-list 1 permit 203.0.113.1 log           !Setting up the access lists
access-list 2 permit 209.165.202.129 log
access-list 3 permit 10.0.0.1 log
access-list 4 permit 192.0.2.1 log

route-map IN permit 10                        !Setting up the route maps
  match ip address 2
  match mpls-label
!
route-map IN permit 11
  match ip address 4
!
route-map OUT permit 12
  match ip address 3
!
route-map OUT permit 13
  match ip address 1
  set mpls-label
!
end

```

## 設定例：ルータリフレクタ 2 (MPLS VPN サービスプロバイダー)

RR2 は、マルチホップ、マルチプロトコル EBGp を使用して、RR1 と VPNv4 ルートを交換します。また、この設定では、自律システム間でネクストホップ情報および VPN ラベルが維持されるように指定されています。

```

ip subnet-zero
ip cef
!
interface Loopback0
  ip address 192.0.2.1 255.255.255.255
  no ip directed-broadcast
!
interface Serial1/1
  ip address 209.165.201.10 255.0.0.0
  no ip directed-broadcast
  no ip mroute-cache
!
router ospf 20
  log-adjacency-changes
  network 192.0.2.1 0.0.0.0 area 200
  network 209.165.201.20 0.255.255.255 area 200
!
router bgp 200
  bgp cluster-id 1
  bgp log-neighbor-changes
  timers bgp 10 30
  neighbor 10.0.0.1 remote-as 100
  neighbor 10.0.0.1 ebgp-multihop 255
  neighbor 10.0.0.1 update-source Loopback0

```

```

neighbor 209.165.202.129 remote-as 200
neighbor 209.165.202.129 update-source Loopback0
no auto-summary
!
address-family vpnv4
neighbor 10.0.0.1 activate
neighbor 10.0.0.1 next-hop-unchanged           !Multihop VPNv4 session with RR1
neighbor 10.0.0.1 send-community extended      !with next-hop-unchanged
neighbor 209.165.202.129 activate
neighbor 209.165.202.129 route-reflector-client !VPNv4 session with PE2
neighbor 209.165.202.129 send-community extended
exit-address-family
!
ip default-gateway 3.3.0.1
no ip classless
!
end

```

## 設定例 : ASBR2 (MPLS VPN サービスプロバイダー)

ASBR2 は、ASBR1 と IPv4 ルートおよび MPLS ラベルを交換します。ただし、ASBR1 とは異なり、ASBR2 は RR を使用して IPv4 ルートおよび MPLS ラベルを PE2 に反映しません。ASBR2 は、ASBR1 から学習した IPv4 ルートおよび MPLS ラベルを IGP に再配布します。これで、PE2 がこれらのプレフィックスに到達できるようになります。

```

ip subnet-zero
ip cef
!
mpls label protocol tdp
!
interface Loopback0
ip address 209.165.200.226 255.255.255.255
no ip directed-broadcast
!
interface Ethernet1/0
ip address 209.165.201.2 255.0.0.0
no ip directed-broadcast
no ip mroute-cache
!
interface Ethernet1/2
ip address 209.165.201.4 255.0.0.0
no ip directed-broadcast
no ip mroute-cache
mpls label protocol tdp
mpls ip
!
router ospf 20
log-adjacency-changes
auto-cost reference-bandwidth 1000
redistribute connected subnets
redistribute bgp 200 subnets           ! Redistributing the routes learned from
passive-interface Ethernet1/0          ! ASBR1(EBGP+labels session) into IGP
network 209.165.200.226 0.0.0.0 area 200 ! so that PE2 will learn them
network 209.165.201.5 0.255.255.255 area 200
!
router bgp 200
bgp log-neighbor-changes
timers bgp 10 30
neighbor 192.0.2.1 remote-as 200
neighbor 192.0.2.1 update-source Loopback0
neighbor 209.165.201.6 remote-as 100
no auto-summary

```

```

!
address-family ipv4
  redistribute ospf 20                ! Redistributing IGP into BGP
  neighbor 209.165.201.6 activate      ! so that PE2 & RR2 loopbacks
  neighbor 209.165.201.6 advertisement-interval 5 ! will get into the BGP-4 table.
  neighbor 209.165.201.6 route-map IN in
  neighbor 209.165.201.6 route-map OUT out
  neighbor 209.165.201.6 send-label
  neighbor 209.165.201.7 activate
  neighbor 209.165.201.7 advertisement-interval 5
  neighbor 209.165.201.7 route-map IN in
  neighbor 209.165.201.7 route-map OUT out
  neighbor 209.165.201.7 send-label
  no auto-summary
  no synchronization
  exit-address-family
!
address-family vpnv4
  neighbor 192.0.2.1 activate
  neighbor 192.0.2.1 send-community extended
  exit-address-family
!
ip default-gateway 3.3.0.1
ip classless
!
access-list 1 permit 209.165.202.129 log      !Setting up the access lists
access-list 2 permit 203.0.113.1 log
access-list 3 permit 192.0.2.1 log
access-list 4 permit 10.0.0.1 log

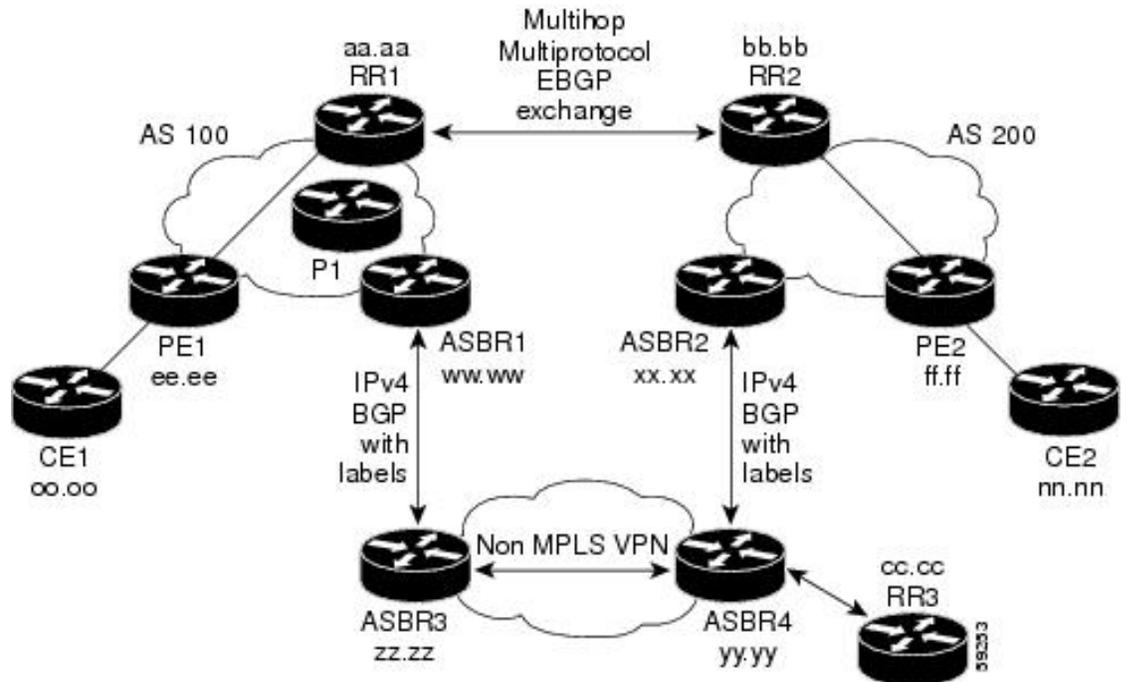
route-map IN permit 11                    !Setting up the route maps
  match ip address 2
  match mpls-label
!
route-map IN permit 12
  match ip address 4
!
route-map OUT permit 10
  match ip address 1
  set mpls-label
!
route-map OUT permit 13
  match ip address 3
end

```

## 設定例 : BGPを使用して非MPLSVPNサービスプロバイダー経由でルートおよび MPLS ラベルを配布する Inter-AS

次の図に、非 MPLS VPN サービスプロバイダー経由で接続された2つの MPLS VPN サービスプロバイダーを示します。ネットワークの中間にある自律システムは、Label Distribution Protocol (LDP; ラベル配布プロトコル) または Tag Distribution Protocol (TDP) を使用して MPLS ラベルを配布するバックボーン自律システムとして設定されます。また、TDP や LDP の代わりにトラフィック エンジニアリング トンネルを使用して、非 MPLS VPN サービスプロバイダーで LSP を構築できます。

図 35: 非 MPLS VPN サービスプロバイダー経由でのルートと MPLS ラベルの配布



ここでは、BGP を使用して非 MPLS VPN サービスプロバイダー経由でルートおよび MPLS ラベルを配布する Inter-AS の次の設定例について説明します。

## 設定例：ルートリフレクタ 1（非 MPLS VPN サービスプロバイダー）

RR1 の設定例では、次のことが指定されています。

- RR1 は、マルチプロトコル、マルチホップ EBGP を使用して、RR2 と VPNv4 ルートを交換します。
- VPNv4 ネクスト ホップ情報および VPN ラベルは、自律システム間で保存されます。
- RR1 から PE1 に次の内容が反映されます。
  - RR2 から学習した VPNv4 ルート
  - ASBR1 から学習した IPv4 ルートおよび MPLS ラベル

```
ip subnet-zero
ip cef
!
interface Loopback0
 ip address 10.0.0.1 255.255.255.255
 no ip directed-broadcast
!
interface Serial1/2
 ip address 209.165.201.8 255.0.0.0
 no ip directed-broadcast
 clockrate 124061
!
```

## 設定例 : ASBR1 (非 MPLS VPN サービスプロバイダー)

```

router ospf 10
  log-adjacency-changes
  auto-cost reference-bandwidth 1000
  network 10.0.0.1 0.0.0.0 area 100
  network 209.165.201.9 0.255.255.255 area 100
!
router bgp 100
  bgp cluster-id 1
  bgp log-neighbor-changes
  timers bgp 10 30
  neighbor 203.0.113.1 remote-as 100
  neighbor 203.0.113.1 update-source Loopback0
  neighbor 209.165.200.225 remote-as 100
  neighbor 209.165.200.225 update-source Loopback0
  neighbor 192.0.2.1 remote-as 200
  neighbor 192.0.2.1 ebgp-multihop 255
  neighbor 192.0.2.1 update-source Loopback0
  no auto-summary
!
address-family ipv4
  neighbor 203.0.113.1 activate
  neighbor 203.0.113.1 route-reflector-client                !IPv4+labels session to PE1

  neighbor 203.0.113.1 send-label
  neighbor 209.165.200.225 activate
  neighbor 209.165.200.225 route-reflector-client          !IPv4+labels session
to ASBR1
  neighbor 209.165.200.225 send-label
  no neighbor 192.0.2.1 activate
  no auto-summary
  no synchronization
  exit-address-family
!
address-family vpnv4
  neighbor 203.0.113.1 activate
  neighbor 203.0.113.1 route-reflector-client              !VPNv4 session with PE1
  neighbor 203.0.113.1 send-community extended
  neighbor 192.0.2.1 activate
  neighbor 192.0.2.1 next-hop-unchanged                   !MH-VPNv4 session with RR2
  neighbor 192.0.2.1 send-community extended              with next-hop-unchanged

  exit-address-family
!
ip default-gateway 3.3.0.1
no ip classless
!
snmp-server engineID local 00000009020000D0584B25C0
snmp-server community public RO
snmp-server community write RW
no snmp-server ifindex persist
snmp-server packetsize 2048
!
end

```

## 設定例 : ASBR1 (非 MPLS VPN サービスプロバイダー)

ASBR1 は、ASBR2 と IPv4 ルートおよび MPLS ラベルを交換します。

この例では、ASBR1 で、次のルートマップを使用してルートがフィルタリングされています。

- OUT というルート マップでは、ASBR1 において、PE1 ルート (ee.aa) はラベルを付けて配布し、RR1 ルート (aa.aa) はラベルを付けずに配布する必要があることが指定されています。
- IN というルート マップでは、ASBR1 にラベル付きの PE2 ルート (ff.aa) とラベルなしの RR2 ルート (bb.bb) を受け入れさせるように指定しています。

```

ip subnet-zero
ip cef distributed
mpls label protocol tdp
!
interface Loopback0
ip address 209.165.200.225 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface Serial3/0/0
ip address 209.165.201.7 255.0.0.0
no ip directed-broadcast
ip route-cache distributed
!
interface Ethernet0/3
ip address 209.165.201.18 255.0.0.0
no ip directed-broadcast
no ip mroute-cache
mpls label protocol ldp
mpls ip
!
router ospf 10
log-adjacency-changes
auto-cost reference-bandwidth 1000
redistribute connected subnets
passive-interface Serial3/0/0
network 209.165.200.225 0.0.0.0 area 100
network dd.0.0.0 0.255.255.255 area 100

router bgp 100
bgp log-neighbor-changes
timers bgp 10 30
neighbor 10.0.0.1 remote-as 100
neighbor 10.0.0.1 update-source Loopback0
neighbor kk.0.0.1 remote-as 200
no auto-summary
!
address-family ipv4
redistribute ospf 10 ! Redistributing IGP into BGP
neighbor 10.0.0.1 activate ! so that PE1 & RR1 loopbacks
neighbor 10.0.0.1 send-label ! get into BGP table
neighbor 209.165.201.3 activate
neighbor 209.165.201.3 advertisement-interval 5
neighbor 209.165.201.3 send-label
neighbor 209.165.201.3 route-map IN in ! Accepting routes specified in route map
IN
neighbor 209.165.201.3 route-map OUT out ! Distributing routes specified in route map
OUT
no auto-summary
no synchronization
exit-address-family
!
ip default-gateway 3.3.0.1
ip classless

```

## 設定例：ルータリフレクタ 2（非 MPLS VPN サービスプロバイダー）

```

!
access-list 1 permit 203.0.113.1 log
access-list 2 permit 209.165.202.129 log
access-list 3 permit 10.0.0.1 log
access-list 4 permit 192.0.2.1 log
!
route-map IN permit 10
  match ip address 2
  match mpls-label
!
route-map IN permit 11
  match ip address 4
!
route-map OUT permit 12
  match ip address 3
!
route-map OUT permit 13
  match ip address 1
  set mpls-label
!
end

```

## 設定例：ルータリフレクタ 2（非 MPLS VPN サービスプロバイダー）

RR2 は、マルチホップ、マルチプロトコル EBGP を使用して、RR1 と VPNv4 ルートを交換します。また、この設定では、自律システム間でネクストホップ情報および VPN ラベルが維持されるように指定されています。

```

ip subnet-zero
ip cef
!
interface Loopback0
  ip address 192.0.2.1 255.255.255.255
  no ip directed-broadcast
!
interface Serial1/1
  ip address 209.165.201.10 255.0.0.0
  no ip directed-broadcast
  no ip mroute-cache
!
router ospf 20
  log-adjacency-changes
  network 192.0.2.1 0.0.0.0 area 200
  network 209.165.201.20 0.255.255.255 area 200
!
router bgp 200
  bgp cluster-id 1
  bgp log-neighbor-changes
  timers bgp 10 30
  neighbor 10.0.0.1 remote-as 100
  neighbor 10.0.0.1 ebgp-multihop 255
  neighbor 10.0.0.1 update-source Loopback0
  neighbor 209.165.202.129 remote-as 200
  neighbor 209.165.202.129 update-source Loopback0
  no auto-summary
!
  address-family vpnv4
    neighbor 10.0.0.1 activate
    neighbor 10.0.0.1 next-hop-unchanged !MH vpnv4 session with RR1
    neighbor 10.0.0.1 send-community extended !with next-hop-unchanged
    neighbor 209.165.202.129 activate
    neighbor 209.165.202.129 route-reflector-client !vpnv4 session with PE2
    neighbor 209.165.202.129 send-community extended

```

```

    exit-address-family
    !
    ip default-gateway 3.3.0.1
    no ip classless
    !
    end

```

## 設定例 : ASBR2 (非 MPLS VPN サービスプロバイダー)

ASBR2 は、ASBR1 と IPv4 ルートおよび MPLS ラベルを交換します。ただし、ASBR1 とは異なり、ASBR2 は RR を使用して IPv4 ルートおよび MPLS ラベルを PE2 に反映しません。ASBR2 は、ASBR1 から学習した IPv4 ルートおよび MPLS ラベルを IGP に再配布します。これで、PE2 がこれらのプレフィックスに到達できるようになります。

```

ip subnet-zero
ip cef
!
mpls label protocol tdp
!
interface Loopback0
 ip address 209.165.200.226 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet0/1
 ip address 209.165.201.11 255.0.0.0
 no ip directed-broadcast
!
interface Ethernet1/2
 ip address 209.165.201.4 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
 mpls label protocol tdp
 mpls ip
!
router ospf 20
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 redistribute bgp 200 subnets           !redistributing the routes learned from
 passive-interface Ethernet0/1         !ASBR2 (EBGP+labels session) into IGP
 network 209.165.200.226 0.0.0.0 area 200 !so that PE2 will learn them
 network 209.165.201.5 0.255.255.255 area 200
!
router bgp 200
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor 192.0.2.1 remote-as 200
 neighbor 192.0.2.1 update-source Loopback0
 neighbor 209.165.201.21 remote-as 100
 no auto-summary
!
 address-family ipv4                       ! Redistributing IGP into BGP
 redistribute ospf 20                       ! so that PE2 & RR2 loopbacks
 neighbor 209.165.201.21 activate           ! will get into the BGP-4 table
 neighbor 209.165.201.21 advertisement-interval 5
 neighbor 209.165.201.21 route-map IN in
 neighbor 209.165.201.21 route-map OUT out
 neighbor 209.165.201.21 send-label
 no auto-summary
 no synchronization
 exit-address-family

```

## 設定例 : ASBR3 (非 MPLS VPN サービスプロバイダー)

```

!
address-family vpnv4
  neighbor 192.0.2.1 activate
  neighbor 192.0.2.1 send-community extended
  exit-address-family
!
ip default-gateway 3.3.0.1
ip classless
!
access-list 1 permit 209.165.202.129 log
access-list 2 permit 203.0.113.1 log
access-list 3 permit 192.0.2.1 log
access-list 4 permit 10.0.0.1 log
!
route-map IN permit 11
  match ip address 2
  match mpls-label
!
route-map IN permit 12
  match ip address 4
!
route-map OUT permit 10
  match ip address 1
  set mpls-label
!
route-map OUT permit 13
  match ip address 3
!
end

```

## 設定例 : ASBR3 (非 MPLS VPN サービスプロバイダー)

ASBR3 は、非 MPLS VPN サービスプロバイダーに属しています。ASBR3 は、ASBR1 との間で IPv4 ルートおよび MPLS ラベルを交換します。また、ASBR3 は、ASBR1 から学習したルートを RR3 経由で ASBR3 に渡します。



(注) IBGP を使用してルートおよびラベルを配布する場合は、学習した EBGP ルートを IBGP に再配布しないでください。このような設定はサポートされていません。

```

ip subnet-zero
ip cef
!
interface Loopback0
  ip address 209.165.200.227 255.255.255.255
  no ip directed-broadcast
  no ip route-cache
  no ip mroute-cache
!
ip routing
mpls label protocol ldp
mpls ldp router-id Loopback0 force

interface GigabitEthernet1/0/1
ip address 209.165.201.12 255.0.0.0

interface TenGigabitEthernet1/1/1
no switchport
ip address 209.165.201.3 255.0.0.0
load-interval 30

```

```
mpls ip

!
router ospf 30
log-adjacency-changes
auto-cost reference-bandwidth 1000
redistribute connected subnets
network 209.165.200.227 0.0.0.0 area 300
network 209.165.201.13 0.255.255.255 area 300
!
router bgp 300
bgp log-neighbor-changes
timers bgp 10 30
neighbor 10.0.0.3 remote-as 300
neighbor 10.0.0.3 update-source Loopback0
neighbor 209.165.201.7 remote-as 100
no auto-summary
!
address-family ipv4
neighbor 10.0.0.3 activate          ! IBGP+labels session with RR3
neighbor 10.0.0.3 send-label
neighbor 209.165.201.7 activate     ! EBGP+labels session with ASBR1
neighbor 209.165.201.7 advertisement-interval 5
neighbor 209.165.201.7 send-label
neighbor 209.165.201.7 route-map IN in
neighbor 209.165.201.7 route-map OUT out
no auto-summary
no synchronization
exit-address-family
!
ip classless
!
access-list 1 permit 203.0.113.1 log
access-list 2 permit 209.165.202.129 log
access-list 3 permit 10.0.0.1 log
access-list 4 permit 192.0.2.1 log
!
route-map IN permit 10
match ip address 1
match mpls-label
!
route-map IN permit 11
match ip address 3
!
route-map OUT permit 12
match ip address 2
set mpls-label
!
route-map OUT permit 13
match ip address 4
!
ip default-gateway 3.3.0.1
ip classless
!
end
```

### 設定例：ルートリフレクタ 3（非 MPLS VPN サービスプロバイダー）

RR3 は、MPLS ラベル付きの IPv4 ルートを ASBR3 および ASBR4 に反映する非 MPLS VPN RR です。

```
ip subnet-zero
mpls label protocol tdp
```

## 設定例 : ASBR4 (非 MPLS VPN サービスプロバイダー)

```

mpls traffic-eng auto-bw timers
no mpls ip
!
interface Loopback0
 ip address 10.0.0.3 255.255.255.255
 no ip directed-broadcast
!
interface POS0/2
 ip address 209.165.201.15 255.0.0.0
 no ip directed-broadcast
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 crc 16
 clock source internal
!
router ospf 30
 log-adjacency-changes
 network 10.0.0.3 0.0.0.0 area 300
 network 209.165.201.16 0.255.255.255 area 300
!
router bgp 300
 bgp log-neighbor-changes
 neighbor 209.165.201.2 remote-as 300
 neighbor 209.165.201.2 update-source Loopback0
 neighbor 209.165.200.227 remote-as 300
 neighbor 209.165.200.227 update-source Loopback0
 no auto-summary
!
address-family ipv4
 neighbor 209.165.201.2 activate
 neighbor 209.165.201.2 route-reflector-client
 neighbor 209.165.201.2 send-label ! IBGP+labels session with ASBR3
 neighbor 209.165.200.227 activate
 neighbor 209.165.200.227 route-reflector-client
 neighbor 209.165.200.227 send-label ! IBGP+labels session with ASBR4
 no auto-summary
 no synchronization
 exit-address-family
!
ip default-gateway 3.3.0.1
ip classless
!
end

```

## 設定例 : ASBR4 (非 MPLS VPN サービスプロバイダー)

ASBR4 は、非 MPLS VPN サービスプロバイダーに属しています。ASBR4 と ASBR3 は、RR3 経由で IPv4 ルートと MPLS ラベルを交換します。



(注) IBGP を使用してルートおよびラベルを配布する場合は、学習した EBGP ルートを IBGP に再配布しないでください。このような設定はサポートされていません。

```

ip subnet-zero
ip cef distributed
!
interface Loopback0
 ip address 209.165.201.2 255.255.255.255
 no ip directed-broadcast

```

```
no ip route-cache
no ip mroute-cache
!
interface Ethernet0/2
 ip address 209.165.201.21 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
!
ip routing
mpls label protocol ldp
mpls ldp router-id Loopback0 force

interface GigabitEthernet1/0/1
ip address 209.165.201.17 255.0.0.0

interface TenGigabitEthernet1/1/1
no switchport
ip address 209.165.201.14 255.0.0.0
load-interval 30
mpls ip

!
router ospf 30
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 passive-interface Ethernet0/2
 network 209.165.201.2 0.0.0.0 area 300
 network 209.165.201.16 0.255.255.255 area 300
 network 209.165.201.13 0.255.255.255 area 300
!
router bgp 300
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor 10.0.0.3 remote-as 300
 neighbor 10.0.0.3 update-source Loopback0
 neighbor 209.165.201.11 remote-as 200
 no auto-summary
!
 address-family ipv4
 neighbor 10.0.0.3 activate
 neighbor 10.0.0.3 send-label
 neighbor 209.165.201.11 activate
 neighbor 209.165.201.11 advertisement-interval 5
 neighbor 209.165.201.11 send-label
 neighbor 209.165.201.11 route-map IN in
 neighbor 209.165.201.11 route-map OUT out
 no auto-summary
 no synchronization
 exit-address-family
!
ip classless
!
access-list 1 permit 209.165.202.129 log
access-list 2 permit 203.0.113.1 log
access-list 3 permit 192.0.2.1 log
access-list 4 permit 10.0.0.1 log
!
route-map IN permit 10
 match ip address 1
 match mpls-label
!
route-map IN permit 11
```

```

    match ip address 3
  !
  route-map OUT permit 12
    match ip address 2
    set mpls-label
  !
  route-map OUT permit 13
    match ip address 4
  !
  ip default-gateway 3.3.0.1
  ip classless
  !
end

```

## MPLS VPN Inter-AS IPv4 BGP ラベル配布の設定の機能履歴

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレーンで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、[www.cisco.com/go/cfn](http://www.cisco.com/go/cfn) に移動します。Cisco.com のアカウントは必要ありません。

リリース	機能	機能情報
Cisco IOS XE Gibraltar 16.11.1	MPLS VPN Inter-AS IPv4 BGP ラベル配布	この機能を使用すると、バーチャルプライベートネットワーク (VPN) サービスプロバイダーネットワークを設定できます。このネットワークでは、自律システム境界ルータ (ASBR) が、プロバイダーエッジ (PE) ルータのマルチプロトコル ラベル スイッチング (MPLS) ラベル付きの IPv4 ルートを交換します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



## 第 22 章

# シームレス MPLS の設定

- [シームレス MPLS に関する情報 \(377 ページ\)](#)
- [シームレス MPLS の設定方法 \(379 ページ\)](#)
- [シームレス MPLS の設定例 \(384 ページ\)](#)
- [シームレス MPLS の機能履歴 \(387 ページ\)](#)

## シームレス MPLS に関する情報

次の項では、シームレス MPLS について説明します。

### シームレス MPLS の概要

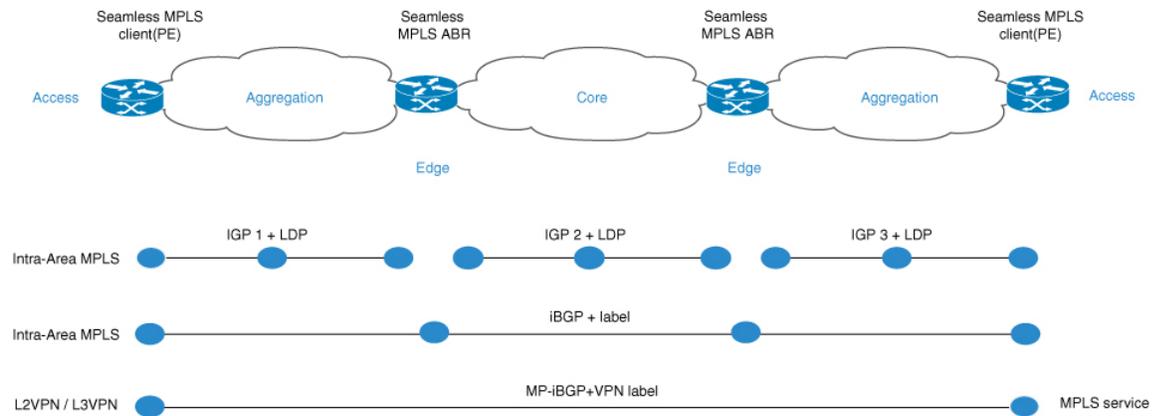
シームレス MPLS は、複数のネットワークを単一の MPLS ドメインに統合するための、非常に柔軟でスケーラブルなアーキテクチャを提供します。これは、既存の既知のプロトコルに基づいています。

大規模な MPLS ネットワークでは、ネットワークのさまざまな部分に複数のタイプのプラットフォームとサービスを配置できます。このようなネットワークは、通常、コアエリアと集約エリアなどのエリアに分割され、各エリアに異なる内部ゲートウェイプロトコル (IGP) があります。あるエリアの IGP プレフィックスを別のエリアに配布することはできません。IGP プレフィックスを配布できない場合、エンドツーエンドのラベルスイッチパス (LSP) は確立できません。これは、ネットワークの拡張性に影響します。

シームレス MPLS では、エンドツーエンド LSP を確立することで、拡張性が向上します。シームレス MPLS は、プロバイダーエッジ (PE) ルータのループバックプレフィックスを転送するために、IGP ではなくボーダー ゲートウェイ プロトコル (BGP) を使用します。BGP は、プレフィックスをエンドツーエンドで配布します。これにより、あるドメインの IGP プレフィックスを別のドメインにインストールする必要がなくなります。

シームレス MPLS は、サービスプレーンとトランスポートプレーンの分離を導入し、エンドツーエンドのサービスに依存しないトランスポートを提供します。これにより、ネットワークトランスポート ノードでサービス固有の設定が不要になります。

## シームレス MPLS のアーキテクチャ



図は、3つの異なるエリア（1つのコアエリアと2つの集約エリア）があるネットワークを示しています。各エリアでは独自のIGPが実行され、エリア境界ルータ（ABR）ではエリア間の再配布は行われません。エンドツーエンドMPLS LSPを提供するためには、BGPを使用する必要があります。BGPは、ドメイン全体にラベルを付けてPEルータのループバックをアドバタイズし、エンドツーエンドLSPを提供します。BGPはPEとABRの間に導入されます。

シームレスMPLSは、BGPを使用してエンドツーエンドMPLS LSPを提供します。BGPはPEとABRの間に導入されます。BGPはIPv4プレフィックスとラベルを送信します。BGPは、ドメイン全体にラベルを付けてPEルータのループバックをアドバタイズし、エンドツーエンドLSPを提供します。

ネットワークでIGPを使用する場合、プレフィックスのネクストホップアドレスはPEルータのループバックプレフィックスです。このプレフィックスは、ネットワークの他の部分で使用されているIGPには認識されません。ネクストホップアドレスは、IGPプレフィックスへの再帰には使用できません。これを回避するために、プレフィックスはBGPで伝送されます。ABRはルートリフレクタ（RR）として設定されます。RRは、反映されたiBGPプレフィックスの場合でも、ネクストホップをRR自体に設定するように設定されます。

次の2つのシナリオが考えられます。

- ABRは、ABRによってネットワークの集約部分にアドバタイズされる（BGPによって反映される）プレフィックスのネクストホップをABR自体に設定しません。ABRは、コアIGPから集約IGPにABRのループバックプレフィックスを再配布する必要があります。（コアからの）ABRループバックプレフィックスのみを集約部分にアドバタイズする必要があります。リモート集約部分からのPEルータのループバックプレフィックスは不要です。
- ABRは、ABRによって集約部分にアドバタイズされた（BGPによって反映された）プレフィックスのネクストホップをABR自体に設定します。このため、ABRはABRのループバックプレフィックスをコアIGPから集約IGPに再配布する必要はありません。

いずれのシナリオでも、ABR は、ABR によってネットワークの集約部分からコア部分にアドバタイズされた（BGP によって反映された）プレフィックスのネクストホップを ABR 自体に設定します。

## シームレス MPLS の設定方法

次の項では、シームレス MPLS の設定方法について説明します。

### PE ルータでのシームレス MPLS の設定

次の手順を使用して、PE ルータでシームレス MPLS を設定できます。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# configure terminal	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 3	<b>interface loopback slot/port</b> 例： Device(config-if)# interface Loopback0	ループバック インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<b>ip address ip-address subnet-mask</b> 例： Device(config-if)ip address 10.100.1.4 255.255.255.255	インターフェイスの IP アドレスを入力します。
ステップ 5	<b>interface ethernet slot/port</b> 例： Device(config-if)# interface Ethernet1/0	イーサネット インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	<b>no ip address</b> 例： Device(config-if)# no ip address	IP アドレス定義を削除します。

	コマンドまたはアクション	目的
ステップ 7	<b>xconnect peer-ip-address vcid encapsulation mpls</b>  例： Device(config-if)# xconnect 10.100.1.5 100 encapsulation mpls	カプセル化するためのトンネリング方式として MPLS を指定します。
ステップ 8	<b>router ospf process-id</b>  例： Device(config)# router ospf 2	OSPF ルーティングプロセスを設定します。
ステップ 9	<b>network ip-address wild-mask area area-id</b>  例： Device(config-router)# network 10.2.0.0 0.0.255.255 area 0	OSPF を実行するインターフェイスを定義し、それらのインターフェイスに対するエリア ID を定義します。
ステップ 10	<b>network ip-address wild-mask area area-id</b>  例： Device(config-router)# network 10.100.1.4 0.0.0.0 area 0	OSPF を実行するインターフェイスを定義し、それらのインターフェイスに対するエリア ID を定義します。
ステップ 11	<b>router bgp autonomous-system-number</b>  例： Device(config)# router bgp 1	BGP ルーティングプロセスを設定します。
ステップ 12	<b>bgp log neighbor changes</b>  例： Device(config-router)# bgp log neighbor changes	BGP ネイバーリセットのロギングを有効にします。
ステップ 13	<b>address-family ipv4</b>  例： Device(config-router)# address-family ipv4	アドレスファミリ 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	<b>network network-number mask network-mask</b>  例： Device(config-router-af)# network 10.100.1.4 mask 255.255.255.255	BGP およびマルチプロトコル BGP ルーティングプロセスによってアドバタイズされるネットワークを指定します。
ステップ 15	<b>no bgp default ipv4 unicast</b>  例： Device(config-router-af)# no bgp default ipv4 unicast	ピアリングセッションを確立するためのデフォルトの IPv4 ユニキャスト アドレス ファミリを無効にします。

	コマンドまたはアクション	目的
ステップ 16	<b>no bgp default route-target filter</b> 例 : Device (config-router-af) # no bgp default route-target filter	BGP の route-target コミュニティフィルタリングを無効にします。
ステップ 17	<b>neighbor ip-address remote-as autonomous-system-number</b> 例 : Device (config-router-af) # neighbor 10.100.1.1 remote-as 1	BGP ネイバーテーブルまたはマルチプロトコル BGP ネイバーテーブルにエントリを追加します。
ステップ 18	<b>neighbor ip-address update-source interface-type interface-number</b> 例 : Device (config-router-af) # neighbor 10.100.1.1 update-source Loopback0	BGP セッションが、TCP 接続の動作インターフェイスを使用できるようにします。
ステップ 19	<b>neighbor ip-address send-label</b> 例 : Device (config-router-af) # neighbor 10.100.1.1 send-label	BGP ルートとともに MPLS ラベルをネイバー BGP ルータに送信できるように BGP ルータを設定します。

## ルータリフレクタでのシームレス MPLS の設定

次の手順を使用して、ルータリフレクタでシームレス MPLS を設定できます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"><li>パスワードを入力します (要求された場合)。</li></ul>
ステップ 2	<b>configure terminal</b> 例 : Device# configure terminal	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 3	<b>interface loopback slot/port</b> 例 : Device (config-if) # interface Loopback0	ループバック インターフェイスを設定し、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ます。

	コマンドまたはアクション	目的
ステップ 4	<b>ip address ip-address subnet-mask</b> 例： Device(config-if)# ip address 10.100.1.1 255.255.255.255	インターフェイスの IP アドレスを入力します。
ステップ 5	<b>router ospf process-id</b> 例： Device(config)# router ospf 1	OSPF ルーティング プロセスを設定します。
ステップ 6	<b>network ip-address wild-mask area area-id</b> 例： Device(config-router)# network 10.1.0.0 0.0.255.255 area 0	OSPF を実行するインターフェイスを定義し、それらのインターフェイスに対するエリア ID を定義します。
ステップ 7	<b>network ip-address wild-mask area area-id</b> 例： Device(config-router)# 10.100.1.1 0.0.0.0 area 0	OSPF を実行するインターフェイスを定義し、それらのインターフェイスに対するエリア ID を定義します。
ステップ 8	<b>exit</b> 例： Device(config-router)#exit	コンフィギュレーションモードを終了します。
ステップ 9	<b>router ospf process-id</b> 例： Device(config)# router ospf 2	OSPF ルーティング プロセスを設定します。
ステップ 10	<b>redistribute ospf instance-tag route-map map-name</b> 例： Device(config-router)# redistribute ospf 1 subnets match internal route-map ospf1-into-ospf2	1つのルーティングドメインから OSPF にルートを注入します。
ステップ 11	<b>network ip-address wild-mask area area-id</b> 例： Device(config-router)# network 10.2.0.0 0.0.255.255 area 0	OSPF を実行するインターフェイスを定義し、それらのインターフェイスに対するエリア ID を定義します。
ステップ 12	<b>exit</b> 例： Device(config-router)#exit	コンフィギュレーションモードを終了します。
ステップ 13	<b>router bgp autonomous-system-number</b> 例：	BGP ルーティング プロセスを設定します。

	コマンドまたはアクション	目的
	Device(config)# router bgp 1	
ステップ 14	<b>bgp log neighbor changes</b> 例 : Device(config-router)# bgp log neighbor changes	BGP ネイバー リセットのロギングを有効にします。
ステップ 15	<b>address-family ipv4</b> 例 : Device(config-router)# address family ipv4	アドレス ファミリ コンフィギュレーション モードを開始します。
ステップ 16	<b>neighbor ip-address remote-as autonomous-system-number</b> 例 : Device(config-route-af)# neighbor 10.100.1.2 remote-as 1	BGP ネイバー テーブル または マルチプロトコル BGP ネイバー テーブル に エントリ を追加 します。
ステップ 17	<b>neighbor ip-address update-source interface-type interface-number]</b> 例 : Device(config-router-af)# neighbor 10.100.1.2 update-source Loopback0	BGP セッション が、TCP 接続 の動作 インターフェイス を使用 できるよう に します。
ステップ 18	<b>neighbor ip-address next-hop-self all</b> 例 : Device(config-router-af)# neighbor 10.100.1.2 next-hop-self all	ルータ を BGP スピーキング ネイバー または ピア グループ のネクストホップ として 設定 します。
ステップ 19	<b>neighbor ip-address send-label</b> 例 : Device(config-router-af)# neighbor 10.100.1.2 send-label	BGP ルート とともに MPLS ラベル を ネイバー BGP ルータ に送信 できるよう に BGP ルータ を設定 します。
ステップ 20	<b>neighbor ip-address remote-as autonomous-system-number</b> 例 : Device(config-router-af)# neighbor 10.100.1.4 remote-as 1	BGP ネイバー テーブル または マルチプロトコル BGP ネイバー テーブル に エントリ を追加 します。
ステップ 21	<b>neighbor ip-address update-source interface-type interface-number]</b> 例 : Device(config-router-af)# neighbor 10.100.1.4 update-source Loopback0	BGP セッション が、TCP 接続 の動作 インターフェイス を使用 できるよう に します。

	コマンドまたはアクション	目的
ステップ 22	<b>neighbor ip-address route-reflector-client</b> 例： Device(config_router-af)# neighbor 10.100.1.4 route-reflector-client	ルータを BGP ルートリフレクタとして設定し、指定したネイバーをそのクライアントとして設定します。
ステップ 23	<b>neighbor ip-address next-hop-self all</b> 例： Device(config-router-af)# neighbor 10.100.1.4 next-hop-self all	ルータを BGP スピーキングネイバーまたはピアグループのネクストホップとして設定します。
ステップ 24	<b>neighbor ip-address send-label</b> 例： Device(config-router-af)# neighbor 10.100.1.4 send-label	BGP ルートとともに MPLS ラベルをネイバー BGP ルータに送信できるように BGP ルータを設定します。
ステップ 25	<b>exit</b> 例： Device(config-router)# exit	コンフィギュレーションモードを終了します。
ステップ 26	<b>ip prefix-list name seq number permit prefix</b> 例： Device(config)# ip prefix-list prefix-list-ospf1-into-ospf2 seq 5 permit 10.100.1.1/32	IP パケットまたはルートと照合するプレフィックスリストを作成します。
ステップ 27	<b>route-map name permit sequence-number</b> 例： Device(config)# route-map ospf1-into-ospf2 permit 10	ルート マップのエントリを作成します。ルートマップ コンフィギュレーション モードを開始します。
ステップ 28	<b>match ip address prefix-list prefix-list-name</b> 例： Device(config-route-map)# match ip address prefix-list prefix-list-ospf1-into-ospf2	プレフィックスリストで許可された宛先 IP ネットワーク番号アドレスを含むルートを配布します。

## シームレス MPLS の設定例

次の項に、シームレス MPLS の設定例を示します。

## 例：PE ルータ 1 でのシームレス MPLS の設定

次に、PE ルータ 1 でシームレス MPLS を設定する例を示します。

```
Device(config-if)#interface Loopback0
Device(config-if)#ip address 10.100.1.4 255.255.255.255
!
Device(config-if)# interface Ethernet1/0
Device(config-if)# no ip address
Device(config-if)# xconnect 10.100.1.5 100 encapsulation mpls
!
Device(config)# router ospf 2
Device(config-router)# network 10.2.0.0 0.0.255.255 area 0
Device(config-router)# network 10.100.1.4 0.0.0.0 area 0
!
Device(config)#router bgp 1
Device(config-router)# bgp log-neighbor-changes
Device(config-router)# address family ipv4
Device(config-router-af)# network 10.100.1.4 mask 255.255.255.255
Device(config-router-af)# no bgp default ipv4 unicast
Device(config-router-af)# no bgp default route-target filter
Device(config-router-af)# neighbor 10.100.1.1 remote-as 1
Device(config-router-af)# neighbor 10.100.1.1 update-source Loopback0
Device(config-router-af)# neighbor 10.100.1.1 send-label
```

## 例：ルートリフレクタ 1 でのシームレス MPLS の設定

次に、ルートリフレクタ 1 にシームレス MPLS を設定する例を示します。

```
Device(config-if)# interface Loopback0
Device(config-if)# ip address 10.100.1.1 255.255.255.255
Device(config)# router ospf 1
Device(config-router)# network 10.1.0.0 0.0.255.255 area 0
Device(config-router)# network 10.100.1.1 0.0.0.0 area 0
!
Device(config)# router ospf 2
Device(config-router)# redistribute ospf 1 subnets match internal route-map
ospf1-into-ospf2
Device(config-router)# network 10.2.0.0 0.0.255.255 area 0
!
Device(config)# router bgp 1
Device(config-router)# bgp log-neighbor-changes
Device(config-router)# address family ipv4
Device(config-router-af)# neighbor 10.100.1.2 remote-as 1
Device(config-router-af)# neighbor 10.100.1.2 update-source Loopback0
Device(config-router-af)# neighbor 10.100.1.2 next-hop-self all
Device(config-router-af)# neighbor 10.100.1.2 send-label
Device(config-router-af)# neighbor 10.100.1.4 remote-as 1
Device(config-router-af)# neighbor 10.100.1.4 update-source Loopback0
Device(config-router-af)# neighbor 10.100.1.4 route-reflector-client
Device(config-router-af)# neighbor 10.100.1.4 next-hop-self all
Device(config-router-af)# neighbor 10.100.1.4 send-label

Device(config)# ip prefix-list prefix-list-ospf1-into-ospf2 seq 5 permit 10.100.1.1/32

Device(config)# route-map ospf1-into-ospf2 permit 10
Device(config-route-map)# match ip address prefix-list prefix-list-ospf1-into-ospf2
```

## 例：PE ルータ 2 でのシームレス MPLS の設定

次に、PE ルータ 2 でシームレス MPLS を設定する例を示します。

```
Device(config-if)#interface Loopback0
Device(config-if)#ip address 10.100.1.5 255.255.255.255
!
Device(config-if)# interface Ethernet1/0
Device(config-if)# no ip address
Device(config-if)# xconnect 10.100.1.4 100 encapsulation mpls
!
Device(config)# router ospf 3
Device(config-router)# network 10.3.0.0 0.0.255.255 area 0
Device(config-router)# network 10.100.1.5 0.0.0.0 area 0
!
Device(config)#router bgp 1
Device(config-router)# bgp log-neighbor-changes
Device(config-router)# address family ipv4
Device(config-router-af)# network 10.100.1.5 mask 255.255.255.255
Device(config-router-af)# no bgp default ipv4 unicast
Device(config-router-af)# no bgp default route-target filter
Device(config-router-af)# neighbor 10.100.1.2 remote-as 1
Device(config-router-af)# neighbor 10.100.1.2 update-source Loopback0
Device(config-router-af)# neighbor 10.100.1.2 send-label
```

## 例：ルートリフレクタ 2 でのシームレス MPLS の設定

次に、ルートリフレクタ 2 にシームレス MPLS を設定する例を示します。

```
Device(cofig-if)# interface Loopback0
Device(cofig-if)# ip address 10.100.1.2 255.255.255.255
Device(config)# router ospf 1
Device(config-router)# network 10.1.0.0 0.0.255.255 area 0
Device(config-router)# network 10.100.1.2 0.0.0.0 area 0
!
Device(config)# router ospf 3
Device(config-router)# redistribute ospf 1 subnets match internal route-map
ospf1-into-ospf3
Device(config-router)# network 10.3.0.0 0.0.255.255 area 0
!
Device(config)# router bgp 1
Device(config-router)# bgp log-neighbor-changes
Device(config-router)# address family ipv4
Device(config-router-af)# neighbor 10.100.1.1 remote-as 1
Device(config-router-af)# neighbor 10.100.1.1 update-source Loopback0
Device(config-router-af)# neighbor 10.100.1.1 next-hop-self all
Device(config-router-af)# neighbor 10.100.1.1 send-label
Device(config-router-af)# neighbor 10.100.1.5 remote-as 1
Device(config-router-af)# neighbor 10.100.1.5 update-source Loopback0
Device(config-router-af)# neighbor 10.100.1.5 route-reflector-client
Device(config-router-af)# neighbor 10.100.1.5 next-hop-self all
Device(config-router-af)# neighbor 10.100.1.5 send-label

Device(config)# ip prefix-list prefix-list-ospf1-into-ospf3 seq 5 permit 10.100.1.1/32

Device(config)# route-map ospf1-into-ospf3 permit 10
Device(conifg-route-mao)# match ip address prefix-list prefix-list-ospf1-into-ospf3
```

## シームレス MPLS の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Gibraltar 16.12.1	シームレスな MPLS	シームレス MPLS は、複数のネットワークを単一の MPLS ドメインに統合するための、非常に柔軟でスケーラブルなアーキテクチャを提供します。これは、既存の既知のプロトコルに基づいています。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



## 翻訳について

このドキュメントは、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。