MPLS：レイヤ 3 コンフィギュレーション ガイド

初版：2012 年 11 月 05 日

最終更新：2013 年 07 月 30 日

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

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

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

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)

© 2013-2014 Cisco Systems, Inc. All rights reserved.

目 次

最初にお読みください 1

MPLS バーチャル プライベート ネットワーク 3

機能情報の確認 3

MPLS バーチャル プライベート ネットワークの前提条件 4

MPLS バーチャル プライベート ネットワークの制約事項 4

MPLS バーチャル プライベート ネットワークに関する情報 6

MPLS バーチャル プライベート ネットワークの定義 6

MPLS バーチャル プライベート ネットワークの仕組み 8

MPLS バーチャル プライベート ネットワークでの Virtual Routing and Forwarding テーブルの仕組み 8

MPLS バーチャル プライベート ネットワークにおける VPN ルーティング情報の配布方法 9

MPLS 転送 9

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 9

MPLS バーチャル プライベート ネットワークの利点 10

MPLS バーチャル プライベート ネットワークの設定方法 13

コア ネットワークの設定 13

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 13

コアにおける MPLS の設定 14

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 14

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 14

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 16

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 17

RIPv2 を PE デバイスと CE デバイス間のルーティング プロトコルに設定 18

PE デバイスと CE デバイス間のスタティック ルートの設定 20

バーチャル プライベート ネットワークの設定の確認 21

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 22

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 22
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 23
MPLS バーチャル プライベート ネットワーク（VPN）の設定例 24
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 24
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 25
その他の参考資料 26
MPLS バーチャル プライベート ネットワークの機能情報 27
Multiprotocol BGP MPLS VPN 29
機能情報の確認 29
Multiprotocol BGP MPLS VPN の前提条件 30
Multiprotocol BGP MPLS VPN に関する情報 30
MPLS バーチャル プライベート ネットワークの定義 30
MPLS バーチャル プライベート ネットワークの仕組み 31
MPLS バーチャル プライベート ネットワークでの Virtual Routing and Forwarding テーブルの仕組み 31
MPLS バーチャル プライベート ネットワークにおける VPN ルーティング情報の配布方法 32
VPN ルーティング情報の BGP 配布 32
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 33
Multiprotocol BGP MPLS VPN の設定方法 34
PE デバイスおよびルート リフレクタでのマルチプロトコル BGP 接続の設定 34
トラブルシューティングのヒント 36
BGP を PE デバイスと CE デバイス間のルーティング プロトコルに設定 36
バーチャル プライベート ネットワークの設定の確認 38
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 38
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 39
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 39
Multiprotocol BGP MPLS VPN の設定例 41
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 41

その他の参考資料 42
Multiprotocol BGP MPLS VPN の機能情報 42
MPLS VPN OSPF PE および CE サポート 45
機能情報の確認 45
MPLS VPN OSPF PE および CE サポートの前提条件 46
MPLS VPN OSPF PE および CE サポートに関する情報 46
MPLS VPN OSPF PE および CE サポートの概要 46
MPLS VPN OSPF PE および CE サポートの設定方法 46
OSPF を PE デバイスと CE デバイス間のルーティング プロトコルに設定 46
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 49
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 49
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 50
MPLS VPN OSPF PE および CE サポートの設定例 51
例：OSPF を使用した MPLS VPN の設定 51
その他の参考資料 52
MPLS VPN OSPF PE および CE サポートの機能情報 52
MPLS VPN による PE および CE 間の EIGRP サポート 55
機能情報の確認 55
MPLS VPN による PE および CE 間の EIGRP サポートの前提条件 56
MPLS VPN による PE および CE 間の EIGRP サポートについての情報 56
MPLS VPN による PE および CE 間の EIGRP サポートの概要 56
MPLS VPN による PE および CE 間の EIGRP サポートの設定方法 56
EIGRP を PE デバイスと CE デバイス間のルーティング プロトコルに設定 56
MPLS VPN における EIGRP 再配布の設定 59
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 61
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 62
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 62
MPLS VPN による PE および CE 間の EIGRP サポートの設定例 64
例：EIGRP を使用した MPLS VPN の設定 64
その他の参考資料 65

MPLS VPN による PE および CE 間の EIGRP サポートの機能情報 65

IPv6 VPN over MPLS 67

機能情報の確認 67

IPv6 VPN over MPLS の前提条件 68

IPv6 VPN over MPLS の制約事項 68

IPv6 VPN over MPLS に関する情報 68

IPv6 VPN over MPLS の概要 68

IPv6 VPN over MPLS のアドレッシングの考慮事項 69

IPv6 VPN over MPLS の基本的な機能 70

IPv6 VPN アーキテクチャの概要 70

IPv6 VPN ネクスト ホップ 71

MPLS 転送 71

VRF の概念 72

IPv6 VPN スケーラビリティ 72

IPv6 MPLS VPN の高度な機能 73

Internet Access 73

マルチ自律システム バックボーン 74

Carrier Supporting Carrier 76

IPv6 VPN over MPLS の設定方法 76

IPv6 用の Virtual Routing and Forwarding インスタンスの設定 76

インターフェイスへの VRF のバインド 79

PE から CE へのルーティング用のスタティック ルートの設定 80

eBGP の PE から CE へのルーティング セッションの設定 81

iBGP 用の IPv6 VPN アドレス ファミリの設定 83

スケーラビリティ向上のためのルート リフレクタの設定 84

インターネット アクセスの設定 92

インターネット ゲートウェイの設定 93

VPN PE への iBGP 6PE ピアリングの設定 93

パブリック ドメインへのゲートウェイとしてのインターネット ゲートウェイの設定 94

インターネットへの eBGP ピアリングの設定 96

IPv6 VPN PE の設定 97

VRF からインターネット ゲートウェイへのデフォルト スタティック ルートの設定 97
デフォルト テーブルから VRF へのスタティック ルートの設定 98
インターネット ゲートウェイへの iBGP 6PE ピアリングの設定 99
IPv6 VPN 用のマルチ自律システム バックボーンの設定 101
マルチ自律システム バックボーン用の PE VPN の設定 103
ルート リフレクタへの iBGP IPv6 VPN ピアリングの設定 103
ルート リフレクタへの IPv4 とラベルの iBGP ピアリングの設定 105
マルチ自律システム バックボーン用のルート リフレクタの設定 107
PE VPN へのピアリングの設定 107
ルート リフレクタの設定 109
自律システム境界ルータとのピアリングの設定 112
別の ISP ルート リフレクタとのピアリングの設定 113
ASBR の設定 116
ルート リフレクタ RR1 とのピアリングの設定 116
他の ISP ASBR2 とのピアリングの設定 118
IPv6 VPN 用の CSC の設定 120
IPv6 VPN over MPLS の設定例 122
例：IPv6 VPN over MPLS ルーティング 122
例：BGP IPv6 アクティビティ サマリー 122
例：BGP IPv6 テーブルのダンプ 122
例：IPv6 ルーティング テーブルのダンプ 122
例：IPv6 VPN over MPLS フォワーディング 123
例：PE-CE 接続 123
例：PE インポジション パス 124
例：PE ディスポジション パス 125
例：ラベル スイッチ パス 125
例：IPv6 VPN over MPLS VRF 126
例：VRF 情報 126
例：IPv4 ネクスト ホップを使用した IPv6 VPN の設定 127
その他の参考資料 127
IPv6 VPN over MPLS の機能情報 128

用語集 130

MPLS VPN への ID 番号の割り当て 133

機能情報の確認 133

MPLS VPN ID の制約事項 134

MPLS VPN ID に関する情報 134

MPLS VPN ID の概要 134

MPLS VPN ID の構成要素 134

MPLS VPN ID を使用する管理アプリケーション 135

Dynamic Host Configuration Protocol 135

リモート認証ダイヤルイン ユーザ サービス 135

MPLS VPN ID の設定方法 136

MPLS VPN ID の指定 136

MPLS VPN ID 設定の確認 137

MPLS VPN への ID 番号の割り当ての設定例 138

例：MPLS VPN ID の指定 138

例：MPLS VPN ID の設定の確認 139

その他の参考資料 139

MPLS VPN ID の機能情報 140

リモート アクセス MPLS VPN 143

機能情報の確認 143

リモート アクセス MPLS VPN の前提条件 144

リモート アクセス MPLS VPN の制約事項 144

リモート アクセス MPLS VPN に関する情報 144

リモート アクセス MPLS VPN の概要 144

MPLS VPN アーキテクチャ 145

MPLS VPN への PPP over Ethernet 146

リモート アクセス MPLS VPN の設定方法 147

MPLS コア ネットワークの設定 147

PPPoE の設定 148

仮想テンプレート インターフェイスの設定 148

ブロードバンド アグリゲーション グループでの PPPoE の設定 149

バーチャル プライベート ネットワークの設定と関連付け 151

リモート アクセス MPLS VPN の設定例 151
例：PPPoE セッション用の 1 つの VRF を使用したリモート アクセス MPLS VPN の設定 151
その他の参考資料 153
リモート アクセス MPLS VPN の機能情報 154
用語集 155
Multi-VRF サポート 157
機能情報の確認 157
Multi-VRF サポートの前提条件 158
Multi-VRF サポートの制約事項 158
Multi-VRF サポートに関する情報 158
Multi-VRF サポート機能の動作 158
Multi-VRF サポート機能を使用してネットワークでパケットが転送されるしくみ 159
Multi-VRF サポート機能を設定する場合の考慮事項 160
Multi-VRF サポートの設定方法 161
VRF の設定 161
ルーティング プロトコルとしての BGP の設定 163
PE から CE への MPLS 転送およびシグナリングで BGP を使用する場合の設定 165
BGP 以外のルーティング プロトコルの設定 168
PE から CE への MPLS 転送およびシグナリングで LDP を使用する場合の設定 170
Multi-VRF サポートの設定例 170
例：PE デバイスでの Multi-VRF サポートの設定 171
例：CE デバイスでの Multi-VRF サポートの設定 172
その他の参考資料 173
Multi-VRF サポートの機能情報 174
ポリシーベース ルーティングを使用した Multi-VRF 選択 175
機能情報の確認 176
ポリシーベース ルーティングを使用した Multi-VRF 選択の前提条件 176
ポリシーベース ルーティングを使用した Multi-VRF 選択の制限事項 176
ポリシーベース ルーティングを使用した Multi-VRF 選択に関する情報 177
一致基準に基づいた VPN トラフィックのポリシー ルーティング 177
ポリシーベース ルーティングの set コマンド 178

VRF インスタンスのポリシールーティング パケット 178
通常のルーティングおよび転送動作の変更 179
継承 VRF、VRF 間、および VRF からグローバルへのルーティングのサポート 180
ポリシーベース ルーティングを使用した Multi-VRF 選択の設定方法 181
ポリシーベース ルーティングを使用した Multi-VRF 選択の一致基準の定義 181
標準アクセス リストとともにポリシーベース ルーティングを使用した Multi-VRF 選択の設定 182
名前付き拡張アクセスリストとともにポリシーベースルーティングを使用した Multi-VRF 選択の設定 183
ルート マップでの Multi-VRF 選択の設定 184
インターフェイスでポリシーベース ルーティングと IP VRF 受信を使用した Multi-VRF 選択の設定 187
ポリシーベース ルーティングを使用した Multi-VRF 選択の設定の確認 188
ポリシーベース ルーティングを使用した Multi-VRF 選択の設定例 191
例：ポリシーベース ルーティングを使用した Multi-VRF 選択の一致基準の定義 191
例：ルート マップでの Multi-VRF 選択の設定 191
その他の参考資料 192
ポリシーベース ルーティングを使用した Multi-VRF 選択の機能情報 192
用語集 194
ポリシーベース ルーティングを使用した MPLS VPN VRF 選択 195
機能情報の確認 195
ポリシーベース ルーティングを使用した MPLS VPN VRF 選択の前提条件 196
ポリシーベース ルーティングを使用した MPLS VPN VRF 選択の制約事項 196
ポリシーベース ルーティングを使用した MPLS VPN VRF 選択に関する情報 197
ポリシーベース ルーティングを使用した MPLS VPN VRF 選択の概要 197
ポリシーベース ルーティングの set 句：概要 197
パケット長に基づくポリシーベース ルーティング VRF 選択の一致基準 198
ポリシーベース ルーティングを使用した MPLS VPN VRF 選択の設定方法 198
標準アクセス リストを使用した ポリシーベース ルーティング VRF 選択の設定 198

名前付きアクセス リストを使用した ポリシーベース ルーティング VRF 選択の設定 199
ルート マップでのポリシーベース ルーティング VRF 選択の設定 201
インターフェイスでのポリシーベース ルーティングの設定 203
インターフェイスでの IP VRF Receive の設定 204
ポリシーベース ルーティングを使用した MPLS VPN VRF 選択の設定の確認 206
ポリシーベース ルーティングを使用した MPLS VPN VRF 選択の設定例 207
例：アクセス リストでのポリシーベース ルーティング VRF 選択の定義 207
例：ポリシーベース ルーティングを使用した VRF 選択の確認 207
例：一致基準の確認 207
例：ルートマップ設定の確認 208
例：ポリシーベース ルーティング VRF 選択ポリシーの確認 208
その他の参考資料 208
ポリシーベース ルーティングを使用した MPLS VPN VRF 選択の機能情報 209
カスタマー エッジ（CE）ラベル単位での MPLS VPN 211
機能情報の確認 211
CE ラベル単位での MPLS VPN の前提条件 212
CE ラベル単位での MPLS VPN の制約事項 212
CE ラベル単位での MPLS VPN に関する情報 213
CE ラベル単位での MPLS VPN 機能 213
CE ラベル単位での MPLS VPN の設定方法 214
CE ラベル単位機能の設定 214
CE ラベル単位での MPLS VPN の設定例 215
例：CE ラベル単位での MPLS VPN 215
その他の参考資料 216
CE ラベル単位での MPLS VPN の機能情報 216
VRF 認識システム メッセージ ロギング 219
機能情報の確認 219
VRF 認識システム メッセージ ロギングの前提条件 220
VRF 認識システム メッセージ ロギングの制約事項 220
VRF 認識システム メッセージ ロギングに関する情報 220
VRF 認識システム メッセージ ロギングの利点 220

MPLS VPN ネットワーク内のプロバイダー エッジ デバイス上の VRF 認識システム メッセージ ロギング 221
VRF-Lite が設定されたカスタマー エッジ デバイスでの VRF 認識システム メッセージ ロギング 221
ロギング コマンドのメッセージ レベル 222
VRF 認識システム メッセージ ロギングの設定および確認方法 223
ルーティング デバイスでの VRF の設定 223
VRF とインターフェイスの関連付け 225
ルーティング デバイスでの VRF 認識システム メッセージ ロギングの設定 227
VRF 認識システム メッセージ ロギング操作の確認 229
VRF 認識システム メッセージ ロギングの設定例 231
例：ルーティング デバイスでの VRF の設定 231
例：VRF とインターフェイスの関連付け 231
例：ルーティング デバイスでの VRF 認識システム メッセージ ロギングの設定 231
その他の参考資料 232
VRF 認識システム メッセージ ロギングの機能情報 232
用語集 234
MPLS VPN の実行中の VRF の表示 235
機能情報の確認 235
MPLS VPN の実行中の VRF の表示の前提条件 236
MPLS VPN の実行中の VRF の表示の制約事項 236
MPLS VPN の実行中の VRF の表示に関する情報 236
MPLS VPN の実行中の VRF の表示で表示される設定要素 236
VRF ルーティング プロトコル設定の表示 237
VRF に直接関連していない設定の表示 238
その他の参考資料 238
MPLS VPN の実行中の VRF の表示の機能情報 239
用語集 241
MPLS VPN 半二重 VRF 243
機能情報の確認 243
MPLS VPN 半二重 VRF の前提条件 244

MPLS VPN 半二重 VRF の制約事項 244
MPLS VPN 半二重 VRF に関する情報 244
MPLS VPN 半二重 VRF 概要 244
アップストリーム VRF とダウンストリーム VRF 245
リバース パス転送チェック 246
MPLS VPN 半二重 VRF の設定方法 246
スポーク PE デバイスでのアップストリーム VRF とダウンストリーム VRF の設定 246
VRF とインターフェイスの関連付け 248
AAA サーバ用のダウンストリーム VRF の設定 250
MPLS VPN 半二重 VRF 設定の確認 250
MPLS VPN 半二重 VRF の設定例 254
例：スポーク PE デバイスでのアップストリーム VRF とダウンストリーム VRF の設定 254
例：VRF とインターフェイスの関連付け 254
例：MPLS VPN 半二重 VRF の設定：スタティック CE-PE ルーティングを使用した例 255
例：RADIUS サーバとスタティック CE-PE ルーティングを使用した MPLS VPN 半二重 VRF の設定 256
例：ダイナミック CE-PE ルーティングを使用した MPLS VPN 半二重 VRF の設定 257
その他の参考資料 259
MPLS VPN 半二重 VRF の機能情報 260
MPLS VPN BGP ローカル コンバージェンス 263
機能情報の確認 263
MPLS VPN BGP ローカル コンバージェンスの前提条件 264
MPLS VPN BGP ローカル コンバージェンスの制約事項 264
MPLS VPN BGP ローカル コンバージェンスに関する情報 265
BGP によるリンク障害処理の仕組み 265
MPLS VPN BGP ローカル コンバージェンス機能によるリンク処理の仕組み 266
リンク障害検出の仕組み 267
MPLS VPN BGP ローカル コンバージェンスの設定方法 268

IPv4 による MPLS VPN BGP ローカル コンバージェンスの設定 268
IPv6 での MPLS VPN BGP ローカル コンバージェンスの設定 269
例 271
トラブルシューティングのヒント 272
MPLS VPN BGP ローカル コンバージェンスの設定例 272
例：MPLS VPN BGP ローカル コンバージェンス 272
例：6VPE 6PE の MPLS VPN BGP ローカル コンバージェンス 275
その他の参考資料 278
MPLS VPN BGP ローカル コンバージェンスの機能情報 279
IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI 283
機能情報の確認 283
IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI の前提条件 284
IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI の制約事項 284
IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI に関する情報 284
IPv4 と IPv6 の MPLS VPN で共通の VRF に関する概念 284
単一プロトコル VRF からマルチプロトコル VRF への移行 285
マルチプロトコル VRF 設定の特性 286
IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI の設定方法 287
IPv4 および IPv6 MPLS VPN 用の VRF の設定 287
マルチプロトコル VRF とインターフェイスの関連付け 290
IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI 設定の確認 291
IPv4 だけの単一プロトコル VRF からマルチプロトコル VRF 設定への移行 294
IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI の設定例 296
例：マルチプロトコル VRF 設定、非共通ポリシーを持つ単一プロトコル 296
例：マルチプロトコル VRF 設定、非共通ポリシーを持つマルチプロトコル 297
例：マルチプロトコル VRF 設定、共通ポリシーを持つマルチプロトコル 297
例：マルチプロトコル VRF 設定、共通ポリシーと非共通ポリシーを持つマルチプロトコル 297
例：IPv4 および IPv6 VPN 用の VRF の設定 298
例：マルチプロトコル VRF とインターフェイスの関連付け 298
例：IPv4 だけの単一プロトコル VRF 設定からマルチプロトコル VRF 設定への移行 299

その他の参考資料 300
IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI の機能情報 301
用語集 303
MPLS over GRE 307
機能情報の確認 307
MPLS VPN L3VPN over GRE の前提条件 308
MPLS VPN L3VPN over GRE の制約事項 308
MPLS VPN L3VPN over GRE に関する情報 308
MPLS VPN L3VPN over GRE の概要 308
PE-to-PE トンネリング 309
P-to-PE トンネリング 310
P-to-P トンネリング 310
MPLS VPN L3VPN over GRE の設定方法 311
MPLS over GRE トンネル インターフェイスの設定 311
MPLS VPN L3VPN over GRE の設定例 313
例：非 MPLS ネットワークにまたがる GRE トンネルの設定 313
例：MPLS VPN L3VPN over GRE を使用した MPLS の設定 313
その他の参考資料 314
MPLS VPN L3VPN over GRE の機能情報 315
IP トンネルを介した MPLS VPN 6VPE サポート 317
機能情報の確認 317
IP トンネルを介した MPLS VPN 6VPE のサポートに関する情報 318
MPLS 転送 318
GRE トンネルを介した 6VPE 318
その他の参考資料 319
IP トンネルを介した MPLS VPN 6VPE サポートの機能情報 320
IPv6 VRF 認識システム メッセージ ロギング 321
機能情報の確認 321
IPv6 VRF 認識システム メッセージ ロギングの前提条件 322
IPv6 VRF 認識システム メッセージ ロギングの制約事項 322
IPv6 VRF 認識システム メッセージ ロギングに関する情報 322
VRF 認識システム メッセージ ロギングの利点 322

MPLS VPN ネットワーク内のプロバイダー エッジ デバイス上の VRF 認識システム メッセージ ロギング 323
VRF-Lite が設定されたカスタマー エッジ デバイスでの VRF 認識システム メッセージ ロギング 323
ロギング コマンドのメッセージ レベル 324
IPv6 VRF 認識システム メッセージ ロギングの設定方法 325
ルーティング デバイスでの VRF の設定 325
VRF とインターフェイスの関連付け 326
ルーティング デバイスでのロギングの送信元インターフェイスとして VRF を設定 328
IPv6 VRF 認識システム メッセージ ロギングの確認 329
IPv6 VRF 認識システム メッセージ ロギングの設定例 330
例：ルーティング デバイスでの VRF の設定 330
例：VRF とインターフェイスの関連付け 330
例：ルーティング デバイス上でのロギングの送信元インターフェイスとしての VRF の設定 330
IPv6 VRF 認識システム メッセージ ロギングのその他の参考資料 331
IPv6 VRF 認識システム メッセージ ロギングの機能情報 332

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

Cisco IOS XE Release 3.7.0E（Catalyst スイッチ用）および Cisco IOS XE Release 3.17S（アクセスおよびエッジ ルーティング用）の 2 つのリリースが、集約された単一のリリース バージョンとして Cisco IOS XE 16 に統合され、進化しました。スイッチングおよびルーティングのポートフォリオに含まれる幅広いアクセス製品とエッジ製品を盛り込んだ単一のリリースが実現します。

（注） 技術構成ガイドにある機能情報の表には、その機能がいつ導入されたかが記載されています。その機能で他のプラットフォームがいつサポートされるようになったかについては、記載されている場合とされていない場合があります。特定の機能がご使用のプラットフォームでサポートされているかどうかを確認するには、製品のランディング ページに掲載されている技術構成ガイドを参照してください。ご使用の製品のランディング ページに技術構成ガイドが表示されていれば、機能はそのプラットフォームでサポートされていることを意味します。

第 2 章

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。この章では、MPLS VPN の作成方法について説明します。

- 機能情報の確認，3 ページ
- MPLS バーチャル プライベート ネットワークの前提条件，4 ページ
- MPLS バーチャル プライベート ネットワークの制約事項，4 ページ
- MPLS バーチャル プライベート ネットワークに関する情報，6 ページ
- MPLS バーチャル プライベート ネットワークの設定方法，13 ページ
- MPLS バーチャル プライベート ネットワーク（VPN）の設定例，24 ページ
- その他の参考資料，26 ページ
- MPLS バーチャル プライベート ネットワークの機能情報，27 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 に移動します。Cisco.com のアカウントは必要ありません。

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。
- Cisco Express Forwarding は、PE デバイスを含め、コア内のすべてのデバイスでイネーブルにする必要があります。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」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。これらのコマンド バリエーションは、タグ転送情報ベース（TFIB）をサポートするソフトウェア リリースではサポートされていません。プレフィックスが通過する再帰ルートがいったん失われて再び現れる場合、TFIB はプレフィックスを解決できません。ただし、MPLS Forwarding Infrastructure（MFI）をサポートするリリースでは、これらのコマンド バリエーションがサポートされています。サポートされているリリースの詳細については、『*Multiprotocol Label Switching Command Reference*』を参照してください。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は、次の **ip route** コマンドがサポートされます。

- **ip route***destination-prefixmaskinterfacenext-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発信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は、次の **ip route** コマンドがサポートされます。

- **ip route***destination-prefixmask***interface1next-hop1**
- **ip route***destination-prefixmask***interface2next-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は、次の **ip route** コマンドがサポートされません。

- **ip route***destination-prefixmasknext-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 シェアリングをイネーブルにする場合は、次の **ip route** コマンドがサポートされません。

- **ip route***destination-prefixmasknext-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 シェアリングをイネーブルにする場合は、次の **ip route** コマンドがサポートされません。

- **ip route***destination-prefixmask***next-hop1**
- **ip route***destination-prefixmask***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-namedestination-prefixmasknext-hop-address*
- **ip route vrf***vrf-namedestination-prefixmaskinterfacenext-hop-address*
- **ip route vrf***vrf-namedestination-prefixmask***interface1next-hop1**
- **ip route vrf***vrf-namedestination-prefixmask***interface2next-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は、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-namedestination-prefixmasknext-hop-address***global**
- **ip route vrf***vrf-namedestination-prefixmaskinterfacenext-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発信インターフェイスを使用するロード シェアリングをイネーブルにする場合は、次の **ip route** コマンドがサポートされます。

- **ip route***destination-prefixmask***interface1next-hop1**
- **ip route***destination-prefixmask***interface2next-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 シェアリングをイネーブルにする場合は、次の **ip route** コマンドがサポートされません。

- **ip route vrf***destination-prefixmasknext-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 シェアリングをイネーブルにする場合は、次の **ip route** コマンドがサポートされません。

- **ip route vrf***destination-prefixmask***next-hop1global**
- **ip route vrf***destination-prefixmask***next-hop2global**

MPLS VPN 環境でスタティック ルートを設定し、ネクスト ホップおよびインターフェイスが同じ VRF にある場合は、次の **iproutevrf** コマンドがサポートされません。

- **ip route vrf***vrf-namedestination-prefixmask***next-hop1***vrf-namedestination-prefixmask***next-hop1**
- **ip route vrf***vrf-namedestination-prefixmask***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は、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-namedestination-prefixmaskinterfacenext-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発信インターフェイスを使用するロード シェアリングをイネーブルにする場合は、次の **ip route** コマンドがサポートされます。

- **ip route***destination-prefixmask***interface1nexthop1**
- **ip route***destination-prefixmask***interface2nexthop2**

MPLS バーチャル プライベート ネットワークに関する情報

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。

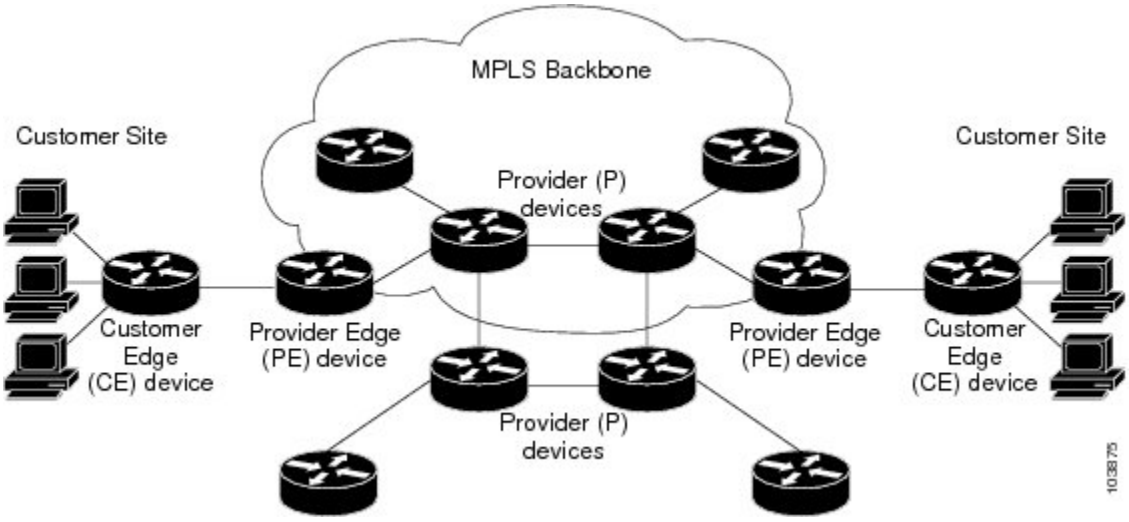
MPLS VPN の管理や拡張は、従来の VPN よりも簡単です。新しいサイトが MPLS VPN に追加された場合、更新する必要があるのは、カスタマーサイトにサービスを提供するサービスプロバイダーのエッジ デバイスだけです。

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 ネットワークでの Virtual Routing and Forwarding テーブルの仕組み

各バーチャル プライベート ネットワーク（VPN）は、1 つ以上の Virtual Routing and Forwarding（VRF）インスタンスに関連付けられています。VRF では、PE デバイスに接続されているカスタマー サイトの VPN メンバーシップを定義します。VRF は、次のコンポーネントで構成されています。

- IP ルーティング テーブル
- 取得した Cisco Express Forwarding テーブル
- 転送テーブルを使用する一連のインターフェイス
- ルーティング テーブルに格納されている情報を制御するための一連のルールおよびルーティング プロトコル パラメータ

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 つのサイトを複数の VPNs 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。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。

パケット転送情報は、VRF ごとに IP ルーティング テーブルおよび Cisco Express Forwarding テーブルに格納されます。各 VRF カスタマーに対して、別個の一連のルーティング テーブルおよび Cisco Express Forwarding テーブルが維持されます。これらのテーブルにより、VPN の外側に情報が転送されないようになっているほか、VPN の外側のパケットも VPN 内のデバイスに転送されないようになっています。

MPLS バーチャル プライベート ネットワークにおける VPN ルーティング情報の配布方法

バーチャルプライベート ネットワーク（VPN）ルーティング情報の配布は、Border Gateway Protocol（BGP）拡張コミュニティによって実装される VPN ルート ターゲット コミュニティを使用して制御されます。VPN ルーティング情報は、次のように配布されます。

- カスタマー エッジ（CE）デバイスから学習した VPN ルートが BGP に注入されると、VPN ルート ターゲット拡張コミュニティ属性のリストが、そのルートに関連付けられます。通常、ルート ターゲット コミュニティ拡張値のリストは、ルートの学習元の Virtual Routing and Forwarding（VRF）インスタンスに関連付けられているルート ターゲットのエクスポート リストから設定されます。
- ルート ターゲット拡張コミュニティのインポート リストは、各 VRF に関連付けられています。インポート リストには、ルートが VRF にインポートされるために、ルートに設定されている必要のある、ルート ターゲット拡張コミュニティ属性が定義されています。たとえば、ある特定の VRF のインポート リストにルート ターゲット拡張コミュニティ A、B、および C が含まれている場合、これらのルート ターゲット拡張コミュニティ A、B、または C のいずれかを伝送するすべての VPN ルートが VRF にインポートされます。

MPLS 転送

Virtual Routing and Forwarding（VRF）IP ルーティング テーブルおよび VRF Cisco Express Forwarding テーブルに格納されているルーティング情報に基づき、マルチプロトコル ラベル スイッチング（MPLS）を使用してパケットが宛先に転送されます。

プロバイダー エッジ（PE）デバイスでは、カスタマー エッジ（CE）デバイスから学習した各カスタマープレフィックスにラベルをバインドし、他の PE デバイスにアドバタイズするプレフィックスのネットワーク到達可能性情報に、そのラベルを含めます。PE デバイスは、プロバイダー ネットワークを介して CE デバイスから受信したパケットを転送するときに、宛先 PE デバイスから学習したラベルを使用してパケットにラベルを付けます。宛先 PE デバイスは、ラベルの付いたパケットを受信すると、そのラベルをポップし、パケットを正しい CE デバイスに誘導するために使用します。プロバイダー バックボーン経由のラベル転送は、ダイナミック ラベル スイッチングまたはトラフィック エンジニアリング パスのいずれかに基づきます。バックボーンを通過するカスタマー データ パケットが伝達するラベルには、2 つのレベルがあります。

- 最上位ラベルによって、パケットが正しい PE デバイスに誘導されます。
- 2 番めのラベルは、PE デバイスがパケットを CE デバイスに転送する方法を示します。

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に Virtual Routing and 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 を展開し、次のような付加価値サービスを提供する基盤を構築できます。

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ことができます。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 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だけではありません。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。カスタマーがそ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、スケーラビリティが重要となります。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、複数組み合わせて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 のその他のスケーラビリティ機能は、PE デバイス間での VPN ルートのパーティショニング、およびコア 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 と Interior Gateway Protocol（IGP）ルートのパーティショニングから得られます。

- 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、カスタマー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、カスタマー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 ラ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 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 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 プロバイダーのカスタマーは、サービス プロバイダーのその他のカスタマーのアドレッシング計画とは関係なく、独自のアドレッシング計画を設計できます。多くのカスタマーは、RFC 1918 で定義されているようにプライベート アドレス空間を使用しており、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、カスタマーは、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たあとに、加入者によって定義されたポリシーに従って集約され、プロバイダーで実行され、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 の独自な特長として、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ことができます。

CEデバイス上でMPLSをサポートする必要がなく、カスタマーのイントラネットに変更を加える必要がないため、エンド ユーザの移行作業は簡単になります。

MPLS バーチャル プライベート ネットワークの設定方法

コア ネットワークの設定

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。

手順の概要

1. ネットワークのサイズを識別します。
2. コアにおけるルーティング プロトコルを識別します。
3. MPLS VPN ハイ アベイラビリティのサポートが必要であるかどうかを判断します。
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であるかどうかを決定します。

手順の詳細

	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。 • サポートする必要があるカスタマーの数 • カスタマーごとに必要となる VPN の数 • 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
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である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て、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。

	コマンドまたはアクション	目的
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であるかどうかを決定します。	設定手順については、『*MPLS Layer 3 VPNs Inter-AS and CSC Configuration Guide*』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 トラフィック エンジニアリング リソース予約プロトコル（RSVP）。設定については、『*MPLS Traffic Engineering Path Calculation and Setup Configuration Guide*』の「MPLS Traffic Engineering and Enhancements」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

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 Virtual Routing and Forwarding（VRF）設定を定義します。IPv4 と IPv6 の VRF を定義するには、『*MPLS Layer 3 VPNs Configuration Guide*』の「IPv6 VPN over MPLS」モジュールの「Configuring a Virtual Routing and Forwarding Instance for IPv6」セクションを参照してください。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **ip vrf***vrf-name*
4. **rd***route-distinguisher*
5. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
6. **import map***route-map*
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**イネーブル化** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**ip vrf***vrf-name* 例： `Device(config)# ip vrf vpn1`	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。 • *vrf-name* 引数は、VRF に割り当てる名前です。

ステップ 4	**rd***route-distinguisher*
	
	例：
	`Device(config-vrf)# rd 100:1`
		ルーティング テーブルと転送テーブルを作成します。
		
		• *route-distinguisher* 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。
		
		  • 16 ビットの AS 番号：32 ビットの番号。101:3 など。
		
		  • 32 ビットの IP アドレス：16 ビットの番号。10.0.0.1:1 など。

ステップ 5	**route-target** {**import** | **export** | **both**} *route-target-ext-community* 例： `Device(config-vrf)# route-target import 100:1`	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。 • **import** 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。 • **export** 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。 • **both** 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。 • *route-target-ext-community* 引数により、route-target 拡張コミュニティ属性が、インポートやエクスポートの route-target 拡張コミュニティの VRF リストに追加されます。

	コマンドまたはアクション	目的
ステップ 6	**import map***route-map* 例： `Device(config-vrf)# import map vpn1-route-map`	（任意）VRF のインポート ルート マップを設定します。 • *route-map* 引数は、VRF のインポート ルート マップとして使用されるルート マップを指定します。
ステップ 7	**exit** 例： `Device(config-vrf)# exit`	（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 Virtual Routing and Forwarding（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。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***typenumber*
4. **ip vrf forwarding***vrf-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**interface***typenumber* 例： `Device(config)# interface FastEthernet 1/0/0`	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。 • *type* 引数には、設定するインターフェイスのタイプを指定します。 • *number* 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	**ip vrf forwarding***vrf-name* 例： `Device(config-if)# ip vrf forwarding vpn1`	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。 • *vrf-name* 引数は、VRF に割り当てる名前です。
ステップ 5	**end** 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。Border Gateway Protocol（BGP）、Routing Information Protocol バージョン 2（RIPv2）、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。

RIPv2 を PE デバイスと CE デバイス間のルーティング プロトコルに設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router rip**
4. **version** {**1** | **2**}
5. **address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*]
6. **network***ip-address*
7. **redistribute***protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric***metric-value*] [**metric-type***type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag***tag-value*] [**route-map***map-tag*] [**subnets**]
8. **exit-address-family**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router rip** 例： `Device(config)# router rip`	Routing Information Protocol（RIP）を有効にします。
ステップ 4	**version** {**1** | **2**} 例： `Device(config-router)# version 2`	デバイスでグローバルに使用される RIP のバージョンを指定します。

	コマンドまたはアクション	目的
ステップ 5	**address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*] 例： `Device(config-router)# address-family ipv4 vrf vpn1`	IPv4 アドレス ファミリ タイプを指定し、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。 • **multicast** キーワードは、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。 • **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。 • **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 VRF の名前を指定します。
ステップ 6	**network***ip-address* 例： `Device(config-router-af)# network 192.168.7.0`	PE から CE へのリンク上で RIP をイネーブルにします。
ステップ 7	**redistribute***protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric***metric-value*] [**metric-type***type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag***tag-value*] [**route-map***map-tag*] [**subnets**] 例： `Device(config-router-af)# redistribute bgp 200`	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。 • RIPv2 ルーティング プロトコルの場合、**redistribute bgp***as-number* コマンドを使用します。
ステップ 8	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	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。
ステップ 9	**end** 例： `Device(config-router)# 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 デバイス間のスタティック ルートの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **ip route vrf***vrf-name*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*]
5. **redistribute***protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric***metric-value*] [**metric-type***type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag***tag-value*] [**route-map***map-tag*] [**subnets**]
6. **redistribute***protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric***metric-value*] [**metric-type***type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag***tag-value*] [**route-map***map-tag*] [**subnets**]
7. **exit-address-family**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**ip route vrf***vrf-name* 例： `Device(config)# ip route vrf 200`	すべてのプロバイダー エッジからカスタマー エッジへの（PE-to-CE）セッションのスタティック ルート パラメータを定義し、ルータ 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	**address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*] 例： `Device(config-router)# address-family ipv4 vrf vpn1`	IPv4 アドレス ファミリ タイプを指定し、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。 • **multicast** キーワードは、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。 • **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。

	コマンドまたはアクション	目的
		• **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 VRF の名前を指定します。
ステップ 5	**redistribute***protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric***metric-value*] [**metric-type***type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag***tag-value*] [**route-map***map-tag*] [**subnets**] 例： `Device(config-router-af)# redistribute static`	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。 • Virtual Routing and Forwarding（VRF）スタティック ルートを VRF Border Gateway Protocol（BGP）テーブルに再配布するには、**redistribute static** コマンドを使用します。 その他の引数とキーワードについては、コマンド リファレンス ページを参照してください。
ステップ 6	**redistribute***protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric***metric-value*] [**metric-type***type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag***tag-value*] [**route-map***map-tag*] [**subnets**] 例： `Device(config-router-af)# redistribute connected`	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。 • 直接接続ネットワークを VRF BGP テーブルに再配布するには、**redistribute connected** コマンドを使用します。
ステップ 7	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	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。
ステップ 8	**end** 例： `Device(config-router)# end`	（任意）終了して、特権 EXEC モードに戻ります。

バーチャル プライベート ネットワークの設定の確認

ルート識別子を Virtual Routing and Forwarding（VRF）インスタンス用に設定する必要があります。また、VRF を伝送するインターフェイス上でマルチプロトコル ラベル スイッチング（MPLS）を

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。

手順の概要

1. **show ip vrf**

手順の詳細

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

手順の概要

1. イネーブル化
2. **ping** [*protocol*] {*host-name* | *system-address*}
3. **trace** [*protocol*] [*destination*]
4. **show ip route** [*ip-address* [*mask*] [**longer-prefixes**]] | *protocol* [*process-id*]] | [**list** [*access-list-name* | *access-list-number*]

手順の詳細

ステップ 1 イネーブル化
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、ある CE デバイスから別の CE デバイスへ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ある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

手順の概要

1. イネーブル化
2. **show ip route vrf***vrf-name* [*prefix*]
3. **show ip cef vrf***vrf-name* [*ip-prefix*]

手順の詳細

ステップ 1 イネーブル化
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 Routing and Forwarding（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。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シスコ エクスプレス フォワーディング 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

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
ip 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 FastEthernet0/0/0 ip vrf forwarding vpn1 ip address 192.0.2.3 255.255.255.0 no cdp enable interface FastEthernet1/1/0 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	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 FastEthernet0/0/0 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

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
ip 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 FastEthernet0/0/0 ip vrf forwarding vpn1 ip address 192.0.2.3 255.255.255.0 no cdp enable ! interface FastEthernet1/1/0 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	ip cef ! interface Loopback0 ip address 10.0.0.9 255.255.255.255 ! interface FastEthernet0/0/0 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

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 Command List, All Releases』
MPLS および MPLS アプリケーションに関連するコマンドの説明	『Cisco IOS Multiprotocol Label Switching Command Reference』
Cisco Express Forwarding の設定	『*Cisco Express Forwarding Configuration Guide*』の「Configuring Basic Cisco Express Forwarding」モジュール
Border Gateway Protocol（BGP）ロード シェアリング	『*MPLS Layer 3 VPNs Inter-AS and CSC Configuration Guide*』の「Load Sharing MPLS VPN Traffic」モジュール
LDP の設定	『*MPLS Label Distribution Protocol Configuration Guide*』の「MPLS Label Distribution Protocol (LDP)」モジュール
MPLS トラフィック エンジニアリング リソース予約プロトコル（RSVP）の設定	『*MPLS Traffic Engineering Path Calculation and Setup Configuration Guide*』の「MPLS Traffic Engineering and Enhancements」モジュール
IPv6 VPN over MPLS	『*MPLS Layer 3 VPNs Configuration Guide*』の「IPv6 VPN over MPLS」モジュール

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。	http://www.cisco.com/cisco/web/support/index.html

MPLS バーチャル プライベート ネットワークの機能情報

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 に移動します。Cisco.com のアカウントは必要ありません。

表 *1*：*MPLS* バーチャル プライベート ネットワークの機能情報

機能名	リリース	機能情報
『MPLS Virtual Private Networks』		MPLS バーチャルプライベートネットワーク機能により、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 ネットワークを使用して、複数のサイトを相互接続できます。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。

第 3 章

Multiprotocol BGP MPLS VPN

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）は、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。各サイトには、1 つ以上のプロバイダー エッジ（PE）デバイスに接続される 1 つ以上のカスタマー エッジ（CE）デバイスがあります。PE は、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）を使用して、互いに動的に通信します。

- 機能情報の確認，29 ページ
- Multiprotocol BGP MPLS VPN の前提条件，30 ページ
- Multiprotocol BGP MPLS VPN に関する情報，30 ページ
- Multiprotocol BGP MPLS VPN の設定方法，34 ページ
- Multiprotocol BGP MPLS VPN の設定例，41 ページ
- その他の参考資料，42 ページ
- Multiprotocol BGP MPLS VPN の機能情報，42 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 に移動します。Cisco.com のアカウントは必要ありません。

Multiprotocol BGP MPLS VPN の前提条件

コアで MPLS バーチャル プライベート ネットワーク（VPN）を設定します。

Multiprotocol BGP MPLS VPN に関する情報

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。

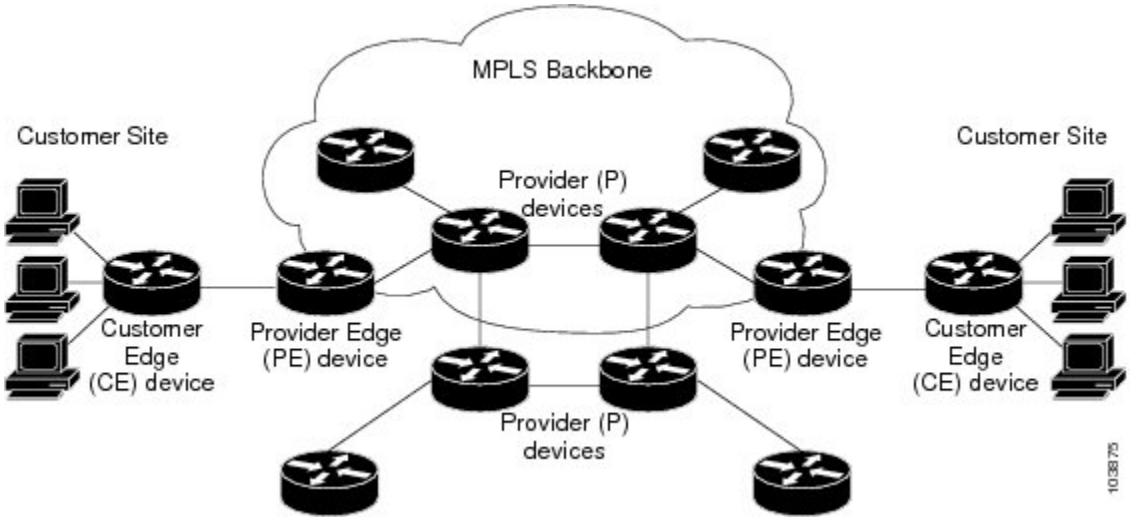
MPLS VPN の管理や拡張は、従来の VPN よりも簡単です。新しいサイトが MPLS VPN に追加された場合、更新する必要があるのは、カスタマーサイトにサービスを提供するサービスプロバイダーのエッジ デバイスだけです。

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 *2*：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 ネットワークでの Virtual Routing and Forwarding テーブルの仕組み

各バーチャル プライベート ネットワーク（VPN）は、1 つ以上の Virtual Routing and Forwarding（VRF）インスタンスに関連付けられています。VRF では、PE デバイスに接続されているカスタマー サイトの VPN メンバーシップを定義します。VRF は、次のコンポーネントで構成されています。

- IP ルーティング テーブル
- 取得した Cisco Express Forwarding テーブル
- 転送テーブルを使用する一連のインターフェイス

- ルーティング テーブルに格納されている情報を制御するための一連のルールおよびルーティング プロトコル パラメータ

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 つのサイトを複数の VPNs 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。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。

パケット転送情報は、VRF ごとに IP ルーティング テーブルおよび Cisco Express Forwarding テーブルに格納されます。各 VRF カスタマーに対して、別個の一連のルーティング テーブルおよび Cisco Express Forwarding テーブルが維持されます。これらのテーブルにより、VPN の外側に情報が転送されないようになっているほか、VPN の外側のパケットも VPN 内のデバイスに転送されないようになっています。

MPLS バーチャル プライベート ネットワークにおける VPN ルーティング情報の配布方法

バーチャルプライベートネットワーク（VPN）ルーティング情報の配布は、Border Gateway Protocol（BGP）拡張コミュニティによって実装される VPN ルート ターゲット コミュニティを使用して制御されます。VPN ルーティング情報は、次のように配布されます。

- カスタマー エッジ（CE）デバイスから学習した VPN ルートが BGP に注入されると、VPN ルート ターゲット拡張コミュニティ属性のリストが、そのルートに関連付けられます。通常、ルート ターゲット コミュニティ拡張値のリストは、ルートの学習元の Virtual Routing and Forwarding（VRF）インスタンスに関連付けられているルート ターゲットのエクスポート リストから設定されます。
- ルート ターゲット拡張コミュニティのインポート リストは、各 VRF に関連付けられています。インポート リストには、ルートが VRF にインポートされるために、ルートに設定されている必要のある、ルート ターゲット拡張コミュニティ属性が定義されています。たとえば、ある特定の VRF のインポート リストにルート ターゲット拡張コミュニティ A、B、および C が含まれている場合、これらのルート ターゲット拡張コミュニティ A、B、または C のいずれかを伝送するすべての VPN ルートが VRF にインポートされます。

VPN ルーティング情報の BGP 配布

プロバイダー エッジ（PE）デバイスは、次のソースから IP プレフィックスを学習します。

- スタティック設定によりカスタマー エッジ（CE）デバイスから
- CE デバイスとのボーダー ゲートウェイ プロトコル（BGP）セッション
- CE デバイスと交換する Routing Information Protocol（RIP）

IP プレフィックスは、IPv4 アドレス ファミリのメンバです。PE デバイスは、IP プレフィックスを学習した後、その IP プレフィックスを 8 バイトのルート識別子（RD）に結合することで、VPN-IPv4 プレフィックスに変換します。生成されたプレフィックスは、VPN-IPv4 アドレス ファ

ミリのメンバです。このプレフィックスによって、カスタマー サイトでグローバルに一意でない（登録されていないプライベート）IP アドレスが使用される場合でも、カスタマーのアドレスが一意に識別されます。VPN-IPv4 プレフィックスを生成するために使用されるルート識別子は、PE デバイス上で Virtual Routing and Forwarding（VRF）に関連付けられているコンフィギュレーション コマンドによって指定されます。

BGP は、各 VPN の VPN-IPv4 プレフィックスに関する到達可能性情報を配布します。BGP 通信は、次の 2 つのレベルで行われます。

- 自律システム（内部 BGP（IBGP））と呼ばれる、IP ドメイン内
- 自律システム間（外部 BGP（EBGP））

PE と PE 間のセッションまたは PE とルート リフレクタ（RR）間のセッションは、IBGP セッションであり、PE と CE 間のセッションは EBGP セッションです。Enhanced Interior Gateway Routing Protocol（EIGRP）PE-CE 環境では、EIGRP 内部ルートが 1 つの PE によって BGP に再配布されると、次に、別の PE によって EIGRP に戻されます。このとき、このルートの送信元ルータ ID が 2 番めの PE のルータ ID に設定され、元の内部ルータ ID が置き換えられます。

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だけ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。

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に Virtual Routing and 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。

Multiprotocol BGP MPLS VPN の設定方法

PE デバイスおよびルート リフレクタでのマルチプロトコル BGP 接続の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router bgp***as-number*
4. **no bgp default ipv4-unicast**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **address-family vpnv4** [**unicast**]
8. **neighbor** {*ip-address* | *peer-group-name*} **send-community extended**
9. **neighbor** {*ip-address* | *peer-group-name*} **activate**
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp***as-number* 例： `Device(config)# router bgp 100`	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。 • *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。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。

	コマンドまたはアクション	目的
ステップ 4	**no bgp default ipv4-unicast** 例： `Device(config-router)# no bgp default ipv4-unicast`	（任意）IPv4 ユニキャスト アドレス ファミリをすべてのネイバーでディセーブルにします。 • このネイバーをマルチプロトコル ラベル スイッチング（MPLS）ルートだけに使用している場合は、**no bgp default ipv4-unicast** コマンドを使用します。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor 10.0.0.1 remote-as 100`	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。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。 • *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。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Device(config-router)# neighbor 10.0.0.1 activate`	ネイバー BGP デバイスとの情報交換を有効にします。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 7	**address-family vpnv4** [**unicast**] 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 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。 • **unicast** キーワード（任意）では、VPNv4 ユニキャスト アドレス プレフィックスを指定します。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **send-community extended** 例： `Device(config-router-af)# neighbor 10.0.0.1 send-community extended`	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。 • *ip-address* 引数には、BGP 対応ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 9	**neighbor** {*ip-address* | *peer-group-name*} **activate**	ネイバー BGP デバイスとの情報交換を有効にします。 • *ip-address* 引数には、ネイバーの 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
	例： `Device(config-router-af)# neighbor 10.0.0.1 activate`	• *peer-group-name* 引数には、BGP ピア グループの名前を指定します。
ステップ 10	**end** 例： `Device(config-router-af)# end`	（任意）終了して、特権 EXEC モードに戻ります。

トラブルシューティングのヒント

show ip bgp neighbor コマンドを入力すると、ネイバーが稼働中であることを確認できます。このコマンドが成功しなかった場合は、**debug ip bgp***ip-address***events** コマンドを入力します。ここで、*ip-address* はネイバーの IP アドレスです。

BGP を PE デバイスと CE デバイス間のルーティング プロトコルに設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router bgp***as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*]
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **exit-address-family**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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	**configure terminal** 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	**router bgp***as-number* 例： `Device(config)# router bgp 100`	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。 • *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。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。
ステップ 4	**address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*] 例： `Device(config-router)# address-family ipv4 vrf vpn1`	IPv4 アドレス ファミリ タイプを指定し、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。 • **multicast** キーワードは、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。 • **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。 • **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 VRF の名前を指定します。
ステップ 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router-af)# neighbor 10.0.0.1 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。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。 • *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。
ステップ 6	**neighbor** {*ip-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 10.0.0.1 activate`	ネイバー BGP デバイスとの情報交換を有効にします。 • *ip-address* 引数には、ネイバーの IP アドレスを指定します。 • *peer-group-name* 引数には、BGP ピア グループの名前を指定します。

	コマンドまたはアクション	目的
ステップ 7	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	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。
ステップ 8	**end** 例： `Device(config-router)# end`	（任意）終了して、特権 EXEC モードに戻ります。

バーチャル プライベート ネットワークの設定の確認

ルート識別子を Virtual Routing and Forwarding（VRF）インスタンス用に設定する必要があります。また、VRF を伝送するインターフェイス上でマルチプロトコル ラベル スイッチング（MPLS）を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。

手順の概要

1. **show ip vrf**

手順の詳細

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

手順の概要

1. イネーブル化
2. **ping** [*protocol*] {*host-name* | *system-address*}
3. **trace** [*protocol*] [*destination*]
4. **show ip route** [*ip-address* [*mask*] [**longer-prefixes**]] | *protocol* [*process-id*]] | [**list** [*access-list-name* | *access-list-number*]

手順の詳細

ステップ 1 イネーブル化
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、ある CE デバイスから別の CE デバイスへ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ある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

手順の概要

1. イネーブル化
2. **show ip route vrf***vrf-name* [*prefix*]
3. **show ip cef vrf***vrf-name* [*ip-prefix*]

手順の詳細

ステップ 1 **イネーブル化**
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 Routing and Forwarding（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。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シスコ エクスプレス フォワーディング 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。

Multiprotocol BGP MPLS VPN の設定例

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
```ip 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 FastEthernet0/0/0 ip vrf forwarding vpn1 ip address 192.0.2.3 255.255.255.0 no cdp enable ! interface FastEthernet1/1/0 ip address 192.0.2.2 255.255.255.0 mpls label protocol ldp mpls ip ! router ospf 100 network 10.0.0. 0.0.0.0 area 100 network 192.0.2.1 255.255.255.0 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 neighbor 198.51.100.1 remote-as 200 neighbor 198.51.100.1 activate neighbor 198.51.100.1 as-override neighbor 198.51.100.1 advertisement-interval 5 no auto-summary no synchronization exit-address-family```	```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 FastEthernet0/0 ip address 198.51.100.1 255.255.255.0 no cdp enable ! router bgp 200 bgp log-neighbor-changes neighbor 198.51.100.2 remote-as 100 ! address-family ipv4 redistribute connected neighbor 198.51.100.2 activate neighbor 198.51.100.2 advertisement-interval 5 no auto-summary no synchronization exit-address-family```

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 Command List, All Releases』
MPLS および MPLS アプリケーションに関連するコマンドの説明	『Cisco IOS Multiprotocol Label Switching Command Reference』
MPLS バーチャル プライベート ネットワークの設定	『*MPLS Layer 3 VPNs Configuration Guide*』の「MPLS Virtual Private Networks」モジュール

標準および RFC

RFC	Title
RFC 2283	『*Multiprotocol Extensions for BGP-4*』
RFC 2547	『*BGP/MPLS VPNs*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。	http://www.cisco.com/cisco/web/support/index.html

Multiprotocol BGP MPLS VPN 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 に移動します。Cisco.com のアカウントは必要ありません。

表 *2*：***Multiprotocol BGP MPLS VPN*** の機能情報

機能名	リリース	機能情報
Multiprotocol BGP MPLS VPN	12.0(11)ST 12.2(9)S 12.2(17b)SXA 12.2(27)SBB 12.3(8)T 15.2(1)S Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.5S	MPLS VPN は、MPLS プロバイダー コア ネットワークを通じて相互接続されている一連のサイトから構成されます。各サイトには、1 つ以上の PE に接続される 1 つ以上の CE デバイスがあります。Multiprotocol BGP MPLS VPN 機能により、PE は MP-BGP を使用して動的に相互通信できます。 この機能は、Cisco IOS Release 12.0(11)ST で導入されました。 この機能は、Cisco IOS Release 12.2(9)S、12.2(17b)SXA、12.2(27)SBB、12.3(8)T、および 15.2(1)S で統合されました。 この機能は、Cisco IOS XE Release 2.1 で、Cisco ASR 1000 シリーズ ルータに実装されました。 Cisco IOS XE Release 3.5S では、Cisco ASR 903 ルータのサポートが追加されました。 追加または変更されたコマンドはありません。

第 4 章

MPLS VPN OSPF PE および CE サポート

MPLS VPN OSPF PE および CE のサポート機能を使用すると、サービス プロバイダーは、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）内のプロバイダー エッジ（PE）デバイスとカスタマー エッジ（CE）デバイスの間で、Open Shortest Path First（OSPF）を設定できます。この機能により、VPN 内の複数の CE デバイスに接続されている PE デバイス上で、各インターフェイスまたはサブインターフェイスに別のルータ ID が設定されるため、デバイスがサイト間でルーティング情報を交換するときの柔軟性が向上します。MPLS VPN は、MPLS プロバイダー コア ネットワークにより相互接続されている一連のサイトから構成されます。各顧客サイトでは、1 つ以上の CE デバイスが、1 つ以上の PE デバイスに接続されます。

- 機能情報の確認，45 ページ
- MPLS VPN OSPF PE および CE サポートの前提条件，46 ページ
- MPLS VPN OSPF PE および CE サポートに関する情報，46 ページ
- MPLS VPN OSPF PE および CE サポートの設定方法，46 ページ
- MPLS VPN OSPF PE および CE サポートの設定例，51 ページ
- その他の参考資料，52 ページ
- MPLS VPN OSPF PE および CE サポートの機能情報，52 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 に移動します。Cisco.com のアカウントは必要ありません。

MPLS VPN OSPF PE および CE サポートの前提条件

- MPLS レイヤ 3 VPN を設定します。
- コアで Border Gateway Protocol（BGP）を設定します。

MPLS VPN OSPF PE および CE サポートに関する情報

MPLS VPN OSPF PE および CE サポートの概要

この機能を使用すると、サービス プロバイダーは、MPLS VPN ネットワーク内のプロバイダーエッジ（PE）デバイスとカスタマーエッジ（CE）デバイスの間で、Open Shortest Path First（OSPF）を設定できます。

この機能により、VPN 内の複数の CE デバイスに接続されている PE デバイス上で、各インターフェイスまたはサブインターフェイスに別のルータ ID が設定されるため、デバイスがサイト間でルーティング情報を交換するときの柔軟性が向上します。

MPLS VPN OSPF PE および CE サポートの設定方法

OSPF を PE デバイスと CE デバイス間のルーティング プロトコルに設定

Open Shortest Path First（OSPF）を使用する PE から CE へのルーティング セッションを設定するには、次の作業を実行します。

（注） MPLS VPN PE-CE 環境でのシスコによる OSPF 実装には、RFC4576 との互換性があります。

はじめる前に

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、PE デバイスを設定します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router ospf***process-id* [**vrf***vpn-name*]
4. **network***ip-addresswildcard-mask***area***area-id*
5. **address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*]
6. **redistribute***protocol* | [**process-id**] | {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric***metric-value*] [**metric-type***type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag***tag-value*] [**route-map***map-tag*] [**subnets**]
7. **exit-address-family**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router ospf***process-id* [**vrf***vpn-name*] 例： `Device(config)# router ospf 1 vrf grc`	OSPF ルーティングをイネーブルにして、ルータ コンフィギュレーション モードを開始します。 • *process-id* 引数は OSPF プロセスを示します。 • **vrf***vpn-name* キーワードおよび引数は、バーチャル プライベート ネットワーク（VPN）を識別します。VPN ルートを受信する Virtual Routing and Forwarding（VRF）インスタンスごとに個別の OSPF プロセスを作成します。
ステップ 4	**network***ip-addresswildcard-mask***area***area-id* 例： `Device(config-router)# network 10.0.0.1 0.0.0.3 area 20`	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。 • *ip-address* 引数は、IP アドレスを識別します。 • *wildcard-mask* 引数により、「don't care」（一致する必要のない）ビットが含まれた IP アドレス タイプのマスクを識別します。

	コマンドまたはアクション	目的
		• *area-id* 引数により、OSPF アドレス範囲と関連付けられるエリアを識別します。10 進数値または IP アドレスのいずれかで指定できます。IP サブネットにエリアを関連付けるには、*area-id* 引数の値としてサブネット アドレスを指定します。
ステップ 5	**address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*] 例： `Device(config-router)# address-family ipv4 vrf vpn1`	IPv4 アドレス ファミリ タイプを指定し、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。 • **multicast** キーワードは、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。 • **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。 • **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 VRF の名前を指定します。
ステップ 6	**redistribute***protocol* | [**process-id**] | {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric***metric-value*] [**metric-type***type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag***tag-value*] [**route-map***map-tag*] [**subnets**] 例： `Device(config-router-af)# redistribute rip metric 1 subnets`	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。 すべての内部ボーダー ゲートウェイ プロトコル（IBGP）ルートが VRF に配布されるようにするには、さまざまなプロトコルを含める必要があります。
ステップ 7	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	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。
ステップ 8	**end** 例： `Device(config-router)# end`	（任意）終了して、特権 EXEC モードに戻ります。

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

手順の概要

1. イネーブル化
2. **ping** [*protocol*] {*host-name* | *system-address*}
3. **trace** [*protocol*] [*destination*]
4. **show ip route** [*ip-address* [*mask*] [**longer-prefixes**]] | *protocol* [*process-id*]] | [**list** [*access-list-name* | *access-list-number*]

手順の詳細

ステップ 1 イネーブル化
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、ある CE デバイスから別の CE デバイスへ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ある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

手順の概要

1. イネーブル化
2. **show ip route vrf***vrf-name* [*prefix*]
3. **show ip cef vrf***vrf-name* [*ip-prefix*]

手順の詳細

ステップ 1 イネーブル化
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 Routing and Forwarding（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。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シスコ エクスプレス フォワーディング 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 VPN OSPF PE および CE サポートの設定例

例：OSPF を使用した MPLS VPN の設定

PE の設定	CE の設定
```ip 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 FastEthernet0/0/0 ip vrf forwarding vpn1 ip address 34.0.0.2 255.0.0.0 no cdp enable ! router ospf 1000 vrf vpn1 log-adjacency-changes redistribute bgp 100 metric-type 1 subnets network 10.0.0.13 0.0.0.0 area 10000 network 34.0.0.0 0.255.255.255 area 10000 ! 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 ospf 1000 match internal external 1 external 2 no auto-summary no synchronization exit-address-family```	```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 FastEthernet0/0/0 ip address 34.0.0.1 255.0.0.0 no cdp enable ! router ospf 1000 log-adjacency-changes auto-cost reference-bandwidth 1000 redistribute connected subnets network 34.0.0.0 0.255.255.255 area 1000 network 10.0.0.0 0.0.0.0 area 1000```

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 Master Command List, All Releases』
MPLS と MPLS アプリケーション コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』

標準および RFC

標準/RFC	Title
RFC 4576	『*Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。	http://www.cisco.com/cisco/web/support/index.html

MPLS VPN OSPF PE および CE サポートの機能情報

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 に移動します。Cisco.com のアカウントは必要ありません。

表 *3*：*MPLS VPN OSPF PE* および *CE* サポートの機能情報

機能名	リリース	機能情報
MPLS VPN OSPF PE および CE サポート	12.0(5)T 12.0(11)ST 12.0(21)ST 12.2(17b)SXA 12.2(28)SB Cisco IOS XE Release 2.1	MPLS VPN OSPF PE および CE サポート機能により、サービスプロバイダーがマルチプロトコル 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）内のプロバイダー エッジ（PE）デバイスとカスタマー エッジ（CE）デバイス間で、Open Shortest Path First（OSPF）を設定できます。 この機能は、Cisco IOS Release 12.0(5)T で導入されました。 この機能は、Cisco IOS Release 12.0(11)ST、12.0(21)ST、12.2(17b)SXA、および 12.2(28)SB で統合されました。 この機能は、Cisco IOS XE Release 2.1 で、Cisco ASR 1000 シリーズ ルータに実装されました。 追加または変更されたコマンドはありません。

第 5 章

MPLS VPN による PE および CE 間の EIGRP サポート

MPLS VPN による PE および CE 間の EIGRP サポート機能により、サービス プロバイダーは、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）のプロバイダー エッジ（PE）デバイスとカスタマー エッジ（CE）デバイスの間で Enhanced Interior Gateway Routing Protocol（EIGRP）を設定し、EIGRP のネイティブ サポートを必要とするカスタマーに MPLS VPN サービスを提供します。MPLS VPN は、MPLS プロバイダー コア ネットワークにより相互接続されている一連のサイトから構成されます。各顧客サイトでは、1 つ以上の CE デバイスが、1 つ以上の PE デバイスに接続されます。

- 機能情報の確認，55 ページ
- MPLS VPN による PE および CE 間の EIGRP サポートの前提条件，56 ページ
- MPLS VPN による PE および CE 間の EIGRP サポートについての情報，56 ページ
- MPLS VPN による PE および CE 間の EIGRP サポートの設定方法，56 ページ
- MPLS VPN による PE および CE 間の EIGRP サポートの設定例，64 ページ
- その他の参考資料，65 ページ
- MPLS VPN による PE および CE 間の EIGRP サポートの機能情報，65 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 に移動します。Cisco.com のアカウントは必要ありません。

MPLS VPN による PE および CE 間の EIGRP サポートの前提条件

- MPLS レイヤ 3 VPN を設定します。
- ネットワーク コアで Border Gateway Protocol（BGP）を設定します。

MPLS VPN による PE および CE 間の EIGRP サポートについての情報

MPLS VPN による PE および CE 間の EIGRP サポートの概要

プロバイダー エッジ（PE）デバイスとカスタマー エッジ（CE）デバイスの間で Enhanced Interior Gateway Routing Protocol（EIGRP）を使用すると、MPLS 対応 Border Gateway Protocol（BGP）コア ネットワークを介して EIGRP カスタマー ネットワークを透過的に接続できるため、EIGRP ルートは、内部 BGP（iBGP）として BGP ネットワーク全体で VPN を介して再配布されます。

MPLS VPN による PE および CE 間の EIGRP サポートの設定方法

EIGRP を PE デバイスと CE デバイス間のルーティング プロトコルに設定

EIGRP を使用する、PE から CE へのルーティング セッションを設定するには、次の作業を実行します。

はじめる前に

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、PE デバイスを設定します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router bgp***as-number*
4. **no synchronization**
5. **neighbor***ip-address***remote-as***as-number*
6. **neighbor***ip-address***update-source loopback***interface-number*
7. **address-family vpnv4**
8. **neighbor***ip-address***activate**
9. **neighbor***ip-address***send-community extended**
10. **exit-address-family**
11. **address-family ipv4 vrf***vrf-name*
12. **redistribute eigrp***as-number* [**metric***metric-value*] [**route-map***map-name*]
13. **no synchronization**
14. **exit-address-family**
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp***as-number* 例： `Device(config)# router bgp 10`	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 プロセスを作成します。
ステップ 4	**no synchronization** 例： `Device(config-router)# no synchronization`	IGP と同期するまで待たずにアドバタイズメントを送信するように BGP を設定します。

	コマンドまたはアクション	目的
ステップ 5	**neighbor***ip-address***remote-as***as-number* 例： `Device(config-router)# neighbor 10.0.0.1 remote-as 10`	指定されたネイバーまたはピア グループとのピアリングを確立します。 • このステップでは、別の CE サイトの CE デバイスに接続している PE デバイスとの間で iBGP セッションを確立します。
ステップ 6	**neighbor***ip-address***update-source loopback***interface-number* 例： `Device(config-router)# neighbor 10.0.0.1 update-source loopback 0`	TCP 接続の動作インターフェイスを使用するように BGP を設定します。 • この設定手順は、必須ではありません。ただし BGP ルーティングプロセスは、インターフェイスまたはリンクのフラッピングの影響をそれほど受けません。
ステップ 7	**address-family vpnv4** 例： `Device(config-router)# address-family vpnv4`	標準 IPv4 アドレスプレフィックスを使用するルーティング セッション（BGP、RIP、スタティック ルーティング セッションなど）を設定するため、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 8	**neighbor***ip-address***activate** 例： `Device(config-router-af)# neighbor 10.0.0.1 activate`	指定されたネイバーまたはピア グループとのピアリングを確立します。 • このステップでは、PE デバイス間での VPNv4 ルーティングの交換を有効にします。
ステップ 9	**neighbor***ip-address***send-community extended** 例： `Device(config-router-af)# neighbor 10.0.0.1 send-community extended`	指定したネイバーに拡張コミュニティ属性を送信するようにローカル デバイスを設定します。 • このステップは、EIGRP 拡張コミュニティ属性を交換する場合に必須です。
ステップ 10	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	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て、ルータ 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	**address-family ipv4 vrf***vrf-name* 例： `Device(config-router)# address-family ipv4 vrf RED`	EIGRP VRF 用の IPv4 アドレス ファミリを設定し、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。 • アドレス ファミリ VRF は、PE デバイスと CE デバイスの間で稼働する EIGRP VRF ごとに設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 12	**redistribute eigrp***as-number* [**metric***metric-value*] [**route-map***map-name*] 例： `Device(config-router-af)# redistribute eigrp 101`	EIGRP VRF を BGP に再配布します。 • CE ネットワークの自律システム番号は、このステップで設定されます。
ステップ 13	**no synchronization** 例： `Device(config-router-af)# no synchronization`	IGP と同期するまで待たずにアドバタイズメントを送信するように BGP を設定します。
ステップ 14	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	アドレスファミリ コンフィギュレーション モードを終了して、ルータ コンフィギュレーション モードを開始します。
ステップ 15	**end** 例： `Device(config-router)# end`	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 モードを開始します。

MPLS VPN における EIGRP 再配布の設定

MPLS VPN で EIGRP 再配布を有効にするため、VPN サービスを提供するすべての PE デバイスでこの作業を実行します。

はじめる前に

外部 EIGRP 自律システムおよび非 EIGRP ネットワークからのルートが EIGRP CE デバイスに再配布される前に、これらのルートのメトリックを設定する必要があります。メトリックは、再配布ステートメントで **redistribute**（IP）コマンドまたは **default-metric**（EIGRP）コマンドを使用して設定できます。別の EIGRP 自律システムから、またはメトリックが設定されていない非 EIGRP ネットワークから外部ルートを受信した場合、ルートは CE デバイスにアドバタイズされません。

（注） ネイティブ EIGRP VRF 間の再配布はサポートされていません。これは、設計された動作です。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router eigrp***as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*]
5. **network***ip-addresswildcard-mask*
6. **redistribute bgp** {*as-number*} [**metric***bandwidthdelayreliabilityloadmtu*] [**route-map***map-name*]
7. **autonomous-system***as-number*
8. **exit-address-family**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router eigrp***as-number* 例： `Device(config)# router eigrp 1`	ルータ コンフィギュレーションモードを開始し、EIGRP ルーティング プロセスを作成します。 • PE デバイスの EIGRP ルーティング プロセスはこの手順で作成されます。
ステップ 4	**address-family ipv4** [**multicast** | **unicast** | **vrf***vrf-name*] 例： `Device(config-router)# address-family ipv4 vrf RED`	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 を作成します。 • VRF 名は、前の項で作成した VRF 名と一致している必要があります。
ステップ 5	**network***ip-addresswildcard-mask* 例： `Device(config-router-af)# network 172.16.0.0 0.0.255.255`	VRF のネットワークを指定します。 • EIGRP に含めるインターフェイスを指定するには、network コマンドを使用します。VRF は、network コマンドのワイルドカード マスク範囲内にあるアドレスを使用して設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	**redistribute bgp** {*as-number*} [**metric***bandwidthdelayreliabilityloadmtu*] [**route-map***map-name*] 例： `Device(config-router-af)# redistribute bgp 10 metric 10000 100 255 1 1500`	BGP を EIGRP に再配布します。 • BGP ネットワークの自律システム番号とメトリックは、このステップで設定されます。BGP を CE サイトの EIGRP に再配布して、EIGRP 情報を伝送する BGP ルートを受け入れるようにする必要があります。また、BGP ネットワークにメトリックを指定する必要があります。このメトリックはこのステップで設定します。
ステップ 7	**autonomous-system***as-number* 例： `Device(config-router-af)# autonomous-system 101`	カスタマー サイトの EIGRP ネットワークの自律システム番号を指定します。
ステップ 8	**exit-address-family** 例： `Device(config-router-af)# exit-address-family`	アドレス ファミリ コンフィギュレーション モードを終了して、ルータ 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	**end** 例： `Device(config-router)# end`	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 モードを開始します。

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

手順の概要

1. イネーブル化
2. **ping** [*protocol*] {*host-name* | *system-address*}
3. **trace** [*protocol*] [*destination*]
4. **show ip route** [*ip-address* [*mask*] [**longer-prefixes**]] | *protocol* [*process-id*]] | [**list** [*access-list-name* | *access-list-number*]

手順の詳細

ステップ 1 イネーブル化
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、ある CE デバイスから別の CE デバイスへ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ある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

手順の概要

1. イネーブル化
2. **show ip route vrf***vrf-name* [*prefix*]
3. **show ip cef vrf***vrf-name* [*ip-prefix*]

手順の詳細

ステップ 1 **イネーブル化**
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 Routing and Forwarding（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。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シスコ エクスプレス フォワーディング 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 VPN による PE および CE 間の EIGRP サポートの設定例

例：EIGRP を使用した MPLS VPN の設定

PE の設定	CE の設定
ip 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 FastEthernet0/0/0 ip vrf forwarding vpn1 ip address 34.0.0.2 255.0.0.0 no cdp enable interface FastEthernet1/1/0 ip address 30.0.0.1 255.0.0.0 mpls label protocol ldp mpls ip router eigrp 1000 auto-summary ! address-family ipv4 vrf vpn1 redistribute bgp 100 metric 10000 100 255 1 1500 network 34.0.0.0 distribute-list 20 in no auto-summary autonomous-system 1000 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 eigrp no auto-summary no synchronization exit-address-family	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 FastEthernet0/0/0 ip address 34.0.0.1 255.0.0.0 no cdp enable ! router eigrp 1000 network 34.0.0.0 auto-summary

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 Master Command List, All Releases』
MPLS と MPLS アプリケーション コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』

標準および RFC

標準/RFC	Title
RFC 4576	『*Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。	http://www.cisco.com/cisco/web/support/index.html

MPLS VPN による PE および CE 間の EIGRP サポートの機能情報

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 に移動します。Cisco.com のアカウントは必要ありません。

表 *4*：*MPLS VPN* による *PE* および *CE* 間の *EIGRP* サポートの機能情報

機能名	リリース	機能情報
MPLS VPN による PE および CE 間の EIGRP サポート	12.0(22)S 12.2(15)T 12.2(18)S 12.2(18)SXD 12.2(27)SBB 12.3(2)T Cisco IOS XE Release 2.1	MPLS VPN による PE および CE 間の EIGRP サポート機能により、サービスプロバイダーは、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）のプロバイダー エッジ（PE）デバイスとカスタマー エッジ（CE）デバイスの間で Enhanced Interior Gateway Routing Protocol（EIGRP）を設定し、EIGRP のネイティブ サポートを必要とするカスタマーに MPLS VPN サービスを提供します。 この機能は、Cisco IOS Release 12.0(22)S で導入されました。 この機能は、Cisco IOS Release 12.2(15)T、12.2(18)S、12.2(18)SXD、12.2(27)SBB、および 12.3(2)T で統合されました。 この機能は、Cisco IOS XE Release 2.1 で、Cisco ASR 1000 シリーズ ルータに実装されました。 追加または変更されたコマンドはありません。

第 6 章

IPv6 VPN over MPLS

Border Gateway Protocol over Multiprotocol Label Switching の VPN 機能は、プロバイダー エッジ（PE）ベースのバーチャルプライベート ネットワーク（VPN）モデルの実装です。原則として、IPv4 VPN と IPv6 VPN との間に相違点はありません。IPv4 と IPv6 のどちらにおいても、マルチプロトコル ボーダー ゲートウェイ プロトコル（BGP）は、マルチプロトコル ラベル スイッチング（MPLS）VPN for IPv6（VPNv6）アーキテクチャの中心的存在です。サービス プロバイダー バックボーンを介して IPv6 ルートを配布するために使用され、同じ手順を使用して、重複するアドレス、再配布ポリシー、およびスケーラビリティの問題が処理されます。

- 機能情報の確認，67 ページ
- IPv6 VPN over MPLS の前提条件，68 ページ
- IPv6 VPN over MPLS の制約事項，68 ページ
- IPv6 VPN over MPLS に関する情報，68 ページ
- IPv6 VPN over MPLS の設定方法，76 ページ
- IPv6 VPN over MPLS の設定例，122 ページ
- その他の参考資料，127 ページ
- IPv6 VPN over MPLS の機能情報，128 ページ
- 用語集，130 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 に移動します。Cisco.com のアカウントは必要ありません。

IPv6 VPN over MPLS の前提条件

IPv6 VPN の動作を設定する前に、ネットワークで次のサービスが稼働している必要があります。

- プロバイダー バックボーン デバイスのマルチプロトコル 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）プロバイダー エッジ（PE）デバイスおよびプロバイダー デバイスの VPN コードと MPLS
- VPN サービスを提供するすべてのデバイスにおける Border Gateway Protocol（BGP）
- 各 MPLS 対応デバイスでの Cisco Express Forwarding スイッチング
- サービス クラス（CoS）機能

IPv6 VPN over MPLS の制約事項

IPv6 VPN over MPLS（6VPE）は、マルチプロトコル ラベル スイッチング（MPLS）IPv4 シグナリング コアをサポートしています。MPLS IPv6 シグナリング コアはサポートされません。

IPv6 VPN over MPLS に関する情報

IPv6 VPN over MPLS の概要

マルチプロトコル ボーダー ゲートウェイ プロトコル（BGP）は、IPv4 と IPv6 の両方において、マルチプロトコル ラベル スイッチング（MPLS）IPv6 バーチャル プライベート ネットワーク（VPN）アーキテクチャの中心的存在です。サービス プロバイダー バックボーンを介して IPv6 ルートを配布するために使用され、同じ手順を使用して、重複するアドレス、再配布ポリシー、およびスケーラビリティの問題が処理されます。

IPv6 には重複するアドレス空間はありませんが、IPv6 アドレスの先頭にはルート識別子（RD）が付加されます。ネットワーク層到達可能性情報（NLRI）の 3 タプル形式（長さ、IPv6 プレフィックス、およびラベルを含む）は、マルチプロトコル BGP を使用してこれらのルートを配布するように定義されます。拡張コミュニティ属性（たとえばルート ターゲット）は、エクスポートされたルートにタグを付け、インポートされたルートをフィルタリングすることによって、ルーティング情報の再配布を制御するために使用されます。

スケーラビリティを実現するために、ルート リフレクタを使用してルーティング パスを集中させ、完全プロバイダーエッジ（PE）メッシュを回避することができます。ルート リフレッシュ、自動ルート フィルタリング、アウトバウンド ルート フィルタリングなどの IPv6 の BGP 機能は、

各 PE に保持されるルートの数を削減するのに役立ちます。このマニュアルでは、IPv6 と IPv4 の次の相違点に焦点を当てます。

- 新しいマルチプロトコル BGP IPv6 VPN アドレス ファミリの作成と IPv6 VPN アドレス形式の仕様
- 新しい IPv6 VPN NLRI の仕様
- デバイスに IPv4 ベースの MPLS コアがある場合の BGP ネクストホップ符号化の仕様

プロバイダー間トポロジおよび Carrier Supporting Carrier（CSC）トポロジなどの一部の IPv6 VPN 機能は、BGP-MPLS IPv6 VPN に固有です。自律システム境界ルータ（ASBR）間のリンクなど、それ以外のものは、転送されるアドレスファミリとは関係なく、IPv4 だけ、IPv6 だけ、または両方をサポートすることがあります。

IPv6 VPN over MPLS のアドレッシングの考慮事項

展開するバーチャルプライベートネットワーク（VPN）モデルに関係なく、ホストが 1 つの VPN 内の 1 つのサイトを使用して他のサイトと通信したり、パブリック リソースと通信したりできるようにする、VPN のアドレッシング計画を定義する必要があります。

VPN IPv4 サイトは、多くの場合、アドレッシング計画にプライベートアドレッシングを使用します。これらのアドレスについて、登録の必要はありません。パブリック ネットワーク上でルーティングすることもできません。プライベートサイト内のホストでパブリック ドメインにアクセスする必要がある場合、ホストは常に、そのホストの代わりにパブリック アドレスを検出するデバイスを通過します。IPv4 では、このデバイスに、ネットワーク アドレス変換またはアプリケーション プロキシを指定できます。

IPv6 ではより大きいアドレス空間を使用できるため、IPv6 アドレッシングを実現する最も簡単なアプローチは、プライベート アドレッシング計画に IPv6 グローバル アドレスを使用することです。別のアプローチとして、Unique Local Addresses（ULA）を使用する方法があります。ULA は、それらのスコープに基づいてサイト境界で簡単にフィルタリングできます。また、ULA はインターネット サービス プロバイダー（ISP）非依存であり、永続的または間欠的なインターネット接続がないサイト内での通信に使用できます。

IPv6 VPN over MPLS（6VPE）では、ULA は通常のグローバルアドレスとして処理されます。ULA プレフィックスは、パブリック ドメイン内に表示されないように、デバイス設定によってフィルタリングされます。ピア上のリンクローカル アドレスが、Border Gateway Protocol（BGP）（IPv6 または IPv6 VPN）スピーカーによってアナウンスされることはありません。

パブリック ドメインにアクセスする必要があるプライベートサイト内のホストは、ルーティング可能なグローバルアドレスを使用してホストの代わりにパブリック リソースにアクセスする IPv6 アプリケーション プロキシ（Web ページにアクセスするための Web プロキシなど）を介して、これを行うことができます。または、ホスト自身のパブリック アドレスを使用することもできます。後者の場合、ULA が配置されているときには、IPv6 ホストもまたルーティング可能なグローバルアドレスを使用して設定されます。ソースアドレス選択アルゴリズムは、宛先アドレスに基づいて、どちらか一方を選択するために使用されます。

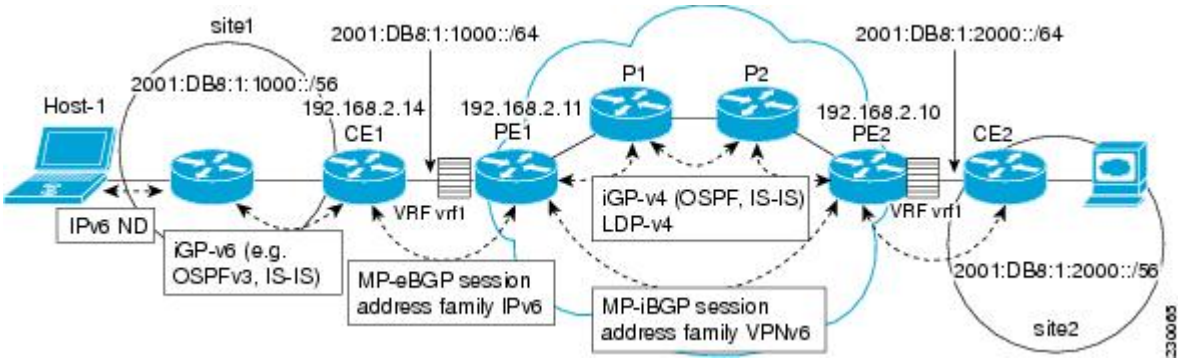
IPv6 VPN over MPLS の基本的な機能

IPv6 VPN over MPLS（6VPE）は、既存のマルチプロトコル ラベル スイッチング（MPLS）IPv4 コア ネットワークを利用して、IPv6 と IPv4 の共存を活用します。

IPv6 VPN アーキテクチャの概要

次の図に、IPv6バーチャルプライベートネットワーク（VPN）アーキテクチャの重要な特徴を示します。

図 *3*：簡単な *IPv6 VPN* アーキテクチャ



カスタマーエッジ（CE）デバイスは、プロバイダー エッジ（PE）デバイスを使用してプロバイダー バックボーンに接続されます。PE デバイスは、プロバイダー（上図の P1 および P2）デバイスを使用して接続されます。プロバイダー（P）デバイスは VPN ルートを認識せず、IPv6 over MPLS（6VPE）の場合は、IPv4 しかサポートしていないこともあります。PE デバイスだけが VPN 固有の作業を実行します。6VPE の場合、PE デバイスはデュアル スタック（IPv4 および IPv6）デバイスになります。

VPN 動作のルーティング コンポーネントは、コア ルーティングとエッジ ルーティングに分けられます。PE デバイスと P デバイスを含むコア ルーティングは、一般的に Open Shortest Path First（OSPF）または Intermediate System-to-Intermediate System（IS-IS）などの IPv4 Interior Gateway Protocol（IGP）によって実行されます。上図の場合、IGP は内部ルートだけをプロバイダーの自律システムに配布します。コア ルーティングにより、P および PE デバイス間の接続が可能になります。

エッジ ルーティングは、PE ペア間のルーティングと PE と CE 間のルーティングの 2 方向で発生します。PE ペア間のルーティングは、IPv6 VPN アドレス ファミリを使用したマルチプロトコル内部 BGP（iBGP）を使用して実行されます。この方式は、入力 PE デバイスでは適切なルート エクスポート ポリシーを、出力 PE デバイスでは適切なルート インポート ポリシーを使用して、PE-CE ルーティングを介して CE から学習したルートを配布します。

CE とその PE 間のルーティングは、VPN ルーティングおよび転送（VRF）認識であるルーティング プロトコルを使用して行います。スタティック ルート、外部 BGP（eBGP）、および Enhanced Interior Gateway Routing Protocol（EIGRP）は VRF インスタンス認識です。上図の場合、CE（CE1）

と PE（PE1）間で eBGP が使用されます。同時に、CE は VPN サイト（上図のサイト 1）内で IPv6 IGP を実行します。CE は、IGP ルートをマルチプロトコル eBGP アドレス ファミリ IPv6 に再配布します。これらのルートは、PE で vrf1 という名前の VRF にインストールされ、この VRF に定義されているエクスポート ポリシーに応じて、リモート PE（上図の PE2）に転送されます。

IPv6 VPN ネクスト ホップ

デバイスが MP_REACH_NLRI 属性を使用してプレフィックスをアナウンスすると、1 つのプロバイダー エッジ（PE）で稼働してい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）が、リモート PE に送信されるアップデート メッセージ内に BGP ネクスト ホップを挿入します。このネクストホップは、受信されたアップデートから伝播されるか（たとえば、PE がルート リフレクタの場合など）、またはアップデート メッセージを送信する PE（出力 PE）のアドレスになります。

IPv6 バーチャル プライベート ネットワーク（VPN）アドレス ファミリの場合、PE スピーカー間のネットワークの特性に関係なく、ネクストホップは IPv6 VPN アドレスである必要があります。ルート識別子（RD）は重要でないため（アドレスは VPN の一部ではありません）、0 に設定されます。プロバイダー ネットワークがネイティブ IPv6 ネットワークの場合、ネクスト ホップの残りの部分は出力 PE の IPv6 アドレスになります。そうでない場合は、IPv6 にマッピングされたアドレスとして使用される IPv4 アドレスになります（たとえば、::FFFF:IPv4 アドレス）。

MPLS 転送

1 つのカスタマー サイトから IPv6 トラフィックを受信すると、入力プロバイダー エッジ（PE）デバイスはマルチプロトコル ラベル スイッチング（MPLS）を使用して、Border Gateway Protocol（BGP）ネクストホップとして識別された出力 PE デバイスに向けて、バックボーンを介して IPv6 バーチャル プライベート ネットワーク（VPN）パケットをトンネリングします。入力 PE デバイスは、一般的に IPv6 パケットの先頭に外部ラベルおよび内部ラベルを付加してから、出力インターフェイスにパケットを渡します。

通常の動作では、転送パス上のプロバイダー（P）デバイスは最初のラベルの先にあるフレームの内部を調べません。プロバイダー（P）デバイスは着信ラベルを発信ラベルと交換するか、または次のデバイスが PE デバイスの場合には着信ラベルを削除します。着信ラベルの削除は、最後から 2 番めのホップのポッピングと呼ばれます。残りのラベル（BGP ラベル）は、カスタマー サイトへの出力 PE インターフェイスを識別するために使用されます。また、ラベルは、最後の P デバイスからプロトコル バージョン（IPv6）を隠します。そうしない場合、IPv6 パケットを転送することが必要になります。

P デバイスは IPv6 VPN ルートを知りません。IPv6 ヘッダーは 1 つ以上の MPLS ラベルの下に隠されたままになります。P デバイスで、送達できない MPLS カプセル化 IPv6 パケットを受信した場合のオプションは 2 つあります。P デバイスが IPv6 対応の場合、IPv6 ヘッダーを公開し、IPv6 メッセージ用のインターネット制御メッセージプロトコル（ICMP）を構築して、MPLS カプセル化メッセージを元のパケットの送信元に送信します。P デバイスが IPv6 対応でない場合、パケットをドロップします。

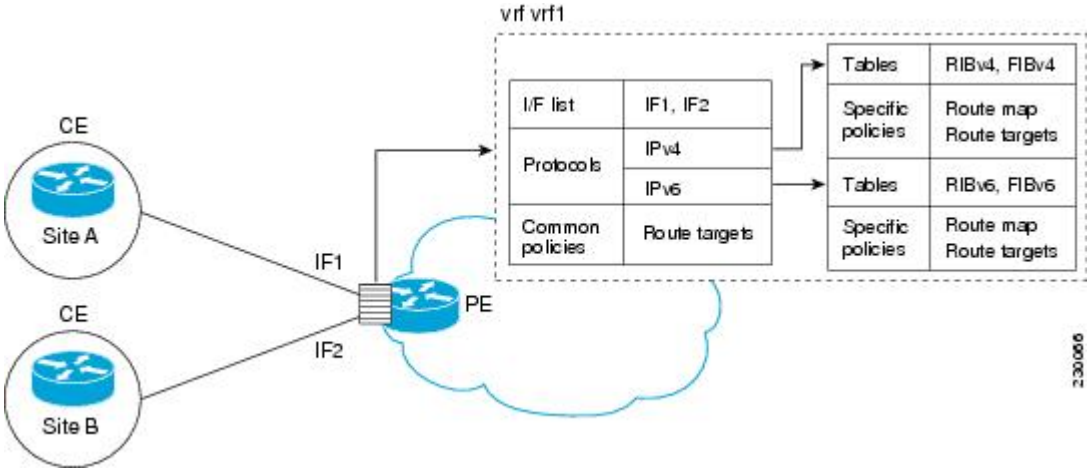
VRF の概念

Virtual Routing and Forwarding（VRF）エンティティは、プライベートなカスタマー固有のルーティング情報ベース（RIB）および転送情報ベース（FIB）とともに動作します。IPv4 ルーティング テーブルと IPv6 ルーティング テーブルは区別されますが、2 つのプロトコルで特定のカスタマーの同じ VRF を共有すると便利です。

IPv6 VPN の顧客は、デュアルスタックのホストとデバイスを展開するか、IPv4 インフラストラクチャの一部を IPv6 ノードでシャドウイングする、VPNv4 の顧客である可能性が高くなっています。複数の配置モデルが可能です。一部のカスタマーは、IPv4 と IPv6 に別々の論理インターフェイスを使用して、それぞれに異なる VRF を定義しています。このアプローチでは IPv4 および IPv6 に別々のポリシーを設定できる柔軟性が提供されますが、同じポリシーを共有することはできなくなります。もう 1 つのアプローチのマルチプロトコル VRF では、プロバイダー エッジ-カスタマー エッジ（PE-CE）インターフェイス上で単一の VRF を保持し、IPv4、IPv6、または両方に対してイネーブルにします。これにより、共通または別々のポリシーを IP バージョンごとに定義できるようになります。このアプローチを使用すると、VRF は、PE で検出されるテーブル、インターフェイス、およびポリシーのセットとしてより適切に定義され、この PE に接続されている特定の VPN のサイトによって使用されます。

下図に、マルチプロトコル VRF を示します。ここでは、vrf1 という名前の VRF が IPv4 と IPv6 の両方に対してイネーブルになっており、2 つのインターフェイス（IF1、IF2）、2 つのテーブル セット（IPv4 RIB と FIB、IPv6 RIB と FIB）、および共通または個別のポリシー セットに関連付けられています。

図 *4*：マルチプロトコル *VRF*



IPv6 VPN スケーラビリティ

ボーダー ゲートウェイ プロトコル-マルチプロトコル ラベル スイッチング（BGP-MPLS）IPv6 VPN などのプロバイダーエッジ（PE）ベースのバーチャル プライベート ネットワーク（VPN）は、カスタマー エッジ（CE）ベースの VPN よりも拡張性があります。ネットワーク設計者は、

ネットワークの設計時にスケーリングを考慮する必要があります。次の点について考慮する必要があります。

- Virtual Routing and Forwarding（VRF）テーブル サイズおよび BGP テーブル サイズなどのルーティング テーブル サイズ
- PE の平方数として増加する BGP セッション数

ルーティング テーブル サイズに関する問題は、多数のカスタマー サイトを処理する PE で発生します。これらの PE は、接続されているカスタマーごとに 1 つのルーティング情報ベース（RIB）および転送情報ベース（FIB）を持つだけではなく、PE の BGP テーブル（個々の VRF のすべてのエントリが統合される）もそれに応じて増加します。もう 1 つのスケーラビリティの問題は、プロバイダー ネットワーク内の PE の数が一定のレベル以上に増加したときに発生します。同じ VPN に属する多くのサイトが多数の PE に広がっていると想定した場合、マルチプロトコル BGP セッションの数は $(n-1) \times n/2$ のように急速に増加します。ここで、n は PE の数です。

IPv6 VPN over MPLS には、次の機能が含まれています。

- ルート更新と自動ルートフィルタリング：VRF にインポートされるルートだけがローカルで保持されるため、ルーティング テーブルのサイズが制限されます。インポート ポリシーが変更された場合は、ルート リフレッシュを送信して、ルーティング アップデートの再送信を照会できます。
- アウトバウンドルートフィルタリング（ORF）：アップデートがネットワーク上に不必要に送信されないように、入力 PE が出力 PE にフィルタをアドバタイズできるようにします。
- ルート リフレクタ：ルート リフレクタ（RR）は、他の iBGP ピアから学習した iBGP ルートを伝播する内部 BGP（iBGP）ピアです。RR は iBGP セッションを集中させるために使用されます。

IPv6 MPLS VPN の高度な機能

IPv4 用のバーチャルプライベートネットワーク（VPN）からインターネットへのアクセス、マルチ自律システム バックボーン、Carrier Supporting Carrier（CSC）などの高度なマルチプロトコル ラベル スイッチング（MPLS）機能は、一般的に IPv6 でも IPv4 でも同じです。ただし、IPv6 over MPLS（6VPE）のアドレッシングと動作は、IPv4 バックボーン上とは違いがあります。

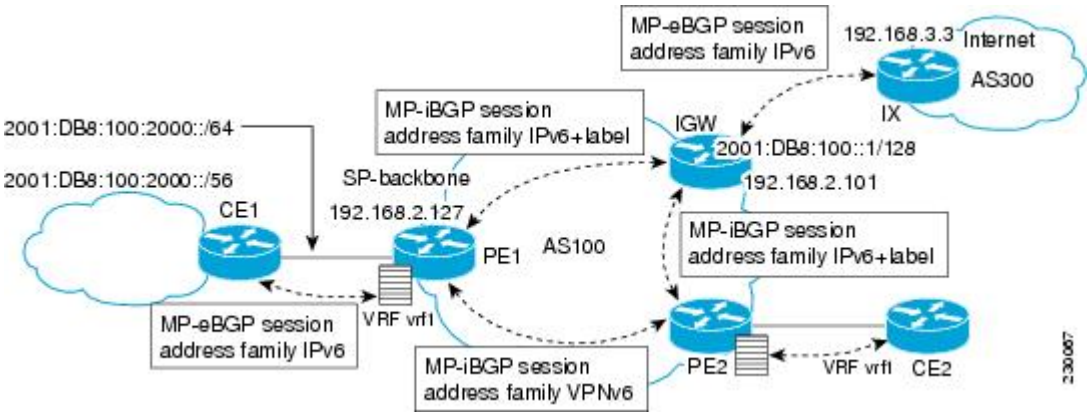
ここでは、高度な IPv6 MPLS VPN 機能の概念について説明します。

Internet Access

大部分のバーチャルプライベートネットワーク（VPN）サイトでインターネットへのアクセスが必要になります。RFC 4364 には、インターネットへの IPv4 および IPv6 VPN アクセスをイネーブルにするモデルセットが記載されています。あるモデルでは、1 つのインターフェイスがインターネットに接続するためにカスタマー エッジ（CE）によって使用され、別のインターフェイスが Virtual Routing and Forwarding（VRF）インスタンスに接続するために使用されます。別のモデルでは、すべてのインターネット ルートが VRF に再配布されます。ただし、このアプローチには、VRF ごとにインターネット ルートを複製する必要があるというデメリットがあります。

あるシナリオでは、IPv6デフォルトテーブルで見つかったインターネットゲートウェイを指すネクスト ホップとともに、スタティック ルートが VRF テーブルに挿入されます。下図に、このシナリオを示します。ここでは、インターネットアクセスが vrf1 という名前の VRF 内のカスタマーに提供されます。

図 *5*：インターネット アクセス トポロジ



インターネット経由でパブリック リソースにアクセスするカスタマー サイトは、パブリック プレフィックスによって認識されている必要があります。IPv4 とは異なり、IPv6 では、サイト境界から発信されたときにプライベート アドレスをパブリック アドレスに変換するネットワーク アドレス変換（NAT）メカニズムは提供されません。これは、サイト内のホストがパブリック アドレスで対話し、公的領域に現れることを意味します。

発信トラフィックの場合、入力プロバイダー エッジ（PE1）の VRF テーブルに設定されているデフォルト ルートは、VPN 外の宛先に向かうトラフィックをインターネット ゲートウェイに誘導します。

着信トラフィックでは、接続の PE（上図の PE1）を介してカスタマーサイトのトラフィックを送信するには、ルートがインターネット ゲートウェイに存在する必要があります。このルートは、入力 PE（PE1）により、（IPv6 アドレス ファミリ設定を含む）マルチプロトコル内部ボーダー ゲートウェイ プロトコル（iBGP）を使用して配布されます。そのため、インターネット ゲートウェイの VPN PE ごとに特別な設定を行う必要はありません。それでもなお、PE1 の着信トラフィックの場合は、サイトの VRF を指すカスタマー サイト グローバル プレフィックスのデフォルト テーブルに、ルートが存在している必要があります。

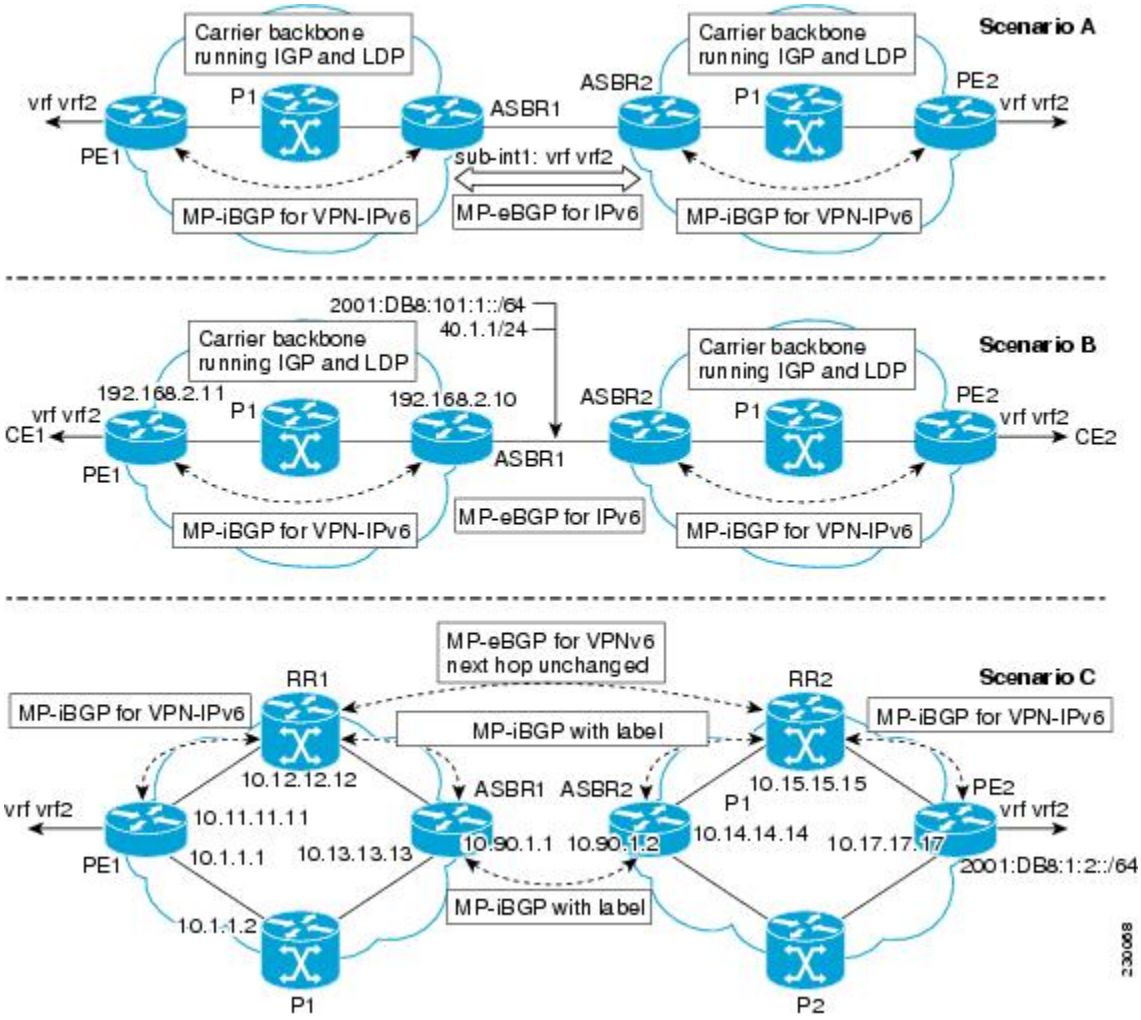
マルチ自律システム バックボーン

IPv4 が配置されていたすべての場所に IPv6 が配置されていると想定した場合、プロバイダー間バーチャル プライベート ネットワーク（VPN）の問題は、IPv6 および IPv4 で似ています。

自律システム境界を横断する IPv6配置の場合、プロバイダーはピアリング モデルを入手するか、または VPNv4 用に設置されているピアリング モデルを使用する必要があることがあります。

次の図は、IPv6 VPN におけるプロバイダー間のシナリオを示します。

図 *6*：プロバイダー間のシナリオ



自律システム境界ルータ（ASBR）間で使用されるネットワーク プロトコルに応じて、上図の 3 つのシナリオで複数の実装オプションを使用できます。たとえば、ASBR 間のマルチプロトコル外部 Border Gateway Protocol（eBGP）IPv6 VPN ピアリングを提案しているシナリオ B では、IPv6 または IPv4 リンクのどちらでも使用できます。

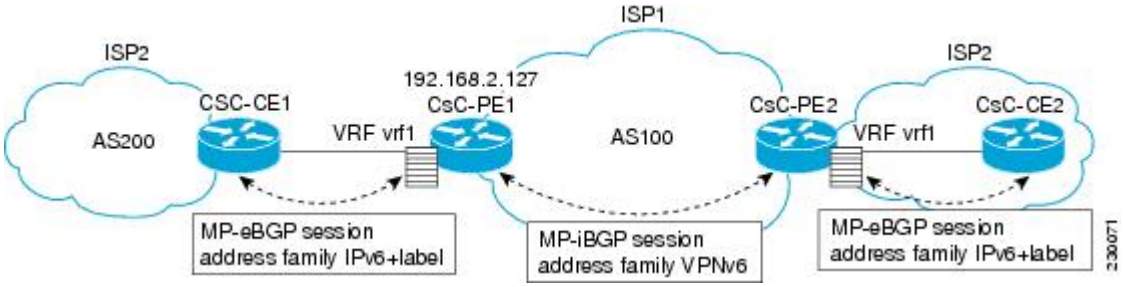
シナリオ C の場合、マルチホップ マルチプロトコル eBGP は、個々の自律システムのルート リフレクタ全体に IPv6 VPN ルートを再配布します。プロバイダー エッジ（PE）デバイスへのラベル付き IPv4 ルートは（IPv6 over MPLS の場合）、完全なラベル付きスイッチ パスがエンドツーエンドで設定されるように、ASBR 全体にアドバタイズされる必要があります。

Carrier Supporting Carrier

Carrier Supporting Carrier（CSC）機能はカスタマー サービス プロバイダーにバーチャル プライベート ネットワーク（VPN）アクセスを提供します。そのため、このサービスではインターネット サービス プロバイダー（ISP）マルチプロトコル ラベル スイッチング（MPLS）バックボーンを介してルートを交換し、トラフィックを送信する必要があります。通常のプロバイダー エッジ（PE）との唯一の違いは、CSC カスタマー エッジ（CE）から CSC-PE へのインターフェイス上に、IP から MPLS への転送ではなく MPLS から MPLS への転送を提供することです。

次の図に、2 つの ISP のインターフェイスの重要点を示します。

図 7：***CSC IPv6 over MPLS* の設定例**



IPv6 VPN over MPLS の設定方法

IPv6 用の Virtual Routing and Forwarding インスタンスの設定

Virtual Routing and Forwarding（VRF）インスタンスは、サポートされているアドレス ファミリごとにイネーブルにしたり設定したりできる、アドレス ファミリ非依存のオブジェクトです。VRF の設定は、次の 3 つの手順で構成されています。

- VRF のアドレス ファミリ非依存部分の設定
- VRF を使用するための IPv4 のイネーブル化および設定
- VRF を使用するための IPv6 のイネーブル化および設定

VRF には名前およびルート識別子（RD）が与えられます。RD は特定の Border Gateway Protocol（BGP）アドレス ファミリのコンテキスト内にある重複するアドレスを区別するために使用されるものですが、アドレス ファミリのコンテキスト外で設定されます。IPv4 VPN アドレスと IPv6 VPN アドレスとで別々の RD を持っていても問題はありません。Cisco デバイスでは、設定および VPN 管理を簡素化するために RD は同じになっています。

ユーザは、アドレス ファミリ コンテキストを使用しない場合に IPv4 と IPv6 間で共通のポリシーを設定できます。この機能はルート ターゲット（インポートおよびエクスポート）共有であり、

IPv4 ポリシーがすでに設定済みで、IPv6 ポリシーを IPv4 ポリシーと同じようにする必要がある移行シナリオで役立ちます。

IPv4 および IPv6 アドレス ファミリは、それぞれ個別にイネーブル化したり設定したりできます。このレベルで入力したルート ターゲット ポリシーは、アドレス ファミリ非依存の設定時に指定されている可能性のあるグローバル ポリシーに優先することに注意してください。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **mpls ipv6 vrf**
4. **vrf definition***vrf-name*
5. **rd***route-distinguisher*
6. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
7. **exit**
8. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf***vrf-name*] | **vrf***vrf-name*]
9. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
10. **exit**
11. **address-family ipv6** [**vrf***vrf-name*] [**unicast** | **multicast**]
12. **route-target** {**import** | **export** | **both**} *route-target-ext-community*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**mpls ipv6 vrf** 例： `Device(config)# mpls ipv6 vrf`	VRF 内で IPv6 をグローバルにイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**vrf definition***vrf-name* 例： `Device(config)# vrf definition vrf1`	VPN VRF ルーティング テーブルを設定し、VRF 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	**rd***route-distinguisher* 例： `Device(config-vrf)# rd 100:1`	VRF の RD を指定します。
ステップ 6	**route-target** {**import** | **export** | **both**} *route-target-ext-community* 例： `Device(config-vrf)# route target import 100:10`	IPv4 と IPv6 の両方のルート ターゲット VPN 拡張コミュニティを指定します。
ステップ 7	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了します。
ステップ 8	**address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf***vrf-name*] | **vrf***vrf-name*] 例： `Device(config)# 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、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。
ステップ 9	**route-target** {**import** | **export** | **both**} *route-target-ext-community* 例： `Device(config-vrf-af)# route target import 100:11`	IPv4 固有のルート ターゲット VPN 拡張コミュニティを指定します。
ステップ 10	**exit** 例： `Device(config-vrf-af)# exit`	この VRF のアドレス 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
ステップ 11	**address-family ipv6** [**vrf***vrf-name*] [**unicast** | **multicast**] 例： `Device(config-vrf)# address-family ipv6`	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 12	**route-target** {**import** | **export** | **both**} *route-target-ext-community* 例： `Device(config-vrf-af)# route target import 100:12`	IPv6 固有のルート ターゲット VPN 拡張コミュニティを指定します。

インターフェイスへの VRF のバインド

どのインターフェイスがどの Virtual Routing and Forwarding（VRF）インスタンスに属するかを指定するために、IPv4 と IPv6 の両方に対して **vrf forwarding** コマンドを使用します。インターフェイスは、複数の VRF に属すことはできません。インターフェイスが VRF にバインドされると、以前に設定したアドレス（IPv4 および IPv6）は削除されるため、再設定が必要になります。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***type number*
4. **vrf forwarding***vrf-name*
5. **ip address***ip-address mask* [**secondary**]
6. **ipv6address** {*ipv6-address*/*prefix-length* | *prefix-namesub-bits*/*prefix-length*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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	**configure terminal** 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	**interface***type number* 例： `Device(config)# interface GigabitEthernet 0/0/0`	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**vrf forwarding***vrf-name* 例： `Device(config-if)# vrf forwarding vrf1`	VPN 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。 • このコマンドを入力する前に設定されたすべての IPv4 または IPv6 アドレスが削除される点に注意してください。
ステップ 5	**ip address***ip-address mask* [**secondary**] 例： `Device(config-if)# ip address 10.10.10.1 255.255.255.0`	インターフェイスに IPv4 アドレスを設定します。
ステップ 6	**ipv6address** {*ipv6-address*/*prefix-length* | *prefix-namesub-bits*/*prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:100:1::1/64`	インターフェイスに IPv6 アドレスを設定します。

PE から CE へのルーティング用のスタティック ルートの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **ipv6route** [**vrf***vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-typeinterface-number* [*ipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag***tag*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**ipv6route** [**vrf***vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-typeinterface-number* [*ipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag***tag*] 例： `Device(config)# ipv6 route vrf vrf1 ::/0 2001:DB8:200::1 nexthop-vrf default`	指定したネクストホップを使用して、指定した IPv6 スタティック ルートをインストールします。

eBGP の PE から CE へのルーティング セッションの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router bgp***autonomous-system-number*
4. **address-family ipv6** [**vrf***vrf-name*] [**unicast** | **multicast**]
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number*
6. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp***autonomous-system-number* 例： `Device(config)# router bgp 100`	ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロセスを設定します。
ステップ 4	**address-family ipv6** [**vrf***vrf-name*] [**unicast** | **multicast**] 例： `Device(config-router)# address-family ipv6 vrf vrf1`	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 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router-af)# neighbor 2001:DB8:100:1::2 remote-as 200`	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 6	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 2001:DB8:100:1::2 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。

iBGP 用の IPv6 VPN アドレス ファミリの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router bgp***autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number*
6. **address-family vpnv6** [**unicast**]
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate**
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
9. **extended**] **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp***autonomous-system-number* 例： `Device(config)# router bgp 100`	BGP ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor 192.168.2.11 remote-as 100`	マルチプロトコル Border Gateway Protocol（BGP）ネイバー テーブルにエントリを追加します。 • IPv6 VPN の場合、BGP セッションを IPv4 ベースのコア ネットワークで転送できるようにするために、ピア アドレスは一般的に IPv4 アドレスになります。

	コマンドまたはアクション	目的
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number* 例： `Device(config-router)# neighbor 192.168.2.11 update-source Loopback 0`	BGPセッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 6	**address-family vpnv6** [**unicast**] 例： `Device(config-router)# address-family vpnv6`	ルーティングセッションを設定するために、デバイスをアドレスファミリ コンフィギュレーションモードに設定します。
ステップ 7	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 192.168.2.11 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**] 例： `Device(config-router-af)# neighbor 192.168.2.11 send-community extended`	コミュニティ属性をBGPネイバーに送信する必要があることを指定します。
ステップ 9	**extended**] **exit** 例： `Device(config-router-af)# exit`	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。

スケーラビリティ向上のためのルート リフレクタの設定

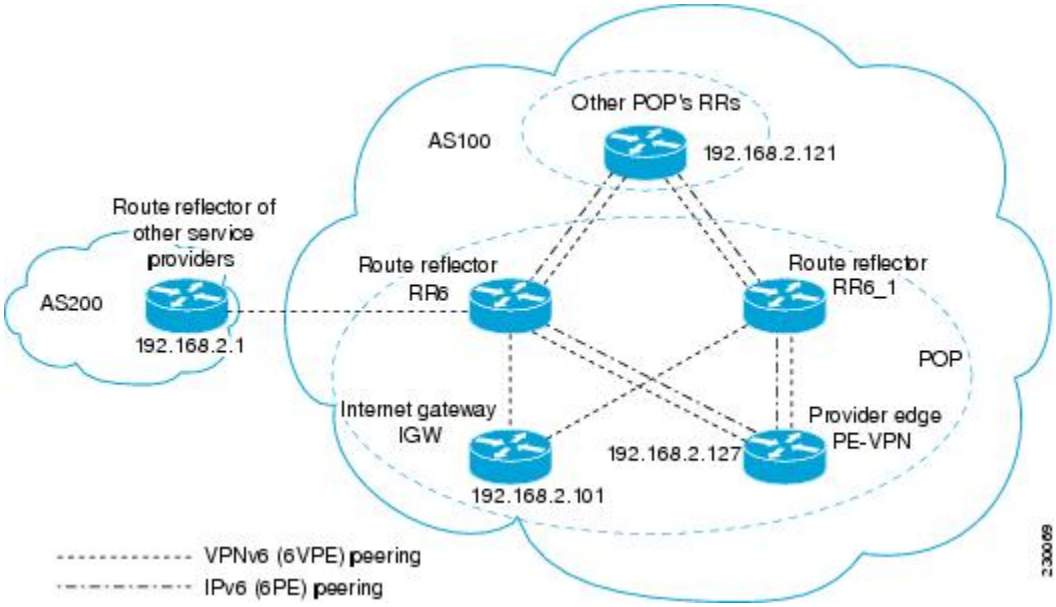
この作業では、冗長性のために 2 つのルート リフレクタ（RR）が設定されます。RR を配置すると、Border Gateway Protocol（BGP）セッションの数が大幅に削減され、これによりスケーラビリティが向上します。通常、1 つの RR が内部ボーダー ゲートウェイ プロトコル（IBGP）スピーカーとピアリングして、BGP セッションの完全メッシュが防止されます。

マルチプロトコル ラベル スイッチング（MPLS）ベースのコアの場合、RR はラベル スイッチ パスの一部ではないため、ネットワーク内の任意の場所に配置できます。たとえば、フラットな RR

設計では、RR はレベル 1 の Point of Presence（POP）に配置でき、完全メッシュ トポロジで互いにピアリングします。階層型の RR 設計では、RR はレベル 1 とレベル 2 の POP に配置でき、レベル 1 POP で互いにピアリングし、レベル 2 の RR ともピアリングします。

既存の MPLS ネットワーク（たとえば、VPNv4 サービスを提供するネットワーク）に IPv6 over MPLS（6VPE）を配置する一般的なケースでは、一部の RR 設計がすでに実施されている可能性が高く、IPv6 バーチャル プライベート ネットワーク（VPN）サービス用に同様の RR インフラストラクチャを配置できます。次の図に、ISP POP 内の RR とその RR クライアント セット間の主なピアリング ポイントを示します。

図 *8*：ルート リフレクタのピアリング設計



次のリストの BGP RR クライアントを、各 POP の IPv6 RR（上記の図の RR6 および RR6_1）デバイスごとに設定する必要があります。

- ISP カスタマーに IPv6 VPN アクセスを提供する POP のプロバイダー エッジ（PE）デバイス（PE-VPN）。これには、カスタマー サイトを相互接続するための IPv6 VPN（6VPE）ピアリングと、VPN カスタマーにインターネット アクセスを提供するための IPv6 ピアリング（6PE）の両方が含まれます（「インターネット アクセスの設定」を参照）。
- PE カスタマーに IPv6 インターネットへのアクセスを提供するために、POP 内に配置されるインターネット ゲートウェイ（IGW）（「インターネット アクセスの設定」を参照）。
- 他のサービス プロバイダーの RR。この機能は、相互自律システムの接続を提供するために使用されるもので、IPv6 と IPv6 VPN ピアリングの両方が含まれます。このサービスについては、「IPv6 VPN 用のマルチ自律システム バックボーンの設定」で説明します。
- 他の POP 内の RR。IPv6 と IPv6 VPN の両方のアドレス ファミリがイネーブルになっている場合、すべての RR が互いにピアリングします。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerbgp***autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number*
6. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number*
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number*
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number*
9. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number*
10. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number*
11. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number*
12. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]
13. **address-familyipv6**
14. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
15. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**
16. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**
17. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
18. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**
19. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**
20. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
21. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**
22. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**
23. **exit**
24. **address-familyvpnv6** [**unicast**
25. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
26. **neighbor**{*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
27. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**
28. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
29. **neighbor**{*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
30. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**
31. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
32. **neighbor**{*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
33. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**
34. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **next-hop-unchanged** [**allpaths**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**routerbgp***autonomous-system-number* 例： `Device(config)# router bgp 100`	BGP ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor 192.168.2.101 remote-as 100`	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て、インターネット アクセスを提供するためにインターネット ゲートウェイとのピアリングを提供します。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number* 例： `Device(config-router)# neighbor 192.168.2.101 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 6	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor 192.168.2.121 remote-as 100`	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て、他の POP の RR とのピアリングを提供します。
ステップ 7	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number* 例： `Device(config-router)# neighbor 192.168.2.121 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレ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 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor 192.168.2.127 remote-as 100`	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 9	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number* 例： `Device(config-router)# neighbor 192.168.2.127 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 10	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor 192.168.2.1 remote-as 200`	（任意）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て、VPN 間サービスを提供するためにピア ISP の RR とのピアリングを提供します。
ステップ 11	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number* 例： `Device(config-router)# neighbor 192.168.2.1 update-source Loopback 0`	（任意）BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 12	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*] 例： `Device(config-router)# neighbor 192.168.2.1 ebgp-multihop`	（任意）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 13	**address-familyipv6** 例： `Device(config-router)# address-family ipv6`	（任意）インターネット アクセス サービスを提供するために、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。

	コマンドまたはアクション	目的
ステップ 14	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** 例： `Device(config-router-af)# neighbor 192.168.2.101 activate`	（任意）このアドレス ファミリの情報を、指定したネイバーと交換できるようにします。
ステップ 15	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** 例： `Device(config-router-af)# neighbor 192.168.2.101 send-label`	（任意）BGP ルートを介して MPLS ラベルをネイバー BGP デバイスに送信できるよう、BGP デバイスを有効化します。
ステップ 16	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client** 例： `Device(config-router-af)# neighbor 192.168.2.101 route-reflector-client`	（任意）デバイスを 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 17	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** 例： `Device(config-router-af)# neighbor 192.168.2.121 activate`	（任意）このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 18	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** 例： `Device(config-router-af)# neighbor 192.168.2.121 send-label`	（任意）BGP ルートを介して MPLS ラベルをネイバー BGP デバイスに送信できるよう、BGP デバイスを有効化します。
ステップ 19	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client** 例： `Device(config-router-af)# neighbor 192.168.2.121 route-reflector-client`	（任意）指定したネイバーをルート リフレクタクライアントとして設定します。

	コマンドまたはアクション	目的
ステップ 20	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** 例： `Device(config-router-af)# neighbor 192.168.2.127 activate`	（任意）このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 21	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** 例： `Device(config-router-af)# neighbor 192.168.2.127 send-label`	（任意）BGP ルートを介して MPLS ラベルをネイバー BGP デバイスに送信できるよう、BGP デバイスを有効化します。
ステップ 22	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client** 例： `Device(config-router-af)# neighbor 192.168.2.127 route-reflector-client`	（任意）指定したネイバーをルート リフレクタ クライアントとして設定します。
ステップ 23	**exit** 例： `Device(config-router-af)# exit`	（任意）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。
ステップ 24	**address-familyvpnv6** [**unicast** 例： `Device(config-router)# address-family vpnv6`	ルーティング セッションを設定するために、デバイスをアドレスファミリ コンフィギュレーション モードに設定します。
ステップ 25	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** 例： `Device(config-router-af)# neighbor 192.168.2.121 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 26	**neighbor**{*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**] 例： `Device(config-router-af)# neighbor 192.168.2.21 send-community extended`	コミュニティ属性を BGP ネイバーに送信する必要があることを指定します。

	コマンドまたはアクション	目的
ステップ 27	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client** 例： `Device(config-router-af)# neighbor 192.168.2.121 route-reflector-client`	指定したネイバーをルート リフレクタ クライアントとして設定します。
ステップ 28	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** 例： `Device(config-router-af)# neighbor 192.168.2.127 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 29	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**] 例： `Device(config-router-af)# neighbor 192.168.2.127 send-community extended`	コミュニティ属性を BGP ネイバーに送信する必要があることを指定します。
ステップ 30	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client** 例： `Device(config-router-af)# neighbor 192.168.2.127 route-reflector-client`	指定したネイバーをルート リフレクタ クライアントとして設定します。
ステップ 31	**neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate** 例： `Device(config-router-af)# neighbor 192.168.2.1 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 32	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**] 例： `Device(config-router-af)# neighbor 192.168.2.1 send-community extended`	コミュニティ属性を BGP ネイバーに送信する必要があることを指定します。

	コマンドまたはアクション	目的
ステップ 33	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client** 例： `Device(config-router-af)# neighbor 192.168.2.1 route-reflector-client`	指定したネイバーをルート リフレクタ クライアントとして設定します。
ステップ 34	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **next-hop-unchanged** [**allpaths** 例： `Device(config-router-af)# neighbor 192.168.2.1 next-hop-unchanged allpaths`	EBGP マルチホップ ピアで、パスのネクストホップを変更せずに伝播できるようにします。

インターネット アクセスの設定

IPv6 バーチャル プライベート ネットワーク（VPN）アクセスを持つお客様は、IPv6 を介してインターネットにアクセスできる必要があります。このサービスの設計は、グローバル インターネット アクセス サービスと似ています。レベル 1 Point Of Presence（POP）に配置されている IPv6 VPN over MPLS（6VPE）デバイス（IGW デバイスと共存）はネイティブにインターネット ゲートウェイ（IGW）にアクセスできますが、レベル 2 およびレベル 3 POP に配置されている、IGW に直接アクセスできない 6VPE デバイスは、6PE を介して最も近いレベル 1 POP の IGW にアクセスできます。

このような 6VPE デバイスで VPN インターネット アクセスを設定するには、IGW との Border Gateway Protocol（BGP）ピアリングの設定が必要になります（多くの場合、「スケーラビリティ向上のためのルート リフレクタの設定」の項で説明したように、IPv6 RR を使用します）。次に、ユーザは、プライベート ドメイン（VRF）とパブリック ドメイン（インターネット）間の通信をイネーブルにするように、相互テーブル ルーティングを設定する必要があります。

上図に、次の設定作業を示します。

インターネット ゲートウェイの設定

VPN PE への iBGP 6PE ピアリングの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router bgp***autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number*
6. **address-family ipv6**
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate**
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp***autonomous-system-number* 例： `Device(config)# router bgp 100`	ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor 192.168.2.127 remote-as 100`	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て、バーチャル プライベート ネットワーク（VPN）プロバイダーエッジ（PE）とのピアリングを提供します。

	コマンドまたはアクション	目的
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number* 例： `Device(config-router)# neighbor 192.168.2.127 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 6	**address-family ipv6** 例： `Device(config-router)# address-family ipv6`	グローバルテーブルの到達可能性を交換するために、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 7	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 192.168.2.127 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** 例： `Device(config-router-af)# neighbor 192.168.2.127 send-label`	BGP ルートとともにマルチプロトコル ラベル スイッチング（MPLS）ラベルをネイバー BGP デバイスに送信できるように BGP デバイスを設定して、PE VPN が MPLS を介してインターネット ゲートウェイに到達できるようにします。

パブリック ドメインへのゲートウェイとしてのインターネット ゲートウェイの設定

「VPN PE への iBGP 6PE ピアリングの設定」で設定した 6PE ピアリング設定を使用します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router bgp***autonomous-system-number*
4. **address-family ipv6**
5. **network***ipv6-address*/*prefix-length*
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp***autonomous-system-number* 例： `Device(config)# router bgp 100`	ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロセスを設定します。
ステップ 4	**address-family ipv6** 例： `Device(config-router)# address-family ipv6`	グローバルテーブルの到達可能性を交換するために、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 5	**network***ipv6-address/prefix-length* 例： `Device(config-router-af)# network 2001:DB8:100::1/128`	プロバイダーエッジ（PE）バーチャルプライベートネットワーク（VPN）によって使用されるネクストホップのネットワーク ソースを設定します。
ステップ 6	**exit** 例： `Device(config-router-af)# exit`	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。

インターネットへの eBGP ピアリングの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router bgp***autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number*
5. **address-family ipv6**
6. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate**
7. **aggregate-address***addressmask* [**as-set**] [**summary-only**] [**suppress-map***map-name*] [**advertise-map***map-name*] [**attribute-map***map-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp***autonomous-system-number* 例： `Device(config)# router bgp 100`	ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor FE80::300::1 GigabitEthernet0/0/0 remote-as 300`	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て、PE（PE-VPN）とのピアリングを提供します。 • ピアリングは、リンクローカル アドレス経由で行われることに注意してください。
ステップ 5	**address-family ipv6** 例： `Device(config-router)# address-family ipv6`	グローバル テーブルの到達可能性を交換するために、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。

	コマンドまたはアクション	目的
ステップ 6	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor FE80::300::1 GigabitEthernet0/0/0 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 7	**aggregate-address***addressmask* [**as-set**] [**summary-only**] [**suppress-map***map-name*] [**advertise-map***map-name*] [**attribute-map***map-name*] 例： `Device(config-router-af)# aggregate-address 2001:DB8::/32 summary-only`	集約プレフィックスを作成してから、インターネットにアドバタイズします。

IPv6 VPN PE の設定

VRF からインターネット ゲートウェイへのデフォルト スタティック ルートの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6route** [**vrf***vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-typeinterface-number* [*ipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag***tag*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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	**configureterminal** 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	**ipv6route** [**vrf***vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-typeinterface-number* [*ipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag***tag*] 例： `Device(config)# ipv6 route vrf vrf1 ::/0 2001:DB8:100::1 nexthop-vrf default`	発信トラフィックを VRF から発信できるようにするために、VRF からインターネット ゲートウェイへのデフォルト スタティック ルートを設定します。

デフォルト テーブルから VRF へのスタティック ルートの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6route** [**vrf***vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-typeinterface-number* [*ipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag***tag*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**ipv6route** [**vrf***vrf-name*] *ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-typeinterface-number* [*ipv6-address*]} [**nexthop-vrf** [*vrf-name1* | **default**]] [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [*next-hop-address*] [**tag***tag*] 例： `Device(config)# ipv6 route 2001:DB8:100:2000::/64 nexthop-vrf vrf1`	着信トラフィックが VRF に到達できるようにするために、デフォルト テーブルから VRF へのスタティック ルートを設定します。

インターネット ゲートウェイへの iBGP 6PE ピアリングの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router bgp***autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number*
6. **address-family ipv6** [**vrf***vrf-name*] [**unicast** | **multicast**]
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate**
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**
9. **network***ipv6-address*/*prefix-length*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp***autonomous-system-number* 例： `Device(config)# router bgp 100`	ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor 192.168.2.101 remote-as 100`	インターネット ゲートウェイとピアリングするために、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 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number* 例： `Device(config-router)# neighbor 192.168.2.101 update-source Loopback 0`	BGPセッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 6	**address-family ipv6** [**vrf***vrf-name*] [**unicast** | **multicast**] 例： `Device(config-router)# address-family ipv6`	グローバルテーブルの到達可能性を交換するために、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 7	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 192.168.2.101 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** 例： `Device(config-router-af)# neighbor 192.168.2.101 send-label`	バーチャル プライベート ネットワーク（VPN）プロバイダー エッジ（PE）がマルチプロトコル ラベル スイッチング（MPLS）を介してインターネット ゲートウェイに到達できるようにするために、このネイバーに対するこのアドレス ファミリのラベル交換を有効にします。
ステップ 9	**network***ipv6-address*/*prefix-length* 例： `Device(config-router-af)# network 2001:DB8:100:2000::/64`	Virtual Routing and Forwarding（VRF）プレフィックスをインターネット ゲートウェイに提供します。

IPv6 VPN 用のマルチ自律システム バックボーンの設定

2 つのバーチャル プライベート ネットワーク（VPN）サイトは異なるサービス プロバイダーに接続されているため、これらのサイトを異なる自律システムに接続できます。この場合、その VPN に接続されているプロバイダー エッジ（PE）デバイスは、内部ボーダー ゲートウェイ プロトコル（iBGP）接続を互いに維持したり、共通のルート リフレクタを使用して維持したりすることはできません。この状況では、何らかの方法で外部 BGP（eBGP）を使用して、VPN-IPv6 アドレスを配布する必要があります。

次に、2 つのシナリオでの設定例を示します。1 つは、自律システム境界ルータ（ASBR）間のマルチプロトコル eBGP-IPv6 VPN ピアリングで IPv4 リンクを使用し、もう 1 つは同じピアリングで IPv6 リンクを使用します。ASBR 間のピアリングが IPv4 リンク経由で実行される場合、ASBR1 の BGP 設定は次のようになります。

```
router bgp 1001
no bgp default ipv4-unicast
no bgp default route-target filter
neighbor 192.1.1.1 remote-as 1002
neighbor 192.168.2.11 remote-as 1001
neighbor 192.168.2.11 update-source Loopback1
!
 address-family vpnv6
!Peering to ASBR2 over an IPv4 link
 neighbor 192.1.1.1 activate
 neighbor 192.1.1.1 send-community extended
!Peering to PE1 over an IPv4 link
 neighbor 192.168.2.11 activate
 neighbor 192.168.2.11 next-hop-self
 neighbor 192.168.2.11 send-community extended
```

ASBR 間のピアリングが IPv6 リンク経由で実行される場合、ASBR1 の BGP 設定は次のようになります。

```
router bgp 1001
neighbor 2001:DB8:101::72d remote-as 1002
!
 address-family vpnv6
!Peering to ASBR2 over an IPv6 link
 neighbor 2001:DB8:101::72d activate
 neighbor 2001:DB8:101::72d send-community extended
```

次の複数の作業は、マルチホップ マルチプロトコル eBGP を使用して個々の自律システムのルート リフレクタ（RR）全体に VPN ルートを再配布する、マルチ自律システム バックボーン用の PE VPN を設定する方法を示しています。PE へのラベル付き IPv4 ルートは、完全なラベル スイッチ パス（LSP）がエンドツーエンドで設定されるように、ASBR 全体にアドバタイズされます。

このシナリオでは、ASBR は VPN 対応ではなく、RR だけが VPN 対応になっています。次の設定を有効にし、かつ理解しておく必要があります。

- ASBR では、ピアリングするサービス プロバイダーに PE のループバック アドレスを提供しています。提供される内容は次のとおりです。
  - リモート サービス プロバイダーのロケーションでネクストホップ解決をイネーブルにするための、VPN PE の IPv4 ループバック アドレス（/32）。

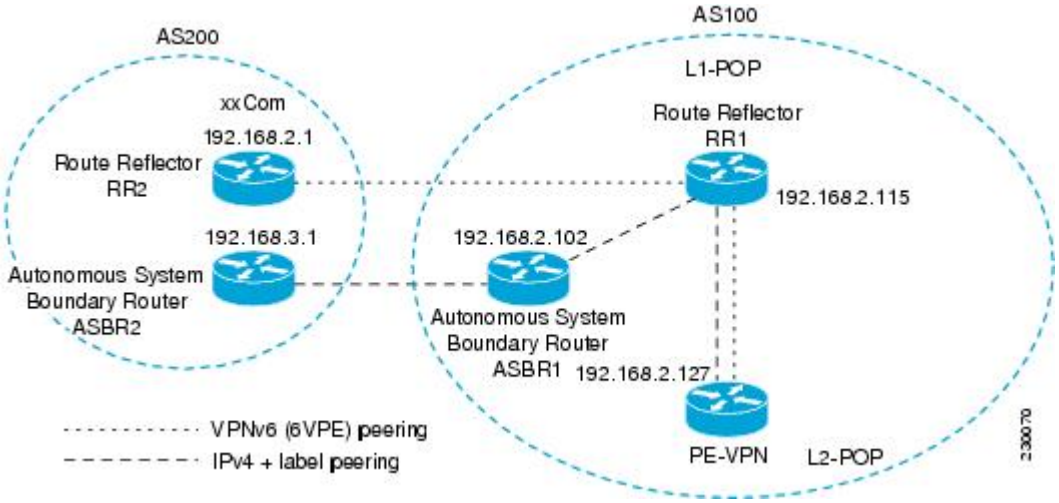
- プロバイダー間（RR 間）eBGP ピアリングをイネーブルにするための、VPN RR の IPv4 ループバック アドレス（/32）。

- VPN PE の IPv4 ループバック アドレスの場合、ラベルがエンドツーエンド LSP を確立するように、アドレス提供は、ラベルとともにリモート PE までマルチプロトコル BGP を介して実行されます。そのため、次の MP-BGP ピアリングが VPNv4 用に設定されています。
  - VPN PE は VPN RR と iBGP ピアリングする。
  - ASBR は VPN RR と iBGP ピアリングする。
  - ASBR はリモート サービス プロバイダーの ASBR と eBGP ピアリングする。
- 各サービス プロバイダーの VPN RR は、eBGP を介して互いにピアリングして、VPN ルートを交換します。エンドツーエンド LSP が RR 経由にならないように、ネクスト ホップは変更せずに転送されます。

このシナリオで IPv6 VPN 相互自律システム アクセスをイネーブルにするには、ISP 側で PE VPN および RR での設定を変更する必要があります。同様のサービスを VPNv4 に提供するには、同じ RR を設定します。この場合、RR と ASBR 間のピアリングおよび ASBR 間のピアリングは IPv4 VPN と IPv6 VPN の両方で使用される IPv4 ネクストホップのラベルを交換するだけなので、ASBR は完全に IPv6 非対応のままであり、ここで必要な設定変更はありません。

次の図に、PE-VPN デバイス（IPv6 VPN アクセスを提供）から xxCom ネットワークへの IPv6 プロバイダー間接続をイネーブルにするために必要な BGP ピアリング ポイントを示します。

図 *9*：相互自律システム シナリオ *C* をイネーブルにするための *BGP* ピアリング ポイント



レベル 2 Point Of Presence（POP）にある IPv6 VPN PE から相互自律システム通信をイネーブルにするには、次の追加の BGP ピアリングが必要です。

- PE VPN から、RR1 という名前のルート リフレクタへの、ラベルを伴う IPv4 ピアリング（VPNv4相互自律システムが同じLSPを使用して同じノードに配置されている場合は、すでに設定されています）。
- RR1 から ASBR1 への、ラベルを伴う IPv4 ピアリング
- ASBR1 と ASBR2 間の、ラベルを伴う IPv4 ピアリング
- IPv6 VPN ルートを交換するための、RR1 と RR2（他の自律システムのルート リフレクタ）間の IPv6 VPN ピアリング
- RR1 との IPv6 VPN ピアリングIPv6 VPN サービスを拡張するために使用されているそのルートリフレクタが自律システム機能に使用されている場合、この機能もまたすでに設定済みである可能性があります（「スケーラビリティ向上のためのルート リフレクタの設定」を参照）。

IPv6 VPN 用のマルチ自律システム バックボーンの設定は、次の作業で構成されます。

マルチ自律システム バックボーン用の PE VPN の設定

ルート リフレクタへの iBGP IPv6 VPN ピアリングの設定

RR1 という名前のルート リフレクタへの内部ボーダー ゲートウェイ プロトコル（IBGP）IPv6 バーチャルプライベートネットワーク（VPN）ピアリングを設定するには、次の作業を実行します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router bgp***autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number*
6. **address-family vpnv6** [**unicast**]
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate**
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
9. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp***autonomous-system-number* 例： `Device(config)# router bgp 100`	BGP ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor 192.168.2.115 remote-as 100`	相互自律システム機能を備えたルート リフレクタとピアリングするために、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 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number* 例： `Device(config-router)# neighbor 192.168.2.115 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 6	**address-family vpnv6** [**unicast**] 例： `Device(config-router)# address-family vpnv6`	（任意）ルーティング セッションを設定するために、デバイスをアドレス ファミリ コンフィギュレーション モードに設定します。
ステップ 7	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 192.168.2.115 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]	コミュニティ属性を BGP ネイバーに送信する必要があることを指定します。

	コマンドまたはアクション	目的
	例： `Device(config-router-af)# neighbor 192.168.2.115 send-community extended`	
ステップ 9	**exit** 例： `Device(config-router-af)# exit`	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。

ルート リフレクタへの IPv4 とラベルの iBGP ピアリングの設定

RR1 という名前のルート リフレクタへの IPv4 およびラベルの内部ボーダー ゲートウェイ プロトコル（IBGP）ピアリングを設定するには、次の作業を実行します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router bgp***autonomous-system-number*
4. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf***vrf-name*] | **vrf***vrf-name*]
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate**
6. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp***autonomous-system-number* 例： `Device(config)# router bgp 100`	BGP ルーティング プロセスを設定します。
ステップ 4	**address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf***vrf-name*] | **vrf***vrf-name*] 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、標準IPv4アドレスプレフィックスを使用するルーティング セッションを設定します。
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 192.168.2.115 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 6	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** 例： `Device(config-router-af)# neighbor 192.168.2.115 send-label`	エンドツーエンド ラベル スイッチ パス（LSP）を設定するためのラベルとともにリモートプロバイダーエッジ（PE）ピア IPv4 ループバックを RR1 経由で受信するために、このネイバーに対するこのアドレス ファミリのラベル交換を有効にします。

マルチ自律システム バックボーン用のルート リフレクタの設定

PE VPN へのピアリングの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router bgp***autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number*
6. **address-family vpnv6** [**unicast**]
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate**
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
9. **exit**
10. **address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf***vrf-name*] | **vrf***vrf-name*]
11. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate**
12. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**
13. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp***autonomous-system-number* 例： `Device(config)# router bgp 100`	ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロセスを設定します。

	コマンドまたはアクション	目的
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor 192.168.2.115 remote-as 100`	InterAS 用のルート リフレクタとピアリングするために、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 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number* 例： `Device(config-router)# neighbor 192.168.2.115 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 6	**address-family vpnv6** [**unicast**] 例： `Device(config-router)# address-family vpnv6`	（任意）デバイスをアドレス ファミリ コンフィギュレーション モードに設定します。
ステップ 7	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 192.168.2.115 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**] 例： `Device(config-router-af)# neighbor 192.168.2.115 send-community extended`	コミュニティ属性を BGP ネイバーに送信する必要があることを指定します。
ステップ 9	**exit** 例： `Device(config-router-af)# exit`	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。
ステップ 10	**address-family ipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf***vrf-name*] | **vrf***vrf-name*] 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、標準 IPv4 アドレス プレフィックスを使用するルーティング 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
ステップ 11	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 192.168.2.115 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 12	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** 例： `Device(config-router-af)# neighbor 192.168.2.115 send-label`	エンドツーエンドラベルスイッチパス（LSP）を設定するためのラベルとともにリモート PE IPv4 ループバックをローカル プロバイダー エッジ（PE）に送信するために、このネイバーに対するこのアドレス ファミリのラベル交換を有効にします。
ステップ 13	**exit** 例： `Device(config-router-af)# exit`	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。

ルート リフレクタの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router bgp***autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number*
6. **address-family vpnv6** [**unicast**]
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate**
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
9. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client**
10. **exit**
11. **address-familyipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf***vrf-name*] | **vrf***vrf-name*]
12. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate**
13. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**
14. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp***autonomous-system-number* 例： `Device(config)# router bgp 100`	ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor 192.168.2.127 remote-as 100`	インターンのバーチャル プライベート ネットワーク（VPN）プロバイダー エッジ（PE）とピアリングするため、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 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number* 例： `Device(config-router)# neighbor 192.168.2.127 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 6	**address-family vpnv6** [**unicast**] 例： `Device(config-router)# address-family vpnv6`	（任意）デバイスをアドレス ファミリ コンフィギュレーション モードに設定します。
ステップ 7	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 192.168.2.127 activate`	このアドレス ファミリの情報を、指定したネイバーと交換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 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**] 例： `Device(config-router-af)# neighbor 192.168.2.127 send-community extended`	コミュニティ属性を BGP ネイバーに送信する必要があることを指定します。
ステップ 9	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **route-reflector-client** 例： `Device(config-router-af)# neighbor 192.168.2.127 route-reflector-client`	指定したネイバーをルート リフレクタ クライアントとして設定します。
ステップ 10	**exit** 例： `Device(config-router-af)# exit`	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。
ステップ 11	**address-familyipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf***vrf-name*] | **vrf***vrf-name*] 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、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。
ステップ 12	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 192.168.2.127 activate`	このアドレスファミリの情報を、指定したネイバーと交換できるようにします。
ステップ 13	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** 例： `Device(config-router-af)# neighbor 192.168.2.127 send-label`	エンドツーエンドLSPを設定するためのラベルとともにリモート PE IPv4 ループバックをローカル PE に送信するために、このネイバーに対するこのアドレスファミリのラベル交換をイネーブルにします。
ステップ 14	**exit** 例： `Device(config-router-af)# exit`	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。

自律システム境界ルータとのピアリングの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerbgp***autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number*
6. **address-familyipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf***vrf-name*] | **vrf***vrf-name*]
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate**
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**routerbgp***autonomous-system-number* 例： `Device(config)# router bgp 100`	ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor 192.168.2.102 remote-as 100`	ASBR1 とピアリングするために、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。

	コマンドまたはアクション	目的
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number* 例： `Device(config-router)# neighbor 192.168.2.102 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 6	**address-familyipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf***vrf-name*] | **vrf***vrf-name*] 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、標準IPv4アドレスプレフィックスを使用するルーティング セッションを設定します。
ステップ 7	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 192.168.2.102 activate`	このアドレスファミリの情報を、指定したBGPネイバーと交換できるようにします。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** 例： `Device(config-router-af)# neighbor 192.168.2.102 send-label`	エンドツーエンドラベル スイッチ パス（LSP）を設定するラベルとともにリモート PE IPv4 ループバックを受信するために、このネイバーに対するこのアドレス ファミリのラベル交換を有効にします。

別の ISP ルート リフレクタとのピアリングの設定

インターネット サービス プロバイダー（ISP）ルート リフレクタ RR2 とのピアリングを設定するには、次の作業を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerbgp***autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number*
6. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]
7. **address-familyvpnv6** [**unicast**]
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate**
9. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
10. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **next-hop-unchanged** [**allpaths**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**routerbgp***autonomous-system-number* 例： `Device(config)# router bgp 100`	ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor 192.168.2.1 remote-as 100`	RR2 とピアリングする外部 BGP（eBGP）のために、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 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number*	BGP セッションで、指定したインターフェイスの送信元アドレ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
	例： `Device(config-router)# neighbor 192.168.2.1 update-source Loopback 0`	
ステップ 6	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*] 例： `Device(config-router)# neighbor 192.168.2.1 ebgp-multihop`	（任意）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 7	**address-familyvpnv6** [**unicast**] 例： `Device(config-router)# address-family vpnv6`	（任意）ルーティング セッションを設定するために、デバイスをアドレス ファミリ コンフィギュレーション モードに設定します。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 192.168.2.1 activate`	このアドレス ファミリの情報を、指定したBGPネイバーと交換できるようにします。
ステップ 9	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**] 例： `Device(config-router-af)# neighbor 192.168.2.1 send-community extended`	コミュニティ属性をBGPネイバーに送信する必要があることを指定します。
ステップ 10	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **next-hop-unchanged** [**allpaths**] 例： `Device(config-router-af)# neighbor 192.168.2.1 next-hop-unchanged allpaths`	eBGP マルチホップ ピアで、パスのネクスト ホップを変更せずに伝播できるようにします。

ASBR の設定

ルート リフレクタ RR1 とのピアリングの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerbgp***autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number*
6. **address-familyipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf***vrf-name*] | **vrf***vrf-name*
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate**
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**
9. exit

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**routerbgp***autonomous-system-number* 例： `Device(config)# router bgp 100`	ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor 192.168.2.115 remote-as 100`	RR1 とピアリングするために、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。

	コマンドまたはアクション	目的
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number* 例： `Device(config-router)# neighbor 192.168.2.115 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 6	**address-familyipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf***vrf-name*] | **vrf***vrf-name* 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、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。
ステップ 7	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 192.168.2.115 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** 例： `Device(config-router-af)# neighbor 192.168.2.115 send-label`	エンドツーエンド ラベル スイッチ パス（LSP）を設定するためのラベルとともにリモート PE IPv4 ループバックをローカル PE に送信するために、このネイバーに対するこのアドレス ファミリのラベル交換を有効にします。
ステップ 9	exit 例： `Device(config-router-af)# exit`	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。

他の ISP ASBR2 とのピアリングの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **routerbgp***autonomous-system-number*
4. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number*
5. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number*
6. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]
7. **address-familyipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf***vrf-name*] | **vrf***vrf-name*]
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate**
9. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**
10. **network** {*network-number* [**mask***network-mask*] | *nsap-prefix*} [**route-map***map-tag*]
11. **network** {*network-number* [**mask***network-mask*] | *nsap-prefix*} [**route-map***map-tag*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**routerbgp***autonomous-system-number* 例： `Device(config)# router bgp 100`	ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロセスを設定します。
ステップ 4	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router)# neighbor 192.168.3.1 remote-as 100`	ASBR2 とピアリングするために、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。

	コマンドまたはアクション	目的
ステップ 5	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source***interface-typeinterface-number* 例： `Device(config-router)# neighbor 192.168.3.1 update-source Loopback 0`	BGP セッションで、指定したインターフェイスの送信元アドレスを使用できるようにします。
ステップ 6	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*] 例： `Device(config-router)# neighbor 192.168.3.1 ebgp-multihop`	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 7	**address-familyipv4** [**mdt** | **multicast** | **tunnel** | **unicast** [**vrf***vrf-name*] | **vrf***vrf-name*] 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、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor 192.168.3.1 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 9	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** 例： `Device(config-router-af)# neighbor 192.168.3.1 send-label`	エンドツーエンド ラベル スイッチ パス（LSP）を設定するため、ラベルとともにリモート プロバイダー エッジ（PE）IPv4 ループバックを受信するために、このネイバーに対するこのアドレス ファミリのラベル交換を有効にします。
ステップ 10	**network** {*network-number* [**mask***network-mask*] | *nsap-prefix*} [**route-map***map-tag*] 例： `Device(config-router-af)# network 192.168.2.27 mask 255.255.255.255`	ネットワークをこの自律システムにローカルとしてフラグして、ネットワークを BGP テーブルに入力します。この設定は PE VPN ループバック用です。

	コマンドまたはアクション	目的
ステップ 11	**network** {*network-number* [**mask***network-mask*] | *nsap-prefix*} [**route-map***map-tag*] 例： `Device(config-router-af)# network 192.168.2.15 mask 255.255.255.255`	ネットワークをこの自律システムにローカルとしてフラグして、ネットワークを BGP テーブルに入力します。この設定は RR1 ループバック用です。

IPv6 VPN 用の CSC の設定

CsC-PE1 と CsC-CE1 のピアリング設定を行うには、次の作業を実行します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **hostname***name*
4. **routerbgp***autonomous-system-number*
5. **address-familyipv6** [**vrf***vrf-name*] [**unicast** | **multicast**]
6. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number*
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate**
8. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 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	**hostname***name* 例： `Device(config)# hostname CSC-PE1`	ネットワーク サーバのホスト名を指定または修正します。
ステップ 4	**routerbgp***autonomous-system-number* 例： `Device(config)# router bgp 100`	ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロセスを設定します。
ステップ 5	**address-familyipv6** [**vrf***vrf-name*] [**unicast** | **multicast**] 例： `Device(config-router)# address-family ipv6 vrf ISP2`	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	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router-af)# neighbor FE80::866C:99 GigabitEthernet0/0/0 remote-as 200`	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 7	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **activate** 例： `Device(config-router-af)# neighbor FE80::866C:99 GigabitEthernet0/0/0 activate`	このアドレス ファミリの情報を、指定した BGP ネイバーと交換できるようにします。
ステップ 8	**neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **send-label** 例： `Device(config-router-af)# neighbor FE80::866C:99 GigabitEthernet0/0/0 send-label`	このネイバーに対するこのアドレス ファミリのラベル交換をイネーブルにします。

IPv6 VPN over MPLS の設定例

例：IPv6 VPN over MPLS ルーティング

例：BGP IPv6 アクティビティ サマリー

```
Device# show bgp ipv6 summary

For address family: IPv6 Unicast
BGP router identifier 192.168.2.126, local AS number 33751
BGP table version is 15, main routing table version 15
12 network entries using 1692 bytes of memory
22 path entries using 1672 bytes of memory
5/4 BGP path/bestpath attribute entries using 580 bytes of memory
14 BGP rrinfo entries using 336 bytes of memory
2 BGP AS-PATH entries using 48 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 4328 total bytes of memory
Dampening enabled. 0 history paths, 0 dampened paths
BGP activity 13/1 prefixes, 23/1 paths, scan interval 60 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.2.146     4 33751     991     983       15    0    0 16:26:21       10
192.168.2.147     4 33751     991     983       15    0    0 16:26:22       10
FE80::4F6B:44 GigabitEthernet1/0/0
                4 20331     982     987       15    0    0 14:55:52        1
```

例：BGP IPv6 テーブルのダンプ

次の例に示すように、各テーブル（BGP IPv6、BGP IPv6 VPN など）を個別に確認できます。

```
Device# show bgp ipv6 unicast
BGP table version is 15, local router ID is 192.168.2.126
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric    LocPrf Weight Path
* i2001:DB8:100::/48 ::FFFF:192.168.2.101     0    100      0 10000 ?
*>i                 ::FFFF:192.168.2.101     0    100      0 10000 ?
* i2001:DB8::1/128   ::FFFF:192.168.2.101     0    100      0  i
*>i                 ::FFFF:192.168.2.101     0    100      0  i
```

例：IPv6 ルーティング テーブルのダンプ

次の例に示すように、IPv6 ルーティング テーブルは、ルーティング可能なエントリを導出した各ルーティング プロトコルを識別できます。

```
Device# show ipv6 route
IPv6 Routing Table - default - 13 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
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
B   2001:DB8:100::/48 [200/0]
```

```
     via 192.168.2.101 Default-IP-Routing-Table, indirectly connected
B   2001:DB8::1/128 [200/0]
     via 192.168.2.101 Default-IP-Routing-Table, c
LC  2001:DB8::26/128 [0/0]
     via Loopback0, receive
```

IPv6 ルーティングの観点から見ると、MPLS バックボーンを介して到達可能なエントリが、間接的に接続されているものとしてリストされます。これは、MPLS がレイヤ 2 トンネル メカニズムを提供しているためです。

例：IPv6 VPN over MPLS フォワーディング

例：PE-CE 接続

ipv6 ping および **traceroute** コマンドは、ローカルに接続されている場合でも、マルチプロトコル ラベル スイッチング（MPLS）バックボーンを介してリモートで接続されている場合でも、プロバイダー エッジ（PE）からカスタマー エッジ（CE）への接続を確認するのに役立ちます。

デバイスがローカルに接続されている場合は、次の例に示すように、CE のリンクローカル アドレス（外部 BGP ピアリングに使用される）を指定して、**ipv6 ping** コマンドを使用できます。

```
Device# ping FE80::4F6B:44%
Loopback0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::4F6B:44, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/33/48 ms
```

また、**ipv6 ping** コマンドを使用すると、リモート PE または CE の到達可能性もテストできますが、使用できるのは IPv6 グローバル アドレスだけです（リンクローカル アドレスはリンクの向こう側にはアドバタイズされません）。

```
Device# ping 2001:DB8:1120:1::44
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:1120:1:44::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/33/48 ms
```

MPLS を介した **ping ipv6** および **traceroute** コマンド機能は、PE および CE に対して 1 つの IPv6 グローバル プレフィックスをアナウンスするように要求することに注意してください。各 6PE デバイスは、自律システムのエッジでフィルタリングされる 2001:DB8::PE#/128 をアナウンスします。各 IPv6 CE は 2001:DB8:*prefix*:CE#/128 を設定し、これを特定的でないプレフィックスの一部としてアナウンスします（2001:DB8:*prefix*::/n）。

リモート PE および CE の到達可能性は、**traceroute** コマンドを使用してテストできます。すべての PE を **no mpls ip propagate-ttl forwarded** コマンドで設定してある場合、**traceroute** コマンドを CE から実行すると、その出力には IPv6 ノードだけが表示されます。

```
Device# traceroute 2001:DB8::1
Type escape sequence to abort.
Tracing the route to 2001:DB8::1
  1 2001:DB8::26 [AS 33751] 32 msec 32 msec 20 msec
  2 2001:DB8::1 [AS 33751] [MPLS: Label 73 Exp 0] 20 msec 20 msec 20 msec
  3 2001:DB8::1 [AS 33751] 28 msec 20 msec 20 msec
```

P デバイスが ICMPv6 をサポートしているイメージでアップグレードされた後に PE デバイスで **traceroute** コマンドを実行すると（このとき、存続可能時間（TTL）が伝播される）、次の例に示すように、P デバイスの応答も表示されます。

```
Device# traceroute 2001:DB8::1

Type escape sequence to abort.
Tracing the route to 2001:DB8::1
  1 ::FFFF:172.20.25.1 [MPLS: Labels 38/73 Exp 0] 40 msec 32 msec 32 msec
  2 ::FFFF:172.20.10.1 [MPLS: Labels 30/73 Exp 0] 60 msec 32 msec 32 msec
  3 2001:DB8::1 [MPLS: Label 73 Exp 0] 32 msec 32 msec 16 msec
```

ping ipv6 コマンドと **traceroute** コマンドを 6VPE デバイスから実行すると、どちらのコマンドも VPNv4 の場合とまったく同様に *vrf* 引数を受け付けます。

traceroute コマンドは MPLS バックボーン全体のパスの評価には役立ちますが、データプレーン障害のトラブルシューティングには役立たないことに注意してください。P デバイスは IPv6 対応ではないため（VPNv4 対応でもない）、**traceroute** コマンドに応答して生成された ICMPv6 メッセージは、受信されたラベル スタックを使用して出力 PE に転送されます。出力 PE は ICMPv6 メッセージを traceroute の送信元にルーティングできます。MPLS パスが切断されている場合は ICMP メッセージからも切断されるため、ICMP メッセージは出力 PE に到達できません。

例：PE インポジション パス

Cisco デバイスで、IPv6 のインポジション パスのトラブルシューティングに最も役立つツールは、**show ipv6 cef** コマンドです。

次の例に示すように、**show ipv6 cef** コマンドを使用すると、各宛先プレフィックスに使用される IPv6 転送テーブルとラベル スタックが表示されます。

```
Device# show ipv6 cef

2001:DB8:100::/48
  nexthop 172.20.25.1 GigabitEtherent0/0/0 label 38 72
2001:DB8::1/128
  nexthop 172.20.25.1 GigabitEtherent0/0/0 label 38 73
2001:DB8::26/128
  attached to Loopback0, receive
```

次の例に示すように、**show ipv6 cef** コマンドを使用すると、転送テーブル内の特定の IPv6 エントリの詳細を表示したり、宛先の解決方法やラベル スタックの計算方法を分析したりできます。

```
Device# show ipv6 cef 2001:DB8:100::/48 internal

2001:DB8:100::/48, epoch 0, RIB[B], refcount 4
  sources: RIB
..
  recursive via 192.168.2.101[IPv4:Default] label 72, fib 0252B1F8, 1 terminal fib
    path 024F56A8, path list 024F0BA8, share 0/1, type attached nexthop
    ifnums: (none)
     path_list contains at least one resolved destination(s). HW IPv4 notified.
    nexthop 172.20.25.1 GigabitEtherent0/0/0 label 38, adjacency IP adj out of
GigabitEtherent0/0/0 0289BEF0
  output chain: label 72 label 38 TAG adj out of GigabitEtherent0/0/0 0289BD80
```

前述の例の詳細出力には、ラベル スタックを構成している各ラベルに、個別に追跡できる発信元がそれぞれ含まれていることが示されています。次の例に示すように、Border Gateway Protocol（BGP）テーブルには一番下のラベルが格納されています。

```
Device# show bgp ipv6 unicast 2001:DB8:100::/48
```

```
BGP routing table entry for 2001:DB8:100::/48, version 2
Paths: (2 available, best #2, table default)
  Advertised to update-groups:
     1
  10000
    ::FFFF:192.168.2.101 (metric 30) from 192.168.2.147 (192.168.2.147)
      Origin incomplete, metric 0, localpref 100, valid, internal
      Originator: 192.168.2.101, Cluster list: 192.168.2.147,
      mpls labels in/out nolabel/72
  10000
    ::FFFF:192.168.2.101 (metric 30) from 192.168.2.146 (192.168.2.146)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Originator: 192.168.2.101, Cluster list: 192.168.2.146,
      mpls labels in/out nolabel/72
```

次の例に示すように、ラベル配布プロトコル（LDP）ではその他のラベルが表示されます。

```
Device# show mpls ldp bindings 192.168.2.101 32

  lib entry: 192.168.2.101/32, rev 56
        local binding:  label: 40
        remote binding: lsr: 192.168.2.119:0, label: 38
Device# show mpls ldp bindings 172.20.25.0 24
  lib entry: 172.20.25.0/24, rev 2
        local binding: label: imp-null
        remote binding: lsr: 192.168.2.119:0, label: imp-null
```

例：PE ディスポジション パス

次の例を使用して、ディスポジション パスをトラブルシューティングします。

次に、ディスポジション パスをトラブルシューティングするためのマルチプロトコル ラベル スイッチング（MPLS）転送テーブル情報の例を示します。

```
Device# show mpls forwarding-table

Local  Outgoing      Prefix            Bytes Label   Outgoing   Next Hop
Label  Label or VC   or Tunnel Id      Switched      interface
16     Pop Label     192.168.2.114/32    0             GE0/0/0   point2point
17     26            192.168.2.146/32    0             GE0/0/0   point2point
..
72     No Label      2001:DB8:100::/48   63121         GE1/0/0   point2point
73     Aggregate     2001:DB8::1/128   24123
```

次に、スイッチングに使用されるラベルの例を示します。ラベルは iBGP（この例では 6PE）によってアナウンスされており、確認が可能です。

```
Device# show bgp ipv6 2001:DB8:100::/48

BGP routing table entry for 2001:DB8:100::/48, version 2
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
     2
  10000
    FE80::2710:2 (FE80::2710:2) from FE80::2710:2 GigabitEthernet1/0/0 (192.168.2.103)
      Origin incomplete, metric 0, localpref 100, valid, external, best,
```

例：ラベル スイッチ パス

6PE および 6VPE ラベル スイッチ パス（LSP）エンドポイントは IPv4 アドレスであるため、LSP をトラブルシューティングする IPv4 ツールが、IPv6 トラフィックのブラックホール化につながるデータプレーン障害の検出に役立ちます。

次に、LSP を分析するために LSP IPv4 エンドを表示する例を示します。

```
Device# show ipv6 route 2001:DB8::1/128

Routing entry for 2001:DB8::1/128
  Known via "bgp 33751", distance 200, metric 0, type internal
  Route count is 1/1, share count 0
  Routing paths:
    192.168.2.101%Default-IP-Routing-Table indirectly connected
      MPLS Required
      Last updated 02:42:12 ago
```

次に、traceroute LSP の例を示します。

```
Device# traceroute mpls ipv4 192.168.2.101/32 verbose

Tracing MPLS Label Switched Path to 192.168.2.101/32, timeout is 2 seconds
Codes: '!' - success, 'Q' - request not transmitted,
       '.' - timeout, 'U' - unreachable,
       'R' - downstream router but not target,
       'M' - malformed request
Type escape sequence to abort.
  0 172.20.25.2 0.0.0.0 MRU 1500 [Labels: 38 Exp: 0]
R 1 172.20.25.1 0.0.0.0 MRU 1500 [Labels: 30 Exp: 0] 40 ms, ret code 6
R 2 172.20.10.1 0.0.0.0 MRU 1504 [Labels: implicit-null Exp: 0] 60 ms, ret code 6
! 3 172.20.40.1 48 ms
```

例：IPv6 VPN over MPLS VRF

例：VRF 情報

次のコマンド入力では、6VPE の VRF 情報が表示されます。

次に、cisco1 という名前の Virtual Routing and Forwarding（VRF）インスタンスに関連付けられているシスコ エクスプレス フォワーディング FIB からの出力例を示します。

```
Device# show ipv6 cef vrf cisco1

 2001:8::/64
  attached to GigabitEthernet0/0/1
 2001:8::3/128
  receive
 2002:8::/64
  nexthop 10.1.1.2 GigabitEthernet0/1/0 label 22 19
 2010::/64
  nexthop 2001:8::1 GigabitEthernet0/0/1
 2012::/64
  attached to Loopback1
 2012::1/128
  receive
```

次に、cisco1 という名前の VRF に関連付けられている IPv6 ルーティング テーブルに関する出力例を示します。

```
Device# show ipv6 route vrf cisco1

IPv6 Routing Table cisco1 - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
C   2001:8::/64 [0/0]
     via ::, GigabitEthernet0/0/1
```

```
L   2001:8::3/128 [0/0]
     via ::, GigabitEthernet0/0/1
B   2002:8::/64 [200/0]
     via ::FFFF:192.168.1.4,
B   2010::/64 [20/1]
     via 2001:8::1,
C   2012::/64 [0/0]
     via ::, Loopback1
L   2012::1/128 [0/0]
     via ::, Loopback1
```

例：IPv4 ネクスト ホップを使用した IPv6 VPN の設定

次に、6VPE ネクスト ホップの例を示します。

```
interface Loopback0
 ip address 192.168.2.11 255.255.255.255
!
router bgp 100
 neighbor 192.168.2.10 remote-as 100
 neighbor 192.168.2.10 update-source Loopback0
!
 address-family vpnv6
 neighbor 192.168.2.10 activate
 neighbor 192.168.2.10 send-community extended
 exit-address-family
```

デフォルトでは、アドバタイズされるネクスト ホップはIPv6バーチャルプライベート ネットワーク（VPN）アドレスになります。

```
[0:0]::FFFF:192.168.2.10
```

[RD]::FFFF:IPv4-address の形式の 192 ビット アドレスであることに注意してください。

Border Gateway Protocol（BGP）IPv6 VPN ピアが共通サブネットを共有する場合、MP_REACH_NLRI 属性には、グローバル アドレス ネクスト ホップに加えてリンクローカル アドレス ネクスト ホップも含まれます。この状況は、一般的に、自律システム境界ルータ（ASBR）が互いに向き合っている相互自律システム トポロジで発生します。この場合、リンクローカル ネクスト ホップがローカルに使用され、グローバル ネクスト ホップは BGP によって再アドバタイズされます。

BGP ネクスト ホップは、ラベル スタックを構築する場合の中心要素です。内部ラベルはBGP ネットワーク層到達可能性情報（NLRI）から取得され、外部ラベルは BGP ネクスト ホップに埋め込まれた IPv4 アドレスに到達するラベル配布プロトコル（LDP）ラベルになります。

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 Master Command List, All Releases』
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide Library*』

関連項目	マニュアル タイトル
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『IPv6 Feature Mapping』
『Configuring MPLS Layer 3 VPNs』	『*MPLS Layer 3 VPNs Configuration Guide*』の「MPLS Virtual Private Networks」モジュール

標準および RFC

標準/RFC	Title
IPv6 に関する RFC	IPv6 の RFC

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。	http://www.cisco.com/cisco/web/support/index.html

IPv6 VPN over MPLS 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 に移動します。Cisco.com のアカウントは必要ありません。

表 *5*：*IPv6 VPN over MPLS* の機能情報

機能名	リリース	機能情報
IPv6 VPN over MPLS（6VPE）	12.2(28)SB 12.2(33)SRB 12.2(33)SXI 12.4(20)T 15.0(1)S Cisco IOS XE Release 3.1S Cisco IOS XE Release 3.6S	MPLS を介した IPv6 VPN（6VPE）の IPv4 コアインフラストラクチャ機能を使用すると、ISP はカスタマーに IPv6 VPN サービスを提供できます。 この機能は、Cisco IOS Release 12.2(28)SB で導入されました。 この機能は、Cisco IOS Release 12.2(33)SRB、12.2(33)SXI、12.4(20)T、および 15.0(1)S で統合されました。 Cisco IOS XE Release 3.1S では、この機能は Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに実装されました。 Cisco IOS XE リリース 3.6S では、Cisco ASR 903 ルータのサポートが追加されました。 次のコマンドが導入または変更されました： **aggregate-address**、**address-family ipv6**、**address-family vpnv6**、**ipv6 route**、**mls ipv6 vrf**、**neighbor activate**、**neighbor ebgp-multihop**、**neighbor next-hop-unchanged**、**neighbor remote-as**、**neighbor route-reflector-client**、**neighbor send-community**、**neighbor send-label**、**neighbor update-source**、**network**、**rd**、**router bgp**、**route-target**、**vrf definition**、**vrf forwarding**。
IPv6 VPN over MPLS（6VPE）InterAS オプション	12.2(33)SB2 Cisco IOS XE Release 3.1S	IPv6 は、この機能をサポートします。

用語集

- **6VPE デバイス**：IPv4 ベースの MPLS コア上に BGP-MPLS IPv6 VPN サービスを提供するプロバイダー エッジ デバイス。コア方向のインターフェイスで 6PE 概念を実装する IPv6 VPN PE のデュアル スタック デバイスです。
- **カスタマー エッジ（CE）デバイス**：VPN カスタマー サイトに接続するサービス プロバイダー デバイス。
- **転送情報ベース（FIB）**：IP データグラムの転送に必要な情報を含むテーブル。FIB には、少なくとも、到達可能な宛先ネットワーク プレフィックスごとにインターフェイス識別子とネクストホップ情報が格納されます。
- **インバウンド ルート フィルタリング（IRF）**：受信側 PE デバイスによってインポートされない着信 BGP アップデートをフィルタリングするために使用される BGP 機能。
- **IPv6 プロバイダー エッジ（6PE）デバイス**：BGP ベースのメカニズムを実行して、MPLS 対応の IPv4 クラウド上で IPv6 アイランドを相互接続するデバイス。
- **IPv6 VPN アドレス**：IPv6 VPN アドレスは、8 バイトのルート識別子（RD）で始まり、16 バイトの IPv6 アドレスで終わる、24 バイトの識別子です。IPv6 VPN アドレスと呼ばれることもあります。
- **IPv6 VPN アドレス ファミリ**：アドレス ファミリ識別子（AFI）は特定のネットワーク層プロトコルを識別し、後続 AFI（SAFI）は追加情報を提供します。AFI IPv6 SAFI VPN（AFI=2、SAFI=128）は、IPv6 VPN アドレス ファミリと呼ばれます。IPv6 VPN アドレス ファミリと呼ばれることもあります。同様に、AFI IPv4 SAFI VPN は VPNv4 アドレス ファミリと呼ばれます。
- **ネットワーク層到達可能性情報（NLRI）**：BGP では、ルートおよびそのルートへのアクセス方法を記述した NLRI を含むルーティング アップデート メッセージが送信されます。この場合、NLRI がプレフィックスとなります。BGP アップデート メッセージでは、1 つ以上の NLRI プレフィックス、および NLRI プレフィックスのルートの属性が伝送されます。ルート属性には、BGP ネクスト ホップ ゲートウェイ アドレスおよびコミュニティ値が含まれています。
- **アウトバウンド ルート フィルタリング（ORF）**：発信 BGP ルーティング アップデートのフィルタリングに使用される BGP 機能。
- **Point of Presence（POP）**：装置にインストールされている中継キャリアが、地域通信事業者と相互接続する物理的なロケーション。
- **プロバイダー エッジ（PE）デバイス**：VPN カスタマー サイトに接続されるサービス プロバイダー デバイス。
- **ルート識別子（RD）**：グローバルに一意な IPv6 VPN アドレスを形成するために、IPv6 プレフィックスの先頭に付加される 64 ビットの値。
- **ルーティング情報ベース（RIB）**：ルーティング テーブルとも呼ばれます。

- **仮想ルーティングおよび転送（VRF）**：PE内のVPNルーティングおよび転送インスタンス。
- **VRF テーブル**：VRF に関連付けられているルーティングおよび転送テーブル。これは、PE デバイスがカスタマーごとに独立したルーティング状態を維持できるようにするカスタマー固有のテーブルです。

第 7 章

MPLS VPN への ID 番号の割り当て

RFC 2685 に記載のとおり、バーチャル プライベート ネットワーク（VPN）を VPN 識別番号によって識別できます。MPLS VPN ID 機能の実装は、VPN を識別するために使用されます。

- 機能情報の確認，133 ページ
- MPLS VPN ID の制約事項，134 ページ
- MPLS VPN ID に関する情報，134 ページ
- MPLS VPN ID の設定方法，136 ページ
- MPLS VPN への ID 番号の割り当ての設定例，138 ページ
- その他の参考資料，139 ページ
- MPLS VPN ID の機能情報，140 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 に移動します。Cisco.com のアカウントは必要ありません。

MPLS VPN ID の制約事項

MPLS VPN ID 機能を使用して、ルーティング情報の配布を制御したり、IP アドレスを Multiplotocol Border Gateway Protocol（MP-BGP）VPNv4 ルーティング アップデート内の MPLS VPN ID 番号に関連付けたりすることはありません。

MPLS VPN ID に関する情報

MPLS VPN ID の概要

RFC 2685 に記載のとおり、バーチャル プライベート ネットワーク（VPN）を VPN 識別番号によって識別できます。VPN ID 機能の実装は、VPN を識別するために使用されます。VPN ID 機能を使用して、ルーティング情報の配布を制御したり、IP アドレスをマルチプロトコル ボーダー ゲートウェイ プロトコル（MP-BGP）VPNv4 ルーティング アップデート内の VPN ID 番号に関連付けたりすることはありません。

1 つのデバイスに複数の VPN を設定できます。VPN はプライベートであり、別の VPN やインターネットでも使用される可能性があるプライベートアドレス空間を使用します。VPN で使用される IP アドレスは、それが存在する VPN でだけ重要となります。VPN 名（固有の ASCII 文字列）を使用して、デバイスに設定された特定の VPN を参照できます。また、デバイス内で特定の VPN を識別するために VPN ID を使用することもできます。VPN ID は標準仕様（RFC 2685）に準拠しています。VPN の VPN ID を一貫させるには、その VPN にサービスを提供しているサービス プロバイダー ネットワーク内のすべてのデバイスに同じ VPN ID を割り当てます。

（注） VPN の VPN ID の設定はオプションです。デバイス内で設定されている VPN を識別するために、引き続き VPN 名を使用できます。VPN 名は VPN ID の設定の影響を受けません。これらは VPN を識別するための 2 つの独立したメカニズムです。

MPLS VPN ID の構成要素

RFC 2685 で定義されている各 MPLS VPN ID は、次の要素で構成されます。

- 3 オクテットの 16 進数である組織固有識別子（OUI）：IEEE 登録局は、ISO/IEC 8802 規格の下でコンポーネントを製造するあらゆる企業に OUI を割り当てます。OUI は、ローカル エリア ネットワーク アプリケーションとメトロポリタン エリア ネットワーク アプリケーションで使用するための、汎用的な LAN MAC アドレスとプロトコル ID を生成するために使用されます。たとえば、Cisco Systems の OUI は 00-03-6B（16 進数）です。

- バーチャル プライベート ネットワーク（VPN）インデックス：企業内での VPN を示す 4 オクテットの 16 進数。

次の **vpn id** コマンドを使用して、VPN ID を指定します。

vpn id*oui*:*vpn-index*

コロンは OUI と VPN インデックスを区切ります。

MPLS VPN ID を使用する管理アプリケーション

MPLS VPN ID でバーチャル プライベート ネットワーク（VPN）を管理するために複数のアプリケーションを使用できます。Remote Authentication Dial-In User Service（RADIUS）や Dynamic Host Configuration Protocol（DHCP）などのリモート アクセス アプリケーションでは、MPLS VPN ID 機能を使用して VPN を識別できます。RADIUS は、各ユーザの認証情報に基づいて適切な VPN ユーザにダイヤルイン ユーザを割り当てるために、MPLS VPN ID を使用できます。

Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol（DHCP）を使用すると、ネットワーク管理者は組織のネットワークでの IP アドレスの割り当てを集中管理および自動化できます。DHCP アプリケーションは、次のように MPLS VPN ID を使用します。

1. バーチャル プライベート ネットワーク（VPN）DHCP クライアントは、Virtual Routing and Forwarding（VRF）インターフェイスからプロバイダーエッジ（PE）デバイスに接続するように要求します。
2. PE デバイスは、そのインターフェイスに関連付けられている VPN ID を特定します。
3. PE デバイスは、IP アドレスを割り当てるために、VPN ID とその他の情報を含む要求を DHCP サーバに送信します。
4. DHCP サーバは、VPN ID と IP アドレス情報を使用して要求を処理します。
5. DHCP サーバは PE デバイスに応答を返し、VPN DHCP クライアントが VPN にアクセスできるようになります。

リモート認証ダイヤルイン ユーザ サービス

RADIUS サーバ（またはデーモン）は、1 つ以上のクライアント ネットワーク アクセス サーバ（NAS）に認証およびアカウンティング サービスを提供します。RADIUS サーバは、ユーザを認証し、このユーザへのサービス提供にクライアントが必要とするすべての設定情報を返します。

一般に、ユーザ ログインは、NAS から RADIUS サーバへのクエリー（Access-Request）と、それに対応するサーバからの応答（Access-Accept または Access-Reject）からなります。

- Access-Request パケットには、ユーザ名、暗号化されたパスワード、NAD IP アドレス、および MPLS VPN ID とポートが含まれています。要求の形式は、ユーザが開始することを望んでいるセッションの種類についての情報も提供します。
- RADIUS サーバは、ユーザ名を見つけてパスワードを確認した場合、Access-Accept 応答を返します。応答には、このセッションに使用するパラメータを表す属性と値のペアのリストが

含まれています。ユーザが認証されない場合、RADIUS サーバにより Access-Reject が送信され、アクセスが拒否されます。

MPLS VPN ID の設定方法

MPLS VPN ID の指定

はじめる前に

プロバイダー エッジ（PE）デバイスで設定されている各 Virtual Routing and Forwarding（VRF）インスタンスには、MPLS VPN ID を設定できます。同じ VPN ID の同じ Virtual Private Network（VPN）に属するすべての PE デバイスを設定します。サービス プロバイダー ネットワークで VPN ID が一意になるようにします。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **ip vrf***vrf-name*
4. **vpn id***oui*:*vpn-index* :

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**ip vrf***vrf-name* 例： `Device(config)# ip vrf vrf1`	VRF ルーティング テーブルとシスコ エクスプレス フォワーディング テーブルを作成し、VRF コンフィギュレーション モードを開始します。 • *vrf-name*：VRF に割り当てられる名前。

	コマンドまたはアクション	目的
ステップ 4	**vpn id***oui*:*vpn-index* : 例： `Device(config-vrf)# vpn id a1:3f6c`	VPN ID を VRF に割り当てます。 • *oui*：組織固有識別子。IEEE がこの ID を企業に割り当てます。この OUI は 3 オクテットに制限されています。 • *vpn Index*：社内で VPN を識別する値です。この VPN インデックスは 4 オクテットに制限されています。

MPLS VPN ID 設定の確認

手順の概要

1. イネーブル化
2. **show ip vrf**
3. **show ip vrf id**
4. **show ip vrf detail**

手順の詳細

ステップ 1 イネーブル化

特権 EXEC モードをイネーブルにします。

例：

```
Device> enable
Device#
```

ステップ 2 **show ip vrf**

プロバイダー エッジ（PE）デバイスの Virtual Routing and Forwarding（VRF）テーブルに関する情報を表示します。この例は、3 つの VRF テーブル vpn1、vpn2、および vpn5 を示します。

例：

```
Device# show ip vrf

  Name                              Default RD          Interfaces
  vpn1                              100:1               FastEthernet1/1/1
                                                        FastEthernet1/0/0
  vpn2                              <not set>
  vpn5                              500:1               Loopback2
```

ステップ 3 **show ip vrf id**

PEデバイスに、指定したMPLS VPN IDが含まれていることを確認します。次の例は、VRFテーブルvpn1とvpn2だけにVPN IDが割り当てられていることを示しています。VRFテーブルvpn5は、VPN IDがないため表示されません。

例：

```
Device# show ip vrf id

VPN Id          Name                            RD
2:3             vpn2                            <not set>
A1:3F6C         vpn1                            100:1
```

ステップ 4 **show ip vrf detail**

PEデバイスですべてのVRFを表示します。このコマンドでは、デバイスに設定されているすべてのMPLS VPN ID、それに関連付けられているVRF名、およびVRFルート識別子（RD）が表示されます。PEデバイスのVRFテーブルにMPLS VPN IDが割り当てられていない場合、VRFエントリは出力に含まれません。

例：

```
Device# show ip vrf detail

VRF vpn1; default RD 100:1; default VPNID A1:3F6C
  Interfaces:
    FastEthernet1/1/1       FastEthernet1/0/1
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1                 RT:500:1
  No import route-map
  No export route-map
VRF vpn2; default RD <not set>; default VPNID 2:3
  No interfaces
  Connected addresses are not in global routing table
  No Export VPN route-target communities
  No Import VPN route-target communities
  No import route-map
  No export route-map
VRF vpn5; default RD 500:1; default VPNID <not set>
  Interfaces:
```

MPLS VPN への ID 番号の割り当ての設定例

例：MPLS VPN ID の指定

次の例は、vpn1 という Virtual Routing and Forwarding（VRF）テーブルに割り当てられている MPLS VPN ID を示します。

```
Device# configure terminal
```

```
Device(config)# ip vrf vpn1
Device(config-vrf)# vpn id a1:3f6c
```

例：MPLS VPN ID の設定の確認

次に、**show ip vrf detail** コマンド（MPLS VPN ID 設定を変更するために使用できるコマンドの 1 つ）の出力例を示します。プロバイダー エッジ（PE）デバイスのすべての Virtual Routing and Forwarding（VRF）インスタンスを確認するときにこのコマンドを使用します。このコマンドでは、デバイスに設定されているすべての MPLS VPN ID、それに関連付けられている VRF 名、および VRF ルート識別子（RD）が表示されます。PE デバイスの VRF テーブルに VPN ID が割り当てられていない場合、その VRF エントリは出力に含まれません。

```
Device# show ip vrf detail

VRF vpn1; default RD 100:1; default VPNID A1:3F6C
  Interfaces:
    FastEthernet1/1/1       FastEthernet1/0/1
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1                 RT:500:1
  No import route-map
  No export route-map
VRF vpn2; default RD <not set>; default VPNID 2:3
  No interfaces
  Connected addresses are not in global routing table
  No Export VPN route-target communities
  No Import VPN route-target communities
  No import route-map
  No export route-map
VRF vpn5; default RD 500:1; default VPNID <not set>
  Interfaces:
```

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 Master Command List, All Releases』
MPLS と MPLS アプリケーション コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』

標準および RFC

標準/RFC	Title
IEEE 標準 802-1990	『*IEEE Local and Metropolitan Area Networks: Overview and Architecture*』

標準/RFC	Title
RFC 2685	『*Virtual Private Networks Identifier*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。	http://www.cisco.com/cisco/web/support/index.html

MPLS VPN ID 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 に移動します。Cisco.com のアカウントは必要ありません。

表 *6*：***MPLS VPN ID*** の機能情報

機能名	リリース	機能の設定情報
MPLS VPN ID	12.0(17)ST 12.2(8)T 12.2(11)S 12.2(17b)SXA 12.2(27)SBB Cisco IOS XE Release 2.1	RFC 2685 に記載のとおり、VPN を VPN 識別番号によって識別できます。VPN ID 機能の実装は、VPN を識別するために使用されます。 この機能は、Cisco IOS Release 12.0(17)ST で導入されました。 この機能は、Cisco IOS Release 12.2(8)T、12.2(11)S、12.2(17b)SXA、および 12.2(27)SBB で統合されました。 Cisco IOS XE Release 2.1 では、この機能は Cisco ASR 1000 シリーズ アグリゲーション サービスルータに導入されました。 追加または変更されたコマンドはありません。

第 8 章

リモート アクセス MPLS VPN

リモート アクセス MPLS VPN 機能を使用すると、サービス プロバイダーは、リモート ユーザにスケーラブルなエンドツーエンド バーチャル プライベート ネットワーク（VPN）サービスを提供することができます。この機能は、マルチプロトコル ラベル スイッチング（MPLS）対応のバックボーンとブロードバンド アクセス機能を統合します。

- 機能情報の確認，143 ページ
- リモート アクセス MPLS VPN の前提条件，144 ページ
- リモート アクセス MPLS VPN の制約事項，144 ページ
- リモート アクセス MPLS VPN に関する情報，144 ページ
- リモート アクセス MPLS VPN の設定方法，147 ページ
- リモート アクセス MPLS VPN の設定例，151 ページ
- その他の参考資料，153 ページ
- リモート アクセス MPLS VPN の機能情報，154 ページ
- 用語集，155 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 に移動します。Cisco.com のアカウントは必要ありません。

リモート アクセス MPLS VPN の前提条件

- バーチャル プライベート ネットワーク（VPN）の動作を設定する前に、ネットワークで次の Cisco サービスが稼働している必要があります。
  - サービス プロバイダーのバックボーン デバイスにおけるマルチプロトコル ラベル スイッチング（MPLS）
  - Tag Distribution Protocol（TDP）またはラベル配布プロトコル（LDP）
  - VPN サービスを提供するすべてのデバイスにおける Border Gateway Protocol（BGP）
  - それぞれの MPLS 対応デバイスにおける、Cisco Express Forwarding スイッチング
- 同じ VPN に属する複数のプロバイダー エッジ（PE）デバイスは、同じ VPN ID で設定されている必要があります。VPN ID は、サービス プロバイダー ネットワーク上で一意である必要があります。

リモート アクセス MPLS VPN の制約事項

- バーチャル プライベート ネットワーク（VPN）ID を使用して、ルーティング情報の配布を制御したり、IP アドレスを関連付けたりすることはありません。

リモート アクセス MPLS VPN に関する情報

リモート アクセス MPLS VPN の概要

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）を使用することで、サービス プロバイダーは、ネットワークを通じて安定したセキュアなパスを提供する、スケーラブルでコスト効率の高い VPN サービスを展開できます。企業は、MPLS バックボーンの使用を通じて、インターネット サービス プロバイダー（ISP）ネットワーク内で地理的に分散したサイトに接続します。サイトは相互に接続され、MPLS VPN を形成します。

リモート アクセス MPLS VPN 機能を使用すると、サービス プロバイダーは、リモート ユーザにスケーラブルなエンドツーエンド VPN サービスを提供することができます。リモート アクセス MPLS VPN 機能は、MPLS 対応のバックボーンとブロードバンド アクセス機能を統合します。アクセス VPN と MPLS VPN を統合することで、サービス プロバイダーは以下のことが可能です。

- リモート ユーザとリモート オフィスが、企業ネットワークにシームレスにアクセスできるようにする
- さまざまな ISP やリテール サービス プロバイダーに平等なアクセスを提供する

- ブロードバンド アクセス ネットワークを MPLS 対応のバックボーンに統合する
- 企業顧客に、リモートアクセス（RA）ユーザとオフィスを使用したエンドツーエンドの VPN サービスを提供する
- ネットワーク アクセスと接続機能を、ISP の機能から分離する

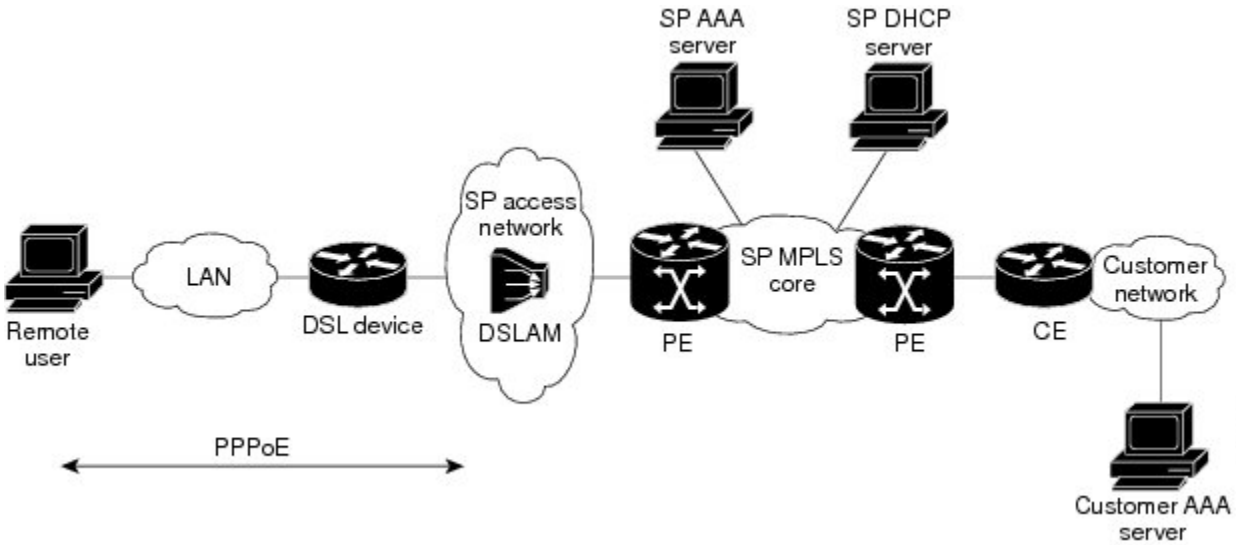
MPLS VPN アーキテクチャ

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）アーキテクチャを使用すると、サービス プロバイダーは、MPLS VPN ネットワークを一度構築し、新しい顧客向けの VPN を必要に応じて追加し、確立済みのネットワークに含めることができます。MPLS VPN を構成する要素は次のとおりです。

- カスタマー エッジ（CE）デバイス：顧客のネットワーク内のサブスクライバが接続するデバイス。CE デバイスは、サービス プロバイダーのエッジデバイス（PE デバイス）に接続します。CE デバイスは、PE デバイスへのリモート アクセス セッションを開始します。
- プロバイダー エッジ（PE）デバイス：サービス プロバイダーの MPLS コア ネットワークのエッジにあるデバイス。PE デバイスは 1 つ以上の CE デバイスに接続し、それらの CE デバイスに関連付けられた VPN へのルートに関する完全な知識を持っています。PE デバイスは、関連付けられた CE デバイスが接続されていない VPN へのルートに関する知識を持っていません。
- プロバイダー（P）デバイス：プロバイダーのコア ネットワークを構成するサービス プロバイダー デバイス。P デバイスは VPN 情報を割り当てず、CE デバイスに関する知識がありません。代わりに、P デバイスの主な焦点は、ラベル スイッチングにあります。

以下の図は、MPLS VPN ネットワーク アーキテクチャの一例を示したものです。

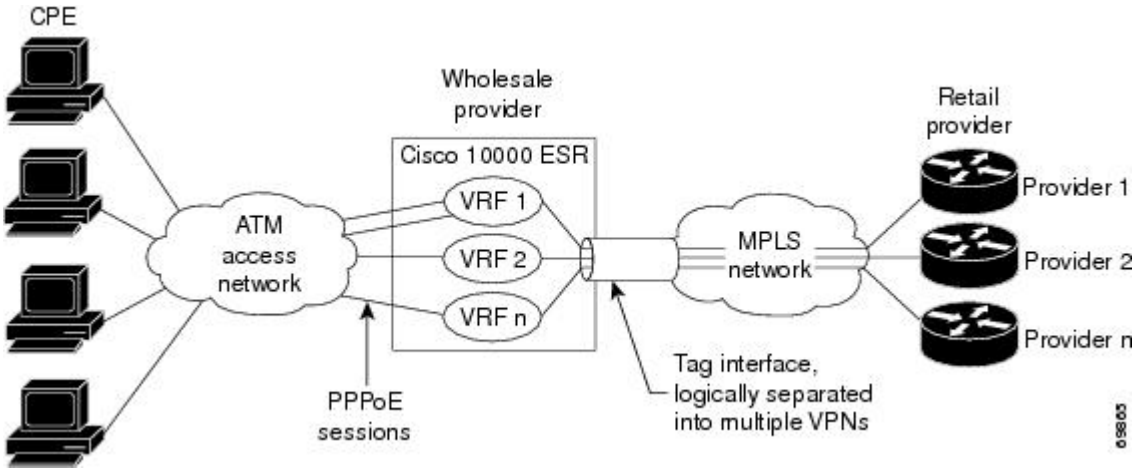
図 *10*：*MPLS VPN* ネットワークの例



MPLS VPN への PPP over Ethernet

次の図は、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）への統合された PPP over Ethernet（PPPoE）アクセスのトポロジを示しています。

図 *11*：*MPLS VPN* への *PPPoE* アクセス トポロジ



上図で、サービス プロバイダーは、すべての顧客サイトを相互接続する MPLS VPN を使用します。サービス プロバイダーのコア ネットワークは、VPN サービスの機能を備えた MPLS バックボーンです。サービス プロバイダーは、すべてのリモート アクセス機能を顧客に提供します。ネットワーク側のインターフェイスはタグ付きインターフェイスであり、複数の VPN に論理的に分けられています。

リモート アクセスは、PPPoE 接続を使用して提供されます。このモデルでは、リモート ユーザが社内ネットワークとの接続を確立しようとすると、PPPoE セッションが開始され、サービス プロバイダーの仮想ホーム ゲートウェイ（VHG）またはプロバイダー エッジ（PE）デバイスで終端されます。特定のカスタマーエッジ（CE）デバイスに接続されているすべてのリモート ホストは、CE デバイスが接続されている VPN に属している必要があります。

MPLS VPN への PPPoE アーキテクチャは、次の特製を備えた柔軟なアーキテクチャです。

- リモート ホストは、複数の同時 PPPoE セッションを、それぞれ異なる VPN に対して作成できます。
- 複数のリモート ホストが同じ CE デバイスの背後にある場合、各リモート ホストは異なる VPN にログインできます。
- 各 VHG または PE デバイスには、可能なすべての VPN の Virtual Routing and Forwarding（VRF）インスタンスがあらかじめインスタンス化されているので、どのリモート ホストも、任意の VPN にいつでもログインできます。この設定では、VRF が RADIUS サーバを通じて適用される必要があるため、スケーラビリティの問題を引き起こす可能性があります。

VHG デバイスまたは PE デバイスが着信 PPPoE セッションを処理するときに、次のイベントが発生します。

1. PPPoE セッションは、ブロードバンド アクセス ネットワーク上で開始されます。
2. VHG/PE デバイスは、PPPoE セッションを受け入れて終端します。
3. VHG/PE デバイスは、次のように、仮想アクセス インターフェイス（VAI）の設定情報を取得します。
   - VHG/PE は、一般にセッションの VRF マッピングを含む、仮想テンプレート インターフェイスの設定情報を取得します。
   - VHG/PE は、VPN がリモート ユーザを認証するために、顧客またはサービス プロバイダーの RADIUS サーバに個別の要求を送信します。
   - VPN の VRF インスタンスは、VHG または PE 上でインスタンス化されます。VPN の VRF には、特定の VPN に関連するルーティング テーブルとその他の情報が含まれています。

通常、顧客の RADIUS サーバは顧客の VPN 内にあります。VHG/PE デバイスと顧客の RADIUS サーバの間のトランザクションが顧客の VPN 内のルート上で実行されるように、VHG/PE デバイスには、VPN 内で有効な少なくとも 1 つの IP アドレスが割り当てられます。

1. VHG/PE デバイスは、アカウンティング レコードをサービス プロバイダーのプロキシ RADIUS サーバに転送し、そこでアカウンティング レコードが記録されて、顧客の適切な RADIUS サーバに転送されます。
2. VHG/PE は CPE の IP アドレスを取得します。アドレスは次のいずれかから割り当てられます。
   - ローカル アドレス プール
   - アドレス プールを指定したり、アドレスを直接提供する、サービス プロバイダーの RADIUS サーバ
   - サービス プロバイダーの DHCP サーバ
3. これで CPE が顧客の VPN に接続されます。パケットがリモート ユーザとの間で流れることができます。

リモート アクセス MPLS VPN の設定方法

MPLS コア ネットワークの設定

マルチプロトコル ラベル スイッチング（MPLS）コア ネットワークを設定するには、インターフェイス上で IP パケットのラベル スイッチングをイネーブルにし、Virtual Routing and Forwarding（VRF）インスタンスを設定し、VRF を関連付け、プロバイダー エッジ（PE）と PE 間のマルチプロトコル Border Gateway Protocol（BGP）ルーティング セッションを設定します。

PPPoE の設定

仮想テンプレート インターフェイスの設定

仮想アクセス インターフェイスの作成時にダイナミックに設定および適用される仮想テンプレート インターフェイスを作成するには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface virtual-template***number*
4. **ip unnumbered ethernet***number*
5. **ppp authentication chap**
6. **ppp ipcp address required**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**interface virtual-template***number* 例： `Device(config)# interface virtual-template 1`	仮想テンプレートインターフェイスを作成し、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	**ip unnumbered ethernet***number* 例： `Device(config-if)# ip unnumbered ethernet 1`	LAN 上の特定の IP アドレスを割り当てずに IP をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 5	**ppp authentication chap** 例： `Device(config-if)# ppp authentication chap`	仮想テンプレート インターフェイスで PPP 認証をイネーブルにします。
ステップ 6	**ppp ipcp address required** 例： `Device(config-if)# ppp ipcp address required`	（レガシー ダイヤルアップおよびDSL ネットワークの場合は必須です。）PPP セッションがリモート IP アドレス 0.0.0.0 で設定されないようにします。

ブロードバンド アグリゲーション グループでの PPPoE の設定

PPP over Ethernet（PPPoE）に対応してブロードバンド アグリゲーション（BBA）グループを設定し、それを適切な仮想テンプレート インターフェイスにリンクするには、次の手順を実行します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **bba-group pppoe** {**name** | **global**}
4. **virtual-template***template-number*
5. **sessions per-mac limit***per-mac-limit*
6. **sessions max limit***global-pppoe-session-limit*
7. **exit**
8. **interface gigabitethernet***slot/subslot/port.*[*subinterface*]
9. **encapsulation dot1q***vlan-id*
10. **pppoe enable** [**group***group-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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	**configure terminal** 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	**bba-group pppoe** {**name** | **global**} 例： `Device(config)# bba-group pppoe bba1`	BBA グループが PPPoE セッションの確立に使用されるように設定し、BBA コンフィギュレーション モードを開始します。 • name 引数は BBA グループを指定します。複数の BBA グループを作成できます。 • global キーワードは、BBBA グループ名が指定されていない場合に使用されるデフォルト BBA グループです。
ステップ 4	**virtual-template***template-number* 例： `Device(config-bba)# virtual-template 20`	仮想アクセスインターフェイス（VAI）のクローンを作成する際に使用される仮想テンプレート インターフェイスを指定します。
ステップ 5	**sessions per-mac limit***per-mac-limit* 例： `Device(config-bba)# sessions per-mac limit 32000`	（任意）PPPoE プロファイルの MAC アドレスあたりの PPPoE セッションの最大数を指定します。
ステップ 6	**sessions max limit***global-pppoe-session-limit* 例： `Device(config-bba)# sessions max limit 32000`	（任意）デバイスで実行可能な PPPoE セッションの最大数を指定し、PPPoE セッション カウントしきい値を設定します。
ステップ 7	**exit** 例： `Device(config-bba)# exit`	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	**interface gigabitethernet***slot/subslot/port.*[*subinterface*] 例： `Device(config)# interface gigabitethernet 2/0/0.2`	BBA グループをアタッチ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
ステップ 9	**encapsulation dot1q***vlan-id* 例： `Device(config-subif)# encapsulation dot1q 2`	802.1q サブインターフェイスを作成し、VLAN ID を指定します。
ステップ 10	**pppoe enable** [**group***group-name*] 例： `Device(config-subif)# pppoe enable group bba1`	VLAN に BBA グループを接続します。

バーチャル プライベート ネットワークの設定と関連付け

バーチャル プライベート ネットワーク（VPN）を設定し仮想テンプレート インターフェイスに関連付けることで、VPN サービスをマルチプロトコル ラベル スイッチング（MPLS）設定に追加できます。

リモート アクセス MPLS VPN の設定例

例：PPPoE セッション用の 1 つの VRF を使用したリモート アクセス MPLS VPN の設定

次に、PPP over Ethernet（PPPoE）セッションに 1 つの Virtual Routing and Forwarding（VRF）インスタンスを使用してリモート アクセス MPLS VPN 機能を設定する例を示します。

```
!
!Enables the AAA access control model.
aaa new-model
!
!Configures AAA accounting.
aaa authentication login default none
aaa authentication enable default none
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization network default local
aaa session-id common
enable password cisco
!
username pppoe password 0 pppoe
username common password 0 common
!
!Creates the common VRF.
ip vrf common
```

```
rd 100:1000
route-target export 100:1000
route-target import 100:1000
!
!Specifies the BBA group to be used to establish PPPoE sessions and specifies the maximum
!number of PPPoE sessions to be established over a vlan.
bba-group pppoe
virtual-template 1
sessions per-mac limit 32000
!
no virtual-template snmp
!
!Configures the small buffer.
buffers small permanent 15000
!
!Defines the general loopback interface used for reachability to the router and as a
!source IP address for sessions (IBGP, TDP, and so on).
interface Loopback0
ip address 10.16.3.1 255.255.255.255
ip ospf network point-to-point
!
!Creates a loopback interface in the vpn1 VRF. You do this for each customer VRF you IP
!unnumber interfaces to.
interface Loopback1
ip vrf forwarding vpn1
ip address 10.24.1.1 255.255.255.255
!
interface Loopback2
ip vrf forwarding vpn2
ip address 10.8.1.2 255.255.255.255
!
interface gigaethernet 0/0/0
load-interval 30
negotiation auto
no cdp enable
interface gigaethernet 0/0/0.9
encapsulation dot1q 9
pppoe enable
no cdp enable
!
!Enables label switching of IP packets on the interface.
interface GigabitEthernet1/0/0
ip address 10.1.10.1 255.255.0.0
no ip redirects
load-interval 30
negotiation auto
tag-switching ip
!
!Defines the virtual template and associates the common VRF with it.
interface Virtual-Template1
ip vrf forwarding common
ip unnumbered Loopback1
peer default ip address pool common
ppp authentication chap
!
!Configures OSPF to advertise the networks.
router ospf 100
log-adjacency-changes
auto-cost reference-bandwidth 1000
network 10.16.3.1 0.0.0.0 area 0
network 10.1.0.0 0.0.255.255 area 0
!
router rip
version 2
!
!Enters address family configuration mode to configure the VRF for PE to CE routing
!sessions.
address-family ipv4 vrf common
version 2
network 10.0.0.0
no auto-summary
exit-address-family
!
```

```
!Configures BGP to advertise the networks for the VPN.
router bgp 100
no synchronization
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor 172.16.1.4 remote-as 100
neighbor 172.16.1.4 activate
!
!Enters address family configuration mode to configure the common VRF for PE to CE routing
!sessions.
address-family ipv4 vrf common
no auto-summary
no synchronization
aggregate-address 10.10.0.0 255.255.0.0 summary-only
exit-address-family
!
address-family vpnv4
neighbor 172.16.1.4 activate
neighbor 172.16.1.4 send-community both
exit-address-family
!
!Specifies the IP local pool to use for the VRF address assignment.
ip local pool common 10.10.1.1 10.10.126.0
ip classless
!Enters routing information in the routing table for the VRF.
ip route 10.0.0.0 255.0.0.0 FastEthernet0/0/0 10.9.0.1
ip route vrf common 10.22.0.0 255.255.0.0 Null0
ip route vrf common 10.30.0.0 255.255.0.0 2.1.1.1 3
ip route vrf common 10.32.0.0 255.255.0.0 2.2.151.1 2
ip route vrf common 10.33.0.0 255.255.0.0 2.3.101.1 2
no ip http server
ip pim bidir-enable
!
no cdp run
!
!Specifies the RADIUS host and configures RADIUS accounting. radius-server retransmit is
!on by default and cannot be removed.
radius-server host 10.19.100.150 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key test
radius-server authorization permit missing Service-Type
radius-server vsa send authentication
call admission limit 90
!
```

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 Master Command List, All Releases』
MPLS と MPLS アプリケーション コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』
基本的な MPLS VPN	「MPLS Virtual Private Networks」モジュール

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。	http://www.cisco.com/cisco/web/support/index.html

リモート アクセス MPLS VPN 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 に移動します。Cisco.com のアカウントは必要ありません。

表 *7*：リモート アクセス *MPLS VPN* の機能情報

機能名	リリース	機能情報
リモート アクセス MPLS VPN	Cisco IOS XE Release 2.1	リモート アクセス MPLS VPN 機能を使用すると、サービス プロバイダーは、リモートユーザにスケーラブルなエンドツーエンド VPN サービスを提供することができます。この機能は MPLS 対応バックボーンとブロードバンド アクセス機能を統合します。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

用語集

CE：Customer Edge（カスタマー エッジ）。

PPPoE：Point-to-Point Protocol over Ethernet。

PE：Provider Edge（プロバイダー エッジ）。

第 9 章

Multi-VRF サポート

Multi-VRF サポート機能を使用すると、同じカスタマー エッジ（CE）デバイス内でルーティングおよび転送テーブルの複数のインスタンスを設定および維持できます。

- 機能情報の確認，157 ページ
- Multi-VRF サポートの前提条件，158 ページ
- Multi-VRF サポートの制約事項，158 ページ
- Multi-VRF サポートに関する情報，158 ページ
- Multi-VRF サポートの設定方法，161 ページ
- Multi-VRF サポートの設定例，170 ページ
- その他の参考資料，173 ページ
- Multi-VRF サポートの機能情報，174 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 に移動します。Cisco.com のアカウントは必要ありません。

Multi-VRF サポートの前提条件

バーチャルプライベートネットワーク（VPN）を使用するには、ネットワークのコアおよびプロバイダー エッジ（PE）デバイスを設定する必要があります。

Multi-VRF サポートの制約事項

- Multi-VRF サポート機能は、レイヤ 3 インターフェイスでのみ設定できます。
- Multi-VRF サポート機能は、Interior Gateway Routing Protocol（IGRP）や Intermediate System to Intermediate System（IS-IS）ではサポートされません。
- 特定のデバイスの特定の VPN ルーティングおよび転送（VRF）インスタンスのラベル配布は、ボーダー ゲートウェイ プロトコル（BGP）またはラベル配布プロトコル（LDP）のいずれかで処理できます。ただし、両方のプロトコルで同時に処理することはできません。
- マルチキャストは、Multi-VRF サポート機能で設定されているレイヤ 3 インターフェイスでは実行できません。

Multi-VRF サポートに関する情報

Multi-VRF サポート機能の動作

Multi-VRF サポート機能を使用すると、サービス プロバイダーは複数のバーチャル プライベートネットワーク（VPN）をサポートすることができ、複数の VPN で IP アドレスが重複することが可能になります。Multi-VRF サポート機能は、入力インターフェイスを使用して複数の異なる VPN のルートを区別し、1 つまたは複数のレイヤ 3 インターフェイスを各仮想ルーティングおよび転送（VRF）インスタンスに関連付けることによって仮想パケット転送テーブルを作成します。VRF のインターフェイスは、FastEthernet ポートなどの物理インターフェイス、または VLAN スイッチ仮想インターフェイス（SVI）などの論理インターフェイスにすることができますが、レイヤ 3 インターフェイスは、一度に複数の VRF に属することはできません。Multi-VRF サポート機能により、オペレータはカスタマー エッジ（CE）デバイス上で複数のルーティング ドメインをサポートできます。各ルーティング ドメインでは、独自のセットのインターフェイスと独自のセットのルーティングおよび転送テーブルが使用されます。Multi-VRF サポート機能は、CE がサポートする各ルーティング ドメインに CE のラベル スイッチド パス（LSP）を拡張することができます。

Multi-VRF サポート機能は次のように動作します。

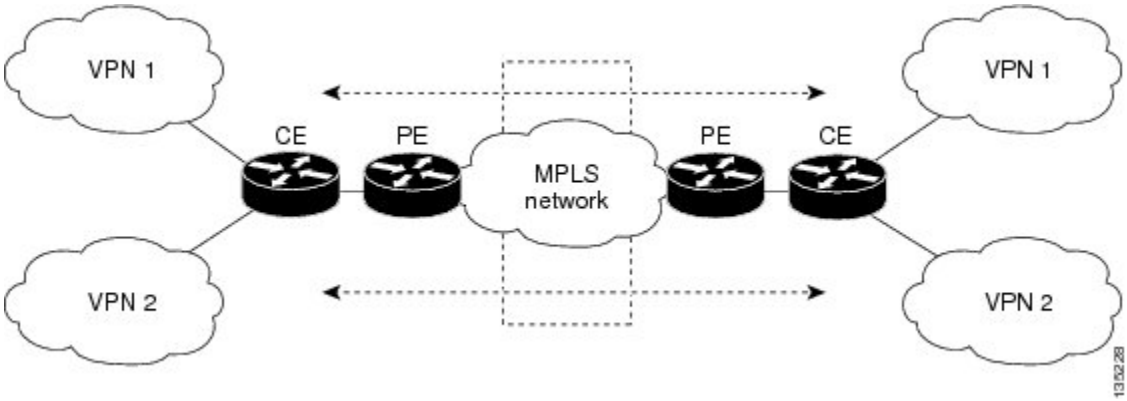
- 各 CE デバイスは、プロバイダー エッジ（PE）デバイスにサイトのローカル ルートをアドバタイズし、プロバイダー エッジ（PE）デバイスからリモート VPN ルートを学習します。

- PE デバイスは、スタティック ルーティング、またはボーダー ゲートウェイ プロトコル（BGP）、ルーティング情報プロトコル バージョン 1（RIPv1）または RIPv2 などのルーティング プロトコルを使用して、CE デバイスとルーティング情報を交換します。
- PE デバイスは、ラベル配布プロトコル（LDP）または BGP を介して CE デバイスと MPLS ラベル情報を交換します。
- PE デバイスは、すべてのサービス プロバイダーの VPN ルートを PE で維持せずに済むようにするため、直接接続された VPN のみの VPN ルートを維持する必要があります。各 PE デバイスは、直接接続しているサイトごとに VRF を維持します。すべてのサイトが同じ VPN に参加している場合、PE デバイス上の複数のインターフェイスを 1 つの VRF に関連付けることができます。各 VPN は、指定された VRF にマッピングされます。CE デバイスからローカル VPN ルートを学習した後、PE デバイスは、内部 BGP（iBGP）を介して他の PE デバイスと VPN ルーティング情報を交換します。

Multi-VRF サポート機能を使用すると、複数のカスタマーが 1 つの CE デバイスを共有でき、1 つの物理リンクのみが CE と PE デバイスの間で使用されます。共有 CE デバイスは、カスタマーごとに別個の VRF テーブルを維持し、カスタマーの独自のルーティング テーブルに基づいて各カスタマーのパケットをルーティングします。Multi-VRF サポート機能により、PE デバイスの限定機能が CE デバイスにまで拡張され、個別の VRF テーブルの維持を通して、VPN のプライバシーとセキュリティをブランチ オフィスにまで拡張できるようになります。

下の図は、各 CE デバイスが 2 つの CE デバイスであるかのように機能する構成を示します。Multi-VRF サポート機能はレイヤ 3 機能なので、VRF に関連付けられている各インターフェイスはレイヤ 3 インターフェイスである必要があります。

図 *12*：複数の仮想 *CE* デバイスとして動作する各 *CE* デバイス



Multi-VRFサポート機能を使用してネットワークでパケットが転送されるしくみ

次に、上の図に示すような、Multi-VRF カスタマー エッジ（CE）対応ネットワークのパケット転送プロセスを示します。

- CE がバーチャル プライベート ネットワーク（VPN）からパケットを受信すると、CE は入力インターフェイスに基づいたルーティングテーブルを検索します。ルートが見つかると、CE はそのルートのプロバイダーエッジ（PE）から受信したマルチプロトコル ラベル スイッチング（MPLS）ラベルを強制し、パケットを PE に転送します。
- 入力PEがCEからパケットを受信すると、対応するラベルスタックで着信ラベルを交換し、MPLS ネットワークにパケットを送信します。
- 出力 PE がネットワークからパケットを受信すると、CE からルートのために以前に受信したラベルで VPN ラベルを交換し、CE にパケットを転送します。
- CE が出力 PE からパケットを受信すると、パケットの着信ラベルを使用して、正しい VPN にパケットを転送します。

マルチ VRF を設定するには、VRF テーブルを作成し、その VRF に関連付けられているレイヤ 3 インターフェイスを指定します。次に、VPN 内、および CE と PE 間にルーティング プロトコルを設定します。ボーダー ゲートウェイ プロトコル（BGP）は、プロバイダーのバックボーンでの VPN ルーティング情報の配布で優先されるルーティング プロトコルです。

マルチ VRF ネットワークには、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：これは、VPN コミュニティの他のすべてのメンバのリストです。各 VPN コミュニティ メンバの VPN ルート ターゲットを設定する必要があります。
- VPN コミュニティ PE デバイスのマルチプロトコル BGP ピアリング：VPN コミュニティのすべてのメンバに VRF の到達可能情報を伝播します。VPN コミュニティのすべての PE デバイスで BGP ピアリングを設定する必要があります。
- VPN 転送：VPN サービス プロバイダー ネットワーク上の VPN コミュニティ メンバ間ですべてのトラフィックを転送します。

Multi-VRF サポート機能を設定する場合の考慮事項

- Multi-VRF サポート機能を持つデバイスは、複数のカスタマーによって共有され、各カスタマーが独自のルーティング テーブルを持ちます。
- 各カスタマーはそれぞれ異なる仮想ルーティングおよび転送（VRF）テーブルを使用するため、同じ IP アドレスを再利用できます。重複する IP アドレスは、異なるバーチャル プライベート ネットワーク（VPN）で許可されます。
- Multi-VRF サポート機能を使用すると、複数のカスタマーがプロバイダーエッジ（PE）デバイスとカスタマー エッジ（CE）デバイスの間で同じ物理リンクを共有できます。複数の VLAN を持つトランク ポートでは、カスタマー間のパケットが分割されます。それぞれのお客様には独自の VLAN があります。
- PE デバイスでは、Multi-VRF サポート機能の使用と、複数の CE デバイスの使用に違いはありません。
- Multi-VRF サポート機能は、パケットスイッチング レートには影響しません。

Multi-VRF サポートの設定方法

VRF の設定

仮想ルーティングおよび転送（VRF）インスタンスを設定するには、次の手順を実行します。プロバイダー エッジ（PE）デバイスおよびカスタマー エッジ（CE）デバイスの両方で VRF を設定するようにします。

VRF が設定されていない場合、デバイスには、次のデフォルト設定が適用されます。

- VRF は定義されていません。
- インポート マップ、エクスポート マップ、ルート マップは定義されていません。
- VRF の最大ルートはありません。
- グローバル ルーティング テーブルはインターフェイスにあります。

（注） マルチキャストは、Multi-VRF サポート機能と同じレイヤ 3 インターフェイス上に同時に設定することはできません。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **ip routing**
4. **ip vrf***vrf-name*
5. **rd***route-distinguisher*
6. **route-target** {**export** | **import** | **both**} *route-target-ext-community*
7. **import map***route-map*
8. **exit**
9. **interface***typeslot*/*subslot*/*port*[**.***subinterface*]
10. **ip vrf forwarding***vrf-name*
11. **end**
12. **show ip vrf**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**ip routing** 例： `Device(config)# ip routing`	IP ルーティングをイネーブルにします。
ステップ 4	**ip vrf***vrf-name* 例： `Device(config)# ip vrf v1`	VRF 名を指定し、VRF 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	**rd***route-distinguisher* 例： `Device(config-vrf)# rd 100:1`	ルート識別子を指定して VRF テーブルを作成します。 自律システム番号および任意の数（xxx:y）、または IP アドレスおよび任意の数（A.B.C.D:y）のいずれかを入力します。
ステップ 6	**route-target** {**export** | **import** | **both**} *route-target-ext-community* 例： `Device(config-vrf)# route-target export 100:1`	指定された VRF のインポート、エクスポート、またはインポートおよびエクスポート ルート ターゲット コミュニティのリストを作成します。 自律システム番号および任意の数（xxx:y）、または IP アドレスおよび任意の数（A.B.C.D:y）のいずれかを入力します。 （注） このコマンドは、BGP が稼働している場合にだけ有効です。
ステップ 7	**import map***route-map* 例： `Device(config-vrf)# import map importmap1`	（任意）VRF にルート マップを対応付けます。

	コマンドまたはアクション	目的
ステップ 8	**exit** 例： `Device(config-vrf)# exit`	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	**interface***typeslot/subslot/port*[*.subinterface*] 例： `Device(config)# interface fastethernet3/0/0.10`	VRF に関連付けるレイヤ 3 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。 インターフェイスはルーテッド ポートまたは SVI に設定できます。
ステップ 10	**ip vrf forwarding***vrf-name* 例： `Device(config-if)# ip vrf forwarding v1`	VRF をレイヤ 3 インターフェイスに対応付けます。
ステップ 11	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 12	**show ip vrf** 例： `Device# show ip vrf`	VRF 設定を表示します。

ルーティング プロトコルとしての BGP の設定

ほとんどのルーティング プロトコルは、カスタマー エッジ（CE）デバイスとプロバイダー エッジ（PE）デバイス間で使用できます。ただし、次の理由で、外部BGP（eBGP）が推奨されます。

- BGP は、多数の CE デバイスと通信するのに複数のアルゴリズムを必要としません。
- BGPは、さまざまな管理によって稼働するシステム間でルーティング情報を渡すように設計されています。
- BGP によって、CE デバイスにルート属性を簡単に渡すことができます。

BGP がルーティング プロトコルとして使用されている場合、PE デバイスと CE デバイス間のマルチプロトコル ラベル スイッチング（MPLS）ラベル交換の処理にもその BGP を使用できます。対照的に、Open Shortest Path First（OSPF）、Enhanced Interior Gateway Routing Protocol（EIGRP）、

ルーティング情報プロトコル（RIP）、またはスタティック ルーティングが使用されている場合は、ラベル配布プロトコル（LDP）をラベルのシグナリングに使用する必要があります。

BGP を PE から CE へのルーティング セッションのために設定するには、CE デバイスと PE デバイスで次の手順を実行します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router bgp***autonomous-system-number*
4. **network***ip-address***mask***network-mask*
5. **redistribute ospf***process-id***match internal**
6. **network***ip-address wildcard-mask***area***area-id*
7. **address-family ipv4 vrf***vrf-name*
8. **neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number*
9. **neighbor***address***activate**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp***autonomous-system-number* 例： `Device(config)# router bgp 100`	BGP ルーティング プロセスを他の BGP デバイスに渡す自律システム番号で設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**network***ip-address***mask***network-mask* 例： `Device(config-router)# network 10.0.0.0 mask 255.255.255.0`	BGP を使用してアナウンスするネットワークおよびマスクを指定します。

	コマンドまたはアクション	目的
ステップ 5	**redistribute ospf***process-id***match internal** 例： `Device(config-router)# redistribute ospf 2 match internal`	OSPF 内部ルートを再配布するようにデバイスを設定します。
ステップ 6	**network***ip-address wildcard-mask***area***area-id* 例： `Device(config-router)# network 10.0.0.0 255.255.255.0 area 0`	OSPF を実行しているネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を識別します。
ステップ 7	**address-family ipv4 vrf***vrf-name* 例： `Device(config-router)# address-family ipv4 vrf v12`	次の 2 つのコマンドに関連付ける仮想ルーティングおよび転送（VRF）インスタンスの名前を識別し、VRF アドレスファミリ モードを開始します。
ステップ 8	**neighbor** {*ip-address* | *peer-group-name*} **remote-as***as-number* 例： `Device(config-router-af)# neighbor 10.0.0.3 remote-as 100`	ネイバー アドレス（またはピア グループ名）のこのデバイスの BGP ネイバー テーブルおよびネイバーの自律システム番号を通知します。
ステップ 9	**neighbor***address***activate** 例： `Device(config-router-af)# neighbor 10.0.0.3 activate`	IPv4 アドレスファミリ ネイバーのアドバタイズメントをアクティブ化します。

PE から CE への MPLS 転送およびシグナリングで BGP を使用する場合の設定

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にボーダー ゲートウェイ プロトコル（BGP）を使用する場合は、CE デバイスと PE デバイスの両方の仮想ルーティングおよび転送（VRF）インターフェイスのラベルをシグナリングするように BGP を設定します。ルータ コンフィギュレーション レベルと、各インターフェイスごとに、シグナリングをグローバルに有効にする必要があります。

- ルータ コンフィギュレーション レベルでは、**neighbor send-label** コマンドを使用して、BGP を介したマルチプロトコル ラベル スイッチング（MPLS）ラベルのシグナリングをイネーブルにします。
- インターフェイス レベルでは、**mpls bgp forwarding** コマンドを使用して、PE から CE への外部 BGP（eBGP）セッションに使用されるインターフェイスで MPLS 転送をイネーブルにします。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router bgp***autonomous-system-number*
4. **address-family ipv4 vrf***vrf-name*
5. **neighbor***address***send-label**
6. **neighbor***address***activate**
7. **end**
8. **configure terminal**
9. **interface***typeslot*/*subslot*/*port*[**.***subinterface*]
10. **mpls bgp forwarding**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router bgp***autonomous-system-number* 例： `Device(config)# router bgp 100`	BGP ルーティング プロセスを他のデバイスに渡す BGP 自律システム番号で設定し、ルータ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**address-family ipv4 vrf***vrf-name* 例： `Device(config-router)# address-family ipv4 vrf v12`	次の 2 つのコマンドに関連付ける VRF インスタンスの名前を識別し、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。
ステップ 5	**neighbor***address***send-label** 例： `Device(config-router-af)# neighbor 10.0.0.3 send-label`	BGP を使用して IPv4 ルートとともに MPLS ラベルをピアデバイスに配布できるようにデバイスを設定します。 このコマンドを発行するときに BGP セッションが実行中の場合、BGP セッションが再開されるまでコマンドは有効になりません。
ステップ 6	**neighbor***address***activate** 例： `Device(config-router-af)# neighbor 10.0.0.3 activate`	IPv4 アドレスファミリ ネイバーのアドバタイズメントをアクティブ化します。
ステップ 7	**end** 例： `Device(config-router-af)# end`	特権 EXEC モードに戻ります。
ステップ 8	**configure terminal** 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 9	**interface***typeslot*/*subslot*/*port*[**.***subinterface*]	BGPセッションで使用されるインターフェイスのインターフェイス コンフィギュレーション モードを開始します。 インターフェイスはルーテッド ポートまたは SVI に設定できます。 例： `Device(config)# interface fastethernet3/0/0.10`
ステップ 10	**mpls bgp forwarding** 例： `Device(config-if)# mpls bgp forwarding`	インターフェイスで MPLS 転送をイネーブルにします。

BGP 以外のルーティング プロトコルの設定

ルーティング情報プロトコル（RIP）、Enhanced Interior Gateway Routing Protocol（EIGRP）、Open Shortest Path First（OSPF）、またはスタティック ルーティングを使用できます。この設定はOSPFを使用しますが、その他のプロトコルでもプロセスは同じです。

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OSPFを使用する場合は、ルータ コンフィギュレーション モードで **capability vrf-lite** コマンドを発行します。

（注） RIP、EIGRP、OSPF、またはスタティック ルーティングが使用されている場合、ラベルのシグナリングにラベル配布プロトコル（LDP）を使用する必要があります。

Multi-VRF サポート機能は、Interior Gateway Routing Protocol（IGRP）や Intermediate System to Intermediate System（IS-IS）ではサポートされません。

Multi-VRF サポート機能が設定されているレイヤ 3 インターフェイスにマルチキャストを同時に設定することはできません。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router ospf***process-id* [**vrf***vpn-name*]
4. **log-adjacency-changes**
5. **redistribute bgp***autonomous-system-number***subnets**
6. **network***ip-addresssubnet-mask***area***area-id*
7. **end**
8. **show ip ospf**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**router ospf***process-id* [**vrf***vpn-name*] 例： `Device(config)# router ospf 100 vrf v1`	OSPF ルーティングをイネーブルにし、仮想ルーティングおよび転送（VRF）テーブルを指定して、ルータ 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	**log-adjacency-changes** 例： `Device(config-router)# log-adjacency-changes`	（任意）隣接ステートの変更を記録します。 これは、デフォルトの状態です。
ステップ 5	**redistribute bgp***autonomous-system-number***subnets** 例： `Device(config-router)# redistribute bgp 800 subnets`	デバイスをボーダー ゲートウェイ プロトコル（BGP）ネットワークから OSPF ネットワークに情報を再配布するように設定します。
ステップ 6	**network***ip-addresssubnet-mask***area***area-id* 例： `Device(config-router)# network 10.0.0.0 255.255.255.0 area 0`	OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を示します。
ステップ 7	**end** 例： `Device(config-router)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show ip ospf** 例： `Device# show ip ospf`	OSPF ルーティング プロセスに関する情報を表示します。

PE から CE への MPLS 転送およびシグナリングで LDP を使用する場合の設定

手順の概要

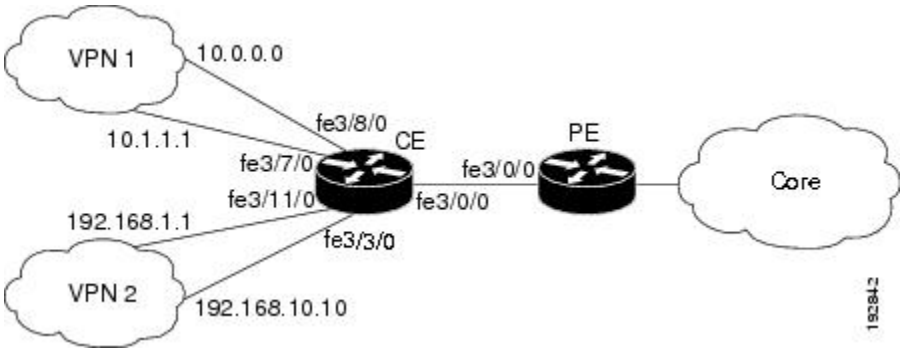
1. イネーブル化
2. **configure terminal**
3. **interface***typeslot*/*subslot*/*port*[**.***subinterface*]
4. **mpls ip**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**interface***typeslot*/*subslot*/*port*[**.***subinterface*] 例： `Device(config)# interface fastethernet3/0/0.10`	VRF に関連付けられたインターフェイスのインターフェイス コンフィギュレーション モードを開始します。インターフェイスはルーテッド ポートまたは SVI に設定できます。
ステップ 4	**mpls ip** 例： `Device(config-if)# mpls ip`	このインターフェイスの通常のルーテッド パスで IPv4 パケットの MPLS 転送をイネーブルにします。

Multi-VRF サポートの設定例

次の図は、Multi-VRF トポロジの例です。



例：PE デバイスでの Multi-VRF サポートの設定

次に、VRF を設定する例を示します。

```
configure terminal
ip vrf v1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 exit
ip vrf v2
 rd 100:2
 route-target export 100:2
 route-target import 100:2
 exit
```

次に、ルーティングおよびラベルの交換の両方に BGP を使用して、PE から CE への接続を設定する例を示します。

```
router bgp 100
 address-family ipv4 vrf v2
  neighbor 10.0.0.8 remote-as 800
  neighbor 10.0.0.8 activate
  neighbor 10.0.0.8 send-label
  exit
 address-family ipv4 vrf vl
  neighbor 10.0.0.8 remote-as 800
  neighbor 10.0.0.8 activate
  neighbor 10.0.0.8 send-label
  end
configure terminal
 interface fastethernet3/0/0.10
  ip vrf forwarding v1
  ip address 10.0.0.3 255.255.255.0
  mpls bgp forwarding
  exit
 interface fastethernet3/0/0.20
  ip vrf forwarding v2
  ip address 10.0.0.3 255.255.255.0
  mpls bgp forwarding
  exit
```

次に、ルーティングおよび LDP ラベルの交換に OSPF を使用して、PE から CE への接続を設定する例を示します。

```
router ospf 100 vrf v1
 network 10.0.0.0 255.255.255.0 area 0
 exit
router ospf 101 vrf v2
 network 10.0.0.0 255.255.255.0 area 0
```

```
 exit
interface fastethernet3/0/0.10
 ip vrf forwarding v1
 ip address 10.0.0.3 255.255.255.0
 mpls ip
 exit
interface fastethernet3/0/0.20
 ip vrf forwarding v2
 ip address 10.0.0.3 255.255.255.0
 mpls ip
 exit
```

例：CE デバイスでの Multi-VRF サポートの設定

次に、VRF の設定例を示します。

```
configure terminal
 ip routing
 ip vrf v11
  rd 800:1
  route-target export 800:1
  route-target import 800:1
  exit
 ip vrf v12
  rd 800:2
  route-target export 800:2
  route-target import 800:2
  exit
```

次に、CE デバイスの VPN 接続を設定する例を示します。

```
interface fastethernet3/8/0
 ip vrf forwarding v11
 ip address 10.0.0.8 255.255.255.0
 exit
interface fastethernet3/11/0
 ip vrf forwarding v12
 ip address 10.0.0.8 255.255.255.0
 exit
router ospf 1 vrf v11
 network 10.0.0.0 255.255.255.0 area 0
 network 10.0.0.0 255.255.255.0 area 0
 exit
router ospf 2 vrf v12
 network 10.0.0.0 255.255.255.0 area 0
 network 10.0.0.0 255.255.255.0 area 0
 exit
```

（注） BGP が PE デバイスと CE デバイス間のルーティングに使用されている場合、次の例に示すコマンドを使用して、PE デバイスからの BGP 学習ルートを OSPF に再配布できます。

```
router ospf 1 vrf v11
 redistribute bgp 800 subnets
 exit
router ospf 2 vrf v12
 redistribute bgp 800 subnets
 exit
```

次に、ルーティングおよびラベルの交換の両方に BGP を使用して、PE から CE への接続を設定する例を示します。

```
router bgp 800
 address-family ipv4 vrf v12
```

```
 neighbor 10.0.0.3 remote-as 100
 neighbor 10.0.0.3 activate
 neighbor 10.0.0.3 send-label
 redistribute ospf 2 match internal
 exit
 address-family ipv4 vrf vl1
 neighbor 10.0.0.3 remote-as 100
 neighbor 10.0.0.3 activate
 neighbor 10.0.0.3 send-label
 redistribute ospf 1 match internal
 end
interface fastethernet3/0/0.10
  ip vrf forwarding vl1
  ip address 10.0.0.8 255.255.255.0
  mpls bgp forwarding
  exit
interface fastethernet3/0/0.20
  ip vrf forwarding vl2
  ip address 10.0.0.8 255.255.255.0
  mpls bgp forwarding
  exit
```

次に、ルーティングおよびラベル交換用 LDP の両方に OSPF を使用して、PE から CE への接続を設定する例を示します。

```
router ospf 1 vrf vl1
 network 10.0.0.0 255.255.255.0 area 0
 exit
router ospf 2 vrf vl2
 network 10.0.0.0 255.255.255.0 area 0
 exit
interface fastethernet3/0/0.10
  ip vrf forwarding vl1
  ip address 10.0.0.3 255.255.255.0
  mpls ip
  exit
interface fastethernet3/0/0.20
  ip vrf forwarding vl2
  ip address 10.0.0.3 255.255.255.0
  mpls ip
  exit
```

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 Master Command List, All Releases』
MPLS と MPLS アプリケーション コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』
マルチ VRF を使用する OSPF	『*OSPF Configuration Guide*』の「OSPF Support for Multi-VRF in CE Routers」モジュール

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。	http://www.cisco.com/cisco/web/support/index.html

Multi-VRF サポートの機能情報

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 に移動します。Cisco.com のアカウントは必要ありません。

表 *8* : ***Multi-VRF*** サポートの機能情報

機能名	リリース	機能情報
Multi-VRF サポート		Multi-VRF サポート機能を使用すると、同じ CE デバイス内でルーティングおよび転送テーブルの複数のインスタンスを設定および維持できます。

第 10 章

ポリシーベース ルーティングを使用した Multi-VRF 選択

ポリシーベース ルーティング（PBR）を使用した Multi-VRF 選択機能を使用すると、プロバイダー エッジ（PE）のデバイス上の指定されたインターフェイスが、IP アクセス リストで定義されているパケット長や一致基準に基づいて、バーチャル プライベート ネットワーク（VPN）にパケットをルーティングできます。

VPN ルーティングおよび転送（VRF）の選択は、ルート マップ、グローバル ルーティング テーブルまたは指定した VRF を経由するポリシー ルーティング パケットにより有効にすることができます。

VRF インスタンスのポリシー ルーティング パケットは、ルートマップ コマンドと **set** コマンドを使用して有効にすることができます。

サポートされるハードウェアでの同じインターフェイス上で、ポリシーベース ルーティングを使用した Multi-VRF 選択機能と送信元 IP アドレス機能に基づいた MPLS VPN VRF 選択機能の両方を設定できます。

- 機能情報の確認，176 ページ
- ポリシーベース ルーティングを使用した Multi-VRF 選択の前提条件，176 ページ
- ポリシーベース ルーティングを使用した Multi-VRF 選択の制限事項，176 ページ
- ポリシーベース ルーティングを使用した Multi-VRF 選択に関する情報，177 ページ
- ポリシーベース ルーティングを使用した Multi-VRF 選択の設定方法，181 ページ
- ポリシーベース ルーティングを使用した Multi-VRF 選択の設定例，191 ページ
- その他の参考資料，192 ページ
- ポリシーベース ルーティングを使用した Multi-VRF 選択の機能情報，192 ページ
- 用語集，194 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 に移動します。Cisco.com のアカウントは必要ありません。

ポリシーベース ルーティングを使用した Multi-VRF 選択の前提条件

- デバイスは、この機能を設定できるようにするために、ポリシーベースルーティング（PBR）をサポートする必要があります。PBR をサポートしないプラットフォームでは、送信元 IP アドレス機能に基づいて MPLS VPN VRF 選択機能を使用します。
- この機能を設定する前に、バーチャル プライベート ネットワーク（VPN）の Virtual Routing and Forwarding（VRF）インスタンスを定義する必要があります。VRF が存在しない場合は、コンソールにエラー メッセージが表示されます。

ポリシーベース ルーティングを使用した Multi-VRF 選択の制限事項

- ルーティングを支援するすべてのコマンドは、ハードウェア スイッチングもサポートします。ただし、Cisco Discovery Protocol 情報はラインカード上で使用できないため、**set ip next-hop verify availability** コマンドは除きます。
- プロトコル独立マルチキャスト（PIM）およびマルチキャスト パケットはポリシーベース ルーティング（PBR）をサポートしていません。また、この機能の一致基準になっている送信元 IP アドレスには、PIM とマルチキャスト パケットを設定できません。
- **set vrf** および **set ip global next-hop** コマンドは、**set default interface**、**set interface**、**set ip default next-hop**、および **set ip next-hop** コマンドとともに設定できます。ただし、**set vrf** および **set ip global next-hop** コマンドは、**set default interface**、**set interface**、**set ip default next-hop**、および **set ip next-hop** コマンドより優先されます。これら 3 つの **set** コマンドのいずれかとともに **set vrf** コマンドを設定しようとした場合、エラー メッセージは表示されません。

- ポリシーベース ルーティングを使用した Multi-VRF 選択機能は IP プレフィックス リストでは設定できません。
- **set global** および **set vrf** コマンドは、ルート マップに同時に適用することはできません。
- ポリシーベース ルーティングを使用した Multi-VRF 選択機能は、VRF-lite、つまり、デバイスで実行される IP ルーティング プロトコルだけをサポートします。マルチプロトコル ラベル スイッチング（MPLS）およびバーチャルプライベート ネットワーク（VPN）は設定できません。ただし、**set vrf** コマンドは、MPLS VPN シナリオで機能します。

ポリシーベース ルーティングを使用した Multi-VRF 選択に関する情報

一致基準に基づいた VPN トラフィックのポリシー ルーティング

ポリシーベースルーティングを使用したMulti-VRF選択機能は、送信元IPアドレスに基づくMPLS VPN VRF選択機能を拡張したものです。ポリシーベース ルーティングを使用したMulti-VRF選択機能では、一致基準に基づいてバーチャルプライベートネットワーク（VPN）トラフィックをポリシールーティングできます。一致基準は、IPアクセスリストに定義されるか、またはパケット長に基づいて定義されます。シスコ ソフトウェアがサポートする一致基準は、次のとおりです。

- IP アクセス リスト：IP アドレス、IP アドレスの範囲、および他の IP パケット アクセス リストのフィルタリング オプションに基づいて、一致基準を定義します。サポートされるアクセス リストは、名前付きアクセス リスト、番号付きアクセス リスト、標準アクセス リスト、および拡張アクセス リストです。一致基準の定義にはシスコ ソフトウェアのすべての IP アクセス リスト設定オプションを使用できます。
- パケット長：パケットの長さ（バイト単位）に基づいて、一致基準を定義します。パケット長フィルタは、**match length** ルート マップ コンフィギュレーション コマンドを使用してルート マップに定義します。

ポリシー ルーティングはルート マップで定義します。ルート マップは、**ip policy route-map** インターフェイス コンフィギュレーション コマンドを使用して着信インターフェイスに適用します。IP アクセス リストは、**match ip address** ルートマップ コンフィギュレーション コマンドを使用して、ルート マップに適用されます。パケット長の一致基準は、**match length** ルートマップ コンフィギュレーション コマンドを使用してルート マップに適用されます。**設定**アクションは、**set vrf** ルート マップ コンフィギュレーション コマンドを使用して定義します。一致基準が評価され、適切な VRF が **set** コマンドによって選択されます。この組み合わせを使用すると、着信 VPN トラフィックの一致基準を定義し、VPN パケットをポリシーに従って適切な Virtual Routing and Forwarding（VRF）にルーティングできます。

ポリシーベース ルーティングの set コマンド

VRF インスタンスのポリシールーティング パケット

仮想ルーティングおよび転送（VRF）インスタンスのポリシールーティング パケットを有効にするには、次の **set** コマンドとともにルート マップ コマンドを使用できます。これらは、デバイスがパケットのルーティング中に使用する順で一覧されています。

- **set tos**：IP パケットのヘッダーのタイプ オブ サービス（TOS）ビットを設定します。
- **set df**：IP パケットのヘッダーの Don't Fragment（DF）ビットを設定します。
- **set vrf**：指定されたインターフェイスを介してパケットをルーティングします。宛先インターフェイスは VRF インスタンスにだけ属することができます。
- **set global**：グローバル ルーティング テーブルを使用してパケットをルーティングします。このコマンドは、特定の VRF に属する入力パケットをグローバル ルーティング テーブルを介してルーティングする場合に有効です。
- **set ip vrf next-hop**：指定された VRF の下に IPv4 ネクスト ホップがある必要がある場合の、ポリシー ルーティングのルート マップの一致基準を満たす IPv4 パケットの出力先を示しています。
- **set ipv6 vrf next-hop**：指定された VRF の下に IPv6 ネクスト ホップがある必要がある場合の、ポリシー ルーティングのルート マップの一致基準を満たす IPv6 パケットの出力先を示しています。
- **set ip global next-hop**：ポリシー ルーティングのルート マップの一致基準を満たしたパケットのうち、シスコ ソフトウェアでグローバル ルーティング テーブルが使用されている IPv4 パケットの転送先を示しています。global キーワードは、IPv4 ネクストホップがグローバル ルーティング テーブル下にあることを明示的に定義します。
- **set ipv6 global next-hop**：ポリシー ルーティングのルート マップの一致基準を満たしたパケットのうち、シスコ ソフトウェアでグローバル ルーティング テーブルが使用されている IPv6 パケットの転送先を示しています。global キーワードは、IPv6 ネクストホップがグローバル ルーティング テーブル下にあることを明示的に定義します。
- **set interface**：パケットが VRF に入るときに、レイヤ 2 書き換え情報を使用できる場合は、set interface ポリシーに従って同じ VRF 下の出力インターフェイスからパケットをルーティングします。
- **set ip default vrf**：IPv4 継承 VRF ルーティングと、VRF 間ルーティングを提供します。継承 VRF ルーティングでは、VRF インターフェイスに到着する IPv4 パケットは、同じ出力 VRF インターフェイスでルーティングされます。VRF 間ルーティングでは、VRF インターフェイスに到着する IPv4 パケットは、他の出力 VRF インターフェイスのいずれかを介してルーティングされます。
- **set ipv6 default vrf**：IPv6 の継承 VRF ルーティングと、VRF 間ルーティングを提供します。継承 VRF ルーティングでは、VRF インターフェイスに到着する IPv6 パケットは、同じ出力

VRF インターフェイスでルーティングされます。VRF 間ルーティングでは、VRF インターフェイスに到着する IPv6 パケットは、他の出力 VRF インターフェイスのいずれかを介してルーティングされます。

- **set ip default global**：グローバル ルーティングに IPv4 VRF を提供します。
- **set ipv6 default global**：グローバル ルーティングに IPv6 VRF を提供します。
- **set default interface**：ポリシー ルーティングのルート マップの一致条件を満たしたパケットのうち、宛先に対する明示ルートを持っていないパケットの出力先を示します。インターフェイスは任意の VRF に属することができます。
- **set ip default next-hop**：ポリシー ルーティングのルート マップの一致条件を満たしたパケットのうち、シスコ ソフトウェアが宛先に対する明示ルートを持っていない IPv4 パケットの出力先を指定します。
- **set ipv6 default next-hop**：ポリシー ルーティングのルート マップの一致条件を満たしたパケットのうち、シスコ ソフトウェアが宛先に対する明示ルートを持っていない IPv6 パケットの出力先を指定します。

通常のルーティングおよび転送動作の変更

ポリシーベース ルーティング（PBR）を設定するときに、標準のルーティングおよび転送動作を変更するために次の 6 種類の **set** コマンドを使用できます。**set ip next-hop** コマンドの潜在的な例外を除き、これらの **set** コマンドを設定すると、パケットが仮想ルーティングおよび転送（VRF）インスタンスに属していない場合は、インターフェイスに入るパケットのルーティング動作がオーバーライドされます。パケットはグローバル ルーティング テーブルを介して出力インターフェイスからルーティングされます。

- **set default interface**：ポリシー ルーティングのルート マップの一致条件を満たしたパケットのうち、宛先に対する明示ルートを持っていないパケットの出力先を示します。
- **set interface**：パケットが VRF インターフェイスに入るときに、レイヤ 2 書き換え情報を使用できる場合は、set interface ポリシーに従って同じ VRF 下の出力インターフェイスからパケットをルーティングします。

（注） インターフェイスはピアツーピア（P2P）インターフェイスである必要があります。

- **set ip default next-hop**：ポリシー ルーティングのルート マップの一致条件を満たしたパケットのうち、シスコ ソフトウェアが宛先に対する明示ルートを持っていない IPv4 パケットの出力先を指定します。
- **set ipv6 default next-hop**：ポリシー ルーティングのルート マップの一致条件を満たしたパケットのうち、シスコ ソフトウェアが宛先に対する明示ルートを持っていない IPv6 パケットの出力先を指定します。

- **set ip next-hop**：ポリシー ルーティングのルート マップの一致条件を満たした IPv4 パケットの出力先を指定します。IPv4 パケットが VRF インターフェイスで受信され、同じ VPN 内の別のインターフェイスから送信されている場合、着信パケットの VRF のコンテキストはインターフェイスから継承されます。
- **set ipv6 next-hop**：ポリシー ルーティングのルート マップの一致条件を満たした IPv6 パケットの出力先を指定します。IPv6 パケットが VRF インターフェイスで受信され、同じバーチャル プライベート ネットワーク（VPN）内の別のインターフェイスから送信されている場合、着信パケットの VRF のコンテキストはインターフェイスから継承されます。

継承 VRF、VRF 間、および VRF からグローバルへのルーティングのサポート

ポリシーベース ルーティング（PBR）を使用した Multi-VRF 選択機能は、継承 VRF および VRF 間ルーティングをサポートします。継承 VRF ルーティングでは、仮想ルーティングおよび転送（VRF）インターフェイスに到着するパケットは、同じ出力 VRF インターフェイスによってルーティングされます。VRF 間ルーティングでは、VRF インターフェイスに到着するパケットは、他の出力 VRF インターフェイスのいずれかを介してルーティングされます。

VRF からグローバルへのルーティングによって、任意の VRF インターフェイスに入るパケットがグローバル ルーティング テーブルを介してルーティングされます。パケットが VRF インターフェイスに到着すると、宛先のルックアップは、通常、対応する VRF テーブルでのみ実行されます。パケットがグローバル インターフェイスに到着した場合、宛先のルックアップはグローバル ルーティング テーブルで実行されます。

ポリシーベース ルーティングを使用した Multi-VRF 選択機能は、継承 VRF、VRF 間、および VRF からグローバルへのルーティングをサポートするために、次の **set** コマンドを変更します。これらのコマンドは、デバイスがパケットのルーティング中に使用する順で示されています。

- **set global**：グローバル ルーティング テーブルを使用してパケットをルーティングします。このコマンドは、特定の VRF に属する入力パケットをグローバル ルーティング テーブルを介してルーティングする場合に有効です。
- **set ip global next-hop**：ポリシー ルーティングのルート マップの一致基準を満たしたパケットのうち、シスコ ソフトウェアでグローバル ルーティング テーブルが使用されている IPv4 パケットの転送先を示しています。
- **set ipv6 global next-hop**：ポリシー ルーティングのルート マップの一致基準を満たしたパケットのうち、シスコ ソフトウェアでグローバル ルーティング テーブルが使用されている IPv6 パケットの転送先を示しています。
- **set ip vrf next-hop**：デバイスが VRF テーブルの IPv4 ネクスト ホップをルックアップするようにします。IPv4 パケットが VRF に属するインターフェイスに到着し、パケットが別の VRF 経由でルーティングされる必要がある場合は、**set ip vrf next-hop** コマンドを使用できます。
- **set ipv6 vrf next-hop**：デバイスが VRF テーブルの IPv6 ネクスト ホップをルックアップするようにします。IPv6 パケットが VRF に属するインターフェイスに到着し、パケットが別の VRF 経由でルーティングされる必要がある場合は、**set ipv6 vrf next-hop** コマンドを使用できます。

- **set ip default vrf**：IPv4 継承 VRF ルーティングと、VRF 間ルーティングを提供します。IPv4 継承 VRF ルーティングでは、VRF インターフェイスに到着する IPv4 パケットは、同じ出力 VRF インターフェイスでルーティングされます。VRF 間ルーティングでは、VRF インターフェイスに到着する IPv4 パケットは、他の出力 VRF インターフェイスのいずれかを介してルーティングされます。
- **set ipv6 default vrf**：IPv6 の継承 VRF ルーティングと、VRF 間ルーティングを提供します。IPv6 継承 VRF ルーティングでは、VRF インターフェイスに到着する IPv6 パケットは、同じ出力 VRF インターフェイスでルーティングされます。VRF 間ルーティングでは、VRF インターフェイスに到着する IPv6 パケットは、他の出力 VRF インターフェイスのいずれかを介してルーティングされます。
- **set interface**：パケットが VRF に入るときに、レイヤ 2 書き換え情報を使用できる場合は、set interface ポリシーに従って同じ VRF 下の出力インターフェイスからパケットをルーティングします。
- **set default interface**：ポリシー ルーティングのルート マップの一致条件を満たしたパケットのうち、宛先に対する明示ルートを持っていないパケットの出力先を示します。インターフェイスは任意の VRF に属することができます。
- **set ip next-hop**：IPv4 パケットを、グローバル ルーティング テーブルを介して IPv4 間のルーティングおよび転送環境でルーティングします。
- **set ipv6 next-hop**：IPv6 パケットを、グローバル ルーティング テーブルを介して IPv6 間のルーティングおよび転送環境でルーティングします。
- **set vrf**：ルート マップでマッチングが適切に行われた後で、適切な VRF を選択します。VRS 対応 PSV では、VRF 間（または VRF から VRF への）スイッチングが許可されます。

ポリシーベース ルーティングを使用した Multi-VRF 選択の設定方法

ポリシーベース ルーティングを使用した Multi-VRF 選択の一致基準の定義

デフォルトのルーティングと転送を使用する代わりに選択的にパケットをルーティングするために、ポリシーベース ルーティング（PBR）を使用した Multi-VRF 選択機能の一致基準を定義します。

ポリシーベース ルーティング（PBR）を使用した Multi-VRF 選択の一致基準は、アクセス リストで定義します。標準アクセス リスト、名前付きアクセス リスト、および拡張アクセス リストがサポートされています。

match length ルートマップ コンフィギュレーション コマンドを設定して、パケット長に基づいて一致基準を定義できます。この設定オプションはすべてルート マップの中だけで定義されます。

ここでは、PBR ルート選択を設定する方法について説明します。

標準アクセス リストとともにポリシーベース ルーティングを使用した Multi-VRF 選択の設定

はじめる前に

ここでは、仮想ルーティングおよび転送（VRF）インスタンス、および関連する IP アドレスがすでに定義されていると見なされます。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **access-list***access-list-number* {**deny** | **permit**} [**source***source-wildcard*] [**log**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**access-list***access-list-number* {**deny** | **permit**} [**source***source-wildcard*] [**log**] 例： `Device(config)# access-list 40 permit source 10.1.1.0/24 0.0.0.255`	アクセス リストを作成し、ルートマップの一致基準を定義します。 • 一致基準は、IP アドレス、IP アドレスの範囲、および他の IP パケット アクセス リストのフィルタリング オプションに基づいて定義できます。サポートされるアクセス リストは、名前付きアクセス リスト、番号付きアクセス リスト、標準アクセス リスト、および拡張アクセス リストです。一致基準を定義するために、すべての IP アクセス リスト設定オプションを使用できます。 • この例は、番号 40 の標準アクセス リストを作成しています。このフィルタは、10.1.1.0/24 サブネット内の IP アドレスを持つすべてのホストからのトラフィックを許可します。

名前付き拡張アクセス リストとともにポリシーベース ルーティングを使用した Multi-VRF 選択の設定

名前付き拡張アクセス リストでポリシーベース ルーティング（PBR）を使用した Multi-VRF 選択を設定するには、次の手順を実行します。

はじめる前に

ここでは、仮想ルーティングおよび転送（VRF）インスタンス、および関連する IP アドレスがすでに定義されていると見なされます。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **ip access-list** {**standard** | **extended**} [*access-list-name* | *access-list-number*]
4. [*sequence-number*] {**permit** | **deny**} *protocolsourcesource-wildcarddestinationdestination-wildcard* [**option***option-value*] [**precedence***precedence*] [**tos***tos*] [**ttl***operator-vaue*] [**log**] [**time-range***time-range-name*] [**fragments**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**ip access-list** {**standard** | **extended**} [*access-list-name* | *access-list-number*] 例： `Device(config)# ip access-list extended NAMEDACL`	IP アクセス リストのタイプを指定し、対応するアクセス リスト コンフィギュレーション モードを開始します。 • 標準、拡張、または名前付きアクセス リストを指定できます。
ステップ 4	[*sequence-number*] {**permit** | **deny**} *protocolsourcesource-wildcarddestinationdestination-wildcard* [**option***option-value*] [**precedence***precedence*] [**tos***tos*] [**ttl***operator-vaue*] [**log**] [**time-range***time-range-name*] [**fragments**]	アクセス リストでパケットを許可または拒否する基準を定義します。 • 一致基準は、IP アドレス、IP アドレスの範囲、および他の IP パケット アクセス リス

	コマンドまたはアクション	目的
	例： `Device(config-ext-nacl)# permit ip any any option any-options`	トのフィルタリング オプションに基づいて定義できます。サポートされるアクセス リストは、名前付きアクセス リスト、番号付きアクセス リスト、標準アクセス リスト、および拡張アクセス リストです。一致基準を定義するために、すべての IP アクセス リスト設定オプションを使用できます。 • この例は、設定された IP オプションをすべて許可する名前付きアクセス リストを作成しています。

ルート マップでの Multi-VRF 選択の設定

着信パケットは、ルート マップに定義された一致基準を使用してフィルタリングされます。マッチングが適切に行われたあと、**set** コマンド コンフィギュレーションによって、アウトバウンド バーチャル プライベート ネットワーク（VPN）パケットをポリシーに従ってルーティングする VRF が決定されます。

はじめる前に

ルート マップを設定する前に仮想ルーティングおよび転送（VRF）インスタンスを定義する必要があります。そうしないと、エラー メッセージがコンソールに表示されます。

受信エントリは、**ip vrf receive** コマンドを使用して VRF 選択テーブルに追加する必要があります。ルート マップで match と set の処理が行われたときにローカル VRF テーブルに受信エントリがない場合、パケットの宛先がローカルであればそのパケットはドロップされます。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **route-map***map-tag* [**permit** | **deny**] [*sequence-number*]
4. 次のいずれかを実行します。
   - **set ip vrf***vrf-name***next-hop***global-ipv4-address* [*...global-ipv4-address*]
   - **set ipv6 vrf***vrf-name***next-hop***global-ipv6-address* [*...global-ipv6-address*]
   - **set ip next-hop recursive vrf***global-ipv4-address* [*...global-ipv4-address*]
   - **set ip global next-hop***global-ipv4-address* [*...global-ipv4-address*]
   - **set ipv6 global next-hop***global-ipv6-address* [*...global-ipv6-address*]
5. 次のいずれかを実行します。
   - **match ip address** {*acl-number* [*acl-name* | *acl-number*]}
   - **match length***minimum-lengthmaximum-length*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**route-map***map-tag* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map map1 permit 10`	あるルーティング プロトコルから別のルーティング プロトコルへ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。

	コマンドまたはアクション	目的

ステップ 4	次のいずれかを実行します。
	• **set ip vrf***vrf-name***next-hop***global-ipv4-address* [*...global-ipv4-address*]
	• **set ipv6 vrf***vrf-name***next-hop***global-ipv6-address* [*...global-ipv6-address*]
	• **set ip next-hop recursive vrf***global-ipv4-address* [*...global-ipv4-address*]
	• **set ip global next-hop***global-ipv4-address* [*...global-ipv4-address*]
	• **set ipv6 global next-hop***global-ipv6-address* [*...global-ipv6-address*]
	例：
	`Device(config-route-map)# set ip vrf myvrf next-hop 10.0.0.0`
	例：
	`Device(config-route-map)# set ipv6 vrf myvrf next-hop 2001.DB8:4:1::1/64`
	例：
	`Device(config-route-map)# set ip next-hop recursive vrf 10.0.0.0`
	例：
	`Device(config-route-map)# set ip global next-hop 10.0.0.0`
	例：
	`Device(config-route-map)# set ipv6 global next-hop 2001.DB8:4:1::1/64`
		指定された VRF よりも IPv4 ネクスト ホップが低い必要がある場合に、ポリシー ルーティングのルート マップの一致基準を満たすパケットを転送する宛先を示します。
		指定された VRF よりも IPv6 ネクスト ホップが低い必要がある場合に、ポリシー ルーティングのルート マップの一致基準を満たすパケットを転送する宛先を示します。
		ルート マップに設定されている一致基準を満たすパケットのために宛先またはネクスト ホップが使用される IPv4 アドレスを示します。
		ソフトウェアがグローバル ルーティング テーブルを使用するポリシー ルーティングのルート マップの一致条件を満たすパケットを転送するための IPv4 アドレスを示します。
		ソフトウェアがグローバル ルーティング テーブルを使用するポリシー ルーティングのルート マップの一致条件を満たすパケットを転送するための IPv6 アドレスを示します。

ステップ 5	次のいずれかを実行します。 • **match ip address** {*acl-number* [*acl-name* | *acl-number*]}	標準アクセス リストまたは拡張アクセス リストで宛先ネットワーク番号のアドレスが許可されているルートを配布し、一致したパケットのポリシー ルーティングを行います。IP アクセス リストがサポートされます。

	コマンドまたはアクション	目的

	• **match length***minimum-lengthmaximum-length*
	
	例：
	`Device(config-route-map)# match ip address 1`
	`or`
	
	例：
	`Device(config-route-map)# match length 3 200`
		• この例は、標準アクセス リスト 1 を使用して一致基準を定義するように、ルート マップを設定しています。
		
		IP ヘッダー中のレイヤ 3 パケット長をクラス マップ中の一致条件として指定します。
		
		• この例は、長さが 3 ～ 200 バイトのパケットに一致するルート マップを設定しています。

ステップ 6	**end** 例： `Device(config-route-map)# end`	特権 EXEC モードに戻ります。

インターフェイスでポリシーベース ルーティングと IP VRF 受信を使用した Multi-VRF 選択の設定

ルート マップは、**ip policy route-map** インターフェイス コンフィギュレーション コマンドを使用して着信インターフェイスにアタッチします。

送信元 IP アドレスは仮想ルーティングおよび転送（VRF）選択テーブルに追加する必要があります。VRF 選択は一方向（単一方向）の機能で、着信インターフェイスに適用されます。ルート マップで **match** と **set** の処理が行われたときにローカル VRF テーブルに受信エントリがない場合、パケットの宛先がローカルであればそのパケットはドロップされます。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***typenumber* [*name-tag*]
4. **ip policy route-map***map-tag*
5. **ip vrf receive***vrf-name*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**interface***typenumber* [*name-tag*] 例： `Device(config)# interface FastEthernet 0/1/0`	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	**ip policy route-map***map-tag* 例： `Device(config-if)# ip policy route-map map1`	インターフェイスでポリシー ルーティングに使用するルート マップを特定します。 • この設定例は、map1 という名前のルート マップをインターフェイスに付加しています。
ステップ 5	**ip vrf receive***vrf-name* 例： `Device(config-if)# ip vrf receive VRF-1`	インターフェイスに関連付けられた IP アドレスを VRF テーブルに追加します。 • このコマンドは、VRF 選択に使用される VRF ごとに設定する必要があります。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

ポリシーベース ルーティングを使用した Multi-VRF 選択の設定の確認

ポリシーベース ルーティング（PBR）を使用した Multi-VRF 選択機能の設定を確認するには、次の手順を実行します。コマンドは任意の順序で入力できます。

手順の概要

1. **show ip access-list** [*access-list-number* | *access-list-name*]
2. **show route-map** [*map-name*]
3. **show ip policy**

手順の詳細

ステップ 1 **show ip access-list** [*access-list-number* | *access-list-name*]

ポリシーベース ルーティングを使用した Multi-VRF 選択の一致基準の設定を確認します。コマンド出力には、3 つの標準アクセス リストに一致基準として定義された 3 つのサブネット範囲が表示されます。

例：

```
Device# show ip access-list

Standard IP access list 40
 10 permit 10.1.0.0, wildcard bits 0.0.255.255
Standard IP access list 50
 10 permit 10.2.0.0, wildcard bits 0.0.255.255
Standard IP access list 60
 10 permit 10.3.0.0, wildcard bits 0.0.255.255
```

ステップ 2 **show route-map** [*map-name*]

ルート マップ内の **match** および **set** コマンドを確認します。

例：

```
Device# show route-map
```

出力には、各ルート マップ シーケンスの一致基準および設定アクションが表示されます。また、出力には、ルート マップ シーケンスごとに、ポリシー ルーティングが行われたパケット数とバイト数も表示されます。

例：

```
Device# show route-map map1

route-map map1, permit, sequence 10
Match clauses:
Set clauses:
 ip next-hop vrf myvrf 10.5.5.5  10.6.6.6  10.7.7.7
 ip next-hop global 10.8.8.8  10.9.9.9
Policy routing matches: 0 packets, 0 bytes
Device# show route-map map2
route-map map2, permit, sequence 10
Match clauses:
Set clauses:
 vrf myvrf
Policy routing matches: 0 packets, 0 bytes
Device# show route-map map3
route-map map3, permit, sequence 10
Match clauses:
Set clauses:
 global
Policy routing matches: 0 packets, 0 bytes
```

次の **show route-map** コマンドは、**set ip vrf next-hop** コマンドの出力を表示します。

例：

```
Device(config)# route-map test

Device(config-route-map)# set ip vrf myvrf next-hop
Device(config-route-map)# set ip vrf myvrf next-hop 192.168.3.2
Device(config-route-map)# match ip address 255 101
Device(config-route-map)# end
Device# show route-map

route-map test, permit, sequence 10
 Match clauses:
  ip address (access-lists): 101
 Set clauses:
  ip vrf myvrf next-hop 192.168.3.2
 Policy routing matches: 0 packets, 0 bytes
```

次の **show route-map** コマンドは、**set ip global** コマンドの出力を表示します。

例：

```
Device(config)# route-map test
Device(config-route-map)# match ip address 255 101
Device(config-route-map)# set ip global next-hop 192.168.4.2
Device(config-route-map)# end
Device# show route-map

*May 25 13:45:55.551: %SYS-5-CONFIG_I: Configured from console by consoleout-map
route-map test, permit, sequence 10
 Match clauses:
  ip address (access-lists): 101
 Set clauses:
  ip global next-hop 192.168.4.2
 Policy routing matches: 0 packets, 0 bytes
```

ステップ 3 **show ip policy**

ポリシーベース ルーティングを使用した Multi-VRF 選択のポリシーを確認します。

例：

```
Device# show ip policy
```

次の **show ip policy** コマンド出力には、ポリシー ルーティングを設定したインターフェイスおよび関連付けられたルート マップが表示されます。

例：

```
Device# show ip policy

Interface                Route map
FastEthernet0/1/0        PBR-VRF-Selection
```

ポリシーベース ルーティングを使用した Multi-VRF 選択の設定例

例：ポリシーベース ルーティングを使用した Multi-VRF 選択の一致基準の定義

次に、3 つの標準アクセス リストを作成して、3 つの異なるサブネットワークの一致基準を定義する例を示します。FastEthernet インターフェイス 0/1/0 で受信されたすべてのパケットは、PBR-VRF-Selection ルート マップを経由して、同じルートマップ シーケンスで一致した仮想ルーティングおよび転送（VRF）にルーティングされます。パケットの送信元 IP アドレスが 10.1.0.0/24 サブネットに含まれる場合は、ルーティングおよび転送に VRF1 が使用されます。

```
access-list 40 permit source 10.1.0.0 0.0.255.255
access-list 50 permit source 10.2.0.0 0.0.255.255
access-list 60 permit source 10.3.0.0 0.0.255.255
route-map PBR-VRF-Selection permit 10
 match ip address 40
 set vrf VRF1
 !
route-map PBR-VRF-Selection permit 20
 match ip address 50
 set vrf VRF2
 !
route-map PBR-VRF-Selection permit 30
 match ip address 60
 set vrf VRF3
 !
interface FastEthernet 0/1/0
 ip address 192.168.1.6 255.255.255.252
 ip vrf forwarding VRF4
 ip policy route-map PBR-VRF-Selection
 ip vrf receive VRF1
 ip vrf receive VRF2
 ip vrf receive VRF3
```

例：ルート マップでの Multi-VRF 選択の設定

次の例は、myvrf という名前の仮想ルーティングおよび転送（VRF）インターフェイスにポリシーベース ルーティングを適用し、ネクスト ホップの IP アドレスを 10.0.0.2 として指定する **set ip vrf next-hop** コマンドを示します。

```
Device(config)# route-map map1 permit
Device(config)# set vrf myvrf
Device(config-route-map)# set ip vrf myvrf next-hop 10.0.0.2
Device(config-route-map)# match ip address 101
Device(config-route-map)# end
```

次の例は、デバイスがグローバル ルーティング テーブルでネクスト ホップ アドレス 10.0.0.1 を使用するように指定する、**set ip global** コマンドを示します。

```
Device(config-route-map)# set ip global next-hop 10.0.0.1
```

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 Master Command List, All Releases』
MPLS と MPLS アプリケーション コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』
IP アクセス リスト コマンド	『*Cisco IOS Security Command Reference*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。	http://www.cisco.com/cisco/web/support/index.html

ポリシーベース ルーティングを使用した Multi-VRF 選択の機能情報

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 に移動します。Cisco.com のアカウントは必要ありません。

表 *9*：ポリシーベース ルーティングを使用した *Multi-VRF* 選択の機能情報

機能名	リリース	機能情報
ポリシーベース ルーティング（PBR）を使用した Multi-VRF 選択	12.2(33)SRB1 12.2(33) SXH1 12.4(24)T Cisco IOS XE Release 2.2	ポリシーベース ルーティング（PBR）を使用した Multi-VRF 選択機能を使用すると、プロバイダー エッジ（PE）のルータ上の指定されたインターフェイスが、IP アクセス リストで定義されているパケット長や一致基準に基づいて、バーチャルプライベート ネットワーク（VPN）にパケットをルーティングできます。この機能と、MPLS VPN 送信元 IP アドレスに基づく VRF 選択機能は、同じインターフェイス上で一緒に設定できます。 この機能は、Cisco IOS Release 12.2(33)SRB1 で導入されました。 サポートは、Cisco IOS Release 12.2(33)SXH1 で追加されました。 この機能は、Cisco IOS Release 12.4(24)T で統合されました。 Cisco IOS XE Release 2.2 では、この機能は Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに実装されました。 次のコマンドが変更されました。**set ip global next-hop**、**set ip vrf next-hop**

機能名	リリース	機能情報
IPv6 VRF 対応 PBR のネクストホップの機能拡張	15.2(2)S Cisco IOS XE Release 3.6S	この機能は、Cisco IOS Release 15.2(2)S で導入されました。 Cisco IOS XE Release 3.6S では、この機能は Cisco ASR 1000 シリーズ アグリゲーション サービスルータに導入されました。 次のコマンドが導入されました。**set ipv6 default next-hop**、**set ipv6 next-hop (PBR)**

用語集

CE デバイス：カスタマーエッジデバイス。カスタマー ネットワークに属し、プロバイダーエッジ（PE）デバイスとのインターフェイスとなるデバイス。

継承 VRF ルーティング：VRF インターフェイスに到着したパケットは、同じ出力 VRF インターフェイスでルーティングされます。

VRF 間ルーティング：VRF インターフェイスに到着するパケットは、他の出力 VRF のインターフェイス経由でルーティングされます。

IP：Internet Protocol（インターネット プロトコル）。TCP/IP スタックにおいてコネクションレス型のネットワーク間サービスを提供するネットワーク層プロトコル。IP では、アドレッシング、タイプオブサービス指定、フラグメンテーションと再編成、セキュリティなどの機能が提供されます。RFC 791 に定義されています。

PBR：Policy-Based Routing（ポリシーベース ルーティング）。PBR では、受信パケットをどのようにルーティングするかをユーザが手動で設定することができます。

PE デバイス：プロバイダー エッジ デバイス。サービス プロバイダーのネットワークの一部であり、CEデバイスに接続されたデバイス。これは、スタティック ルーティングまたはBGP、RIPv1、RIPv2 などのルーティング プロトコルを使用してCEデバイスとルーティング情報を交換します。

VPN：Virtual Private Network（バーチャル プライベート ネットワーク）。共通のルーティング テーブルを共有するサイトのコレクション。VPN は、ISP バックボーン ネットワーク上で帯域幅を共有するための安全な方法を提供します。

VRF：VPN Routing and Forwarding（VPN ルーティングおよび転送）インスタンス。VRF は、IP ルーティング テーブル、取得されたルーティング テーブル、そのルーティング テーブルを使用する一連のインターフェイス、ルーティング テーブルに登録されるものを決定する一連のルールおよびルーティング プロトコルで構成されています。

VRF-lite：サービス プロバイダーが複数の VPN をサポートし、VPN 間で IP アドレスを重複して使用できるようにする機能。

第 11 章

ポリシーベース ルーティングを使用した MPLS VPN VRF 選択

ポリシーベース ルーティングを使用した MPLS VPN VRF 選択機能は、送信元 IP アドレスに基づく MPLS VPN VRF 選択機能を拡張したものです。この機能によってポリシーベース ルーティング（PBR）メカニズムが導入され、複数の VPN ルーティングおよび転送（VRF）選択の一致基準に基づいてバーチャル プライベート ネットワーク（VPN）トラフィックの分類と転送が行われます。

- 機能情報の確認，195 ページ
- ポリシーベース ルーティングを使用した MPLS VPN VRF 選択の前提条件，196 ページ
- ポリシーベース ルーティングを使用した MPLS VPN VRF 選択の制約事項，196 ページ
- ポリシーベース ルーティングを使用した MPLS VPN VRF 選択に関する情報，197 ページ
- ポリシーベース ルーティングを使用した MPLS VPN VRF 選択の設定方法，198 ページ
- ポリシーベース ルーティングを使用した MPLS VPN VRF 選択の設定例，207 ページ
- その他の参考資料，208 ページ
- ポリシーベース ルーティングを使用した MPLS VPN VRF 選択の機能情報，209 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 に移動します。Cisco.com のアカウントは必要ありません。

ポリシーベース ルーティングを使用した MPLS VPN VRF 選択の前提条件

- デバイスは、ポリシーベース ルーティング（PBR）をサポートしている必要があります。PBR をサポートしていないプラットフォームについては、「送信元 IP アドレスに基づく MPLS VPN VRF 選択」機能を使用します。
- この機能を設定する前に Virtual Routing and Forwarding（VRF）インスタンスを定義しておく必要があります。VRF が存在しない場合は、コンソールにエラー メッセージが表示されます。
- ポリシーベース ルーティングを使用した MPLS VPN VRF 選択機能を設定する前に、VRF および関連する IP アドレスが定義されていることを確認します。
- このマニュアルでは、ネットワークでマルチプロトコル Border Gateway Protocol（mBGP）、マルチプロトコル ラベル スイッチング（MPLS）、および Cisco Express Forwarding がイネーブルになっていることを前提としています。

ポリシーベース ルーティングを使用した MPLS VPN VRF 選択の制約事項

- ポリシーベース ルーティングを使用した MPLS VPN VRF 選択機能は、サービス プロバイダー（-p-）イメージでのみサポートされます。
- ポリシーベース ルーティングを使用した MPLS VPN VRF 選択機能と送信元 IP アドレスに基づく MPLS VPN VRF 選択機能は同じデバイス上に共存できますが、同じインターフェイスにはこれらの機能を同時に設定できません。これは、これらの機能の設定を誤った場合に Virtual Routing and Forwarding（VRF）テーブル選択の衝突を防ぐよう設計された動作です。同じインターフェイス上で **ip vrf select source** コマンドと **ip policy route-map** コマンドを設定しようとすると、コンソールにエラー メッセージが表示されます。
- プロトコル独立マルチキャスト（PIM）およびマルチキャスト パケットはポリシーベース ルーティング（PBR）をサポートしていません。また、この機能の一致基準になっている送信元 IP アドレスには、PIM とマルチキャスト パケットを設定できません。
- ポリシーベース ルーティングを使用した MPLS VPN VRF 選択機能は IP プレフィックス リストでは設定できません。

ポリシーベース ルーティングを使用した MPLS VPN VRF 選択に関する情報

ポリシーベース ルーティングを使用した MPLS VPN VRF 選択の概要

ポリシーベース ルーティングを使用した MPLS VPN VRF 選択機能は、送信元 IP アドレスに基づく MPLS VPN VRF 選択機能を拡張したものです。Virtual Routing and Forwarding（VRF）選択機能のポリシーベース ルーティング（PBR）実装を使用すると、ポリシーの一致基準に基づいてバーチャルプライベートネットワーク（VPN）トラフィックをルーティングできます。一致基準の定義はIPアクセスリストであったり、パケット長であったりします。シスコ ソフトウェアがサポートする一致基準は、次のとおりです。

- IP アクセス リスト：IP アドレス、IP アドレスの範囲、および他の IP パケット アクセス リストのフィルタリング オプションに基づいて、一致基準を定義します。サポートされるアクセス リストは、名前付きアクセス リスト、番号付きアクセス リスト、標準アクセス リスト、および拡張アクセス リストです。一致基準の定義にはシスコ ソフトウェアのすべての IP アクセス リスト設定オプションを使用できます。
- パケット長：パケットの長さ（バイト単位）に基づいて、一致基準を定義します。パケット長フィルタは、**match length** ルート マップ コンフィギュレーション コマンドを使用してルート マップに定義します。

ポリシー ルーティングはルート マップで定義します。ルート マップは、**ip policy route-map** インターフェイスコンフィギュレーションコマンドを使用して着信インターフェイスに適用します。IP アクセス リストは、**match ip address** ルートマップ コンフィギュレーション コマンドを使用して、ルート マップに適用されます。パケット長の一致基準は、**match length** ルートマップ コンフィギュレーション コマンドを使用してルート マップに適用されます。設定アクションは、**set vrf** ルート マップ コンフィギュレーション コマンドを使用して定義します。一致基準が評価されると、set 句によって適切な VRF が選択されます。この組み合わせを使用すると、着信 VPN トラフィックの一致基準を定義し、VPN パケットをポリシーに従って適切な VRF にルーティングできます。

ポリシーベース ルーティングの set 句：概要

ポリシーベースルーティング（PBR）を設定する場合は、次の 4 つの set 句を使用して通常のルーティングおよび転送動作を変更できます。

- **set default interface**
- **set interface**
- **set ip default next-hop**
- **set ip next-hop**

いずれかの set 句を設定すると、パケットの通常のルーティングおよび転送動作は上書きされます。

ポリシーベース ルーティングを使用した MPLS VPN VRF 選択機能には、標準のルーティングおよび転送動作の変更に使用できる 5 番めの set 句が導入されました。**set vrf** コマンドは、ルートマップでマッチングが適切に行われた後で適切な Virtual Routing and Forwarding（VRF）インスタンスを選択するために使用します。

パケット長に基づくポリシーベース ルーティング VRF 選択の一致基準

ポリシーベース ルーティング（PBR）Virtual Routing and Forwarding（VRF）ルート選択に使用する一致基準は、アクセスリストに定義します。サポートされているアクセスリストは、標準アクセス リストおよび名前付きアクセス リストです。一致基準は、**match length** ルートマップ コンフィギュレーション コマンドを使用することで、パケット長に基づいて定義することもできます。この設定オプションはすべてルート マップの中だけで定義されます。

ポリシーベース ルーティングを使用した MPLS VPN VRF 選択の設定方法

標準アクセス リストを使用した ポリシーベース ルーティング VRF 選択の設定

VPN トラフィックのデータ パケット送信を許可または拒否するために、標準アクセス リストを作成し、そのリストにポリシーベース ルーティング（PBR）Virtual Routing and Forwarding（VRF）ルート選択の一致基準を定義するには、次のコマンドを使用します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **access-list***access-list-number* {**deny** | **permit**} *source-addr* [*source-wildcard*] [**log**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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	**configure terminal** 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	**access-list***access-list-number* {**deny** | **permit**} *source-addr* [*source-wildcard*] [**log**] 例： `Device(config)# access-list 40 permit 10.1.0.0/24 0.0.0.255`	アクセス リストを作成し、ルートマップの一致基準を定義します。 • 一致基準は、IP アドレス、IP アドレスの範囲、および他の IP パケット アクセス リストのフィルタリング オプションに基づいて定義できます。サポートされるアクセス リストは、名前付きアクセス リスト、番号付きアクセス リスト、標準アクセス リスト、および拡張アクセス リストです。一致基準の定義にはシスコ ソフトウェアのすべての IP アクセス リスト設定オプションを使用できます。 • この例は、番号 40 の標準アクセス リストを作成しています。このフィルタにより、10.1.0.0/24 サブネットの IP アドレスを持つホストからのトラフィックが許可されます。

名前付きアクセス リストを使用したポリシーベース ルーティング VRF 選択の設定

Virtual Routing and Forwarding（VPN）トラフィックのデータ パケット送信を許可または拒否するために、名前付きアクセス リストにポリシーベース ルーティング（PBR）Virtual Routing and Forwarding（VRF）ルート選択の一致基準を定義するには、次のコマンドを使用します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **ip access-list** {**standard** | **extended**} [*access-list-name* | *access-list-number*]
4. [*sequence-number*] {**permit** | **deny**} *protocolsource-addrsource-wildcarddestination-addrdestination-wildcard* [**option***option-value*] [**precedence***precedence*] [**tos***tos*] [**log**] [**time-range***time-range-name*] [**fragments**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**イネーブル化** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**ip access-list** {**standard** | **extended**} [*access-list-name* | *access-list-number*] 例： `Device(config)# ip access-list extended NAMEDACL`	IP アクセス リストのタイプを指定し、対応するアクセス リスト コンフィギュレーション モードを開始します。 • 標準、拡張、または名前付きのアクセス リストを使用できます。
ステップ 4	[*sequence-number*] {**permit** | **deny**} *protocolsource-addrsource-wildcarddestination-addrdestination-wildcard* [**option***option-value*] [**precedence***precedence*] [**tos***tos*] [**log**] [**time-range***time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# permit ip any any option any-options`	アクセス リストでパケットを許可または拒否する基準を定義します。 • 一致基準は、IP アドレス、IP アドレスの範囲、および他の IP パケット アクセス リストのフィルタリング オプションに基づいて定義できます。サポートされるアクセスリストは、名前付きアクセスリスト、番号付きアクセスリスト、標準アクセスリスト、および拡張アクセスリストです。一致基準の定義にはシスコ ソフトウェアのすべての IP アクセス リスト設定オプションを使用できます。 • この例は、設定された IP オプションをすべて許可する名前付きアクセス リストを作成しています。

ルート マップでのポリシーベース ルーティング VRF 選択の設定

バーチャル プライベート ネットワーク（VPN）トラフィックのデータ パケット送信を許可または拒否するために、アウトバウンド VPN パケットをポリシーに従ってルーティングする VRF を設定するには、次のコマンドを使用します。

着信パケットは、ルート マップに定義された一致基準を使用してフィルタリングされます。マッチングが適切に行われたあと、**set vrf** コマンド コンフィギュレーションによって、アウトバウンド VPN パケットをポリシーに従ってルーティングする VRF が決定されます。

はじめる前に

- ルート マップを設定する前に、Virtual Routing and Forwarding（VRF）インスタンスを定義しておく必要があります。定義されていない場合はコンソールにエラー メッセージが表示されます。
- 受信エントリは、**ip vrf receive** コマンドを使用して VRF 選択テーブルに追加する必要があります。ルート マップで match と set の処理が行われたときにローカル VRF テーブルに受信エントリがない場合、パケットの宛先がローカルであればそのパケットはドロップされます。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **route-map***map-tag* [**permit** | **deny**] [*sequence-number*]
4. 次のいずれかを実行します。
   - **match ip address** {*acl-number* [*acl-number* ...| *acl-name* ...]| *acl-name* [*acl-name* ...| *acl-number* ...]}
   -
   - **match length***minimum-lengthmaximum-length*
5. **set vrf***vrf-name*
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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	**configure terminal** 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	**route-map***map-tag* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map map1 permit 10`	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。 あるルーティング プロトコルから別のルーティング プロトコルへ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ます。

ステップ 4	次のいずれかを実行します。
	
	• **match ip address** {*acl-number* [*acl-number* ...| *acl-name* ...]| *acl-name* [*acl-name* ...| *acl-number* ...]}
	•
	• **match length***minimum-lengthmaximum-length*
	
	例：
	
	`Device(config-route-map)# match ip address 1`
	
	例：
	
	`Device(config-route-map)# match length 3 200`
		標準アクセス リストまたは拡張アクセス リストで宛先ネットワーク番号のアドレスが許可されているルートを配布し、一致したパケットのポリシー ルーティングを行います。
		
		• IP アクセス リストがサポートされます。
		
		• この例は、標準アクセス リスト 1 を使用して一致基準を定義するように、ルート マップを設定しています。
		
		または
		
		IP ヘッダー中のレイヤ 3 パケット長をクラス マップ中の一致条件として指定します。
		
		• この例は、サイズが 3 ～ 200 バイトのパケットに一致するルート マップを設定しています。

ステップ 5	**set vrf***vrf-name* 例： `Device(config-route-map)# set vrf map1`	ポリシーベース ルーティング（PBR）VRF 選択の同じルート マップ シーケンスで適切にマッチングが行われた VPN パケットをルーティングする VRF を定義します。 • この例は、一致したパケットをポリシーに従って map1 という名前の VRF にルーティングします。
ステップ 6	**exit** 例： `Device(config-route-map)# exit`	グローバル コンフィギュレーション モードに戻ります。

インターフェイスでのポリシーベース ルーティングの設定

着信バーチャル プライベート ネットワーク（VPN）トラフィック データ パケットをフィルタリングするには、次のコマンドを使用します。着信パケットは、ルート マップに定義された一致基準を使用してフィルタリングされます。

ルート マップは着信インターフェイスに適用されます。ルート マップは、**ip policy route-map** グローバル コンフィギュレーション コマンドを使用して着信インターフェイスにアタッチします。

（注）

- ポリシーベース ルーティングを使用した MPLS VPN VRF 選択機能と送信元 IP アドレスに基づく MPLS VPN VRF 選択機能は同じデバイス上に共存できますが、同じインターフェイスには 2 つの機能を同時に設定できません。これは、これらの機能の設定を誤った場合に Virtual Routing and Forwarding（VRF）テーブル選択の衝突を防ぐよう設計された動作です。同じインターフェイス上で **ip vrf select source** コマンドと **ip policy route-map** コマンドを設定しようとすると、コンソールにエラー メッセージが表示されます。

>

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***typenumber* [*name-tag*]
4. **ip policy route-map***map-tag*
5. **ip vrf receive***vrf-name*
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**interface***typenumber* [*name-tag*] 例： `Device(config)# interface FastEthernet 0/1/0`	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	**ip policy route-map***map-tag* 例： `Device(config-if)# ip policy route-map map1`	インターフェイスでポリシー ルーティングに使用するルート マップを特定します。 • この設定例は、map1 という名前のルートマップをインターフェイスに付加しています。
ステップ 5	**ip vrf receive***vrf-name* 例： `Device(config-if)# ip vrf receive VRF1`	インターフェイスに関連付けられた IP アドレスを VRF テーブルに追加します。 • このコマンドは、VRF 選択に使用される VRF ごとに設定する必要があります。
ステップ 6	**exit** 例： `Device(config-if)# exit`	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 モードに入ります。

インターフェイスでの IP VRF Receive の設定

Virtual Routing and Forwarding（VRF）ルーティング テーブル内の接続されたルート エントリとしてインターフェイスの IP アドレスを挿入するには、次のコマンドを使用します。このことにより、パケットがドロップされなくなります。

VRF 選択テーブルには送信元 IP アドレスを追加する必要があります。VRF 選択は一方向（単一方向）の機能で、着信インターフェイスに適用されます。ルート マップで match と set の処理が行われたときにローカル VRF テーブルに VRF 受信エントリがない場合、パケットの宛先がローカルであればそのパケットはドロップされます。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***typenumber* [*name-tag*]
4. **ip policy route-map***map-tag*
5. **ip vrf receive***vrf-name*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**interface***typenumber* [*name-tag*] 例： `Device(config)# interface FastEthernet 0/1/0`	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	**ip policy route-map***map-tag* 例： `Device(config-if)# ip policy route-map map1`	インターフェイスでポリシールーティングに使用するルート マップを特定します。 • この設定例は、map1 という名前のルートマップをインターフェイスに付加しています。
ステップ 5	**ip vrf receive***vrf-name* 例： `Device(config-if)# ip vrf receive VRF1`	インターフェイスに関連付けられた IP アドレスを VRF テーブルに追加します。 • このコマンドは、VRF 選択に使用される VRF ごとに設定する必要があります。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

ポリシーベース ルーティングを使用した MPLS VPN VRF 選択の設定の確認

手順の概要

1. イネーブル化
2. **show ip access-list** [*access-list-number* | *access-list-name*]
3. **show route-map** [*map-name*]
4. **show ip policy**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show ip access-list** [*access-list-number* | *access-list-name*] 例： `Device# show ip access-list`	現在のすべての IP アクセス リストの内容を表示します。 • アクセス リストに定義された一致基準を確認するには、このコマンドを使用します。名前付きアクセス リストと番号付きアクセス リストの両方がサポートされます。
ステップ 3	**show route-map** [*map-name*] 例： `Device# show route-map`	設定されたすべてのルート マップ、または指定した 1 つのルート マップだけを表示します。 • ルート マップ内の match 句および set 句を確認するには、このコマンドを使用します。
ステップ 4	**show ip policy** 例： `Device# show ip policy`	ポリシールーティングに使用されるルートマップを表示します。 • このコマンドを使用すると、ルート マップおよび関連付けられたインターフェイスを表示できます。

ポリシーベース ルーティングを使用した MPLS VPN VRF 選択の設定例

例：アクセス リストでのポリシーベース ルーティング VRF 選択の定義

次に、3 つの標準アクセス リストを作成して、3 つの異なるサブネットの一致基準を定義する例を示します。FastEthernet 0/1/0 インターフェイスで受信されたすべてのパケットは、ポリシーベース ルーティング（PBR）VRF 選択ルート マップを経由して、同じルートマップ シーケンスで一致した Virtual Routing and Forwarding（VRF）インスタンスにルーティングされます。パケットの送信元 IP アドレスが 10.1.0.0/24 サブネットに含まれる場合は、ルーティングおよび転送に VRF1 が使用されます。

```
access-list 40 permit 10.1.0.0 0.0.255.255
access-list 50 permit 10.2.0.0 0.0.255.255
access-list 60 permit 10.3.0.0 0.0.255.255
route-map PBR-VRF-Selection permit 10
 match ip address 40
 set vrf VRF1
 !
route-map PBR-VRF-Selection permit 20
 match ip address 50
 set vrf VRF2
 !
route-map PBR-VRF-Selection permit 30
 match ip address 60
 set vrf VRF3
 !
interface FastEthernet0/1/0
 ip address 10.1.0.0/24 255.255.255.252
 ip policy route-map PBR-VRF-Selection
 ip vrf receive VRF1
 ip vrf receive VRF2
 ip vrf receive VRF3
```

例：ポリシーベース ルーティングを使用した VRF 選択の確認

次に、定義された一致基準とルート マップ ポリシー設定を確認する例を示します。

例：一致基準の確認

ポリシーベースルーティング（PBR）VRF 選択の一致基準の設定を確認するには、**show ip access-list** コマンドを使用します。

次の **show ip access-list** コマンド出力には、3 つの標準アクセス リストに一致基準として定義された、3 つのサブネット範囲が表示されます。

```
Device# show ip access-list
```

```
Standard IP access list 40
    10 permit 10.1.0.0, wildcard bits 0.0.255.255
Standard IP access list 50
    10 permit 10.2.0.0, wildcard bits 0.0.255.255
Standard IP access list 60
    10 permit 10.3.0.0, wildcard bits 0.0.255.255
```

例：ルートマップ設定の確認

ルート マップの設定を確認するには、**show route-map** コマンドを使用します。出力には、各ルートマップ シーケンスの一致基準および設定アクションが表示されます。また、出力には、ルートマップ シーケンスごとに、ポリシー ルーティングが行われたパケット数とバイト数も表示されます。

```
Device# show route-map

route-map PBR-VRF-Selection, permit, sequence 10
  Match clauses:
    ip address (access-lists): 40
  Set clauses:
    vrf VRF1
  Policy routing matches: 0 packets, 0 bytes
route-map PBR-VRF-Selection, permit, sequence 20
  Match clauses:
    ip address (access-lists): 50
  Set clauses:
    vrf VRF2
  Policy routing matches: 0 packets, 0 bytes
route-map PBR-VRF-Selection, permit, sequence 30
  Match clauses:
    ip address (access-lists): 60
  Set clauses:
    vrf VRF3
  Policy routing matches: 0 packets, 0 bytes
```

例：ポリシーベース ルーティング VRF 選択ポリシーの確認

次の **showippolicy** コマンド出力には、ポリシー ルーティングを設定したインターフェイスおよび関連付けられたルート マップが表示されます。

```
Device# show ip policy

Interface                Route map
FastEthernet0/1/0        PBR-VRF-Selection
```

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 Master Command List, All Releases』
MPLS と MPLS アプリケーション 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	Link
★枠で囲まれた Technical Assistance の場合★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。	http://www.cisco.com/cisco/web/support/index.html

ポリシーベース ルーティングを使用した MPLS VPN VRF 選択の機能情報

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 に移動します。Cisco.com のアカウントは必要ありません。

表 *10*：ポリシーベース ルーティングを使用した *MPLS VPN VRF* 選択の機能情報

機能名	リリース	機能情報
ポリシーベース ルーティングを使用した MPLS VPN VRF 選択	12.3(7)T 12.2(25)S 12.2(33)SRB 12.2(33)SXI Cisco IOS XE Release 2.2	ポリシーベース ルーティングを使用した MPLS VPN VRF 選択機能は、送信元 IP アドレスに基づく MPLS VPN VRF 選択機能を拡張したものです。この機能によってポリシーベース ルーティング（PBR）メカニズムが導入され、複数の VPN ルーティングおよび転送（VRF）選択の一致基準に基づいてバーチャル プライベート ネットワーク（VPN）トラフィックの分類と転送が行われます。 この機能は、Cisco IOS Release 12.3(7)T で導入されました。 この機能は、Cisco IOS Releases 12.2(25)S、12.2(33)SRB、および 12.2(33)SXI で統合されました。 Cisco IOS XE Release 2.2 では、この機能は Cisco ASR 1000 シリーズ アグリゲーション サービスルータに導入されました。 次のコマンドが導入または変更されました：**ip vrf receive**、**set vrf**。

第 12 章

カスタマー エッジ（CE）ラベル単位での MPLS VPN

カスタマー エッジ（CE）ラベル単位での MPLS VPN 機能を使用すると、すべての即時ネクストホップまたはネクストホップのセットに対し、プロバイダーエッジ（PE）で単一の VPN ラベルを設定できます。

CE ラベル単位での MPLS VPN 機能は、グローバル コンフィギュレーション モードでイネーブル（またはディセーブル）にできます。

- 機能情報の確認，211 ページ
- CE ラベル単位での MPLS VPN の前提条件，212 ページ
- CE ラベル単位での MPLS VPN の制約事項，212 ページ
- CE ラベル単位での MPLS VPN に関する情報，213 ページ
- CE ラベル単位での MPLS VPN の設定方法，214 ページ
- CE ラベル単位での MPLS VPN の設定例，215 ページ
- その他の参考資料，216 ページ
- CE ラベル単位での MPLS VPN の機能情報，216 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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 に移動します。Cisco.com のアカウントは必要ありません。

CE ラベル単位での MPLS VPN の前提条件

- Virtual Routing and Forwarding（VRF）ドメインで以下のいずれかの機能がイネーブルになっている場合、CE ラベル単位での MPLS VPN 機能を設定する前に、それらの機能をディセーブルにします。
  - 外部ボーダー ゲートウェイ プロトコル（EBGP）マルチパス機能
  - 内部ボーダー ゲートウェイ プロトコル（IBGP）マルチパス機能
  - Carrier Supporting Carrier（CSC）機能
- マルチプロトコル ラベル スイッチング（MPLS）レイヤ 3 VPN を設定する前に、MPLS、ラベル配布プロトコル（LDP）、およびシスコ エクスプレス フォワーディングをネットワークにインストールする必要があります。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。

CE ラベル単位での MPLS VPN の制約事項

- CE ラベル単位での MPLS VPN 機能をイネーブルにすると、Border Gateway Protocol（BGP）の再コンバージェンスが行われます。その結果、マルチプロトコル ラベル スイッチング（MPLS）VPN コアから発信されるトラフィックでデータ損失が発生する可能性があります。

（注） スケジュールされた MPLS メンテナンス ウィンドウの間にこの機能をイネーブルにすることで、ネットワークの中断を最小限に抑えることができます。また、可能であれば、現在アクティブなデバイスでこの機能をイネーブルにすることは避けてください。

- IPv6 プロバイダー エッジ デバイス（6PE）はサポートされていません。
- プレフィックス非依存コンバージェンス（PIC）はサポートされていません。マルチパスを使用した CE ラベル単位のみがサポートされています。この機能は、次の機能と同時には使用できません。
  - 内部ボーダー ゲートウェイ プロトコル（IBGP）マルチパス機能
  - Carrier Supporting Carrier（CSC）機能

- CE ラベル単位が設定されると、MPLS フォワーディングインフラストラクチャ（MFI）は、スタンバイデバイスにキーとラベル情報をバックアップする必要があります。これはソフトウェアのダウングレードに影響します。
- BGP 最良外部機能を使用すると、ネットワークにバックアップ外部ルートを用意でき、プライマリ外部ルートの接続が失われるのを回避できます。この機能はサポートされていません。
- PE デバイス上での BGP 以外のプロトコルからのルートのインポートはサポートされていません。
- ネクスト ホップがゼロのすべてのネットワークでは、ネクスト ホップが確実に判別できないため、ネットワークごとに 1 つのラベルが割り当てられます。
- 1 つの VRF ドメインに同じアドレスを持つ複数のネイバーがある場合は、CE ごとのラベルを使用しないでください。
- シングル ホップ EBGP のみがサポートされます。マルチホップ EBGP はサポートされません。
- 高可用性構成でスタンバイからのスイッチオーバー後にラベルが維持されるのは、BGP セッションを確立する前に BGP グレースフル リスタートが設定されている場合のみです。

CE ラベル単位での MPLS VPN に関する情報

CE ラベル単位での MPLS VPN 機能

プロバイダーエッジ（PE）デバイスには、ローカルおよびリモート ルートが格納されており、各ルートに対するラベル エントリも含まれています。分散プラットフォームでは、プレフィックス単位のラベルによりメモリが消費されます。多数の Virtual Routing and Forwarding（VRF）ドメインとルートが存在する場合、プレフィックス単位のラベルにより消費されるメモリ量が問題となります。CE ラベル単位の割り当てを使用する目的は、PE デバイスのルーティング テーブルの追加のルックアップを避け、ラベル スペースを節約することです。

CE ラベル単位の MPLS VPN 機能を使用すると、一意のカスタマーエッジ（CE）ピア デバイスからアドバタイズされたすべてのルートで同じラベルを使用できます。PE デバイスは、すべての即時ネクスト ホップ（ほとんどの場合、ネクスト ホップ CE ルータ）に 1 個のラベルを割り当てます。このラベルは直接、ネクストホップにマップされるため、データ フォワーディング中に VRF ルート ルックアップが実行されることはありません。ただし、割り当てられるラベルの数は、プレフィックス 1 つにつき 1 つではなく、CE 1 つにつき 1 つです。BGP はすべてのネクスト ホップを認識するため、各ネクスト ホップにラベルを割り当てます（各 PE-CE インターフェイスではありません）。

CE ラベル単位での MPLS VPN の設定方法

CE ラベル単位機能の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **mpls label mode** {**vrf***vrf-name* | **all-vrfs**} **protocol** {**bgp-vpnv4** | **bgp-vpnv6** | **all-afs**} {**per-ce**}
4. **end**
5. **show ip vrf detail**
6. **show mpls forwarding-table**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードを開始します。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**mpls label mode** {**vrf***vrf-name*	**all-vrfs**} **protocol** {**bgp-vpnv4**	**bgp-vpnv6**	**all-afs**} {**per-ce**} 例： `Device(config)# mpls label mode all-vrfs protocol bgp-vpnv6 per-ce`	CE ラベル単位での MPLS VPN 機能の設定
ステップ 4	**end** 例： `Device(config)# end`	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。

	コマンドまたはアクション	目的
ステップ 5	**show ip vrf detail** 例： `Device# show ip vrf detail`	VRF ラベル モードを表示します。
ステップ 6	**show mpls forwarding-table** 例： `Device# show mpls forwarding-table`	マルチプロトコル ラベル スイッチング（MPLS）ラベル転送情報ベース（LFIB）の内容が表示されます。

CE ラベル単位での MPLS VPN の設定例

例：CE ラベル単位での MPLS VPN

```
Device> enable
Device# configure terminal
Device(config)# mpls label mode all-vrfs protocol bgp-vpnv6 per-ce
Device(config)# end
```

CE ラベル単位の設定に関する情報を表示するには、**show** コマンドを使用できます。

次に、定義されている VPN ルーティングおよび転送（VRF）インスタンスと関連付けられているインターフェイスを表示する例を示します。

```
PE1# show ip vrf detail

VRF red (VRF Id = 1); default RD 1:1; default VPNID <not set="">
  New CLI format, supports multiple address-families
  Flags: 0x180C
  Interfaces:
    Et1/0                    Et2/0
VRF Table ID = 1
  Flags: 0x0
  Export VPN route-target communities
    RT:1:1
  Import VPN route-target communities
    RT:1:1
  No import route-map
  No global export route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-ce
```

次に、MPLS ラベル転送情報ベース（LFIB）の内容を表示する例を示します。

```
PE1# show mpls forwarding-table

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         Pop Label  1.1.1.1/32       0             Et0/0      10.0.0.1
18         No Label   nh-id(1)         0             Et2/0      10.0.2.2
```

```
19          No Label   nh-id(2)          0              Et1/0      10.0.1.2
20          No Label   nh-id(3)          0              Et1/0      10.0.1.2
22          No Label   nh-id(5)          0              Et1/0      10.0.1.2
            No Label   nh-id(5)          0              Et2/0      10.0.2.2
```

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 Command List, All Releases』
MPLS コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』

標準および RFC

標準/RFC	Title
RFC 2547	『*BGP/MPLS*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。	http://www.cisco.com/cisco/web/support/index.html

CE ラベル単位での MPLS VPN 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 に移動します。Cisco.com のアカウントは必要ありません。

表 *11*：*CE* ラベル単位での *MPLS VPN* の機能情報

機能名	リリース	機能情報
CE ラベル単位での MPLS VPN		CE ラベル単位での MPLS VPN 機能により、プロバイダーエッジで（PE）即時ネクスト ホップまたは一連のネクスト ホップに対して単一 VPN ラベルを設定できます。 次のコマンドが導入または変更されました：**show mpls forwarding-table**、**mpls label mode**

第 13 章

VRF 認識システム メッセージ ロギング

VRF 認識システム メッセージのロギング（Syslog）機能は、デバイスがバーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）インターフェイスを介して接続されている syslog サーバ ホストにシステム ロギング（syslog）メッセージを送信できるようにします。

ロギング情報は、ネットワークのモニタリングとトラブルシューティングに使用できます。本機能は、VRF を通じて接続されたネットワーク トラフィックにこの機能を拡張します。

- 機能情報の確認，219 ページ
- VRF 認識システム メッセージ ロギングの前提条件，220 ページ
- VRF 認識システム メッセージ ロギングの制約事項，220 ページ
- VRF 認識システム メッセージ ロギングに関する情報，220 ページ
- VRF 認識システム メッセージ ロギングの設定および確認方法，223 ページ
- VRF 認識システム メッセージ ロギングの設定例，231 ページ
- その他の参考資料，232 ページ
- VRF 認識システム メッセージ ロギングの機能情報，232 ページ
- 用語集，234 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 に移動します。Cisco.com のアカウントは必要ありません。

VRF 認識システム メッセージ ロギングの前提条件

バーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）認識システム メッセージロギング機能を設定する前に、ルーティングデバイスでVRFインスタンスを設定し、VRF をインターフェイスに関連付ける必要があります。

VRF 認識システム メッセージ ロギングの制約事項

Virtual Routing and Forwarding（VRF）システム ロギング メッセージの送信元アドレスを指定することはできません。VRF 認識システム メッセージ ロギング機能は、すべての VRF 認識システム ロギング メッセージの発信元アドレスとして VRF インターフェイス アドレスを使用します。

VRF 認識システム メッセージ ロギングに関する情報

VRF 認識システム メッセージ ロギングの利点

バーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）インスタンスは、IP ルーティングの拡張機能で、複数のルーティング インスタンスを提供します。VRFは、各 VPN に個別の IP ルーティングおよび転送テーブルを提供します。VRF 認識システム メッセージ ロギング機能を設定する前に、ルーティング デバイスで VRF を設定する必要があります。

ルーティング デバイスで VRF 認識システム メッセージ ロギング機能を設定した後、デバイスは VRF インターフェイスを通じて syslog ホストに syslog メッセージを送信できます。その後、ロギング メッセージを使用して、VRF で接続されたネットワーク トラフィックの監視とトラブルシューティングを行うことができます。VRF 認識システム メッセージ ロギング機能がルーティング デバイスで設定されていない場合、この利点は得られません。ルーティング デバイスは、グローバル ルーティング テーブルのみを通じて syslog ホストに syslog メッセージを送信します。

VRF を設定できる以下の任意のデバイス上で、VRF インターフェイスを通じてシステム ロギング メッセージを受信できます。

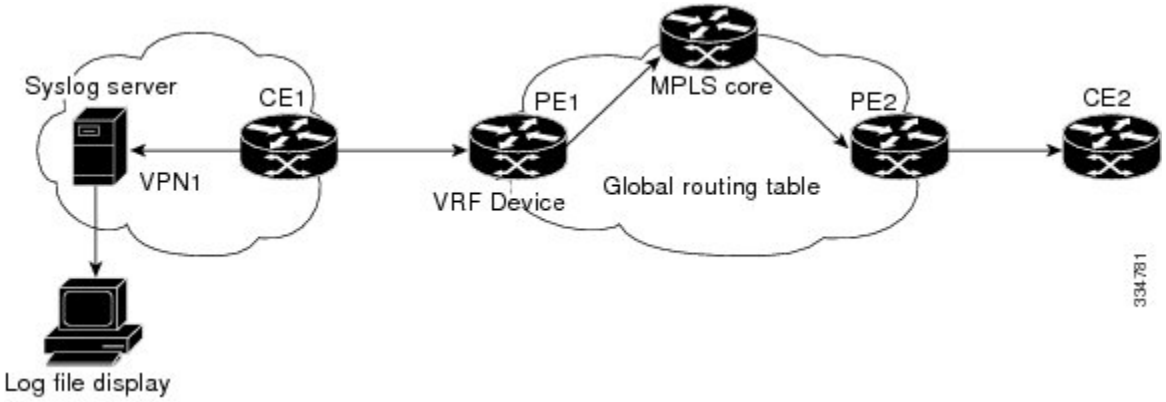
- レイヤ 3 MPLS VPN ネットワーク サービスを提供するために、マルチプロトコル ラベル スイッチング（MPLS）およびマルチプロトコル ボーダー ゲートウェイ プロトコル（BGP）と共に使用されているプロバイダー エッジ（PE）デバイス。
- マルチプロトコル BGP を使用しない VRF 実装である VRF-Lite 用に設定されたカスタマー エッジ（CE）デバイス。

MPLS VPN ネットワーク内のプロバイダー エッジ デバイス上の VRF 認識システム メッセージ ロギング

レイヤ 3 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）ネットワーク内のプロバイダー エッジ（PE）デバイスで、VRF 認識システム メッセージ ロギング機能を設定できます。PE デバイスは、Virtual Routing and Forwarding（VRF）インターフェイスを通じて、VPN 内にある 1 台の syslog サーバに、syslog メッセージを送信できます。

次の図は、MPLS VPN ネットワークと、VRF VPN1 に関連付けられている PE デバイスで設定されている VRF 認識システム メッセージ ロギング機能を示します。PE デバイスは、VRF インターフェイスを通じて、VPN1 にある syslog サーバにログ メッセージを送信します。端末上で syslog サーバからのメッセージを表示できます。

図 *13*：*MPLS VPN* と、カスタマー エッジ デバイス上で設定された *VRF* 認識システム メッセージ ロギング



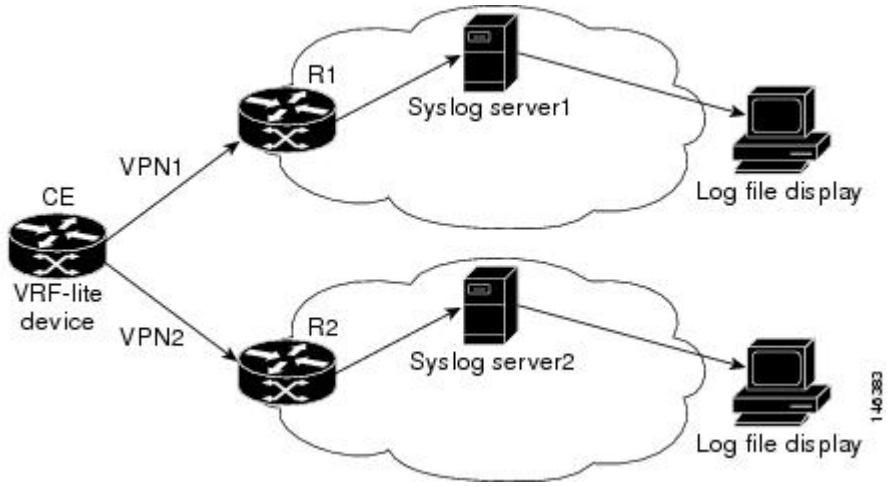
VRF-Lite が設定されたカスタマー エッジ デバイスでの VRF 認識システム メッセージ ロギング

VRF-Lite 機能が設定されたカスタマー エッジ（CE）デバイスで、VRF 認識システム メッセージ ロギング機能を設定できます。CE デバイスは、Virtual Routing and Forwarding（VRF）インターフェイスを通じて、複数の n バーチャル プライベート ネットワーク（VPN）の syslog サーバに、syslog メッセージを送信できます。CE デバイスは、ルータまたはスイッチのいずれかです。

次の図は、VRF-Lite CE デバイス上で設定された VRF 認識システム メッセージ ロギング機能を示します。CE デバイスは、VPN1 または VPN2 内の syslog サーバか、VPN1 と VPN2 の両方のサー

バに VRF syslog メッセージを送信できます。1 台の VRF-Lite CE デバイスで複数の VRF を設定でき、デバイスは多数の顧客にサービスを提供できます。

図 *14*：*VRF-Lite* カスタマー エッジ デバイス上で設定された *VRF* システム メッセージ ロギング



ロギング コマンドのメッセージ レベル

VRF 認識システム メッセージ ロギング機能を設定するときに使用できる **logging** コマンドのメッセージ レベルの一覧を次の表に示します。この表に記載されている情報には、キーワード レベル名と番号、その説明、関連付けられている syslog 定義が含まれています。**logging trap***level* および **logging buffered***severity-level* コマンドでは、レベル キーワード名またはレベル番号のいずれかを使用できます。

表 *12*：*logging* コマンドのメッセージ レベル

重大度の名前	レベル番号	説明	syslog 定義
emergencies	**0**	システムが使用不可	LOG_EMERG
alerts	**1**	即時処理が必要	LOG_ALERT
critical	**2**	クリティカルな状態	LOG_CRIT
errors	**3**	エラー状態	LOG_ERR
warnings	**4**	警告状態	LOG_WARNING
通知	**5**	正常だが注意を要する状態	LOG_NOTICE
informational	**6**	情報メッセージだけ	LOG_INFO

重大度の名前	レベル番号	説明	syslog 定義
debugging	7	デバッグ メッセージ	LOG_DEBUG

VRF 認識システム メッセージ ロギングの設定および確認方法

ルーティング デバイスでの VRF の設定

ルーティング デバイスで Virtual Routing and Forwarding（VRF）インスタンスを設定すると、カスタマーがバーチャル プライベート ネットワーク（VPN）に接続できます。ルーティング デバイスとして、マルチプロトコル ラベル スイッチング（MPLS）VPN ネットワークに接続するプロバイダー エッジ（PE）、または VRF-Lite に対応して設定されているカスタマー エッジ（CE）デバイスを使用できます。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **ip vrf***vrf-name*
4. **rd***route-distinguisher*
5. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**ip vrf***vrf-name* 例： `Device(config)# ip vrf vpn1`	VRF インスタンスを定義し、VRF コンフィギュレーション モードを開始します。 • *vrf-name* 引数は、VRF に割り当てられている名前です。

ステップ 4	**rd***route-distinguisher*
	
	例：
	
	`Device(config-vrf)# rd 100:1`
		VRF のルーティング テーブルと転送テーブルを作成します。
		
		• *route-distinguisher* 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、自律システム番号と任意の番号で構成される自律システム番号（ASN）相対 RD、または IP アドレスと任意の番号で構成される IP アドレス相対 RD のいずれかです。
		• 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：10.0.0.1:1 などの 16 ビット数値

ステップ 5	**route-target** {**import** | **export** | **both**} *route-target-ext-community* 例： `Device(config-vrf)# route-target both 100:1`	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。 • **import** 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。 • **export** 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。 • **both** 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。 • *route-target-ext-community* 引数により、route-target 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 route-target 拡張コミュニティの VRF リストに追加されます。 ルート ターゲットはターゲット VPN 拡張コミュニティを指定します。拡張コミュニティはルート識別子と同様に、自律システム番号と任意の数字、または IP アドレスと任意の数字で構成されます。番号は、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：101:3 などの 32 ビット数値 • 32 ビット IP アドレス：10.0.0.2.15: 1 などの 16 ビット数値

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config-vrf)# end`	特権 EXEC モードに戻ります。

VRF とインターフェイスの関連付け

Virtual Routing and Forwarding（VRF）インスタンスをインターフェイスに関連付けるには、次の手順を実行します。バーチャル プライベート ネットワーク（VPN）トラフィックを転送する前に、VRF がインターフェイスに関連付けられている必要があります。

（注） VRF システム ロギング メッセージの発信元アドレスは設定できません。VRF 認識システム メッセージ ロギング機能は、すべての VRF 認識システム ロギング メッセージの発信元アドレスとして VRF インターフェイス アドレスを使用します。

VRF を設定しインターフェイスに関連付けたら、ルーティング デバイス上で VRF 認識システム メッセージ ロギング機能を設定できます。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***typenumber*
4. **ip vrf forwarding***vrf-name*
5. **end**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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	**configure terminal** 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	**interface***typenumber* 例： `Device(config)# interface FastEthernet 0/0/0`	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。 • *type* 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。 • *number* 引数で、ポート、コネクタ、またはインターフェイスカードの番号を指定します。この番号は、インストール時に工場で割り当てられるか、またはポート、コネクタやインターフェイス カードをシステムに追加するときに割り当てられます。番号は、**show interfaces** コマンドで表示できます。
ステップ 4	**ip vrf forwarding***vrf-name* 例： `Device(config-if)# ip vrf forwarding vpn1`	VRF をインターフェイスまたはサブインターフェイスと関連付けます。 • *vrf-name* 引数は、インターフェイスを指定された VRF に関連付けます。
ステップ 5	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 6	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーションの変更を NVRAM に保存します。

ルーティング デバイスでの VRF 認識システム メッセージ ロギングの設定

VRFインスタンスを介して接続されている状態でネットワーク トラフィックをモニタおよびトラブルシューティングするためにロギング メッセージを使用できるように、ルーティングデバイスで VRF 認識システム メッセージ ロギング機能を設定します。

はじめる前に

この作業を実行するには、次に示す作業を実行しておく必要があります。

- ルーティング デバイスで Virtual Routing and Forwarding（VRF）インスタンスを設定します。
- インターフェイスと VRF を関連付けます。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **logging host** {*ip-address* | *hostname*} [**vrf***vrf-name*]
4. **logging trap***level*
5. **logging facility***facility-type*
6. **logging buffered** [*buffer-size* | *severity-level*]
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**logging host** {*ip-address* | *hostname*} [**vrf***vrf-name*]	syslog メッセージを受信するホストを指定します。 • *ip-address* 引数は、syslog サーバ ホストの IP アドレスです。

	コマンドまたはアクション	目的
	例： `Device(config)# logging host 10.0.150.63 vrf vpn1`	• *hostname* 引数は、syslog メッセージを受信する IP または IPv6 ホストの名前です。 • **vrf***vrf-name* キーワードと引数は、syslog サーバ ホストに接続する VRF を指定します。
ステップ 4	**logging trap***level* 例： `Device(config)# logging trap debugging`	syslog サーバに記録されるメッセージを重大度に基づいて制限します。 • *level* 引数は、指定したレベルに syslog サーバへのメッセージのロギングを制限します。レベル番号またはレベル名を入力できます。使用可能なキーワードの説明については、「ロギング コマンドのメッセージ レベル」を参照してください。
ステップ 5	**logging facility***facility-type* 例： `Device(config)# logging facility local6`	（任意）エラー メッセージが送信される syslog ファシリティを設定します。 • *facility-type* 引数は、syslog ファシリティ タイプ キーワードを指定します。ローカルに定義されているメッセージの場合、使用可能なキーワードの範囲は local0 ～ local7 です。デフォルトは **local7** です。
ステップ 6	**logging buffered** [*buffer-size* | *severity-level*] 例： `Device(config)# logging buffered debugging`	（任意）デバイスの内部バッファに記録されるメッセージを、重大度に基づいて制限します。 • *buffer-size* 引数は、4096 ～ 4,294,967,295 バイトのバッファ サイズです。デフォルトのサイズは、プラットフォームによって異なります。 • *severity-level* 引数は、バッファへのメッセージの記録を、指定したレベルに制限します。レベル名またはレベル番号を入力できます。使用可能なキーワードのリストについては、「ロギング コマンドのメッセージ レベル」を参照してください。デフォルトのロギング レベルはプラットフォームによって異なりますが、一般には 7 です。このレベルでは、すべてのレベル（0 ～ 7）のメッセージがバッファに記録されます。
ステップ 7	**end** 例： `Device(config)# end`	（任意）特権 EXEC モードに戻ります。

VRF 認識システム メッセージ ロギング操作の確認

手順の概要

1. イネーブル化
2. **show running-config | include logging**
3. **show ip vrf interfaces**
4. **show running-config** [**interface***typenumber*]
5. **ping vrf***vrf-nametarget-ip-address*
6. **exit**

手順の詳細

ステップ 1 イネーブル化

特権 EXEC モードをイネーブルにします。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 running-config | include logging**

Virtual Routing and Forwarding（VRF）インスタンスのロギング ホストとデバイスのロギング設定を表示します。

例：

```
Device# show running-config | include logging

logging queue-limit 100
logging buffered 100000 debugging
mpls ldp logging neighbor-changes
logging trap debugging
logging facility local6
logging host vrf vpn1 10.0.0.3
Device#
```

この例は、サーバ ホスト アドレス 10.0.0.3 を使用した VRF vpn1 の syslog サーバの設定を示しています。

ステップ 3 **show ip vrf interfaces**

syslog サーバ ホストにリンクしている VRF に関連付けられているインターフェイスを表示します。次の例は、VRF インターフェイスと、デバイスで設定されている関連 IP アドレスのリストを表示します。

例：

```
Device# show ip vrf interfaces

Interface              IP-Address       VRF                              Protocol
```

```
FastEthernet0/0/0      10.0.0.0         vpn1                            up
Loopback1              10.0.0.6         vpn1                            up
```

ステップ 4 **show running-config** [**interface***typenumber*]

VRF に関連付けられているインターフェイスの、インターフェイス固有の設定情報を表示します。

例：

```
Device# show running-config interface FastEthernet 0/0/0

Building configuration...
Device#
.
.
.
!
Current configuration : 116 bytes
!
interface FastEthernet0/0/0
 ip vrf forwarding vpn1
 ip address 10.0.0.98 255.0.0.0
 duplex half
 no cdp enable
end
```

この例は、VRF vpn1 の Fast Ethernet インターフェイス 0/0/0 の設定情報を表示します。

ステップ 5 **ping vrf***vrf-nametarget-ip-address*

指定された VRF から syslog サーバ ホスト（*target-ip-address*）に到達できることを確認します。

例：

```
Device# ping vrf vpn1 10.3.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.0.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

この例では、syslog サーバの IP アドレスが 10.3.0.1 であり、VRF が vpn1 です。サーバは 5 回のうち 4 回正常に到達できました。

ステップ 6 **exit**

特権 EXEC モードに戻ります。

例：

```
Device# exit
Device>
```

VRF 認識システム メッセージ ロギングの設定例

例：ルーティング デバイスでの VRF の設定

```
enable
configure terminal
!
ip vrf vpn1
 rd 100:1
 route-target both 100:1
 end
```

例：VRF とインターフェイスの関連付け

```
enable
configure terminal
!
interface FastEthernet 0/0/0
 ip vrf forwarding vpn1
 end
```

例：ルーティング デバイスでの VRF 認識システム メッセージ ロギングの設定

次に、ルーティング デバイスで VRF 認識システム メッセージ ロギング機能を設定する例を示します。syslog サーバ ホストの IP アドレスは 10.0.1.3、VRF は vpn1 です。

```
enable
configure terminal
!
 logging host 10.0.1.3 vrf vpn1
 logging trap debugging
 logging facility local6
 logging buffered 10000
 logging buffered debugging
 end
```

次に、syslog サーバのロギングをオフにする例を示します。

```
enable
configure terminal
!
 no logging 10.0.1.3
 end
```

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 Master Command List, All Releases』
MPLS と MPLS アプリケーション コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』
Catalyst 4500 スイッチでの VRF-Lite 設定の概念とタスク	『*Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*』の「Configuring VRF-lite」の章
ML シリーズ イーサネット カードでの VRF Lite 設定の概念とタスク	『*Ethernet Card Software Feature and Configuration Guide*』の「Configuring VRF-lite」の章（Cisco ONS 15454 SDH、ONS 15454、および ONS 15327）

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。	http://www.cisco.com/cisco/web/support/index.html

VRF 認識システム メッセージ ロギングの機能情報

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。

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 に移動します。Cisco.com のアカウントは必要ありません。

表 *13*：*VRF* 認識システム メッセージ ロギングの機能情報

機能名	リリース	機能情報
VRF 認識システム メッセージ ロギング	12.2(31)SB2 12.2(33)SRA 12.2(33)SXH 12.4(13) 15.1(1)SG Cisco IOS XE Release 2.2 Cisco IOS XE Release 3.3SG	VRF 認識システム メッセージ ロギング機能により、デバイスが VPN VRF インターフェイスを介して接続している syslog サーバ ホストにメッセージを送信できます。 Cisco IOS Release 12.2(31)SB2 では、この機能が Cisco 10000 シリーズ ルータに追加されました。 この機能は、Cisco IOS Release 12.2(33)SRA で統合されました。 Cisco IOS Release 12.2(33)SXH では、この機能が統合されました。 この機能は、 Cisco IOS Release 12.4(13) で統合されました。 この機能は、Cisco IOS Release 15.1(1)SG で統合されました。 Cisco IOS XE Release 2.2 では、この機能は Cisco ASR 1000 シリーズ アグリゲーション サービスルータに実装されました。 この機能は、Cisco IOS XE Release 3.3SG で統合されました。 **logging host** コマンドが変更されました。

用語集

CE デバイス：カスタマーエッジデバイス。VPN プロバイダーと VPN カスタマーの境界にあり、カスタマーに属するデバイス。

LSR：Label Switching Router（ラベル スイッチング ルータ）。各パケット内にカプセル化されている固定長ラベルの値に基づいて MPLS パケットを転送するデバイス。

MPLS：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。ネットワークを介してパケット（フレーム）を転送する方式。ネットワークのエッジにあるデバイスがラベルをパケット（フレーム）に適用できるようにします。ネットワーク コア内の ATM スイッチまたは既存のデバイスは、最小限のルックアップ オーバーヘッドでラベルに従ってパケットを切り替えることができます。

MPLS VPN：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）Virtual Private Network（バーチャル プライベート ネットワーク）。レイヤ 3 バックボーンを使用して、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 ネットワーク インフラストラクチャ。シスコ ネットワークで MPLS VPN を使用すると、スケーラブルなレイヤ 3 VPN バックボーン サービス（アプリケーション、データ ホスティング ネットワーク コマース、テレフォニー サービスなど）を展開および管理する機能をビジネス上のカスタマーに提供できます。

PE デバイス：プロバイダー エッジ デバイス。VPN プロバイダーと VPN カスタマーの境界にあり、プロバイダーに属するデバイス。

VPN：Virtual Private Network（バーチャル プライベート ネットワーク）。管理ポリシー セットにより、共有バックボーン ネットワーク上で相互に通信可能なサイトのグループ。VPN は、1 つまたは複数の物理ネットワークでリソースを共有するセキュアな IP ベースのネットワークです。VPN には、共有のバックボーンで安全に通信できる地理的に分散したサイトが含まれます。「MPLS VPN」も参照してください。

VRF：VPN ルーティングおよび転送インスタンス。VRF は、IP ルーティング テーブル、取得されたルーティング テーブル、そのルーティング テーブルを使用する一連のインターフェイス、ルーティングテーブルに登録されるものを決定する一連のルールおよびルーティングプロトコルで構成されています。一般に、VRF には、PE デバイスに付加される顧客 VPN サイトが定義されたルーティング情報が格納されています。

第 14 章

MPLS VPN の実行中の VRF の表示

MPLS VPN の実行中の VRF の表示機能を使用すると、Cisco IOS CLI オプションで、バーチャル プライベート ネットワーク（VPN）ルーティングおよび転送（VRF）インスタンスに関連する、デバイスの実行コンフィギュレーションの一部を表示できます。特定の VRF、またはデバイスに設定されているすべての VRF の設定を表示できます。

高い負荷がかかっているデバイスでは、コンフィギュレーション ファイルを表示するのに複数のページまたは画面が必要となる場合があります。設定のサイズが大きくなり設定が複雑になると、設定ミスをする可能性も高くなります。デバイスに複数の VRF が設定されていると、問題の追跡が難しくなる場合があります。VRF に関連する設定要素をすべて表示するコマンドを使用すると、VRF 単位でのトラブルシューティングが容易になり、同一デバイス上の異なる VRF の設定同士を比較しやすくなります。

MPLS VPN の実行中の VRF の表示機能の設定作業はありません。

- 機能情報の確認，235 ページ
- MPLS VPN の実行中の VRF の表示の前提条件，236 ページ
- MPLS VPN の実行中の VRF の表示の制約事項，236 ページ
- MPLS VPN の実行中の VRF の表示に関する情報，236 ページ
- その他の参考資料，238 ページ
- MPLS VPN の実行中の VRF の表示の機能情報，239 ページ
- 用語集，241 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 に移動します。Cisco.com のアカウントは必要ありません。

MPLS VPN の実行中の VRF の表示の前提条件

- デバイスにインストールされた、Virtual Routing and Forwarding（VRF）インスタンスをサポートするシスコ ソフトウェア イメージ
- デバイス上に設定された少なくとも 1 つの VRF
- 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）ルーティングおよび転送用の Cisco Express Forwarding

MPLS VPN の実行中の VRF の表示の制約事項

Virtual Routing and Forwarding（VRF）インスタンスに直接リンクされていない、デバイスの実行コンフィギュレーションのすべての要素は表示されません。たとえば、VRF アドレス ファミリ コンフィギュレーション内のボーダー ゲートウェイ プロトコル（BGP）ネイバーに関連付けられたルート マップは表示されません。BGP の VRF アドレス ファミリ コンフィギュレーションは表示されますが、ルートマップ コンフィギュレーションは表示されません。これは一般的な規則ですが、コントローラ設定の表示は例外となります。

MPLS VPN の実行中の VRF の表示に関する情報

MPLS VPN の実行中の VRF の表示で表示される設定要素

show running-config vrf コマンドを入力して、デバイス上の特定の Virtual Routing and Forwarding（VRF）インスタンスまたはすべての VRF に関連付けられている実行コンフィギュレーションを表示できます。特定の VRF の実行コンフィギュレーションを表示するには、VRF の名前を **show running-config vrf** コマンドの引数として使用します。たとえば、vpn3 という名前の VRF の場合、次のように入力します。

```
Device# show running-config vrf vpn3
```

show running-config vrf コマンドで表示されるデバイスの実行コンフィギュレーションの要素は、次のとおりです。

- VRF の設定（VRF サブモードに適用されるすべての設定が含まれます）
- VRF 内にあるインターフェイスごとの設定

show run vrf*vpn-name* コマンドを実行することは、**show running-config interface***type number* を、**show ip vrf***vpn-name* コマンドを使用して表示された各インターフェイスに対して実行するのと同

じです。インターフェイスは、**show ip interface** コマンドを実行したときの表示順序と同じ順序にソートされて表示されます。

チャネライズド インターフェイスの場合は、コントローラの設定が表示されます（**show run controller***controller-name* コマンドによる表示と同様）。

サブインターフェイスの場合は、メインインターフェイスの設定が表示されます。

VRF ルーティング プロトコル設定の表示

Open Shortest Path First（OSPF）、Routing Information Protocol（RIP）、Border Gateway Protocol（BGP）、Enhanced Interior Gateway Routing Protocol（EIGRP）、およびスタティック ルーティングは、Virtual Routing and Forwarding（VRF）設定をサポートするルーティング プロトコルです。

OSPF では、VRF ごとに 1 つのプロセスを使用します。**show running-config vrf** コマンドを実行すると、VRF に関連付けられた OSPF プロセスのすべての設定が表示されます。たとえば、次に OSPF プロセス 101 の出力例を示します。このプロセスは vpn3 という名前の VRF に関連付けられています。

```
router ospf 101 vrf vpn3
 log-adjacency-changes
 area 1 sham-link 10.43.43.43 10.23.23.23 cost 10
 network 172.17.0.0 0.255.255.255 area 1
```

RIP、BGP、および EIGRP は、VRF アドレス ファミリ コンフィギュレーションをサポートします。これらのルーティング プロトコルのいずれかの VRF に VRF アドレス ファミリが存在する場合は、次の形式の設定が表示されます。

```
router
protocol
 {AS
 | PID
}
!
address-family ipv4 vrf
 vrf-name
.
.
.
```

このとき、*protocol* 引数は **rip**、**bgp**、または **eigrp** のいずれかです。*AS* 引数は自律システム番号、PID 引数はプロセス ID です。*vrf-name* 引数は関連付けられた VRF の名前です。

次に、vpn3 という名前の VRF に関連付けられた、自律システム番号 100 の BGP の出力例を示します。

```
!
router bgp 100
!
address-family ipv4 vrf vpn3
 redistribute connected
 redistribute ospf 101 match external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
 !
```

show running-config vrf コマンドでは、VRF で設定されているスタティック ルートの設定も表示されます。次に例を示します。

```
ip route vrf vpn1 10.1.1.0 255.255.255.0 10.30.1.1 global
ip route vrf vpn1 10.1.2.0 255.255.255.0 10.125.1.2
```

VRF に直接関連していない設定の表示

Virtual Routing and Forwarding（VRF）インスタンスに直接リンクされていない設定のすべての要素は表示されません。場合によっては、VRF に直接リンクされていない要素の設定を表示する必要があります。

たとえば、**show running-config vrf** コマンドを実行すると、VRF にシリアル サブインターフェイスが含まれている E1 コントローラの設定が表示されます。このコマンドは、コントローラ設定およびサブインターフェイス コンフィギュレーションを表示します。

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 Master Command List, All Releases』
MPLS と MPLS アプリケーション 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	Link
★枠で囲まれた Technical Assistance の場合★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。	http://www.cisco.com/cisco/web/support/index.html

MPLS VPN の実行中の VRF の表示の機能情報

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 に移動します。Cisco.com のアカウントは必要ありません。

表 *14*：*MPLS VPN* の実行中の *VRF* の表示の機能情報

機能名	リリース	機能情報
MPLS VPN の実行中の VRF の表示	12.2(28)SB 12.0(32)SY 12.2(33)SRB 12.2(33)SXH 12.4(20)T Cisco IOS XE Release 2.5	MPLS VPN の実行中の VRF の表示機能は、VRF にリンクされているデバイスの実行コンフィギュレーションのサブセットを表示する CLI オプションを提供します。特定の VRF、またはデバイスに設定されているすべての VRF の設定を表示できます。VRF に関連する設定要素をすべて表示するコマンドを使用すると、VRF 単位でのトラブルシューティングが容易になり、同一デバイス上の異なる VRF の設定同士を比較しやすくなります。 12.2(28)SB では、この機能が導入されました。 12.0(32)SY では、Cisco IOS 12.0SY リリースのサポートが追加されました。 12.2(33)SRB では、Cisco IOS 12.2SR リリースのサポートが追加されました。 122(33)SXH では、Cisco IOS 12.2SX リリースのサポートが追加されました。 12.4(20)T では、Cisco IOS 12.4T リリースのサポートが追加されました。 Cisco IOS XE Release 2.5S では、Cisco ASR 1000 シリーズルータのサポートが追加されました。
		次のコマンドが導入または変更されました：**show policy-map interface brief**、**show running-config vrf**。

用語集

BGP：Border Gateway Protocol（ボーダー ゲートウェイ プロトコル）。外部ゲートウェイ プロトコル（EGP）の代わりに使用されるドメイン間ルーティング プロトコル。BGP システムは、他の BGP システムと到達可能性情報を交換します。RFC 1163 によって定義されています。

EGP：External Gateway Protocol（外部ゲートウェイ プロトコル）。自律システム間でルーティング情報を交換するためのインターネット プロトコル。EGP は RFC 904 に記載されています。一般用語の外部ゲートウェイ プロトコルと混同しないでください。EGP は、ボーダー ゲートウェイ プロトコル（BGP）に置き換えられた旧式のプロトコルです。

EIGRP：Enhanced Interior Gateway Routing Protocol。シスコが開発した Interior Gateway Routing Protocol（IGRP）を改良したバージョン。優れたコンバージェンス特性と動作効率を示し、リンクステート型プロトコルと距離ベクトル型プロトコルのメリットを兼ね備えています。

IGP：Interior Gateway Protocol（内部ゲートウェイ プロトコル）。自律システム内でルーティング情報の交換に使用するインターネット プロトコル。一般的なインターネット IGP の例としては、Interior Gateway Routing Protocol（IGRP）、Open Shortest Path First（OSPF）、および Routing Information Protocol（RIP）があります。

IGRP：Interior Gateway Routing Protocol。大規模な異機種ネットワークのルーティングに関する問題を解決するためにシスコが開発した Interior Gateway Protocol（IGP）。

MPLS：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。ラベルを使用して IP トラフィックを転送するスイッチング方式。このラベルによって、ネットワーク内のデバイスおよびスイッチが、事前に確立された IP ルーティング情報に基づく各パケットの転送先を指示されます。

OSPF：Open Shortest Path First。インターネット コミュニティの Routing Information Protocol（RIP）の後継アルゴリズムとして提案された、リンクステートの階層型 Interior Gateway Protocol（IGP）ルーティング アルゴリズムおよびルーティング プロトコル。OSPF 機能には、最小コストによるルーティング、マルチパスのルーティング、およびロードバランシングが含まれます。OSPF は、Intermediate System-to-Intermediate System（IS-IS）プロトコルの初期バージョンから派生したものです。

RIP：Routing Information Protocol。UNIX Berkeley Software Distribution（BSD）システムに付属する内部ゲートウェイ プロトコル（IGP）。RIP は、インターネットで最も広く使用されている IGP です。ルーティング メトリックとしてはホップ カウントを使用します。

VPN：Virtual Private Network（バーチャル プライベート ネットワーク）。トンネリングを使用し、公衆 TCP/IP ネットワークを通じて IP トラフィックを安全に転送することを可能にするデバイス構成。

第 15 章

MPLS VPN 半二重 VRF

MPLS VPN 半二重 VRF 機能では、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）サービスの加入者に対してスケーラブルなハブアンドスポーク接続が提供されます。この機能を使用すると、スポークごとに 1 つの Virtual Routing and Forwarding（VRF）インスタンスという要件をなくすことで、ハブアンドスポーク トポロジの制限に対処します。またこの機能は、加入者トラフィックが、アップストリーム ISP 経由でリモート ネットワークにルーティングされるか、別のローカルまたはリモートで接続されたサブスクライバにルーティングされるかにかかわらず、加入者トラフィックが常にホールセール サービス プロバイダーとインターネット サービス プロバイダー（ISP）の間の中央リンクを通過するようにします。

- 機能情報の確認，243 ページ
- MPLS VPN 半二重 VRF の前提条件，244 ページ
- MPLS VPN 半二重 VRF の制約事項，244 ページ
- MPLS VPN 半二重 VRF に関する情報，244 ページ
- MPLS VPN 半二重 VRF の設定方法，246 ページ
- MPLS VPN 半二重 VRF の設定例，254 ページ
- その他の参考資料，259 ページ
- MPLS VPN 半二重 VRF の機能情報，260 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 に移動します。Cisco.com のアカウントは必要ありません。

MPLS VPN 半二重 VRF の前提条件

マルチプロトコル ラベル スイッチング（MPLS）コア ネットワークが機能している必要があります。

MPLS VPN 半二重 VRF の制約事項

次の機能は、MPLS VPN 半二重 VRF 機能が設定されたインターフェイスではサポートされていません。

- マルチキャスト
- MPLS VPN Carrier Supporting Carrier
- MPLS VPN 相互自律システム

MPLS VPN 半二重 VRF に関する情報

MPLS VPN 半二重 VRF 概要

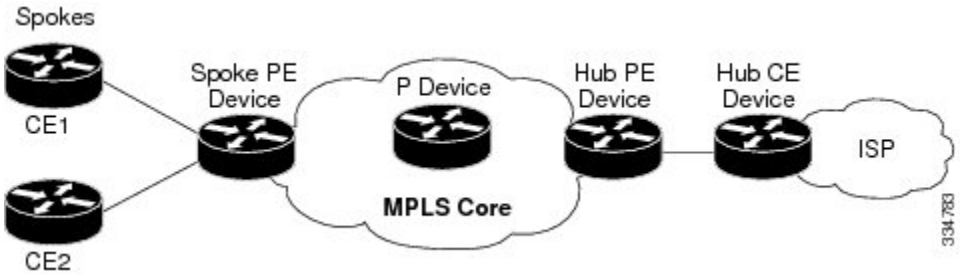
MPLS VPN 半二重 VRF 機能には、次の利点があります。

- MPLS VPN 半二重 VRF 機能は、スポーク プロバイダー エッジ（PE）デバイスでの加入者間のローカル接続を禁止し、加入者がハブ サイトに常に接続されるようにします。同じ PE デバイスに接続しているすべてのサイトは、ハブ サイトを使用して、サイト間のトラフィックを転送する必要があります。これにより、スポーク サイトでのルーティングは、常にアクセス側インターフェイスからネットワーク側インターフェイスに対して、またはネットワーク側インターフェイスからアクセス側インターフェイスに対して実行されます。アクセス側インターフェイスからアクセス側インターフェイスへのルーティングは発生しません。
- MPLS VPN 半二重 VRF 機能は、PE デバイスにおいて、トラフィックをアップストリーム インターネット サービス プロバイダー（ISP）に渡さずにスポーク間のスイッチングをローカルで行うことを禁止します。これにより、加入者は直接相互に接続できなくなり、ホールセール サービス プロバイダーの収益が損なわれることがなくなります。
- MPLS VPN 半二重 VRF 機能では、スポークごとに 1 つの Virtual Routing and Forwarding（VRF）という要件がなくなるため、スケーラビリティが向上します。この機能が設定されていない場合、スポークが同じ PE デバイスに接続されると、スポーク間のトラフィックがホールセール サービス プロバイダーと ISP 間の中央リンクを通過するように、各スポークは異なる VRF

に設定されます。ただし、この設定には拡張性がありません。多数のスポークが同じ PE デバイスに接続されている場合、スポークごとに 1 つの VRF を設定すると、作業が非常に複雑になったり、メモリ使用量が大幅に増加したりします。この状況は、特に、レイヤ 3 バーチャル プライベート ネットワーク（VPN）への高密度リモート アクセスをサポートする大規模ホールセール サービス プロバイダー環境で発生します。

次の図に、サンプル ハブアンドスポーク トポロジを示します。

図 *15*：ハブアンドスポーク トポロジ



アップストリーム VRF とダウンストリーム VRF

MPLS VPN 半二重 VRF 機能では、スポークとハブ PE デバイスとの間で IP トラフィックを転送するために、2 つの単一方向 Virtual Routing and Forwarding（VRF）インスタンスが使用されます。

- アップストリーム VRF は、スポークからハブ プロバイダー エッジ（PE）デバイスに IP トラフィックを転送します。この VRF には、通常、1 つのデフォルト ルートだけが含まれていますが、サマリー ルートや複数のデフォルト ルートが含まれる場合もあります。デフォルト ルートは、アップストリーム インターネット サービス プロバイダー（ISP）に接続しているハブ PE デバイスのインターフェイスをポイントします。デバイスは、ハブ PE デバイスまたはホーム ゲートウェイが送信するルーティング アップデートからデフォルト ルートの情報をダイナミックに学習します。

（注） 通常、アップストリーム VRF はハブに接続されますが、ローカル ドメイン ネーム システム（DNS）やゲーム サーバ サービスなどの、ハブを経由する必要がない別のローカル サービス用の異なるローカルアップストリームインターフェイスをスポーク PE に用意することもできます。

- ダウンストリーム VRF は、ハブ PE デバイスからのトラフィックをスポークに転送して戻します。この VRF には以下のものを含めることができます。
  - 認証、許可、アカウンティング（AAA）サーバまたは Dynamic Host Control Protocol（DHCP）から受信した、スポークの PPP ルートおよびユーザ単位のスタティック ルート

- ハブ PE デバイスからインポートされたルート
- スポークの Border Gateway Protocol（BGP）、Open Shortest Path First（OSPF）、Routing Information Protocol（RIP）、または Enhanced Interior Gateway Routing Protocol（EIGRP）の動的ルート

スポーク PE デバイスは、ダウンストリーム VRF からマルチプロトコル ボーダー ゲートウェイ プロトコル（MP-BGP）にルートを再配布します。このデバイスは、通常、接続されたスポークのマルチプロトコル ラベル スイッチング（MPLS）コアを介してサマリー ルートをアドバタイズします。ハブ PE デバイスに設定された VRF は、アドバタイズされたサマリー ルートをインポートします。

リバース パス転送チェック

Reverse Path Forwarding（RPF）チェックを行うと、IP パケットがデバイスに入るときに、正しいインバウンド インターフェイスを使用するようになります。MPLS VPN 半二重 VRF 機能は、スポーク側のインターフェイスでユニキャスト RPF チェックをサポートしています。ダウンストリームおよびアップストリーム転送にはそれぞれ異なる Virtual Routing and Forwarding（VRF）インスタンスが使用されるため、RPF メカニズムにより、ダウンストリーム VRF で送信元アドレスチェックが確実に行われます。

ユニキャスト RPF は、デフォルトではディセーブルになっています。

MPLS VPN 半二重 VRF の設定方法

スポーク PE デバイスでのアップストリーム VRF とダウンストリーム VRF の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **vrf definition***vrf-name*
4. **rd***route-distinguisher*
5. **address-family** {**ipv4** | **ipv6**}
6. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
7. **exit-address-family**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**イネーブル化** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**vrf definition***vrf-name* 例： `Device(config)# vrf definition vrf1`	Virtual Routing and Forwarding（VRF）テーブルを設定し、VRF コンフィギュレーション モードを開始します。 • *vrf-name* 引数は、VRF の名前です。

ステップ 4	**rd***route-distinguisher*
	
	例：
	
	`Device(config-vrf)# rd 100:1`
		VRF のルーティング テーブルと転送テーブルを作成します。
		
		• *route-distinguisher* 引数では、8 バイトの値を IPv4 プレフィックスに追加してバーチャル プライベート ネットワーク（VPN）IPv4 プレフィックスを作成することを指定します。ルート識別子は、次のいずれかの形式で入力できます。
		  • 16 ビット ASN：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	**address-family** {**ipv4** | **ipv6**} 例： `Device(config-vrf) address-family ipv4`	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。 • **ipv4** キーワードは、VRF の IPv4 アドレス ファミリを指定します。 • **ipv6** キーワードは、VRF の IPv6 アドレス ファミリを指定します。 （注） MPLS VPN 半二重 VRF 機能は、IPv4 アドレスだけをサポートしています。
ステップ 6	**route-target** {**import** | **export** | **both**} *route-target-ext-community*	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。 • **import** キーワードは、ターゲット VPN 拡張コミュニティからルーティング情報をインポートすることを指定します。

	コマンドまたはアクション	目的
	例： `Device(config-vrf-af)# route-target both 100:2`	• **export** キーワードは、ルーティング情報をターゲット VPN 拡張コミュニティにエクスポートすることを指定します。 • **both** キーワードは、ルーティング情報のターゲット VPN 拡張コミュニティからのインポート、およびターゲット VPN 拡張コミュニティへのエクスポートの両方が行われることを指定します。 • *route-target-ext-community* 引数により、route-target 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 route-target 拡張コミュニティの VRF リストに追加されます。
ステップ 7	**exit-address-family** 例： `Device(config-vrf-af)# exit-address-family`	VRF 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。
ステップ 8	**end** 例： `Device(config-vrf)# end`	特権 EXEC モードに戻ります。

VRF とインターフェイスの関連付け

Virtual Routing and Forwarding（VRF）インスタンスをインターフェイスに関連付けるには、次の作業を実行します。これにより VRF がアクティブになります。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***typenumber*
4. **vrf forwarding***vrf-name* [**downstream***vrf-name2*
5. **ip address***ip-addressmask* [**secondary**]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**interface***typenumber* 例： `Device(config)# interface Ethernet 0/1`	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。 • *type* 引数には、設定するインターフェイスのタイプを指定します。 • *number* 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	**vrf forwarding***vrf-name* [**downstream***vrf-name2* 例： `Device(config-if)# vrf forwarding vrf1`	VRF をインターフェイスまたはサブインターフェイスと関連付けます。 • *vrf-name* 引数は、VRF の名前です。 • **downstream***vrf-name2* キーワードと引数の組み合わせは、ピア ルートおよびユーザ単位ルートがインストールされるダウンストリーム VRF の名前です。
ステップ 5	**ip address***ip-addressmask* [**secondary**] 例： `Device(config-if)# ip address 10.24.24.24 255.255.255.255`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。 • *ip-address* 引数は、IP アドレスです。 • *mask* 引数は、関連付けられた IP サブネットのマスクです。 • **secondary** キーワードは、設定されるアドレスがセカンダリ IP アドレスであることを指定する場合に使用します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config-if) end`	特権 EXEC モードに戻ります。

AAA サーバ用のダウンストリーム VRF の設定

ブロードバンドまたはリモート アクセス環境において AAA（RADIUS）サーバ用のダウンストリーム VRF を設定するには、次のシスコ属性値を入力します。

lcp:interface-config=ip vrf forwarding U downstream D

標準 VPN の状況では、代わりに次のシスコ属性値を入力します。

ip:vrf-id=U downstream D

MPLS VPN 半二重 VRF 設定の確認

手順の概要

1. **show vrf** [**ipv4** | **ipv6**] [**brief** | **detail** | **id** | **interfaces** | **lock** | **select**] [*vrf-name*]
2. **show ip route vrf***vrf-name*
3. **show running-config** [**interface***typenumber*]

手順の詳細

ステップ 1 **show vrf** [**ipv4** | **ipv6**] [**brief** | **detail** | **id** | **interfaces** | **lock** | **select**] [*vrf-name*]

デバイスで設定されているすべての Virtual Routing and Forwarding（VRF）インスタンス（関連付けられている各インターフェイスまたは仮想アクセスインターフェイス（VAI）のダウンストリーム VRF を含む）に関する情報を表示します。

例：

```
Device# show vrf
Name     Default RD     Interfaces
Down     100:1          POS3/0/3 [D]
                        POS3/0/1 [D]
         100:3          Loopback2
                        Virtual-Access3 [D]
                        Virtual-Access4 [D]
Up       100:2          POS3/0/3
                        POS3/0/1
         100:4          Virtual-Access3
```

show vrf detail*vrf-name* コマンドを使用して、VRF に関連付けられているすべてのインターフェイス、サブインターフェイス、および VAI を含む、指定した VRF に関する詳細情報を表示します。

vrf-name 引数の値を指定しなかった場合は、デバイスに設定されているすべての VRF に関する詳細情報が表示されます。

次に、ブロードバンドまたはリモート アクセス環境において、vrf1 と呼ばれる VRF の詳細情報を表示する例を示します。

例：

```
Device# show vrf detail vrf1
VRF D; default RD 2:0; default VPNID <not set>
  Interfaces:
         Loopback2           Virtual-Access3 [D]  Virtual-Access4 [D]
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:2:0
  Import VPN route-target communities
    RT:2:1
  No import route-map
  No export route-map
VRF U; default RD 2:1; default VPNID <not set>
  Interfaces:
    Virtual-Access3          Virtual-Access4
  Connected addresses are not in global routing table
  No Export VPN route-target communities
  Import VPN route-target communities
    RT:2:1
  No import route-map
  No export route-map
```

次に、標準バーチャル プライベート ネットワーク（VPN）環境において VRF 詳細を表示する例を示します。

例：

```
Device# show vrf detail
VRF Down; default RD 100:1; default VPNID <not set> VRF Table ID = 1
  Description: import only from hub-pe
  Interfaces:
    Pos3/0/3 [D]        Pos3/0/1:0.1 [D]
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:0
  Import VPN route-target communities
    RT:100:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
 VRF Up; default RD 100:2; default VPNID <not set> VRF Table ID = 2
  Interfaces:
    Pos3/0/1            Pos3/0/3
  Connected addresses are not in global routing table
  No Export VPN route-target communities
  Import VPN route-target communities
    RT:100:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
```

ステップ 2 **show ip route vrf***vrf-name*

指定したVRFのIPルーティングテーブル、およびダウンストリームVRFにインストールされているユーザ単位ルートに関する情報を表示します。

次に、ブロードバンドまたはリモートアクセス環境において、Dと呼ばれるダウンストリームVRFのルーティング テーブルを表示する例を示します。

例：

```
Device# show ip route vrf D

Routing Table: D
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS interarea
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
 10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
U   10.0.0.2/32 [1/0] via 10.0.0.1
S   10.0.0.0/8 is directly connected, Null0
U   10.0.0.5/32 [1/0] via 10.0.0.2
C   10.8.1.2/32 is directly connected, Virtual-Access4
C   10.8.1.1/32 is directly connected, Virtual-Access3
```

次に、標準VPN環境において、Downと呼ばれるダウンストリームVRFのルーティング テーブルを表示する例を示します。

例：

```
Device# show ip route vrf Down

Routing Table: Down
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 10.13.13.13 to network 0.0.0.0
C  10.2.0.0/8 is directly connected, Pos3/0/3
     10.3.0.0/32 is subnetted, 1 subnets
B       10.4.16.16 [200/0] via 10.13.13.13, 1w3d
B  10.6.0.0/8 [200/0] via 10.13.13.13, 1w3d
C  10.0.0.0/8 is directly connected, Pos3/0/1
 10.7.0.0/16 is subnetted, 1 subnets
B   10.7.0.0 [20/0] via 10.0.0.2, 1w3d
     10.0.6.0/32 is subnetted, 1 subnets
B       10.0.6.14 [20/0] via 10.0.0.2, 1w3d
     10.8.0.0/32 is subnetted, 1 subnets
B       10.8.15.15 [20/0] via 10.0.0.2, 1w3d
B*   0.0.0.0/0 [200/0] via 10.0.0.13, 1w3d
```

次に、ブロードバンドまたはリモートアクセス環境において、Uと呼ばれるアップストリームVRFのルーティング テーブルを表示する例を示します。

例：

```
Device# show ip route vrf U
Routing Table: U
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS interarea
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is 192.168.0.20 to network 0.0.0.0
 10.0.0.0/32 is subnetted, 1 subnets
C   10.0.0.8 is directly connected, Loopback2
B*   0.0.0.0/0 [200/0] via 192.168.0.20, 1w5d
```

次に、標準 VPN 環境において、Up と呼ばれるアップストリーム VRF のルーティング テーブルを表示する例を示します。

例：

```
Device# show ip route vrf Up
Routing Table: Up
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 10.13.13.13 to network 0.0.0.0
 10.2.0.0/32 is subnetted, 1 subnets
C   10.2.0.1 is directly connected, Pos3/0/3
     10.3.0.0/32 is subnetted, 1 subnets
B       10.3.16.16 [200/0] via 10.13.13.13, 1w3d
B  10.6.0.0/8 [200/0] via 10.13.13.13, 1w3d
 10.0.0.0/32 is subnetted, 1 subnets
C   10.0.0.1 is directly connected, Pos3/0/1
B*   0.0.0.0/0 [200/0] via 10.13.13.13, 1w3d
```

ステップ 3 **show running-config** [**interface***typenumber*]

関連するアップストリーム VRF とダウンストリーム VRF に関する情報を含む、指定したインターフェイスに関する情報を表示します。

次に、サブインターフェイス POS3/0/1 に関する情報を表示する例を示します。

例：

```
Device# show running-config interface POS 3/0/1
Building configuration...
Current configuration : 4261 bytes
!
interface POS3/0/1
ip vrf forwarding Up downstream Down
ip address 10.0.0.1 255.0.0.0
end
```

MPLS VPN 半二重 VRF の設定例

例：スポーク PE デバイスでのアップストリーム VRF とダウンストリーム VRF の設定

次の例は、Up という名前のアップストリーム Virtual Routing and Forwarding（VRF）インスタンスを設定します。

```
Device> enable
Device# configure terminal
Device(config)# vrf definition Up
Device(config-vrf)# rd 1:0
Device(config-vrf)# address-family ipv4
Device(config-vrf-af)# route-target import 1:0
Device(config-vrf-af)# exit-address-family
```

次に、Down と呼ばれるダウンストリーム VRF を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# vrf definition Down
Device(config-vrf)# rd 1:8
Device(config-vrf)# address-family ipv4
Device(config-vrf-af)# route-target import 1:8
Device(config-vrf-af)# exit-address-family
```

例：VRF とインターフェイスの関連付け

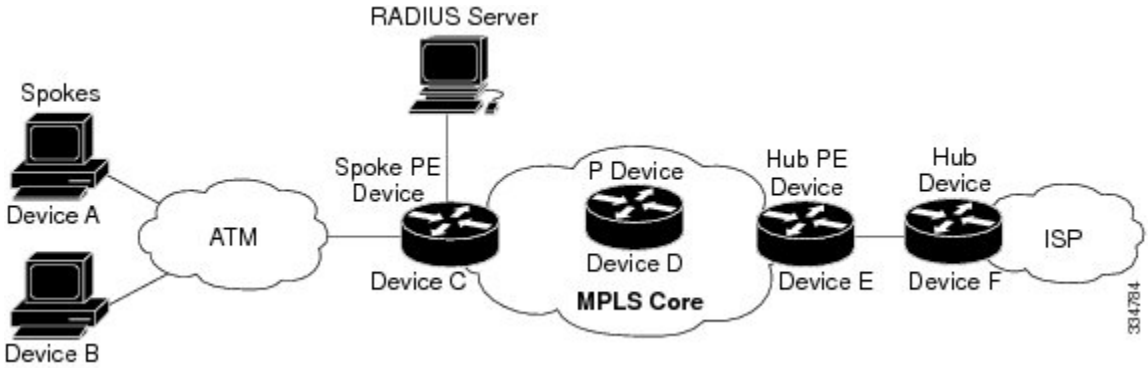
次に、Up という名前の Virtual Routing and Forwarding（VRF）インスタンスを POS3/0/1 サブインターフェイスに関連付け、Down という名前のダウンストリーム VRF を指定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface POS 3/0/1
Device(config-if)# vrf forwarding Up downstream Down
Device(config-if)# ip address 10.0.0.1 255.0.0.0
```

例：MPLS VPN 半二重 VRF の設定：スタティック CE-PE ルーティングを使用した例

この例では、次の図に示すハブアンドスポーク トポロジを使用し、ローカルで認証を行っています（つまり、RADIUS サーバは使用しません）。

図 *16*：トポロジの例




```
vrf definition D
 rd 1:8
 address-family ipv4
 route-target export 1:100
 exit-address-family
!
vrf definition U
 rd 1:0
 address-family ipv4
 route-target import 1:0
 exit-address-family
!
ip cef
vpdn enable
!
vpdn-group U
 accept-dialin
  protocol pppoe
  virtual-template 1
!
interface Loopback 2
 vrf forwarding U
 ip address 10.0.0.8 255.255.255.255
!
interface ATM 2/0
 description Mze ATM3/1/2
 no ip address
 no atm ilmi-keepalive
 pvc 0/16 ilmi
!
 pvc 3/100
  protocol pppoe
!
pvc 3/101
  protocol pppoe
!
```

例：RADIUSサーバとスタティックCE-PEルーティングを使用したMPLS VPN 半二重 VRF の設定

次に、2 つの Point-to-Point Protocol over Ethernet（PPPoE）クライアントを、デバイス C と呼ばれるスポークプロバイダー エッジ（PE）デバイス上の単一 Virtual Routing and Forwarding（VRF）ペアに接続する例を示します。どちらの PPPoE クライアントも同じ VRF 内で設定されていますが、すべての通信はハブ PE デバイスを使用して行われます。半二重 VRF がスポーク PE で設定されています。クライアントの設定は、RADIUS サーバからスポーク PE にダウンロードされます。

この例では、上図に示しているように、ハブアンドスポーク トポロジが使用されます。

（注） ホールセール プロバイダーは、ユーザ認証要求を対応する ISP に転送できます。ISP によってユーザが認証される場合、ホールセール プロバイダーは、PE デバイスに戻される要求に VRF 情報を付加します。

```
aaa new-model
!
aaa group server radius R
 server 10.0.20.26 auth-port 1812 acct-port 1813
!
aaa authentication ppp default group radius
aaa authorization network default group radius
!
vrf defintion D
 description Downstream VRF - to spokes
 rd 1:8
 address-family ipv4
 route-target export 1:100
 exit-address-family
!
vrf definition U
 description Upstream VRF - to hub
 rd 1:0
 address-family ipv4
 route-target import 1:0
 exit-address-family
!
ip cef
vpdn enable
!
vpdn-group U
 accept-dialin
  protocol pppoe
  virtual-template 1
!
interface Loopback2
 vrf forwarding U
 ip address 10.0.0.8 255.255.255.255
!
interface ATM2/0
  pvc 3/100
  protocol pppoe
 !
pvc 3/101
  protocol pppoe
 !
interface virtual-template 1
 no ip address
 ppp authentication chap
```

```
!
router bgp 1
 no synchronization
 neighbor 172.16.0.34 remote-as 1
 neighbor 172.16.0.34 update-source Loopback0
 no auto-summary
 !
address-family vpnv4
  neighbor 172.16.0.34 activate
  neighbor 172.16.0.34 send-community extended
  auto-summary
  exit-address-family
 !
address-family ipv4 vrf U
  no auto-summary
  no synchronization
  exit-address-family
!
address-family ipv4 vrf D
  redistribute static
  no auto-summary
  no synchronization
  exit-address-family
!
ip local pool U-pool 10.8.1.1 2.8.1.100
ip route vrf D 10.0.0.0 255.0.0.0 Null0
!
radius-server host 10.0.20.26 auth-port 1812 acct-port 1813
radius-server key cisco
```

例：ダイナミック CE-PE ルーティングを使用した MPLS VPN 半二重 VRF の設定

次に、Open Shortest Path First（OSPF）を使用して、スポーク サイトにルートをダイナミックにアドバタイズする例を示します。

この例では、上図に示しているように、ハブアンドスポーク トポロジが使用されます。

VRF の作成

```
vrf definition Down
rd 100:1
address-family ipv4
route-target export 100:0
exit-address-family
!
vrf definition Up
rd 100:2
address-family ipv4
route-target import 100:1
exit-address-family
```

MPLS のイネーブル化

```
mpls ldp graceful-restart
mpls ldp router-id Loopback0 force
mpls label protocol ldp
```

コアへの BGP の設定

```
router bgp 100
```

```
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.13.13.13 remote-as 100
 neighbor 10.13.13.13 update-source Loopback0
 !
 address-family vpnv4
 neighbor 10.13.13.13 activate
 neighbor 10.13.13.13 send-community extended
 bgp scan-time import 5
 exit-address-family
```

エッジへの BGP の設定

```
address-family ipv4 vrf Up
no auto-summary
no synchronization
exit-address-family
!
address-family ipv4 vrf Down
redistribute ospf 1000 vrf Down
no auto-summary
no synchronization
exit-address-family
```

スポーク PE のコアに向けたインターフェイスおよびプロセス

```
interface Loopback 0
 ip address 10.11.11.11 255.255.255.255
!
interface POS 3/0/2
 ip address 10.0.1.1 255.0.0.0
 mpls label protocol ldp
 mpls ip
!
router ospf 100
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 nsf enforce global
 redistribute connected subnets
 network 10.11.11.11 0.0.0.0 area 100
 network 10.0.1.0 0.255.255.255 area 100
```

スポーク PE のエッジに向けたインターフェイスおよびプロセス

```
interface Loopback 100
vrf forwarding Down
 ip address 10.22.22.22 255.255.255.255
!
interface POS 3/0/1
vrf forwarding Up downstream Down
 ip address 10.0.0.1 255.0.0.0
!
interface POS 3/0/3
vrf forwarding Up downstream Down
 ip address 10.2.0.1 255.0.0.0
!
router ospf 1000 vrf Down
 router-id 10.22.22.22
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 nsf enforce global
 redistribute connected subnets
 redistribute bgp 100 metric-type 1 subnets
 network 10.22.22.22 0.0.0.0 area 300
```

```
network 10.0.0.0 0.255.255.255 area 300
network 10.2.0.0 0.255.255.255 area 300
default-information originate
```

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 Master Command List, All Releases』
MPLS と MPLS アプリケーション コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』
MPLS VPN	「MPLS Virtual Private Networks」モジュール
IPv4 および IPv6 の VRF の設定	「MPLS VPN VRF CLI for IPv4 and IPv6 VPNs」モジュール

標準および RFC

標準/RFC	Title
RFC 2547	『BGP/MPLS VPNs』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。	http://www.cisco.com/cisco/web/support/index.html

MPLS VPN 半二重 VRF 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 に移動します。Cisco.com のアカウントは必要ありません。

表 *15*：*MPLS VPN* 半二重 *VRF* の機能情報

機能名	リリース	機能情報
MPLS VPN：スタティック ルーティングによる半二重 VRF（HDVRF）のサポート	12.3(6) 12.3(11)T 12.2(28)SB Cisco IOS XE Release 2.5	この機能を使用すると、MPLS VPN のエッジにある同じ PE デバイスに接続する VPN クライアントが、常にハブ サイトを通信に使用するようになります。 この機能は、Cisco IOS Release 12.3(6) で導入されました。 この機能は、Cisco IOS Release 12.4(20)T で統合されました。 この機能は、Cisco IOS Release 12.2(28)SB で統合されました。 Cisco IOS XE Release 2.5 では、この機能は Cisco ASR 1000 シリーズ アグリゲーション サービスルータに実装されました。

機能名	リリース	機能情報
MPLS VPN 半二重 VRF	12.2(28)SB2 12.4(20)T 12.2(33)SRC Cisco IOS XE Release 2.5	Cisco IOS Release 12.2(28)SB2 では、ダイナミック ルーティング プロトコルのサポートが追加されました。 この機能は、Cisco IOS Release 12.4(20)T で統合されました。 この機能は、Cisco IOS Release 12.2(33)SRC で統合されました。 この機能は、Cisco IOS XE Release 2.5 で統合されました。 次のコマンドが導入または変更されました：**ip vrf forwarding**（インターフェイス設定）、**show ip interface**、**show vrf**。

第 16 章

MPLS VPN BGP ローカル コンバージェンス

このマニュアルでは、プロバイダーエッジ（PE）からカスタマーエッジ（CE）リンク障害のダウンタイムの削減について説明します。Border Gateway Protocol（BGP）の再コンバージェンス前に、PE 出力トラフィックを CE へのバックアップ パスに再ルーティングする方法について説明します。MPLS VPN BGP ローカル コンバージェンス機能は「ローカル保護」とも呼ばれます。このマニュアルでは、PE-CE ローカル コンバージェンスの使用方法について説明します。

（注） MPLS VPN BGP ローカル コンバージェンス機能はバーチャル プライベート ネットワーク（VPN）から出て行くトラフィックのみに影響します。したがって、この機能だけではエンドツーエンドのトラフィックを完全には保護できません。

- 機能情報の確認，263 ページ
- MPLS VPN BGP ローカル コンバージェンスの前提条件，264 ページ
- MPLS VPN BGP ローカル コンバージェンスの制約事項，264 ページ
- MPLS VPN BGP ローカル コンバージェンスに関する情報，265 ページ
- MPLS VPN BGP ローカル コンバージェンスの設定方法，268 ページ
- MPLS VPN BGP ローカル コンバージェンスの設定例，272 ページ
- その他の参考資料，278 ページ
- MPLS VPN BGP ローカル コンバージェンスの機能情報，279 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモ

ジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 に移動します。Cisco.com のアカウントは必要ありません。

MPLS VPN BGP ローカル コンバージェンスの前提条件

- MPLS VPN BGP ローカル コンバージェンス リンク保護をイネーブルにする前に、カスタマー サイトとプロバイダー サイトを 2 つ以上のパスで接続する必要があります。
- メインのフォワーディング パスと冗長バックアップ パスの両方を Border Gateway Protocol（BGP）内で設定し、BGP が動作するパス間のロスレス スイッチオーバーをサポートする必要があります。
- パスが BGP に再配布される限り、プロバイダーエッジ（PE）とカスタマーエッジ（CE）の間で、サポートされている任意のルーティング プロトコルを使用できます。IPv4 でサポートされているプロトコルは、外部 BGP（eBGP）、ルーティング情報プロトコル（RIP）、Enhanced Interior Gateway Routing Protocol（EIGRP）、Open Shortest Path First（OSPF）、およびスタティック ルーティングです。IPv6 でサポートされているプロトコルは、eBGP およびスタティック ルーティングです。
- リンクへのバックアップとして機能するすべての PE デバイスには、リンクに関係する Virtual Routing and Forwarding（VRF）テーブルごとに一意のルート識別子を割り当てて、ルート リフレクタが使用可能なすべてのパスを確実にアドバタイズするようにします。
- 必須ではありませんが、バックアップ PE（上図の「PE 2」）は、CE とのリンクが保護されている PE（「PE 1」）で動作しているのと同じシスコ ソフトウェア リリースを実行することを推奨します。

MPLS VPN BGP ローカル コンバージェンスの制約事項

- MPLS VPN BGP ローカル コンバージェンス機能はバーチャル プライベート ネットワーク（VPN）から出て行くトラフィックのみに影響します。したがって、この機能だけではエンドツーエンドのトラフィックを完全には保護できません。
- このリンク保護は、高可用性（HA）ステートフル スイッチオーバー（SSO）中に開始できません。ただし、スイッチオーバーの開始前にこの保護が設定されていたリンクは、スイッチオーバー後も保護されます。
- このリンク保護を含むイメージから、この機能をサポートしないイメージへインサービス ソフトウェア ダウングレードを行った場合、Border Gateway Protocol（BGP）ルートが更新されるとアクティブな保護が停止します。
- BGP でサポートされるネクストホップ コア トンネリング テクノロジーも保護に利用できます。これには、マルチプロトコル ラベル スイッチング（MPLS）、IP/Layer 2 Tunneling Protocol

バージョン 3（L2TPv3）、IP/Generic Routing Encapsulation（GRE）が含まれます。また、プロバイダー エッジ（PE）とカスタマー エッジ（CE）の間では、Carrier Supporting Carrier（CSC）プロトコルもイネーブルにできます。相互自律システム オプション A（バックツーバック VRF）は、両方の自律システムで PE-CE リンクを保護するのと本質的に同じ機能であるため、サポートされます。ただし、相互自律システム オプション B および C 保護は、サポートされません。

- IPv4 の MPLS VPN BGP ローカル コンバージェンス機能は、外部 BGP（eBGP）、ルーティング情報プロトコル（RIP）、Enhanced Interior Gateway Routing Protocol（EIGRP）、Open Shortest Path First（OSPF）およびスタティック ルーティング プロトコルだけをサポートします。
- IPv6 の MPLS VPN BGP ローカル コンバージェンス機能は、eBGP およびスタティック ルーティング プロトコルのみをサポートしています。

MPLS VPN BGP ローカル コンバージェンスに関する情報

BGP によるリンク障害処理の仕組み

レイヤ 3 バーチャル プライベート ネットワーク（VPN）ネットワーク内では、プロバイダー エッジ（PE）とカスタマー エッジ（CE）間のリンクの障害によってカスタマー サイトへの接続が失われる（LoC）場合があり、時間依存型のアプリケーションには好ましくありません。このような機能停止状態が続く場合は、次のいくつかの要因が関係しています。

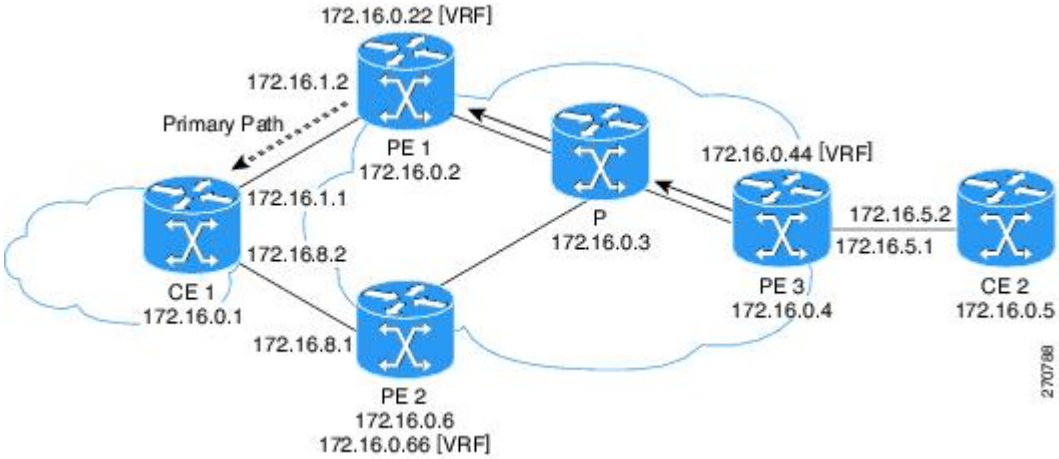
- 障害の検出時間
- 転送のプログラミング
- Border Gateway Protocol（BGP）のコンバージェンス（大規模ネットワークの場合、復旧されたトラフィックが宛先に到着するまでの時間はプレフィックスに応じて異なる）

BGP は PE-CE リンクの障害を検出すると、障害発生中のリンクを通るすべての BGP パスを削除します。BGP は影響を受けるプレフィックスでベストパス アルゴリズムを実行し、各プレフィックスに代替パスを選択します。これらの新しいパス（通常はリモート PE を含む）が転送に設定され、ローカル ラベルは削除されて、すべての BGP ネイバーに BGP withdrawal メッセージが送信されます。（通常はルート リフレクタを間接的に使用して）各 BGP ネイバーが withdrawal メッセージを受信すると、ベストパス アルゴリズムが呼び出され、プレフィックスが代替パスに切り替えられます。接続はこの時点にかぎって復元されます。

MPLS VPN BGP ローカル コンバージェンス機能によるリンク処理の仕組み

MPLS VPN BGP ローカル コンバージェンス機能では、プロバイダー エッジ（PE）とカスタマー エッジ（CE）間のリンクで保護されるプレフィックスに、そのリンクを含まないバックアップ パスが少なくとも 1 つ必要です。（次の図を参照してください）。カスタマー サイトには、プロバイダー サイトへの複数のバックアップ パスが必要です。

図 *17*：プライマリ パスとバックアップ パスが設定されたネットワーク

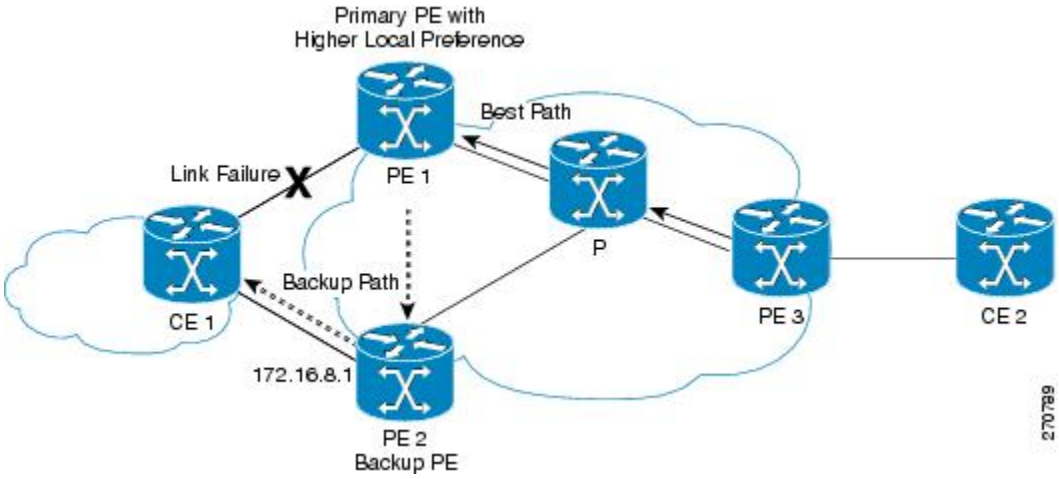


MPLS VPN BGP ローカル コンバージェンス機能では、ネットワーク全体のコンバージェンスを待機するのではなく、障害の発生したリンクのトラフィックをバックアップ パス経由で送信して、接続が失われる時間を短縮します（下図を参照）。ローカル ラベルは 5 分間維持されて、その間に障害が発生したローカルパスからバックアップパスへ、プレフィックスが切り替わります。ラベルは通常どおりに解放されないため、転送は引き続き行われます。

最適パス アルゴリズムは、バックアップ パスを選択します。このため、障害が発生した Border Gateway Protocol（BGP）ベストパス ラベルの代わりにローカル ラベルが適用されています（「ラベル スワッピング」と呼ばれることもあります）。トラフィックはローカルに復元される一方、

BGP withdrawal メッセージはネットワークに伝播されます。最終的に、出力 PE デバイスが収束され、ローカルの修復箇所がバイパスされます。

図 *18*：プライマリ パスで *PE-CE* リンク障害の発生後にバックアップ パスを使用するネットワーク



（注） ローカル ラベルは、5 分間維持されてから解放されます。リモートであって、Carrier Supporting Carrier（CSC）ネットワークの一部ではない BGP プレフィックスは、ローカル ラベルがないために削除されます。ローカル ラベルの削除で発生する遅延により、通常の BGP の追加や BGP パスの削除が変更されることはありません。BGP は、新しいバックアップ ベストパスを通常どおりフォワーディングに再プログラムします。

リンク障害検出の仕組み

ローカル保護では、Border Gateway Protocol（BGP）を使用してインターフェイス障害を検出します。検出には、インターフェイス ドライバまたはルーティング テーブルが使用されます。インターフェイスまたはルートがダウンすると、ルーティング テーブルの対応するパスが削除され、ルーティング アプリケーション プログラミング インターフェイス（API）を使用して BGP に通知されます。

しかし、ルーティング テーブルで障害を検出できない場合（レイヤ 2 スイッチがダウンした場合など）、BGP はホールドダウン タイマーを使用して、ネイバーがダウンしたことを検出します。ただし、BGP セッション タイムアウトのデフォルト値は 3 分間であるため、この検出に時間がかかる場合があります。

この検出時間を短縮するには、BGP セッション タイムアウトの間隔を短くするか（「Configuring Internal BGP Features」を参照）、プロバイダー エッジ（PE）とカスタマー エッジ（CE）間の外部 BGP（eBGP）内で双方向フォワーディング検出（BFD）プロトコルをイネーブルにします。

MPLS VPN BGP ローカル コンバージェンスの設定方法

（注） IPv4 および IPv6 VPN の VPN ルーティングおよび転送（VRF）インスタンスを設定するには、または既存のシングル プロトコル IPv4 専用 VRF をマルチプロトコル VRF 設定にアップグレードするには、『MPLS VPN--VRF CLI for IPv4 and IPv6 VPNs』モジュールを参照してください。

IPv4 による MPLS VPN BGP ローカル コンバージェンスの設定

はじめる前に

カスタマー エッジ（CE）デバイスとプロバイダー エッジ（PE）デバイスが最低でも 2 つのパスで接続されていることを確認します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **ip vrf***vrf-name*
4. **rd***route-distinguisher*
5. **protection local-prefixes**
6. **do show ip vrf detail**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**ip vrf***vrf-name* 例： `Device(config)# ip vrf vpn1`	VRF コンフィギュレーション モードを開始します。 • 名前を付けた VRF に、まだ VRF ルーティング テーブルと Cisco Express Forwarding テーブルが作成されていなかった場合は、このコマンドによってこれらのテーブルが作成され、両

	コマンドまたはアクション	目的
		方のテーブル名が、*vrf-name* 引数に指定した値（この例では vpn1 という名前）になります。
ステップ 4	**rd***route-distinguisher* 例： `Device(config-vrf)# rd 100:3`	（任意）名前を付けた VRF のルート識別子を設定します。 • 指定した VRF にルート識別子があらかじめ設定されていなかった場合は、このコマンドを入力する必要があります。 • ルート識別子の値は、次のいずれかになります。 • 自律システム番号にコロンと任意の数字を続ける（例：100:3）。 または • • IP アドレスにコロンと任意の数字を続ける（例：192.168.122.15:1）。
ステップ 5	**protection local-prefixes** 例： `Device(config-vrf)# protection local-prefixes`	BGP が再コンバージェンスする間ローカル プレフィックスを維持して、PE-CE リンクがダウンした場合に設定済みのバックアップ パスでトラフィックが伝送されるようにします。
ステップ 6	**do show ip vrf detail** 例： `Device(config-vrf)# do show ip vrf detail`	（任意）MPLS VPN BGP ローカル コンバージェンスが設定されたことを確認します。

IPv6 での MPLS VPN BGP ローカル コンバージェンスの設定

はじめる前に

カスタマー エッジ（CE）デバイスとプロバイダー エッジ（PE）デバイスが最低でも 2 つのパスで接続されていることを確認します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **vrf definition***vrf-name*
4. **rd***route-distinguisher*
5. **address-family** [**ipv4** | **ipv6**]
6. **protection local-prefixes**
7. **do show ip vrf detail**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**vrf definition***vrf-name* 例： `Device(config)# vrf definition vrf2`	VRF コンフィギュレーション モードを開始します。 • 名前を付けた Virtual Routing and Forwarding（VRF）に、まだ VRF ルーティング テーブルと Cisco Express Forwarding テーブルが作成されていなかった場合は、このコマンドによってこれらのテーブルが作成され、両方のテーブル名が、*vrf-name* 引数に指定した値（この例では vpn2 という名前）になります。
ステップ 4	**rd***route-distinguisher* 例： `Device(config-vrf)# rd 100:3`	（任意）名前を付けた VRF のルート識別子を設定します。 • 指定した VRF にルート識別子があらかじめ設定されていなかった場合は、このコマンドを入力する必要があります。 • ルート識別子の値は、次のいずれかになります。 　• 自律システム番号にコロンと任意の数字を続ける（例：100:3）。 または

	コマンドまたはアクション	目的
		• • IP アドレスにコロンと任意の数字を続ける（例：192.168.122.15:1）。
ステップ 5	**address-family [ipv4 | ipv6]** 例： `Device(config-vrf)# address-family ipv6`	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、IPv4 または IPv6 プロトコルを指定します。
ステップ 6	**protection local-prefixes** 例： `Device(config-vrf-af)# protection local-prefixes`	Border Gateway Protocol（BGP）が再コンバージェンスする間ローカル プレフィックスを維持して、PE-CE リンクがダウンした場合に設定済みのバックアップ パスでトラフィックが伝送されるようにします。
ステップ 7	**do show ip vrf detail** 例： `Device(config-vrf-af)# do show ip vrf detail`	（任意）MPLS VPN BGP ローカル コンバージェンスが設定されたことを確認します

例

ローカル リンク保護が有効になっていることを確認するには、**show ip vrf detail** コマンドを入力します。保護が有効になっている場合は、「Local prefix protection enabled」というステータス メッセージが出力に表示されます。

```
Device# show ip vrf detail

VRF vpn1 (VRF Id = 1); default RD 100:1; default VPNID <not set>
Interfaces:
    AT1/0/1.1
VRF Table ID = 1
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1                 RT:100:2
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
     Local prefix protection enabled
```

トラブルシューティングのヒント

- プロバイダーエッジ（PE）デバイス上に、安定した状態で、Border Gateway Protocol（BGP）の保護対象プレフィックスに対し、最低でも 2 つのパスが存在することを確認します。保護された PE を使用するパスは、フェールオーバーが発生する前に BGP の最適パスである必要があります。設定を表示するには、**show ip bgp vpnv4 vrf***vpnip-prefix* コマンドを入力します。
- **show ip vrf detail** コマンドを入力して、保護された PE でローカル保護がイネーブルになっていることを確認します。
- トポロジにルート リフレクタが存在する場合は、各 Virtual Routing and Forwarding（VRF）インスタンスに一意のルート識別子があることを確認します。

MPLS VPN BGP ローカル コンバージェンスの設定例

例：MPLS VPN BGP ローカル コンバージェンス

次に、MPLS VPN BGP ローカル コンバージェンスが、リンク障害発生後にトラフィックの損失を防ぐ例を示します。Border Gateway Protocol（BGP）のコンバージェンス前、コンバージェンス中、およびコンバージェンス後にローカル リンク保護の詳細情報を表示するには、**show bgp vpnv4** コマンドおよび **show mpls forwarding-table vrf** コマンドを使用します（次の 3 段階の例を参照）。

（注） **show bgp vpnv4 unicast** コマンドは **show ip bgp vpnv4** コマンドと同等です。

例 1：リンク障害発生前

プライマリ パスとバックアップ パスの両方が設定されています。

```
Device# show bgp vpnv4 unicast all 172.16.0.1
BGP routing table entry for 100:1:172.16.0.1/32, version 2
Paths: (2 available, best #2, table v1)
Flag: 0x820
  Advertised to update-groups:
     1
  100, imported path from 100:2:172.16.0.1/32
    172.16.0.6 (metric 21) from 172.16.0.7 (172.16.0.7)
      Origin incomplete, metric 0, localpref 100, valid, internal
      Extended Community: RT:100:0
      Originator: 172.16.0.6, Cluster list: 172.16.0.7
      mpls labels in/out 16/17
  100
    172.16.1.1 from 172.16.1.1 (172.16.0.1)
      Origin incomplete, metric 0, localpref 100, valid, external, best
      Extended Community: RT:100:0
      mpls labels in/out 16/nolabel
BGP routing table entry for 100:2:172.16.0.1/32, version 9
Paths: (1 available, best #1, no table)
Flag: 0x820
  Not advertised to any peer
```

```
  100
    172.16.0.6 (metric 21) from 172.16.0.7 (172.16.0.7)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:0
      Originator: 172.16.0.6, Cluster list: 172.16.0.7
      mpls labels in/out nolabel/17
```

両方のパスのラベル情報を表示できます。

```
Device# show bgp vpnv4 unicast all labels
Network          Next Hop      In label/Out label
Route Distinguisher: 100:1 (v1)
   172.16.0.1/32    172.16.0.6      16/17
                    172.16.1.1      16/nolabel
   172.16.0.5/32    172.16.0.4      nolabel/23
   172.16.0.22/32   0.0.0.0         17/nolabel(v1)
   172.16.0.44/32   172.16.0.4      nolabel/24
   172.16.0.66/32   172.16.0.6      nolabel/21
   172.16.1.0/24    172.16.1.1      18/nolabel
                    0.0.0.0         18/nolabel(v1)
   172.16.5.0/24    172.16.0.4      nolabel/25
   172.16.8.0/24    172.16.0.6      19/23
                    172.16.1.1      19/nolabel
Route Distinguisher: 100:2
   172.16.0.1/32    172.16.0.6      nolabel/17
   172.16.0.66/32   172.16.0.6      nolabel/21
   172.16.8.0/24    172.16.0.6      nolabel/23
```

PE1（上記の 1 番目の図を参照）転送テーブルには BGP 最適パス情報が格納されています。

```
Device# show mpls forwarding-table vrf v1 172.16.0.1 detail
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         No Label   172.16.0.1/32[V] 570           Et0/0      172.16.1.1
        MAC/Encaps=14/14, MRU=1504, Label Stack{}
        AABBCC000B00AABBCC000C000800
        VPN route: v1
        No output feature configured
```

例 2：リンク障害発生後、BGP のコンバージェンス前

1 つのパスだけでリンク障害が発生した場合は、バックアップ パスを使用できます（上記の 2 番目の図を参照）。

```
Device# show bgp vpnv4 unicast all 172.16.0.1

BGP routing table entry for 100:1:172.16.0.1/32, version 19
Paths: (1 available, best #1, table v1)
  Not advertised to any peer
  100, imported path from 100:2:172.16.0.1/32
    172.16.0.6 (metric 21) from 172.16.0.7 (172.16.0.7)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:0
      Originator: 172.16.0.6, Cluster list: 172.16.0.7
      mpls labels in/out 16/17
BGP routing table entry for 100:2:172.16.0.1/32, version 9
Paths: (1 available, best #1, no table)
  Not advertised to any peer
  100
    172.16.0.6 (metric 21) from 172.16.0.7 (172.16.0.7)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:0
      Originator: 172.16.0.6, Cluster list: 172.16.0.7
      mpls labels in/out nolabel/17
```

バックアップ パス ラベルのラベル情報を表示できます。

```
Device# show bgp vpnv4 unicast all labels
```

```
Network          Next Hop      In label/Out label
Route Distinguisher: 100:1 (v1)
   172.16.0.1/32    172.16.0.6      16/17
   172.16.0.5/32    172.16.0.4      nolabel/23
   172.16.0.22/32   0.0.0.0         17/nolabel(v1)
   172.16.0.44/32   172.16.0.4      nolabel/24
   172.16.0.66/32   172.16.0.6      nolabel/21
   172.16.1.0/24    172.16.0.6      nolabel/22
   172.16.5.0/24    172.16.0.4      nolabel/25
   172.16.8.0/24    172.16.0.6      19/23
Route Distinguisher: 100:2
   172.16.0.1/32    172.16.0.6      nolabel/17
   172.16.0.66/32   172.16.0.6      nolabel/21
   172.16.1.0/24    172.16.0.6      nolabel/22
   172.16.8.0/24    172.16.0.6      nolabel/23
```

PE 1（上記の 1 番目の図を参照）転送テーブルには、新しいラベルと、バックアップ パスにトラフィックを転送するネクストホップ情報が格納されています。

```
Device# show mpls forwarding-table vrf v1 172.16.0.1 detail

Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         17         172.16.0.1/32[V] 0             Et1/0      172.16.3.2
        MAC/Encaps=14/22, MRU=1496, Label Stack{21 17}
        AABBCC000D00AABBCC000C018847 0001500000011000
        VPN route: v1
        No output feature configured
```

例 3：ローカル ラベルの期限後、BGP の再コンバージェンス前

ローカル ラベルの保存期間が終了したため、代わりのローカル ラベルが PE 1 転送テーブル情報から送信されます。

```
Device# show mpls forwarding-table vrf v1 172.16.0.1 detail
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
None       17         172.16.0.1/32[V] 0             Et1/0      172.16.3.2
        MAC/Encaps=14/22, MRU=1496, Label Stack{21 17}
        AABBCC000D00AABBCC000C018847 0001500000011000
        VPN route: v1
        No output feature configured
```

新しい BGP 情報は、上記の 1 番目の図に示す設定に戻ります。

```
Device# show bgp vpnv4 unicast all 172.16.0.1
BGP routing table entry for 100:1:172.16.0.1/32, version 23
Paths: (1 available, best #1, table v1)
  Not advertised to any peer
  100, imported path from 100:2:172.16.0.1/32
    172.16.0.6 (metric 21) from 172.16.0.7 (172.16.0.7)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:0
      Originator: 172.16.0.6, Cluster list: 172.16.0.7
      mpls labels in/out nolabel/17
BGP routing table entry for 100:2:172.16.0.1/32, version 9
Paths: (1 available, best #1, no table)
  Not advertised to any peer
  100
    172.16.0.6 (metric 21) from 172.16.0.7 (172.16.0.7)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:0
      Originator: 172.16.0.6, Cluster list: 172.16.0.7
      mpls labels in/out nolabel/17
Device# show bgp vpnv4 unicast all labels

Network          Next Hop      In label/Out label
Route Distinguisher: 100:1 (v1)
   172.16.0.1/32    172.16.0.6      nolabel/17
```

```
   172.16.0.5/32    172.16.0.4      nolabel/23
   172.16.0.22/32   0.0.0.0         17/nolabel(v1)
   172.16.0.44/32   172.16.0.4      nolabel/24
   172.16.0.66/32   172.16.0.6      nolabel/21
   172.16.1.0/24    172.16.0.6      nolabel/22
   172.16.5.0/24    172.16.0.4      nolabel/25
   172.16.8.0/24    172.16.0.6      nolabel/23
Route Distinguisher: 100:2
   172.16.0.1/32    172.16.0.6      nolabel/17
   172.16.0.66/32   172.16.0.6      nolabel/21
   172.16.1.0/24    172.16.0.6      nolabel/22
   172.16.8.0/24    172.16.0.6      nolabel/23
```

例：6VPE 6PE の MPLS VPN BGP ローカル コンバージェンス

マルチプロトコル ラベル スイッチング（MPLS）を介した Cisco VPN IPv6 プロバイダー エッジ デバイス（6VPE）および Cisco IPv6 プロバイダー エッジ デバイス（6PE）の Border Gateway Protocol（BGP）ローカル コンバージェンスの実行前、実行中、および実行後に、**show bgp vpnv6** および **show mpls forwarding-table vrf** コマンドを使用してローカル リンク保護の詳細ビューを表示できます。次の 3 段階の例にこれを示します。

次の図は、BGP ローカル コンバージェンスが設定されている MPLS VPN を示します。PE-to-CE ルーティング プロトコルは External BGP（eGBP）であり、PE からルート リフレクタ（RR）セッションは GBP VPNv6 です。保護されているプレフィックスは CE 1 ループバックです

（2001:0DB8::/128）。プライマリ パスは PE 1 から CE 1 へのパスです。セカンダリ パスは PE 1 から P および PE3 経由での CE 1 へのパスです。

図 *19*：*MPLS VPN BGP* ローカル コンバージェンス

例 1：リンク障害発生前

プレフィックス 2001:0DB8::/128 に対してプライマリ パスとバックアップ パスの両方が設定されています。2 つのパスの inlabel/outlabel 設定は 28/28 および 28/nolabel です。

```
Device# show bgp vpnv6 unicast all 2001:0DB8::/128
BGP routing table entry for [1:1]2001:0DB8::/128, version 5
Paths: (2 available, best #2, table v1)
 Advertised to update-groups:
     2
  100, imported path from [2:2]2001:0DB8::/128
    ::FFFF:10.6.6.6 (metric 21) from 10.7.7.7 (10.7.7.7)
      Origin incomplete, metric 0, localpref 100, valid, internal
      Extended Community: RT:1:1
      Originator: 10.6.6.6, Cluster list: 10.7.7.7
      mpls labels in/out 28/28
  100
    2001:0DB8:0:ABCD::1 (FE80::A8BB:CCFF:FE00:B00) from 2001:0DB8:0:ABCD::1 (10.1.1.1)
      Origin incomplete, metric 0, localpref 100, valid, external, best

      Extended Community: RT:1:1
      mpls labels in/out 28/nolabel
BGP routing table entry for [2:2]2001:0DB8::/128, version 11
Paths: (1 available, best #1, no table)
  Not advertised to any peer
  100
    ::FFFF:10.6.6.6 (metric 21) from 10.7.7.7 (10.7.7.7)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:1:1
      Originator: 10.6.6.6, Cluster list: 10.7.7.7
      mpls labels in/out nolabel/28
```

PE1 転送テーブルには、新しいラベルと、バックアップ パスにトラフィックを転送するネクストホップ情報が格納されています。

```
Device#
show mpls forwarding-table vrf v1 2001:0DB8::/128 detail
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
28        No Label   2001:0DB8::/128[V]     804          Et0/0     FE80::A8BB:CCFF:FE00:B00

        MAC/Encaps=14/14, MRU=1504, Label Stack{}
        AABBCC000B00AABBCC000C0086DD
        VPN route: v1
        No output feature configured
```

例 2：リンク障害発生後

リンク障害発生後は、バックアップ パスは引き続き使用できますが、元のパスはBGPから削除され、バックアップ パスがアクティブになります。

```
Device# show mpls forwarding-table vrf v1 2001:0DB8::/128 detail
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
28         28         2001:0DB8::/128[V]     0             Et1/0      10.3.0.2
        MAC/Encaps=14/22, MRU=1496, Label Stack{23 28}
        AABBCC000D00AABBCC000C018847 000170000001C000
        VPN route: v1
        No output feature configured
```

設定された時間が経過すると、ローカル ラベルの有効期限が切れます。**show mpls forwarding-table** コマンドの出力でも、ローカル ラベルが期限切れであることが確認できます。

```
Device# show mpls forwarding-table vrf v1 2001:0DB8::/128 detail
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
```

```
None       28         2001:0DB8::/128[V]     0             Et1/0      10.3.0.2
        MAC/Encaps=14/22, MRU=1496, Label Stack{23 28}
        AABBCC000D00AABBCC000C018847 000170000001C000
        VPN route: v1
        No output feature configured
Example 3: After the Link Is Restored
```

リンクが復旧すると、BGP に元のパスが追加され、トラフィックがこのパスに再び切り替わります。

```
Device# show bgp vpnv6 unicast all 2001:0DB8::/128
BGP routing table entry for [1:1]2001:0DB8::/128, version 28
Paths: (2 available, best #1, table v1)
  Advertised to update-groups:
     2
  100
    2001:0DB8:0:ABCD::1 (FE80::A8BB:CCFF:FE00:B00) from 2001:0DB8:0:ABCD::1 (10.1.1.1)
      Origin incomplete, metric 0, localpref 100, valid, external, best
      Extended Community: RT:1:1
      mpls labels in/out 16/nolabel
  100, imported path from [2:2]2001:0DB8::/128
    ::FFFF:10.6.6.6 (metric 21) from 10.7.7.7 (10.7.7.7)
      Origin incomplete, metric 0, localpref 100, valid, internal
      Extended Community: RT:1:1
      Originator: 10.6.6.6, Cluster list: 10.7.7.7
      mpls labels in/out 16/28
BGP routing table entry for [2:2]2001:0DB8::/128, version 11
Paths: (1 available, best #1, no table)
  Not advertised to any peer
  100
    ::FFFF:10.6.6.6 (metric 21) from 10.7.7.7 (10.7.7.7)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:1:1
      Originator: 10.6.6.6, Cluster list: 10.7.7.7
      mpls labels in/out nolabel/28
Device# show mpls for vrf v1 2001:0DB8::/128 detail
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         No Label   2001:0DB8::/128[V] 0         Et0/0      FE80::A8BB:CCFF:FE00:B00
        MAC/Encaps=14/14, MRU=1504, Label Stack{}
        AABBCC000B00AABBCC000C0086DD
        VPN route: v1
        No output feature configured
```

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 Master Command List, All Releases』
MPLS と MPLS アプリケーション コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』
BGP の設定	『*IP Routing: BGP Configuration Guide*』の「*Configuring a Basic BGP Network*」モジュール
障害が発生したフォワーディング パスをすばやく検出するプロトコル	『*IP Routing: BFD Configuration Guide*』の「Bidirectional Forwarding Detection」モジュール

関連項目	マニュアル タイトル
IP および MPLS-VPN 向け BGP PIC エッジの設定	『*MPLS Layer 3 VPNs Configuration Guide*』の「BGP PIC Edge for IP and MPLS VPN」モジュール
内部 BGP 機能の設定	『*IP Routing: BGP Configuration Guide*』の「Configuring Internal BGP Features」モジュール
IPv4 と IPv6 の具体的な状況における VRF の設定	『*MPLS Layer 3 VPNs Configuration Guide*』の「MPLS VPN VRF CLI for IPv4 and IPv6 VPNs」モジュール

標準および RFC

標準/RFC	Title
RFC 2547	『BGP/MPLS VPNs』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。	http://www.cisco.com/cisco/web/support/index.html

MPLS VPN BGP ローカル コンバージェンスの機能情報

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 に移動します。Cisco.com のアカウントは必要ありません。

表 *16*：***MPLS VPN BGP*** ローカル コンバージェンスの機能情報

機能名	リリース	機能情報
MPLS VPN BGP ローカル コンバージェンス	12.2(33)SRC 12.2(33)SB 15.0(1)M Cisco IOS XE Release 3.1S	MPLS VPN BGP ローカル コンバージェンス機能は、BGP の再コンバージェンス前に、PE 出力トラフィックを CE へのバックアップパスに再ルーティングして、PE-CE リンク障害によるダウンタイムを削減します。 この機能は、12.2(33)SRC で Cisco 7200 および Cisco 7600 に導入されました。 この機能は、12.2(33)SB で Cisco 7300 シリーズと Cisco 10000 シリーズのルータで使用可能になりました。 この機能は、Cisco IOS Release 15.0(1)M に統合されました。 この機能は、Cisco IOS XE Release 3.1S で、Cisco ASR 1000 シリーズ ルータに実装されました。 **protection local-prefixes** コマンドが変更されました。

機能名	リリース	機能情報
6VPE 6PE の MPLS VPN BGP ローカル コンバージェンス	15.0(1)S Cisco IOS XE Release 3.1S	6VPE/6PE の MPLS VPN BGP ローカル コンバージェンス機能は、MPLS を介した Cisco VPN IPv6 プロバイダー エッジ デバイス（6VPE）と Cisco IPv6 プロバイダー エッジ デバイス（6PE）の MPLS VPN BGP ローカル コンバージェンスを実装します。 この機能は、15.0(1)S で導入されました。 この機能は、Cisco IOS XE Release 3.1S で、Cisco ASR 1000 シリーズ ルータに実装されました。 **protection local-prefixes** コマンドが変更されました。

第 17 章

IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI

IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI 機能によって、同じ VRF インスタンスで IPv4 および IPv6 VPN をイネーブルにし、単一プロトコル VRF 設定からマルチプロトコル VRF 設定への移行を簡単に実行できる Cisco コマンドが導入されます。マルチプロトコル VRF を使用すると、IPv4 と IPv6 との間でルート ターゲット ポリシー（インポートとエクスポート）を共有したり、IPv4 および IPv6 VPN に異なる route-target ポリシーを設定したりできます。

このマニュアルでは、IPv4 および IPv6 VPN 用のバーチャル プライベート ネットワーク（VPN）ルーティング/転送（VRF）インスタンスの設定方法、および既存の IPv4 だけの単一プロトコル VRF をマルチプロトコル VRF 設定にアップグレードする方法について説明します。

- 機能情報の確認，283 ページ
- IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI の前提条件，284 ページ
- IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI の制約事項，284 ページ
- IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI に関する情報，284 ページ
- IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI の設定方法，287 ページ
- IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI の設定例，296 ページ
- その他の参考資料，300 ページ
- IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI の機能情報，301 ページ
- 用語集，303 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 に移動します。Cisco.com のアカウントは必要ありません。

IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI の前提条件

- 移行する場合は、IPv4 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）Virtual Routing and Forwarding（VRF）インスタンスが存在している必要があります。
- 新たに VRF を設定する場合は、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で、シスコエクスプレスフォワーディング、およびラベル配布プロトコル（LDP）または MPLS トラフィック エンジニアリング（TE）の MPLS ラベル配布方式がイネーブルになっている必要があります。

IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI の制約事項

- マルチプロトコル Virtual Routing and Forwarding（VRF）インスタンスに変換した後は、VRF を IPv4 だけの単一プロトコル VRF に再変換することができません。
- 1 つのインターフェイスは 1 つの VRF にだけ関連付けることができます。同じインターフェイスで、IPv4 用の VRF と、別の IPv6 用の VRF を設定することはできません。
- マルチプロトコル VRF では、IPv4 および IPv6 アドレス ファミリだけを設定できます。IPX や AppleTalk などの他のプロトコルはサポートされていません。

IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI に関する情報

IPv4 と IPv6 の MPLS VPN で共通の VRF に関する概念

IPv6 のバーチャルプライベートネットワーク（VPN）では、アドレスファミリ、ルート識別子、ルート ターゲット、Virtual Routing and Forwarding（VRF）識別子など、IPv4 マルチプロトコル ラベル スイッチング（MPLS）VPN で使用されるものと同じ VRF に関する概念が使用されます。IPv4 と IPv6 の両方の VPN を使用するカスタマーは、これらのアドレス ファミリにおいて VRF ポリシーを共有できます。IPv4 だけの単一プロトコル VRF で行うように、アドレス ファミリごとに個別に VRF ポリシーを定義するのではなく、すべてのアドレス ファミリに適用可能な VRF ポリシーを定義できます。

IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI 機能が導入される前は、VRF は IPv4 アドレス ファミリのみに適用されていました。VRF 名とルーティングおよび転送テーブルの識別子との間、VRF 名とルート識別子（RD）との間、VRF 名と VPN ID との間には、1 対 1 の関係がありました。この設定は、単一プロトコル VRF と呼ばれています。

IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI 機能により、複数アドレス ファミリ（multi-AF）VRF 構造のサポートが導入されました。multi-AF VRF では、同じ VRF に複数のアドレス ファミリを定義できます。名前、およびポリシーのセットによって識別される特定の VRF を、IPv4 VPN と IPv6 VPN の両方に同時に適用できます。ルーティングおよび転送テーブルは IPv4 プロトコルと IPv6 プロトコルで異なりますが、特定のインターフェイスでこの VRF をアクティブにできます。この設定は、マルチプロトコル VRF と呼ばれています。

単一プロトコル VRF からマルチプロトコル VRF への移行

IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI 機能が導入される前は、単一プロトコル IPv4 のみの Virtual Routing and Forwarding（VRF）インスタンスを作成できました。単一プロトコル VRF は、**ip vrf** コマンドを入力して作成していました。インターフェイスで単一プロトコル VRF をアクティブにするには、**ip vrf forwarding**（インターフェイス コンフィギュレーション）コマンドを入力していました。

IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI 機能が導入された後は、**vrf definition** コマンドを入力してマルチプロトコル VRF を作成します。インターフェイスでマルチプロトコル VRF をアクティブにするには、**vrf forwarding** コマンドを入力します。

IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI 機能では、VRF 設定を単一プロトコル VRF モデルからマルチプロトコル VRF モデルに強制的に移行する **vrf upgrade-cli multi-af-mode** {**common-policies** | **non-common-policies**} [**vrf***vrf-name*] コマンドが導入されました。

- route-target ポリシーが、multi-AF VRF に設定されたすべてのアドレス ファミリに適用される場合は、**common-policies** キーワードを使用します。
- route-target ポリシーが、移行元である IPv4 アドレス ファミリにだけ適用される場合は、**non-common-policies** キーワードを使用します。

vrf upgrade-cli コマンドを入力して設定を NVRAM に保存すると、単一プロトコル VRF 設定がマルチプロトコル VRF 設定として保存されます。アップグレード プロセスにおいて、**ip vrf** コマンドが **vrf definition** コマンド（グローバル コンフィギュレーション コマンド）に変換され、**ip vrf forwarding** コマンドが **vrf forwarding** コマンド（インターフェイス コンフィギュレーション コマンド）に変換されます。**vrf upgrade-cli** コマンドは一度だけ実行でき、即時に処理が実行されます。

デバイスには、IPv4 だけの VRF とマルチプロトコル VRF の両方を設定することができます。作成した VRF を編集するには、必ず作成したモードのコマンドを使用します。たとえば、次のマルチプロトコル VRF コマンドを使用して、vrf2 という名前の VRF を作成したとします。

```
Device# configure terminal
Enter configuration command, one per line. End with CNTL/Z
Device(config)# vrf definition vrf2
Device(config-vrf)# rd 2:2
Device(config-vrf)# route-target import 2:2
Device(config-vrf)# route-target export 2:2
Device(config-vrf)# end
```

IPv4 だけの VRF コマンドを使用して VRF vrf2 の編集を試みると、次のメッセージが表示されます。

```
Device# configure terminal
Enter configuration command, one per line. End with CNTL/Z
Device(config)# ip vrf vrf2
% Use 'vrf definition vrf2' command
```

また、マルチプロトコル VRF 用のコマンドを使用して IPv4 だけの VRF の編集を試みると、次のメッセージが表示されます。<vrf-name> は、IPv4 だけの VRF の名前です。

```
% Use 'ip vrf <vrf-name>' command
```

ip vrf *name* コマンドおよび **ip vrf forwarding**（インターフェイス コンフィギュレーション）コマンドは、一定の使用猶予期間後に削除されます。古い IPv4 だけの VRF を新しいマルチプロトコル VRF 設定に移行するには、**vrf upgrade-cli** コマンドを使用します。VRF が IPv4 VPN 用であるか、IPv6 VPN 用であるか、またはその両方であるかにかかわらず、新しい VRF を作成する必要がある場合には、multi-AF 設定をサポートするマルチプロトコル VRF 用の **vrf definition** コマンドおよび **vrf forwarding** コマンドを使用します。

マルチプロトコル VRF 設定の特性

マルチプロトコル Virtual Routing and Forwarding（VRF）設定では、同じアドレス ファミリに IPv4 VRF と IPv6 VRF の両方を設定することも、IPv4 または IPv6 アドレス ファミリのそれぞれに別々の VRF を設定することもできます。マルチプロトコル VRF 設定には、次の特性があります。

- VRF 名によって VRF が識別されますが、この VRF には IPv4 と IPv6 の両方のアドレス ファミリを設定できます。同じインターフェイスで、異なる VRF 名を使用して IPv4 および IPv6 アドレス ファミリを設定することはできません。
- ルート識別子（RD）、VPN ID、および簡易ネットワーク管理プロトコル（SNMP）コンテキストは、特定の VRF の IPv4 と IPv6 の両方のアドレス ファミリによって共有されます。
- address-family 設定の外部で multi-AF VRF モードに指定されたポリシー（ルート ターゲットなど）は、各アドレス ファミリに適用されるデフォルトとなります。ルート ターゲットは、アドレス ファミリの内部および外部で定義できる唯一の VRF 特性です。

マルチプロトコル VRF をインターフェイスに関連付けた場合は、次の特性も適用されます。

- インターフェイスを VRF にバインドすると（**vrf forwarding***vrf-name* コマンド）、そのインターフェイス上のすべての IPv4 および IPv6 アドレスが削除されます。
- VRF を特定のインターフェイスに関連付けると、すべてのアクティブなアドレス ファミリがその VRF に属するようになります。address-family タイプのアドレスが設定されていない場合は、例外的にそのプロトコルはディセーブルになります。
- VRF にバインドされたインターフェイスにアドレスを設定する場合、そのアドレス タイプに対応するアドレス ファミリが当該 VRF でアクティブである必要があります。アクティブでない場合は、まず VRF でアドレス ファミリをアクティブにする必要があるという内容のエラー メッセージが表示されます。

IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI 機能の導入により、単一プロトコル VRF CLI との後方互換性がサポートされています。このことは、同じデバイスで単一プロトコル CLI とマルチプロトコル CLI を使用できることを意味しています。ただし、同じ VRF 設定内でこれら両方を使用することはできません。

単一プロトコル CLI を使用すると、引き続き VRF 内で IPv4 アドレスを定義し、同じインターフェイスのグローバル ルーティング テーブルに IPv6 アドレスを定義できます。

IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI の設定方法

IPv4 および IPv6 MPLS VPN 用の VRF の設定

IPv4 および IPv6 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 Virtual Routing and Forwarding（VRF）インスタンスを設定するには、次の作業を実行します。IPv4 VPN と IPv6 VPN の両方に対して VRF を設定する場合（マルチプロトコル VRF）、VRF 内のすべてのアドレス ファミリに適用される route-target ポリシーを設定することも、VRF 内の個別のアドレス ファミリに適用される route-target ポリシーを設定することもできます。

次に、別々の VRF アドレス ファミリに IPv4 および IPv6 VPN の route-target ポリシーが定義された VRF の設定方法を示します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **vrf definition***vrf-name*
4. **rd***route-distinguisher*
5. **address-family** {**ipv4** | **ipv6**}
6. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
7. **exit-address-family**
8. **address-family** {**ipv4** | **ipv6**}
9. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**vrf definition***vrf-name* 例： `Device(config)# vrf definition vrf1`	VRF ルーティング テーブルを設定し、VRF コンフィギュレーション モードを開始します。 • *vrf-name* 引数は、VRF の名前です。

ステップ 4	**rd***route-distinguisher*
	例：
	`Device(config-vrf)# rd 100:1`
		VRF のルーティング テーブルと転送テーブルを作成します。
		• *route-distinguisher* 引数では、8 バイトの値を IPv4 プレフィックスに追加して VPN IPv4 プレフィックスを作成することを指定します。ルート識別子は、次のいずれかの形式で入力できます。
		  • 16 ビット ASN：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	**address-family** {**ipv4** | **ipv6**} 例： `Device(config-vrf) address-family ipv4`	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。 • **ipv4** キーワードは、VRF の IPv4 アドレス ファミリを指定します。 • **ipv6** キーワードは、VRF の IPv6 アドレス ファミリを指定します。
ステップ 6	**route-target** {**import** | **export** | **both**} *route-target-ext-community* 例： `Device(config-vrf-af)# route-target both 100:2`	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。 • **import** キーワードは、ターゲット VPN 拡張コミュニティからルーティング情報をインポートすることを指定します。 • **export** キーワードは、ルーティング情報をターゲット VPN 拡張コミュニティにエクスポートすることを指定します。 • **both** キーワードは、ルーティング情報のターゲット VPN 拡張コミュニティからのインポート、およびターゲット VPN 拡張コミュニティへのエクスポートの両方が行われることを指定します。

	コマンドまたはアクション	目的
		• *route-target-ext-community* 引数により、route-target 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 route-target 拡張コミュニティの VRF リストに追加されます。
ステップ 7	**exit-address-family** 例： `Device(config-vrf-af)# exit-address-family`	VRF 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。
ステップ 8	**address-family** {**ipv4** | **ipv6**} 例： `Device(config-vrf) address-family ipv6`	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。 • **ipv4** キーワードは、VRF の IPv4 アドレス ファミリを指定します。 • **ipv6** キーワードは、VRF の IPv6 アドレス ファミリを指定します。
ステップ 9	**route-target** {**import** | **export** | **both**} *route-target-ext-community* 例： `Device(config-vrf-af)# route-target both 100:3`	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。 • **import** キーワードは、ターゲット VPN 拡張コミュニティからルーティング情報をインポートすることを指定します。 • **export** キーワードは、ルーティング情報をターゲット VPN 拡張コミュニティにエクスポートすることを指定します。 • **both** キーワードは、ルーティング情報のターゲット VPN 拡張コミュニティからのインポート、およびターゲット VPN 拡張コミュニティへのエクスポートの両方が行われることを指定します。 • *route-target-ext-community* 引数により、route-target 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 route-target 拡張コミュニティの VRF リストに追加されます。 **route-target** コマンドは、各ターゲット コミュニティにつき一度ずつ入力します。
ステップ 10	**end** 例： `Device(config-vrf-af)# end`	特権 EXEC モードに戻ります。

マルチプロトコル VRF とインターフェイスの関連付け

マルチプロトコル Virtual Routing and Forwarding（VRF）インスタンスをインターフェイスに関連付けるには、次の作業を実行します。VRF をインターフェイスに関連付けると、VRF がアクティブになります。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***typenumber*
4. **vrf forwarding***vrf-name*
5. **ip address***ip-address mask* [**secondary**]
6. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-namesub-bits*/*prefix-length*}
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**interface***typenumber* 例： `Device(config)# interface Ethernet 0/1`	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。 • *type* 引数には、設定するインターフェイスのタイプを指定します。 • *number* 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	**vrf forwarding***vrf-name* 例： `Device(config-if)# vrf forwarding vrf1`	VRF をインターフェイスまたはサブインターフェイスと関連付けます。 • *vrf-name* 引数は、VRF の名前です。

	コマンドまたはアクション	目的
ステップ 5	**ip address***ip-address mask* [**secondary**] 例： `Device(config-if)# ip address 10.24.24.24 255.255.255.255`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。 • *ip-address* 引数は、IP アドレスです。 • *mask* 引数は、関連付けられた IP サブネットのマスクです。 • **secondar**y キーワードは、設定されるアドレスがセカンダリ IP アドレスであることを指定する場合に使用します。このキーワードが省略された場合、設定されたアドレスはプライマリ IP アドレスになります。
ステップ 6	**ipv6 address** {*ipv6-address*|*prefix-length* | *prefix-namesub-bits*|*prefix-length*} 例： `Device(config-if)# ipv6 address 2001:0DB8:0300:0201::/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。 • *ipv6-address* 引数は、使用する IPv6 アドレスです。 • *prefix-length* 引数は、IPv6 プレフィックスの長さです。これは、アドレスのうち連続する上位何ビットがプレフィックス（アドレスのネットワーク部）を構成するかを示す 10 進数値です。10 進数値の前にスラッシュ記号が必要です。 • *prefix-name* 引数は、インターフェイスに設定するネットワークを表す上位ビットを指定する一般的なプレフィックスです。 • *sub-bits* 引数は、*prefix-name* 引数で指定された一般的なプレフィックスによって提供されるプレフィックスに連結する、アドレスのサブプレフィックス ビットおよびホスト ビットです。 *sub-bits* 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16 進数値を 16 ビット単位でコロンで区切って指定します。
ステップ 7	**end** 例： `Device(config-if) end`	特権 EXEC モードに戻ります。

IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI 設定の確認

IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI 機能の設定を確認する、つまり Virtual Routing and Forwarding（VRF）設定が multi-AF マルチプロトコル VRF にアップグレードされたことを表示するには、次の作業を実行します。

手順の概要

1. イネーブル化
2. **show running-config vrf** [*vrf-name*]
3. **show vrf**
4. **show vrf detail** [*vrf-name*]
5. **exit**

手順の詳細

ステップ 1 イネーブル化

特権EXECモードをイネーブルにします。プロンプトが表示されたらパスワードを入力します。次に例を示します。

例：

```
Device> enable
Device#
```

ステップ 2 **show running-config vrf** [*vrf-name*]

multi-AF マルチプロトコル VRF 設定へのアップグレードに成功したことを確認します。次に、multi-AF マルチプロトコル VRF にアップグレードする前のコマンド出力例を示します。

例：

```
Device# show running-config vrf vpn2

Building configuration...
Current configuration : 604 bytes
ip vrf vpn2
 rd 1:1
 route-target both 1:1
!
!
interface Loopback1
 ip vrf forwarding vpn2
 ip address 10.43.43.43 255.255.255.255
!
```

次に、すべてのアドレス ファミリの共通ポリシーが設定された multi-AF マルチプロトコル VRF へアップグレードした後の、コマンドの出力例を示します。

例：

```
Device# show running-config vrf vpn1

Building configuration...
Current configuration : 604 bytes
vrf definition vpn1
 rd 1:1
 route-target both 1:1
!
 address-family 1pv4
 exit-address-family
```

```
!
!
interface Loopback1
 ip vrf forwarding vpn1
 ip address 10.43.43.43 255.255.255.255
!
```

この設定には、**vrf definition** コマンドが含まれています。multi-AF マルチプロトコル VRF 設定の **ip vrf** コマンドが **vrf definition** コマンドに置き換えられます。

ステップ 3 **show vrf**

multi-AF マルチプロトコル VRF 設定へのアップグレードに成功したことを確認します。VRF 設定が multi-AF マルチプロトコル VRF 設定に更新されると、**show ip vrf** コマンドが **show vrf** コマンドに置き換えられます。**show vrf** コマンドによって、VRF に定義されているプロトコルが表示されます。次のコマンドは、単一プロトコル VRF 設定を multi-AF マルチプロトコル VRF 設定にアップグレードした後の出力例を示します。

例：

```
Device# show vrf vpn1

  Name                            Default RD     Protocols         Interfaces
  vpn1                            1:1            ipv4              Lo1/0
```

次に、**show ip vrf vp1** コマンドの出力例を示します。この出力を **show vrf vpn1** コマンドの出力と比較してください。VRF の下のプロトコルは表示されません。

例：

```
Device# show ip vrf vrf1

  Name      Default RD   Interface
  vpn1      1:1          Loopback1
```

次に、マルチプロトコル VRF に対する **show vrf** コマンドの出力例を示します。このうちの 1 つには IPv4 と IPv6 プロトコルの両方が含まれています。

例：

```
Device# show vrf

  Name                            Default RD     Protocols         Interfaces
  vpn1                            1:1            ipv4              Lo1/0
  vpn2                            100:3          ipv4              Lo23  AT3/0/0.1
  vpn4                            100:2          ipv4,ipv6
```

ステップ 4 **show vrf detail** [*vrf-name*]

設定が予期されているとおりであることを確認するため、定義されている VRF の全特性を表示します。例えば、VRF vpn1 の VRF が次のように設定されているとします。

例：

```
vrf definition vpn1
 route-target both 100:1
 route-target import 100:2
```

```
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 route-target both 100:1
 route-target import 100:3
 exit-address-family
```

このコマンドにより表示される内容を次に示します。

例：

```
Device# show vrf detail vpn1

VRF vpn1 (VRF Id = 3); default RD <not set>; default VPNID <not set>
  No interfaces
Address family ipv4 (Table ID = 3 (0x3)):
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1                RT:100:2
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
Address family ipv6 (Table ID = 503316483 (0x1E000003)):
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1                RT:100:3
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
```

ステップ 5 **exit**

ユーザ EXEC モードに戻ります。次に例を示します。

例：

```
Device# exit
Device>
```

IPv4 だけの単一プロトコル VRF からマルチプロトコル VRF 設定への移行

単一プロトコル（IPv4 のみ）Virtual Routing and Forwarding（VRF）設定からマルチプロトコル VRF 設定へ移行するには、次の作業を実行します。

マルチプロトコル VRF 設定により、同じ VRF で複数のアドレスファミリを定義できます。名前、およびポリシーのセットによって識別される特定の VRF を、IPv4 VPN と IPv6 VPN の両方に同時

に適用できます。ルーティングおよび転送テーブルは IPv4 プロトコルと IPv6 プロトコルで異なりますが、特定のインターフェイスでこの VRF をアクティブにできます。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **vrf upgrade-cli multi-af-mode** {**common-policies** | **non-common-policies**} [**vrf***vrf-name*]
4. **exit**
5. **show running-config vrf** [*vrf-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**vrf upgrade-cli multi-af-mode** {**common-policies** | **non-common-policies**} [**vrf***vrf-name*] 例： `Device(config)# vrf upgrade-cli multi-af-mode common-policies vrf vpn4`	同じ VRF で複数のアドレス ファミリをサポートするため、デバイスに設定されている 1 つの VRF インスタンスまたはすべての VRF をアップグレードします。 • **multi-af-mode** キーワードは、1 つの単一プロトコル VRF またはすべての VRF を、multi-AF 設定をサポートするマルチプロトコル VRF にアップグレードすることを指定します。 • **common-policies** キーワードは、ルート ターゲット ポリシーを VRF 設定の共通部分にコピーすることを指定します。これにより、このポリシーが multi-AF VRF で設定されているすべてのアドレス ファミリに適用されます。 • **non-common-policies** キーワードは、ルート ターゲット ポリシーを VRF 設定の IPv4 アドレス ファミリにコピーすることを指定します。これにより、このポリシーが IPv4 だけに適用されます。 • **vrf** キーワードは、multi-AF VRF 設定にアップグレードする VRF を指定します。 • *vrf-name* 引数は、multi-AF VRF 設定にアップグレードする単一プロトコル VRF の名前です。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Device(config)# exit`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config vrf** [*vrf-name*] 例： `Device# show running-config vrf vpn4`	特定の VRF インスタンスにリンクしているか、またはデバイス上で設定済みの VRF すべてにリンクしているデバイスの実行コンフィギュレーションに対してサブセットを表示します。 • *vrf-name* 引数は、コンフィギュレーションを表示する VRF の名前です。 （注） マルチプロトコル VRF コマンドをサポートしている Cisco ソフトウェアイメージが、**show running-config vrf** コマンドをサポートしていない場合があります。その場合は、代わりに **show running-config** コマンドを使用できます。

IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI の設定例

例：マルチプロトコル VRF 設定、非共通ポリシーを持つ単一プロトコル

次に、address-family 設定に route-target ポリシーを持つ単一プロトコル（IPv4）用のマルチプロトコル Virtual Routing and Forwarding（VRF）設定の例を示します。

```
vrf definition vrf2
 rd 2:2
 !
 address-family ipv4
 route-target export 2:2
 route-target import 2:2
 exit-address-family
```

RD（2:2）は、VRF vrf2 に定義されたすべてのアドレス ファミリに適用されます。

例：マルチプロトコル VRF 設定、非共通ポリシーを持つマルチプロトコル

次に、route-target ポリシーが別々の address-family 設定で定義されている、IPv4 および IPv6 バーチャル プライベート ネットワーク（VPN）用のマルチプロトコル Virtual Routing and Forwarding（VRF）設定の例を示します。

```
vrf definition vrf2
 rd 2:2
 !
 address-family ipv4
 route-target export 2:2
 route-target import 2:2
 exit-address-family
 !
 address-family ipv6
 route-target export 3:3
 route-target import 3:3
 exit-address-family
```

例：マルチプロトコル VRF 設定、共通ポリシーを持つマルチプロトコル

次に、Virtual Routing and Forwarding（VRF）のグローバル部分に route-target ポリシーが定義された、IPv4 および IPv6 バーチャル プライベート ネットワーク（VPN）用のマルチプロトコル VRF 設定の例を示します。

```
vrf definition vrf2
 rd 2:2
 route-target export 2:2
 route-target import 2:2
  !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
```

route-target ポリシーは、address-family 設定の外部に定義されています。したがって、ポリシーは、VRF vrf2 に定義されたすべてのアドレス ファミリに適用されます。

例：マルチプロトコル VRF 設定、共通ポリシーと非共通ポリシーを持つマルチプロトコル

次に、グローバルおよびアドレス ファミリ エリアの両方で route-target ポリシーが定義されている、マルチプロトコル Virtual Routing and Forwarding（VRF）設定の例を示します。

- IPv6 では、アドレス ファミリの下に route-target 定義が定義されています。これらの定義が使用され、グローバル領域の route-target 定義は無視されます。したがって、IPv6 バーチャル プライベート ネットワーク（VPN）では、インポート 100:2 は無視されます。

- IPv4 では、アドレス ファミリの下に route-target ポリシーは定義されていないため、グローバル定義が使用されます。

```
vrf definition vfr1
 route-target export 100:1
 route-target import 100:1
 route-target import 100:2
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 route-target export 100:1
 route-target import 100:1
 route-target import 100:3
 exit-address-family
```

例：IPv4 および IPv6 VPN 用の VRF の設定

次に、IPv4 および IPv6 バーチャル プライベート ネットワーク（VPN）の Virtual Routing and Forwarding（VRF）インスタンスを設定する例を示します。

```
configure terminal
!
vrf definition vrf1
 rd 100:1
!
 address-family ipv4
 route-target both 100:2
 exit-address-family
!
 address-family ipv6
 route-target both 100:3
 exit-address-family
```

この例では、非共通ポリシーが address family 設定に定義されています。

次に、VRF 設定のグローバル部分に共通ポリシーが定義されている IPv4 および IPv6 用の VRF の例を示します。

```
configure terminal
!
vrf definition vrf2
 rd 200:1
 route-target both 200:2
!
 address-family ipv4
 exit-address-family
!
 address-family ipv6
 exit-address-family
 end
```

例：マルチプロトコル VRF とインターフェイスの関連付け

次の例は、マルチプロトコル Virtual Routing and Forwarding（VRF）インスタンスをいインターフェイスに関連付ける方法を示します。

```
configure terminal
```

```
!
interface Ethernet 0/1
 vrf forwarding vrf1
 ip address 10.24.24.24 255.255.255.255
 ipv6 address 2001:0DB8:0300:0201::/64
 end
```

例：IPv4 だけの単一プロトコル VRF 設定からマルチプロトコル VRF 設定への移行

ここでは、IPv4 だけの単一プロトコル Virtual Routing and Forwarding（VRF）設定からマルチプロトコル VRF 設定に移行する例を示します。

この例は、IPv4 および IPv6 用の VRF CLI をデバイスで実行する前の、IPv4 だけの単一プロトコル VRF を示しています。

```
ip vrf vrf1
 rd 1:1
 route-target both 1:1
interface Loopback1
 ip vrf forwarding V1
 ip address 10.3.3.3 255.255.255.255
```

この例は、単一プロトコル VRF vrf1 からマルチプロトコル VRF 設定への移行を適用する方法を示しています。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
!
Device(config)# vrf upgrade-cli multi-af-mode common-policies vrf vrf1
You are about to upgrade to the multi-AF VRF syntax commands.
You will loose any IPv6 address configured on interfaces
belonging to upgraded VRFs.
Are you sure ? [yes]: yes
Number of VRFs upgraded: 1
Device(config)# exit
```

次に、強制的に移行したあとのマルチプロトコル VRF 設定を示します。

```
vrf definition vrf1
 rd 1:1
 route-target both 1:1
 !
 address-family ipv4
 exit-address-family
!
interface Loopback1
 vrf forwarding V1
 ip address 10.3.3.3 255.255.255.255
```

次に、マルチ AF マルチプロトコル VRF 設定のもう 1 つの例を示します。

```
vrf definition vrf2
 rd 100:1
 address family ipv6
 route-target both 200:1
 exit-address-family
!
ip vrf vrf1
 rd 200:1
 route-target both 200:1
!
interface Ethernet0/0
 vrf forwarding vrf2
```

```
 ip address 10.50.1.2 255.255.255.0
 ipv6 address 2001:0DB8:0:1::/64
!
interface Ethernet0/1
 ip vrf forwarding vrf1
 ip address 10.60.1.2 255.255.255.0
 ipv6 address 2001:0DB8:1 :1::/64
```

この例では、インターフェイス Ethernet0/0 に対して定義されているすべてのアドレス（IPv4 および IPv6）が VRF vrf2 にあります。インターフェイス Ethernet0/1 で、IPv4 アドレスは VRF vrf1 で定義されていますが、IPv6 アドレスはグローバル IPv6 ルーティング テーブルにあります。

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 Master Command List, All Releases』
MPLS と MPLS アプリケーション コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』

標準および RFC

標準/RFC	Title
RFC 1771	『*A Border Gateway Protocol 4 (BGP-4)*』
RFC 4364	『*BGP MPLS/IP Virtual Private Networks (VPNs)*』

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。	http://www.cisco.com/cisco/web/support/index.html

IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI 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 に移動します。Cisco.com のアカウントは必要ありません。

表 *17*：*IPv4* および *IPv6 VPN* 用 *MPLS VPN VRF CLI* の機能情報

機能名	リリース	機能情報
IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI	12.2(33)SB 12.2(33)SRB 12.2(33)SXI 12.4(20)T Cisco IOS XE Release 3.1S	このマニュアルでは、IPv4 および IPv6 VPN 用のマルチプロトコル バーチャル プライベートネットワーク（VPN）ルーティング/転送（VRF）インスタンスの設定方法、および既存の IPv4 だけの単一プロトコル VRF をマルチプロトコル VRF 設定にアップグレードする方法について説明します。 IPv4 および IPv6 VPN 用 MPLS VPN VRF CLI の機能によって、同じマルチプロトコル ラベル スイッチング（MPLS）VRF 設定で IPv4 および IPv6 VPN を有効にし、単一プロトコル VRF 設定からマルチプロトコル VRF 設定への移行を簡単に実行できる Cisco IOS コマンドライン インターフェイス（CLI）コマンドが導入されます。 この機能は、Cisco IOS Release 12.2(33)SB で Cisco 10000 シリーズ ルータに追加されました。 この機能は、Cisco IOS Release 12.2(33)SRB で Cisco 7600 シリーズ ルータに実装されました。 この機能は、Cisco IOS Release 12.2(33)SXI で統合されました。 この機能は、Cisco IOS Release 12.4(2)T で統合されました。 Cisco IOS XE Release 3.1S では、この機能は Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに実装されました。

機能名	リリース	機能情報
		次のコマンドが導入または変更されました：**show vrf**、**vrf definition**、**vrf forwarding**、**vrf upgrade-cli**。

用語集

6PE：IPv6 プロバイダー エッジ デバイス、または IPv6 を使用するマルチプロトコル ラベル スイッチング（MPLS）ラベル スイッチング ルータ（LSR）エッジ ルータ。

6VPE：IPv6 バーチャル プライベート ネットワーク（VPN）プロバイダー エッジ デバイス。

AF：Address Family（アドレス ファミリ）。すべてのメンバが共通のアドレッシング メカニズムを使用してエンドポイントを識別する、関連通信プロトコルのセット。プロトコル ファミリとも呼ばれます。

AFIAddress Family Identifier（アドレス ファミリ識別子）。ネットワーク アドレスに関連付けられたネットワーク層プロトコルの ID を示します。

BGP：Border Gateway Protocol（ボーダー ゲートウェイ プロトコル）。自律システム間で使用されるルーティングプロトコル。このルーティングプロトコルによってインターネットが実現されています。BGP はディスタンスベクトルルーティング プロトコルであり、接続性情報および追加の BGP 属性のセットを伝送します。これらの属性により、特定の宛先に到達するために使用する最善のルートを特定するための一連のポリシーが可能になります。BGP は RFC 1771 で定義されています。

CE：カスタマーエッジデバイス。バーチャルプライベートネットワーク（VPN）カスタマー サイトに接続するサービス プロバイダー デバイス。

FIBForwarding Information Base（転送情報ベース）。データ パケットのスイッチングに関するこの情報が格納されたデータベース。FIB は、ルーティング情報ベース（RIB）の情報に基づいています。転送用にラインカードにインストールされている、選択されたルートの最適なセットです。

HA：High Availability（ハイ アベイラビリティ）。ハイ アベイラビリティは、システムが継続的に動作することとして定義されます。システムが使用可能であるためには、アプリケーション サーバ、データベース サーバ、記憶装置、エンドツーエンド ネットワークを含むすべてのコンポーネントが継続的にサービスを提供する必要があります。

IP：Internet Protocol（インターネット プロトコル）。TCP/IP スタックにおいてコネクションレス型のネットワーク間サービスを提供するネットワーク層プロトコル。IP では、アドレッシング、タイプ オブ サービス指定、フラグメンテーションと再編成、セキュリティなどの機能が提供されます。

IPv4：IP バージョン 4。TCP/IP プロトコル スイートのネットワーク層。IPv4 はコネクションレス型のベスト エフォート パケット スイッチング プロトコルです。

IPv6：IP バージョン 6。IPv4 の代替バージョン。IPv6 は、次世代の IP プロトコルです。IPv6 は IPv4 と下位互換性があり、データ セキュリティや最大ユーザ アドレス数などの IPv4 の弱点を克服できるように設計されています。IPv6 によってアドレス空間が 32 ビットから 128 ビットに広がるため、利用可能なネットワークやシステムの数に実質的に制限がなくなります。また、リアルタイムの音声やビデオのために、Quality of Service（QoS）パラメータもサポートされています。

MFI：MPLS Forwarding Infrastructure。シスコの MPLS サブシステムでは、着信ラベルと発信ラベル、およびそれらのラベルに関連する対応パケットに関する情報を保存するための、ラベル付けに適したデータ構造を指します。

MPLS：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。MPLS は、ネットワークを通してパケット（フレーム）を転送するための方式です。ネットワークのエッジにあるデバイスがラベルをパケット（フレーム）に適用できるようにします。ネットワーク コア内の ATM スイッチまたは既存のデバイスは、最小限のルックアップ オーバーヘッドでラベルに従ってパケットを切り替えることができます。

PE：プロバイダー エッジ デバイス。サービス プロバイダーのネットワークの一部であり、カスタマー エッジ（CE）デバイスに接続されたデバイス。PE デバイス機能は、MLS エッジ ラベル スイッチング ルータ（LSR）の機能と、バーチャル プライベート ネットワーク（VPN）をサポートするためのいくつかの追加機能を組み合わせたものです。

RD（IPv4）：Route Distinguisher（ルート識別子）。IPv4 プレフィックスに連結される 8 バイトの値で、一意の VPN IPv4（VPNv4）プレフィックスを形成します。

RD（IPv6）：Route Distinguisher（ルート識別子）。IPv6 プレフィックスの先頭に付加される 64 ビットの値で、グローバルに一意な VPN-IPv6 アドレスを形成します。

RIB：ルーティング情報ベース。転送情報ベース（FIB）の選択元である、すべての使用可能なルートのセット。基本的に、RIB には、選択できる使用可能なすべてのルートが含まれています。これは、ダイナミック ルーティング プロトコルによって学習されたすべてのルート、すべての直接接続されているネットワーク（つまり、特定のデバイスのインターフェイスが接続されているネットワーク）、およびスタティック ルートなどのその他の設定されているすべてのルートを合せたものです。

RT：Route Target（ルート ターゲット）。プレフィックスがインポートされるバーチャル プライベート ネットワーク（VPN）ルーティング/転送（VRF）ルーティング テーブルを識別するために使用される拡張コミュニティ属性。

VPN：Virtual Private Network（バーチャル プライベート ネットワーク）。ネットワーク間のトラフィックをすべて暗号化することにより、パブリック TCP/IP ネットワーク経由でも IP トラフィックをセキュアに転送できます。VPN は「トンネリング」を使用して、IP レベルですべての情報を暗号化します。

VRF：バーチャル プライベート ネットワーク（VPN）Routing and Forwarding（VPN ルーティングおよび転送）インスタンス。VRF は、IP ルーティング テーブル、取得されたルーティング テーブル、そのルーティング テーブルを使用する一連のインターフェイス、ルーティング テーブルに登録されるものを決定する一連のルールおよびルーティング プロトコルで構成されています。一般に、VRF には、PE デバイスに付加される顧客 VPN サイトが定義されたルーティング情報が格納されています。

VRF テーブル：バーチャル プライベート ネットワーク（VPN）ルーティング/転送（VRF）インスタンスに関連付けられたルーティングおよび転送テーブル。これはカスタマー固有のテーブルであり、これによりプロバイダー エッジ（PE）デバイスは各カスタマーに対して独立したルーティング状態を維持できます。

第 18 章

MPLS over GRE

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。この機能は、MPLS over Generic Routing Encapsulation（MPLSoGRE）を使用して、MPLS パケットを IP トンネルの内部にカプセル化します。IP トンネル内の MPLS パケットのカプセル化は、非 MPLS ネットワーク上でのポイントツーポイント リンクを作成します。

- 機能情報の確認，307 ページ
- MPLS VPN L3VPN over GRE の前提条件，308 ページ
- MPLS VPN L3VPN over GRE の制約事項，308 ページ
- MPLS VPN L3VPN over GRE に関する情報，308 ページ
- MPLS VPN L3VPN over GRE の設定方法，311 ページ
- MPLS VPN L3VPN over GRE の設定例，313 ページ
- その他の参考資料，314 ページ
- MPLS VPN L3VPN over GRE の機能情報，315 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 に移動します。Cisco.com のアカウントは必要ありません。

MPLS VPN L3VPN over GRE 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）が設定され正常に動作していることを確認します。
- PE-to-PE トンネリングでは、Cisco IOS Release 15.2(1)S よりも前のリリースを実行している場合は、同じ送信元アドレスのトンネルを設定します。
- PE-to-PE トンネリングでは、同じ宛先アドレスでトンネルを設定します。
- 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。
  - 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。
- GRE トンネルを設定する前に、IP アドレスを持つループバック インターフェイス（VRF に接続されていないインターフェイス）を設定し、内部的に作成されたトンネルインターフェイスが、このダミー ループバック インターフェイスに対して自身を番号なしに設定することで、IPv4 フォワーディングで有効になるようにします。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。

MPLS VPN L3VPN over GRE の制約事項

MPLS VPN L3VPN over GRE 機能では、次のものはサポートされません。

- トンネル インターフェイスで設定された Quality of Service（QoS）サービス ポリシー。物理またはサブフェイスではサポートされます。
- GRE オプション：シーケンス、チェックサム、およびソース ルート。
- IPv6 Generic Routing Encapsulation（GRE）。
- Carrier Supporting Carrier（CSC）や相互自律システム（Inter-AS）などの拡張機能。

MPLS VPN L3VPN over GRE に関する情報

MPLS VPN L3VPN over GRE の概要

MPLS VPN L3VPN 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。

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）。

下図に示すように、PE デバイスは、Virtual Routing and Forwarding（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。

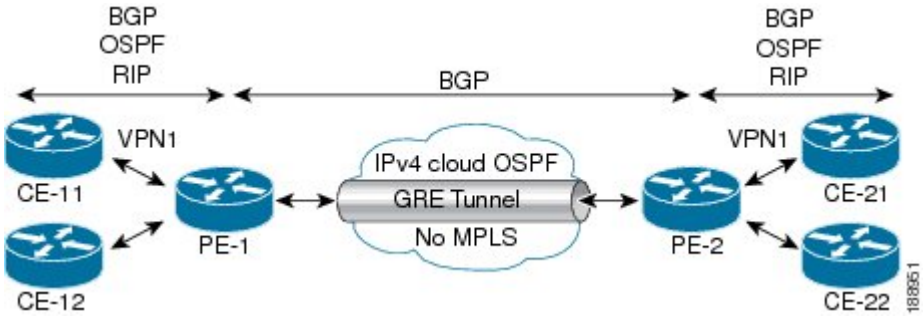
非 MPLS ネットワークのいずれかの側にある PE デバイスは、（非 MPLS ネットワーク内で動作している）ルーティング プロトコルを使用して、非MPLS ネットワークのもう一方の側にある PE デバイスについて学習します。PE デバイス間に確立された学習ルートは、メインまたはデフォルトのルーティング テーブルに格納されます。

反対方向の PE デバイスは、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。

次の図は、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。

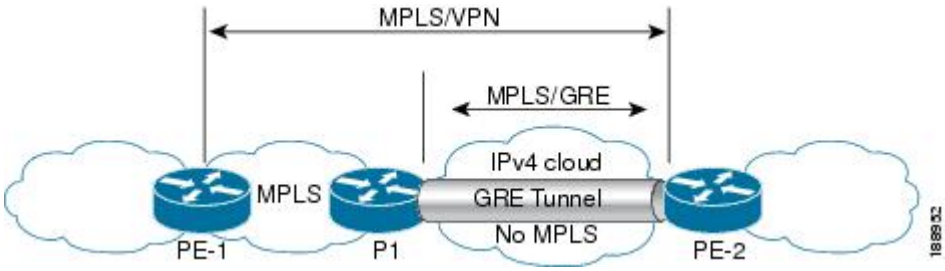
図 *20*：*PE-to-PE* トンネリング



P-to-PE トンネリング

下図に示すように、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 *21*：*P-to-PE* トンネリング

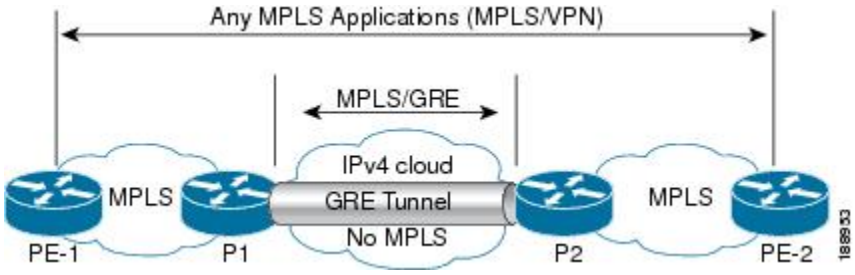


P-to-P トンネリング

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 *22*：***P-to-P*** トンネリング



MPLS VPN L3VPN over GRE の設定方法

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。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface tunnel***tunnel-number*
4. **ip address***ip-address mask*
5. **tunnel source***source-address*
6. **tunnel destination***destination-address*
7. **mpls ip**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • 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	**configure terminal** 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	**interface tunnel***tunnel-number* 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	**ip address***ip-address mask* 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。
ステップ 5	**tunnel source***source-address* 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	**tunnel destination***destination-address* 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	**mpls ip** 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	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

MPLS VPN L3VPN over GRE の設定例

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GREトンネルの設定例を示します。次に、トンネルの両側のプロバイダー エッジ（PE）デバイス（PE1 および PE2）でのトンネルの設定例を示します。

PE1 の設定

```
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)# mpls ip
```

PE2 の設定

```
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)# mpls ip
```

例：MPLS VPN L3VPN over GRE を使用した MPLS の設定

次に、非 MPLS ネットワークにまたがる Generic Routing Encapsulation（GRE）トンネルを使用する基本的なマルチプロトコル ラベル スイッチング（MPLS）設定の例を示します。この例は、上記の最初の図に示されている設定に似ています。

PE1 の設定

```
!
mpls ip
!
ip vrf vpn1
rd 100:1
route-target import 100:1
route-target export 100:1
!
 interface loopback 0
 ip address 10.2.2.2 255.255.255.255
!
 interface GigabitEthernet 0/1/2
 ip address 10.1.1.1 255.255.255.0
!
 interface Tunnel 1
 ip address 10.0.0.1 255.255.255.0
 tunnel source 10.1.1.1
 tunnel destination 10.1.1.2
 mpls ip
!
 interface GigabitEthernet 0/1/3
```

```
 ip vrf forwarding vpn1
 ip address 10.10.0.1 255.255.255.0
!
router bgp 100
neighbor 10.5.5.5 remote-as 100
neighbor 10.5.5.5 update-source loopback0
!
address-family vpnv4
neighbor 10.5.5.5 activate
neighbor 10.5.5.5 send community-extended
!
address-family ipv4 vrf vpn1
neighbor 10.10.0.2 remote-as 20
neighbor 10.10.0.2 activate
!
```

PE2 の設定

```
!
mpls ip
!
ip vrf vpn1
rd 100:1
route-target import 100:1
route-target export 100:1
!
 interface loopback 0
 ip address 10.5.5.5 255.255.255.255
!
 interface GigabitEthernet 0/1/1
 ip address 10.1.1.2 255.255.255.0
!
 interface Tunnel 1
 ip address 10.0.0.2 255.255.255.0
 tunnel source 10.1.1.2
 tunnel destination 10.1.1.1
 mpls ip
!
 interface GigabitEthernet 0/0/5
 ip vrf forwarding vpn1
 ip address 10.1.2.1 255.255.255.0
!
router bgp 100
neighbor 10.2.2.2 remote-as 100
neighbor 10.2.2.2 update-source loopback0
!
address-family vpnv4
neighbor 10.2.2.2 activate
neighbor 10.2.2.2 send community-extended
!
address-family ipv4 vrf vpn1
neighbor 10.1.2.2 remote-as 30
neighbor 10.1.2.2 activate
!
```

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 Command List, All Releases』

関連項目	マニュアル タイトル
マルチプロトコル ラベル スイッチング（MPLS）コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』
Multiprotocol Border Gateway Protocol（MP-BGP）に対応した MPLS VPN ネットワークの設定	「Multiprotocol BGP MPLS VPN」モジュール
ラベル配布プロトコル	『*MPLS Label Distribution Protocol Configuration Guide*』の「Label Distribution Protocol」モジュール
L3 VPN over mGRE トンネルの設定	『Dynamic Layer3 VPNs with Multipoint GRE Tunnels』モジュール

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。	http://www.cisco.com/cisco/web/support/index.html

MPLS VPN L3VPN 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 に移動します。Cisco.com のアカウントは必要ありません。

表 *18*：*MPLS VPN L3VPN over GRE* の機能情報

機能名	リリース	機能情報
MPLS VPN L3VPN over GRE 機能	12.0(22)S 12.0(26)S 12.2(33)SRE 15.0(1)S 15.2(1)S 15.2(4)S Cisco IOS XE Release 2.1	MPLS VPN L3VPN 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。 ご使用のリリースによっては、PE 間トンネル設定で同じ送信元アドレスを使用してトンネルを設定できます。 追加または変更されたコマンドはありません。

第 19 章

IP トンネルを介した MPLS VPN 6VPE サポート

この機能では、IPv4 Generic Routing Encapsulation（GRE）トンネルを使用して、Border Gateway Protocol（BGP）ネクスト ホップに到達するための IPv6 バーチャル プライベート ネットワーク（VPN）over マルチプロトコル ラベル スイッチング（MPLS）機能を提供できます。

- 機能情報の確認，317 ページ
- IP トンネルを介した MPLS VPN 6VPE のサポートに関する情報，318 ページ
- その他の参考資料，319 ページ
- IP トンネルを介した MPLS VPN 6VPE サポートの機能情報，320 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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 に移動します。Cisco.com のアカウントは必要ありません。

IP トンネルを介した MPLS VPN 6VPE のサポートに関する情報

MPLS 転送

1 つのカスタマー サイトから IPv6 トラフィックを受信すると、入力プロバイダー エッジ（PE）デバイスはマルチプロトコル ラベル スイッチング（MPLS）を使用して、Border Gateway Protocol（BGP）ネクストホップとして識別された出力 PE デバイスに向けて、バックボーンを介して IPv6 バーチャル プライベート ネットワーク（VPN）パケットをトンネリングします。入力 PE デバイスは、一般的に IPv6 パケットの先頭に外部ラベルおよび内部ラベルを付加してから、出力インターフェイスにパケットを渡します。

通常の動作では、転送パス上のプロバイダー（P）デバイスは最初のラベルの先にあるフレームの内部を調べません。プロバイダー（P）デバイスは着信ラベルを発信ラベルと交換するか、または次のデバイスが PE デバイスの場合には着信ラベルを削除します。着信ラベルの削除は、最後から 2 番めのホップのポッピングと呼ばれます。残りのラベル（BGP ラベル）は、カスタマー サイトへの出力 PE インターフェイスを識別するために使用されます。また、ラベルは、最後の P デバイスからプロトコル バージョン（IPv6）を隠します。そうしない場合、IPv6 パケットを転送することが必要になります。

P デバイスは IPv6 VPN ルートを知りません。IPv6 ヘッダーは 1 つ以上の MPLS ラベルの下に隠されたままになります。P デバイスで、送達できない MPLS カプセル化 IPv6 パケットを受信した場合のオプションは 2 つあります。P デバイスが IPv6 対応の場合、IPv6 ヘッダーを公開し、IPv6 メッセージ用のインターネット制御メッセージプロトコル（ICMP）を構築して、MPLS カプセル化メッセージを元のパケットの送信元に送信します。P デバイスが IPv6 対応でない場合、パケットをドロップします。

GRE トンネルを介した 6VPE

一部のシスコ ソフトウェア リリースでは、入力プロバイダー エッジ（PE）デバイスが IPv4 総称ルーティング カプセル化（GRE）トンネルと、マルチプロトコル ラベル スイッチング（MPLS）上の IPv6 over MPLS（6VPE）を組み合わせて使用して、Border Gateway Protocol（BGP）ネクストホップとして識別された出力 PE デバイスに向けて、バックボーンを介して IPv6 バーチャル プライベート ネットワーク（VPN）パケットをトンネリングします。

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 Master Command List, All Releases』
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide Library*』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『IPv6 Feature Mapping』

標準および RFC

標準/RFC	Title
IPv6 に関する RFC	IPv6 の RFC

シスコのテクニカル サポート

説明	Link
★枠で囲まれた Technical Assistance の場合★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。	http://www.cisco.com/cisco/web/support/index.html

IP トンネルを介した MPLS VPN 6VPE サポートの機能情報

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 に移動します。Cisco.com のアカウントは必要ありません。

表 *19*：*IP* トンネルを介した *MPLS VPN 6VPE* サポートの機能情報

機能名	リリース	機能情報
IP トンネルを介した MPLS VPN 6VPE サポート	12.2(33)SRB1 12.2(33)SXI Cisco IOS XE Release 3.1S	この機能では、IPv4 GRE トンネルを使用して、BGP ネクスト ホップに到達するための IPv6 VPN over MPLS 機能を提供できます。

第 20 章

IPv6 VRF 認識システム メッセージ ロギング

IPv6 VRF 認識システム メッセージのロギング機能は、デバイスが VPN ルーティングおよび転送（VRF）インターフェイスを介して接続されている IPv6 対応の syslog サーバにシステム ロギング（syslog）メッセージを送信できるようにします。ロギング情報は、ネットワークのモニタリングとトラブルシューティングに使用できます。本機能は、VRF を通じて接続されたネットワーク トラフィックにこの機能を拡張します。

- 機能情報の確認，321 ページ
- IPv6 VRF 認識システム メッセージ ロギングの前提条件，322 ページ
- IPv6 VRF 認識システム メッセージ ロギングの制約事項，322 ページ
- IPv6 VRF 認識システム メッセージ ロギングに関する情報，322 ページ
- IPv6 VRF 認識システム メッセージ ロギングの設定方法，325 ページ
- IPv6 VRF 認識システム メッセージ ロギングの設定例，330 ページ
- IPv6 VRF 認識システム メッセージ ロギングのその他の参考資料，331 ページ
- IPv6 VRF 認識システム メッセージ ロギングの機能情報，332 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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 に移動します。Cisco.com のアカウントは必要ありません。

IPv6 VRF 認識システム メッセージ ロギングの前提条件

IPv6 VPN ルーティングおよび転送（VRF）認識システム メッセージ ロギング機能を設定する前に、ルーティング デバイスで VRF インスタンスを設定し、VRF をインターフェイスに関連付ける必要があります。

IPv6 VRF 認識システム メッセージ ロギングの制約事項

Virtual Routing and Forwarding（VRF）システム ロギング メッセージの送信元アドレスを指定することはできません。IPv6 VRF 認識システム メッセージ ロギング機能は、すべての VRF 認識システム ロギング メッセージについて、送信元アドレスとして VRF インターフェイス アドレスを使用します。

IPv6 VRF 認識システム メッセージ ロギングに関する情報

VRF 認識システム メッセージ ロギングの利点

VPN ルーティングおよび転送（VRF）インスタンスは、IP ルーティングの拡張機能で、複数のルーティング インスタンスを提供します。VRF は、各 VPN に個別の IP ルーティングおよび転送テーブルを提供します。VRF 認識システム メッセージ ロギング機能を設定する前に、ルーティング デバイスで VRF を設定する必要があります。

ルーティング デバイスで VRF 認識システム メッセージ ロギング機能を設定した後、デバイスは VRF インターフェイスを通じて syslog ホストにシステム ロギング（syslog）メッセージを送信できます。その後、ロギング メッセージを使用して、VRF で接続されたネットワーク トラフィックの監視とトラブルシューティングを行うことができます。VRF 認識システム メッセージ ロギング機能がルーティング デバイスで設定されていない場合、ルーティング デバイスは、グローバル ルーティング テーブルのみを通じて syslog ホストに syslog メッセージを送信します。

VRF が設定された以下の任意のデバイス上で、VRF インターフェイスを通じてシステム ロギング メッセージを受信できます。

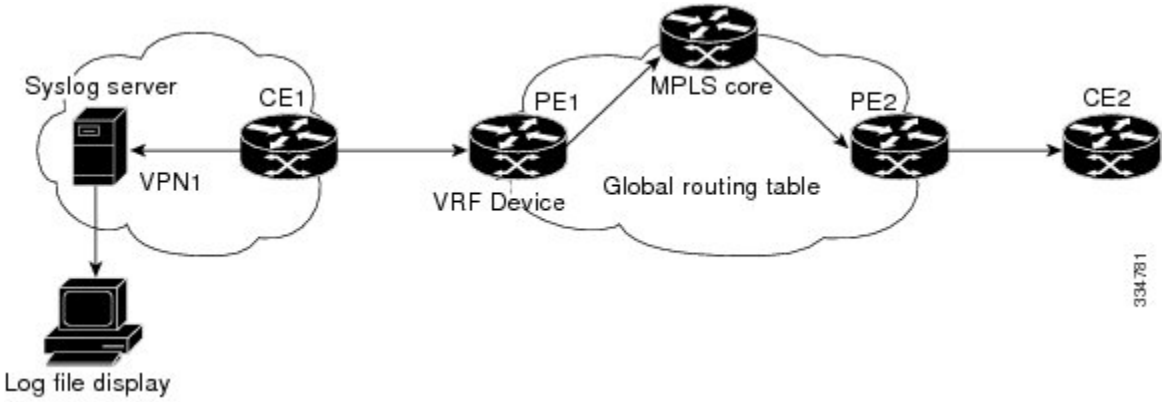
- レイヤ 3 MPLS VPN ネットワーク サービスを提供するために、マルチプロトコル ラベル スイッチング（MPLS）およびマルチプロトコル ボーダー ゲートウェイ プロトコル（BGP）と共に使用されているプロバイダー エッジ（PE）デバイス。
- マルチプロトコル BGP を使用しない VRF 実装である VRF-Lite 用に設定されたカスタマー エッジ（CE）デバイス。

MPLS VPN ネットワーク内のプロバイダー エッジ デバイス上の VRF 認識システム メッセージ ロギング

レイヤ 3 マルチプロトコル ラベル スイッチング（MPLS）VPN ネットワーク内のプロバイダー エッジ（PE）デバイスで、VRF 認識システム メッセージ ロギング機能を設定できます。PE デバイスは、VPN ルーティングおよび転送（VRF）インターフェイスを通じて、VPN 内にある 1 台の syslog サーバに、システム ロギング（syslog）メッセージを送信できます。

次の図は、MPLS VPN ネットワークと、VRF VPN1 に関連付けられている PE デバイスで設定されている VRF 認識システム メッセージ ロギング機能を示します。PE デバイスは、VRF インターフェイスを通じて、VPN1 にある syslog サーバにログ メッセージを送信します。端末上で syslog サーバからのメッセージを表示できます。

図 *23*：*MPLS VPN* と、プロバイダー エッジ デバイス上で設定された *VRF* 認識システム メッセージ ロギング



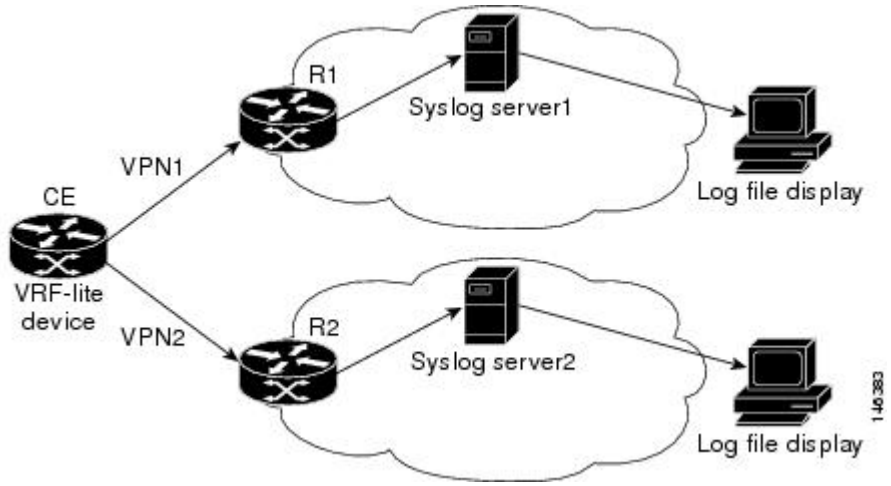
VRF-Lite が設定されたカスタマー エッジ デバイスでの VRF 認識システム メッセージ ロギング

VRF-Lite 機能が設定されたカスタマー エッジ（CE）デバイスで、VRF 認識システム メッセージ ロギング機能を設定できます。CE デバイスは、VPN ルーティングおよび転送（VRF）インターフェイスを通じて、複数の VPN の syslog サーバに、システム ロギング（syslog）メッセージを送信できます。CE デバイスは、ルータまたはスイッチのいずれかです。

次の図は、VRF-Lite CE デバイス上で設定された VRF 認識システム メッセージ ロギング機能を示します。CE デバイスは、VPN1 ネットワークまたは VPN2 ネットワーク内の syslog サーバか、VPN1 ネットワークと VPN2 ネットワークの両方のサーバに VRF syslog メッセージを送信できま

す。1 台の VRF-Lite CE デバイスで複数の VRF を設定でき、デバイスは多数の顧客にサービスを提供できます。

図 *24*：***VRF-Lite*** カスタマー エッジ デバイス上で設定された ***VRF*** システム メッセージ ロギング



ロギング コマンドのメッセージ レベル

VRF 認識システム メッセージ ロギング機能を設定するときに使用できる **logging** コマンドのメッセージ レベルの一覧を次の表に示します。この表に記載されている情報には、キーワード レベル名と番号、その説明、関連付けられている syslog 定義が含まれています。**logging trap***level* および **logging buffered***severity-level* コマンドでは、レベル名とレベル番号のいずれかを使用できます。

表 *20*：***logging*** コマンドのメッセージ レベル

重大度の名前	レベル番号	説明	**syslog** 定義
emergencies	**0**	システムが使用不可	LOG_EMERG
alerts	**1**	即時処理が必要	LOG_ALERT
critical	**2**	クリティカルな状態	LOG_CRIT
errors	**3**	エラー状態	LOG_ERR
warnings	**4**	警告状態	LOG_WARNING
通知	**5**	正常だが注意を要する状態	LOG_NOTICE
informational	**6**	情報メッセージだけ	LOG_INFO

重大度の名前	レベル番号	説明	syslog 定義
debugging	**7**	デバッグ メッセージ	LOG_DEBUG

IPv6 VRF 認識システム メッセージ ロギングの設定方法

ルーティング デバイスでの VRF の設定

ルーティングデバイスでVPNルーティングおよび転送（VRF）インスタンスを設定すると、VPNへのカスタマーの接続が実現します。ルーティング デバイスとして、マルチプロトコル ラベル スイッチング（MPLS）VPNネットワークに接続するプロバイダーエッジ（PE）、またはVRF-Liteに対応して設定されているカスタマー エッジ（CE）デバイスを使用できます。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **vrf definition***vrf-name*
4. **address-family ipv6**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**vrf definition***vrf-name* 例： `Device (config)# vrf definition vpn1`	VRF インスタンスを定義し、VRF コンフィギュレーション モードを開始します。 • *vrf-name* 引数は、VRF に割り当てられている名前です。

	コマンドまたはアクション	目的
ステップ 4	**address-family ipv6** 例： `Device(config-vrf)# address-family ipv6`	定義されている VRF の IPv6 アドレス ファミリを有効にし、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。
ステップ 5	**end** 例： `Device(config-vrf-af)# end`	アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

VRF とインターフェイスの関連付け

VPN ルーティングおよび転送（VRF）インスタンスを設定してインターフェイスに関連付けたら、ルーティング デバイスで VRF 認識システム メッセージ ロギング機能を設定できます。

（注） VRF システム ロギング メッセージの発信元アドレスは設定できません。VRF 認識システム メッセージ ロギング機能は、すべての VRF 認識システム ロギング メッセージの発信元アドレスとして VRF インターフェイス アドレスを使用します。

はじめる前に

VPN トラフィックを転送する前に、VRF がインターフェイスに関連付けられている必要があります。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***typenumber*
4. **vrf forwarding***vrf-name*
5. **no ipv6 address**
6. **ipv6 address***address.prefix*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	例： `Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**interface***typenumber* 例： `Device (config)# interface FastEthernet 0/0/0`	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。 • *type* 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。 • *number* 引数で、ポート、コネクタ、またはインターフェイス カードの番号を指定します。この番号は、インストール時に工場で割り当てられるか、またはポート、コネクタやインターフェイス カードをシステムに追加するときに割り当てられます。使用可能なインターフェイスを確認するには、特権 EXEC モードで **show interfaces** コマンドを使用します。
ステップ 4	**vrf forwarding***vrf-name* 例： `Device(config-if)# vrf forwarding vpn1`	VRF をインターフェイスまたはサブインターフェイスと関連付けます。 • *vrf-name* 引数は、インターフェイスを指定された VRF に関連付けます。
ステップ 5	**no ipv6 address** 例： `Device(config-if)# no ipv6 address`	インターフェイスに設定されている既存の IPv6 アドレスを削除します。
ステップ 6	**ipv6 address***address.prefix* 例： `Device(config-if)# ipv6 address 2001:DB8::1/32`	インターフェイスの IPv6 アドレスを割り当てます。
ステップ 7	**end** 例： `Device(config-if)# end`	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。

ルーティングデバイスでのロギングの送信元インターフェイスとして VRF を設定

はじめる前に

この作業を実行するには、次に示す作業を実行しておく必要があります。

- ルーティング デバイスで Virtual Routing and Forwarding（VRF）インスタンスを設定します。
- インターフェイスと VRF を関連付けます。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **logging source-interface***interface-typeinterface-number***vrf***vrf-name*
4. **logging host ipv6***ipv6-address***vrf***vrf-name*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	イネーブル化 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 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	**logging source-interface***interface-typeinterface-number***vrf***vrf-name* 例： `Device (config)# logging source-interface FastEthernet 0/0/0 vrf vpn1`	VRF インターフェイスをロギングの送信元インターフェイスとして設定します。
ステップ 4	**logging host ipv6***ipv6-address***vrf***vrf-name* 例： `Device(config)# logging host ipv6 2001:DB8:: vrf vpn1`	IPv6 対応ロギング ホストを設定し、 VRF に関連付けます。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config)# end`	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。

IPv6 VRF 認識システム メッセージ ロギングの確認

手順の概要

1. イネーブル化
2. **show running-config | include logging**
3. **show logging**

手順の詳細

ステップ 1 イネーブル化

特権 EXEC モードをイネーブルにします。

- パスワードを入力します（要求された場合）。

例：
```
Device> enable
```

ステップ 2 **show running-config | include logging**

Virtual Routing and Forwarding（VRF）インスタンスのロギング ホストとデバイスのロギング設定を表示します。

この例は、サーバ ホスト アドレス 10.0.0.3 を使用した VRF syslog での syslog サーバの設定を示しています。

例：
```
Device# show running-config | include logging

logging source-interface Ethernet0/1 vrf syslog
logging host ipv6 2001::DB8:1 vrf syslog
```

ステップ 3 **show logging**

syslog の状態を表示します。

例：
```
Device# show logging

Trap logging: level informational, 138 message lines logged
```

```
Logging to 2001:DB8::1 (v6) (udp port 514, audit disabled,
link up),
24 message lines logged,
0 message lines rate-limited,
0 message lines dropped-by-MD,
xml disabled, sequence number disabled
filtering disabled
Logging to 2001:DB8::1 (syslog) (udp port 514,
audit disabled,
link up),
4 message lines logged,
0 message lines rate-limited,
0 message lines dropped-by-MD,
xml disabled, sequence number disabled
filtering disabled
Logging Source-Interface: VRF Name:
GigabitEthernet0/0/0 syslog
```

IPv6 VRF 認識システム メッセージ ロギングの設定例

例：ルーティング デバイスでの VRF の設定

```
Device> enable
Device# configure terminal
Device(config)# vrf definition syslog_v6
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# end
```

例：VRF とインターフェイスの関連付け

```
Device> enable
Device# configure terminal
Device(config)# interface FastEthernet 0/0/0
Device(config-if)# vrf forwarding vpn1
Device(config-if)# no ipv6 address
Device(config-if)# ipv6 address 2001:DB8::1/32
Device(config-if)# end
```

例：ルーティングデバイス上でのロギングの送信元インターフェイスとしての VRF の設定

```
Device> enable
Device# configure terminal
Device(config)# logging source-interface FastEthernet 0/0/0 vrf vpn1
Device(config)# logging host ipv6 address 2001:DB8::1 vrf vpn1
Device(config)# end
```

IPv6 VRF 認識システム メッセージ ロギングのその他の参考資料

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 と MPLS アプリケーション コマンド	『Cisco IOS Multiprotocol Label Switching Command Reference』
Catalyst 4500 スイッチでの VRF-Lite 設定の概念とタスク	『*Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*』の「Configuring VRF-lite」の章
ML シリーズ イーサネット カードでの VRF Lite 設定の概念とタスク	『*Ethernet Card Software Feature and Configuration Guide*』の「Configuring VRF-lite」の章（Cisco ONS 15454 SDH、ONS 15454、および ONS 15327）

シスコのテクニカル サポート

説明	Link
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。 お使いの製品のセキュリティ情報や技術情報を入手するために、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。 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。	http://www.cisco.com/cisco/web/support/index.html

IPv6 VRF 認識システム メッセージ ロギングの機能情報

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。

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 に移動します。Cisco.com のアカウントは必要ありません。

表 *21*：*IPv6 VRF* 認識システム メッセージ ロギングの機能情報

機能名	リリース	機能情報
IPv6 VRF 認識システム メッセージ ロギング		IPv6 VRF 認識システム メッセージのロギング機能は、デバイスが VPN ルーティングおよび転送（VRF）インターフェイスを介して接続されている IPv6 対応の syslog サーバにシステム ロギング（syslog）メッセージを送信できるようにします。ロギング情報は、ネットワークのモニタリングとトラブルシューティングに使用できます。本機能は、VRF を通じて接続されたネットワーク トラフィックにこの機能を拡張します。 次のコマンドが変更されました：**logging source-interface** および **logging host**。