IP ルーティング：プロトコル非依存コンフィギュレーションガイド

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)

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

最初にお読みください 1

基本的な IP ルーティング 3

機能情報の確認 3

基本的な IP ルーティングに関する情報 4

可変長サブネット マスク 4

スタティック ルート 4

デフォルト ルート 6

デフォルト ネットワーク 7

ラスト リゾート ゲートウェイ 7

パスの最大数 8

マルチインターフェイスの負荷分散 8

ルーティング情報の再配布 8

サポートされるメトリック変換 9

no redistribute コマンド実装のプロトコルの違い 10

ルーティング情報発信元のフィルタリング 10

認証キー管理およびサポートされるプロトコル 11

基本的な IP ルーティングの設定方法 12

ルーティング情報の再配布 12

再配布ルートの条件の定義 12

ルーティング ドメイン間でのルートの再配布 16

再配布ルートのオプションの削除 17

ルーティング情報のフィルタリングの設定 18

ルーティング アップデートでのルートのアドバタイジングの制御 18

ルーティング アップデートの処理の制御 19

ルーティング情報の送信元のフィルタリング 19

認証キーの管理 19

IP ネットワークのモニタリングおよびメンテナンス 21

IP ルーティング テーブルからのルートの消去 21
システムおよびネットワーク統計情報の表示 21
基本的な IP ルーティングの設定例 22
例：可変長サブネット マスク 22
例：ダイナミック プロトコルによるスタティック ルートの上書き 23
例：IP ルーティングがディセーブルな場合のスタティック IP ネクストホップとしての IP デフォルト ゲートウェイ 23
例：アドミニストレーティブ ディスタンス 24
例：スタティック ルーティングの再配布 25
例：EIGRP 再配布 25
例：EIGRP と RIP 間の相互再配布 26
例：EIGRP と BGP 間の相互再配布 26
例：OSPF ルーティングおよびルート再配布 27
例：基本的な OSPF 設定 27
例：内部デバイス、ABR、および ASBR の設定 29
例：複雑な OSPF 設定 31
例：デフォルト メトリック値の再配布 33
例：ルート マップを使用した場合と使用しない場合の再配布 34
例：キー管理 36
その他の参考資料 37
基本的な IP ルーティングの機能情報 37
IPv6 ルーティング：スタティック ルーティング 39
機能情報の確認 39
IPv6 ルーティング：スタティック ルーティングの前提条件 40
IPv6 ルーティング：スタティック ルーティングの制約事項 40
IPv6 ルーティング：スタティック ルーティングに関する情報 40
スタティック ルート 40
直接接続されているスタティック ルート 41
再帰スタティック ルート 41
完全指定のスタティック ルート 42
フローティング スタティック ルート 42
IPv6 スタティック ルーティングの設定方法 43

スタティック IPv6 ルートの設定 43
デフォルトのIPv6スタティック ルートを使用するための再帰IPv6スタティック ルートの設定 44
フローティング スタティック IPv6 ルートの設定 45
スタティック IPv6 ルートの設定と動作の確認 46
IPv6 スタティック ルーティングの設定例 47
手動集約の設定例 47
例：トラフィック廃棄の設定 48
例：デフォルトの固定ルートの設定 48
例：フローティング スタティック ルートの設定 49
その他の参考資料 50
IPv6 ルーティング：スタティック ルーティングの機能情報 51
IPv4 ループ フリー代替高速再ルーティング 53
機能情報の確認 53
IPv4 ループ フリー代替高速再ルーティングのための前提条件 54
IPv4 ループ フリー代替高速再ルーティングの制約事項 54
IPv4 ループ フリー代替高速再ルーティングに関する情報 55
IS-IS および IP FRR 55
修復パス 56
LFA の概要 56
LFA の計算 57
RIB とルーティング プロトコル間の連携 57
IPv4 ループ フリー代替高速再ルーティングの設定方法 58
高速再ルーティングのサポートの設定 58
IPv4 ループ フリー代替高速再ルーティングの設定例 61
例：IPv4 ループ フリー代替高速再ルーティングの設定のサポート 61
その他の参考資料 62
IPv4 ループ フリー代替高速再ルーティングの設定に関する機能情報 63
IP イベント減衰 65
機能情報の確認 65
IP イベント減衰の制約事項 66
IP イベント減衰に関する情報 66

IP イベント減衰の概要 66
インターフェイス状態変化イベント 67
抑制しきい値 67
半減期 67
再使用しきい値 67
最大抑制時間 68
関連コンポーネント 68
ルート タイプ 68
サポートされているプロトコル 69
ネットワーク展開 69
IP イベント減衰の利点 70
IP イベント減衰の設定方法 71
IP イベント減衰のイネーブル化 71
IP イベント減衰の確認 72
IP イベント減衰の設定例 73
IP イベント減衰の設定例 73
IP イベント減衰の確認の例 73
その他の参考資料 74
IP イベント減衰の機能情報 75
用語集 76
PBR 再帰ネクスト ホップ 79
機能情報の確認 79
PBR 再帰ネクスト ホップの制約事項 80
PBR 再帰ネクスト ホップに関する情報 80
PBR 再帰ネクスト ホップの概要 80
PBR 再帰ネクスト ホップの設定方法 80
再帰ネクストホップ IP アドレスの設定 80
再帰ネクストホップ設定の確認 84
PBR 再帰ネクスト ホップの設定例 85
例：再帰ネクストホップ IP アドレス 85
PBR 再帰ネクスト ホップに関するその他の参考資料 86
PBR 再帰ネクスト ホップの機能情報 87

複数のトラッキング オプションに対する PBR サポート 89

機能情報の確認 89

複数のトラッキング オプションに対する PBR サポートの概要 90

オブジェクト トラッキング 90

複数のトラッキング オプションに対する PBR サポートの機能設計 90

複数のトラッキング オプションに対する PBR サポートの設定方法 90

Cisco IOS Release 12.3(11)T、12.2(25)S、およびそれ以前 91

複数のトラッキング オプションに対する PBR サポートの設定 94

複数のトラッキング オプションに対する PBR サポートの設定例 99

Cisco IOS Release 12.3(11)T、12.2(25)S、およびそれ以前 99

例：複数のトラッキング オプションに対する PBR サポートの設定 99

その他の参考資料 100

コマンド リファレンス 101

複数のトラッキング オプションに対する PBR サポートの機能情報 101

PBR 一致トラック オブジェクト 103

機能情報の確認 103

PBR 一致トラック オブジェクトの制限 103

PBR 一致トラック オブジェクトに関する情報 104

PBR 一致トラック オブジェクトの概要 104

PBR 一致トラック オブジェクトの設定方法 105

PBR 一致トラック オブジェクトの設定 105

PBR 一致トラック オブジェクトの確認 106

PBR 一致トラック オブジェクトの設定例 107

例：PBR 一致トラック オブジェクトの設定 107

例：PBR 一致トラック オブジェクトの確認 107

PBR 一致トラック オブジェクトに関するその他の参考資料 107

PBR 一致トラック オブジェクトに関する機能情報 108

IPv6 ポリシーベース ルーティング 109

機能情報の確認 109

IPv6 ポリシーベース ルーティングに関する情報 110

ポリシーベース ルーティングの概要 110

ポリシーベース ルーティングの機能 111

パケット マッチング 111
set 文を使用したパケット転送 112
ポリシーベース ルーティングを使用する場合 112
IPv6 ポリシーベース ルーティングをイネーブルにする方法 113
インターフェイスでの IPv6 PBR の有効化 113
ローカル PBR for IPv6 の有効化 117
PBR for IPv6 の設定と動作の確認 118
PBR for IPv6 のトラブルシューティング 118
IPv6 ポリシーベース ルーティングの設定例 119
例：インターフェイスでの PBR のイネーブル化 119
例：ローカル PBR for IPv6 の有効化 119
例：show ipv6 policy コマンドの出力 120
例：Route-Map 情報の確認 120
IPv6 ポリシーベース ルーティングのその他の参考資料 120
IPv6 ポリシーベース ルーティングの機能情報 121
ポリシーベース ルーティングを使用した Multi-VRF 選択 123
機能情報の確認 124
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 124
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 124
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 125
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 125
ポリシーベース ルーティングの set コマンド 126
VRF インスタンスのポリシールーティング パケット 126
通常のルーティングおよび転送動作の変更 127
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 128
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 129
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 129
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 130
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 131

ルート マップでの Multi-VRF 選択の設定 132
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 135
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 136
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 139
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 139
例：ルート マップでの Multi-VRF 選択の設定 139
その他の参考資料 140
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 140
用語集 142
Multi-VRF サポート 143
機能情報の確認 143
Multi-VRF サポートの前提条件 144
Multi-VRF サポートの制約事項 144
Multi-VRF サポートに関する情報 144
Multi-VRF サポート機能の動作 144
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 145
Multi-VRF サポート機能を設定する場合の考慮事項 146
Multi-VRF サポートの設定方法 147
VRF の設定 147
ルーティング プロトコルとしての BGP の設定 149
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 151
BGP 以外のルーティング プロトコルの設定 154
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 156
Multi-VRF サポートの設定例 156
例：PE デバイスでの Multi-VRF サポートの設定 157
例：CE デバイスでの Multi-VRF サポートの設定 158
その他の参考資料 159
Multi-VRF サポートの機能情報 160
デフォルトのパッシブ インターフェイス 161
機能情報の確認 161
デフォルトのパッシブ インターフェイスに関する情報 162

デフォルトのパッシブ インターフェイス 162
インターフェイスからのルーティング アップデートの防止 162
デフォルトのパッシブ インターフェイスの設定方法 163
デフォルトのパッシブ インターフェイスの設定 163
デフォルトのパッシブ インターフェイスの設定例 165
例：OSPF のパッシブ インターフェイスの設定 165
例：OSPF のデフォルトのパッシブ インターフェイスの設定 166
その他の参考資料 166
デフォルトのパッシブ インターフェイスの機能情報 167
Policy-Based Routing：ポリシーベース ルーティング 169
機能情報の確認 169
ポリシーベース ルーティングの前提条件 170
ポリシーベース ルーティングの概要 170
Policy-Based Routing：ポリシーベース ルーティング 170
ポリシーベース ルーティングの設定方法 171
ポリシーベース ルーティングの設定 171
ポリシーベース ルーティングの設定例 174
その他の参考資料 174
ポリシーベース ルーティングの機能情報 174
BDI 経由の PPPoE 177
BDI 経由の PPPoE の制限 177
機能情報の確認 177
BDI 経由の PPPoE に関する情報 178
PPPoE 178
ブリッジ ドメイン インターフェイス 178
BDI 経由の PPPoE 178
BDI 経由の PPPoE の設定方法 178
BDI 経由の PPPoE の有効化 178
BDI 経由の PPPoE の無効化 179
BDI 経由の PPPoE の設定例 179
BDI 経由の PPPoE に関するその他の参考資料 179
BDI 経由の PPPoE の機能情報 181

SGT ベースの PBR 183

機能情報の確認 183

SGT ベースの PBR の制限 184

SGT ベースの PBR に関する情報 184

Cisco TrustSec 184

SGT ベースの PBR 184

SGT ベースの PBR の設定方法 185

一致セキュリティ グループ タグの設定 185

インターフェイスへのルートマップの割り当て 186

SGT ベースの PBR の設定の表示と確認 187

SGT ベースの PBR の設定例 188

例：SGT ベースの PBR 188

SGT ベースの PBR に関するその他の参考資料 189

SGT ベースの PBR の機能情報 189

SGT ベースの QoS 191

機能情報の確認 191

SGT ベースの QoS の前提条件 192

SGT ベースの QoS の制限 192

SGT ベースの QoS に関する情報 192

SGT ベースの QoS 192

SGT ベースの QoS の設定方法 193

ユーザ グループ、デバイス、または役割ベースの QoS ポリシーの設定 193

ポリシーマップの設定とインターフェイスへの割り当て 194

SGT ベースの QoS の設定の表示と確認 195

SGT ベースの QoS の設定例 196

例：ユーザ グループ、デバイス、または役割ベースの QoS ポリシーの設定 196

SGT ベースの QoS に関するその他の参考資料 197

SGT ベースの QoS の機能情報 197

ポリシーベース ルーティングのデフォルト ネクストホップ ルート 199

機能情報の確認 199

ポリシーベース ルーティングのデフォルト ネクストホップ ルートに関する情報 200

Policy-Based Routing：ポリシーベース ルーティング 200

IP ヘッダーでの優先順位の設定 201
ポリシーベース ルーティングのデフォルト ネクストホップ ルートの設定方法 202
ポリシーベース ルーティングのデフォルト ネクストホップ ルートの優先順位の設定 202
ポリシーベース ルーティングのデフォルト ネクストホップ ルートの設定例 204
例：ポリシーベース ルーティング 204
その他の参考資料 204
ポリシーベース ルーティングのデフォルト ネクストホップ ルートの機能情報 205
VRF 用 PBR ネクストホップ可用性確認 207
機能情報の確認 207
VRF 用 PBR ネクストホップ可用性確認に関する情報 208
VRF 用 PBR ネクストホップ可用性確認の概要 208
VRF 用 PBR ネクストホップ可用性確認の設定方法 209
継承された IP VRF 用 PBR ネクストホップ可用性確認の設定 209
継承された IPv6 VRF 用 PBR ネクストホップ可用性確認の設定 213
VRF 間用 PBR ネクストホップ可用性確認の設定 217
VRF 用 PBR ネクストホップ可用性確認の設定例 220
例：継承された IP VRF 用 PBR ネクストホップ可用性確認の設定 220
例：継承された IPv6 VRF 用 PBR ネクストホップ可用性確認の設定 221
例：VRF 間用 PBR ネクストホップ可用性確認の設定 221
VRF 用 PBR ネクストホップ可用性確認に関するその他の参考資料 222
VRF 用 PBR ネクストホップ可用性確認に関する機能情報 222
BGP による QoS ポリシー伝搬 225
機能情報の確認 225
BGP による QoS ポリシー伝搬の前提条件 226
BGP による QoS ポリシー伝搬に関する情報 226
BGP による QoS ポリシー伝搬の利点 226
BGP による QoS ポリシー伝搬の設定方法 227
コミュニティ リストに基づいた BGP による QoS ポリシー伝搬の設定 227
自律システム パス属性に基づいた BGP による QoS ポリシー伝搬の設定 230
アクセス リストに基づいた BGP による QoS ポリシー伝搬の設定 232
BGP による QoS ポリシー伝搬のモニタリング 235

BGP による QoS ポリシー伝搬の設定例 236
例：BGP による QoS ポリシー伝搬の設定 236
その他の参考資料 238
BGP による QoS ポリシー伝搬の機能情報 239
NetFlow ポリシー ルーティング 241
機能情報の確認 241
NetFlow ポリシー ルーティングの前提条件 242
NetFlow ポリシー ルーティングの制約事項 242
NetFlow ポリシー ルーティングに関する情報 242
NetFlow ポリシー ルーティング 242
ネクストホップの到達可能性 243
その他の参考資料 244
NetFlow ポリシー ルーティングの機能情報 245
再帰スタティック ルート 247
機能情報の確認 247
再帰スタティック ルートの制約事項 248
再帰スタティック ルートに関する情報 248
再帰スタティック ルートのインストール方法 248
VRF での再帰スタティック ルートのインストール 248
ルート マップを使用した再帰スタティック ルートのインストール 250
再帰スタティック ルートの設定例 252
例：VRF での再帰スタティック ルートのインストール 253
例：ルート マップを使用した再帰スタティック ルートのインストール 253
再帰スタティック ルートに関する追加情報 254
再帰スタティック ルートの機能情報 254

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）以降、これら2つのリリースは、単一の統合されたリリースバージョンである Cisco IOS XE 16 に進化（合体）されています。これにより、スイッチングとルーティングのポートフォリオにおいて広範囲のアクセス製品およびエッジ製品をカバーする単一のリリースが提供されます。

（注） テクノロジー コンフィギュレーション ガイドにある「機能情報」表には、機能が導入された時期が記載されています。その機能が他のプラットフォームでサポートされた時期については、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、ご使用の製品のランディング ページに掲載されているテクノロジー コンフィギュレーション 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 ページにテクノロジー コンフィギュレーション ガイドが表示されていれば、その機能はプラットフォームでサポートされています。

第 2 章

基本的な IP ルーティング

この章では、基本的な IP ルーティングを設定する方法について説明します。インターネット プロトコル（IP）は、パケットのルーティングのためのアドレシング情報と制御情報が格納された、ネットワーク層（レイヤ 3）プロトコルです。IP は RFC 791 に規定されており、インターネット プロトコル スイートの主要なネットワーク層プロトコルです。

- 機能情報の確認，3 ページ
- 基本的な IP ルーティングに関する情報，4 ページ
- 基本的な IP ルーティングの設定方法，12 ページ
- 基本的な IP ルーティングの設定例，22 ページ
- その他の参考資料，37 ページ
- 基本的な IP ルーティングの機能情報，37 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。

基本的な IP ルーティングに関する情報

可変長サブネット マスク

Enhanced Interior Gateway Routing Protocol（EIGRP）、Intermediate System-to-Intermediate System（IS-IS）、Open Shortest Path First（OSPF）、Routing Information Protocol（RIP）バージョン 2、およびスタティック ルートは、可変長サブネット マスク（VLSM）をサポートします。VLSM により、異なるインターフェイスの同じネットワーク番号に別のマスクを使用できるため、IP アドレスを維持し、使用可能なアドレス空間をより効率的に使用できます。ただし、VLSM を使用すると、ネットワーク管理者によるアドレスの割り当てや現行の管理も難しくなります。

VLSM および適切なアドレス割り当て方法の詳細については、RFC 1219 を参照してください。

（注） VLSM の使用決定については、慎重に検討してください。アドレス割り当ては間違えやすく、一般的に VLSM を使用したネットワークのモニタは複雑になります。

VLSM を実装する最善の方法は、既存のアドレッシング計画を維持し、いくつかのネットワークを段階的に VLSM に移行してアドレス レンジを回復することです。

スタティック ルート

スタティック ルートは、指定のパスを通るように発信元と宛先の間でパケットを移動させるユーザ定義のルートです。スタティック ルートは、デバイスが特定の宛先へのルートを確立できない場合に重要になることがあります。また、ルーティングできないすべてのパケットを送るラストリゾート ゲートウェイを指定する場合にも役立ちます。

スタティック ルートを設定するには、**ip route***prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [*distance*] [*name*] [**permanent** | **track***number*] [**tag***tag*] グローバル コンフィギュレーション コマンドを使用します。

スタティック ルートは、削除されるまでデバイス設定に残ります（**no ip route** グローバル コンフィギュレーションコマンドを使用します）。ただし、アドミニストレーティブディスタンス値を慎重に割り当てることにより、ダイナミックルーティング情報でスタティックルートを上書きすることができます。アドミニストレーティブ ディスタンスは、個々のルータやルータのグループなど、ルーティング情報送信元の信頼性を表す数値です。数値的に、アドミニストレーティブ ディスタンスは 0 ～ 255 の整数です。通常は、値が大きいほど、信頼性の格付けが下がります。アドミニストレーティブ ディスタンスが 255 の場合はルーティング情報の送信元をまったく信頼できないため、無視する必要があります。

各ダイナミック ルーティング プロトコルには、デフォルトのアドミニストレーティブ ディスタンスが設定されています（下の表を参照）。ダイナミックルーティングプロトコルからの情報でスタティック ルートを上書きする場合は、スタティック ルートのアドミニストレーティブ ディスタンスがダイナミック プロトコルのものよりも大きいことを確認します。

表 *1*：ダイナミック ルーティング プロトコルのデフォルト アドミニストレーティブ ディスタンス

ルートの送信元	デフォルト距離
接続されているインターフェイス	0
スタティック ルート	1
Enhanced Interior Gateway Routing Protocol（EIGRP）サマリー ルート	5
外部ボーダーゲートウェイ プロトコル（BGP）	20
内部 EIGRP	90
Interior Gateway Routing Protocol（IGRP）	100
Open Shortest Path First（OSPF）	110
Intermediate System to Intermediate System（IS-IS）	115
ルーティング情報プロトコル（RIP）	120
外部ゲートウェイ ルーティング プロトコル（EGP）	140
On Demand Routing（ODR）	160
外部 EIGRP	170
内部 BGP	200
不明（Unknown）	255

インターフェイスを指定したスタティック ルートは、**redistribute static** ルータ コンフィギュレーション コマンドが RIP、EIGRP、およびその他のダイナミック ルーティング プロトコルに指定されているかどうかにかかわらず、それらのルーティング プロトコルを介してアドバタイズされます。これらのスタティック ルートがアドバタイズされるのは、インターフェイスを指し示すスタティック ルートが接続された結果、静的な性質を失ったとルーティング テーブルで見なされるためです。ただし、**network** コマンドで定義されたネットワーク以外のインターフェイスに対してスタティック ルートを定義する場合は、ダイナミック ルーティング プロトコルに **redistribute static** コマンドを指定しない限り、ルートはアドバタイズされません。

インターフェイスがダウンすると、ダウンしたインターフェイスを経由するすべてのスタティック ルートが IP ルーティング テーブルから削除されます。また、スタティック ルートの転送先デ

バイスアドレスに指定されたアドレスに有効なネクストホップをソフトウェアが検出できない場合も、IP ルーティング テーブルからスタティック ルートが削除されます。

（注） E クラスの送信元アドレス（240.0.0.0/4）を持つパケットは、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでドロップされますが、RFC 1812（IP Version 4 ルータの要件）は、特に送信元アドレスに対してでなく、宛先アドレスに対してのみこの動作を定義します。

デフォルト ルート

ラスト リゾート ゲートウェイとしても知られるデフォルト ルートは、ルーティング テーブルに明示的には表示されていないネットワークにアドレス指定されたパケットをルーティングするために使用されます。デバイスはすべてのネットワークへのルートを定められない場合があります。完全なルーティング機能を提供するために、ネットワーク管理者は一部のデバイスをスマート デバイスとして使用し、残りのデバイスにそのスマートデバイスへのデフォルトルートを提供します。（スマートデバイスにはインターネットワーク全体のルーティングテーブルに関する情報が格納されます）デフォルト ルートは、個別のデバイスに動的に渡すことも、手動で設定することもできます。

ほとんどのダイナミックな内部ルーティングプロトコルには、スマートデバイスがダイナミックなデフォルト情報を生成し、それを他のデバイスに渡す処理を発生させるメカニズムが含まれます。

次のコマンドを使用してデフォルト ルートを設定できます。

- **ip default-gateway**
- **ip default-network**
- **ip route 0.0.0.0 0.0.0.0**

IP ルーティングがデバイス上でディセーブルな場合にデフォルト ゲートウェイを定義するには、**ip default-gateway** グローバル コンフィギュレーション コマンドを使用できます。たとえば、デバイスがホストの場合、デバイスのデフォルト ゲートウェイを定義するためにこのコマンドを使用できます。また、このコマンドは、デバイスがブートモードのときに、デバイスにシスコ ソフトウェアイメージを転送するために使用できます。ブートモードでは、IP ルーティングはデバイスでイネーブルにされていません。

ip default-gateway コマンドとは異なり、デバイスで IP ルーティングがイネーブルになっている場合に **ip default-network** コマンドを使用できます。**ip default-network** コマンドを使用してネットワークを指定すると、デバイスは、インストールのためのそのネットワークへのルートを、そのデバイスのラスト リゾート ゲートウェイとして認識します。

ip default-network コマンドを使用して設定されたラスト リゾート ゲートウェイは、デフォルト ルートを伝播させるルーティング プロトコルに応じて、異なる方法で伝播されます。デフォルト ルートを伝播する Interior Gateway Routing Protocol（IGRP）と Enhanced Interior Gateway Routing Protocol（EIGRP）では、**ip default-network** コマンドで指定されたネットワークは IGRP または EIGRP で認識されている必要があります。ネットワークは、ルーティング テーブルの IGRP また

はEIGRPから派生したネットワークである必要があります。または、ネットワークへのルートを生成するために使用するスタティック ルートは、IGRP または EIGRP に再配布されるか、これらのプロトコルに **network** コマンドを使用してアドバタイズする必要があります。ラスト リゾート ゲートウェイが **ip default-network** コマンドを使用して設定されている場合、ルーティング情報プロトコル（RIP）は、ネットワーク 0.0.0.0 にルートをアドバタイズします。**ip default-network** コマンドで指定されたネットワークは、明示的に RIP でアドバタイズする必要はありません。

ip route 0.0.0.0 0.0.0.0 コマンドを使用して、ネットワーク 0.0.0.0 0.0.0.0 へのスタティック ルートを作成することは、デバイスのラスト リゾート ゲートウェイを設定するもう 1 つの方法です。**ip default-network** コマンドと同様に、0.0.0.0 へのスタティック ルートを使用することは、ルーティング プロトコルには依存しません。ただし、IP ルーティングをデバイスでイネーブルにする必要があります。IGRP はネットワーク 0.0.0.0 へのルートを認識しません。したがって、**ip route 0.0.0.0 0.0.0.0** コマンドを使用して作成されたデフォルト ルートを伝播できません。**ip default-network** コマンドを使用して、IGRP がデフォルト ルートを伝搬するようにします。

EIGRP は、ネットワーク 0.0.0.0 へのルートを伝播しますが、スタティック ルートはルーティング プロトコルに再配布する必要があります。

シスコ ソフトウェアのリリースによっては、**ip route 0.0.0.0 0.0.0.0** コマンドを使用して作成されたデフォルト ルートは、RIP デバイスによって自動的にアドバタイズされます。一部のリリースでは、ルートが RIP によって学習されていない場合、RIP はデフォルト ルートをアドバタイズしません。**redistribute** コマンドを使用して、RIP へのルートの再配布が必要な場合があります。

ip route 0.0.0.0 0.0.0.0 コマンドを使用して作成されたデフォルト ルートは、Open Shortest Path First（OSPF）および Intermediate System to Intermediate System（IS-IS）で伝播されません。また、これらのデフォルト ルートは、OSPF または IS-IS に **redistribute** コマンドを使用して再配布できません。OSPF または IS-IS ルーティング ドメインにデフォルト ルートを生成するには、**default-information originate** コマンドを使用します。

デフォルト ネットワーク

デフォルト ネットワークは、ルーティング テーブルに確立されていない宛先にパケットをルーティングするために使用されます。IP ルーティングがデバイスでイネーブルになっている場合にデフォルト ネットワークを設定するには、**ip default-network***network-number* グローバル コンフィギュレーション コマンドを使用できます。デフォルト ネットワークを設定すると、デバイスは、インストールのためのそのネットワークへのルートを、そのデバイスのラスト リゾート ゲートウェイとして認識します。

ラスト リゾート ゲートウェイ

デフォルト情報をダイナミック ルーティング プロトコルを介して渡している場合、その他の設定は不要です。ルーティング テーブルは定期的にスキャンされ、デフォルト ルートとして最適なデフォルト ネットワークが選択されます。ルーティング情報プロトコル（RIP）の場合、ネットワーク 0.0.0.0 という唯一の選択肢しかありません。Enhanced Interior Gateway Routing Protocol（EIGRP）の場合、システム デフォルトの候補となるいくつかのネットワークがある場合があります。シスコ ソフトウェアは、アドミニストレーティブ ディスタンスとメトリックの両方の情報を使用し

て、デフォルトルート（ラストリゾートゲートウェイ）を判断します。選択したデフォルトルートは、**show ip route** 特権 EXEC コマンドのラストリゾートゲートウェイの表示に表示されます。

ダイナミックなデフォルト情報がソフトウェアに渡されない場合、デフォルトルートの候補を **ip default-network** グローバル コンフィギュレーション コマンドで指定します。この方法では、**ip default-network** コマンドは引数として未接続ネットワークを使用します。このネットワークが任意のソース（ダイナミックまたはスタティック）のルーティング テーブルに表示される場合、デフォルトルート候補としてフラグが付けられ、デフォルトルートとして使用できる選択肢になります。

デバイスのデフォルトネットワークにインターフェイスがなく、そのネットワークに対するルートはある場合、そのネットワークはデフォルトパス候補と見なされます。ルート候補は検査され、アドミニストレーティブ ディスタンスおよびメトリックに基づいて最適な候補が選択されます。最適なデフォルトパスに対するゲートウェイは、ラストリゾートゲートウェイになります。

パスの最大数

デフォルトでは、ほとんどの IP ルーティング プロトコルでルーティング テーブルに最大 4 つのパラレルルートがインストールされます。スタティック ルートには、常に 6 つのルートがインストールされます。ボーダー ゲートウェイ プロトコル（BGP）は例外で、デフォルトでは宛先へのパスが 1 つ（最良パス）しか許可されていません。ただし、BGP は、等コストおよび不等コストマルチパスのロード シェアリングを使用するように設定できます。

ルーティングテーブルへのインストールを設定できるパラレルルートの数は、インストールされているシスコ ソフトウェアのバージョンによって変わります。許可されるパラレルパスの最大数を変更するには、ルータ コンフィギュレーション モードで **maximum-paths***number-paths* コマンドを使用します。

マルチインターフェイスの負荷分散

マルチインターフェイスの負荷分散により、複数のインターフェイスにわたって同じ宛先に向かうトラフィックを効率的に制御できます。**traffic-share min** ルータ コンフィギュレーション コマンドでは、同じ宛先に複数のパスを使用できる場合、最小メトリックのパスだけがルーティング テーブルにインストールされるように指定します。許可されるパスの数が 7 つ以上になることはありません。ダイナミック ルーティング プロトコルの場合、パスの数は **maximum-paths** ルータ コンフィギュレーション コマンドによって制御します。スタティック ルートの発信元には、6 つのパスをインストールできます。それよりも多くのパスを利用できる場合、余分なパスは廃棄されます。インストールされたいくつかのパスがルーティング テーブルから削除されると、保留中のルートが自動的に追加されます。

ルーティング情報の再配布

シスコ ソフトウェアは、複数のルーティングプロトコルを同時に実行するだけでなく、あるルーティング プロトコルから別のルーティング プロトコルに情報を再配布できます。たとえば、Enhanced Interior Gateway Routing Protocol（EIGRP）で送信されたルートを、ルーティング情報プ

ロトコル（RIP）を使用して再アドバタイズしたり、EIGRP プロトコルを使用してスタティック ルートを再アドバタイズするようにデバイスを設定できます。あるルーティング プロトコルから別のルーティング プロトコルへの再配布は、すべての IP ベース ルーティング プロトコルで設定できます。

また、2 つのドメイン間でルート マップを設定することにより、ルーティング ドメイン間でルートの再配布を条件に応じて制御することもできます。ルート マップは、permit および deny ステートメント、match および set 句、およびシーケンス番号を使用して設定されるルートまたはパケット フィルタです。

再配布はプロトコルに依存しない機能ですが、**match** および **set** コマンドのいくつかは特定のプロトコルに固有のものです。

1 つまたは複数の **match** コマンドおよび 1 つまたは複数の **set** コマンドを、ルート マップ コンフィギュレーション モードで設定します。**match** コマンドがない場合、すべてが一致します。**set** コマンドがない場合、設定アクションは実行されません。

再配布用のルート マップを定義するには、**route-map***map-tag* [**permit** | **deny**] [*sequence-number*] グローバル コンフィギュレーション コマンドを使用します。

ルーティングプロトコルのメトリックを、必ずしも別のルーティングプロトコルのメトリックに変換する必要はありません。たとえば、RIP メトリックはホップ カウントですが、EIGRP メトリックは 5 つのメトリック値の組み合わせです。このような場合、再配布されるルートにダイナミック メトリックが割り当てられます。この場合の再配布は、ルーティングループを防ぐために、インバウンド フィルタリングと共に一貫して慎重に適用する必要があります。

redistribute コマンドに設定したオプションを削除するには、期待する結果が得られるように **no redistribute** コマンドを慎重に使用する必要があります。

サポートされるメトリック変換

ここでは、ルーティング プロトコル間でサポートされる自動メトリック変換について説明します。次の説明では、メトリック変換に代わるデフォルト再配布メトリックが定義されていないことを前提とします。

- ルーティング情報プロトコル（RIP）は自動的にスタティック ルートを再配布できます。スタティック ルートにはメトリック 1（直接接続）が割り当てられます。
- ボーダー ゲートウェイ プロトコル（BGP）は、通常、ルーティング アップデートでメトリックを送信しません。
- スタティック ルートと関連のインターフェイスが Enhanced Interior Gateway Routing Protocol（EIGRP）ネットワーク ステートメントで扱われる限り、EIGRP は他の EIGRP ルートの自律システムから自動的にスタティック ルートを再配布できます。EIGRP は、スタティック ルートに対して、直接接続として指定するメトリックを割り当てます。EIGRP は、他の自律システムの EIGRP アップデートから派生したルートのメトリックを変更しません。

（注） デフォルト メトリックが設定されている限り、すべてのプロトコルが他のルーティング プロトコルからルートを再配布できることに注意してください。

no redistribute コマンド実装のプロトコルの違い

注意 **redistribute** コマンドに設定したオプションを削除するには、期待する結果が得られるように **no redistribute** コマンドを慎重に使用する必要があります。ほとんどの場合、キーワードを変更またはディセーブルにしても、他のキーワードの状態には影響しません。

異なるプロトコルでは、**no redistribute** コマンドは次のように異なる方法で実装されます。

- ボーダー ゲートウェイ プロトコル（BGP）、Open Shortest Path First（OSPF）、およびルーティング情報プロトコル（RIP）の設定で、**no redistribute** コマンドは、実行コンフィギュレーションの **redistribute** コマンドから、指定されたキーワードのみを除外します。これらでは、その他のプロトコルから再配布するときに、減算キーワードの方式を使用します。たとえば、BGP で **no redistribute static route-map interior** を設定する場合、ルート マップのみが再配布から除外され、**redistribute static** がフィルタなしでそのまま残ります。
- **no redistribute isis** コマンドは、実行コンフィギュレーションから Intermediate System to Intermediate System（IS-IS）の再配布を削除します。IS-IS は、IS-IS が再配布されているかどうかや、プロトコルを再配布しているかどうかに関係なく、コマンド全体を削除します。
- Enhanced Interior Gateway Routing Protocol（EIGRP）は、EIGRP コンポーネント バージョン rel5 より前の減算キーワード方式を使用していました。EIGRP コンポーネント バージョン rel5 以降、**no redistribute** コマンドによって、他のプロトコルから再配布するときに **redistribute** コマンド全体が削除されます。

ルーティング情報発信元のフィルタリング

いくつかのルーティング情報が他の情報よりも正確な場合があるため、ルーティング情報発信元のフィルタリングにより、さまざまな発信元からのルーティング情報に優先順位を付けられます。アドミニストレーティブ ディスタンスは、個々のデバイスやデバイスのグループなど、ルーティング情報発信元の信頼性を表す数値です。大規模なネットワークでは、一部のルーティング プロトコルとデバイスが、ルーティング情報発信元として他よりも信頼性が高い場合があります。また、複数のルーティングプロセスがIPの同じデバイスで実行されている場合、同じルートを複数のルーティングプロセスによってアドバタイズできます。アドミニストレーティブディスタンスの値を指定すると、デバイスはルーティング情報の送信元をインテリジェントに区別できるようになります。常にルーティングプロトコルのアドミニストレーティブディスタンスが最短（値が最小）であるルートが選択されます。

ネットワークごとに独自の要件があるため、アドミニストレーティブ ディスタンスの割り当てに関する一般的なガイドラインはありません。ネットワーク全体のアドミニストレーティブ ディスタンスの適切なマトリクスを判断する必要があります。

たとえば、Enhanced Interior Gateway Routing Protocol（EIGRP）とルーティング情報プロトコル（RIP）を使用するデバイスを検討します。EIGRP から派生するルーティング情報を RIP から派生するルーティング情報よりも信頼すると仮定します。この例では、デフォルトの EIGRP アドミニストレーティブ ディスタンスがデフォルトの RIP アドミニストレーティブ ディスタンスよりも小さいため、デバイスは EIGRP から派生する情報を使用して RIP から派生する情報を無視します。ただし、EIGRP から派生する情報の発信元が失われた場合（発信元ネットワークの停電など）、デバイスは EIGRP から派生する情報が再提示されるまで RIP から派生する情報を使用します。

（注） アドミニストレーティブ ディスタンスを使用して、同じルーティング プロトコルを実行しているデバイスからのルーティング情報を格付けすることもできます。フォワーディング ループなど、整合性のないルーティング情報が生じる可能性があるため、アドミニストレーティブ ディスタンスのこの特定用途に不慣れな場合、この使用方法は推奨しません。

（注） ルートの重みは、**distance** コマンドでは設定できなくなりました。ルートの重みを設定するには、ルート マップを使用します。

認証キー管理およびサポートされるプロトコル

キー管理を使用すると、ルーティング プロトコルで使用される認証キーを制御できます。キー管理をサポートしないプロトコルもあります。認証キーは、ディレクタ レスポンス プロトコル（DRP）エージェント、Enhanced Interior Gateway Routing Protocol（EIGRP）、およびルーティング情報プロトコル（RIP）バージョン 2 で利用可能です。

キーチェーンを定義し、キーチェーンに属するキーを特定し、各キーの有効期間を指定して認証キーを管理できます。各キーには独自のキー ID があります（**key chain** コンフィギュレーション コマンドで指定します）。キー ID はローカルに保存されます。キー ID、およびメッセージに関連付けられたインターフェイスの組み合わせにより、使用中の認証アルゴリズムおよびメッセージ ダイジェスト アルゴリズム 5（MD5）認証キーが一意に識別されます。

複数のキーにライフタイムを設定できます。存在する有効なキーの数にかかわらず、送信される認証パケットは1つだけです。キー番号はソフトウェアによって昇順に調べられ、最初に見つかった有効なキーが使用されます。キー変更中は、有効期間が重なっても問題ありません。

基本的な IP ルーティングの設定方法

ルーティング情報の再配布

ルート マップを使用した再配布の制御の有無にかかわらず、1 つのルーティング ドメインから別のルーティング ドメインにルートを再配布できます。どのルートを再配布するかを制御するには、ルート マップを設定し、**redistribute** コマンドからルート マップを参照します。

ここでは、使用するプロトコルに応じて、ルート（ルート マップ）を再配布するための条件を定義する方法、ルートを再配布する方法、ルートの再配布のためにオプションを削除する方法について説明します。

再配布ルートの条件の定義

ルート マップは、ルート再配布を制御するため（またはポリシー ベース ルーティングを実装するため）に使用できます。1 つのルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を定義するには、**route-map** コマンドを設定します。その後、必要に応じて、ルート マップ コンフィギュレーション モードで少なくとも 1 個の **match** コマンドを使用します。少なくとも 1 個の **match** コマンドがこのタスクで使用されるのは、このタスクの目的が、再配布の基準となる 1 つ以上の条件を定義する方法を示すことであるためです。

（注） ルート マップは、**match** コマンドには必要はありませんが、**set** コマンドにのみ指定できます。**match** コマンドがない場合、すべてがルート マップに一致します。

（注） この表以外にも、**match** コマンドは多数あります。追加の **match** コマンドについては、『*Cisco IOS Master Command List*』を参照してください。

コマンドまたはアクション	目的
match as-path *path-list-number*	BGP 自律システム パス アクセス リストを照合します。
match community {*standard-list-number* | *expanded-list-number* | *community-list-name* **match community**[**exact**]}	BGP コミュニティを照合します。
match ip address {*access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...*| *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*]}	パケットのポリシー ルーティングが許可されている、または標準アクセス リスト、拡張アクセス リスト、またはプレフィックス リストで許可されている宛先ネットワーク アドレスを持つルートを照合します。
match metric *metric-value*	指定したメトリックを持つルートに一致します。
match ip next-hop {*access-list-number* | *access-list-name*} [*access-list-number* | *access-list-name*]	指定されたアクセス リストの 1 つによって渡された、ネクストホップ デバイス アドレスを照合します。
match tag *tag-value* [*tag-value*]	指定したタグの値に一致します。
match interface *type number* [*type number*]	指定したインターフェイスをネクストホップとして使用するルートを照合します。
match ip route-source {*access-list-number* | *access-list-name*} [*access-list-number* | *access-list-name*]	アドバタイズされたアクセス リストによって指定されたアドレスを照合します。
match route-type {**local** | **internal** | **external** [**type-1** | **type-2**] | **level-1** | **level-2**}	指定したルートのタイプに一致します。

一致基準が満たされた場合（ルート マップによって再配布されるルートで）に、システムが実行するルーティング アクションを任意に指定するには、必要に応じて、ルート マップ コンフィギュレーション モードで 1 つまたは複数の **set** コマンドを使用します。

（注） ルートマップは、**set** コマンドには必要はありませんが、**match** コマンドにのみ指定できます。

（注） このテーブルに示されない他の **set** コマンドがあります。追加の **set** コマンドについては、『*Cisco IOS Master Command List*』を参照してください。

コマンドまたはアクション	目的
set community {*community-number* [**additive**] [**well-known**] | **none**}	コミュニティ属性を設定します（BGP用）。
set dampening *halflife reuse suppress max-suppress-time*	ルート ダンプニング パラメータを設定します（BGP 用）。
set local-preference *number-value*	パスにローカル プリファレンス値を割り当てます（BGP 用）。
set origin {**igp** | **egp** *as-number* | **incomplete**}	ルート オリジン コードを設定します。
set as-path{**tag** | **prepend** *as-path-string* }	自律システムパスを変更します（BGP用）。
set next-hop *next-hop*	ネクスト ホップのアドレスを指定します。
set automatic-tag	タグ テーブルの自動計算をイネーブルにします。
set level {**level-1** | **level-2** | **level-1-2** | **stub-area** | **backbone**}	ルートをインポートするエリアを指定します。
set metric *metric-value*	再配布されるルートのメトリック値を設定します（EIGRP以外のすべてのプロトコル）。
set metric *bandwidth delay reliability load mtu*	再配布されるルートのメトリック値を設定します（EIGRP 専用）。
set metric-type {**internal** | **external** | **type-1** | **type-2**}	再配布されるルートのメトリック タイプを設定します。
set metric-type internal	ネクスト ホップの内部ゲートウェイ プロトコル（IGP）メトリックと一致するように、外部 BGP ネイバーにアドバタイズされるプレフィックスの Multi Exit Discriminator（MED）値を設定します。

コマンドまたはアクション	目的
set tag *tag-value*	再配布されるルートに適用するタグ値を設定します。

ルーティング ドメイン間でのルートの再配布

1 つのルーティング ドメインから別のルーティング ドメインにルートを再配布してルート再配布を制御するには、この作業を実行します。この作業は、BGP ドメインに OSPF ルートを再配布する方法を示します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router bgp***autonomous-system*
4. **redistribute***protocolprocess-id*
5. **default-metric***number*
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	**router bgp***autonomous-system* 例： `Device(config)# router bgp 109`	BGP ルーティング プロセスをイネーブルにし、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	**redistribute***protocolprocess-id* 例： `Device(config-router)# redistribute ospf 2 1`	指定されたルーティング ドメインから別のルーティング ドメインにルートを再配布します。

	コマンドまたはアクション	目的
ステップ 5	**default-metric***number* 例： `Device(config-router)# default-metric 10`	再配布されたルートのデフォルトのメトリック値を設定します。 （注） **redistribute** コマンドで指定されたメトリック値は、**default-metric** コマンドを使用して指定されたメトリック値に優先します。
ステップ 6	**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 モードに戻ります。

再配布ルートのオプションの削除

注意 **redistribute** コマンドに設定したオプションを削除するには、期待する結果が得られるように **no redistribute** コマンドを慎重に使用する必要があります。

異なるプロトコルでは、**no redistribute** コマンドは次のように異なる方法で実装されます。

- BGP、OSPF、RIP の設定では、**no redistribute** コマンドは、実行コンフィギュレーションの **redistribute** コマンドから、指定されたキーワードのみを削除します。これらでは、その他のプロトコルから再配布するときに、減算キーワードの方式を使用します。たとえば、BGP で **no redistribute static route-map interior** を設定する場合、ルート マップのみが再配布から除外され、**redistribute static** がフィルタなしでそのまま残ります。
- **no redistribute isis** コマンドは、実行コンフィギュレーションから IS-IS 再配布を削除します。IS-IS は、IS-IS が再配布されているかどうかや、プロトコルを再配布しているかどうかに関係なく、コマンド全体を削除します。
- EIGRP は、EIGRP コンポーネント バージョン rel5 の前は、減算キーワード方式を使用していました。EIGRP コンポーネント バージョン rel5 以降、**no redistribute** コマンドによって、他のプロトコルから再配布するときに **redistribute** コマンド全体が削除されます。
- **no redistribute connected** コマンドで、**redistribute** コマンドが **router bgp** または **router ospf** コマンドで設定されている場合、動作は減算になります。**router isis** または **router eigrp** コマンドで設定されている場合、動作はコマンドの完全な削除になります。

次の OSPF コマンドは、ルータ コンフィギュレーション モードの再配布から削除されるさまざまなオプションを示します。

コマンドまたはアクション	目的
no redistribute connected metric 1000 subnets	設定されたメトリックの値 1000 と設定されたサブネットを削除し、設定で **redistribute connected** コマンドを保持します。
no redistribute connected metric 1000	設定されたメトリックの値 1000 を削除し、設定で **redistribute connected subnets** コマンドを保持します。
no redistribute connected subnets	設定されたサブネットを削除し、設定で **redistribute connected metric***metric-value* コマンドを保持します。
no redistribute connected	**redistribute connected** コマンドとコマンドに設定されたすべてのオプションを削除します。

ルーティング情報のフィルタリングの設定

（注） ルートが Open Shortest Path First（OSPF）プロセス間で再配信される場合、OSPF メトリックは保持されません。

ルーティング アップデートでのルートのアドバタイジングの制御

他のデバイスが 1 つまたは複数のルートを学習しないように、ルーティング アップデートでのルートのアドバタイズを抑制できます。ルーティング アップデートでルートのアドバタイズを抑制するには、ルータ コンフィギュレーション モードで、**distribute-list** {*access-list-number* | *access-list-name*} **out** [*interface-name* | *routing-process* | *as-number*] コマンドを使用します。

Open Shortest Path First（OSPF）では、インターフェイス名を指定できません。OSPF に使用する場合、この機能は外部ルートにのみ適用されます。

ルーティング アップデートの処理の制御

着信アップデートに含まれている特定のルートを処理することを回避したい場合があります（これは、Open Shortest Path First（OSPF）または Intermediate System to Intermediate System（IS-IS）には適用されません）。着信アップデートのルートを抑制するには、**distribute-list** {*access-list-number* | *access-list-name*} **in** [*interface-typeinterface-number*] コマンドをルータ コンフィギュレーション モードで使用します。

ルーティング情報の送信元のフィルタリング

ルーティング情報発信元をフィルタリングするには、**distance***ip-addresswildcard-mask* [*ip-standard-acl* | *ip-extended-acl* | *access-list-name*] コマンドをルータ コンフィギュレーション モードで使用します。

認証キーの管理

手順の概要

1. イネーブル化
2. **configure terminal**
3. **key chain***name-of-chain*
4. **key***number*
5. **key-string***text*
6. **accept-lifetime***start-time* {**infinite** | *end-time* | **duration***seconds*}
7. **send-lifetime***start-time* {**infinite** | *end-time* | **duration***seconds*}
8. **end**
9. **show key chain**

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： 複数のキーにライフタイムを設定できます。存在する有効なキーの数にかかわらず、送信される認証パケットは1つだけです。キー番号はソフトウェアによって昇順に調べられ、最初に見つかった有効なキーが使用されます。キー変更中は、有効期間が重なっても問題ありません。 `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	**key chain***name-of-chain* 例： `Device(config)# key chain chain1`	キー チェーンを定義して、キー チェーン コンフィギュレーション モードを開始します。
ステップ 4	**key***number* 例： `Device(config-keychain)# key 1`	キーチェーンの認証キーの番号を識別します。キーの範囲は 0 ～ 2147483647 です。キーの ID 番号は連続している必要はありません。
ステップ 5	**key-string***text* 例： `Device(config-keychain-key)# key-string string1`	キー ストリングを確認します。
ステップ 6	**accept-lifetime***start-time* {**infinite** | *end-time* | **duration***seconds*} 例： `Device(config-keychain-key)# accept-lifetime 13:30:00 Dec 22 2011 duration 7200`	キーを受け入れることができる期間を指定します。
ステップ 7	**send-lifetime***start-time* {**infinite** | *end-time* | **duration***seconds*} 例： `Device(config-keychain-key)# send-lifetime 14:30:00 Dec 22 2011 duration 3600`	キーを送信できる期間を指定します。
ステップ 8	**end** 例： `Device(config-keychain-key)# end`	キーチェーン キー 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。
ステップ 9	**show key chain** 例： `Device# show key chain`	（任意）認証キー情報を表示します。

IP ネットワークのモニタリングおよびメンテナンス

IP ルーティング テーブルからのルートの消去

特定のテーブルのすべての内容を削除できます。特定の構造の内容が無効になっている、または無効であると思われるときに、テーブルの消去が必要になる場合があります。

IP ルーティング テーブルから 1 つまたは複数のルートを除外するには、**clear ip route** {*network* [*mask*] | *****} コマンドを特権 EXEC モードで使用します。

システムおよびネットワーク統計情報の表示

システムおよびネットワークの統計情報を表示するには、次の **show** コマンドを使用できます。IP ルーティング テーブル、キャッシュ、データベースの内容など、特定の統計情報を表示できます。また、ノードの到達可能性に関する情報を表示し、デバイスから送信されたパケットがネッ

トワークを通過するルーティング パスを検出することもできます。この情報は、リソースの使用状況を判定してネットワークの問題を解決するために使用されます。

コマンドまたはアクション	目的
show ip cache policy	ポリシー ルート キャッシュのキャッシュ エントリを表示します。
show ip local policy	ローカル ポリシー ルート マップがある場合はそれを表示します。
show ip policy	ポリシー ルート マップを表示します。
show ip protocols	アクティブ ルーティング プロトコルのパラメータと現在の状態を表示します。
show ip route ［*ip-address* ［*mask*］ ［**longer-prefixes**］ ｜ *protocol* ［*process-id*］ ｜ **list** ｛**access-list-number** ｜ *access-list-name*｝ ｜ **static download**］	ルーティング テーブルの現在の状態を表示します。
show ip route summary	サマリー形式でルーティング テーブルの現在のステータスを表示します。
show ip route supernets-only	スーパーネットを表示します。
show key chain ［*name-of-chain*］	認証キーの情報を表示します。
show route-map ［*map-name*］	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。

基本的な IP ルーティングの設定例

例：可変長サブネット マスク

次の例では、クラス B ネットワーク アドレス 172.16.0.0 に 2 つの異なるサブネット マスクを使用します。/24 サブネット マスクは、LAN インターフェイスに使用されます。/24 マスクの場合、1 つのサブネットにつきホスト IP アドレスを 254 個持つサブネットを 265 個使用できます。/24 マスクを使用するサブネット範囲の最後のサブネット（172.16.255.0）は、ポイントツーポイント インターフェイスでの使用に予約されており、さらに長い/30マスクを割り当てられます。172.16.255.0 で /30 マスクを使用すると、1 つのサブネットにつきホスト アドレスを 2 つ持つサブネットが 64 個（172.16.255.0 ～ 172.16.255.252）作成されます。

注意：一義的なルーティングを確実なものにするために、ネットワーク内のLANインターフェイスには 172.16.255.0/24 を割り当てないでください。

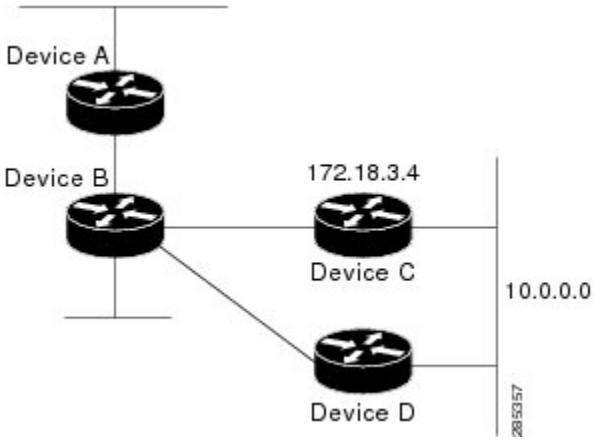
```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 172.16.1.1 255.255.255.0
Device(config-if)# ! 8 bits of host address space reserved for GigabitEthernet interfaces
Device(config-if)# exit
Device(config)# interface Serial 0/0/0
Device(config-if)# ip address 172.16.255.5 255.255.255.252
Device(config-if)# ! 2 bits of address space reserved for point-to-point serial interfaces
Device(config-if)# exit
Device(config)# router rip
Device(config-router)# network 172.16.0.0
Device(config-router)# ! Specifies the network directly connected to the device
```

例：ダイナミック プロトコルによるスタティック ルートの上書き

次の例では、アドミニストレーティブ ディスタンスが 110 未満のルートを使用できない場合、デバイス B（スタティック ルートをインストール済み）からネットワーク 10.0.0.0 へのパケットは 172.18.3.4 経由でルーティングされます。次の図は、この例を示します。アドミニストレーティブ ディスタンスが 110 未満のプロトコルによって学習されたルートにより、デバイス B はネットワーク 10.0.0.0 宛てのトラフィックを代替パスであるデバイス D を経由させて送ります。

```
Device(config)# ip route 10.0.0.0 255.0.0.0 172.18.3.4 110
```

図 *1*：スタティック ルートの上書き



例：IP ルーティングがディセーブルな場合のスタティック IP ネクストホップとしての IP デフォルト ゲートウェイ

次の例では、IP ルーティングがディセーブルの場合に、デフォルト ルートとして IP アドレス 172.16.5.4 を設定する例を示します。

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

```
Device(conf)# no ip routing
Device(conf)# ip default-gateway 172.16.15.4
```

例：アドミニストレーティブ ディスタンス

次の例では、**router eigrp** グローバル コンフィギュレーション コマンドで、自律システム 1 での Enhanced Interior Gateway Routing Protocol（EIGRP）ルーティングを設定します。**network** コマンド設定により、ネットワーク 192.168.7.0 と 172.16.0.0 で EIGRP ルーティングが指定されます。1 つめの **distance** ルータ コンフィギュレーション コマンドでは、デフォルトのアドミニストレーティブ ディスタンスが 255 に設定されます。これにより、明示的なディスタンスが設定されていないデバイスからのルーティング アップデートをすべて無視するようにデバイスに対して指示します。2 つめの **distance** コマンドでは、内部 EIGRP ルートに 80 のアドミニストレーティブ ディスタンス、外部 EIGRP ルートに 100 のアドミニストレーティブ ディスタンスが設定されます。3 つめの **distance** コマンドでは、アドレス 172.16.1.3 のデバイスに 120 のアドミニストレーティブ ディスタンスが設定されます。

```
Device(config)# router eigrp 1
Device(config-router)# network 192.168.7.0
Device(config-router)# network 172.16.0.0
Device(config-router)# distance 255
Device(config-router)# distance eigrp 80 100
Device(config-router)# distance 120 172.16.1.3 0.0.0.0
```

（注） EIGRP から派生したルートのアドミニストレーティブ ディスタンスを設定するには、**distance eigrp** コマンドを使用する必要があります。

次の例では、アドレス 192.168.7.18 のデバイスにアドミニストレーティブ ディスタンス 100 を割り当て、サブネット 192.168.7.0 のその他すべてのデバイスにアドミニストレーティブ ディスタンス 200 を割り当てます。

```
Device(config-router)# distance 100 192.168.7.18 0.0.0.0
Device(config-router)# distance 200 192.168.7.0 0.0.0.255
```

ただし、これら 2 つのコマンドの順序を逆にすると、アドレス 192.168.7.18 のデバイスを含め、サブネット 192.168.7.0 のすべてのデバイスにアドミニストレーティブ ディスタンス 200 が割り当てられます。

```
Device(config-router)# distance 200 192.168.7.0 0.0.0.255
Device(config-router)# distance 100 192.168.7.18 0.0.0.0
```

（注） アドミニストレーティブ ディスタンスの割り当ては、固有の問題を解決するために使用できます。ただし、アドミニストレーティブディスタンスは、ルーティングループまたは他のネットワーク障害が発生しないように、慎重に一貫して適用する必要があります。

次の例では、学習される IP ルートのディスタンス値は 90 です。デフォルトのアドミニストレーティブ ディスタンス値が 110 のルートよりも、これらの IP ルートが優先されます。

```
Device(config)# router isis
Device(config-router)# distance 90 ip
```

例：スタティック ルーティングの再配布

次の例では、3 つのスタティック ルートが指定されます。そのうち 2 つはアドバイタイズされます。スタティック ルートは、**redistribute static** ルータ コンフィギュレーション コマンドを指定し、これら 2 つのネットワークだけが Enhanced Interior Gateway Routing Protocol（EIGRP）プロセスに渡されることを許可するアクセス リストを指定することによって作成されます。再配布されるスタティック ルートは、ルーティング ループ発生の可能性を最小限に抑えるために、1 つのデバイスだけから発信される必要があります。

```
Device(config)# ip route 192.168.2.0 255.255.255.0 192.168.7.65
Device(config)# ip route 192.168.5.0 255.255.255.0 192.168.7.65
Device(config)# ip route 10.10.10.0 255.255.255.0 10.20.1.2
Device(config)# !
Device(config)# access-list 3 permit 192.168.2.0 0.0.255.255
Device(config)# access-list 3 permit 192.168.5.0 0.0.255.255
Device(config)# access-list 3 permit 10.10.10.0 0.0.0.255
Device(config)# !
Device(config)# router eigrp 1
Device(config-router)# network 192.168.0.0
Device(config-router)# network 10.10.10.0
Device(config-router)# redistribute static metric 10000 100 255 1 1500
Device(config-router)# distribute-list 3 out static
```

例：EIGRP 再配布

Enhanced Interior Gateway Routing Protocol（EIGRP）ルーティング プロセスは、1 つの自律システムだけにルーティング情報を提供します。シスコ ソフトウェアは、サービスを提供する自律システムごとに個別のEIGRPプロセスを実行し、異なるルーティングデータベースを維持する必要があります。ただし、これらのルーティング データベース間でルーティング情報を転送できます。

次の設定では、ネットワーク 10.0.0.0 が EIGRP 自律システム 1 の下で設定され、ネットワーク 192.168.7.0 が EIGRP 自律システム 101 の下で設定されます。

```
Device(config)# router eigrp 1
Device(config-router)# network 10.0.0.0
Device(config-router)# exit
Device(config)# router eigrp 101
Device(config-router)# network 192.168.7.0
```

次の例では、ネットワーク 192.168.7.0 からのルートが自律システム 1 に再配布されます（自律システム 101 からのその他のルーティング情報は渡しません）。

```
Device(config)# access-list 3 permit 192.168.7.0
Device(config)# !
Device(config)# route-map 101-to-1 permit 10
Device(config-route-map)# match ip address 3
Device(config-route-map)# set metric 10000 100 1 255 1500
Device(config-route-map)# exit
Device(config)# router eigrp 1
Device(config-router)# redistribute eigrp 101 route-map 101-to-1
Device(config-router)#!
```

次の例は、ネットワーク 192.168.7.0 から自律システム 1 にルートを再配布するための代替方法です。前の設定とは違い、この方法では再配布されるルートのメトリックを設定できません。

```
Device(config)# access-list 3 permit 192.168.7.0
```

```
Device(config)# !
Device(config)# router eigrp 1
Device(config-router)# redistribute eigrp 101
Device(config-router)# distribute-list 3 out eigrp 101
Device(config-router)# !
```

例：EIGRP と RIP 間の相互再配布

内部ルーティング プロトコルとしてルーティング情報プロトコル（RIP）を使用する大学での WAN を想定します。ルーティング プロトコルとして Enhanced Interior Gateway Routing Protocol（EIGRP）を使用する地域ネットワーク 172.16.0.0 にこの大学が WAN を接続すると想定します。この場合の目的は、地域ネットワーク内のデバイスに、大学のネットワーク内のネットワークをアドバタイズすることです。

次の例では、相互再配布が EIGRP と RIP の間に構成されます。

```
Device(config)# access-list 10 permit 172.16.0.0
Device(config)# !
Device(config)# router eigrp 1
Device(config-router)# network 172.16.0.0
Device(config-router)# redistribute rip metric 10000 100 255 1 1500
Device(config-router)# default-metric 10
Device(config-router)# distribute-list 10 out rip
Device(config-router)# exit
Device(config)# router rip
Device(config-router)# redistribute eigrp 1
Device(config-router)# !
```

この例では、EIGRP ルーティング プロセスが開始されます。**network** ルータ コンフィギュレーション コマンドにより、ネットワーク 172.16.0.0（地域ネットワーク）が EIGRP ルーティング情報を送受信するように設定されます。**redistribute** ルータ コンフィギュレーション コマンドにより、RIP から派生したルーティング情報がルーティング アップデートでアドバタイズされるように設定されます。**default-metric** ルータ コンフィギュレーション コマンドにより、EIGRP メトリックが RIP から派生したすべてのルートに割り当てられます。**distribute-list** ルータ コンフィギュレーション コマンドにより、シスコ ソフトウェアに対して、アクセス リスト 10（この例では定義されません）を使用して、各送信アップデートのエントリを制限するように指示します。アクセス リストにより、地域ネットワークへの大学ルートの不正なアドバタイズが防止されます。

例：EIGRP と BGP 間の相互再配布

次の例では、Enhanced Interior Gateway Routing Protocol（EIGRP）とボーダー ゲートウェイ プロトコル（BGP）の間で相互再配布が設定されます。

EIGRP ルーティング プロセス 101 からのルートは BGP 自律システム 50000 に挿入されます。フィルタは、適切なルート（この場合は 3 つのネットワーク）がアドバタイズされるように設定されます。BGP 自律システム 50000 からのルートが、EIGRP ルーティング プロセス 101 に挿入されます。同じフィルタが使用されます。

```
Device(config)# ! All networks that should be advertised from R1 are controlled with ACLs:

Device(config)# access-list 1 permit 172.18.0.0 0.0.255.255
Device(config)# access-list 1 permit 172.16.0.0 0.0.255.255
Device(config)# access-list 1 permit 172.25.0.0 0.0.255.255
Device(config)# ! Configuration for router R1:
```

```
Device(config)# router bgp 50000
Device(config-router)# network 172.18.0.0
Device(config-router)# network 172.16.0.0
Device(config-router)# neighbor 192.168.10.1 remote-as 2
Device(config-router)# neighbor 192.168.10.15 remote-as 1
Device(config-router)# neighbor 192.168.10.24 remote-as 3
Device(config-router)# redistribute eigrp 101
Device(config-router)# distribute-list 1 out eigrp 101
Device(config-router)# exit
Device(config)# router eigrp 101
Device(config-router)# network 172.25.0.0
Device(config-router)# redistribute bgp 50000
Device(config-router)# distribute-list 1 out bgp 50000
Device(config-router)# !
```

注意 他の適切なオプションがない場合、BGP は内部ゲートウェイ プロトコル（IGP）に再配布されます。BGP から IGP への再配布は、配布リスト、IP プレフィックス リスト、およびプレフィックス番号を制限するためのルート マップ ステートメントを使用した適切なフィルタと共に適用されます。

例：OSPF ルーティングおよびルート再配布

OSPF は、通常、多数の内部ルータ、エリア境界ルータ（ABR）、および自律システム境界ルータ（ASBR）間での調整が必要です。OSPF ベースのデバイスは最低でも、すべてのデフォルト パラメータ値を使用し、認証なしで、インターフェイスをエリアに割り当てて設定できます。

ここでは、次の設定例について説明します。

- 最初の例は、基本的な OSPF コマンドを示した簡単な設定です。
- 2 番目の例は、任意に割り当てられた単一の OSPF 自律システム内での内部デバイス、ABR、および ASBR の設定を示しています。
- 3 番目の例は、より複雑な設定と、OSPF ベースのルーティング環境の制御で使用できるさまざまなツールの用途を示しています。

例：基本的な OSPF 設定

次の例では、OSPF ルーティング プロセス 1 をイネーブルにし、エリア 0.0.0.0 にギガビット イーサネット インターフェイス 0/0/0 を接続し、OSPF から RIP と OSPF から RIP に再配布するシンプルな OSPF の設定を示します。

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 172.16.1.1 255.255.255.0
Device(config-if)# ip ospf cost 1
Device(config-if)# exit
Device(config)# interface GigabitEthernet 1/0/0
Device(config-if)# ip address 172.17.1.1 255.255.255.0
Device(config-if)# exit
Device(config)# router ospf 1
Device(config-router)# network 172.18.0.0 0.0.255.255 area 0.0.0.0
Device(config-router)# redistribute rip metric 1 subnets
Device(config-router)# exit
Device(config)# router rip
```

```
Device(config-router)# network 172.17.0.0
Device(config-router)# redistribute ospf 1
Device(config-router)# default-metric 1
Device(config-router)# !
```

次の例では、4 つのエリア ID を 4 つの IP アドレス範囲に割り当てています。この例では、OSPF ルーティング プロセス 1 が初期化され、4 つの OSPF エリア（10.9.50.0、2、3、および 0）が定義されます。エリア 10.9.50.0、2、および 3 は特定のアドレス範囲をマスクし、エリア 0 は他のすべてのネットワークで OSPF をイネーブルにします。

```
Device(config)# router ospf 1
Device(config-router)# network 172.18.20.0 0.0.0.255 area 10.9.50.0
Device(config-router)# network 172.18.0.0 0.0.255.255 area 2
Device(config-router)# network 172.19.10.0 0.0.0.255 area 3
Device(config-router)# network 0.0.0.0 255.255.255.255 area 0
Device(config-router)# exit
Device(config)# ! GigabitEthernet interface 0/0/0 is in area 10.9.50.0:
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 172.18.20.5 255.255.255.0
Device(config-if)# exit
Device(config)# ! GigabitEthernet interface 1/0/0 is in area 2:
Device(config)# interface GigabitEthernet 1/0/0
Device(config-if)# ip address 172.18.1.5 255.255.255.0
Device(config-if)# exit
Device(config)# ! GigabitEthernet interface 2/0/0 is in area 2:
Device(config)# interface GigabitEthernet 2/0/0
Device(config-if)# ip address 172.18.2.5 255.255.255.0
Device(config-if)# exit
Device(config)# ! GigabitEthernet interface 3/0/0 is in area 3:
Device(config)# interface GigabitEthernet 3/0/0
Device(config-if)# ip address 172.19.10.5 255.255.255.0
Device(config-if)# exit
Device(config)# ! GigabitEthernet interface 4/0/0 is in area 0:
Device(config)# interface GigabitEthernet 4/0/0
Device(config-if)# ip address 172.19.1.1 255.255.255.0
Device(config-if)# exit
Device(config)# ! GigabitEthernet interface 5/0/0 is in area 0:
Device(config)# interface GigabitEthernet 5/0/0
Device(config-if)# ip address 10.1.0.1 255.255.0.0
Device(config-if)# !
```

各 **network** ルータ コンフィギュレーション コマンドは順番に評価されるため、設定ではこれらのコマンドの特定の順序が重要になります。シスコ ソフトウェアは、各インターフェイスの *address/wildcard-mask* ペアを順番に評価します。詳細については、『*IP Routing Protocols Command Reference*』を参照してください。

1 つめの **network** コマンドについて考察します。エリア ID 10.9.50.0 が、サブネット 172.18.20.0 があるインターフェイスに設定されます。ギガビット イーサネット インターフェイス 0/0/0 に一致が判定されたと仮定します。ギガビット イーサネット インターフェイス 0/0/0 はエリア 10.9.50.0 だけに接続されます。

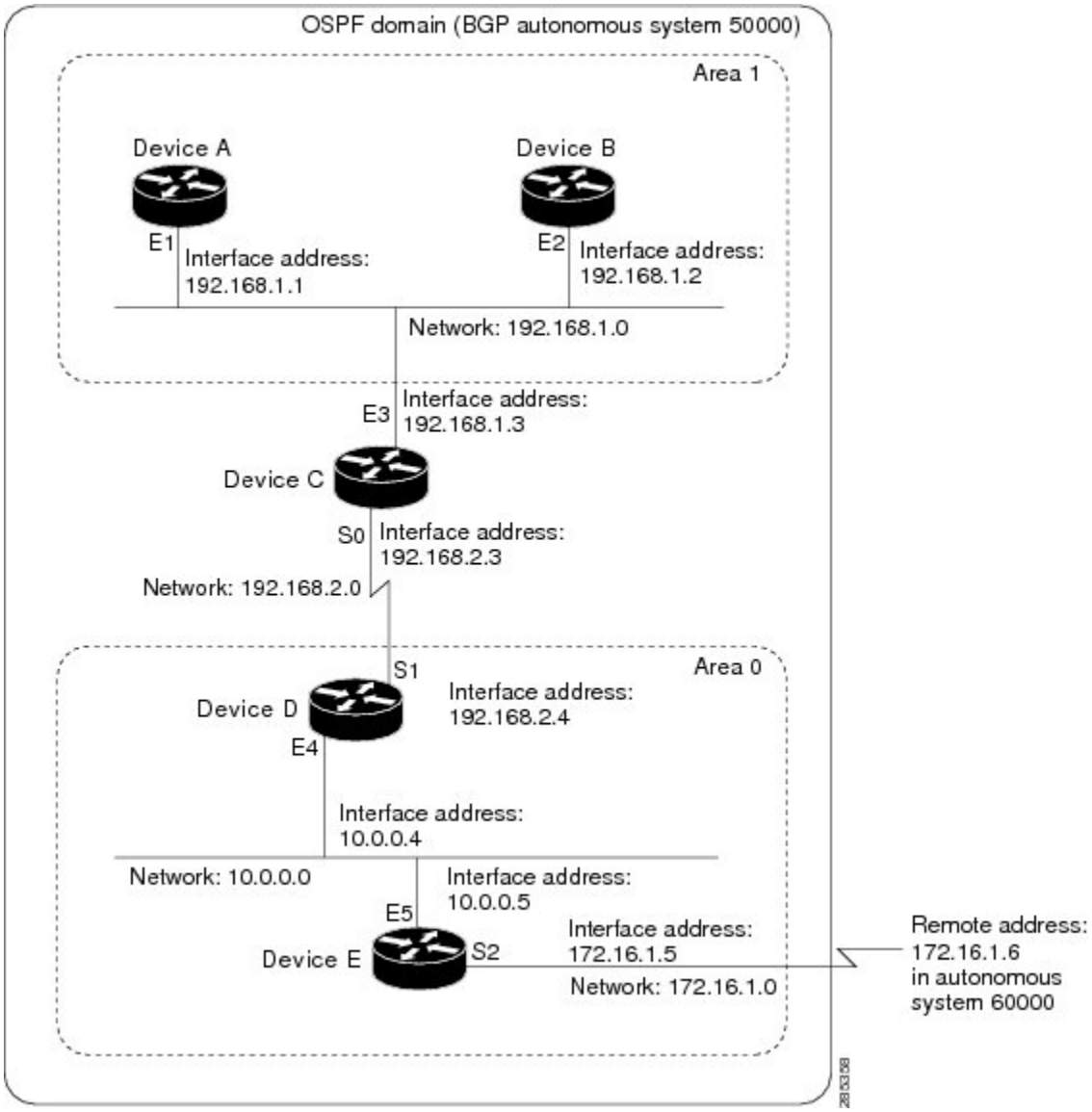
2 つめの **network** コマンドが次に評価されます。エリア 2 について、同じ処理がすべてのインターフェイスに適用されます（ギガビット イーサネット インターフェイス 0/0/0 を除く）。ギガビット イーサネット インターフェイス 1/0/0 に一致が判定されたと仮定します。OSPF がそのインターフェイスに対してイネーブルになり、ギガビット イーサネット 1/0/0 がエリア 2 に接続されます。

インターフェイスを OSPF エリアに接続するこのプロセスは、すべての **network** コマンドに対して継続します。この例にある最後の **network** コマンドは特別な場合なので、注意してください。このコマンドを使用すると、すべての利用可能なインターフェイス（明示的に別のエリアに接続されていないもの）が、エリア 0 に接続されます。

例：内部デバイス、ABR、および ASBR の設定

次の図は、単一の OSPF 自律システム内にあるさまざまなデバイスの設定例を図示した一般的なネットワーク マップです。

図 *2*：*OSPF* 自律システム ネットワーク マップの例



この設定では、OSPF 自律システム 1 に 5 つのデバイスが設定されています。

- デバイス A とデバイス B は、両方ともエリア 1 内の内部デバイスです。
- デバイス C は OSPF ABR です。デバイス C では、エリア 1 が E3 に割り当てられ、エリア 0 が S0 に割り当てられることに注意してください。

- デバイス D は、エリア 0（バックボーン エリア）の内部デバイスです。この場合、どちらの **network** ルータ コンフィギュレーション コマンドも同じエリア（エリア 0、つまりバックボーン エリア）を指定しています。
- デバイス E は OSPF ASBR です。Border Gateway Protocol（BGP）ルートは OSPF に再配布され、これらのルートは OSPF によってアドバタイズされることに注意してください。

（注） OSPF 自律システムのすべてのエリアの定義を、自律システム内のすべてのデバイスの設定に含める必要はありません。直接接続されたエリアだけ、定義する必要があります。次の例では、ABR（デバイス C）がエリア 1 にサマリー リンク ステート アドバタイズメント（LSA）を挿入するときに、エリア 0 のルートがエリア 1 のデバイス（デバイス A およびデバイス B）によって学習されます。

自律システム 60000 は、IP アドレス 172.16.1.6 で、外部ピアへの BGP リンクを介して外部に接続されます。

次に、上の図の一般的なネットワーク マップの設定例を示します。

デバイス A の設定 -- 内部デバイス

```
Device(config)# interface GigabitEthernet 1/0/0
Device(config-if)# ip address 192.168.1.1 255.255.255.0
Device(config-if)# exit
Device(config)# router ospf 1
Device(config-router)# network 192.168.1.0 0.0.0.255 area 1
Device(config-router)# exit
```

デバイス B の設定 -- 内部デバイス

```
Device(config)# interface GigabitEthernet 2/0/0
Device(config-if)# ip address 192.168.1.2 255.255.255.0
Device(config-if)# exit
Device(config)# router ospf 1
Device(config-router)# network 192.168.1.0 0.0.0.255 area 1
Device(config-router)# exit
```

デバイス C の設定 -- ABR

```
Device(config)# interface GigabitEthernet 3/0/0
Device(config-if)# ip address 192.168.1.3 255.255.255.0
Device(config-if)# exit
Device(config)# interface Serial 0/0/0
Device(config-if)# ip address 192.168.2.3 255.255.255.0
Device(config-if)# exit
Device(config)# router ospf 1
Device(config-router)# network 192.168.1.0 0.0.0.255 area 1
Device(config-router)# network 192.168.2.0 0.0.0.255 area 0
Device(config-router)# exit
```

デバイス D の設定 -- 内部デバイス

```
Device(config)# interface GigabitEthernet 4/0/0
Device(config-if)# ip address 10.0.0.4 255.0.0.0
```

```
Device(config-if)# exit
Device(config)# interface Serial 1/0/0
Device(config-if)# ip address 192.168.2.4 255.255.255.0
Device(config-if)# exit
Device(config)# router ospf 1
Device(config-router)# network 192.168.2.0 0.0.0.255 area 0
Device(config-router)# network 10.0.0.0 0.255.255.255 area 0
Device(config-router)# exit
```

デバイス E の設定 -- ASBR

```
Device(config)# interface GigabitEthernet 5/0/0
Device(config-if)# ip address 10.0.0.5 255.0.0.0
Device(config-if)# exit
Device(config)# interface Serial 2/0/0
Device(config-if)# ip address 172.16.1.5 255.255.255.0
Device(config-if)# exit
Device(config)# router ospf 1
Device(config-router)# network 10.0.0.0 0.255.255.255 area 0
Device(config-router)# redistribute bgp 50000 metric 1 metric-type 1
Device(config-router)# exit
Device(config)# router bgp 50000
Device(config-router)# network 192.168.0.0
Device(config-router)# network 10.0.0.0
Device(config-router)# neighbor 172.16.1.6 remote-as 60000
```

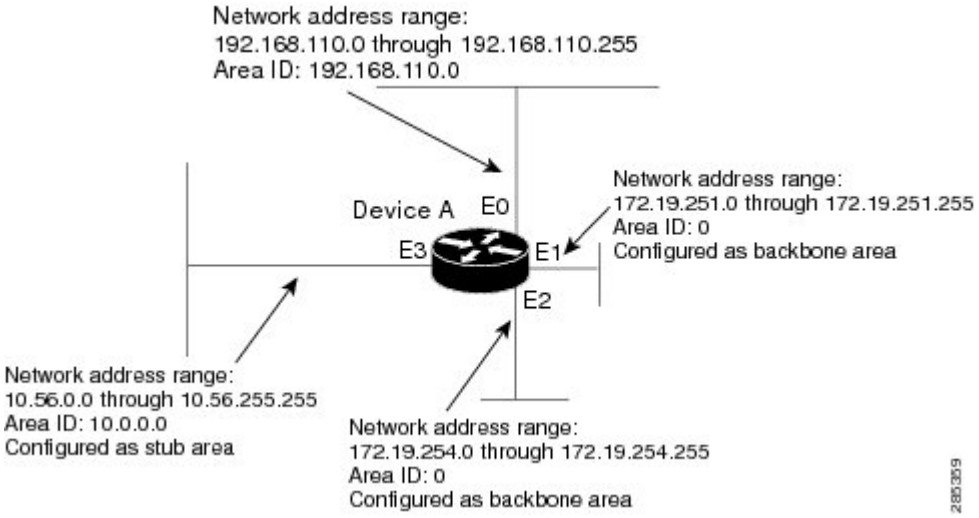
例：複雑な OSPF 設定

次の設定例では、ABR の設定でいくつかのタスクを実行しています。これらのタスクは 2 つの一般カテゴリに分けられます。

- 基本的な OSPF 設定
- ルートの再配布

この設定で概略を示した個々のタスクについて、次に簡単に説明します。次の図は、インターフェイスのネットワーク アドレス範囲とエリア割り当てを示します。

図 *3*：*OSPF* のインターフェイスとエリア指定の設定例



この例の基本的な設定作業は、次のとおりです。

- ギガビットイーサネットインターフェイス 0/0/0 からギガビットイーサネットインターフェイス 3/0/0 のアドレス範囲を設定します。
- 各インターフェイスで OSPF をイネーブルにします。
- 各エリアおよび各ネットワークに OSPF 認証パスワードを設定します。
- リンクステート メトリックおよびその他の OSPF インターフェイス設定オプションを割り当てます。
- エリア ID 10.0.0.0 のスタブ エリアを作成します（**area** ルータ コンフィギュレーション コマンドの **authentication** および **stub** オプションは、別々の **area** コマンド エントリで指定されますが、1 つの **area** コマンドにマージできます）。
- バックボーン エリア（エリア 0）を指定します。

再配布に関連した設定タスクを次に示します。

- さまざまなオプションが設定された OSPF に Enhanced Interior Gateway Routing Protocol（EIGRP）およびルーティング情報プロトコル（RIP）を再配布します（メトリック タイプ、メトリック、タグ、およびサブネットなど）。
- EIGRP と OSPF を RIP に再配布する。

次に、OSPF の設定例を示します。

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 192.168.110.201 255.255.255.0
```

```
Device(config-if)# ip ospf authentication-key abcdefgh
Device(config-if)# ip ospf cost 10
Device(config-if)# exit
Device(config)# interface GigabitEthernet 1/0/0
Device(config-if)# ip address 172.19.251.201 255.255.255.0
Device(config-if)# ip ospf authentication-key ijklmnop
Device(config-if)# ip ospf cost 20
Device(config-if)# ip ospf retransmit-interval 10
Device(config-if)# ip ospf transmit-delay 2
Device(config-if)# ip ospf priority 4
Device(config-if)# exit
Device(config)# interface GigabitEthernet 2/0/0
Device(config-if)# ip address 172.19.254.201 255.255.255.0
Device(config-if)# ip ospf authentication-key abcdefgh
Device(config-if)# ip ospf cost 10
Device(config-if)# exit
Device(config)# interface GigabitEthernet 3/0/0
Device(config-if)# ip address 10.56.0.201 255.255.0.0
Device(config-if)# ip ospf authentication-key ijklmnop
Device(config-if)# ip ospf cost 20
Device(config-if)# ip ospf dead-interval 80
Device(config-if)# exit
```

次の設定では、OSPF はネットワーク 172.19.0.0 にあります。

```
Device(config)# router ospf 1
Device(config-router)# network 10.0.0.0 0.255.255.255 area 10.0.0.0
Device(config-router)# network 192.168.110.0 0.0.0.255 area 192.168.110.0
Device(config-router)# network 172.19.0.0 0.0.255.255 area 0
Device(config-router)# area 0 authentication
Device(config-router)# area 10.0.0.0 stub
Device(config-router)# area 10.0.0.0 authentication
Device(config-router)# area 10.0.0.0 default-cost 20
Device(config-router)# area 192.168.110.0 authentication
Device(config-router)# area 10.0.0.0 range 10.0.0.0 255.0.0.0
Device(config-router)# area 192.168.110.0 range 192.168.110.0 255.255.255.0
Device(config-router)# area 0 range 172.19.251.0 255.255.255.0
Device(config-router)# area 0 range 172.19.254.0 255.255.255.0
Device(config-router)# redistribute eigrp 200 metric-type 2 metric 1 tag 200 subnets
Device(config-router)# redistribute rip metric-type 2 metric 1 tag 200
Device(config-router)# exit
```

次の設定では、EIGRP 自律システム 1 が 172.19.0.0 にあります。

```
Device(config)# router eigrp 1
Device(config-router)# network 172.19.0.0
Device(config-router)# exit
Device(config)# ! RIP for 192.168.110.0:
Device(config)# router rip
Device(config-router)# network 192.168.110.0
Device(config-router)# redistribute eigrp 1 metric 1
Device(config-router)# redistribute ospf 201 metric 1
Device(config-router)# exit
```

例：デフォルト メトリック値の再配布

次の例では、自律システム 1 のデバイスが Routing Information Protocol（RIP）と Enhanced Interior Gateway Routing Protocol（EIGRP）の両方を実行するよう設定されています。この例では、RIP を使用して EIGRP から派生したルートをアドバタイズし、EIGRP から派生したルートに RIP メトリック 10 を割り当てます。

```
Device(config)# router rip
Device(config-router)# redistribute eigrp 1
```

```
Device(config-router)# default-metric 10
Device(config-router)# exit
```

例：ルート マップを使用した場合と使用しない場合の再配布

ここでは、ルート マップを使用した場合と、使用しない場合の再配布の例を示します。IP および Connectionless Network Service（CLNS）の両方のルーティング プロトコルの例が示されています。

次の例では、すべての Open Shortest Path First（OSPF）ルートを Enhanced Interior Gateway Routing Protocol（EIGRP）に再配布します。

```
Device(config)# router eigrp 1
Device(config-router)# redistribute ospf 101
Device(config-router)# exit
```

次の例では、ホップ カウントが 1 のルーティング情報プロトコル（RIP）ルートを OSPF に再配布しています。これらのルートは、メトリック 5、メトリック タイプ 1、およびタグ 1 の外部リンク ステート アドバタイズメント（LSA）として OSPF に再配布されます。

```
Device(config)# router ospf 1
Device(config-router)# redistribute rip route-map rip-to-ospf
Device(config-router)# exit
Device(config)# route-map rip-to-ospf permit
Device(config-route-map)# match metric 1
Device(config-route-map)# set metric 5
Device(config-route-map)# set metric-type type 1
Device(config-route-map)# set tag 1
Device(config-route-map)# exit
```

次の例では、OSPF で学習されたタグ 7 のルートを、RIP メトリック 15 として再配布しています。

```
Device(config)# router rip
Device(config-router)# redistribute ospf 1 route-map 5
Device(config-router)# exit
Device(config)# route-map 5 permit
Device(config-route-map)# match tag 7
Device(config-route-map)# set metric 15
```

次の例では、シリアル インターフェイス 0/0/0 のネクスト ホップ デバイスで、OSPF エリア内およびエリア間ルートをボーダー ゲートウェイ プロトコル（BGP）に 5 の INTER_AS メトリックで再配布します。

```
Device(config)# router bgp 50000
Device(config-router)# redistribute ospf 1 route-map 10
Device(config-router)# exit
Device(config)# route-map 10 permit
Device(config-route-map)# match route-type internal
Device(config-route-map)# match interface serial 0/0/0
Device(config-route-map)# set metric 5
```

次の例では、2 つのタイプのルートを（IP と CLNS のいずれもサポートする）統合 IS-IS ルーティング テーブルに再配布しています。1 つめのタイプは、タグ 5 の OSPF 外部 IP ルートです。これらのルートは、メトリック 5 のレベル 2 IS-IS リンクステート パケット（LSP）に挿入されます。2 番目のタイプは CLNS アクセス リスト 2000 と一致する ISO-IGRP から発生した CLNS プレフィックスです。これらのルートはメトリック 30 のレベル 2 IS-IS LSP に再配布されます。

```
Device(config)# router isis
Device(config-router)# redistribute ospf 1 route-map 2
Device(config-router)# redistribute iso-igrp nsfnet route-map 3

Device(config-router)# exit
```

```
Device(config)# route-map 2 permit
Device(config-route-map)# match route-type external
Device(config-route-map)# match tag 5
Device(config-route-map)# set metric 5
Device(config-route-map)# set level level-2
Device(config-route-map)# exit
Device(config)# route-map 3 permit
Device(config-route-map)# match address 2000
Device(config-route-map)# set metric 30
Device(config-route-map)# exit
```

次の設定では、タグ 1、2、3、および 5 の OSPF 外部ルータがそれぞれメトリック 1、1、5、および 5 の RIP に再配布されています。タグ 4 の OSPF ルートは再配布されません。

```
Device(config)# router rip
Device(config-router)# redistribute ospf 101 route-map 1
Device(config-router)# exit
Device(config)# route-map 1 permit
Device(config-route-map)# match tag 1 2
Device(config-route-map)# set metric 1
Device(config-route-map)# exit
Device(config)# route-map 1 permit
Device(config-route-map)# match tag 3
Device(config-route-map)# set metric 5
Device(config-route-map)# exit
Device(config)# route-map 1 deny
Device(config-route-map)# match tag 4
Device(config-route-map)# exit
Device(config)# route map 1 permit
Device(config-route-map)# match tag 5
Device(config-route-map)# set metric 5
Device(config-route-map)# exit
```

次の設定の場合、RIP が学習したネットワーク 172.18.0.0 のルートと ISO-IGRP が学習したプレフィックス 49.0001.0002 のルートを、メトリック 5 の IS-IS レベル 2 LSP に再配布します。

```
Device(config)# router isis
Device(config-router)# redistribute rip route-map 1
Device(config-router)# redistribute iso-igrp remote route-map 1
Device(config-router)# exit
Device(config)# route-map 1 permit
Device(config-route-map)# match ip address 1
Device(config-route-map)# match clns address 2
Device(config-route-map)# set metric 5
Device(config-route-map)# set level level-2
Device(config-route-map)# exit
Device(config)# access-list 1 permit 172.18.0.0 0.0.255.255
Device(config)# clns filter-set 2 permit 49.0001.0002...
```

次の設定例では、**default-information** ルータ コンフィギュレーション コマンドでルート マップを参照する手順を示しています。このような参照は、「条件付きのデフォルト発信元」と呼ばれます。172.20.0.0 がルーティング テーブルにある場合、OSPF はタイプ 2 メトリック 5 のデフォルト ルート（ネットワーク 0.0.0.0）を発信します。

```
Device(config)# route-map ospf-default permit
Device(config-route-map)# match ip address 1
Device(config-route-map)# set metric 5
Device(config-route-map)# set metric-type type-2
Device(config-route-map)# exit
Device(config)# access-list 1 172.20.0.0 0.0.255.255
Device(config)# router ospf 101
Device(config-router)# default-information originate route-map ospf-default
```

例：キー管理

次の例では、chain1 という名前のキー チェーンが設定されます。この例では、ソフトウェアは有効なキーとして key1 を常に受け入れて送信します。キー key2 は午後 1 時 30 分から午後 3 時 30 分まで受け入れられ、午後 2 時から午後 3 時まで送信されます。時間帯が重複することにより、キーを移行することができ、またデバイスの設定時間の不一致も許容されます。同様に、キー key3 はすぐに key2 に従い、時刻の相違に対処するためそれぞれに 30 分あります。

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip rip authentication key-chain chain1
Device(config-if)# ip rip authentication mode md5
Device(config-if)# exit
Device(config)# router rip
Device(config-router)# network 172.19.0.0
Device(config-router)# version 2
Device(config-router)# exit
Device(config)# key chain chain1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string key1
Device(config-keychain-key)# exit
Device(config-keychain)# key 2
Device(config-keychain-key)# key-string key2
Device(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2005 duration 7200
Device(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2005 duration 3600
Device(config-keychain-key)# exit
Device(config-keychain)# key 3
Device(config-keychain-key)# key-string key3
Device(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2005 duration 7200
Device(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2005 duration 3600
Device(config-keychain-key)# end
```

次の例では、chain1 という名前のキー チェーンが設定されます。

```
Device(config)# key chain chain1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string key1
Device(config-keychain-key)# exit
Device(config-keychain)# key 2
Device(config-keychain-key)# key-string key2
Device(config-keychain-key)# accept-lifetime 00:00:00 Dec 5 2004 23:59:59 Dec 5 2005
Device(config-keychain-key)# send-lifetime 06:00:00 Dec 5 2004 18:00:00 Dec 5 2005
Device(config-keychain-key)# exit
Device(config-keychain)# exit
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 172.19.104.75 255.255.255.0 secondary 172.19.232.147
255.255.255.240
Device(config-if)# ip rip authentication key-chain chain1
Device(config-if)# media-type 10BaseT
Device(config-if)# exit
Device(config)# interface GigabitEthernet 1/0/0
Device(config-if)# no ip address
Device(config-if)# shutdown
Device(config-if)# media-type 10BaseT
Device(config-if)# exit
Device(config)# interface Fddi 0
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# no keepalive
Device(config-if)# exit
Device(config)# interface Fddi 1/0/0
Device(config-if)# ip address 172.16.1.1 255.255.255.0
Device(config-if)# ip rip send version 1
Device(config-if)# ip rip receive version 1
Device(config-if)# no keepalive
Device(config-if)# exit
```

```
Device(config)# router rip
Device(config-router)# version 2
Device(config-router)# network 172.19.0.0
Device(config-router)# network 10.0.0.0
Device(config-router)# network 172.16.0.0
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
IP ルーティングのプロトコル独立型コマンド	『Cisco IOS IP Routing: Protocol-Independent 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

基本的な IP ルーティングの機能情報

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 *2*：基本的な *IP* ルーティングの機能情報

機能名	リリース	機能情報
IP ルーティング		IP ルーティング機能により、このモジュールと他の IP ルーティングプロトコルのモジュールで説明されている基本的な IP ルーティング機能が導入されました。

第 3 章

IPv6 ルーティング：スタティック ルーティング

この機能は、IPv6 のスタティック ルーティングを提供します。スタティック ルートは、手動で設定され、2 つのネットワーク デバイス間の明示パスを定義します。

- 機能情報の確認，39 ページ
- IPv6 ルーティング：スタティック ルーティングの前提条件，40 ページ
- IPv6 ルーティング：スタティック ルーティングの制約事項，40 ページ
- IPv6 ルーティング：スタティック ルーティングに関する情報，40 ページ
- IPv6 スタティック ルーティングの設定方法，43 ページ
- IPv6 スタティック ルーティングの設定例，47 ページ
- その他の参考資料，50 ページ
- IPv6 ルーティング：スタティック ルーティングの機能情報，51 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 ルーティング：スタティック ルーティングの前提条件

スタティック IPv6 ルートでデバイスを設定する前に、**ipv6 unicast-routing** 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 IPv6 パケットの転送を有効にし、1 つ以上のインターフェイスで IPv6 を有効にし、そのインターフェイスで IPv6 アドレスを設定する必要があります。

IPv6 ルーティング：スタティック ルーティングの制約事項

- IPv6 スタティック ルートは、IPv4 **ip route** コマンドのタグおよび永続キーワードをサポートしません。
- IPv6 は、仮想ルーティングおよび転送（VRF）テーブルへのスタティック ルートの挿入をサポートしていません。
- スタティック設定が、リブート時やユーザがデバイスを切断して再接続するときに失われるため、ダイナミック インターフェイス上でスタティック設定を設定しないでください。

IPv6 ルーティング：スタティック ルーティングに関する情報

スタティック ルート

ネットワーキングデバイスでは、手動で設定したルート情報、またはルーティングプロトコルを使用してダイナミックに学習したルート情報を使用して、パケットを転送します。スタティックルートは、手動で設定され、2つのネットワークデバイス間の明示パスを定義します。ダイナミック ルーティング プロトコルとは異なり、スタティック ルートは動的に更新されず、ネットワーク トポロジが変更された場合は手動で再設定する必要があります。スタティックルートを使用する利点は、セキュリティが高まり、リソースが効率化されることです。スタティック ルートでは、ダイナミックルーティングプロトコルよりも少ない帯域幅を使用し、ルートの計算および通信にCPUサイクルが使用されません。スタティックルートを使用する場合の主なデメリットは、ネットワーク トポロジが変更された場合に自動的に再設定されないことです。

スタティック ルートはダイナミック ルーティング プロトコルに再配布できますが、ダイナミック ルーティング プロトコルによって生成されたルートは、スタティック ルーティング テーブルに再配布できません。スタティックルートを使用するルーティングループの設定を回避するアルゴリズムはありません。

スタティック ルートは、外部ネットワークへのパスが 1 つしかない小規模ネットワークでは有用です。また、大規模ネットワークの場合は、より厳格な制御が必要な、他のネットワークへの特定のタイプのトラフィックやリンクにセキュリティを提供します。一般に、大半のネットワークでは、ダイナミック ルーティング プロトコルを使用してネットワーキング デバイス間の通信を行いますが、特殊なケース用として 1 つまたは 2 つのスタティック ルートを設定している場合があります。

直接接続されているスタティック ルート

直接接続されたスタティック ルートでは、出力インターフェイスだけが指定されます。宛先は、出力インターフェイスに直接接続されていると想定されるため、パケットの宛先はネクストホップ アドレスとして使用されます。次に、このような定義の例を示します。

```
ipv6 route 2001:DB8::/32 gigabitethernet1/0/0
```

この例では、アドレス プレフィックス 2001:DB8::/32 を持つすべての宛先がインターフェイス GigabitEthernet1/0/0 経由で直接到達可能であることを指定しています。

直接接続されたスタティック ルートは、有効な IPv6 インターフェイス（つまり、アップ状態にあり、かつ IPv6 がイネーブルになっているインターフェイス）を示している場合にかぎり、IPv6 ルーティング テーブルに挿入される候補となります。

再帰スタティック ルート

再帰スタティック ルートでは、ネクストホップだけが指定されます。出力インターフェイスはネクスト ホップから取得されます。次に、このような定義の例を示します。

```
ipv6 route 2001:DB8::/32 2001:DB8:3000:1
```

この例では、アドレス プレフィックス 2001:DB8::/32 を持つすべての宛先が、アドレス 2001:DB8:3000:1 を持つホストを介して到着可能であることを指定しています。

再帰スタティック ルートが有効である（つまり、IPv6 ルーティング テーブルに挿入される候補である）のは、指定したネクストホップが直接的または間接的に有効な IPv6 出力インターフェイスに解決され、ルートが自己再帰型ではなく、再帰深度が IPv6 転送の最大再帰深度を超えていない場合だけです。

自身のネクスト ホップ解決に使用されるのがそのルート自身である場合、ルートは自己再帰します。たとえば、IPv6 ルーティング テーブルに次のルートがあるとします。

```
IPv6 Routing Table - 9 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
R   2001:DB8::/32 [130/0]
     via ::, Serial2/0
B   2001:DB8:3000:0/16 [200/45]
     Via 2001:DB8::0104
```

次の例では、再帰 IPv6 スタティック ルートを定義します。

```
ipv6 route
2001:DB8::/32 2001:0BD8:3000:1
```

このスタティック ルートは、自己再帰型であるため、IPv6ルーティングテーブルには挿入されません。スタティック ルートのネクスト ホップ 2001:DB8:3000:1 は、自身が再帰ルートである（つまり、ネクスト ホップだけを指定する）BGP ルート 2001:DB8:3000:0/16 を介して解決されます。BGP ルートのネクスト ホップ 2001:DB8::0104 はスタティック ルートを介して解決されます。したがって、スタティック ルートは、スタティック ルート自身のネクスト ホップを解決するために使用されることになります。

一般に、自己再帰型スタティック ルートの手動設定は禁止されていませんが、有用ではありません。ただし、IPv6ルーティングテーブルに挿入された再帰スタティックルートが、ダイナミック ルーティング プロトコルを介して学習された、ネットワークでの何らかの一時的変更の結果として自己再帰になる場合があります。このような状況が発生すると、スタティック ルートが自己再帰になった事実が検出され、そのスタティック ルートは IPv6 ルーティング テーブルから削除されます（設定からは削除されません）。以降のネットワーク変更によって、スタティック ルートが自己再帰でなくなる場合があります。この場合、そのスタティックルートはIPv6ルーティングテーブルに再挿入されます。

完全指定のスタティック ルート

完全指定のスタティックルートでは、出力インターフェイスとネクストホップの両方が指定されています。この形式のスタティックルートは、出力インターフェイスがマルチアクセスインターフェイスであり、ネクスト ホップを明示的に識別する必要がある場合に使用されます。ネクスト ホップは、指定した出力インターフェイスに直接接続されている必要があります。次の例に、完全指定のスタティック ルートの定義を示します。

```
ipv6 route 2001:DB8:/32 gigabitethernet1/0/0 2001:DB8:3000:1
```

完全指定のルートが有効である（つまり、IPv6 ルーティング テーブルに挿入される候補である）のは、指定した IPv6 インターフェイスが IPv6 対応であり、かつアップ状態となっている場合です。

フローティング スタティック ルート

フローティング スタティック ルートは、設定されたルーティング プロトコルを介して学習されたダイナミック ルートのバックアップに使用されるスタティック ルートです。フローティング スタティックルートには、バックアップしているルーティングプロトコルよりも大きなアドミニストレーティブディスタンスが設定されています。このため、ルーティングプロトコルを介して学習されたダイナミック ルートは、フローティング スタティック ルートよりも常に優先して使用されます。ルーティングプロトコルを介して学習されたダイナミックルートが失われると、フローティング スタティック ルートが代わりに使用されます。次に、フローティング スタティック ルートを定義する例を示します。

```
ipv6 route 2001:DB8:/32 gigabitethernet1/0/0 2001:DB8:3000:1 210
```

3 つのタイプの IPv6 スタティック ルートのいずれも、フローティング スタティック ルートとして使用できます。フローティング スタティック ルートは、ダイナミック ルーティング プロトコルよりも大きいアドミニストレーティブ ディスタンスを使用して設定する必要があります。これは、小さいアドミニストレーティブ ディスタンスが設定されたルートの方が優先されるためです。

（注） デフォルトで、スタティック ルートはダイナミック ルートよりも小さいアドミニストレーティブ ディスタンスを持っているため、スタティック ルートは、ダイナミック ルートよりも優先して使用されます。

IPv6 スタティック ルーティングの設定方法

スタティック IPv6 ルートの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6route***ipv6-prefix*/*prefix-lengthipv6-address* | *interface-typeinterface-numberipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | **unicast**| **multicast**] [**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。
ステップ 3	**ipv6route***ipv6-prefix*/*prefix-lengthipv6-address*	*interface-typeinterface-numberipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance*	**unicast**| **multicast**] [**tag***tag*]	スタティック IPv6 ルートを設定します。 • デフォルトのスタティック IPv6 ルートは、シリアル インターフェイス上で設定されます。

	コマンドまたはアクション	目的
	例： `Device(config)# ipv6 route ::/0 serial 2/0`	• この表の直後の構文例で、スタティック ルートを設定するための **ipv6route** コマンドの特別な使用法を参照してください。

デフォルトの IPv6 スタティック ルートを使用するための再帰 IPv6 スタティック ルートの設定

デフォルトでは、再帰 IPv6 スタティック ルートは、デフォルト ルート（::/0）を使用して解決されません。従来の動作に戻して、デフォルト ルートを使用して解決できるようにするには、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. **ipv6routestaticresolvedefault**

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	**ipv6routestaticresolvedefault** 例： `Device(config)# ipv6 route static resolve default`	デフォルトの IPv6 スタティック ルートを使用して再帰 IPv6 スタティック ルートを解決できるようにします。

フローティング スタティック IPv6 ルートの設定

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6route***ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-typeinterface-numberipv6-address*}} [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [**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。
ステップ 3	**ipv6route***ipv6-prefix*/*prefix-length* {*ipv6-address* | *interface-typeinterface-numberipv6-address*}} [*administrative-distance*] [*administrative-multicast-distance* | **unicast** | **multicast**] [**tag***tag*] 例： `Device(config)# ipv6 route 2001:DB8::/32 serial 2/0 201`	スタティック IPv6 ルートを設定します。 • この例では、フローティング スタティック IPv6 ルートが設定されます。 • デフォルトのアドミニストレーティブ ディスタンスは、次のとおりです。 　• 接続されたインターフェイス：0 　• スタティック ルート：1 　• Enhanced Interior Gateway Routing Protocol（EIGRP）サマリー ルート：5 　• 外部ボーダー ゲートウェイ プロトコル（eBGP）：20 　• 内部 Enhanced IGRP：90 　• IGRP：100 　• Open Shortest Path First（OSPF）：110 　• Intermediate System-to-Intermediate System（IS-IS）：115

	コマンドまたはアクション	目的
		• ルーティング情報プロトコル（RIP）：120 • 外部ゲートウェイ プロトコル（EGP）：140 • EIGRP 外部ルート：170 • 内部 BGP：200 • 不明：255

スタティック IPv6 ルートの設定と動作の確認

手順の概要

1. イネーブル化
2. 次のいずれかを実行します。
   - **showipv6static** [*ipv6-address* | *ipv6-prefix*/*prefix-length*][**interface***interface-typeinterface-number*] [**recursive**] [**detail**]
   - **showipv6route** [*ipv6-address* | *ipv6-prefix*/*prefix-length* | *protocol* | *interface-typeinterface-number*]
3. **debugipv6routing**

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	次のいずれかを実行します。 • **showipv6static** [*ipv6-address* | *ipv6-prefix*/*prefix-length*][**interface***interface-typeinterface-number*] [**recursive**] [**detail**] • **showipv6route** [*ipv6-address* | *ipv6-prefix*/*prefix-length* | *protocol* | *interface-typeinterface-number*]	IPv6 ルーティング テーブルの現在の内容を表示します。 • これらの例は、IPv6 スタティック ルートを表示する 2 つの方法を示しています。

	コマンドまたはアクション	目的

	例：
	`Device# show ipv6 static`
	
	例：
	`Device# show ipv6 route static`	

ステップ 3	**debugipv6routing** 例： `Device# debug ipv6 routing`	IPv6 ルーティング テーブルの更新およびルート キャッシュの更新に関するデバッグ メッセージを表示します。

IPv6 スタティック ルーティングの設定例

スタティック ルートは、さまざまな目的に使用できます。一般的な使用方法は、次のとおりです。

- 手動集約
- トラフィック廃棄
- デフォルトの固定ルート
- バックアップ ルート

多くの場合、シスコ ソフトウェアには、同一の目的を果たすための代替メカニズムが用意されています。スタティック ルートを使用するか、またはいずれかの代替メカニズムを使用するかは、ローカルの状況によって決まります。

手動集約の設定例

次に、RIP にアドバタイズされるローカル インターフェイス プレフィックスを集約するために使用するスタティック ルートの例を示します。スタティック ルートは、廃棄ルートとしても機能し、より具体的なインターフェイスプレフィックスの対象とならない 2001:DB8:1::/48 宛先に対する、ルータが受信したパケットを廃棄します。

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet0/0/0
Router(config-if)# ipv6 address 2001:DB8:2:1234/64
Router(config-if)# exit
```

```
Router(config)#
Router(config)# interface gigabitethernet1/0/0
Router(config-if)# ipv6 address 2001:DB8:3:1234/64
Router(config-if)# exit
Router(config)#
Router(config)# interface gigabitethernet2/0/0
Router(config-if)# ipv6 address 2001:DB8:4:1234/64
Router(config-if)# exit
Router(config)#
Router(config)# interface gigabitethernet3/0/0
Router(config-if)# ipv6 address 2001:DB8::1234/64
Router(config-if)# ipv6 rip one enable
Router(config-if)# exit
Router(config)#
Router(config)# ipv6 router rip one
Router(config-rtr)# redistribute static
Router(config-rtr)# exit
Router(config)#
Router(config)# ipv6 route 2001:DB8:1:1/48 null0
Router(config)# end
Router#
00:01:30: %SYS-5-CONFIG_I: Configured from console by console
Router# show ipv6 route static

IPv6 Routing Table - 3 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, 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
S   2001:DB8:1::/48 [1/0]
     via ::, Null0
```

例：トラフィック廃棄の設定

インターフェイス null0 をポイントするようにスタティック ルートを設定することで、特定のプレフィックスへのトラフィックを廃棄できます。たとえば、プレフィックス 2001:DB8:42:1/64 へのすべてのトラフィックを廃棄する必要がある場合は、次のスタティック ルートが定義されます。

```
Device> enable
Device# configure
 terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ipv6 route 2001:DB8:42:1::/64 null0
Device(config)# end
```

例：デフォルトの固定ルートの設定

デフォルトのスタティック ルートは、多くの場合、単純なルータ トポロジで使用されます。次の例では、ルータは、GigabitEthernet 0/0/0 を介してそのローカル サイトに接続され、Serial 2/0/0 と Serial 3/0/0 を介して主要な企業メッセージに接続されます。非ローカル トラフィックはすべて、2 つのシリアル インターフェイスを介してルーティングされます。

```
Router(config)# interface gigabitethernet0/0/0
Router(config-if)# ipv6 address 2001:DB8:17:1234/64
Router(config-if)# exit
Router(config)# interface Serial2/0/0
Router(config-if)# ipv6 address 2001:DB8:1:1234/64
```

```
Router(config-if)# exit
Router(config)# interface Serial3/0/0
Router(config-if)# ipv6 address 2001:DB8:2:124/64
Router(config-if)# exit
Router(config)# ipv6 route ::/0 Serial2/0
Router(config)# ipv6 route ::/0 Serial3/0
Router(config)# end
Router#
00:06:30: %SYS-5-CONFIG_I: Configured from console by console
Router# show ipv6 route static
IPv6 Routing Table - 7 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, 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
S   ::/0 [1/0]
     via ::, Serial2/0
     via ::, Serial3/0
```

例：フローティング スタティック ルートの設定

多くの場合、フローティングスタティックルートは、接続の問題が発生した場合にバックアップパスを提供するために使用されます。次の例では、ルータは、GigabitEthernet0/0/0 を介してネットワーク コアに接続されており、IS-IS を介してルート 2001:DB8:1:1/32 を学習します。GigabitEthernet0/0/0 インターフェイスに障害が発生するか、またはルート 2001:DB8:1:1/32 が IS-IS を介して学習されなくなった（ネットワークのいずれかの箇所で接続が失われていることを示します）場合、トラフィックはバックアップ ISDN インターフェイスを介してルーティングされます。

```
Router> enable
Router# configure
 terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet0/0/0
Router(config-if)# ipv6 address 2001:DB8:17:1234/64
Router(config-if)# exit
Router(config)# interface gigabitethernet0/0/0
Router(config-if)# ipv6 address 2001:DB8:1:1234/64
Router(config-if)# ipv6
 router
 isis
Router(config-if)# exit
Router(config)# router isis
Router(config-router)# net 42.0000.0000.0000.0001.00
Router(config-router)# exit
Router(config)# interface BRI1/0
Router(config-if)# encapsulation ppp
Router(config-if)# ipv6 enable
Router(config-if)# isdn switch-type basic-net3
Router(config-if)# ppp authentication chap optional
Router(config-if)# ppp multilink
Router(config-if)# exit
Router(config)# dialer-list 1 protocol ipv6 permit
Router(config)# ipv6 route 2001:DB8:1::/32 BRI1/0 200
Router(config)# end
Router#
00:03:07: %SYS-5-CONFIG_I: Configured from console by console
```

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
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	Title
IPv6 に関する RFC	*IPv6 の RFC*

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

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 ルーティング：スタティック ルーティングの機能情報

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 *3*：*IPv6* ルーティング：スタティック ルーティングの機能情報

機能名	リリース	機能情報
IPv6 ルーティング：スタティック ルーティング	12.0(22)S 12.2(2)T 12.2(14)S 12.2(17a)SX1 12.2(25)SG 12.2(28)SB 12.2(33)SRA Cisco IOS XE Release 2.1	スタティック ルートは、手動で設定され、2 つのネットワーク デバイス間の明示パスを定義します。 次のコマンドが導入または変更されました。**ipv6 route**、**ipv6 route static resolve default**、**show ipv6 route**、**show ipv6 static**

第 4 章

IPv4 ループ フリー代替高速再ルーティング

リンクやルータに障害が発生すると、分散ルーティング アルゴリズムによって障害を考慮した新しいルートが計算されます。計算のための時間をルーティングの遷移と呼びます。遷移が完了し、すべてのルータがネットワーク上の共通のビューで収束されるまで、送信元と宛先のペア間の接続は中断されます。事前計算済みの代替ネクスト ホップを使用してルーティングの遷移時間を 50 ミリ秒より少なくするために、IPv4 ループ フリー代替高速再ルーティング機能を使用できます。リンク障害の通知を受けると、ルータはトラフィック損失を減らすために、修復パスにすぐに切替えます。

IPv4 ループ フリー代替高速再ルーティングは、修復パスの事前計算をサポートします。修復パスの計算は、Intermediate System-to-Intermediate System（IS-IS）ルーティング プロトコルによって実行され、結果の修復パスはルーティング情報ベース（RIB）に送信されます。修復パスのインストールは、シスコ エクスプレス フォワーディング（以前は CEF と呼ばれる）と Open Shortest Path First（OSPF）によって実行されます。

- 機能情報の確認，53 ページ
- IPv4 ループ フリー代替高速再ルーティングのための前提条件，54 ページ
- IPv4 ループ フリー代替高速再ルーティングの制約事項，54 ページ
- IPv4 ループ フリー代替高速再ルーティングに関する情報，55 ページ
- IPv4 ループ フリー代替高速再ルーティングの設定方法，58 ページ
- IPv4 ループ フリー代替高速再ルーティングの設定例，61 ページ
- その他の参考資料，62 ページ
- IPv4 ループ フリー代替高速再ルーティングの設定に関する機能情報，63 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。

IPv4 ループ フリー代替高速再ルーティングのための前提条件

- ループ フリー代替（LFA）高速再ルーティング（FRR）は、インターフェイスがポイントツーポイントインターフェイスである場合だけ、インターフェイスを介して到達可能なパスを保護できます。
- LAN インターフェイスが 1 つのネイバーに物理的に接続されている場合、LFA FRR で保護するために、LAN インターフェイスをポイントツーポイント インターフェイスとして設定する必要があります。

IPv4 ループ フリー代替高速再ルーティングの制約事項

- マルチプロトコル ラベル スイッチング（MPLS）トラフィック エンジニアリング（TE）トンネルは保護インターフェイスとして使用できません。ただし、MPLS TE トンネルは、TE トンネルがプライマリ パスとして使用される限り、保護（修復）インターフェイスとして使用できます。
- ロードバランス サポートは、FRR で保護されたプレフィックスで利用可能ですが、50 ミリ秒のカットオーバーの時間は保証されません。
- 最大 8 個の FRR 保護のインターフェイスで同時にカットオーバーを実行することができます。
- レイヤ 3 VPN だけがサポートされます。
- IPv4 マルチキャストはサポートされていません。
- IPv6 はサポートされていません。
- IS-IS は、プライマリ インターフェイスがトンネルであるプレフィックスの LFA を計算しません。
- LFA 計算は、同じレベルまたは領域に属するインターフェイスまたはリンクに制限されます。したがって、バックアップ LFA の計算時に同じ LAN 上のすべてのネイバーを除外すると、トポロジのサブセットで修復を使用できなくなる可能性があります。
- 物理インターフェイスおよび物理ポートチャネル インターフェイスのみ保護されます。サブインターフェイス、トンネル、および仮想インターフェイスは保護されません。

- TE ラベル スイッチド パス（LSP）は、バックアップ パスとして使用できます。ただし、プライマリ パスは、リング トポロジの FRR を完了するために使用できる物理インターフェイスである必要があります。
- ボーダー ゲートウェイ プロトコル（BGP）プレフィックス独立コンバージェンス（PIC）と IP FRR は、同じプレフィックスに使用されない限り、同じインターフェイス上に設定できます。

次の制限は、ASR 903 シリーズ アグリゲーション サービス ルータに適用されます。

- Cisco ASR 903 シリーズ アグリゲーション サービス ルータで LFA FRR をイネーブルにするには、**mpls ldp explicit-null** コマンドを有効にする必要があります。**implicit-null** キーワードはサポートされていません。
- ASR 903 は最大 4000 の LFA FRR ルートをサポートします。
- LFA FRR は、等コスト マルチパス（ECMP）ではサポートされません。
- リモート LFA トンネルは、ハイ アベイラビリティ対応ではないため、ステートフル スイッチオーバー（SSO）と共存できますが、SSO 準拠ではありません。
- 双方向フォワーディング（BFD）によってトリガされる高速再ルーティングはサポートされません。LFA FRR トポロジの一部になっているインターフェイスでは、BFD を設定しないでください。

IPv4 ループ フリー代替高速再ルーティングに関する情報

IS-IS および IP FRR

ローカル リンクがネットワークで失敗した場合、IS-IS は、影響を受けるすべてのプレフィックスの新しいプライマリ ネクストホップ ルートを再計算します。これらのプレフィックスは、RIB および転送情報ベース（FIB）で更新されます。プライマリ プレフィックスがフォワーディング プレーンで更新されるまで、影響を受けるプレフィックス宛てのトラフィックは廃棄されます。このプロセスには数百ミリ秒かかることがあります。

IP FRR で、IS-IS はプライマリ パスで障害が発生した場合に使用するために、フォワーディング プレーンに対する LFA ネクストホップ ルートを計算します。LFA はプレフィックスごとに計算されます。

特定のプライマリ パスに複数の LFA がある場合、IS-IS はプライマリ パスの単一 LFA を選ぶために、タイブレーク ルールを使用します。複数 LFA パスを持つプライマリ パスの場合、プレフィックスは LFA パス間で均等に分散されます。

修復パス

修復パスでは、ルーティングの遷移時にトラフィックが転送されます。リンクまたはルータに障害が発生すると、物理層の信号が失われるため、当初は隣接ルータしかこの障害を認識できません。ネットワーク内のその他すべてのルータは、この障害に関する情報がルーティング プロトコルによって伝播されるまで（これには数百ミリ秒かかる可能性があります）、この障害の性質と場所を認識しません。したがって、このネットワーク障害の影響を受けたパケットがそれぞれの宛先に到達するように準備する必要があります。

障害が発生したリンクに隣接するルータは、障害が発生したリンクを使用していた可能性のあるパケットに対して、一連の修復パスを使用します。これらの修復パスは、ルータが障害を検出してから、ルーティングの遷移が完了するまで使用されます。ルーティングの遷移が完了するまでに、ネットワーク内のすべてのルータは転送データを変更し、障害が発生したリンクはルーティングの計算から除外されます。

修復パスは、障害が検出されるとすぐにアクティブになるようにするために、障害を予測して事前計算されます。

IPv4 LFA FRR 機能では次の修復パスを使用します。

- 等コストマルチパス（ECMP）は、宛先の等コストパス分割セットのメンバーとしてリンクを使用します。セットの他のメンバーは、リンクに障害が発生したときに代替パスを提供できます。
- LFA は、ループバックしないで宛先にパケットを送るネクストホップ ルートです。ダウンストリーム パスは LFA のサブセットです。

LFA の概要

LFA はプライマリ ネイバー以外のノードです。トラフィックは、ネットワーク障害発生後に LFA にリダイレクトされます。LFA は、失敗について認識せずに転送を決定します。

LFA は、トラフィックの転送に障害のある要素を使用したり、保護ノードを使用することはできません。LFA はループを発生させてはなりません。LFA は、インターフェイスがプライマリ パスとして使用できる限り、デフォルトでサポートされるすべてのインターフェイスでイネーブルになります。

プレフィックスごとの LFA を使用する利点は次のとおりです。

- プライマリ パスでリンクがダウンした場合、修復パスが移行中にトラフィックを転送します。
- プレフィックスごとの LFA を持つすべての宛先が保護されます。これにより、サブセット（障害の遠端のノード）のみが保護されない状態で残ります。

LFA の計算

プレフィックスごとに LFA を計算する汎用アルゴリズムについては、RFC 5286 を参照してください。IS-IS は、メモリ使用量を減らすための少量の変更とともに RFC 5286 を実装します。保護のプレフィックスを検証する前にすべてのネイバーの最短パス優先（SPF）計算を実行する代わりに、IS-IS は SPF 計算がネイバーごとに実行された後でプレフィックスを検査します。IS-IS は SPF 計算の実行後にプレフィックスを検査するため、IS-IS は SPF 計算がネイバーごとに実行された後も最適な修復パスを保持します。IS-IS では、すべてのネイバーに対する SPF の結果を保存する必要はありません。

RIB とルーティング プロトコル間の連携

ルーティングプロトコルは、タイブレークアルゴリズムを実装して、プレフィックスの修復パスを計算します。計算の結果は、プライマリ パス付きの一連のプレフィックスになり、いくつかのプライマリ パスが修復パスに関連付けられます。

タイブレーク アルゴリズムは特定の条件を満たすか、または特定の属性を持つ LFA を考慮します。複数の LFA がある場合、**fast-reroute per-prefix** コマンドに **tie-break** キーワードを設定します。ルールによってすべての候補 LFA が除外される場合、そのルールはスキップされます。

プライマリ パスには、複数の LFA を設定できます。デフォルトのタイブレーク ルールを実装し、ユーザがこれらのルールを変更できるようにするには、ルーティング プロトコルが必要です。タイブレーク アルゴリズムの目的は、複数の候補 LFA を除外し、プレフィックス単位のプライマリ パスごとに 1 つの LFA を選択し、プライマリ パスが失敗したときに複数の候補 LFA でトラフィックを分散させることです。

タイブレーク ルールでは、すべての候補を除外することはできません。

タイブレークには、次の属性が使用されます。

- ダウンストリーム：保護された宛先へのメトリックが宛先へのノードを保護しているメトリックよりも低い候補を除外します。
- ラインカード分離：保護されたパスと同じラインカードを共有している候補を除外します。
- 共有リスク リンク グループ（SRLG）：保護されたパス SRLG のいずれかに属する候補を除外します。
- 負荷分散：保護されたパスを共有するプレフィックスで残りの候補を分散させます。
- 最低修復パス メトリック：保護されたプレフィックスへのメトリックが高い候補を除外します。
- ノードの保護：保護されたノードではない候補を除外します。
- プライマリ パス：ECMP ではない候補を除外します。
- セカンダリ パス：ECMP の候補を除外します。

IPv4 ループ フリー代替高速再ルーティングの設定方法

高速再ルーティングのサポートの設定

（注） LFA 計算はすべてのルートに対してイネーブルになり、FRR はサポートされるすべてのインターフェイスでイネーブルになります。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **ip router isis** *area-tag*
6. **isis tag** *tag-number*
7. **exit**
8. **interface** *type number*
9. **ip address** *ip-address mask*
10. **ip router isis** *area-tag*
11. **isis tag** *tag-number*
12. **exit**
13. **router isis** *area-tag*
14. **net** *net*
15. **fast-reroute per-prefix** {**level-1** | **level-2**} {**all** | **route-map** *route-map-name*}
16. **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** *type number* 例： `Device(config)# interface GigabitEthernet0/0/0`	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 address** *ip-address mask* 例： `Device(config-if)# ip address 10.1.1.1 255.255.255.0`	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。
ステップ 5	**ip router isis** *area-tag* 例： `Device(config-if)# ip router isis ipfrr`	インターフェイス上で IP の IS-IS ルーティング プロセスを設定して、エリア指示子をルーティング プロセスに添付します。
ステップ 6	**isis tag** *tag-number* 例： `Device(config-if)# isis tag 17`	IP プレフィックスが IS-IS リンクステート パケット（LSP）に追加されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
ステップ 7	**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 モードに戻ります。
ステップ 8	**interface** *type number* 例： `Device(config)# interface GigabitEthernet0/0/1`	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 9	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 192.168.255.2 255.255.255.0`	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。

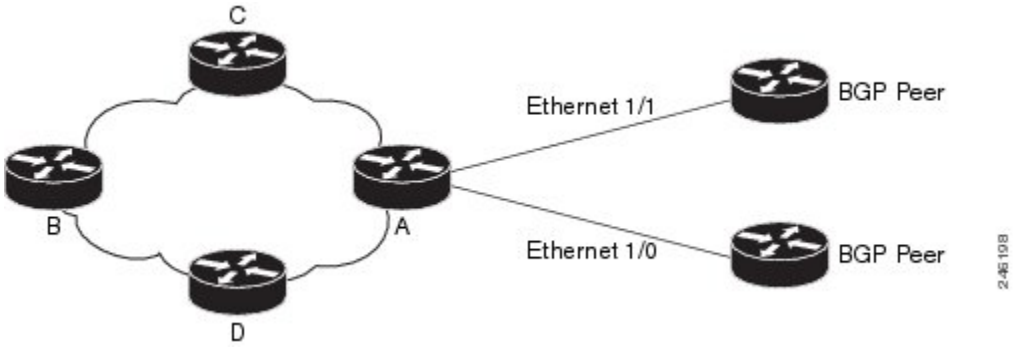
	コマンドまたはアクション	目的
ステップ 10	**ip router isis** *area-tag* 例： `Device(config-if)# ip router isis ipfrr`	インターフェイス上で IP の IS-IS ルーティング プロセスを設定して、エリア指示子をルーティング プロセスに添付します。
ステップ 11	**isis tag** *tag-number* 例： `Device(config-if)# isis tag 17`	IP プレフィックスが IS-IS LSP に追加されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
ステップ 12	**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 モードに戻ります。
ステップ 13	**router isis** *area-tag* 例： `Device(config)# router isis ipfrr`	IS-IS ルーティング プロトコルをイネーブルにし、IS-IS プロセスを指定して、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 14	**net** *net* 例： `Device(config-router)# net 49.0001.0101.2800.0001.00`	ルーティング プロセスの IS-IS Network Entity（NET）を設定します。
ステップ 15	**fast-reroute per-prefix** {**level-1** | **level-2**} {**all** | **route-map** *route-map-name*} 例： `Device(config-router)# fast-reroute per-prefix level-2 all`	プレフィックス単位の FRR をイネーブルにします。 • すべてのプレフィックスを保護するために、**all** キーワードを設定します。
ステップ 16	**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。

IPv4 ループ フリー代替高速再ルーティングの設定例

例：IPv4 ループ フリー代替高速再ルーティングの設定のサポート

次の図は、インターフェイス タグを使用して BGP ネクスト ホップを保護する IPv4 LFA FRR を示します。

図 *4*：サンプル *IPv4 LFA FRR* 設定



次に、上記の図に示すように、ルータ A の IPv4 LFA FRR を設定する例を示します。ルータ A は、タグ 17 とともにプレフィックス 10.0.0.0/24 と 192.168.255.0/24 をアドバタイズします。

```
Device# configure terminal
Device(config)# interface GigabitEthernet0/0/0
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# ip router isis ipfrr
Device(config-if)# isis tag 17
Device(config-if)# exit
Device(config)# interface GigabitEthernet0/0/1
Device(config-if)# ip address 192.168.255.2 255.255.255.0
Device(config-if)# ip router isis ipfrr
Device(config-if)# isis tag 17
Device(config-if)# exit
Device(config)# router isis ipfrr
Device(config-router)# net 49.0001.0001.0001.0001.00
Device(config-router)# fast-reroute per-prefix level-2
```

次に、上記の図に示すように、他のルータの IPv4 LFA FRR を設定する例を示します。他のルータは、ルータ A に設定された 2 つのプレフィックスの修復パスの計算にタグ 17 を使用できます。

```
Device(config)# router isis
Device(config-router)# net 47.0004.004d.0001.0001.c11.1111.00
Device(config-router)# fast-reroute per-prefix level-2 route-map ipfrr-include
Device(config-router)# exit
Device(config)# route-map ipfrr-include
Device(config-router)# match tag 17
```

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	『*Master Commands List, All Releases*』
MPLS コマンド	『*Multiprotocol Label Switching Command Reference*』
IP ルーティング：Protocol-Independent コマンド	『*IP Routing: Protocol-Independent Command Reference*』
IS-IS コマンド	『*IP Routing: ISIS Command Reference*』

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

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 ループ フリー代替高速再ルーティングの設定に関する機能情報

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*：*IPv4* ループ フリー代替高速再ルーティングの設定に関する機能情報

機能名	リリース	機能情報
IPv4 ループ フリー代替高速再ルーティング		リンクやルータに障害が発生すると、配布されたルーティング アルゴリズムによって、変更を考慮した新しいルートが計算されます。計算のための時間をルーティングの遷移と呼びます。遷移が完了し、すべてのルータがネットワーク上の共通のビューで収束されるまで、送信元と宛先のペア間の接続は中断されます。事前計算済みの代替ネクスト ホップを使用してルーティングの遷移時間を 50 ミリ秒より少なくするために、IPv4 ループ フリー代替高速再ルーティング機能を使用できます。リンク障害の通知を受けると、ルータはトラフィック損失を減らすために、修復パスにすぐに切替えます。 IPv4 ループ フリー代替高速再ルーティングは、修復パスの事前計算に重点を置いています。修復パスの計算は、IS-IS ルーティング プロトコルによって実行され、結果（修復パス）はRIBに送信されます。修復パスのインストールは、シスコ エクスプレス フォワーディングによって実行されます。 Cisco IOS XE Release 3.6S では、この機能は ASR 903 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。**debug isis fast-reroute**、**fast-reroute load-sharing disable**、**fast-reroute per-prefix**、**fast-reroute tie-break**、**show isis fast-reroute**

第 5 章

IP イベント減衰

IPイベント減衰機能は、設定可能な指数関数的減少メカニズムを導入し、過剰なインターフェイス フラッピング イベントによるネットワーク内のルーティング プロトコルおよびルーティング テーブルに対する影響を抑制します。ネットワーク オペレータはこの機能を使用し、フラップが発生しているローカル インターフェイスをルータが自動的に特定して、選択的に減衰するように設定できます。

- 機能情報の確認，65 ページ
- IP イベント減衰の制約事項，66 ページ
- IP イベント減衰に関する情報，66 ページ
- IP イベント減衰の設定方法，71 ページ
- IP イベント減衰の設定例，73 ページ
- その他の参考資料，74 ページ
- IP イベント減衰の機能情報，75 ページ
- 用語集，76 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。

IP イベント減衰の制約事項

サブインターフェイスの制約事項

この機能により設定できるのは、プライマリ インターフェイスのみです。プライマリ インターフェイスの設定は、すべてのサブインターフェイスに対しデフォルトで適用されます。IP イベント減衰は、インターフェイス上の個々のサブインターフェイスのフラップはトラッキングしません。

仮想テンプレートはサポート外

仮想テンプレートから仮想アクセス インターフェイスへの減衰のコピーはサポートされません。これは、仮想テンプレートを使用する既存のアプリケーションでは、減衰の有用性が限定的であるためです。インターフェイスでフラップが発生すると仮想アクセス インターフェイスはリリースされ、インターフェイスがアップしてネットワークに対して使用可能になると、新しい接続と仮想アクセス インターフェイスが取得されます。減衰状態はインターフェイスに対して設定されるため、インターフェイスのフラップより長く続くことはありません。

IPX ルーティング プロトコルはサポート外

Internetwork Packet Exchange（IPX）プロトコルは、IP イベント減衰機能ではサポートされません。ただし、この機能がイネーブルになっている場合、このプロトコルの IPX バリアントは、アップおよびダウン状態イベント情報をそのまま受信します。これにより、問題やルーティングの問題が生じることはありません。

IP イベント減衰に関する情報

IP イベント減衰の概要

インターフェイス状態変化は、インターフェイスが管理上アップまたはダウンした場合や、インターフェイスで状態が変化した場合に発生します。インターフェイスで状態が変化したりフラップが発生すると、状態の変化に影響されるルートの状態がルーティング プロトコルに通知されます。インターフェイスの状態が変化するたびに、ネットワーク内のすべての影響を受けるデバイスで、最良パスを再計算し、ルーティング テーブルでルートをインストールまたは削除し、有効なルートをピア ルータにアドバタイズする必要があります。過剰なフラップが発生する不安定なインターフェイスは、ネットワークの他のデバイスに大量のシステム処理リソースを消費させ、ルーティング プロトコルでフラップが発生しているインターフェイスとの同期が失われる原因になる可能性があります。

IP イベント減衰機能は、設定可能な指数関数的減少メカニズムを導入し、過剰なインターフェイス フラッピング イベントによるネットワーク内のルーティング プロトコルおよびルーティング テーブルに対する影響を抑制します。ネットワーク オペレータはこの機能を使用し、フラップが発生しているローカル インターフェイスをルータが自動的に特定して、選択的に減衰するように

設定できます。インターフェイスの減衰により、インターフェイスでフラップが発生せず安定するまで、ネットワークからインターフェイスが除外されます。IPイベント減衰機能を設定すると、悪影響が広がらないように障害を分離することで、コンバージェンス時間とネットワーク全体の安定性を向上します。これにより、ネットワークの他のデバイスのシステム処理リソースの使用率が減少し、ネットワーク全体の安定性が向上します。

インターフェイス状態変化イベント

この項では、IP イベント減衰機能のインターフェイス状態変化イベントについて説明します。この機能は、過剰なインターフェイスのフラップや状態変化の影響を抑制するために使用される、設定可能な指数関数的減少メカニズムを採用しています。IPイベント減衰機能がイネーブルになっている場合、過剰なルート更新情報をフィルタリングすることによって、フラップが発生しているインターフェイスは、ルーティング プロトコルの観点から減衰されます。フラップが発生しているインターフェイスが特定され、ペナルティを割り当てられ、必要に応じて抑制され、インターフェイスが安定すればネットワークで利用可能になります。

抑制しきい値

抑制しきい値は、フラップが発生しているインターフェイスをルータが減衰するトリガーとなる、累積ペナルティの値です。フラップが発生しているインターフェイスはルータによって特定され、アップおよびダウン状態変化ごとにペナルティを割り当てられますが、インターフェイスは自動的には減衰されません。ルータは、フラップが発生しているインターフェイスの累積ペナルティをトラッキングします。累積ペナルティがデフォルトまたは設定済みの抑制しきい値に到達すると、インターフェイスが減衰状態になります。

半減期

半減期は、累積ペナルティの指数関数的な減少の速さを指定します。インターフェイスが減衰状態になると、ルータは、インターフェイスの以後のアップおよびダウン状態変化をモニタします。インターフェイスでペナルティの累積が続き、抑制しきい値の範囲内に留まっている間は、インターフェイスは減衰されたままです。インターフェイスが安定しフラップが発生しなくなると、半減期が終了するごとに、ペナルティが半分に減らされます。ペナルティが再使用しきい値に低下するまで、累積ペナルティが減らされていきます。半減期タイマーの設定可能な範囲は 1 ～ 30 秒です。デフォルトの半減期タイマーは 5 秒です。

再使用しきい値

累積ペナルティが減らされて再使用しきい値まで低下すると、ルートの抑制がなくなり、ネットワーク上の他のデバイスに対して使用可能になります。再使用値の範囲は 1 ～ 20,000 ペナルティです。デフォルト値は 1000 ペナルティです。

最大抑制時間

最大抑制時間は、インターフェイスにペナルティが割り当てられている場合に、インターフェイスの抑制状態を維持できる時間の上限を表します。最大抑制時間は 1 ～ 20,000 秒で設定できます。最大ペナルティ タイマーのデフォルトは 20 秒またはデフォルトの半減期の 4 倍（5 秒）です。累積ペナルティの最大値は、最大抑制時間、再使用しきい値、および半減期に基づいて算出されます。

関連コンポーネント

インターフェイスで減衰が設定されていない場合や、減衰が設定されていても抑制されていない場合、インターフェイス状態が移行してもIPイベント減衰機能によってルーティングプロトコルの動作が変更されることはありません。ただし、インターフェイスが抑制されている場合、インターフェイスの抑制がなくなるまで、ルーティングプロトコルとルーティングテーブルは、インターフェイスの状態移行の以降の影響を受けません。

ルート タイプ

次のインターフェイスは、この機能の設定の影響を受けます。

- 接続ルート：
  - 減衰されたインターフェイスの接続ルートは、ルーティングテーブルにインストールされません。
  - 減衰されたインターフェイスの抑制がなくなり、インターフェイスがアップしていれば、接続ルートはルーティング テーブルにインストールされます。
- スタティック ルート：
  - 減衰されたインターフェイスに割り当てられているスタティック ルートは、ルーティング テーブルにインストールされません。
  - 減衰されたインターフェイスの抑制がなくなり、インターフェイスがアップしていれば、スタティック ルートはルーティング テーブルにインストールされます。

（注） この機能を設定できるのはプライマリ インターフェイスのみです。また、すべてのサブインターフェイスには、プライマリ インターフェイスと同じ減衰設定が適用されます。IP イベント減衰は、インターフェイス上の個々のサブインターフェイスのフラップはトラッキングしません。

サポートされているプロトコル

IP イベント減衰機能は、Routing Information Protocol（RIP）、Open Shortest Path First（OSPF）、Enhanced Interior Gateway Routing Protocol（EIGRP）、Intermediate System-to-Intermediate System（IS-IS）、Border Gateway Protocol（BGP）、Connectionless Network Services（CLNS）、Hot Standby Routing Protocol（HSRP）をサポートします。次の一覧は、これらのプロトコルでのこの機能の動作に関する一般的な情報を示しています。

- RIP、OSPF、EIGRP、IS-IS、および BGP：
  - インターフェイスが減衰されると、ルーティングプロトコルによってインターフェイスがダウンしたと見なされます。ルーティングプロトコルは、減衰されたインターフェイスを介したこのピアルータとの隣接関係を保持しないか、このインターフェイスに関連するルータから他のピア ルートへのアドバタイズメントを生成しません。
  - インターフェイスの抑制がなくなり、ネットワークに対して使用可能になると、ルーティングプロトコルによって、インターフェイスがアップであると見なされます。ルーティングプロトコルは、インターフェイスがアップ状態であるという通知を受け、ルーティング条件は通常に戻ります。
- HSRP：
  - インターフェイスが減衰されると、HSRP によってダウンしたと見なされます。HSRP は減衰されたインターフェイスからの HSRP メッセージを生成しなくなります。または、減衰されたインターフェイスで受信されたメッセージに応答しなくなります。インターフェイスの抑制がなくなり、ネットワークに対して使用可能になると、HSRP はアップ状態の通知を受け、通常の動作に戻ります。
- CLNS：
  - インターフェイスが減衰されると、インターフェイスが IP ルーティングと CLNS ルーティングの両方で等しく減衰します。IS-IS、IP、CLNS ルーティングなどの統合ルーティングプロトコルは近接的に相互接続されており、個別に減衰を適用することができないため、インターフェイスは IP と CLNS の両方に対して減衰されます。

（注） IPイベント減衰機能がイネーブルになっていない場合や、インターフェイスが減衰されていない場合は、ルーティング プロトコルへの影響はありません。

ネットワーク展開

実際のネットワーク展開では、一部のルータでインターフェイス減衰が設定されない場合や、ルータによってはこの機能がサポートされていない場合もあります。ポイントツーポイント インターフェイスの他端のルータや同じマルチキャスト LAN のルータで、インターフェイス減衰がオンに

なっていない場合や、この機能が実装されていない場合であっても、ルーティングに関する大きな問題はないと思われます。インターフェイスが減衰されているルータ上では、このインターフェイスに関連付けられているルートは使用されません。このインターフェイスからはパケットが送信されず、インターフェイスの反対側のルータではルーティング プロトコルのアクティビティが開始されません。ただし、それらのルータは自身のインターフェイスがアップであると認識し、減衰されたインターフェイスへのパケット転送を開始できるため、反対側のルータが、このサブネットに関連付けられているルーティング テーブル内に一部のルートをインストールする可能性があります。この状況では、減衰されたインターフェイスを持つルータは、ルーティング テーブル内のルートに応じて、これらのパケットの転送を開始します。

IPイベント減衰機能は、ネットワーク内に新しい情報を追加しません。実際、減衰の効果は、ルーティング情報のサブセットをネットワークから除外することです。したがって、減衰の結果としてループは発生しません。

IP イベント減衰の利点

処理負荷の低減

IPイベント減衰機能は、設定可能な指数関数的減少メカニズムを採用しており、ルーティング プロトコルでの過剰なインターフェイスフラッピングイベントの影響を抑制します。短時間に受信される過剰なインターフェイスのアップおよびダウン状態変化は処理されず、システム リソースを消費しません。ネットワーク内の他のルータは、フラップが発生しているルートのためにシステム リソースを消費する必要がありません。

コンバージェンスの短縮

IP イベント減衰機能は、悪影響が広がらないように障害を分離することで、コンバージェンス時間とネットワーク全体の安定性を向上します。問題のルータがサービスを終了したり起動したりするたびにルーティングテーブルが再構築されないので、リンク フラップが発生していないルータは早くコンバージェンスに到達します。

ネットワークの安定性の向上

IP イベント減衰機能によって、ネットワークの安定性が向上します。フラップが発生しているインターフェイスを持つルータは、インターフェイスが安定するまで、フラップが発生しているインターフェイスをネットワークから除外します。このため、他のルータは、インターフェイスが安定するまで、影響を受けるルータ周辺のトラフィックを単純にリダイレクトし、これによってルータでパケットが破棄されないようにできます。

IP イベント減衰の設定方法

IP イベント減衰のイネーブル化

IPイベント減衰機能をイネーブルにするには、インターフェイスコンフィギュレーションモードで **dampening** コマンドを入力します。すでに減衰が設定されているインターフェイスに対してこのコマンドを適用すると、減衰状態はすべてリセットされ、累積ペナルティが0に設定されます。インターフェイスが減衰されている場合、累積ペナルティは再使用しきい値まで低下し、減衰しているインターフェイスはネットワークに対して使用可能になります。ただし、フラップ カウントは保持されます。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **interface***typenumber*
4. **dampening** [*half-life-period reuse-threshold*] [*suppress-threshold max-suppress* [*restart-penalty*]]
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： `Router> 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： `Router# 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： `Router(config)#` **interface** *type number*	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、特定のインターフェイスを設定します。
ステップ 4	**dampening** [*half-life-period reuse-threshold*] [*suppress-threshold max-suppress* [*restart-penalty*]]	インターフェイス減衰をイネーブル化します。

	コマンドまたはアクション	目的
	例： `Router(config-if)# dampening`	• 引数なしで **dampening** コマンドを入力すると、デフォルトの設定パラメータでインターフェイス減衰がイネーブルになります。 • 手動で *restart-penalty* 引数のタイマーを設定する場合、すべての引数に対して手動で値を入力する必要があります。
ステップ 5	**end** 例： `Router(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 モードを開始します。

IP イベント減衰の確認

IPイベント減衰機能の設定を確認するには、**show dampening interface** コマンドまたは **show interface dampening** コマンドを使います。

clear counters コマンドは、フラップ カウントをクリアして 0 にリセットするために使用できます。このコマンドは、減衰状態や累積ペナルティなど、その他のすべてのパラメータおよび状態には影響しません。

手順の概要

1. イネーブル化
2. **showdampeninginterface**
3. **showinterfacedampening**

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： `Router> 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	**showdampeninginterface** 例： `Router# show dampening interface`	減衰されたインターフェイスを表示します。
ステップ 3	**showinterfacedampening** 例： `Router# show interface dampening`	減衰されたローカルルータ上のインターフェイスを表示します。

IP イベント減衰の設定例

IP イベント減衰の設定例

次に、ギガビット イーサネット インターフェイス 0/0/0 でインターフェイス減衰を設定し、半減期を 30 秒、再使用しきい値を 1500、抑制しきい値を 10000、最大抑制時間を 120 秒に設定する例を示します。

```
interface GigabitEthernet 0/0/0
 dampening 30 1500 10000 120
```

次に、ATM インターフェイス 2/0/0 でインターフェイス減衰を設定し、デフォルトのインターフェイス減衰値を使用する例を示します。

```
interface atm 2/0/0
 dampening
```

次に、ルータがリロードされた後、最初にインターフェイスがアップしたときに、ギガビット イーサネット インターフェイス 0/0/0 で 500 のペナルティを適用するようにルータを設定する例を示します。

```
interface GigabitEthernet 0/0/0
 dampening 5 500 1000 20 500
```

IP イベント減衰の確認の例

show dampening interface コマンドの出力では、インターフェイス減衰の概要が表示されます。

```
Router# show dampening interface
3 interfaces are configured with dampening.
No interface is being suppressed.
Features that are using interface dampening:
  IP Routing
```

show interface dampening コマンドの出力では、減衰パラメータおよびローカル ルータ上のインターフェイスの状態の概要が表示されます。次に、**show interface dampening** コマンドの出力例を示します。

```
Router# show interface dampening
GigabitEthernet0/0/0
  Flaps Penalty    Supp ReuseTm   HalfL  ReuseV   SuppV  MaxSTm    MaxP Restart
      0       0   FALSE       0       5    1000    2000      20   16000       0
ATM2/0/0
  Flaps Penalty    Supp ReuseTm   HalfL  ReuseV   SuppV  MaxSTm    MaxP Restart
      0       0   FALSE       0       5    1000    2000      20   16000       0
POS2/0/0
  Flaps Penalty    Supp ReuseTm   HalfL  ReuseV   SuppV  MaxSTm    MaxP Restart
      0       0   FALSE       0       5    1000    2000      20   16000       0
```

その他の参考資料

ここでは、IP イベント減衰機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
IP ルーティングのプロトコル独立型コマンド	『*Cisco IOS IP Routing: Protocol-Independent Command Reference*』
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』

標準

規格	Title
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

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

RFC

RFC	Title
この機能がサポートする新しい RFC または変更された RFC はありません。また、この機能は既存の規格に対するサポートに影響を及ぼしません。	--

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/en/US/support/index.html

IP イベント減衰の機能情報

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*：*IP* イベント減衰の機能情報

機能名	リリース	機能情報
IP イベント減衰	Cisco IOS XE Release 2.1	IP イベント減衰機能は、設定可能な指数関数的減少メカニズムを導入し、過剰なインターフェイス フラッピング イベントによるネットワーク内のルーティングプロトコルおよびルーティング テーブルに対する影響を抑制します。ネットワーク オペレータはこの機能を使用し、フラップが発生しているローカル インターフェイスをルータが自動的に特定して、選択的に減衰するように設定できます。 この機能は、Cisco ASR 1000 シリーズのアグリゲーションサービスルータで導入されました。 次のコマンドがこの機能によって導入されました。**dampening**、**debugdampening**、**showdampeninginterface**、**showinterfacedampening**

用語集

イベント減衰：インターフェイス状態の変化による過剰なルート調整メッセージをフィルタリングすることによって、IP のルーティングテーブルおよびルーティングプロトコルの観点から、フラップが発生しているインターフェイスをルータが減衰する処理。

フラップ：短時間でのアップからダウン、およびダウンからアップへの急速なインターフェイス状態の変化。

半減期：累積ペナルティの指数関数的減少の割合を決める値。

最大ペナルティ：この値を超えて割り当てられたペナルティが増加しない最大値。最大抑制時間に基づきます。

最大抑制時間：ペナルティが割り当てられている場合に、インターフェイスの抑制状態を維持できる時間の上限。

ペナルティ：インターフェイスでフラップが発生した場合にインターフェイスに割り当てられる値。この値はフラップごとに増加し、時間と共に減少します。減少の割合は、半減期によって異なります。

再使用しきい値：この値を過ぎると、インターフェイスの抑制がなくなり、再び使用できるようになるしきい値。

抑制しきい値：フラップが発生しているインターフェイスの減衰をルータでトリガーする、累積ペナルティの値。累積ペナルティがこの値を超えると、ルーティング プロトコルの観点から、インターフェイス状態はダウンと見なされます。

抑制状態：インターフェイスを抑制すると、ルーティング プロトコルの観点からインターフェイスがネットワークから除外される。インターフェイスは、割り当てられているペナルティを超える頻度でフラップが発生すると、抑制状態になります。

第 6 章

PBR 再帰ネクスト ホップ

PBR 再帰ネクスト ホップ機能はルート マップを強化し、ポリシーベース ルーティング（PBR）で使用する再帰ネクスト ホップ IP アドレスの設定をイネーブルにします。再帰ネクストホップ IP アドレスはルーティング テーブルにインストールされ、直接接続されていないサブネットにすることができます。再帰ネクストホップ IP アドレスを使用できない場合、パケットはデフォルト ルートを使ってルーティングされます。

Cisco Express Forwarding（CEF）やプロセス スイッチングはインフラストラクチャを提供するため、この機能の利点は CEF ロードシェアリングです。

- 機能情報の確認，79 ページ
- PBR 再帰ネクスト ホップの制約事項，80 ページ
- PBR 再帰ネクスト ホップに関する情報，80 ページ
- PBR 再帰ネクスト ホップの設定方法，80 ページ
- PBR 再帰ネクスト ホップの設定例，85 ページ
- PBR 再帰ネクスト ホップに関するその他の参考資料，86 ページ
- PBR 再帰ネクスト ホップの機能情報，87 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。

PBR 再帰ネクスト ホップの制約事項

サブネットへの複数の等コスト ルートが **set next-hop recursive** コマンドによって設定されている場合は、ロード バランシングはルートへのすべての隣接関係が解決された場合にだけ行われます。いずれかの隣接関係が解決されていなければ、ロード バランシングは行われず、隣接関係が解決されたルートのうち 1 つだけが使用されます。隣接のいずれも解決しない場合、パケットが処理されて隣接の少なくとも 1 つが解決されることで、ハードウェアの隣接のプログラミングにつながります。ポリシー ベース ルーティングは、ルーティング プロトコルまたはその他の方法に依存してすべての隣接を解決し、その結果、ロード バランシングが発生します。

IPv6 用の PBR 再帰ネクスト ホップではロード シェアリングはサポートされません。

PBR 再帰ネクスト ホップに関する情報

PBR 再帰ネクスト ホップの概要

PBR 再帰ネクスト ホップ機能はルート マップを強化し、ポリシーベース ルーティング（PBR）で使用する再帰ネクスト ホップ IP アドレスの設定をイネーブルにします。再帰ネクストホップ IP アドレスはルーティング テーブルにインストールされ、直接接続されていないサブネットにすることができます。再帰ネクストホップ IP アドレスを使用できない場合、パケットはデフォルト ルートを使ってルーティングされます。

IPv6 用の PBR 再帰ネクスト ホップは、直接接続されていないネクストホップもサポートしています。指定された再帰ネクスト ホップはホスト アドレスまたはサブネット アドレスのいずれかです。ルーティング テーブルが検索され、アドレスの最長一致に基づいてネクストホップが取得されます。このような再帰ネクスト ホップは、ルートマップのエントリあたり 1 件しかサポートされません。

PBR 再帰ネクスト ホップの設定方法

再帰ネクストホップ IP アドレスの設定

CEF またはプロセス スイッチングにより提供されるインフラストラクチャは、ネクストホップ IP アドレスへの再帰を実行します。設定の順序は次のとおりです。この順序はルーティングに影響します。

1. Next-hop
2. ネクストホップ再帰
3. インターフェイス

4 デフォルト ネクストホップ

5 デフォルト インターフェイス

ネクストホップ アドレスおよび再帰ネクストホップ IP アドレスの両方が同じルートマップ エントリに存在する場合は、ネクストホップが使用されます。ネクスト ホップが使用できない場合、再帰ネクスト ホップが使用されます。再帰ネクスト ホップを使用できず、他に IP アドレスが存在しない場合、パケットはデフォルトルーティングテーブルを使ってルーティングされ、ドロップされません。パケットがドロップされると考えられる場合は、**recursive** キーワードを指定した **setipnext-hop** コマンドの後に **setinterfacenull0** 設定を使用します。

再帰ネクストホップ ルータの IP アドレスを設定するには、次の作業を実行します。

はじめる前に

ロードシェアリングが必要な場合は、パケット単位または宛先単位のロードシェアリング用にCEF ロードシェアリングを設定する必要があります。ロードバランシングは、**setipnext-hoprecursive** コマンドで設定したサブネットへの等コスト ルートすべてに対して行う必要があります。

この機能は、中央集中システムおよび分散システムで使用できます。

（注） サポートされる再帰ネクストホップ IP アドレスは、ルートマップ エントリごとに 1 つのみです。

>

手順の概要

1. イネーブル化
2. **configureterminal**
3. **access-list***access-list-number*{**deny**|**permit**} *source*[*source-wildcard*] [**log**]
4. **route-map***map-tag*
5. 次のいずれかを実行します。
   - **setipnext-hop***ip-address*
   - **setipv6next-hop***ip-address*
6. 次のいずれかを実行します。
   - **setipnext-hop**{*ip-address* [...*ip-address*] | **recursive***ip-address*}
   - **setipv6next-hop**{*ipv6-address* [...*ipv6-address*] | **recursive***ipv6-address*}
7. 次のいずれかを実行します。
   - **matchipaddress***access-list-number*
   - **matchipv6address** {**prefix-list***prefix-list-name*|*access-list-name*}
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： `Router> 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： `Router# 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： `Router(config)# access-list 101 permit 10.60.0.0 0.0.255.255`	アクセス リストを設定します。設定例では、10.60.0.0.0.0.255.255 サブネット内に分類されるすべての発信元 IP アドレスが許可されます。

	コマンドまたはアクション	目的
ステップ 4	**route-map***map-tag* 例： `Router(config)# route-map abccomp`	ポリシー ルーティングをイネーブルにし、ルート マップ コンフィギュレーション モードを開始します。

ステップ 5	次のいずれかを実行します。
	• **setipnext-hop***ip-address*
	• **setipv6next-hop***ip-address*
	
	例：
	
	`Router(config-route-map)# set ip next-hop 10.10.1.1`
	
	例：
	`Router(config-route-map)# set ipv6 next-hop 2001:DB8:2003:1::95`
		ネクストホップ ルータ IPv4 または IPv6 アドレスを設定します。
		（注） この IPv4 または IPv6 アドレスは、ネクストホップ再帰ルータ設定とは別に設定します。

ステップ 6	次のいずれかを実行します。
	• **setipnext-hop**{*ip-address* [*...ip-address*] | **recursive***ip-address*}
	• **setipv6next-hop**{*ipv6-address* [*...ipv6-address*] | **recursive***ipv6-address*}
	
	例：
	
	`Router(config-route-map)# set ip next-hop recursive 10.20.3.3`
	
	例：
	`Router(config-route-map)# set ipv6 next-hop recursive 2001:DB8:2003:2::95`
		再帰ネクストホップ IPv4/IPv6 アドレスを設定します。
		（注） 中継 IP アドレスが宛先への短いルートである場合、この設定によって、パケットが再帰 IP アドレスを使ってルーティングされるとは限りません。

ステップ 7	次のいずれかを実行します。 • **matchipaddress***access-list-number* • **matchipv6address** {**prefix-list***prefix-list-name*|*access-list-name*}	一致するアクセス リストを設定します。

	コマンドまたはアクション	目的

	例：
	`Router(config-route-map)# match ip address 101`
	
	例：
	`Router(config-route-map)# match ipv6 address kmd`	

ステップ 8	**end** 例： `Router(config-route-map)# end`	現在のルートマップ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。

再帰ネクストホップ設定の確認

再帰ネクストホップ設定を確認するには、次の手順を実行します。

手順の概要

1. **showrunning-config | beginabccomp**
2. **showroute-map***map-name*

手順の詳細

ステップ 1 **showrunning-config | beginabccomp**

次の例に示すように、ネクストホップの IPv4/IPv6 アドレスと再帰ネクストホップの IPv4/IPv6 アドレスを確認するには、次のコマンドを使用します。

例：

```
Router# show running-config | begin abccomp
route-map abccomp permit 10
 match ip address 101 ! Defines the match criteria for an access list.
 set ip next-hop recursive 10.3.3.3 ! If the match criteria are met, the recursive IP  address is
 set.
 set ip next-hop 10.1.1.1 10.2.2.2 10.4.4.4

Router# show running-config | begin abccomp
route-map abccomp permit 10
 match ip address kmd! Defines the match criteria for an access list.
 set ipv6 next-hop recursive 2001:DB8:3000:1 ! If the match criteria are met, the recursive IPv6
```

```
 address is set.
 set ipv6 next-hop 2001:DB8:3000:1 2001:DB8:4000:1 2001:DB8:5000:1
```

ステップ 2 **showroute-map***map-name*

このコマンドを次の例のように使用し、ルート マップを表示します。

例：

```
Router# show route-map abccomp
route-map abccomp, permit, sequence 10
 Match clauses:
  ip address (access-lists): 101
 Set clauses:
  ip next-hop recursive 10.3.3.3
  ip next-hop 10.1.1.1 10.2.2.2 10.4.4.4
 Policy routing matches: 0 packets, 0 bytes

Router# show route-map abccomp
route-map abccomp, permit, sequence 10
 Match clauses:
  ipv6 address (access-lists): kmd
 Set clauses:
  ipv6 next-hop recursive 2001:DB8:3000:1
  ipv6 next-hop 2001:DB8:3000:1 2001:DB8:4000:1 2001:DB8:5000:1
 Policy routing matches: 0 packets, 0 bytes
```

PBR 再帰ネクスト ホップの設定例

例：再帰ネクストホップ IP アドレス

次に、IP アドレス 10.3.3.3 を再帰ネクストホップ ルータとして設定する例を示します。

```
route-map abccomp
 set ip next-hop 10.1.1.1
 set ip next-hop 10.2.2.2
 set ip next-hop recursive 10.3.3.3
 set ip next-hop 10.4.4.4
```

次に、IPv6アドレス2001:DB8:2003:1::95を再帰ネクストホップルータとして設定する例を示します。

```
route-map abccomp
 set ipv6 next-hop 2001:DB8:2003:1::95
 set ipv6 next-hop 2001:DB8:2004:3::96
 set ipv6 next-hop recursive 2001:DB8:2005:2::95
 set ipv6 next-hop 2001:DB8:2006:1::95
```

PBR 再帰ネクスト ホップに関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
『Cisco IOS Master Command List, All Releases』	『Cisco IOS Master Command List, All Releases』
IP ルーティングのプロトコル独立型コマンド：コマンド構文の詳細、コマンドモード、デフォルト設定、使用上の注意事項、および例	『Cisco IOS IP Routing: Protocol-Independent Command Reference』
基本的なシステム管理の実行	『*Basic System Management Configuration Guide*』
最大パス数の変更	『*BGP Configuration Guide*』の「BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN」モジュール
BGP ルート マップ設定作業および設定例。	『*BGP Configuration Guide*』の「Connecting to a Service Provider Using External BGP」モジュール
BGP コミュニティとルート マップ。	『*BGP Configuration Guide*』の「BGP Cost Community」モジュール
IPv6 ポリシーベース ルーティング	『*IP ルーティング：プロトコル非依存コンフィギュレーション ガイド*』の「IPv6 ポリシーベース ルーティング」モジュール

RFC

RFC	Title
RFC 791	*Internet Protocol*（インターネット プロトコル）
RFC 1219	可変長サブネット マスク

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/en/US/support/index.html

PBR 再帰ネクスト ホップの機能情報

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*：*PBR* 再帰ネクスト ホップの機能情報

機能名	リリース	機能情報
PBR 再帰ネクスト ホップ	Cisco IOS XE Release 2.2	PBR 再帰ネクスト ホップ機能はルート マップを強化し、ポリシーベース ルーティング（PBR）で使用する再帰ネクスト ホップ IP アドレスの設定をイネーブルにします。 次のコマンドが、この機能によって変更されました。 **setipnext-hop**、**showroute-map**

機能名	リリース	機能情報
IPv6 の PBR 再帰ネクスト ホップ	Cisco IOS XE リリース 3.12S	PBR 再帰ネクスト ホップ IPv6 機能はルートマップを強化し、ポリシーベース ルーティング（PBR）で使用する再帰ネクスト ホップ IPv6 アドレスの設定を有効にします。 導入または変更された新しいコマンドはありません。

第 7 章

複数のトラッキング オプションに対する PBR サポート

複数のトラッキング オプションに対する PBR サポート機能は、Cisco Discovery Protocol（CDP）を使ったオブジェクト トラッキングの機能を拡張し、追加の方法を使って、ポリシーベース ルーティング（PBR）処理でオブジェクトが使用可能かどうかを確認できます。確認方法として使用できるのは、Internet Control Message Protocol（ICMP）ping、ユーザ データグラム プロトコル（UDP）ping、または HTTP GET です。

- 機能情報の確認，89 ページ
- 複数のトラッキング オプションに対する PBR サポートの概要，90 ページ
- 複数のトラッキング オプションに対する PBR サポートの設定方法，90 ページ
- 複数のトラッキング オプションに対する PBR サポートの設定例，99 ページ
- その他の参考資料，100 ページ
- コマンド リファレンス，101 ページ
- 複数のトラッキング オプションに対する PBR サポートの機能情報，101 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。

複数のトラッキングオプションに対するPBRサポートの概要

オブジェクト トラッキング

オブジェクト トラッキングは、次のようなオブジェクトをモニタする独立したプロセスです。

- インターフェイスの回線プロトコルの状態
- ルーティング テーブル内のエントリの存在
- ping など、Service Assurance Agent（SAA）動作の結果

ホットスタンバイ ルータ プロトコル（HSRP）、Virtual Router Redundancy Protocol（VRRP）、Gateway Load Balancing Protocol（GLBP）、（この機能を使用した）PBR などのクライアントは、特定のトラッキング対象オブジェクトを登録して、オブジェクトの状態が変化したときに処理を実行できます。

複数のトラッキング オプションに対する PBR サポートの機能設計

複数のトラッキング オプションに対する PBR サポート機能は、トラッキング プロセスを通じて使用できるすべてのオブジェクトへのPBRアクセスを提供します。トラッキングプロセスを使って、ICMP ping 到達可能性、ルーティング隣接関係、リモート デバイス上で実行中のアプリケーション、ルーティング情報ベース（RIB）内のルートなどの個々のオブジェクトや、インターフェイス回線プロトコルの状態をトラッキングできます。

オブジェクト トラッキングは次のように機能します。PBR は、特定のオブジェクトのトラッキングが必要なことをトラッキングプロセスに通知します。一方、トラッキングプロセスはそのオブジェクトの状態が変化した場合に PBR に通知します。

複数のトラッキングオプションに対するPBRサポートの設定方法

Cisco IOS Release 12.3(14)T で IP サービス レベル契約（SLA）に新しい構文が導入されたため、この項の作業は実行している Cisco IOS Release によって異なります。この機能を使用するには、Cisco IOS Release 12.3(4)T、12.2(25)S 以降のリリースを実行している必要があります。ここでは、次のタスクについて説明します。

Cisco IOS Release 12.3(11)T、12.2(25)S、およびそれ以前

複数のトラッキング オプションに対するPBRサポートを設定するには、次の作業を実行します。この作業では、ルート マップを作成および設定し、トラッキング対象オブジェクトの到達可能性を確認します。

はじめる前に

この作業では、Cisco IOS Release 12.3(11)T、12.2(25)S 以前のリリースを実行中のネットワーキング デバイスが必要です。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **rtr***operation-number*
4. **typeechoprotocol***protocol-typetarget* [**source-ipaddr***ip-address*]
5. **exit**
6. **rtrschedule***operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*monthday* | *daymonth*] | **pending** | **now** | **after***hh*:*mm*:*ss*}] [**ageout***seconds*]
7. **track***object-number***rtr***entry-number*[**reachability**]
8. **delay**{**up***seconds* [**down***seconds*] | [**up***seconds*]**down***seconds*}
9. **exit**
10. **interface***typenumber*
11. **ipaddress***ip-addressmask*[**secondary**]
12. **ippolicyroute-map***map-tag*
13. **exit**
14. **route-map***map-tag* [**permit** | **deny**] [*sequence-number*]
15. **setipnext-hopverify-availability** [*next-hop-addresssequence***track***object*]
16. **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： `Router> 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： `Router# 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	**rtr***operation-number* 例： `Router(config)# rtr 1`	SAA RTR コンフィギュレーション モードを開始し、SAA 動作を設定します。
ステップ 4	**typeechoprotocol***protocol-typetarget* [**source-ipaddr***ip-address*] 例： `Router(config-rtr)# type echo protocol ipicmpecho 10.1.1.10`	SAA エンドツーエンド エコー応答時間プローブ動作を設定します。
ステップ 5	**exit** 例： `Router(config-rtr)# exit`	SAA RTR コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 6	**rtrschedule***operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*monthday* | *daymonth*] | **pending** | **now** | **after***hh*:*mm*:*ss*}] [**ageout***seconds*] 例： `Router(config)# rtr schedule 1 life forever start-time now`	SAA 動作の時間パラメータを設定します。
ステップ 7	**track***object-number***rtr***entry-number*[**reachability**] 例： `Router(config)# track 123 rtr 1 reachability`	Response Time Reporter（RTR）オブジェクトの到達可能性をトラッキングし、トラッキング 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	**delay**{**up***seconds* [**down***seconds*] | [**up***seconds*]**down***seconds*} 例： `Router(config-track)# delay up 60 down 30`	（任意）追跡対象オブジェクトのステート変更の通信を遅延させる時間（秒）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	**exit** 例： `Router(config-track)# exit`	トラッキング コンフィギュレーション モードを終了し、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 10	**interface***typenumber* 例： `Router(config)# interface ethernet 0`	インターフェイスのタイプと番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**ipaddress***ip-addressmask*[**secondary**] 例： `Router(config-if)# ip address 10.1.1.11 255.0.0.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。 • IPv4 アドレスの設定手順については、『*Cisco IOS IP Addressing Services Configuration Guide*』の「Configuring IPv4 Addresses」の章を参照してください。
ステップ 12	**ippolicyroute-map***map-tag* 例： `Router(config-if)# ip policy route-map alpha`	ポリシー ルーティングをイネーブルにし、ポリシー ルーティングに使用するルートマップを指定します。
ステップ 13	**exit** 例： `Router(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、ルータをグローバル コンフィギュレーション モードに戻します。
ステップ 14	**route-map***map-tag* [**permit** | **deny**] [*sequence-number*] 例： `Router(config)# route-map alpha`	ルート マップを指定し、ルート マップ コンフィギュレーション モードを開始します。
ステップ 15	**setipnext-hopverify-availability** [*next-hop-addresssequence***track***object*] 例： `Router(config-route-map)# set ip next-hop verify-availability 10.1.1.1 10 track 123`	ルート マップを設定し、トラッキング対象オブジェクトの到達可能性を確認します。

	コマンドまたはアクション	目的
ステップ 16	**end** 例： `Router(config-route-map)# end`	ルートマップ コンフィギュレーション モードを終了し、ルータを特権 EXEC モードに戻します。

複数のトラッキング オプションに対する PBR サポートの設定

複数のトラッキング オプションに対する PBR サポートを設定するには、次の作業を実行します。この作業では、ルート マップを作成および設定し、トラッキング対象オブジェクトの到達可能性を確認します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipslamonitor***operation-number*
4. **typeechoprotocolipIcmpEcho**{*destination-ip-address*|*destination-hostname*}[**source-ipaddr** {*ip-address*|*hostname*} | **source-interface***interface-name*]
5. **exit**
6. **ipslamonitorschedule***operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*monthday* | *daymonth*] | **pending** | **now** | **after***hh*:*mm*:*ss*}] [**ageout***seconds*] [**recurring**]
7. **track***object-number***rtr***entry-number*[**reachability**|**state**]
8. **delay** {**up***seconds* [**down***seconds*] | [**up***seconds*]**down***seconds*}
9. **exit**
10. **interface***typenumber*
11. **ipaddress***ip-addressmask*[**secondary**]
12. **ippolicyroute-map***map-tag*
13. **exit**
14. **route-map***map-tag* [**permit** | **deny**] [*sequence-number*]
15. **setipnext-hopverify-availability** [*next-hop-addresssequence***track***object*]
16. **end**
17. **showtrack***object-number*
18. **showroute-map** [*map-name*| **all**| **dynamic**]

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	**ipslamonitor***operation-number* 例： `Device(config)# ip sla monitor 1`	Cisco IOS IP サービス レベル契約（SLA）動作設定を開始し、IP SLA モニタ 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	**typeechoprotocolipIcmpEcho**{*destination-ip-address*|*destination-hostname*}[**source-ipaddr** {*ip-address*|*hostname*} | **source-interface***interface-name*] 例： `Device(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1`	IP SLA Internet Control Message Protocol（ICMP）エコープローブ動作を設定します。
ステップ 5	**exit** 例： `Device(config-sla-monitor)# exit`	IP SLA モニタ コンフィギュレーション モードを終了し、デバイスをグローバル コンフィギュレーション モードに戻します。
ステップ 6	**ipslamonitorschedule***operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*monthday* | *daymonth*] | **pending** | **now** | **after***hh*:*mm*:*ss*}] [**ageout***seconds*] [**recurring**] 例： `Device(config)# ip sla monitor schedule 1 life forever start-time now`	単一の Cisco IOS IP SLA 動作のスケジューリング パラメータを設定します。 • この例では、IP SLA 動作の時間パラメータを設定します。

	コマンドまたはアクション	目的
ステップ 7	**track***object-number***rtr***entry-number*[**reachability**|**state**] 例： `Device(config)# track 123 rtr 1 reachability`	Response Time Reporter（RTR）オブジェクトの到達可能性をトラッキングし、トラッキング 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	**delay** {**up***seconds* [**down***seconds*] | [**up***seconds*]**down***seconds*} 例： `Device(config-track)# delay up 60 down 30`	（任意）トラッキング対象オブジェクトの通信状態変化の遅延時間（秒）を指定します。
ステップ 9	**exit** 例： `Device(config-track)# exit`	トラッキング コンフィギュレーション モードを終了し、デバイスをグローバル コンフィギュレーション モードに戻します。
ステップ 10	**interface***typenumber* 例： `Device(config)# interface serial 2/0`	インターフェイスのタイプと番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**ipaddress***ip-addressmask*[**secondary**] 例： `Device(config-if)# ip address 192.168.1.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスまたはセカンダリ IP アドレスを指定します。 • IPv4 アドレスの設定手順については、『*Cisco IOS IP Addressing Services Configuration Guide*』の「Configuring IPv4 Addresses」の章を参照してください。 • この例では、着信インターフェイスの IP アドレスを指定します。これは、ポリシールーティングが

	コマンドまたはアクション	目的
		イネーブル化されるインターフェイスです。
ステップ 12	**ippolicyroute-map***map-tag* 例： `Device(config-if)# ip policy route-map alpha`	ポリシー ルーティングをイネーブルにし、ポリシー ルーティングに使用するルート マップを指定します。
ステップ 13	**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、デバイスをグローバル コンフィギュレーション モードに戻します。
ステップ 14	**route-map***map-tag* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map alpha`	ルート マップを指定し、ルート マップ コンフィギュレーション モードを開始します。
ステップ 15	**setipnext-hopverify-availability** [*next-hop-addresssequence***track***object*] 例： `Device(config-route-map)# set ip next-hop verify-availability 10.1.1.1 10 track 123`	ルート マップを設定し、トラッキング対象オブジェクトの到達可能性を確認します。 • この例では、デバイスが到達可能である場合、シリアル インターフェイス 2/0 で受信したパケットを 10.1.1.1 へ転送するようにポリシーを設定します。
ステップ 16	**end** 例： `Device(config-route-map)# end`	ルートマップ コンフィギュレーション モードを終了し、デバイスを特権 EXEC モードに戻します。

	コマンドまたはアクション	目的
ステップ 17	**showtrack***object-number* 例： `Device# show track 123`	（任意）トラッキング情報を表示します。 • このコマンドを使用して、設定を確認します。「例」のセクションでこのタスクの出力を参照してください。
ステップ 18	**showroute-map** [*map-name*| **all**| **dynamic**] 例： `Device# show route-map alpha`	（任意）ルートマップ情報を表示します。 • この例では、「alpha」という名前のルートマップに関する情報を表示します。「例」のセクションでこのタスクの出力を参照してください。

例

次の **showtrack** コマンドからの出力は、トラッキング対象オブジェクト 123 が到達可能であることを示しています。

```
Device# show track 123
Track 123
  Response Time Reporter 1 reachability
  Reachability is Up
    2 changes, last change 00:00:33
  Delay up 60 secs, down 30 secs
  Latest operation return code: OK
  Latest RTT (millisecs) 20
  Tracked by:
    ROUTE-MAP 0
```

次の **showroute-map** コマンドからの出力は、この作業で設定した「alpha」という名前のルートマップに関する情報を示しています。

```
Device# show route-map alpha
route-map alpha, permit, sequence 10
  Match clauses:
  Set clauses:
    ip next-hop verify-availability 10.1.1.1 10 track 123  [up]
  Policy routing matches: 0 packets, 0 bytes
```

複数のトラッキングオプションに対するPBRサポートの設定例

Cisco IOS Release 12.3(11)T、12.2(25)S、およびそれ以前

次の例では、Cisco IOS リリース 12.3(11)T、12.2(25)S、またはそれ以前のリリースを実行しているルータ上で、PBR 用にオブジェクト トラッキングを設定しています。

イーサネット インターフェイス 0 で受信したパケットを、デバイスが到達可能である（ping に応答する）場合に限り、10.1.1.1 へ転送するポリシーを設定します。10.1.1.1 がアップしていない場合は、10.2.2.2 へパケットを転送します。10.2.2.2 も到達不可能な場合ポリシー ルーティングは失敗し、ルーティング テーブルに従ってパケットをルーティングします。

リモート デバイスに対して ping を実行するため、2 つの Response Time Reporter (RTR) を設定して、RTR をトラッキングします。ポリシー ルーティングがトラッキング対象 RTR の状態をモニタし、それらの状態に基づいて転送を決定します。

```
! Define and start the RTRs.
rtr 1
 type echo protocol ipicmpecho 10.1.1.1
rtr schedule 1 start-time now life forever
!
rtr 2
 type echo protocol ipicmpecho 10.2.2.2
rtr schedule 2 start-time now life forever
!
! Track the RTRs.
track 123 rtr 1 reachability
track 124 rtr 2 reachability
!
! Enable policy routing on the incoming interface.
interface ethernet 0
 ip address 10.4.4.4 255.255.255.0
 ip policy route-map beta
!
! 10.1.1.1 is via this interface.
interface ethernet 1
 ip address 10.1.1.254 255.255.255.0
!
! 10.2.2.2 is via this interface.
interface ethernet 2
 ip address 10.2.2.254 255.255.255.0
!
! Define a route map to set the next-hop depending on the state of the tracked RTRs.
route-map beta
 set ip next-hop verify-availability 10.1.1.1 10 track 123
 set ip next-hop verify-availability 10.2.2.2 20 track 124
```

例：複数のトラッキング オプションに対する PBR サポートの設定

次の例は、複数のトラッキング オプションに対する PBR サポートの設定方法を示しています。

イーサネット インターフェイス 0 で受信したパケットを、デバイスが到達可能である（ping に応答する）場合に限り、10.1.1.1 へ転送するポリシーを設定します。10.1.1.1 がアップしていない場

合は、10.2.2.2 へパケットを転送します。10.2.2.2 も到達不可能な場合ポリシー ルーティングは失敗し、ルーティング テーブルに従ってパケットをルーティングします。

リモート デバイスに対して ping を実行するため、2 つの RTR を設定して、RTR をトラッキングします。ポリシー ルーティングがトラッキング対象RTRの状態をモニタし、それらの状態に基づいて転送を決定します。

```
! Define and start the RTRs.
ip sla monitor 1
 type echo protocol ipicmpecho 10.1.1.1
ip sla monitor schedule 1 start-time now life forever
!
ip sla monitor 2
 type echo protocol ipicmpecho 10.2.2.2
ip sla monitor schedule 2 start-time now life forever
!
! Track the RTRs.
track 123 rtr 1 reachability
track 124 rtr 2 reachability
!
! Enable policy routing on the incoming interface.
interface ethernet 0
 ip address 10.4.4.4 255.255.255.0
 ip policy route-map beta
!
! 10.1.1.1 is via this interface.
interface ethernet 1
 ip address 10.1.1.254 255.255.255.0
!
! 10.2.2.2 is via this interface.
interface ethernet 2
 ip address 10.2.2.254 255.255.255.0
!
! Define a route map to set the next-hop depending on the state of the tracked RTRs.
route-map beta
 set ip next-hop verify-availability 10.1.1.1 10 track 123
 set ip next-hop verify-availability 10.2.2.2 20 track 124
```

その他の参考資料

ここでは、複数のトラッキング オプションに対するPBRサポート機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS ソフトウェア内でのオブジェクト トラッキング	『*Cisco IOS IP Application Services Configuration Guide*』の「Configuring Enhanced Object Tracking」の章
IP アドレスの設定	『*Cisco IOS IP Addressing Services Configuration Guide*』の「Configuring IPv4 Addresses」の章

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/en/US/support/index.html

コマンド リファレンス

次のコマンドは、このモジュールで説明した機能で導入または修正されたものです。これらのコマンドの詳細については、『*Cisco IOS IP Routing: Protocol-Independent Command Reference*』を参照してください。すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup でコマンド検索ツールを使用するか、http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html で『*Cisco IOS Master Command List, All Releases*』を参照してください。

- **setipnext-hopverify-availability**

複数のトラッキングオプションに対するPBR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 *7*：複数のトラッキング オプションに対する *PBR* サポートの機能情報

機能名	リリース	機能情報
複数のトラッキング オプションに対する PBR サポート		複数のトラッキング オプションに対する PBR サポート機能は、Cisco Discovery Protocol（CDP）を使ったオブジェクトトラッキングの機能を拡張し、追加の方法を使って、ポリシーベースルーティング（PBR）処理でオブジェクトが使用可能かどうかを確認できます。確認方法として使用できるのは、Internet Control Message Protocol（ICMP）ping、ユーザ データグラム プロトコル（UDP）ping、または HTTP GET です。 **setipnext-hopverify-availability** コマンドは、この機能によって導入または変更されました。

第 8 章

PBR 一致トラック オブジェクト

PBR 一致トラック オブジェクト機能を使用すると、ポリシーベース ルーティング（PBR）中にデバイスがスタブ オブジェクトをトラッキングすることができます。

- 機能情報の確認，103 ページ
- PBR 一致トラック オブジェクトの制限，103 ページ
- PBR 一致トラック オブジェクトに関する情報，104 ページ
- PBR 一致トラック オブジェクトの設定方法，105 ページ
- PBR 一致トラック オブジェクトの確認，106 ページ
- PBR 一致トラック オブジェクトの設定例，107 ページ
- PBR 一致トラック オブジェクトに関するその他の参考資料，107 ページ
- PBR 一致トラック オブジェクトに関する機能情報，108 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。

PBR 一致トラック オブジェクトの制限

- ルート マップ シーケンスで同時に使用できる一致トラック オブジェクトは 1 つだけです。

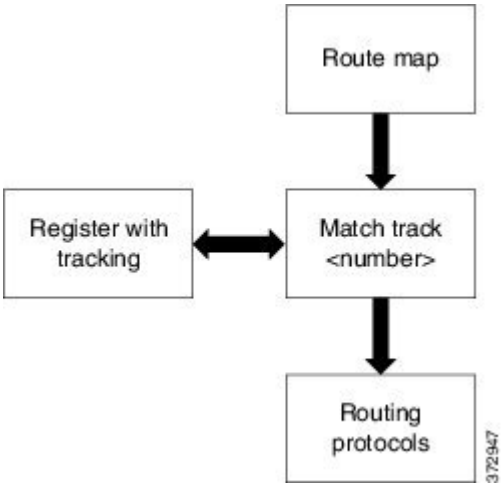
- 別の一致トラック オブジェクトを設定する前に、既存の一致トラック オブジェクトを削除する必要があります。一致トラック オブジェクト番号設定を削除すると、一致トラック オブジェクトはトラッキング コンポーネントから登録解除されます。

PBR 一致トラック オブジェクトに関する情報

PBR 一致トラック オブジェクトの概要

一致トラック オブジェクトとしてトラッキングするスタブ オブジェクトを参照します。デバイスは一致トラック オブジェクトが存在するか確認し、ない場合はエラー メッセージを出力します。その後、このオブジェクトのトラッキングのため、トラッキング コンポーネントへの登録がなされます。登録に失敗すると、デバイスはエラーを出力します。

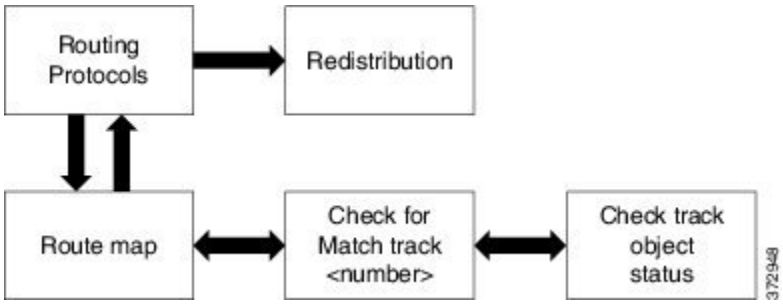
図 *5*：一致トラック オブジェクトの登録



再配布時に、ルーティング プロトコルは、ルート マップに既存のルートとの一致がないか確認します。これにより、特定の一致基準に該当する正確なルート マップが得られます。一致トラック

オブジェクトとともにこのルートマップを適用すると、デバイスは一致トラック オブジェクトのステータスを確認し、特定のルート マップを提供します。

図 *6*：ルーティング プロトコルを使用する再配布時のルート マップ



デバイスは、ルート フィルタリングと配布に Border Gateway Protocol（BGP）を使用します。デバイスは既存の通知機能を使用して、ルーティング プロトコルに対して新しい match 句に関する通知を送信します。また、再配布時のポリシーベース ルーティング（PBR）クエリに基づいて、一致トラック オブジェクトのステータス変更についてルーティング プロトコルに通知します。

PBR 一致トラック オブジェクトの設定方法

PBR 一致トラック オブジェクトの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **route-map** *map-tag*
4. **match track** *track-object-number*
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）。

	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* 例： `Device(config)# route-map abc`	ポリシー ルーティングをイネーブルにし、ルートマップ コンフィギュレーション モードを開始します。
ステップ 4	**match track** *track-object-number* 例： `Device(config-route-map)# match track 2`	スタブ オブジェクトをトラッキングします。値の範囲は 1 ～ 1000 です。 （注） このコマンドは、指定したトラック オブジェクトがデバイスで利用可能な場合のみ有効です。
ステップ 5	**end** 例： `Device(config-route-map)# end`	特権 EXEC モードに戻ります。

PBR 一致トラック オブジェクトの確認

手順の概要

1. イネーブル化
2. **show route-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	**show route-map** *map-name* 例： `Device# show route-map abc`	特定のルートマップに関する簡単な情報を表示します。

PBR 一致トラック オブジェクトの設定例

例：PBR 一致トラック オブジェクトの設定

```
Device> enable
Device# configure terminal
Device(config)# route-map abc
Device(config-route-map)# match track 2
Device(config-route-map)# end
```

例：PBR 一致トラック オブジェクトの確認

show route-map *map-name* コマンドの出力例

特定のルートマップに関する情報を表示するには、**show route-map** *map-name* コマンドを特権 EXEC モードで使用します。

```
Device> enable
Device# show route-map abc
route-map abc, permit, sequence 10
  Match clauses:
    track-object 2
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
```

PBR 一致トラック オブジェクトに関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

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/support

PBR 一致トラック オブジェクトに関する機能情報

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。

機能名	リリース	機能情報
PBR 一致トラック オブジェクト	Cisco IOS XE リリース 3.13S	PBR 一致トラック オブジェクト機能を使用すると、ポリシーベース ルーティング中にデバイスがスタブ オブジェクトをトラッキングすることができます。 次のコマンドが導入されました。**match track** *track-object-number*

第 9 章

IPv6 ポリシーベース ルーティング

IPv6 と IPv4 の両方でポリシーベース ルーティング（PBR）を使用することにより、ユーザは受信したパケットのルーティング方法を手動で設定できます。PBR では、複数の属性を使用してユーザがパケットを識別し、ネクスト ホップまたはパケットが送信される出力インターフェイスを指定することができます。PBR では、基本的なパケット マーキング機能も提供します。

- 機能情報の確認，109 ページ
- IPv6 ポリシーベース ルーティングに関する情報，110 ページ
- IPv6 ポリシーベース ルーティングをイネーブルにする方法，113 ページ
- IPv6 ポリシーベース ルーティングの設定例，119 ページ
- IPv6 ポリシーベース ルーティングのその他の参考資料，120 ページ
- IPv6 ポリシーベース ルーティングの機能情報，121 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 ポリシーベース ルーティングに関する情報

ポリシーベース ルーティングの概要

ポリシーベース ルーティング（PBR）は、トラフィック フローに定義ポリシーを設定し、ルートにおけるルーティング プロトコルへの依存度を軽くして、パケットのルーティングを柔軟に行えるようにします。したがって、PBR は、ルーティング プロトコルで提供される既存のメカニズムを拡張および補完することにより、ルーティングの制御を強化します。PBR を使用すると、IPv6 precedence を設定できます。単純なポリシーでは、これらのタスクのいずれかを使用し、複雑なポリシーでは、これらすべてのタスクを使用できます。高コストリンク上のプライオリティ トラフィックなど、特定のトラフィックのパスを指定することもできます。IPv6 PBR は Cisco ASR 1000 シリーズ プラットフォーム上でサポートされます。

PBR for IPv6 は、転送される IPv6 パケットおよび送信される IPv6 パケットの両方に適用できます。転送されるパケットの場合、PBR for IPv6 は、次の転送パスでサポートされる IPv6 入力インターフェイス機能として実装されます。

- プロセス
- シスコ エクスプレス フォワーディング（旧称 CEF）
- 分散型シスコ エクスプレス フォワーディング

ポリシーは、IPv6 アドレス、ポート番号、プロトコル、またはパケットのサイズに基づいて作成できます。

PBR を使用すると、次の作業を実行できます。

- 拡張アクセス リスト基準に基づいてトラフィックを分類する。リストにアクセスし、次に一致基準を設定します。
- 差別化されたサービス クラスをイネーブルにする機能をネットワークに与える IPv6 precedence ビットを設定する。
- 特定のトラフィック エンジニアリング パスにパケットをルーティングする。ネットワークを介して特定の Quality of Service（QoS）を得るためにパケットをルーティングする必要がある場合があります。

PBR を使用すると、ネットワークのエッジでパケットを分類およびマーキングできます。PBR では、precedence 値を設定することにより、パケットをマーキングします。precedence 値は、ネットワーク コアにあるデバイスが適切な QoS をパケットに適用するために直接使用でき、これにより、パケットの分類がネットワーク エッジで維持されます。

ポリシーベース ルーティングの機能

ポリシーベースルーティング（PBR）がイネーブルのインターフェイスで受信するすべてのパケットは、ルート マップと呼ばれる拡張パケット フィルタを経由して渡されます。PBR で使用するルート マップは、ポリシーを要求し、パケットの転送先を判断します。

ルート マップは文で構成されています。ルート マップ文は、permit または deny としてマークでき、次の方法で解釈されます。

- パケットが、permit とマークされているルート マップのすべての match 文に一致する場合、デバイスは set 文を使用して、パケットのポリシー ルーティングを試みます。それ以外の場合、パケットは通常どおり転送されます。
- パケットが、deny とマークされているルート マップのいずれかの match 文に一致する場合、そのパケットは PBR の影響を受けず、通常どおり転送されます。
- 文が permit とマークされ、パケットがいずれのルート マップ文にも一致しない場合、そのパケットは通常の転送チャネルを介して返送され、宛先ベースのルーティングが実行されます。

パケットの送信元のインターフェイスではなく、パケットを受信するインターフェイスでポリシーベース ルーティング（PBR）インターフェイスを設定する必要があります。

パケット マッチング

IPv6 向けポリシーベースルーティング（PBR）は、関連する PBR ルートマップで **matchipv6address** コマンドを使用してパケット マッチングを行います。パケットの一致基準は、次に示す、IPv6 アクセス リストでサポートされている基準です。

- 入力インターフェイス
- 送信元 IPv6 アドレス（標準または拡張アクセス コントロール リスト（ACL））
- 宛先 IPv6 アドレス（標準または拡張 ACL）
- プロトコル（拡張 ACL）
- 送信元ポートおよび宛先ポート（拡張 ACL）
- DSCP（拡張 ACL）
- フローラベル（拡張 ACL）
- フラグメント（拡張 ACL）

パケットは、PBR ルート マップで **matchlength** コマンドを使用して、パケット長に基づいてマッチングすることもできます。

match 文は、**matchipv6address** コマンドで指定した基準に基づいて最初に評価され、次に、**matchlength** コマンドで指定した基準に基づいて評価されます。したがって、ACL と length 文の両方が使用されている場合、最初にACLによるマッチングがパケットに対して行われます。ACL

マッチングに合格したパケットだけが、パケット長による次のマッチングの対象となります。最後に、ACL と length 文の両方に合格したパケットだけに対してポリシー ルーティングが行われます。

set 文を使用したパケット転送

IPv6 パケット転送に対するポリシーベース ルーティング（PBR）は、PBR ルートマップの複数の set ステートメントを使用して制御されます。これらの set 文は、示された順序で個別に評価され、PBR は各 set 文を順番に使用してパケットの転送を試みます。PBR は、各 set 文を個別に評価します。前の set 文や以降の set 文は参照しません。

PBR for IPv6 のルート マップには、複数の転送文を設定できます。次の set 文を指定できます。

- IPv6 ネクスト ホップ。パケットの送信先となるネクスト ホップ。このネクスト ホップは、ルーティング情報ベース（RIB）に存在し、直接接続され、グローバル IPv6 アドレスである必要があります。このネクスト ホップが無効である場合、set 文は無視されます。
- 出力インターフェイス。パケットは、指定されたインターフェイスの外に転送されます。パケットの宛先アドレスのエントリは、IPv6 RIB に存在する必要があります。指定された出力インターフェイスは、設定されたパスに存在する必要があります。このインターフェイスが無効な場合、文は無視されます。
- デフォルトの IPv6 ネクスト ホップ。パケットの送信先となるネクスト ホップ。グローバル IPv6 アドレスである必要があります。この set 文は、IPv6 RIB のパケット宛先に明示的なエントリがない場合にだけ使用されます。
- デフォルトの出力インターフェイス。パケットは、指定されたインターフェイスの外に転送されます。この set 文は、IPv6 RIB のパケット宛先に明示的なエントリがない場合にだけ使用されます。

（注） PBR が set 文を評価する順序は、上にリストしている順序となります。この順序は、**show** コマンドでリストしているルートマップの set 文での順序とは異なる場合があります。

ポリシーベース ルーティングを使用する場合

特定のパケットを明らかに最短のパス以外の方法でルーティングする必要がある場合は、ポリシーベース ルーティング（PBR）を使用できます。たとえば、PBR を使用して、次の機能を提供できます。

- 同等アクセス
- プロトコル別のルーティング
- 送信元別のルーティング
- 双方向トラフィック対バッチ トラフィックに基づくルーティング

- 専用リンクに基づくルーティング

アプリケーションまたはトラフィックによっては、Quality of Service（QoS）固有のルーティングが有効です。たとえば、在庫記録を本社に送信する場合は高帯域幅で高コストのリンクを短時間使用し、電子メールなどの日常的に使うアプリケーション データは低帯域幅で低コストのリンクで送信します。

IPv6 ポリシーベース ルーティングをイネーブルにする方法

インターフェイスでの IPv6 PBR の有効化

IPv6 のポリシーベース ルーティング（PBR）を有効にするには、パケットの一致基準と目的のポリシールーティングアクションを指定する、ルートマップを作成する必要があります。次に、そのルート マップを必要なインターフェイスに関連付けます。指定されたインターフェイスに到着し、match 句に一致するすべてのパケットに対して、PBR が実行されます。

PBR では、**setvrf** コマンドにより Virtual Routing and Forwarding（VRF）インスタンスとインターフェイス アソシエーションを切り離し、既存の PBR またはルート マップ設定を使用して、アクセス コントロール リスト（ACL）ベースの分類に基づいて VRF を選択できるようになります。このコマンドは、1 つのルータに複数ルーティング テーブルを提供し、ACL 分類に基づいてルートを選択できるようにします。ルータは、ACLに基づいてパケットを分類し、ルーティングテーブルを選択し、宛先アドレスを検索し、パケットをルーティングします。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **route-map***map-tag* [**permit** | **deny**] [*sequence-number*]
4. 次のいずれかを実行します。
   - **matchlength***minimum-lengthmaximum-length*
   - **matchipv6address** {**prefix-list***prefix-list-name* | *access-list-name*}
5. 次のいずれかを実行します。
   - **setipv6precedence***precedence-value*
   - **setipv6next-hop***global-ipv6-address* [*global-ipv6-address...*]
   - **setinterface***typenumber* [*...type number*]
   - **setipv6defaultnext-hop***global-ipv6-address* [*global-ipv6-address...*]
   - **setdefaultinterface***typenumber* [*...type number*]
   - **setvrf***vrf-name*
6. **exit**
7. **interface***typenumber*
8. **ipv6policyroute-map***route-map-name*
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	**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	**route-map***map-tag* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map rip-to-ospf permit`	ルーティング プロトコル間でルートを再配布する条件を定義するか、ポリシー ルーティングを有効にしてルート マップ コンフィギュレーション モードを開始します。

ステップ 4	次のいずれかを実行します。
	• **matchlength***minimum-lengthmaximum-length*
	• **matchipv6address** {**prefix-list***prefix-list-name* | *access-list-name*}
	
	例：
	
	`Device(config-route-map)# match length 3 200`
	
	例：
	
	`Device(config-route-map)# match ipv6 address marketing`
		一致基準を指定します。
		• 次のうちの任意の項目またはすべてを指定できます。
		  • レベル 3 のパケット長とのマッチング。
		  • 指定された IPv6 アクセス リストとのマッチング。
		  • **match** コマンドを指定しない場合、ルート マップはすべてのパケットに適用されます。

ステップ 5	次のいずれかを実行します。
	• **setipv6precedence***precedence-value*
	• **setipv6next-hop***global-ipv6-address* [*global-ipv6-address...*]
	• **setinterface***typenumber* [*...type number*]
	• **setipv6defaultnext-hop***global-ipv6-address* [*global-ipv6-address...*]
	• **setdefaultinterface***typenumber* [*...type number*]
	• **setvrf***vrf-name*
	
	例：
	
	`Device(config-route-map)# set ipv6 precedence 1`
	
	例：
	
	`Device(config-route-map)# set ipv6 next-hop 2001:DB8:2003:1::95`
		基準に一致したパケットに適用するアクション（1 つまたは複数）を指定します。
		• 次のうちの任意の項目またはすべてを指定できます。
		  • IPv6 ヘッダーに precedence 値を設定します。
		  • パケットのルーティング先となるネクストホップを設定します（ネクスト ホップは隣接している必要があります）。
		  • パケットの出力インターフェイスを設定します。
		  • 宛先への明示的なルートがない場合に、パケットのルーティング先となるネクスト ホップを設定します。
		  • 宛先への明示的なルートがない場合に、パケットの出力インターフェイスを設定します。
		  • ポリシーベース ルーティング VRF の選択のために、ルート マップ内に VRF インスタンス選択を設定します。

	コマンドまたはアクション	目的

	例：
	`Device(config-route-map)# set interface GigabitEthernet 0/0/1`
	例：
	`Device(config-route-map)# set ipv6 default next-hop 2001:DB8:2003:1::95`
	例：
	`Device(config-route-map)# set default interface GigabitEthernet 0/0/0`
	例：
	`Device(config-route-map)# set vrf vrfname`	

ステップ 6	**exit** 例： `Device(config-route-map)# exit`	ルート マップ 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。
ステップ 7	**interface***typenumber* 例： `Device(config)# interface FastEthernet 1/0`	インターフェイスのタイプと番号を指定し、ルータ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 8	**ipv6policyroute-map***route-map-name* 例： `Device(config-if)# ipv6 policy-route-map interactive`	インターフェイスで IPv6 PBR に使用するルート マップを特定します。
ステップ 9	**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。

ローカル PBR for IPv6 の有効化

デバイスが生成したパケットに対して、通常はポリシーによるルーティングは行われません。これらのパケットのためのローカル IPv6 ポリシーベース ルーティング（PBR）をイネーブルにするには、この作業を実行して、どのルート マップをデバイスで使用するべきかを示します。

手順の概要

1. イネーブル化
2. **configureterminal**
3. **ipv6localpolicyroute-map***route-map-name*
4. **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	**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	**ipv6localpolicyroute-map***route-map-name* 例： `Device(config)# ipv6 local policy route-map pbr-src-90`	デバイスによって生成されるパケットに対する IPv6 PBR を設定します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

PBR for IPv6 の設定と動作の確認

手順の概要

1. イネーブル化
2. **showipv6policy**

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	**showipv6policy** 例： `Device# show ipv6 policy`	IPv6 ポリシー ルーティング パケットのアクティビティに関する情報を表示します。

PBR for IPv6 のトラブルシューティング

ポリシー ルーティングでは、パケットのさまざまな部分を分析し、次にパケット内の特定のユーザ定義属性に基づいてパケットをルーティングします。

手順の概要

1. イネーブル化
2. **showroute-map** [*map-name* | **dynamic** [*dynamic-map-name* | **application** [*application-name*]] | **all**] [**detailed**]
3. **debugipv6policy** [*access-list-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	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	**showroute-map** [*map-name* | **dynamic** [*dynamic-map-name* | **application** [*application-name*]] | **all**] [**detailed**] 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。
ステップ 3	**debugipv6policy** [*access-list-name*] 例： `Device# debug ipv6 policy`	IPv6 ポリシー ルーティング パケットのアクティビティのデバッグをイネーブルにします。

IPv6 ポリシーベース ルーティングの設定例

例：インターフェイスでの PBR のイネーブル化

次の例では、pbr-dest-1 という名前のルート マップを作成および設定し、パケット一致基準および目的のポリシー ルーティング アクションを指定します。次に、PBR が GigabitEthernet インターフェイス 0/0/1 でイネーブルにされます。

```
ipv6 access-list match-dest-1
  permit ipv6 any 2001:DB8:2001:1760::/32
route-map pbr-dest-1 permit 10
  match ipv6 address match-dest-1
  set interface GigabitEthernet 0/0/0
interface GigabitEthernet0/0/1
  ipv6 policy-route-map interactive
```

例：ローカル PBR for IPv6 の有効化

次の例では、宛先 IPv6 アドレスがアクセス リスト pbr-src-90 で許可されている IPv6 アドレス範囲に一致するパケットが、IPv6 アドレス 2001:DB8:2003:1::95 のデバイスに送信されています。

```
ipv6 access-list src-90
  permit ipv6 host 2001:DB8:2003::90 2001:DB8:2001:1000::/64
route-map pbr-src-90 permit 10
  match ipv6 address src-90
```

```
  set ipv6 next-hop 2001:DB8:2003:1::95
ipv6 local policy route-map pbr-src-90
```

例：show ipv6 policy コマンドの出力

show ipv6 policy コマンドによって、次の例で示すように PBR 設定が表示されます。

```
Device# show ipv6 policy

Interface                 Routemap
GigabitEthernet0/0/0      src-1
```

例：Route-Map 情報の確認

次の **show route-map** コマンドの出力例では、ポリシー一致の数など、特定のルートマップ情報が表示されます。

```
Device# show route-map

route-map bill, permit, sequence 10
  Match clauses:
  Set clauses:
  Policy routing matches:0 packets, 0 bytes
```

IPv6 ポリシーベース ルーティ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 Command List, All Releases』
IP ルーティングのプロトコル独立型コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上の注意事項、および例	『Cisco IOS IP Routing: Protocol-Independent Command Reference』

MIB

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

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 ポリシーベース ルーティングの機能情報

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 *8*：*IPv6* ポリシーベース ルーティングの機能情報

機能名	リリース	機能情報
IPv6 ポリシーベース ルーティング	Cisco IOS XE Release 3.2S	IPv6 向けポリシーベース ルーティングを使用すると、ユーザは、受信したパケットをルーティングする方法を手動で設定できます。 次のコマンドが導入または変更されました。**debug fm ipv6 pbr**、**debug ipv6 policy**、**ipv6 local policy route-map**、**ipv6 policy route-map**、**match ipv6 address**、**match length**、**route-map**、**set default interface**、**set interface**、**set ipv6 default next-hop**、**set ipv6 next-hop (PBR)**、**set ipv6 precedence**、**set vrf**、**show fm ipv6 pbr all**、**show fm ipv6 pbr interface**、**show ipv6 policy**、**show route-map**

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，124 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，124 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，124 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，125 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，129 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，139 ページ
- その他の参考資料，140 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，140 ページ
- 用語集，142 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。

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：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

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，143 ページ
- Multi-VRF サポートの前提条件，144 ページ
- Multi-VRF サポートの制約事項，144 ページ
- Multi-VRF サポートに関する情報，144 ページ
- Multi-VRF サポートの設定方法，147 ページ
- Multi-VRF サポートの設定例，156 ページ
- その他の参考資料，159 ページ
- Multi-VRF サポートの機能情報，160 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。

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。

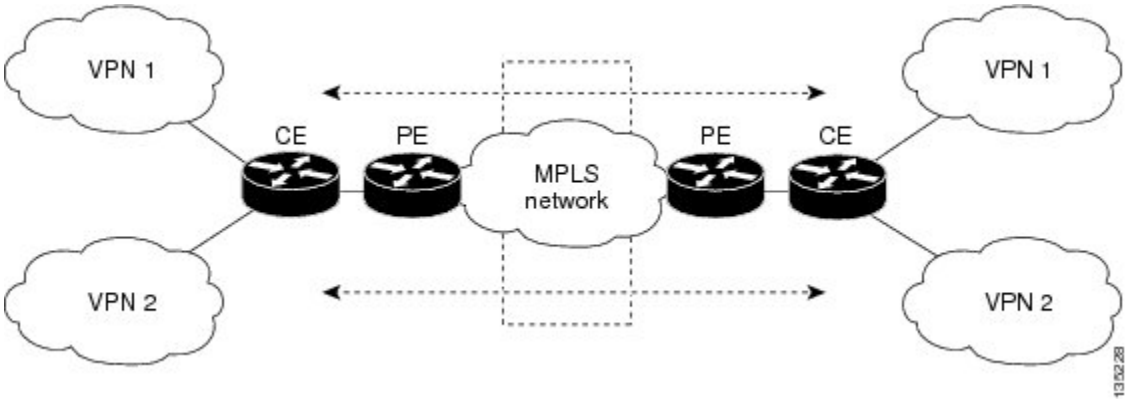
- 各 CE デバイスは、プロバイダー エッジ（PE）デバイスにサイトのローカル ルートをアドバタイズし、プロバイダー エッジ（PE）デバイスからリモート VPN ルートを学習します。

- 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 *7*：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

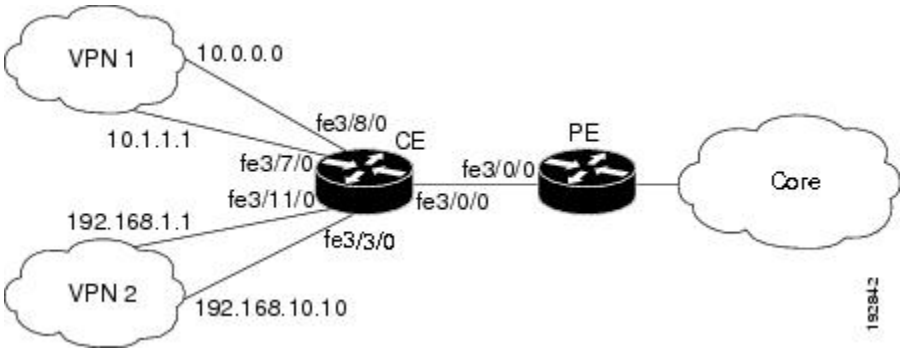
1. イネーブル化
2. **configure terminal**
3. **interface***typeslot*/*subslot*/*port*[**.***subinterface*]
4. **mpls ip**

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 *10*：*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	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.5S	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 12 章

デフォルトのパッシブ インターフェイス

デフォルトのパッシブインターフェイス機能は、すべてのインターフェイスがデフォルトでパッシブとして設定されるように許可することで、配信デバイスの設定を簡素化します。ISP や大規模な企業ネットワークでは、多数のディストリビューションデバイスで200以上のインターフェイスがあります。これらのインターフェイスからルーティング情報を取得するには、すべてのインターフェイスでルーティング プロトコルを設定し、隣接させないインターフェイスで **passive-interface** コマンドを手動設定する必要があります。

- 機能情報の確認，161 ページ
- デフォルトのパッシブ インターフェイスに関する情報，162 ページ
- デフォルトのパッシブ インターフェイスの設定方法，163 ページ
- デフォルトのパッシブ インターフェイスの設定例，165 ページ
- その他の参考資料，166 ページ
- デフォルトのパッシブ インターフェイスの機能情報，167 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。

デフォルトのパッシブ インターフェイスに関する情報

デフォルトのパッシブ インターフェイス

大規模な企業ネットワークでは、多数のディストリビューション デバイスで 200 以上のインターフェイスがあります。デフォルトのパッシブ インターフェイス機能を導入する前に、次の方法でこれらのインターフェイスからルーティング情報を取得できます。

- バックボーン インターフェイスで Open Shortest Path First（OSPF）などのルーティング プロトコルを設定し、接続されたインターフェイスを再配布する。
- すべてのインターフェイスでルーティング プロトコルを設定し、手動でそれらのほとんどをパッシブに設定する。

1 つめの方法の場合、ネットワーク オペレータは、再配布が行われるデバイス レベルでタイプ 5 リンクステート アドバタイズメント（LSA）を常に集約できるわけではありません。そのため、多くのタイプ 5 LSA がドメインでフラッディングされる可能性があります。

2 つめの方法では、多くのタイプ 1 LSA がドメインにフラッディングされる可能性があります。エリア境界ルータ（ABR）は、タイプ 1 LSA のそれぞれに対してタイプ 3 LSA を生成し、それらをバックボーンにフラッディングします。ただし、ABR レベルで固有の集約を実行でき、このとき、バックボーンにはサマリー ルートが 1 つだけ挿入されます。これにより、処理のオーバーヘッドが削減されます。

デフォルトのパッシブ インターフェイス機能を導入する前に、すべてのインターフェイスでルーティング プロトコルを設定し、隣接させないインターフェイスに **passive-interface** ルータ コンフィギュレーション コマンドを手動で設定できます。ただし、一部のネットワークでは、このソリューションは 200 以上のパッシブ インターフェイスを設定することになります。デフォルトのパッシブ インターフェイス機能は、すべてのインターフェイスがデフォルトでパッシブとして設定されるようにすることで、この問題を解決しました。**passive-interface default** コマンドを使用して、すべてのインターフェイスをデフォルトでパッシブとして設定し、隣接が必要な各インターフェイスを **no passive-interface** コマンドを使用して設定できます。

デフォルトのパッシブ インターフェイス機能は配信デバイスの設定を簡素化し、ネットワーク管理者は ISP や大規模な企業ネットワーク インターフェイスからルーティング情報を取得することができます。

インターフェイスからのルーティング アップデートの防止

ローカル ネットワーク上の他のデバイスがダイナミックにルートを学習しないようにするには、ルーティング アップデート メッセージがデバイス インターフェイスから送信されないようにします。この機能は、Border Gateway Protocol（BGP）を除くすべての IP ベース ルーティング プロトコルに適用されます。

Open Shortest Path First（OSPF）および Intermediate System to Intermediate System（IS-IS）は、若干異なる動作をします。OSPF の場合、パッシブに指定したインターフェイス アドレスが OSPF ドメインのスタブ ネットワークとして表示されます。OSPF ルーティング情報は、指定されたデバイスのインターフェイスから送受信されません。IS-IS の場合、指定した IP アドレスはインターフェイス上で IS-IS を実際に実行することなくアドバタイズされます。

指定したインターフェイスからのルーティング アップデートを防止するには、ルータ コンフィギュレーション モードで **passive-interface***type number* コマンドを使用します。

デフォルトのパッシブ インターフェイスの設定方法

デフォルトのパッシブ インターフェイスの設定

Enhanced Interior Gateway Routing Protocol（EIGRP）環境内のデバイスのすべてのインターフェイスをデフォルトでパッシブとして設定し、隣接が必要なインターフェイスだけをアクティブにするには、このタスクを実行します。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **router eigrp** {*autonomous-system-number* | *virtual-instance-number*}
4. **passive-interface** [**default**] [*type number*]
5. **no passive-interface** [**default**] [*type number*]
6. **network***network-address* [*options*]
7. **end**
8. **show ip eigrp interfaces**
9. **show ip interface**

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 eigrp** {*autonomous-system-number* | *virtual-instance-number*} 例： `Device(config)# router eigrp 1`	EIGRP 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。 • *autonomous-system-number*：別の EIGRP アドレスファミリ デバイスに対するサービスを識別するための自律システム番号。ルーティング情報にタグを付加するためにも使用されます。指定できる範囲は 1 ～ 65535 です。 • *virtual-instance-number*：EIGRP 仮想インスタンス名。この名前は、単一ルータ上のすべてのアドレスファミリ デバイス プロセスで一意でなければいけませんが、デバイス間で一意である必要はありません。
ステップ 4	**passive-interface** [**default**] [*type number*] 例： `Device(config-router)# passive-interface default`	デフォルトですべてのインターフェイスをパッシブに設定します。
ステップ 5	**no passive-interface** [**default**] [*type number*] 例： `Device(config-router)# no passive-interface gigabitethernet 0/0/0`	隣接が必要なインターフェイスのみアクティブ化します。
ステップ 6	**network***network-address* [*options*] 例： `Device(config-router)# network 192.0.2.0`	ルーティング プロトコルがアドバタイズするネットワーク リストを指定します。
ステップ 7	**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 モードに戻ります。
ステップ 8	**show ip eigrp interfaces** 例： `Device# show ip eigrp interfaces`	ネットワークのインターフェイスがパッシブに設定されているかどうかを確認します。

	コマンドまたはアクション	目的
ステップ 9	**show ip interface** 例： `Device# show ip interface`	イネーブルにしたインターフェイスがアクティブかどうかを確認します。

デフォルトのパッシブ インターフェイスの設定例

例：OSPF のパッシブ インターフェイスの設定

Open Shortest Path First（OSPF）では、パッシブとして指定されたインターフェイスでは hello パケットは送信されません。したがって、デバイスはネイバーを検出できず、OSPF ネイバーもそのネットワーク上のデバイスを参照できません。つまり、このインターフェイスは OSPF ドメインへのスタブ ネットワークとして表示されます。インターフェイス上で OSPF アクティビティを実行することなく、接続されたネットワークに関連付けられたルートを OSPF ドメインにインポートするときにこの設定が役立ちます。

passive-interface ルータ コンフィギュレーション コマンドは、通常、**network** ルータ コンフィギュレーション コマンドでワイルドカードを指定することによって必要以上のインターフェイスが設定されるときに使用します。次の設定により、OSPF は 172.18.0.0 のすべてのサブネットで実行されます。

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 172.18.1.1 255.255.255.0
Device(config-if)# exit
Device(config)# interface GigabitEthernet 1/0/0
Device(config-if)# ip address 172.18.2.1 255.255.255.0
Device(config-if)# exit
Device(config)# interface GigabitEthernet 2/0/0
Device(config-if)# ip address 172.18.3.1 255.255.255.0
Device(config-if)# exit
Device(config)# router ospf 1
Device(config-router)# network 172.18.0.0 0.0.255.255 area 0
Device(config-router)# exit
```

172.18.3.0 で OSPF を実行しない場合は、次のコマンドを入力します。

```
Device(config)# router ospf 1
Device(config-router)# network 172.18.0.0 0.0.255.255 area 0
Device(config-router)# no passive-interface GigabitEthernet 2/0/0
Device(config-router)# exit
```

例：OSPF のデフォルトのパッシブ インターフェイスの設定

次の例では、ネットワーク インターフェイスを設定し、パッシブとして Open Shortest Path First（OSPF）を実行しているすべてのインターフェイスを設定して、シリアルインターフェイス 0/0/0 を有効にします。

```
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip address 172.19.64.38 255.255.255.0 secondary
Device(config-if)# ip address 172.19.232.70 255.255.255.240
Device(config-if)# no ip directed-broadcast
Device(config-if)# exit
Device(config)# interface Serial 0/0/0
Device(config-if)# ip address 172.24.101.14 255.255.255.252
Device(config-if)# no ip directed-broadcast
Device(config-if)# no ip mroute-cache
Device(config-if)# exit
Device(config)# interface TokenRing 0/0/0
Device(config-if)# ip address 172.20.10.4 255.255.255.0
Device(config-if)# no ip directed-broadcast
Device(config-if)# no ip mroute-cache
Device(config-if)# ring-speed 16
Device(config-if)# exit
Device(config)# router ospf 1
Device(config-router)# passive-interface default
Device(config-router)# no passive-interface Serial 0/0/0
Device(config-router)# network 172.16.10.0 0.0.0.255 area 0
Device(config-router)# network 172.19.232.0 0.0.0.255 area 4
Device(config-router)# network 172.24.101.0 0.0.0.255 area 4
Device(config-router)# 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 IOS Master Command List, All Releases』
IP ルーティングのプロトコル独立型コマンド	『Cisco IOS IP Routing: Protocol-Independent 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

デフォルトのパッシブ インターフェイスの機能情報

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 *11*：デフォルトのパッシブ インターフェイスの機能情報

機能名	リリース	機能情報
デフォルトのパッシブ インターフェイス		ISP や大規模な企業ネットワークでは、多数のディストリビューション デバイスで 200 以上のインターフェイスがあります。これらのインターフェイスからルーティング情報を取得するには、すべてのインターフェイスでルーティング プロトコルを設定し、隣接させないインターフェイスで **passive-interface** コマンドを手動設定する必要がありました。デフォルトのパッシブインターフェイス機能を使用すると、1 つの **passive-interface default** コマンドを使用してデフォルトですべてのインターフェイスをパッシブとして設定し、その後、**no passive-interface** コマンドを使用して隣接させる個々のインターフェイスを設定できるため、ディストリビューション デバイスの設定が簡略化されます。

第 13 章

Policy-Based Routing：ポリシーベース ルーティング

ポリシーベース ルーティング機能は、デバイスがパケットをルーティングする前に、それらのパケットをルート マップに照会するプロセスです。ルート マップは、どのパケットが次にどのデバイスにルーティングされるかを決定します。ポリシーベースルーティングは、宛先ルーティングよりも柔軟性に富んだパケット ルーティング メカニズムです。

- 機能情報の確認，169 ページ
- ポリシーベース ルーティングの前提条件，170 ページ
- ポリシーベース ルーティングの概要，170 ページ
- ポリシーベース ルーティングの設定方法，171 ページ
- ポリシーベース ルーティングの設定例，174 ページ
- その他の参考資料，174 ページ
- ポリシーベース ルーティングの機能情報，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。

ポリシーベース ルーティングの前提条件

ポリシー ベースのルーティングでは、IPBase が最小限のライセンス要件です。

ポリシーベース ルーティングの概要

Policy-Based Routing：ポリシーベース ルーティング

ポリシーベース ルーティングは、デバイスが、パケットをルーティングする前に、それらのパケットをルートマップに照合するプロセスです。ルートマップは、どのパケットが次にどのデバイスにルーティングされるかを決定します。特定のパケットを明らかに最短のパス以外の方法でルーティングする必要がある場合は、ポリシーベース ルーティングを有効にします。ポリシーベース ルーティングを使用すると、同等アクセス、プロトコル依存ルーティング、発信元依存ルーティング、双方向対バッチ トラフィックに基づくルーティング、および専用リンクに基づくルーティングを実現できます。ポリシーベース ルーティングは、宛先ルーティングよりも柔軟性に富んだパケット ルーティング メカニズムです。

ポリシーベースルーティングをイネーブルにするには、ポリシーベースルーティングに使用するルート マップを特定し、ルート マップを作成する必要があります。ルート マップ自体は、一致基準とそのすべての match 句が適合した場合の処理を指定します。

インターフェイスでポリシーベースルーティングを有効にするには、インターフェイス コンフィギュレーション モードで **ip policy route-map***map-tag* コマンドを使用することにより、デバイスがどのルートマップを使用する必要があるかを指定します。宛先IPアドレスがデバイスのインターフェイスの IP アドレスと同じ場合を除き、指定したインターフェイスに着信するパケットはポリシーベース ルーティングの対象になります。この **ip policy route-map** コマンドは、このインターフェイスに着信するすべてのパケットの高速スイッチングを無効にします。

ポリシーベース ルーティングに使用するルート マップを定義するには、**route-map***map-tag* [**permit** | **deny**] [*sequence-number*] グローバル コンフィギュレーション コマンドを使用します。

パケットがポリシーベースでルーティングされるかどうかを知るためにパケットを調べるための基準を定義するには、**match length***minimum-length maximum-length* コマンドまたは **match ip address** {*access-list-number* | *access-list-name*} [*access-list-number* | *access-list-name*] コマンド、またはその両方をルート マップ コンフィギュレーション モードで使用します。ルート マップに match 句がない場合は、すべてのパケットを指します。

ポリシー ルート キャッシュのキャッシュ エントリを表示するには、**show ip cache policy** コマンドを使用します。

（注） ポリシーベース ルーティング（PBR）が CEF や Resource Reservation Protocol（RSVP）との相互作用を行わない場合、PBR との間の誤ったインターフェイスが Mediatrace に表示されます。そのため、PBR が CEF または RSVP との間で直接相互作用するように設定し、Mediatrace が物理インターフェイスではなくトンネル インターフェイスの統計情報のみを収集するようにします。

ポリシーベース ルーティングの設定方法

ポリシーベース ルーティングの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***type number*
4. **ip policy route-map***map-tag*
5. **exit**
6. **route-map***map-tag* [**permit** | **deny**] [*sequence-number*]
7. 次のいずれかまたは両方のコマンドを入力します。
   - **match length**
   - **match ip address**
8. **set ip next-hop** {*ip-address*[*...ip-address*] | **dynamic dhcp** | **encapsulate l3vpn***profile-name* | **peer-address** | **recursive** [**global** | **vrf***vrf-name*] *ip-address* | **verify-availability** [*ip-address sequence***track***track-object-number*]}
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）。

	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 1/0/0`	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。
ステップ 4	**ip policy route-map***map-tag* 例： `Device(config-if)# ip policy route-map equal-access`	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。
ステップ 5	**exit** 例： `Device(config-if)# 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 6	**route-map***map-tag* [**permit** | **deny**] [*sequence-number*] 例： `Device(config)# route-map equal-access permit 10`	ルーティング プロトコル間でルートを再配布する条件を定義するか、ポリシーベース ルーティングをイネーブルにしてルート マップ コンフィギュレーション モードを開始します。 • *map-tag*：ルート マップ用のわかりやすい名前を指定します。 • **permit**：（任意）このルート マップの一致基準が満たされた場合、**permit** キーワードが指定されていると、設定アクションに従ってルートが再配布されます。ポリシー ルーティングの場合、パケットはポリシーに従ってルーティングされます。一致基準が満たされなかった場合、**permit** キーワードが指定されていると、同じマップ タグを持つ次のルート マップがテストされます。あるルートが、同じ名前を共有するルート マップ セットの一致基準のいずれをも満たさない場合、そのセットによる再配布は行われません。 • **deny**：（任意）ルート マップの一致基準が満たされた場合でも、**deny** キーワードが指定されているとルートは再配布されません。ポリシー ルーティングの場合、パケットはポリシーに従ってルーティングされません。また、同じマップ タグ名を共有するルート マップは、これ以上検証されませ

	コマンドまたはアクション	目的
		ん。パケットがポリシー ルーティングの対象にならない場合、通常の転送アルゴリズムが使用されます。 • *sequence-number*：（任意）すでに同じ名前で設定されているルート マップ リスト内の新しいルート マップの位置を指定する番号。このコマンドの **no** 形式を使用すると、このルート マップの **configure terminal** の位置が削除されます。
ステップ 7	次のいずれかまたは両方のコマンドを入力します。 • **match length** • **match ip address** 例： `Device(config-route-map)# match ip address 1`	ポリシーベースでルーティングされるかどうかを知るためにパケットを検査する基準を定義します。
ステップ 8	**set ip next-hop** {*ip-address*[...*ip-address*] | **dynamic dhcp** | **encapsulate l3vpn***profile-name* | **peer-address** | **recursive** [**global** | **vrf***vrf-name*] *ip-address* | **verify-availability** [*ip-address sequence***track***track-object-number*]} 例： `Device(config-route-map)# set ip next-hop 172.16.6.6`	ポリシー ルーティング用のルート マップの match 節を通過したパケットの送出先を指定します。
ステップ 9	**end** 例： `Device(config-route-map)# end`	現在のルートマップ 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。

ポリシーベース ルーティングの設定例

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』
IP ルーティングのプロトコル独立型コマンド	『Cisco IOS IP Routing: Protocol-Independent 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 *12*：ポリシーベース ルーティングの機能情報

機能名	リリース	機能情報
Policy-Based Routing：ポリシーベース ルーティング	Cisco IOS XE Release 2.2	ポリシーベース ルーティング機能は、デバイスがパケットをルーティングする前に、それらのパケットをルート マップに照会するプロセスです。ルート マップは、どのパケットが次にどのデバイスにルーティングされるかを決定します。ポリシーベース ルーティングは、宛先ルーティングよりも柔軟性に富んだパケット ルーティング メカニズムを導入します。 次のコマンドが導入または変更されました。**ip policy route-map**

第 14 章

BDI 経由の PPPoE

BDI 経由の PPPoE 機能を使用すると、Cisco ブリッジ ドメイン インターフェイス（BDI）の VXLAN L2 オーバーレイ ネットワーク経由で PPPoE サブスクライバを終了できます。

- BDI 経由の PPPoE の制限，177 ページ
- 機能情報の確認，177 ページ
- BDI 経由の PPPoE に関する情報，178 ページ
- BDI 経由の PPPoE の設定方法，178 ページ
- BDI 経由の PPPoE に関するその他の参考資料，179 ページ
- BDI 経由の PPPoE の機能情報，181 ページ

BDI 経由の PPPoE の制限

- サービス ポリシーのキューイング機能は BDI インターフェイスではサポートされていません。
- 仮想テンプレートで設定されているキューイング機能による QoS ポリシーがある場合、そのポリシーはセッションに適用されません。

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。

BDI 経由の PPPoE に関する情報

PPPoE

PPPoE は、デジタル加入者線（DSL）の導入時に一般的に使用されるアプリケーションです。PPPoE は、クライアントとサーバでの PPPoE をサポートします。

ブリッジ ドメイン インターフェイス

ブリッジ ドメイン インターフェイス（BDI）は、レイヤ 2 ブリッジ型ネットワークとレイヤ 3 のルーテッドネットワーク トラフィック間のトラフィックの双方向フローを許可する論理インターフェイスです。ブリッジ ドメイン インターフェイスは、ブリッジ ドメインと同じインデックスによって識別されます。各ブリッジ ドメインは、レイヤ 2 ブロードキャスト ドメインを表します。ブリッジ ドメインに関連付けることができるブリッジ ドメイン インターフェイスは、1 つだけです。

ブリッジ ドメイン インターフェイスは以下の機能をサポートしています。

- IP 終了
- レイヤ 3 VPN の終了
- アドレス解決プロトコル（ARP）、G-ARP および P-ARP の処理
- MAC アドレスの割り当て

BDI 経由の PPPoE

PPPoE サブスクライバからの PPPoE セッション要求は、VXLAN トンネル経由で CSR1000v で終了されます。エッジ ルータと CSR1000v の間の VXLAN トンネルでは、PPPoE パケット レイヤのレイヤ 2 接続ができます。

BDI 経由の PPPoE の設定方法

BDI 経由の PPPoE の有効化

```
configure terminal
interface BDI10
```

```
 no ip address
 vlan-id dot1q 10
  pppoe enable group global
exit
```

BDI 経由の PPPoE の無効化

```
configure terminal
interface BDI10
 no ip address
 vlan-id dot1q 10
  no pppoe enable group global
exit
```

BDI 経由の PPPoE の設定例

BDI 経由の PPPoE の設定

```
configure terminal
aaa new-model
aaa authentication ppp default local
username c password 0 c
!
bba-group pppoe global1
virtual-template 1
!
interface virtual-template 1
ppp ipcp address required
ip unnumbered loopback0
peer default ip address pool pool1
ppp authentication pap chap
ppp timeout retry 3
ppp timeout ncp 60
!
interface BDI10
vlan-id dot1q 10
pppoe enable group global1
!
exit
```

BDI 経由の PPPoE に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco CSR 1000V VxLAN サポート	Cisco CSR 1000V VxLAN サポート
『Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide』	『Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide』

関連項目	マニュアル タイトル
IP Routing: Protocol-Independent Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 900 Series)	IP Routing: Protocol-Independent Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 900 Series)
IP Routing: Protocol-Independent Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 920 Series)	IP Routing: Protocol-Independent Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 920 Series)

MIB

MIB	MIB のリンク
• CISCO-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

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

BDI 経由の PPPoE 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*：*BDI* 経由の *PPPoE* の機能情報

機能名	リリース	機能情報
BDI 経由の PPPoE	Cisco IOS XE Denali 16.3.1。	BDI 経由の PPPoE 機能を使用すると、Cisco ブリッジ ドメイン インターフェイス（BDI）の VXLAN L2 オーバーレイ ネットワーク経由で PPPoE サブスクライバを終了できます。 次のコマンドが変更されました。pppoe enable group

第 15 章

SGT ベースの PBR

SGT ベースの PBR 機能では、セキュリティ グループに基づいてパケットを分類し、ポリシーベースルーティング（PBR）で定義されたポリシーに一致する役割にトラフィックをグループ化することができます。

- 機能情報の確認，183 ページ
- SGT ベースの PBR の制限，184 ページ
- SGT ベースの PBR に関する情報，184 ページ
- SGT ベースの PBR の設定方法，185 ページ
- SGT ベースの PBR の設定例，188 ページ
- SGT ベースの PBR に関するその他の参考資料，189 ページ
- SGT ベースの PBR の機能情報，189 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。

SGT ベースの PBR の制限

- SGT ベースの PBR 機能は、番号ベースのタギングを使用したポリシー設定をサポートしていますが、名前ベースのタギングはサポートしていません。
- IOS XE の IPv6 トラフィックについては、SGT ベースの PBR 機能はサポートされていません。
- ダイナミック ルートマップとスタティック ルートマップの両方が同じインターフェイスに関連付けられている場合、ダイナミック ルートマップが優先適用されます。優先適用中は警告メッセージが出力されます。スタティック ルートマップは、ダイナミック ルート マップが削除されると有効になります。
- ルートマップの関連付けを解除する前に、削除しておくことをおすすめします。ルートマップとインターフェイスの関連付けを解除する前にルートマップを削除すると、静的 PBR を設定できなくなります。

SGT ベースの PBR に関する情報

Cisco TrustSec

Cisco TrustSec は、入力側でユーザまたはデバイスのトラフィックにセキュリティ グループ タグ（SGT）を割り当て、その割り当てられたタグに基づいてアクセス ポリシーを適用します。SGT ベースの PBR 機能を使用すると、セキュリティ グループ分類に基づいて PBR を設定できます。これにより、ユーザやデバイスを所定のポリシーに該当する役割にグループ化することができます。

SGT ベースの PBR

セキュリティ グループの分類には、送信先グループや宛先グループが含まれます。これは送信元の SGT と DGT で指定します。SGT ベースの PBR 機能では、SGT/DGT ベースのパケット分類のために PBR ルートマップの match 句を使用できます。SGT ベースの PBR 機能では設定できるタグの数に制限はありませんが、プラットフォームで使用できるメモリに基づいてタグを設定することをお勧めします。SGT ベースの PBR では、VPN ルーティングおよび転送（VRF）選択一致基準を使用できます。これを使用すると、バーチャル プライベート ネットワーク（VPN）トラフィックのポリシーベースの分類と転送ができます。

SGT ベースの PBR の設定方法

一致セキュリティ グループ タグの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **route-map***map-tag*
4. **match security-group source tag***sgt-number*
5. **set ip next-hop***ip-address*
6. **match security-group destination tag***sgt-number*
7. **set ip next-hop***ip-address*
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	**route-map***map-tag* 例： `Device(config)# route-map policy_security`	ルート マップを指定し、ルート マップ コンフィギュレーション モードを開始します。
ステップ 4	**match security-group source tag***sgt-number* 例： `Device(config-route-map)# match security-group source tag 100`	security-group source security tag の値を設定します。
ステップ 5	**set ip next-hop***ip-address* 例： `Device(config-route-map)# set ip next-hop 71.71.71.6`	パケットをルーティングするためのネクスト ホップを指定します。

	コマンドまたはアクション	目的
ステップ 6	**match security-group destination tag***sgt-number* 例： `Device(config-route-map)# match security-group destination tag 150`	security-group destination security tag の値を設定します。
ステップ 7	**set ip next-hop***ip-address* 例： `Device(config-route-map)# set ip next-hop 72.72.72.6`	パケットをルーティングするためのネクスト ホップを指定します。
ステップ 8	**end** 例： `Device(config-route-map)# end`	現在のルートマップ 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。

インターフェイスへのルートマップの割り当て

手順の概要

1. イネーブル化
2. **configure terminal**
3. **interface***typeslot*/*subslot*/*port*[. *subinterface-number*]
4. **ip policy 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	**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***typeslot*/*subslot*/*port*[. *subinterface-number*] 例： `Device(config)#interface gigabitEthernet0/0/0`	インターフェイス情報を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip policy route-map***map-tag* 例： `Device(config-if)#ip policy route-map policy_security`	前のタスクで設定されたルート マップをインターフェイスに割り当てます。

SGT ベースの PBR の設定の表示と確認

手順の概要

1. イネーブル化
2. **show ip policy**
3. **show route-map***map-tag*
4. **show route-map dynamic**

手順の詳細

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 policy**

例：
```
Device# show ip policy

Interface       Route map
Gi0/0/1.77      test
```
IP ポリシー情報を表示します。

ステップ 3 **show route-map***map-tag*

例：

```
Device# show route-map test

route-map test, permit, sequence 10
  Match clauses:
    security-group source tag 100 111
  Set clauses:
    ip next-hop 71.71.71.6
  Policy routing matches: 0 packets, 0 bytes
route-map test, permit, sequence 20
  Match clauses:
    security-group destination tag 200 222
  Set clauses:
    ip next-hop 72.72.72.6
  Policy routing matches: 0 packets, 0 bytes
```

ルートマップ設定を表示します。

ステップ 4 **show route-map dynamic**

例：

```
Device# show route-map dynamic

route-map AAA-02/11/15-12:32:52.955-1-test, permit, sequence 0, identifier 2818572289
Match clauses:
    Security-group source tag 100 300
Set clauses:
 ip next-hop 3.3.3.2
Nexthop tracking current: 3.3.3.2
3.3.3.2, fib_nh:7FDE41661370,oce:7FDE4C540AD0,status:1

 Policy routing matches: 1012 packets, 83458 bytes
Current active dynamic routemaps = 1
```

動的 PBR ルートマップに関する情報を表示します。

SGT ベースの PBR の設定例

例：SGT ベースの PBR

次に、SGT ベースの PBR を設定する例を示します。

例：SGT ベースの PBR

```
enable
 configure terminal
 route-map policy_security
 match security-group source tag 100
 match security-group source tag 111
 set ip next-hop 71.71.71.6
 match security-group destination tag 200
 match security-group destination tag 222
 set ip next-hop 72.72.72.6
 end
 interface gigabitEthernet0/0/0
 ip policy route-map policy_security
```

SGT ベースの PBR に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
Cisco IOS IP Routing Protocol Independent commands	『Cisco IOS IP Routing Protocol-Independent Command Reference』
Cisco TrustSec Overview	『Understanding Cisco TrustSec』

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

SGT ベースの PBR 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*：*SGT* ベースの *PBR* の機能情報

機能名	リリース	機能情報
SGT ベースの PBR		この機能は、**Cisco 4000** シリーズ **ISR** でのみサポートされます。
SGT ベースの PBR	Cisco IOS XE リリース 3.16S	SGT ベースの PBR 機能では、セキュリティ グループ タグ（SGT）に基づいてパケットを分類し、PBR で定義されたポリシーに一致する役割にトラフィックをグループ化することができます。 次のコマンドが導入または変更されました。**interface**、**ip policy route-map**、**match security-group destination tag**、**match security-group source tag**、**route-map**、**show ip policy**、**show route-map**、**show route-map dynamic**、**show platform hardware qfp active classification class-group-manager class-group client pbr**、**show platform hardware qfp active classification feature-manager class-group tcam pbr global details**、**match security-group source tag**、**show platform hardware qfp active feature pbr class-group**、**show platform software pbr fp interface all**、**show platform software pbr rp ac statistics**、**show platform software route-map fp active map**、**show platform software route-map rp active map**

第 16 章

SGT ベースの QoS

SGT ベースの QoS 機能を使用すると、ユーザ グループのパケット分類に使用するセキュリティ グループや、役割ベースまたはデバイス ベースの QoS トラフィック ルーティングを適用することができます。

- 機能情報の確認，191 ページ
- SGT ベースの QoS の前提条件，192 ページ
- SGT ベースの QoS の制限，192 ページ
- SGT ベースの QoS に関する情報，192 ページ
- SGT ベースの QoS の設定方法，193 ページ
- SGT ベースの QoS の設定例，196 ページ
- SGT ベースの QoS に関するその他の参考資料，197 ページ
- SGT ベースの QoS の機能情報，197 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。

SGT ベースの QoS の前提条件

- SGT ベースの QoS の構成で使用されるユーザ グループとデバイスは、所定の SGT グループに割り当てる必要があります。SGT の定義とマッピングは、Cisco ISE、またはネットワークデバイス上の静的 SGT 分類により行うことができます。

SGT ベースの QoS の制限

- SGT ベースの QoS 機能では、ユーザ グループ内のアプリケーションの優先度設定はサポートされていません。
- SGT ベースの QoS 機能では、ポリシー内で一致アプリケーションまたは一致プロトコル基準を一致 SGT 基準と組み合わせて使用することはできません。

SGT ベースの QoS に関する情報

SGT ベースの QoS

セキュリティ グループの分類には、送信先グループや宛先グループが含まれます。これは送信元の SGT と DGT で指定します。SGT ベースの QoS 設定では、定義されたユーザ グループやデバイスに対する帯域や QoS ポリシーの割り当ての優先度設定ができます。SGT ベースの QoS 機能では、複数の QoS ポリシーを、複数のユーザ グループによって開始されたアプリケーションやトラフィックに割り当てることができます。各ユーザ グループは一意の SGT 値によって定義され、階層型および非階層型 QoS 構成をサポートしています。SGT ベースの QoS 機能は、SGT/DGT ベースのパケット分類に使用するユーザ グループおよびデバイス ベースの QoS サービス レベルをサポートしています。SGT ベースの QoS 機能では、QoS ポリシーの優先度設定に使用するコンテキスト情報に基づいてユーザ グループを設定できます。

SGT ベースの QoS の設定方法

ユーザグループ、デバイス、または役割ベースの QoS ポリシーの設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **class-map***class-map-name*
4. **match security-group source tag***sgt-number*
5. **match security-group destination tag***dgt-number*
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	**class-map***class-map-name* 例： `Device(config)# class-map c1`	クラス マップを指定し、クラス マップ コンフィギュレーション モードを開始します。
ステップ 4	**match security-group source tag***sgt-number* 例： `Device(config-cmap)# match security-group source tag 1000`	security-group source security tag の値を設定します。
ステップ 5	**match security-group destination tag***dgt-number* 例： `Device(config-cmap)# match security-group destination tag 2000`	security-group destination security tag の値を設定します。
ステップ 6	**end** 例： `Device(config-cmap)# end`	現在のルート マップ 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。

ポリシーマップの設定とインターフェイスへの割り当て

手順の概要

1. イネーブル化
2. **configure terminal**
3. **policy-map***policy-map-name*
4. **class***class-map-name*
5. **bandwidth percent***number*
6. **set dscp***codepoint value*
7. **end**
8. **interface***type slot*/*subslot*/*port* [. *subinterface-number*]
9. **service-policy** {**input** | **output**} *policy-map-name*
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	**policy-map***policy-map-name* 例： `Device(config)# policy-map p1`	ポリシー マップを指定し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 4	**class***class-map-name* 例： `Device(config-pmap)# class c1`	クラスを指定し、クラスコンフィギュレーションモードを開始します。
ステップ 5	**bandwidth percent***number* 例： `Device(config-pmap-c)# bandwidth percent 20`	bandwidth percent の値を設定します。

	コマンドまたはアクション	目的
ステップ 6	**set dscp***codepoint value* 例： `Device(config-pmap-c)# set dscp ef`	DiffServ コードポイント（DSCP）の値を設定します。
ステップ 7	**end** 例： `Device(config-pmap-c)# end`	ポリシーマップクラスアクションコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 8	**interface***type slot*/*subslot*/*port* [. *subinterface-number*] 例： `Device(config)#interface gigabitEthernet0/0/0.1`	インターフェイス情報を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	**service-policy** {**input** | **output**} *policy-map-name* 例： `Device(config-if)# service-policy input p1`	インターフェイスの入力にポリシー マップを割り当てます。
ステップ 10	**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。

SGT ベースの QoS の設定の表示と確認

手順の概要

1. イネーブル化
2. **show class-map**
3. **debug cpl provisioning**{**api** | **db** | **errors** | **ttc**}

手順の詳細

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 class-map**

例：
```
Device# show class-map

 Class Map match-any class-default (id 0)
   Match any

 Class Map match-all c1 (id 1)
   Match security-group source tag 1000
   Match security-group destination tag 2000
```
クラス マップ情報を表示します。

ステップ 3 **debug cpl provisioning{api | db | errors | ttc}**

例：
```
Device# debug cpl provisioning api

CPL Policy Provisioning Manager API calls debugging is on
```
呼処理言語（CPL）のプロビジョニングのデバッグを有効にします。

SGT ベースの QoS の設定例

例：ユーザグループ、デバイス、または役割ベースの QoS ポリシーの設定

次に、ユーザ グループ、デバイス、またはロール ベースの QoS ポリシーを設定する例を示します。

```
enable
 configure terminal
 class-map c4
  match security-group source tag 7000
  match security-group destination tag 8000
  end
 policy-map p5
  class c4
   bandwidth percent 50
   set dscp ef
   end
 interface gigabitEthernet0/0/0.1
  service-policy input p5
```

SGT ベースの QoS に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Cisco IOS IP Routing Protocol Independent commands	『Cisco IOS IP Routing Protocol-Independent Command Reference』
Cisco TrustSec Overview	『Understanding Cisco TrustSec』

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

SGT ベースの QoS 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*：*SGT* ベースの *QoS* の機能情報

機能名	リリース	機能情報
SGT ベースの QoS	Cisco IOS XE リリース 3.17S	SGT ベースの QoS 機能では、セキュリティ グループ タグ（SGT）に基づいてパケットを分類し、定義済みの QoS ポリシーに一致するようにユーザグループとデバイスにトラフィックをグループ化することができます。 次のコマンドが導入または変更されました。**debug cpl provisioning**, **class-map match security-group destination tag**, **match security-group source tag**, **show class-map**.

第 17 章

ポリシーベース ルーティングのデフォルト ネクストホップ ルート

ポリシーベース ルーティングのデフォルト ネクストホップ ルート機能により、**set ip default next-hop** コマンドの結果として転送されるパケットをハードウェア レベルでスイッチする機能が導入されます。以前のソフトウェア リリースでは、ポリシーベース ルーティング用にルートマップから生成された転送されるパケットは、ソフトウェア レベルで交換されます。

- 機能情報の確認，199 ページ
- ポリシーベース ルーティングのデフォルト ネクストホップ ルートに関する情報，200 ページ
- ポリシーベース ルーティングのデフォルト ネクストホップ ルートの設定方法，202 ページ
- ポリシーベース ルーティングのデフォルト ネクストホップ ルートの設定例，204 ページ
- その他の参考資料，204 ページ
- ポリシーベース ルーティングのデフォルト ネクストホップ ルートの機能情報，205 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。

ポリシーベースルーティングのデフォルトネクストホップ ルートに関する情報

Policy-Based Routing：ポリシーベース ルーティング

ポリシーベース ルーティングは、デバイスが、パケットをルーティングする前に、それらのパケットをルートマップに照合するプロセスです。ルートマップは、どのパケットが次にどのデバイスにルーティングされるかを決定します。特定のパケットを明らかに最短のパス以外の方法でルーティングする必要がある場合は、ポリシーベース ルーティングを有効にします。ポリシーベース ルーティングを使用すると、同等アクセス、プロトコル依存ルーティング、発信元依存ルーティング、双方向対バッチ トラフィックに基づくルーティング、および専用リンクに基づくルーティングを実現できます。ポリシーベース ルーティングは、宛先ルーティングよりも柔軟性に富んだパケット ルーティング メカニズムです。

ポリシーベースルーティングをイネーブルにするには、ポリシーベースルーティングに使用するルート マップを特定し、ルート マップを作成する必要があります。ルート マップ自体は、一致基準とそのすべての match 句が適合した場合の処理を指定します。

インターフェイスでポリシーベースルーティングを有効にするには、インターフェイスコンフィギュレーション モードで **ip policy route-map***map-tag* コマンドを使用することにより、デバイスがどのルートマップを使用する必要があるかを指定します。宛先IPアドレスがデバイスのインターフェイスの IP アドレスと同じ場合を除き、指定したインターフェイスに着信するパケットはポリシーベース ルーティングの対象になります。この **ip policy route-map** コマンドは、このインターフェイスに着信するすべてのパケットの高速スイッチングを無効にします。

ポリシーベース ルーティングに使用するルート マップを定義するには、**route-map***map-tag* [**permit** | **deny**] [*sequence-number*] グローバル コンフィギュレーション コマンドを使用します。

パケットがポリシーベースでルーティングされるかどうかを知るためにパケットを調べるための基準を定義するには、**match length***minimum-length maximum-length* コマンドまたは **match ip address** {*access-list-number* | *access-list-name*} [*access-list-number* | *access-list-name*] コマンド、またはその両方をルート マップ コンフィギュレーション モードで使用します。ルート マップに match 句がない場合は、すべてのパケットを指します。

ポリシー ルート キャッシュのキャッシュ エントリを表示するには、**show ip cache policy** コマンドを使用します。

（注） ポリシーベース ルーティング（PBR）が CEF や Resource Reservation Protocol（RSVP）との相互作用を行わない場合、PBR との間の誤ったインターフェイスが Mediatrace に表示されます。そのため、PBR が CEF または RSVP との間で直接相互作用するように設定し、Mediatrace が物理インターフェイスではなくトンネル インターフェイスの統計情報のみを収集するようにします。

IP ヘッダーでの優先順位の設定

IPヘッダーで優先順位を設定することにより、トラフィックが多い間、そのパケットを他のパケットよりも高い優先順位または低い優先順位で処理するかどうかが決定されます。デフォルトでは、シスコ ソフトウェアはこの値を操作しません。ヘッダーは元々の優先値のままです。

ポリシーベースルーティングがイネーブルの場合、IPヘッダーの優先ビットをデバイスで設定できます。キューイング機能がイネーブルの場合、このようなヘッダーを含むパケットは、別のデバイスに到達すると優先設定に従って送信順に並べられます。キューイング機能がイネーブルでない場合、デバイスは優先ビットに従いません。パケットは FIFO の順序で送信されます。

番号または名前（名前は RFC 791 に基づいています）を使用して、優先順位の設定を変更できます。**set ip precedence** ルート マップ コンフィギュレーション コマンドで値を使用して優先順位を決定するその他の機能をイネーブルにできます。次の表は、使用可能な番号と対応する名前を、最下位から最上位の優先順位の順に一覧表示します。

表 ***16*** : ***IP precedence*** 値

番号	名前
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

set コマンドは、相互に使用できます。前出の表に示された順序で評価されます。使用可能なネクスト ホップはインターフェイスで暗黙指定されます。ローカル デバイスがネクスト ホップを発見して、それが使用可能なインターフェイスの場合は、そのスイッチがパケットをルーティングします。

ポリシーベースルーティングのデフォルトネクストホップ ルートの設定方法

ポリシーベース ルーティングのデフォルト ネクストホップ ルートの優先順位の設定

パケットの優先順位を設定し、一致基準を満たすパケットの出力先を指定するには、この作業を実行します。

（注） **set ip next-hop** コマンドと **set ip default next-hop** コマンドは似ていますが、動作順序が異なります。**set ip next-hop** コマンドを設定すると、最初にポリシー ルーティングを使用してからルーティング テーブルを使用します。**set ip default next-hop** コマンドを設定すると、最初にルーティング テーブルを使用してからポリシー ルーティングで指定されたネクスト ホップが使用されます。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **route-map***route-map-name* [**permit** | **deny**] [*sequence-number*]]
4. **set ip precedence** {*number* | *name*}
5. **set ip next-hop***ip-address* [*ip-address*]
6. **set interface***typenumber* [*...typenumber*]
7. **set ip default next-hop***ip-address* [*ip-address*]
8. **set default interface***typenumber* [*...typenumber*]
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）。

	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***route-map-name* [**permit** | **deny**] [*sequence-number*]] 例： `Device(config)# route-map rm1`	再配布を制御するためのルート マップを定義し、ルート マップ コンフィギュレーション モードに入ります。
ステップ 4	**set ip precedence** {*number* | *name*} 例： `Device(config-route-map)# set ip precedence 5`	IP ヘッダーに優先順位を設定します。 （注） 優先順位の番号または名前を指定できます。
ステップ 5	**set ip next-hop***ip-address* [*ip-address*] 例： `Device(config-route-map)# set ip next-hop 192.0.2.1`	パケットをルーティングするためのネクスト ホップを指定します。 （注） ネクスト ホップは隣接するデバイスである必要があります。
ステップ 6	**set interface***typenumber* [*...typenumber*] 例： `Device(config-route-map)# set interface gigabitethernet 0/0/0`	パケットの出力インターフェイスを指定します。
ステップ 7	**set ip default next-hop***ip-address* [*ip-address*] 例： `Device(config-route-map)# set ip default next-hop 172.16.6.6`	この宛先に対する明示ルートが存在しない場合は、パケットをルーティングするためのネクスト ホップを指定します。 （注） **set ip next-hop** コマンドと同様に、**set ip default next-hop** コマンドでは、隣接するデバイスを指定する必要があります。
ステップ 8	**set default interface***typenumber* [*...typenumber*] 例： `Device(config-route-map)# set default interface serial 0/0/0`	宛先の明示ルートがない場合、パケットの出力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	**end** 例： `Device(config-route-map)# end`	現在のルートマップ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。

ポリシーベースルーティングのデフォルトネクストホップ ルートの設定例

例：ポリシーベース ルーティング

次に、2つの送信元が、異なるサービスプロバイダーに対して同等アクセスを持つ例を示します。パケットの宛先についての明示的なルートがデバイスにない場合、発信元 10.1.1.1 から非同期インターフェイス 1/0/0 に届くパケットは、172.16.6.6 のデバイスに送られます。パケットの宛先についての明示的なルートがデバイスにない場合、発信元172.17.2.2から届くパケットは、192.168.7.7 のデバイスに送られます。デバイスに宛先に関する明示ルートが設定されていないその他のパケットはすべて廃棄されます。

```
Device(config)# access-list 1 permit ip 10.1.1.1
Device(config)# access-list 2 permit ip 172.17.2.2
Device(config)# interface async 1/0/0
Device(config-if)# ip policy route-map equal-access
Device(config-if)# exit
Device(config)# route-map equal-access permit 10
Device(config-route-map)# match ip address 1
Device(config-route-map)# set ip default next-hop 172.16.6.6
Device(config-route-map)# exit
Device(config)# route-map equal-access permit 20
Device(config-route-map)# match ip address 2
Device(config-route-map)# set ip default next-hop 192.168.7.7
Device(config-route-map)# exit
Device(config)# route-map equal-access permit 30
Device(config-route-map)# set default interface null 0
Device(config-route-map)# 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 IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
IP ルーティングのプロトコル独立型コマンド	『Cisco IOS IP Routing: Protocol-Independent 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のデフォルトネクストホップ ルートの機能情報

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 *17*：ポリシーベース ルーティングのデフォルト ネクストホップ ルートの機能情報

機能名	リリース	機能情報
ポリシーベース ルーティングのデフォルト ネクストホップ ルート	12.1(11)E Cisco IOS XE Release 2.2	ポリシーベース ルーティングのデフォルト ネクストホップ ルート機能により、**set ip default next-hop** コマンドの結果として転送されるパケットをハードウェア レベルでスイッチする機能が導入されます。以前のリリースでは、ポリシーベース ルーティング用にルート マップから生成された転送されるパケットは、ソフトウェア レベルに交換されていました。 次のコマンドが導入または変更されました。**set ip default next-hop**

第 18 章

VRF 用 PBR ネクストホップ可用性確認

VRF 用 PBR ネクストホップ可用性確認機能では、Virtual Routing and Forwarding（VRF）インスタンスでの IPv4/IPv6 のネクストホップ可用性を確認することができます。

- 機能情報の確認，207 ページ
- VRF 用 PBR ネクストホップ可用性確認に関する情報，208 ページ
- VRF 用 PBR ネクストホップ可用性確認の設定方法，209 ページ
- VRF 用 PBR ネクストホップ可用性確認の設定例，220 ページ
- VRF 用 PBR ネクストホップ可用性確認に関するその他の参考資料，222 ページ
- VRF 用 PBR ネクストホップ可用性確認に関する機能情報，222 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。

VRF 用 PBR ネクストホップ可用性確認に関する情報

VRF 用 PBR ネクストホップ可用性確認の概要

Cisco IOS ポリシーベース ルーティング（PBR）は、パケットの一致と分類の使用を定義します。また、IP パケットの属性を変更できるアクション ポリシーを設定し、通常の宛先 IP アドレス ベースのルーティングと転送を上書きします。PBR は、グローバル インターフェイスや複数のルーティング インスタンスで適用できます。VRF 用 PBR ネクストホップ可用性確認機能では、Virtual Routing and Forwarding（VRF）インスタンスでの IPv4/IPv6 のネクストホップ可用性を確認することができます。

継承された VRF の場合、VRF インスタンスは入力インターフェイスに基づいています。VRF 間とは、パケットを VRF 間で（たとえば、VRFx から VRFy に）転送することを指します。VRFx から受信した IPv4/IPv6 パケットは VRFy に転送され、ネクスト ホップの可用性が VRFy のインスタンスで確認されます。

VRF 用 PBR ネクストホップ可用性確認の設定方法

継承された IP VRF 用 PBR ネクストホップ可用性確認の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *vpn-route-distinguisher*
5. **route-target export** *route-target-ext-community*
6. **route-target import** *route-target-ext-community*
7. **exit**
8. **ip sla** *operation-number*
9. **icmp-echo** *destination-ip-address*
10. **vrf** *vrf-name*
11. **exit**
12. **ip sla schedule** *operation-number* **life forever start-time now**
13. **track** *object-number* **ip sla** *operation-number*
14. **interface** *type number*
15. **ip vrf forwarding** *vrf-name*
16. **ip address** *ip-address subnet-mask*
17. **exit**
18. **route-map** *map-tag* **permit** *sequence-number*
19. **set ip vrf** *vrf-name* **next-hop verify-availability** *next-hop-address sequence* **track** *object*
20. **exit**
21. **interface** *type number*
22. **ip vrf forwarding** *vrf-name*
23. **ip policy route-map** *map-tag*
24. **ip address** *ip-address subnet-mask*
25. **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 vrf** *vrf-name* 例： `Device(config)# ip vrf RED`	IP VPN ルーティングおよび転送インスタンスを設定し、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 4	**rd** *vpn-route-distinguisher* 例： `Device(config-vrf)# rd 100:1`	ルート識別子を指定します。ルート識別子は自律システム（AS）番号または IP アドレスです。
ステップ 5	**route-target export** *route-target-ext-community* 例： `Device(config-vrf)# route-target export 100:1`	VRF のルート ターゲット拡張コミュニティを作成し、ターゲット VPN 拡張コミュニティからのルーティング情報をエクスポートします。*route-target-ext-community* 引数は AS 番号または IP アドレスです。
ステップ 6	**route-target import** *route-target-ext-community* 例： `Device(config-vrf)# route-target import 100:1`	VRF のルート ターゲット拡張コミュニティを作成し、ターゲット VPN 拡張コミュニティからのルーティング情報をインポートします。*route-target-ext-community* 引数は AS 番号または IP アドレスです。
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、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	**ip sla** *operation-number* 例： `Device(config)# ip sla 1`	Cisco IOS IP サービス レベル契約（SLA）動作を設定し、IP SLA コンフィギュレーション モードに移行します。
ステップ 9	**icmp-echo** *destination-ip-address* 例： `Device(config-ip-sla)# icmp-echo 10.0.0.4`	IP SLA Internet Control Message Protocol（ICMP）エコー動作を設定し、ICMP エコー コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 10	**vrf** *vrf-name* 例： `Device(config-ip-sla-echo)# vrf RED`	VRF インスタンスの IP SLA を設定します。
ステップ 11	**exit** 例： `Device(config-ip-sla-echo)# exit`	ICMP エコー コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**ip sla schedule** *operation-number* **life forever start-time now** 例： `Device(config)# ip sla schedule 1 life forever start-time now`	単一の Cisco IOS IP SLA 動作のスケジューリング パラメータを設定します。
ステップ 13	**track** *object-number* **ip sla** *operation-number* 例： `Device(config)# track 1 ip sla 1`	Cisco IOS IP SLA 動作の状態を追跡し、トラッキング コンフィギュレーション モードを開始します。
ステップ 14	**interface** *type number* 例： `Device(config-track)# interface Ethernet1/0`	インターフェイスのタイプと番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 15	**ip vrf forwarding** *vrf-name* 例： `Device(config-if)# ip vrf forwarding RED`	フォワーディング テーブルを設定します。
ステップ 16	**ip address** *ip-address subnet-mask* 例： `Device(config-if)# ip address 10.0.0.2 255.0.0.0`	インターフェイスの IP アドレスおよびサブネット マスクを指定します。
ステップ 17	**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 モードに戻ります。
ステップ 18	**route-map** *map-tag* **permit** *sequence-number* 例： `Device(config)# route-map test02 permit 10`	既存のルートマップ エントリに対して挿入または削除するシーケンスを指定し、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 19	**set ip vrf** *vrf-name* **next-hop verify-availability** *next-hop-address sequence* **track** *object* 例： `Device(config-route-map)# set ip vrf RED next-hop verify-availability 192.168.23.2 1 track 1`	ルータがルートマップのネクスト ホップへのポリシー ルーティングを実行する前にそのネクストホップの到達可能性を確認するポリシー ルーティングを設定します。
ステップ 20	**exit** 例： `Device(config-route-map)# exit`	ルート マップ 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。
ステップ 21	**interface** *type number* 例： `Device(config)# interface Ethernet0/0`	インターフェイスのタイプと番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 22	**ip vrf forwarding** *vrf-name* 例： `Device(config-if)# ip vrf forwarding RED`	フォワーディング テーブルを設定します。
ステップ 23	**ip policy route-map** *map-tag* 例： `Device(config-if)# ip policy route-map test02`	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。
ステップ 24	**ip address** *ip-address subnet-mask* 例： `Device(config-if)# ip address 192.168.10.2 255.255.255.0`	インターフェイスの IP アドレスおよびサブネット マスクを指定します。
ステップ 25	**end** 例： `Device(config-if)# exit`	特権 EXEC モードに戻ります。

継承された IPv6 VRF 用 PBR ネクストホップ可用性確認の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *vpn-route-distinguisher*
5. **route-target export** *route-target-ext-community*
6. **route-target import** *route-target-ext-community*
7. **exit**
8. **ip sla** *operation-number*
9. **icmp-echo** *destination-ip-address*
10. **vrf** *vrf-name*
11. **exit**
12. **ip sla schedule** *operation-number* **life forever start-time now**
13. **track** *object-number* **ip sla** *operation-number*
14. **interface** *type number*
15. **ip vrf forwarding** *vrf-name*
16. **ip address** *ip-address subnet-mask*
17. **ipv6 address** *ipv6-prefix*
18. **exit**
19. **route-map** *map-tag* **permit** *sequence-number*
20. **set ipv6 vrf** *vrf-name* **next-hop verify-availability** *next-hop-address sequence* **track** *object*
21. **exit**
22. **interface** *type number*
23. **ip vrf forwarding** *vrf-name*
24. **ipv6 policy route-map** *map-tag*
25. **ip address** *ip-address subnet-mask*
26. **ipv6 address** *ipv6-prefix*
27. **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	**ip vrf** *vrf-name* 例： `Device(config)# ip vrf RED`	IP VPN ルーティングおよび転送インスタンスを設定し、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 4	**rd** *vpn-route-distinguisher* 例： `Device(config-vrf)# rd 100:1`	ルート識別子を指定します。ルート識別子は自律システム（AS）番号または IP アドレスです。
ステップ 5	**route-target export** *route-target-ext-community* 例： `Device(config-vrf)# route-target export 100:1`	VRF のルート ターゲット拡張コミュニティを作成し、ターゲット VPN 拡張コミュニティからのルーティング情報をエクスポートします。*route-target-ext-community* 引数は AS 番号または IP アドレスです。
ステップ 6	**route-target import** *route-target-ext-community* 例： `Device(config-vrf)# route-target import 100:1`	VRF のルート ターゲット拡張コミュニティを作成し、ターゲット VPN 拡張コミュニティからのルーティング情報をインポートします。*route-target-ext-community* 引数は AS 番号または IP アドレスです。
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、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	**ip sla** *operation-number* 例： `Device(config)# ip sla 1`	Cisco IOS IP サービス レベル契約（SLA）動作を設定し、IP SLA コンフィギュレーション モードに移行します。
ステップ 9	**icmp-echo** *destination-ip-address* 例： `Device(config-ip-sla)# icmp-echo 10.0.0.4`	IP SLA Internet Control Message Protocol（ICMP）エコー動作を設定し、ICMP エコー コンフィギュレーション モードを開始します。
ステップ 10	**vrf** *vrf-name* 例： `Device(config-ip-sla-echo)# vrf RED`	VRF インスタンスの IP SLA 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	**exit** 例： `Device(config-ip-sla-echo)# exit`	ICMPエコー コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**ip sla schedule** *operation-number* **life forever start-time now** 例： `Device(config)# ip sla schedule 1 life forever start-time now`	単一の Cisco IOS IP SLA 動作のスケジューリング パラメータを設定します。
ステップ 13	**track** *object-number* **ip sla** *operation-number* 例： `Device(config)# track 1 ip sla 1`	Cisco IOS IP SLA 動作の状態を追跡し、トラッキング コンフィギュレーション モードを開始します。
ステップ 14	**interface** *type number* 例： `Device(config-track)# interface Ethernet1/0`	インターフェイスのタイプと番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 15	**ip vrf forwarding** *vrf-name* 例： `Device(config-if)# ip vrf forwarding RED`	フォワーディング テーブルを設定します。
ステップ 16	**ip address** *ip-address subnet-mask* 例： `Device(config-if)# ip address 10.0.0.2 255.0.0.0`	インターフェイスの IP アドレスおよびサブネット マスクを指定します。
ステップ 17	**ipv6 address** *ipv6-prefix* 例： `Device(config-if)# ipv6 address 2001:DB8::/48`	IPv6 プレフィックスを指定します。
ステップ 18	**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 モードに戻ります。
ステップ 19	**route-map** *map-tag* **permit** *sequence-number* 例： `Device(config)# route-map test02 permit 10`	既存のルートマップ エントリに対して挿入または削除するシーケンスを指定し、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 20	**set ipv6 vrf** *vrf-name* **next-hop verify-availability** *next-hop-address sequence* **track** *object* 例： `Device(config-route-map)# set ipv6 vrf RED next-hop verify-availability 2001:DB8:1::1 1 track 1`	ルータがルートマップのネクスト ホップへのポリシー ルーティングを実行する前にそのネクスト ホップの到達可能性を確認するポリシー ルーティングを設定します。
ステップ 21	**exit** 例： `Device(config-route-map)# exit`	ルート マップ 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。
ステップ 22	**interface** *type number* 例： `Device(config)# interface Ethernet0/0`	インターフェイスのタイプと番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 23	**ip vrf forwarding** *vrf-name* 例： `Device(config-if)# ip vrf forwarding RED`	フォワーディング テーブルを設定します。
ステップ 24	**ipv6 policy route-map** *map-tag* 例： `Device(config-if)# ipv6 policy route-map test02`	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。
ステップ 25	**ip address** *ip-address subnet-mask* 例： `Device(config-if)# ip address 192.168.10.2 255.255.255.0`	インターフェイスの IP アドレスおよびサブネット マスクを指定します。
ステップ 26	**ipv6 address** *ipv6-prefix* 例： `Device(config-if)# ipv6 address 2001:DB8::/32`	IPv6 プレフィックスを指定します。
ステップ 27	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

VRF 間用 PBR ネクストホップ可用性確認の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *vpn-route-distinguisher*
5. **route-target export** *route-target-ext-community*
6. **ip vrf** *vrf-name*
7. **no rd** *vpn-route-distinguisher*
8. **rd** *vpn-route-distinguisher*
9. **route-target export** *route-target-ext-community*
10. **interface** *type number*
11. **ip vrf forwarding** *vrf-name*
12. **ip address** *ip-address subnet-mask*
13. **ip policy route-map** *map-tag*
14. **interface** *type number*
15. **ip vrf forwarding** *vrf-name*
16. **ip address** *ip-address subnet-mask*
17. **exit**
18. **ip route vrf** *vrf-name prefix mask interface-type interface-number ip-address*
19. **ip route vrf** *vrf-name prefix mask ip-address*
20. 別のスタティック ルートを確立するには、ステップ 19 を繰り返します。
21. **route-map** *map-tag* **permit** *sequence-number*
22. **match interface** *interface-type interface-number*
23. **set ip vrf** *vrf-name* **next-hop verify-availability** *next-hop-address sequence* **track** *object*
24. **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 BLUE`	IP VPN ルーティングおよび転送インスタンスを設定し、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 4	**rd** *vpn-route-distinguisher* 例： `Device(config-vrf)# rd 800:1`	ルート識別子を指定します。ルート識別子は自律システム（AS）番号または IP アドレスです。
ステップ 5	**route-target export** *route-target-ext-community* 例： `Device(config-vrf)# route-target export 800:1`	VRF のルート ターゲット拡張コミュニティを作成し、ターゲット VPN 拡張コミュニティからのルーティング情報をエクスポートします。 *route-target-ext-community* 引数は AS 番号または IP アドレスです。
ステップ 6	**ip vrf** *vrf-name* 例： `Device(config-vrf)# ip vrf BLUE`	IP VPN ルーティングおよび転送インスタンスを設定します。
ステップ 7	**no rd** *vpn-route-distinguisher* 例： `Device(config-vrf)# no rd 800:1`	指定したルート識別子が削除されます。
ステップ 8	**rd** *vpn-route-distinguisher* 例： `Device(config-vrf)# rd 900:1`	ルート識別子を指定します。ルート識別子は AS 番号または IP アドレスです。
ステップ 9	**route-target export** *route-target-ext-community* 例： `Device(config-vrf)# route-target export 900:1`	VRF のルート ターゲット拡張コミュニティを作成し、ターゲット VPN 拡張コミュニティからのルーティング情報をエクスポートします。 *route-target-ext-community* 引数は AS 番号または IP アドレスです。
ステップ 10	**interface** *type number* 例： `Device(config-vrf)# interface Ethernet0/0`	インターフェイスのタイプと番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**ip vrf forwarding** *vrf-name* 例： `Device(config-if)# ip vrf forwarding RED`	フォワーディング テーブルを設定します。

	コマンドまたはアクション	目的
ステップ 12	**ip address** *ip-address subnet-mask* 例： `Device(config-if)# ip address 192.168.10.2 255.255.255.0`	インターフェイスの IP アドレスおよびサブネットマスクを指定します。
ステップ 13	**ip policy route-map** *map-tag* 例： `Device(config-if)# ip policy route-map test00`	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。
ステップ 14	**interface** *type number* 例： `Device(config-if)# interface Ethernet0/1`	インターフェイスのタイプおよび番号を指定します。
ステップ 15	**ip vrf forwarding** *vrf-name* 例： `Device(config-if)# ip vrf forwarding BLUE`	フォワーディング テーブルを設定します。
ステップ 16	**ip address** *ip-address subnet-mask* 例： `Device(config-if)# ip address 192.168.21.1 255.255.255.0`	インターフェイスの IP アドレスおよびサブネットマスクを指定します。
ステップ 17	**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戻ります。
ステップ 18	**ip route vrf** *vrf-name prefix mask interface-type interface-number ip-address* 例： `Device(config)# ip route vrf BLUE 192.168.10.1 255.255.255.255 Ethernet0/0 192.168.10.1`	スタティック ルートを確立します。
ステップ 19	**ip route vrf** *vrf-name prefix mask ip-address* 例： `Device(config)# ip route vrf BLUE 192.168.23.0 255.255.255.0 192.168.21.2`	スタティック ルートを確立します。
ステップ 20	別のスタティック ルートを確立するには、ステップ 19 を繰り返します。	—

	コマンドまたはアクション	目的
ステップ 21	**route-map** *map-tag* **permit** *sequence-number* 例： `Device(config)# route-map test00 permit 10`	既存のルートマップエントリに対して挿入または削除するシーケンスを指定し、ルートマップ コンフィギュレーション モードを開始します。
ステップ 22	**match interface** *interface-type interface-number* 例： `Device(config-route-map)# match interface Ethernet0/0`	指定したインターフェイスのひとつとしてネクストホップを持つすべてのルートを配布します。
ステップ 23	**set ip vrf** *vrf-name* **next-hop verify-availability** *next-hop-address sequence* **track** *object* 例： `Device(config-route-map)# set ip vrf BLUE next-hop verify-availability 192.168.23.2 1 track 1`	ルータが VRF インスタンスのルートマップのネクストホップへのポリシー ルーティングを実行する前にそのネクスト ホップの到達可能性を確認するポリシー ルーティングを設定します。
ステップ 24	**end** 例： `Device(config-route-map)# end`	特権 EXEC モードに戻ります。

VRF 用 PBR ネクストホップ可用性確認の設定例

例：継承された IP VRF 用 PBR ネクストホップ可用性確認の設定

```
Device> enable
Device# configure terminal
Device(config)# ip vrf RED
Device(config-vrf)# rd 100:1
Device(config-vrf)# route-target export 100:1
Device(config-vrf)# route-target import 100:1
Device(config-vrf)# exit
Device(config)# ip sla 1
Device(config-ip-sla)# icmp-echo 10.0.0.4
Device(config-ip-sla-echo)# vrf RED
Device(config-ip-sla-echo)# exit
Device(config)# ip sla schedule 1 life forever start-time now
Device(config)# track 1 ip sla 1
Device(config-track)# interface Ethernet0/0
Device(config-if)# ip vrf forwarding RED
Device(config-if)# ip address 10.0.0.2 255.0.0.0
Device(config-if)# exit
Device(config)# route-map test02 permit 10
Device(config-route-map)# set ip vrf RED next-hop verify-availability 192.168.23.2 1 track
 1
Device(config-route-map)# interface Ethernet0/0
```

```
Device(config-if)# ip vrf forwarding RED
Device(config-if)# ip policy route-map test02
Device(config-if)# ip address 192.168.10.2 255.255.255.0
Device(config-if)# end
```

例：継承された IPv6 VRF 用 PBR ネクストホップ可用性確認の設定

```
Device> enable
Device# configure terminal
Device(config)# ip vrf RED
Device(config-vrf)# rd 100:1
Device(config-vrf)# route-target export 100:1
Device(config-vrf)# route-target import 100:1
Device(config-vrf)# exit
Device(config)# ip sla 1
Device(config-ip-sla)# icmp-echo 10.0.0.4
Device(config-ip-sla-echo)# vrf RED
Device(config-ip-sla-echo)# exit
Device(config)# ip sla schedule 1 life forever start-time now
Device(config)# track 1 ip sla 1
Device(config-track)# interface Ethernet0/0
Device(config-if)# ip vrf forwarding RED
Device(config-if)# ip policy route-map test02
Device(config-if)# ip address 192.168.10.2 255.255.255.0
Device(config-if)# ipv6 address 2001:DB8::/32
Device(config-if)# interface Ethernet1/0
Device(config-if)# ip vrf forwarding RED
Device(config-if)# ip address 10.0.0.2 255.0.0.0
Device(config-if)# ipv6 address 2001:DB8::/48
Device(config-if)# exit
Device(config)# route-map test02 permit 10
Device(config-route-map)# set ipv6 vrf RED next-hop verify-availability 2001:DB8:1::1 1
track 1
Device(config-route-map)# end
```

例：VRF 間用 PBR ネクストホップ可用性確認の設定

```
Device> enable
Device# configure terminal
Device(config)# ip vrf BLUE
Device(config-vrf)# rd 800:1
Device(config-vrf)# route-target export 800:1
Device(config-vrf)# ip vrf BLUE
Device(config-vrf)# no rd 800:1
Device(config-vrf)# rd 900:1
Device(config-vrf)# route-target export 900:1
Device(config-vrf)# interface Ethernet0/0
Device(config-if)# ip vrf forwarding RED
Device(config-if)# ip address 192.168.10.2 255.255.255.0
Device(config-if)# ip policy route-map test00
Device(config-if)# interface Ethernet0/1
Device(config-if)# ip vrf forwarding BLUE
Device(config-if)# ip address 192.168.21.1 255.255.255.0
Device(config-if)# exit
Device(config)# ip route vrf blue 192.168.10.1 255.255.255.255 Ethernet0/0 192.168.10.1
Device(config)# ip route vrf blue 192.168.23.0 255.255.255.0 192.168.21.2
Device(config)# route-map test00 permit 10
Device(config-route-map)# match interface Ethernet0/0
Device(config-route-map)# set ip vrf blue next-hop verify-availability 192.168.23.2 1 track
 1
Device(config-route-map)# end
```

VRF 用 PBR ネクストホップ可用性確認に関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

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/support

VRF 用 PBR ネクストホップ可用性確認に関する機能情報

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。

機能名	リリース	機能情報
VRF 用 PBR ネクストホップ可用性確認	Cisco IOS XE Release 3.11S	VRF 用 PBR ネクストホップ可用性確認機能では、Virtual Routing and Forwarding（VRF）インスタンスでの IPv4/IPv6 のネクストホップ可用性を確認することができます。

第 19 章

BGP による QoS ポリシー伝搬

BGP による QoS ポリシー伝搬機能を使用すると、ボーダー ゲートウェイ プロトコル（BGP）コミュニティ リスト、BGP 自律システム パス、およびアクセス リストに基づいて IP precedence によってパケットを分類できます。パケットが分類されたら、専用アクセス レート（CAR）および重み付けランダム早期検出（WRED）など、その他の Quality of Service（QoS）機能を使用してビジネス モデルに合うようにポリシーを指定および強化できます。

- 機能情報の確認，225 ページ
- BGP による QoS ポリシー伝搬の前提条件，226 ページ
- BGP による QoS ポリシー伝搬に関する情報，226 ページ
- BGP による QoS ポリシー伝搬の設定方法，227 ページ
- BGP による QoS ポリシー伝搬の設定例，236 ページ
- その他の参考資料，238 ページ
- BGP による QoS ポリシー伝搬の機能情報，239 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。

BGP による QoS ポリシー伝搬の前提条件

- デバイスでボーダー ゲートウェイ プロトコル（BGP）およびシスコ エクスプレス フォワーディング（CEF）または分散型 CEF（dCEF）をイネーブルにします。**bgp-policy** コマンドが有効になっている ATM インターフェイスのサブインターフェイスでは、dCEF がサポートされていないため、CEF モードを使用する必要があります。dCEF では転送機能にルート スイッチ プロセッサ（RSP）ではなく Versatile Interface Processor（VIP）を使用しています。
- ポリシーを定義する。
- BGP 経由でポリシーを適用する。
- BGP コミュニティ リスト、BGP 自律システム パス、またはアクセス リストを設定し、インターフェイスでポリシーをイネーブルにする。
- ポリシーを使用するために専用アクセス レート（CAR）または重み付けランダム早期検出（WRED）をイネーブルにします。

BGP による QoS ポリシー伝搬に関する情報

BGP による QoS ポリシー伝搬の利点

BGP による QoS ポリシー伝搬機能を使用すると、BGP コミュニティ リスト、BGP 自律システム パス、およびアクセス リストに基づいて IP precedence によってパケットを分類できます。パケットが分類されたら、専用アクセス レート（CAR）および重み付けランダム早期検出（WRED）など、その他の QoS 機能を使用してビジネス モデルに合うようにポリシーを指定および強化できます。

BGP による QoS ポリシー伝搬の設定方法

コミュニティ リストに基づいた BGP による QoS ポリシー伝搬の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **route-map***route-map-name* [**permit** | **deny** [*sequence-number*]]
4. **match community** {*standard-list-number* | *expanded-list-number* | *community-list-name* [**exact**]}
5. **set ip precedence** [*number* | *name*]
6. **exit**
7. **router bgp***autonomous-system*
8. **table-map***route-map-name*
9. **exit**
10. **ip community-list***standard-list-number* {**permit** | **deny**} [*community-number*]
11. **interface***typenumber*
12. **bgp-policy** {**source** | **destination**} **ip-prec-map**
13. **exit**
14. **ip bgp-community new-format**
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。

	コマンドまたはアクション	目的
ステップ 3	**route-map***route-map-name* [**permit** | **deny** [*sequence-number*]] 例： `Device(config)# route-map rm1`	再配布を制御するためのルート マップを定義し、ルート マップ コンフィギュレーション モードに入ります。
ステップ 4	**match community** {*standard-list-number* | *expanded-list-number* | *community-list-name* [**exact**]} 例： `Device(config-route-map)# match community 1`	ボーダー ゲートウェイ プロトコル（BGP）のコミュニティ リストと照合します。
ステップ 5	**set ip precedence** [*number* | *name*] 例： `Device(config-route-map)# set ip precedence 5`	コミュニティ リストが一致するときの IP precedence フィールドを設定します。 （注） 優先順位の番号または名前を指定できます。
ステップ 6	**exit** 例： `Device(config-route-map)# exit`	ルート マップ 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。
ステップ 7	**router bgp***autonomous-system* 例： `Device(config)# router bgp 45000`	BGP プロセスをイネーブルにし、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 8	**table-map***route-map-name* 例： `Device(config-router)# table-map rm1`	BGP で学習したルートで IP ルーティング テーブルが更新される場合の、メトリックとタグの値を修正します。
ステップ 9	**exit** 例： `Device(config-router)# exit`	ルータ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 10	**ip community-list***standard-list-number* {**permit** | **deny**} [*community-number*] 例： `Device(config)# ip community-list 1 permit 2`	BGP のコミュニティ リストを作成し、アクセスを制御します。
ステップ 11	**interface***typenumber* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイス（またはサブインターフェイス）を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 12	**bgp-policy** {**source** | **destination**} **ip-prec-map** 例： `Device(config-if)# bgp-policy source ip-prec-map`	IP precedence を使用してパケットを分類します。
ステップ 13	**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 モードに戻ります。
ステップ 14	**ip bgp-community new-format** 例： `Device(config)# ip bgp-community new-format`	（任意）BGP コミュニティ番号を AA:NN（自律システム：コミュニティ番号/4 バイトの数）の形式で表示します。
ステップ 15	**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。

自律システム パス属性に基づいた BGP による QoS ポリシー伝搬の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **route-map***route-map-name* [**permit** | **deny** [*sequence-number*]]
4. **match as-path***path-list-number*
5. **set ip precedence** [*number* | *name*]
6. **exit**
7. **router bgp***autonomous-system*
8. **table-map***route-map-name*
9. **exit**
10. **ip as-path access-list***access-list-number* {**permit** | **deny**} *as-regular-expression*
11. **interface***typenumber*
12. **bgp-policy** {**source** | **destination**} **ip-prec-map**
13. **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***route-map-name* [**permit** | **deny** [*sequence-number*]] 例： `Device(config)# route-map rm1`	再配布を制御するためのルート マップを定義し、ルート マップ コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 4	**match as-path***path-list-number* 例： `Device(config-route-map)# match as-path 2`	ボーダー ゲートウェイ プロトコル（BGP）自律システム パス アクセス リストに照合します。
ステップ 5	**set ip precedence** [*number* | *name*] 例： `Device(config-route-map)# set ip precedence 5`	自律システム パスが一致するときの IP precedence フィールドを設定します。 （注） 優先順位の番号または名前を指定できます。
ステップ 6	**exit** 例： `Device(config-route-map)# exit`	ルート マップ 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。
ステップ 7	**router bgp***autonomous-system* 例： `Device(config)# router bgp 45000`	BGP プロセスをイネーブルにし、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 8	**table-map***route-map-name* 例： `Device(config-router)# table-map rm1`	BGP で学習したルートで IP ルーティング テーブルが更新される場合の、メトリックとタグの値を修正します。
ステップ 9	**exit** 例： `Device(config-router)# exit`	ルータ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**ip as-path access-list***access-list-number* {**permit** | **deny**} *as-regular-expression* 例： `Device(config)# ip as-path access-list 500 permit 45000`	自律システム パスのアクセス リストを定義します。
ステップ 11	**interface***typenumber* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイス（またはサブインターフェイス）を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 12	**bgp-policy** {**source** | **destination**} **ip-prec-map**	IP precedence を使用してパケットを分類します。

	コマンドまたはアクション	目的
	例： `Device(config-if)# bgp-policy source ip-prec-map`	
ステップ 13	**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。

アクセス リストに基づいた BGP による QoS ポリシー伝搬の設定

手順の概要

1. イネーブル化
2. **configure terminal**
3. **route-map***route-map-name* [**permit** | **deny** [*sequence-number*]]
4. **match ip address***access-list-number*
5. **set ip precedence** [*number* | *name*]
6. **exit**
7. **router bgp***autonomous-system*
8. **table-map***route-map-name*
9. **exit**
10. **access-list***access-list-number* {**permit** | **deny**} *source*
11. **interface***typenumber*
12. **bgp-policy** {**source** | **destination**} **ip-prec-map**
13. **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	**route-map***route-map-name* [**permit** | **deny** [*sequence-number*]] 例： `Device(config)# route-map rm1`	再配布を制御するためのルートマップを定義し、ルートマップコンフィギュレーションモードに入ります。
ステップ 4	**match ip address***access-list-number* 例： `Device(config-route-map)# match ip address 69`	アクセス リストを照合します。
ステップ 5	**set ip precedence** [*number* | *name*] 例： `Device(config-route-map)# set ip precedence routine`	自律システム パスが一致するときの IP precedence フィールドを設定します。
ステップ 6	**exit** 例： `Device(config-route-map)# exit`	ルートマップ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。
ステップ 7	**router bgp***autonomous-system* 例： `Device(config)# router bgp 45000`	ボーダーゲートウェイプロトコル（BGP）プロセスをイネーブルにし、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 8	**table-map***route-map-name* 例： `Device(config-router)# table-map rm1`	BGP で学習したルートで IP ルーティング テーブルが更新される場合の、メトリックとタグの値を修正します。
ステップ 9	**exit** 例： `Device(config-router)# exit`	ルータ コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 10	**access-list***access-list-number* {**permit** | **deny**} *source* 例： `Device(config)# access-list 69 permit 10.69.0.0`	アクセス リストを定義します。

	コマンドまたはアクション	目的
ステップ 11	**interface***typenumber* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイス（またはサブインターフェイス）を指定し、インターフェイス コンフィギュレーション モードに入ります。
ステップ 12	**bgp-policy** {**source** | **destination**} **ip-prec-map** 例： `Device(config-if)# bgp-policy source ip-prec-map`	IP precedence を使用してパケットを分類します。
ステップ 13	**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。

BGP による QoS ポリシー伝搬のモニタリング

BGP による QoS ポリシー伝搬機能の設定をモニタするには、次のオプション コマンドを使用します。

コマンドまたはアクション	目的
show ip bgp	適切なコミュニティがプレフィックスで設定されているかどうかを確認するために、ボーダー ゲートウェイ プロトコル（BGP）ルーティング テーブルのエントリを表示します。
show ip bgp community-list *community-list-number*	適切なプレフィックスが選択されているかどうかを確認するために、BGP コミュニティによって許可されたルートを表示します。
show ip cef *network*	シスコ エクスプレス フォワーディングのプレフィックスの優先値が適切かどうかを確認するために、指定された IP アドレスに基づいた転送情報ベース（FIB）テーブルのエントリを表示します。
show ip interface	インターフェイスに関する情報を表示します。
show ip route *prefix*	適切な優先値がプレフィックスで設定されていることを確認するために、ルーティング テーブルの現在のステータスを表示します。

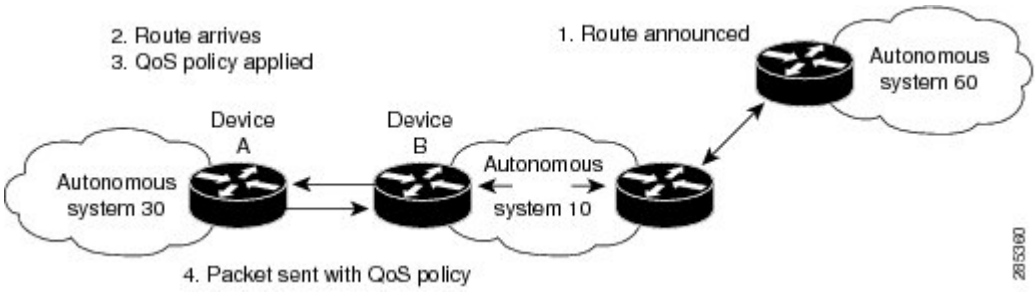
BGP による QoS ポリシー伝搬の設定例

例：BGP による QoS ポリシー伝搬の設定

次の例では、アクセスリスト、ボーダーゲートウェイプロトコル（BGP）コミュニティリスト、およびBGP自律システムパスを照合するためのルートマップを作成し、ネイバーから学習されたルートに IP precedence を適用する方法を示します。

次の図では、デバイスAが自律システム10と自律システム60からのルートを学習します。Quality of Service（QoS）ポリシーは、定義済みのルート マップに一致するすべてのパケットに適用されます。デバイス A から自律システム 10 または自律システム 60 へのパケットは、図の番号付きの手順が示すように、適切な QoS ポリシーで送信されます。

図 *8*：デバイスのルート学習と *QoS* ポリシーの適用



デバイス A の設定

```
interface serial 5/0/0/1:0
ip address 10.28.38.2 255.255.255.0
bgp-policy destination ip-prec-map
no ip mroute-cache
no cdp enable
frame-relay interface-dlci 20 IETF
router bgp 30
 table-map precedence-map
 neighbor 10.20.20.1 remote-as 10
 neighbor 10.20.20.1 send-community
!
ip bgp-community new-format
!
! Match community 1 and set the IP precedence to priority
route-map precedence-map permit 10
 match community 1
 set ip precedence priority
!
! Match community 2 and set the IP precedence to immediate
route-map precedence-map permit 20
 match community 2
 set ip precedence immediate
!
! Match community 3 and set the IP precedence to flash
route-map precedence-map permit 30
 match community 3
 set ip precedence flash
```

```
!
! Match community 4 and set the IP precedence to flash-override
route-map precedence-map permit 40
 match community 4
 set ip precedence flash-override
!
! Match community 5 and set the IP precedence to critical
route-map precedence-map permit 50
 match community 5
 set ip precedence critical
!
! Match community 6 and set the IP precedence to internet
route-map precedence-map permit 60
 match community 6
 set ip precedence internet
!
! Match community 7 and set the IP precedence to network
route-map precedence-map permit 70
 match community 7
 set ip precedence network
!
! Match ip address access list 69 or match autonomous system path 1
! and set the IP precedence to critical
route-map precedence-map permit 75
 match ip address 69
 match as-path 1
 set ip precedence critical
!
! For everything else, set the IP precedence to routine
route-map precedence-map permit 80
 set ip precedence routine
!
! Define community lists
ip community-list 1 permit 60:1
ip community-list 2 permit 60:2
ip community-list 3 permit 60:3
ip community-list 4 permit 60:4
ip community-list 5 permit 60:5
ip community-list 6 permit 60:6
ip community-list 7 permit 60:7
!
! Define the AS path
ip as-path access-list 1 permit ^10_60
!
! Define the access list
access-list 69 permit 10.69.0.0
```

デバイス B の設定

```
router bgp 10
 neighbor 10.30.30.1 remote-as 30
 neighbor 10.30.30.1 send-community
 neighbor 10.30.30.1 route-map send_community out
!
ip bgp-community new-format
!
! Match prefix 10 and set community to 60:1
route-map send_community permit 10
 match ip address 10
 set community 60:1
!
! Match prefix 20 and set community to 60:2
route-map send_community permit 20
 match ip address 20
 set community 60:2
!
! Match prefix 30 and set community to 60:3
route-map send_community permit 30
 match ip address 30
 set community 60:3
!
```

```
! Match prefix 40 and set community to 60:4
route-map send_community permit 40
 match ip address 40
 set community 60:4
!
! Match prefix 50 and set community to 60:5
route-map send_community permit 50
 match ip address 50
 set community 60:5
!
! Match prefix 60 and set community to 60:6
route-map send_community permit 60
 match ip address 60
 set community 60:6
!
! Match prefix 70 and set community to 60:7
route-map send_community permit 70
 match ip address 70
 set community 60:7
!
! For all others, set community to 60:8
route-map send_community permit 80
 set community 60:8
!
! Define access lists
access-list 10 permit 10.61.0.0
access-list 20 permit 10.62.0.0
access-list 30 permit 10.63.0.0
access-list 40 permit 10.64.0.0
access-list 50 permit 10.65.0.0
access-list 60 permit 10.66.0.0
access-list 70 permit 10.67.0.0
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
IP ルーティングのプロトコル独立型コマンド	『Cisco IOS IP Routing: Protocol-Independent Command Reference』
BGP の設定	『*BGP Configuration Guide*』
シスコ エクスプレス フォワーディングの設定	『*Cisco Express Forwarding Configuration Guide*』
専用アクセス レートの設定	『*QoS: Classification Configuration Guide*』（『Quality of Service Solutions Configuration Guide Library』の一部)の「Configuring Committed Access Rate」モジュール

関連項目	マニュアル タイトル
重み付けランダム早期検出の設定	『*QoS: Congestion Avoidance Configuration Guide*』（『Quality of Service Solutions Configuration Guide Library』の一部)の「Configuring Weighted Random Early Detection」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

BGP による QoS ポリシー伝搬の機能情報

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*：*BGP* による *QoS* ポリシー伝搬の機能情報

機能名	リリース	機能情報
BGP による QoS ポリシー伝搬		BGP による QoS ポリシー伝搬機能を使用すると、BGP コミュニティ リスト、BGP 自律システム パス、およびアクセス リストに基づいて IP precedence によってパケットを分類できます。パケットが分類されたら、専用アクセス レート（CAR）および重み付けランダム早期検出（WRED）など、その他の QoS 機能を使用してビジネス モデルに合うようにポリシーを指定および強化できます。
ポリシー ルーティングのインフラストラクチャ		ポリシー ルーティングのインフラストラクチャ機能により、シスコ エクスプレス フォワーディング（CEF）での IP ポリシーベース ルーティングのフル サポートが実現します。CEF により高速スイッチングが徐々に時代遅れになるに伴い、ポリシー ルーティングが CEF と統合され、増大するお客様のパフォーマンス要件に対応します。ポリシー ルーティングがイネーブルの場合、冗長な処理は回避されます。

第 20 章

NetFlow ポリシー ルーティング

NetFlow ポリシー ルーティング（NPR）は、トラフィック エンジニアリングとトラフィック分類をイネーブルにするポリシー ルーティングに、課金、キャパシティ プランニング、およびリアルタイムのトラフィック フローでの情報モニタリングを提供する NetFlow サービスを統合します。IP ポリシー ルーティングは、シスコ エクスプレス フォワーディング（旧称 CEF）、分散型シスコ エクスプレス フォワーディング（旧称 dCEF）、および NetFlow で使用します。

- 機能情報の確認，241 ページ
- NetFlow ポリシー ルーティングの前提条件，242 ページ
- NetFlow ポリシー ルーティングの制約事項，242 ページ
- NetFlow ポリシー ルーティングに関する情報，242 ページ
- その他の参考資料，244 ページ
- NetFlow ポリシー ルーティングの機能情報，245 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。

NetFlow ポリシー ルーティングの前提条件

NetFlow ポリシー ルーティングを機能させるには、次の機能がすでに設定されている必要があります。

- シスコ エクスプレス フォワーディング、分散型シスコ エクスプレス フォワーディング、または NetFlow
- ポリシー ルーティング

NetFlow ポリシー ルーティングの制約事項

- NetFlow ポリシー ルーティング（NPR）は、シスコ エクスプレス フォワーディングをサポートするシスコ プラットフォームでのみ使用可能です。
- 分散された転送情報ベース（FIB）に基づいたポリシー ルーティングは、分散型シスコ エクスプレス フォワーディングをサポートするプラットフォームでのみ使用可能です。
- **set ip next-hop verify-availability** コマンドは、CDP として知られていた Cisco Discovery Protocol データベースを分散型シスコ エクスプレス フォワーディングがサポートしないため、分散型シスコ エクスプレス フォワーディングでサポートされません。

NetFlow ポリシー ルーティングに関する情報

NetFlow ポリシー ルーティング

NetFlow ポリシー ルーティング（NPR）は、トラフィック エンジニアリングとトラフィック分類をイネーブルにするポリシー ルーティングに、課金、キャパシティ プランニング、およびリアルタイムのトラフィック フローでの情報モニタリングを提供する NetFlow サービスを統合します。IP ポリシー ルーティングは、シスコ エクスプレス フォワーディング（旧称 CEF）、分散型シスコ エクスプレス フォワーディング（旧称 dCEF）、および NetFlow で使用します。

NetFlow ポリシー ルーティングは、次のテクノロジーを利用します。

- シスコ エクスプレス フォワーディング。パケットをスイッチするときにルーティング テーブルではなく転送情報ベース（FIB）を参照し、デマンド キャッシング スキームのメンテナンス問題を解決します。
- 分散型シスコ エクスプレス フォワーディング。デマンド キャッシング スキームのスケーラビリティとメンテナンス問題を解決します。
- NetFlow。課金、キャパシティ プランニング、およびトラフィック モニタリング機能を実現します。

次に、NPR の利点を示します。

- NPR は新しいスイッチング サービスを利用します。シスコ エクスプレス フォワーディング、分散型シスコ エクスプレス フォワーディング、および NetFlow はポリシー ルーティングを使用できるようになりました。
- ポリシー ルーティングは広範囲の高速インターフェイスで導入できます。

NPR は、デフォルトのポリシー ルーティング モードです。シスコ エクスプレス フォワーディング、分散型シスコ エクスプレス フォワーディング、または NetFlow でポリシー ルーティングをイネーブルにするために、追加の設定タスクは必要ありません。これらの機能のいずれかがオンになるとすぐに、パケットは自動的に適切なスイッチング パスでポリシー ルーティングの対象になります。

次の例は、シスコ エクスプレス フォワーディングを使用してポリシー ルーティングを設定する例を示します。デバイスがポリシー ルーティングを試行する前に、test という名前のルート マップのネクスト ホップ 10.0.0.8 が Cisco Discovery Protocol ネイバーであることを確認するように、ルートが設定されます。

```
Device(config)# ip cef
Device(config)# interface GigabitEthernet 0/0/1
Device(config-if)# ip route-cache flow
Device(config-if)# ip policy route-map test
Device(config-if)# exit
Device(config)# route-map test permit 10
Device(config-route-map)# match ip address 1
Device(config-route-map)# set ip precedence priority
Device(config-route-map)# set ip next-hop 10.0.0.8
Device(config-route-map)# set ip next-hop verify-availability
Device(config-route-map)# exit
Device(config)# route-map test permit 20
Device(config-route-map)# match ip address 101
Device(config-route-map)# set interface Ethernet 0/0/3
Device(config-route-map)# set ip tos max-throughput
Device(config-route-map)# exit
```

ネクストホップの到達可能性

デバイスがネクスト ホップへのポリシー ルーティングを実行する前に、ルート マップのこのネクスト ホップの到達可能性を検証するためにポリシー ルーティングを設定するには、**set ip next-hop verify-availability** コマンドを使用できます。このコマンドには、次の制限があります。

- これによりパフォーマンスが低下する可能性があります。
- Cisco Discovery Protocol をインターフェイスでイネーブルにする必要があります。
- 直接接続されるネクスト ホップは Cisco Discovery Protocol がイネーブルになったシスコ デバイスである必要があります。
- これは、分散型シスコ エクスプレス フォワーディングの設定とは機能しません。

デバイスがポリシーを使用してネクスト ホップにパケットをルーティングしているときに、ネクスト ホップがダウンしている場合、デバイスはアドレス解決プロトコル（ARP）の使用を試行し

ますが失敗します。この動作はいつまでも続く可能性があります。デバイスで **set ip next-hop verify availability** コマンドを設定することで、この動作を防止できます。このコマンドは、ネクストホップにパケットをルーティングする前に、最初に、このネクストホップがそのデバイスの Cisco Discovery Protocol ネイバーであることを（ルート マップを使用して）確認します。ただし、ネクスト ホップが Cisco Discovery Protocol ネイバーではないデバイスでこのコマンドを設定すると、デバイスは後続のネクストホップを参照します（ある場合）。使用可能なネクストホップがない場合、パケットはポリシーを使用してルーティングされません。メディアまたはカプセル化の一部で Cisco Discovery Protocol がサポートされないため、この設定はオプションです。

set ip next-hop verify availability コマンドが設定されていない場合、パケットはポリシー ルーティングされるか、永続的にルーティングされないまま残ります。

いくつかのネクストホップだけの可用性を確認する場合、異なる基準（アクセス リストの照合またはパケット サイズの照合を使用）で異なるルート マップ エントリ（同じルート マップ名）を設定し、選択的に **set ip next-hop verify availability** コンフィギュレーション コマンドを使用することもできます。

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 IOS Master Command List, All Releases』
IP ルーティングのプロトコル独立型コマンド	『Cisco IOS IP Routing: Protocol-Independent 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

NetFlow ポリシー ルーティングの機能情報

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 *19*：*NetFlow* ポリシー ルーティングの機能情報

機能名	リリース	機能情報
NetFlow ポリシー ルーティング		NetFlow ポリシー ルーティング（NPR）は、ポリシー ルーティングに NetFlow サービスを統合し、トラフィック エンジニアリングとトラフィック分類をイネーブルにします。NetFlow サービス により、課金、キャパシティ プランニング、およびリアルタイムのトラフィック フローでの情報モニタリングが実現されます。IP ポリシー ルーティングは、シスコ エクスプレス フォワーディング、分散型シスコ エクスプレス フォワーディング、および NetFlow と連携します。
ポリシー ルーティングのインフラストラクチャ		ポリシー ルーティングのインフラストラクチャ機能により、シスコ エクスプレス フォワーディングおよび NetFlow での IP ポリシーベース ルーティングのフル サポートが実現します。ポリシー ルーティングと NetFlow の両方がイネーブルの場合、冗長な処理が回避されます。

第 21 章

再帰スタティック ルート

再帰スタティック ルート機能を使用すると、スタティック ルートのネクストホップ アドレスまたは宛先ネットワーク自体が、学習済みルートの一部としてRIBですでに使用可能な場合にも、ルーティング情報ベース（RIB）に再帰スタティック ルートをインストールすることができます。このモジュールでは、再帰スタティック ルートについて説明し、再帰スタティック ルート機能を設定する方法について説明します。

- 機能情報の確認，247 ページ
- 再帰スタティック ルートの制約事項，248 ページ
- 再帰スタティック ルートに関する情報，248 ページ
- 再帰スタティック ルートのインストール方法，248 ページ
- 再帰スタティック ルートの設定例，252 ページ
- 再帰スタティック ルートに関する追加情報，254 ページ
- 再帰スタティック ルートの機能情報，254 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。

再帰スタティック ルートの制約事項

再帰スタティックルートがルートマップを使用してイネーブルになっている場合、仮想ルーティングおよび転送（VRF）インスタンスまたはトポロジごとに 1 つのルート マップだけを入力できます。2 つめのルート マップが入力されると、新しいマップで以前のマップが上書きされます。

再帰スタティック ルートに関する情報

再帰スタティック ルートのインストール方法

VRF での再帰スタティック ルートのインストール

特定の仮想ルーティングおよび転送（VRF）インスタンスに再帰スタティックルートをインストールするには、次の手順を実行します。任意の数の VRF に再帰スタティック ルート機能を設定できます。特定の VRF に再帰スタティック ルートをインストールすると、ネットワークの残りの部分にデフォルトの RIB 動作（再帰スタティック ルートの削除）を維持することができます。

手順の概要

1. イネーブル化
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **address-family** {**ipv4** | **ipv6**}
6. **exit**
7. **exit**
8. **ip route** [**vrf** *vrf-name*] *prefix mask ip-address*
9. **ip route static install-routes-recurse-via-nexthop** [**vrf** *vrf-name*]
10. **end**
11. **show running-config | include install**
12. **show ip route 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	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`	仮想ルーティングおよび転送（VRF）ルーティング テーブル インスタンスを作成し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 100:1`	VRF インスタンスのルート識別子を指定します。
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 IPv4 または IPv6 アドレス ファミリを指定します。
ステップ 6	**exit** 例： `Device(config-vrf-af)# exit`	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 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	**ip route** [**vrf** *vrf-name*] *prefix mask ip-address* 例： `Device(config)# ip route vrf vrf1 10.0.2.0 255.255.255.0 10.0.1.1`	特定の VRF インスタンスに対するスタティック ルートを設定します。
ステップ 9	**ip route static install-routes-recurse-via-nexthop** [**vrf** *vrf-name*] 例： `Device(config)# ip route static install-routes-recurse-via-nexthop vrf vrf1`	特定の VRF インスタンスの RIB にインストールするために、再帰スタティック ルートをイネーブルにします。
ステップ 10	**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 11	**show running-config | include install** 例： `Device# show running-config | inc install`	すべての再帰スタティック ルート コンフィギュレーションを表示します。
ステップ 12	**show ip route vrf** *vrf-name* 例： `Device# show ip route vrf vrf1`	特定の VRF に関連付けられた IP ルーティング テーブルを表示します。

ルート マップを使用した再帰スタティック ルートのインストール

ルート マップで定義された仮想ルーティングおよび転送（VRF）インスタンスに再帰スタティック ルートをインストールするには、この作業を実行します。ネットワークの特定の範囲にのみ再帰スタティック ルートをインストールする場合は、このタスクを実行できます。**route-map** キーワードが **vrf** キーワードなしで使用される場合、ルート マップで定義される再帰スタティック ルートはグローバル VRF またはトポロジに適用されます。

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. **exit**
7. **exit**
8. **ip route** [**vrf** *vrf-name*] *prefix mask ip-address*
9. **access-list** *access-list-number* **permit** *source* [*source-wildcard*]
10. **route-map** *map-tag*
11. **match ip address** *access-list-number*
12. **exit**
13. **ip route static install-routes-recurse-via-nexthop** [**vrf** *vrf-name*] [**route-map** *map-name*]
14. **end**
15. **show running-config | include install**
16. **show ip route 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 definition** *vrf-name* 例： `Device(config)# vrf definition vrf1`	仮想ルーティングおよび転送（VRF）ルーティング テーブル インスタンスを作成し、VRF コンフィギュレーション モードを開始します。
ステップ 4	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 100:1`	VRF インスタンスのルート識別子を指定します。
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 IPv4 または IPv6 アドレスファミリ タイプを指定します。
ステップ 6	**exit** 例： `Device(config-vrf-af)# exit`	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 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	**ip route** [**vrf** *vrf-name*] *prefix mask ip-address* 例： `Device(config)# ip route vrf vrf1 10.0.2.0 255.255.255.0 10.0.1.1`	特定の VRF インスタンスに対するスタティック ルートを設定します。
ステップ 9	**access-list** *access-list-number* **permit** *source* [*source-wildcard*] 例： `Device(config)# access-list 10 permit 10.0.2.0 255.255.255.0`	変換する必要があるアドレスを許可する標準アクセス リストを定義します。

	コマンドまたはアクション	目的
ステップ 10	**route-map** *map-tag* 例： `Device(config)# route-map map1`	ルートの再配布を制御するためのルート マップを定義し、ルート マップ コンフィギュレーション モードに入ります。
ステップ 11	**match ip address** *access-list-number* 例： `Device(config-route-map)# match ip address 10`	標準または拡張アクセスリストで許可された宛先ネットワーク アドレスを持つルートを照合します。
ステップ 12	**exit** 例： `Device(config-route-map)# exit`	ルート マップ コンフィギュレーション モードを終了します。
ステップ 13	**ip route static install-routes-recurse-via-nexthop** [**vrf** *vrf-name*] [**route-map** *map-name*] 例： `Device(config)# ip route static install-routes-recurse-via-nexthop vrf vrf1 route-map map1`	ルート マップで定義された再帰スタティック ルートの特定の VRF の RIB へのインストールをイネーブルにします。
ステップ 14	**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。
ステップ 15	**show running-config | include install** 例： `Device# show running-config | inc install`	すべての再帰スタティック ルート コンフィギュレーションを表示します。
ステップ 16	**show ip route vrf** *vrf-name* 例： `Device# show ip route vrf vrf1`	特定の VRF に関連付けられた IP ルーティング テーブルを表示します。

再帰スタティック ルートの設定例

•

例：VRF での再帰スタティック ルートのインストール

次に、特定の仮想ルーティングおよび転送インスタンスに再帰スタティック ルートをインストールする例を示します。**vrf** キーワードを使用して、再帰スタティック ルートが、指定された VRF のルーティング情報ベース（RIB）にのみインストールされるようにすることができます。ネットワークの残りの部分では、RIB に再帰スタティック ルートをインストールしないというデフォルトの動作が維持されます。次の例は、vrf1 の RIB に 10.0.0.0/8 ルートがすでにダイナミックまたはスタティックにインストールされているという想定に基づいています。

```
Device> enable
Device# configure terminal
Device(config)# vrf definition vrf1
Device(config-vrf)# rd 1:100
Device(config-vrf)# address-family ipv4
Device(config-vrf-af)# exit
Device(config-vrf)# exit
Device(config)# ip route vrf vrf1 10.0.2.0 255.255.255.0 10.0.1.1
Device(config)# ip route static install-routes-recurse-via-nexthop vrf vrf1
Device(config)# end
```

例：ルート マップを使用した再帰スタティック ルートのインストール

ルーティング情報ベース（RIB）にルート マップで定義された再帰スタティック ルートをインストールするには、**route-map** キーワードを使用します。また、指定された VRF だけにルート マップが適用されるようにするために、特定の仮想ルーティングおよび転送（VRF）インスタンスのルート マップを指定することもできます。次の例では、特定の VRF のルート マップが指定されます。次の例は、vrf1 の RIB に 10.0.0.0/8 ルートがすでにスタティックまたはダイナミックにインストールされているという想定に基づいています。

```
Device> enable
Device# configure terminal
Device(config)# vrf definition vrf1
Device(config-vrf)# rd 100:2
Device(config-vrf)# address-family ipv4
Device(config-vrf-af)# exit
Device(config-vrf)# exit
Device(config)# access-list 10 permit 10.0.2.0 255.255.255.0
Device(config)# route-map map1
Device(config-route-map)# match ip address 10
Device(config-route-map)# exit
Device(config)# ip route static install-routes-recurse-via-nexthop vrf vrf1 route-map map1
Device(config)# ip route vrf vrf1 10.0.2.0 255.255.255.0 10.0.1.1
Device(config)# ip route vrf vrf1 10.0.3.0 255.255.255.0 10.0.1.1
Device(config)# end
```

上記の例では、ルート 10.0.2.0 255.255.255.0 10.0.1.1 は RIB にインストールされますが、ルート 10.0.3.0 255.255.255.0 10.0.1.1 はルートマップで定義されたネットワークと一致しないため、RIB にインストールされません。

再帰スタティック ルートに関する追加情報

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』
IP ルーティングのプロトコル独立型コマンド	『Cisco IOS IP Routing: Protocol-Independent 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

再帰スタティック ルートの機能情報

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 *20*：再帰スタティック ルートの機能情報

機能名	リリース	機能情報
再帰スタティック ルート	Cisco IOS XE Release 3.9S	再帰スタティック ルート機能を使用すると、スタティック ルートのネクストホップ アドレスまたは宛先ネットワーク自体が、学習済みルートの一部としてRIBですでに使用可能な場合にも、ルーティング情報ベース（RIB）に再帰スタティック ルートをインストールすることができます。 次のコマンドが導入されました。**ip route static install-recurse-via-nexthop**